Aalto University
School of Science
Master's Programme in Computer, Communication and Information Sciences

Anton Keskisaari

Cybercrime in cloud environments:
Tactics, techniques and procedures

Master's Thesis
Espoo, December 21th, 2021

Supervisor: Professor Tuomas Aura, Aalto University
Advisor: Johannes Töyli, M.Econ, F-Secure Oyj

Aalto University
School of Science
Master's Programme in Computer, Communication and Information Sciences

ABSTRACT OF MASTER'S THESIS

Author: Anton Keskisaari

Title:
Cybercrime in cloud environments: Tactics, techniques and procedures

Date: December 21th, 2021 **Pages:** 91

Major: Computer Science **Code:** SCI3084

Supervisor: Professor Tuomas Aura

Advisor: Johannes Töyli, M.Econ, F-Secure Oyj

Cloud services have become a prevalent part of the IT infrastructure that organizations work with. These services also offer cybercriminals new ways to operate. In this thesis, we map the evolution of cybercrime in cloud environments. The aim is to understand the ways in which cybercriminals attack different cloud environments, how the services are misused, and how cloud is changing the way in which cybercriminals work.

We present case studies on the threat actors' operations changing over time as well as the evolution of initial access attack techniques on platforms where reports on a specific threat actor's operations are not available.

The evolution shows a clear trend towards more diverse and wide spread use of cloud services for the different parts of the attack kill chain. Cloud offers cybercriminals a host of benefits. Attackers have adopted the cloud services to blend into benign traffic, and they use the cloud functionality to perform malicious activity. The cloud is used as a malware hosting platform, as a malware delivery channel, as a phishing platform, and as a channel for command and control. Misconfiguration abuse and cloud-delivered phishing emails are some of the most common initial access vectors into cloud environments. Cloud supply chain attacks and cloud service feature and trust abuse are amongst the most critical attack paths currently and for the future.

Keywords: cyber security, cybercrime, cloud services, threat intelligence

Language: English

Aalto-yliopisto
Perustieteiden korkeakoulu
Tieto-, tietoliikenne- ja informaatiotekniikan maisteriohjelma

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä:	Anton Keskisaari		
Työn nimi:	Tietoturvarikollisuus pilvipalveluissa: Taktiikat, tekniikat ja prosessit		
Päiväys:	21. joulukuuta 2021	**Sivumäärä:**	91
Pääaine:	Tietotekniikka	**Koodi:**	SCI3084
Valvoja:	Professori Tuomas Aura		
Ohjaaja:	KTM Johannes Töyli, F-Secure Oyj		

Pilvipalveluista on tullut vallitseva osa organisaatioiden IT ympäristöistä. Palvelut tarjoavat myös kyberrikollisille uusia tapoja toimia. Tässä tutkimuksessa kartoitamme kyberrikollisten toimintaa ja toimintatapojen kehitystä viime vuosina. Tavoitteena on ymmärtää tavat, joilla kyberrikolliset hyökkäävät pilviympäristöjä vastaan, kuinka palveluita väärinkäytetään ja kuinka ne muokkaavat kyberrikollisten toimintaa.

Esitämme tapaustutkimuksia eri kyberrikollisryhmien operaatioiden muutoksista ja lisäksi hyökkäyksien alun tunkeutumistapoja alustoilla, joilla toimivien yksittäisten toimijoiden operaatioista ei ole saatavilla raportteja.

Tutkimus osoittaa, että kehityksessä on selkeä suunta monimuotoisempaan ja laajalle levittäytyvään pilvipalveluiden hyväksikäyttöön hyökkäys ketjujen eri vaiheissa. Pilvipalvelut tarjoavat kyberrikollisille paljon hyötyjä. Hyökkääjät ovat omaksuneet palveluntarjonnan avukseen rikollisen toimintansa tueksi. Niitä käytetään haittaohjelmien isännöintiin, haittaohjelmien levitykseen, tietojen kalasteluun ja komento ja kontrolli yhteyksiin. Virheellisten asetusten hyväksikäyttö ja pilvipalveluiden kautta lähetetyt kalasteluviestit ovat hyökkääjien yleisimmin käyttämiä hyökkäysvektoreita pilviympäristöihin kohdistetuissa hyökkäyksissä. Pilven toimitusketjut, palveluiden ominaisuuksien ja luottamuksen hyväksikäyttö ovat kriittisimpiä hyökkäyspolkuja nykyisellään sekä tulevaisuudessa.

Asiasanat:	kyberturvallisuus, kyberrikollisuus, pilvipalvelut, uhkatieto
Kieli:	Englanti

Acknowledgements

The work on this thesis was supported by the CC-DRIVER project which has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543. This thesis served as the basis for my contributions to the CC-DRIVER project researching cybercriminality.

I would like to thank F-Secure for the opportunity and the support to conduct my research. Thanks to Johannes Töyli for being the advisor to my thesis and Sami Ruohonen and others for comments and guidance to keep me on track.

Finally, thanks to my family and friends for all the unconditional support over the years.

Helsinki, December 21th, 2021

Anton Keskisaari

Contents

Chapter 1

Introduction

Using cloud services has become a prevalent way of working and the service offerings are constantly evolving. From simple web services to fully fledged corporate infrastructure, almost everything can be rented out and used as a pay-per-use service. This move to the cloud has given businesses considerable benefits for scalability and ease of maintenance, but along with it have come new challenges in the form of complexity and width and in some cases lack of control.

The rapid development and adoption of cloud services has not gone unnoticed by the cybercriminals. Similarly for them, the new platforms and services have brought new possibilities, more attack surface and offered them new tools for operating. In this thesis, we try to map the ways modern cyber criminals maneuver in the cloud environments, what kinds of tactics, techniques and procedures they are using and how they are evolving and adapting to the constantly changing sphere of the cloud. By analysing cybercriminal actions in the cloud environments, we also aim to recognise some of the key problems that enable the attacks and abuse to take place.

1.1 Problem statement

The rapid development and evolution of cloud services is constantly creating new ways for the criminals to abuse the systems, and it is difficult for the defenders to stay ahead in this development, given that most companies are not evolving with security as their primary objective. In order to have the edge in this competition, defenders need to have a coherent understanding of the cloud threat landscape, thus it is necessary to do research on the actions of the criminals.

Cloud adoption is changing the attack surfaces and the whole network

environment. Corporate servers are not located deep in the server rooms of the headquarters but are hosted by a third party. Listing the company computational assets is not as simple as counting the server racks in the basement. Developers are now capable of starting up new server instances, and users are installing cloud apps with ease but the streamlined process can cause problems with asset management when IT department is not informed. The use of cloud services combined with on-premise infrastructure increases the complexity of responsibilities. It can be unclear who is responsible for what.

Service providers are offering companies a variety of cloud services with different benefits to better their business: reduced costs, scalability, continuity, security and so forth. Same can be said for cybercriminals: new attack surfaces, new delivery methods and new ways to blend in. As cloud adoption progresses, moving to the cloud seems to be the obvious choice for cybercriminals as well. As cybercriminals are shifting their targets, they are also evolving their attack vectors and techniques of compromise. This shift from on-premise targets to cloud hosted targets brings some changes and new opportunities for the attackers. Publicly offered cloud services allow the attackers to use the same platforms and services as the targets they are attacking. The use of external services that are also used by the attackers pose new challenges in the attack prevention and detection. Attacker detection in the scope of cloud applications can no longer rely only on detecting the known bad including the use of common attacker tools and techniques (e.g. mimikatz [1], kerberoasting [2]). Admins use the same functionality that the attackers use, meaning detecting the malicious activity becomes a question of behavioural analysis and context, which is then again harder to scale [3].

Cloud is turning out to be the primary way of malware delivery, Netskope Threat Labs found in their research in 2020 that 61% of all malware was delivered via cloud applications[4]. In the newer edition of the report [5], they show that the number grew even more to 68%, with cloud storage applications representing the vast majority. These numbers alone tell the story of the effectiveness of cloud services as a part of the attackers' toolset as well as the level of cloud adoption by the attackers. As the attackers have reframed their traditional attack methods with the use of cloud services, analysing the shift of the tactics, techniques and procedures will help us to tackle the problems that enable the attacks to happen. In this thesis, we try to uncover the progression cybercriminals are going through to shift their focus to the cloud, and we aim to map their main tactics, techniques and procedures in attacking cloud environments.

1.2 Structure of the Thesis

In the second chapter we will briefly introduce the concept of cybercrime to help define the scope of this research. The third chapter will detail the tools and material used in the thesis, underlining the limitations of available data the research. The fourth chapter will give an overview of cloud including the service, deployment, and responsibility models. Understanding the models is crucial to grasp the responsibilities of the defender. Using these models, we can also identify potential weak points. The fifth chapter gives an overview of the current cloud threat landscape referencing the newest reports and publications in the field. The sixth chapter is comprised of case studies detailing the threat actors' developments moving to target cloud and reviewing analysis reports and news on cybercriminal activity. The case studies present different types of cybercriminal groups' actions in different cloud environments and different niches of cybercrime in the cloud. The seventh chapter presents findings based on the case studies, discussing cloud environments as targets, the evolution of attacks on different environments, the problems that enable the attacks and some expectations for the future. The final chapter offers the conclusions, a summary of the research as well its limitations. At the end we present some ideas for future research on cybercriminal activity in the cloud environments.

Abbreviations

ACK	Acknowledgement, a TCP handshake packet
API	Application Programmin Interface
APT	Advanced Persistent Threat
C2	Command and Control
CSP	Content Security Policy, a web security standard to prevent injection attacks
DKIM	DomainKeys Identified Mail
DNS	Domain Name System
HW	Hardware
IAB	Initial Access Broker
IAM	Identity and Access Management
IDN	Internationalized Domain Name
IMAP	Internet Message Access Protocol
IoC	Indicator of Compromise
IRC	Internet Relay Chat
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
OAuth	Open Authorization, an access delegation standard
POP3	Post Office Protocol version 3
POS	Point Of Sale
TCP	Transmission Control Protocol
TTP	Tactics, Techniques and Procedures, used in describing threat actor actions
SAML	Security Assertion Markup Language
SPF	Sender Policy Framework
SSL	Secure Sockets Layer
SSO	Single Sign On
SSRF	Server-Side Request Forgery
SYN	Synchronize, a TCP handshake packet
SW	Software

TLD	Top Level Domain
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Recourse Locator
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
XSS	Cross-Site Scripting

Chapter 2

Cybercrime

Cybercrime has been a loosely defined term used to describe different criminal activity, but in order to use it in a research context we need to have a clear definition of it and the scope in which it is used in this thesis.

For example, the U.S. Department of Justice(DOJ) has a wide definition of computer crime or cybercrime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution"[6]. Additionally, it uses a three-part division to describe cybercrime:

1. Computer (HW/SW) is the target (e.g. theft)
2. Computers is used to attack other computer systems
3. Computer is used as a instrument to commit traditional crime

Cybercrime in the context of this thesis also needs to be differentiated from government backed cyber espionage that can be categorized to be a subclass of cybercrime. This thesis focuses on financially motivated cybercrime that is primarily not linked to any governmental actor or agency. Examples of cybercrime discussed in this thesis include email fraud, theft of credit card data, ransomware attacks and cryptojacking.

Generally, the attack types presented in this research are attacks against computer systems or attacks using computers with the aim to deceive people for financial gain. These attacks also differ in their targeting methods. Some attacks are highly targeted, aimed at high value targets and require a reasonably high level of technical capabilities, whereas other attacks are opportunistic attempts of mass exploitation.

Cloud and cybercrime. The cloud element brings new dimensions to the cybercrime operations. In this thesis, we focus on the embodiments of

cybercrime that include the use of cloud services or attacks that are directly or indirectly attacking cloud environments. This can include singular cloud-related techniques aiding in the execution of different tactics or, for example, attacks conducted solely using cloud applications and functionality.

Chapter 3

Methods

3.1 Tools for the study

The research was done with tactics, techniques and procedures (TTP) evolution in mind, thus threat actor specific case studies were chosen to highlight the changes the attackers have made in their attack operations. After reviewing the available material (e.g., public reports) on attacks, it became clear that threat actor specific evolution would not suffice in all categories of attack tactics and platform types that were of interest. Because of this, in the case of attacks targeting SaaS platforms (e.g., phishing) a more broad view of the attack techniques is covered, although attack examples are also included.

In order for us to be able to discuss the tactics and techniques of the attackers in a coherent manner, we use the Mitre ATT&CK framework. It is a framework based on observations of real attacker actions and is a widely used knowledge base for threat intelligence research. The ATT&CK framework enables us to identify the attacker tactics and techniques in a way that is easily understandable for anyone familiar with the framework. The ATT&CK matrices for different cloud platforms are limited, but we used them jointly with the enterprise matrix when appropriate. Since cloud environments include many of the same components as traditional on-premise environments, many of the attack techniques used in the cloud are the same.

3.2 Case study material

For the case studies, we use publicly available threat intelligence material: analysis reports, articles and news. Due to the fact that we use only open-source reports and material for the case studies, we have to make a notion

about the bias in the research material: the material does not fully cover the field of study. It is clear that, because of the nature of the subject (criminal cyberattacks in the cloud), all types of attacks are not reported and publicly disclosed the way we would hope. Some attack types (e.g., attacks aiming to deploy ransomware) are largely underrepresented in the publicly disclosed reporting. We can expect this to be due to the sensitivity of the topic: organizations are not comfortable with fully disclosing the details of the attacks that have taken place and making the incident response reports publicly readable. Publicly disclosing these type of attacks might also pose security or legal risks for the companies. Furthermore, other types of attacks including cryptomining attacks are easier to study using honeypot infrastructure and observe the attackers. In the case of ransomware, this is not feasible in the same way as setting up a seemingly legitimate organization with a mature infrastructure is not an easy task. We still think that this is not a major problem regarding this study as we do have a good view into the initial attack vectors used by all attackers, including ransomware operators. Material on attackers' actions (both automated and hands-on-keyboard actions) after the initial compromise of the victim networks is not as available as one would hope.

It is only the actions of a hands-on-keyboard attackers in the victim network or the material covering them is not as widely available as one would hope.

Case study material also differs based on the platform context. Detailed reports that attribute the attacks to distinct threat actors are more common for IaaS platforms and less common for SaaS applications. This is likely due to the differences in the nature of the data gathered from the platforms and the feasibility of honeypot style data harvesting.

Chapter 4

Cloud services

Cloud is a term often used by software developers and security engineers, but it can be unclear what is meant by it. In different contexts it can mean many things. In the corporate world, it might point to the platforms offered by big tech companies or in the case of a private person, it might signify specific applications for the end user. In this thesis we use the term cloud in a broad way that is context specific and is not limited to one type of cloud. As attackers do not limit themselves to a single type of cloud (model), we will also view their actions in the cloud with a wider lens, not limiting our view. In this chapter we introduce important concepts and models to better understand the many contexts of cloud.

4.1 Service models

In order to best understand attack tactics and techniques in the cloud environments, we need to understand how the services work. Cloud services can be divided into three main service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). These service models offer services with level of control for the customer. For instance, the service model dictates how much responsibility and access the customer has to the administrative tools of the service. The models also have varying security implications and this is critical to understand in order to secure the systems adequately.

Infrastructure-as-a-Service (IaaS) is a service model offering customers servers, storage and virtualization. The service provider manages the physical infrastructure, including the data center, networks, computer hardware, virtualization platform and virtualized computing resources. The cloud cus-

tomer has the access and control of the overlaying virtual machines, operating systems and storage. The customer has full ability to manage and deploy these virtual machines and their operation and they are also responsible for the security of those virtual machines. The deployment and management is usually done using a command-line-interface (CLI) or a web based interface. IaaS solutions offer ease of deployment, ability to scale and control over the fine details, but they come with the burden of responsibility over for example patching operating systems and software. [7]

Platform-as-a-Service (PaaS) is a service model offering customers a managed platform on which they can build their environment. Similar to IaaS, the service provider manages the underlying infrastructure, but in the PaaS model the service provider manages the virtual machines and applications. The customer is able to manage, provision and run the platform and its applications but does not need to build or maintain the application installations or the infrastructure underneath. PaaS solutions generally offer auto-scaling options and integrate with other services and databases. [7]

Software-as-a-Service (SaaS) is a service model that offers the client subscription or pay-per-use based applications or services fully managed by the service provider. These applications make it easy for an organization to take on new technology without investing in the underlying infrastructure or management. These applications can vary in scale, ranging from single user applications to ones with hundreds of millions of users. [7]

4.2 Shared responsibility model

The three cloud service models also imply sets of responsibilities for the cloud provider and the customer. A clear division of responsibility areas is important in order to secure the systems. The way responsibilities are shared between the cloud provider and customer varies by the service model but also by provider, as every provider has its own services, security mechanisms and protections[8].

Responsibility can be modeled on three different main levels: low-level (consisting of physical and infrastructural elements), mid-level (consisting of virtual machines, operating systems, runtimes etc.), and high-level (consisting of the application level). Data and access security is always the responsibility of the customer.

In the traditional on-premise data center model, the customer (the owner, controller and user) is responsible for all aspects of the data center security.

On the low level, this includes the physical security of the environment including the data center, perimeter network and virtualization platform. In the IaaS model, the low level is considered to be the responsibility of the service provider, while the higher levels are on the responsibility of the cloud customer. In the PaaS model, the service provider takes care of the mid-level including the platform software, operating system, local networking and virtual instances. In the SaaS model, the model with the least amount of customer responsibility, the cloud customer is only responsible for the data security and access. Overall, the more flexibility the service has, the more responsibility the cloud customer has. The actual responsibilities vary depending of the implementation and type of service.[8] See figure 4.1 for an illustration of the division of the responsibilities.

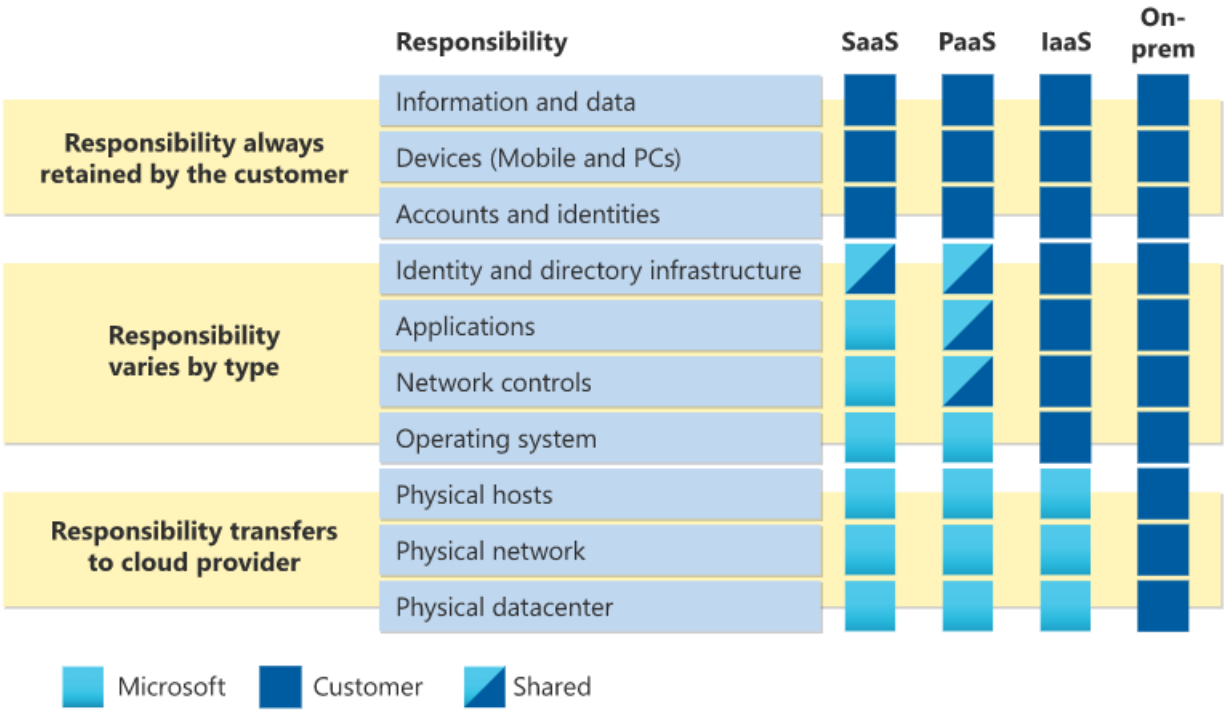

Figure 4.1: Shared responsibility model[9]

4.3 Deployment models

The cloud deployment models offer varying practical advantages and features, and each has its own drawbacks.Similarly to the shared responsibility

models, deployment models offer varying levels of control for the user or customer, private cloud offering the most control, public cloud the least, and hybrid and community cloud being somewhere between, depending on the setup.

In the public cloud model, the cloud infrastructure is owned by a cloud service provider and rents it to the general public. The usage is scalable to the needs of the customer as the service provider manages pooled resources. Public cloud offers high availability and ease of setup and scalability.[10]

Private cloud infrastructure is exclusively in the use of one organization. It can be hosted by a third-party provider or the organization itself, and it can be hosted either on premise or off premise. Generally, private cloud offers more control and better privacy than public cloud.[10]

Community cloud deployments aim to reduce the overhead of setting up private cloud whilst retaining the improved control and privacy that private cloud offers. Community cloud is a private cloud shared by multiple organizations with common interests. It does not offer the same scalability as public cloud.[10]

Hybrid cloud deployments make combined use of different connected cloud services, including public and private cloud. Hybrid cloud offers the benefits of agility and security by allowing the organization to benefit from the scalability of the public cloud for hosting applications that do not require strict privacy while keeping some key components of the business in private cloud for added safety.[10]

4.4 Extensions

Different cloud service providers offer different types of services and platforms that often allow additional extensions to the application or external services to the workflow. In the cloud, these applications are generally using OAuth for permission delegation and authorization. OAuth is an open standard for authorization. It allows the user to give an application or service access to their personal information on the platform without sharing their password with the application. It works by providing the applications or APIs with access tokens.[11]

Many cloud services include the possibility to install OAuth applications. These are third party developed applications that implement additional func-

tionality for the specific cloud service. These applications can create security risks as many service providers allow installing applications via side loading (i.e., directly from the application source, not through the official app store for the service)[12].

Chapter 5

Threat landscape

Organizations are moving their infrastructure to the cloud and increasingly utilizing cloud environments for accelerating, scaling and optimizing their operations. Understanding how this changes the threat landscape is critical. In this chapter we outline the main features of the cloud threat landscape based on public cloud threat landscape reports and other research reports. We cover the general threats cloud environments face, including the threat actors and attack types.

5.1 Threat actors

In their 2020 Cloud Threat Landscape report [13], IBM Security reported that according to their findings financially motivated cybercriminals are the most prevalent group targeting cloud environments. They also note nation state actors to be a persistent risk, but financially motivated cybercriminals still account for the the majority of the attacks targeting cloud systems.

The list of known threat actors targeting cloud systems include groups pursuing phishing operations (e.g., MexOAuth/TA2552), illicit cryptomining (e.g., TeamTNT, Rocke group, Pacha group), formjacking (e.g., Magecart groups), ransomware (e.g., BlackMatter). Overall a multitude of threat actors are using cloud to host parts of their operations. The list of threat actors using cloud applications for malware delivery and hosting is likely exceedingly long as cloud applications (especially cloud storage applications) represent the majority in malware delivery methods [4].

5.2 Attacks and attack vectors

An IBM report [13] noted that the largest part of the cybercriminal attacks targeting cloud environments are opportunistic attacks executed in an automated manner. These automated attacks trying to access cloud assets and harvest credentials also line up with the cloud access sales happening on the underground darknet forums and marketplaces. Research [14] has shown that the different criminal actors have been moving increasingly into specialized roles. For example ransomware operators are buying access from initial access brokers (IAB) from the darknet marketplaces.

Cloud environments and services differ largely, but in general it can be said that the emergence of the cloud has broadened the attack surface. Organizations running their systems on IaaS solutions are still facing the same problems of patching servers and public facing applications. The addition of PaaS- and SaaS-type solutions has given the attackers new avenues for abusing the features of the services. Next we will list some of the major attack vectors used to compromise cloud environments.

5.2.1 Account compromise

Account compromise can be achieved in multiple different ways. These methods include credential stuffing, obtaining leaked credentials or insider help.

Credential stuffing or password spraying is a low-effort yet effective method, often used by cybercriminals [15]. It is usually conducted with specialized scripts, optimizing efficiency and minimizing chances of detection. Credential dumps and leaked databases are also often used as a source of credential combinations. Cloud environments and single sign-on (SSO) applications are common targets as the potential access to intellectual property can be considerable. The severity of the threat the compromised credentials pose can differ according to the maturity of the organizations authentication configurations: lack of multi-factor authentication (MFA) or allowing legacy protocols including IMAP/POP3 that do not conform to MFA are weaknesses known to the attackers and are commonly exploited [16].

Credentials are also often found leaked inadvertently in public repositories like GitHub. This has prompted cybercriminals and defenders to actively scan for secrets in the data. To combat this Github lauched[17] a scanning feature to alert for leaked secrets in new commits.

5.2.2 Misconfiguration abuse

Abusing misconfigurations in cloud servers and applications has been a popular entry way for cybercriminals for years. List of examples of data breaches caused by unsecured data storage instances is extensive [18].

In their report [19] on cloud security, Enterprise Strategy Group listed the most common and impactful misconfigurations faced by organizations. The top most prevalent misconfigurations included:

- Management consoles without password protection or with default password (30%)
- Publicly exposed server workloads (27%)
- Overly permissive service or user accounts (25%)
- Publicly exposed web servers without WAF and/or a load balancer (23%)
- VMs or containers running as root (22%)
- Management interfaces without multi-factor authentication (22%)
- Security group allows traffic to non-allowlisted IPs (22%)
- Disabled logging (19%)
- Management ports open (19%)

The list shows a clear trend of reliance on the default permissions and configurations. CSPs offer default configurations to aid in the process of starting up the cloud infrastructure, but securing the environments beyond the default settings is too often overlooked.

Cybercriminals have also found different ways of abusing these misconfigured systems. Data storage instances have been used for data theft and planting malicious code [20], whereas containerized environments (e.g., Docker and Kubernetes) have been used for illicit cryptomining and more [21]. Exposed and improperly secured cloud resources are an easy target for automated attacks and exploitation.

5.2.3 Phishing

Traditional email-based credential phishing is a common technique for credential harvesting. Commonly credential phishing emails come with links

to phishing pages impersonating cloud service providers. Cloud has given the attackers different options for the email delivery, for example Google's applications have been used to deliver spam and phishing emails [22]. Cloud hosting services also offer a great deal of extra credibility to the phishing pages: phishing site hosted on the targeted domain with a matching SSL-certificate can give the attacker an unexpected advantage.

Consent phishing has been one of the prevalent phishing methods over the last years. As the cloud is becoming the norm, organizations are also adapting to using cloud based applications that rely on the permissions granted by the user or organization. These third party applications also offer an avenue for the attackers. The attackers first create a malicious application typically impersonating a legitimate application or presenting as an utility application. They can then send a phishing email with a link that points the victim to their cloud providers page with a OAuth consent grant prompt to install the application with needed permissions. These cloud malware application based attacks have been common with a high success rate [23]. Typically malicious OAuth applications are aiming to steal data, gather information for a BEC attack, deploy ransomware etc.

5.2.4 Exploiting cloud applications

IaaS environments where cloud customers are managing their own web applications and systems, classic web application vulnerabilities are still common and exploiting them is a effective way to access the environments. OWASP top ten [24] lists the most common and most critical web vulnerabilities and these do apply also for cloud environments, although the architectural differences that cloud brings does have an effect on the criticality of some vulnerabilities. Namely Server-Side-Request-Forgery(SSRF) vulnerabilities are often highly effective ways to exploit cloud applications. By exploiting a SSRF vulnerability the attacker could access important information or possibly gain authentication keys from the internal cloud meta-data instance.

The criminal cloud application exploitation also ranges to the commercial software with published vulnerabilities, taking advantage of unpatched systems. The examples includes some of the top routinely exploited vulnerabilities listed in the US Cybersecurity and Infrastructure Security Agency (CISA) report [25], e.g Pulse Connect Secure VPN vulnerabilities allowing access to cloud platforms. Another recent example of targeting cloud based applications was shown in Trend Micro's report [26] on the Formbook malware shifting to exploit the latest Office 365 zero-day vulnerability, for which Microsoft did already publish a patch during September 2021.

5.3 Post-exploitation activities

Many of the same methods cybercriminals use for monetization when attacking traditional on-premise environments are also common in the cloud. However cloud does change the dynamics and offers new ways to spread more effectively, access more resources and allow for other techniques that are even more destructive than before.

5.3.1 Ransomware

Ransomware is the number one most common malware seen in the cloud [13]. The nature of cloud infrastructure makes ransomware a viable malware type to use: the high connectivity and the access to data. File sharing and syncing services are a great way for the ransomware to pivot further in the environments.

5.3.2 Data theft

Cloud environments often host a vast amount of data of importance for the organization and what is important to the organizations is often of interest to the cybercriminals as well. Information including credit card numbers, sensitive personally identifiable information and financial communications are commonly exfiltrated in attacks. Unsecured cloud databases have been a major contributor in the statistics for data theft [27].

5.3.3 Cryptojacking

One of the biggest selling points of cloud services is the benefit of scalability and near limitless resource availability. From the cybercriminal perspective this pairs up perfectly with cryptomining. In practice cryptomining is exchanging computing power for rewards, and as computing power is abundant and readily available in the cloud, it makes cloud a prime target for resource hijacking operations using the systems for cryptomining. In the last years, cryptojacking attackers have taken up cloud as a major target. In many cases the attacks have been automated or worm-like attacks abusing misconfigurations in containerization platforms or management systems (e.g., Docker and Kubernetes, see chapter 6). Other attacks have included taking advantage of free automated processing features offered by cloud providers [28].

5.3.4 Operational abuse

Cloud offers cybercriminals similar benefits as to the legitimate cloud customers. In some cases it is beneficial for the attacker to compromise an environment and use that infrastructure to launch further attacks. This way the attacker can obtain an additional cover, credibility or a way to bypass defences. Hosting phishing pages or malicious documents on legitimate organizations compromised cloud servers gives the attacks extended credibility, as the domain and certificates are from the compromised organization. It also gives the attackers an extra layer of cover for their operation as the host is not directly tied to known attacker operated domains or IP addresses.

Cloud platforms and applications offer attackers covert ways to operate. Netskope Threat Labs report [5] included statistics showing malware delivery through cloud applications. Their report showed that in the end of second quarter of 2021, 68% of all malware downloads were delivered from cloud applications, majority being from cloud storage applications and second most common type was collaboration and development applications. The use of cloud applications as malware delivery channel allows the attackers to use the allowlisted channels used by the organizations, bypass blocklists and blend in with the benign network traffic. Although the usage of cloud storage means that the stored malware might be shortly deleted by the service provider, the positives of cloud hosting seem to be outweighing the downsides. The agility and cover of trust are enough to make cloud an effective malware hosting and delivery channel.

5.3.5 Business Email Compromise

Business Email Compromise (BEC) is a type of attack where an attacker uses their illegitimate access to an email account to fraud the targeted organization [29]. BEC has proven to be a major threat to businesses and is causing considerable losses to the victims. In their announcement [30] in April 2020, the Federal Bureau of Investigation (FBI) mention that between January 2014 and October 2019 the Internet Crime Complaint Center (IC3) received complaints for more than $2.1 billion in losses caused by BEC scams. To note, this number was a total from only two major cloud based email services, and includes only the cases that were reported. IC3 has been tracking BEC related losses since 2013, and the number has been consistently increasing since.

In 2020 observed amount of BEC attacks decreased slightly, although reports signal monetary losses to be increasing, pointing to more targeted and sophisticated attacks [31].

Chapter 6

Case studies

In this chapter we examine different threat actors or types of attacks that are targeting and abusing the cloud environments. We explain their activities according to the level of public reporting on the cases and when possible show the evolution of their TTPs. The chosen cases are ones which had a sufficient amount of available reporting and data, and can be considered to adequately represent their own niche of cybercrime.

6.1 Magecart formjacking

Magecart is a umbrella term for different threat actors attacking e-commerce sites with digital credit card skimmers. They are mainly targeting online stores by injecting malicious code to the page, stealing and exfiltrating the unsuspecting visitors credit card information when entered. Magecart style attacks targeting Magento e-commerce platforms have been seen at least since 2014 [32]. Figure 6.1 showcases the general formjacking attack flow. Notable cases of Magecart attacks include the breach of British Airways [33] and Newegg [34]. Traditionally the attackers have taken advantage of servers running old versions of the Magento system, exploiting known web vulnerabilities to inject Javascript sniffers into the site. There has been a considerable amount of sniffer families and variants [35]. We will first take a look at the ways Magecart groups have operated historically and then move onto other examples of cloud related attacks.

6.1.1 Traditional formjacking

Two of the most well known attacks attributed to Magecart groups are the aforementioned British Airways and Newegg attacks. Both of these attacks

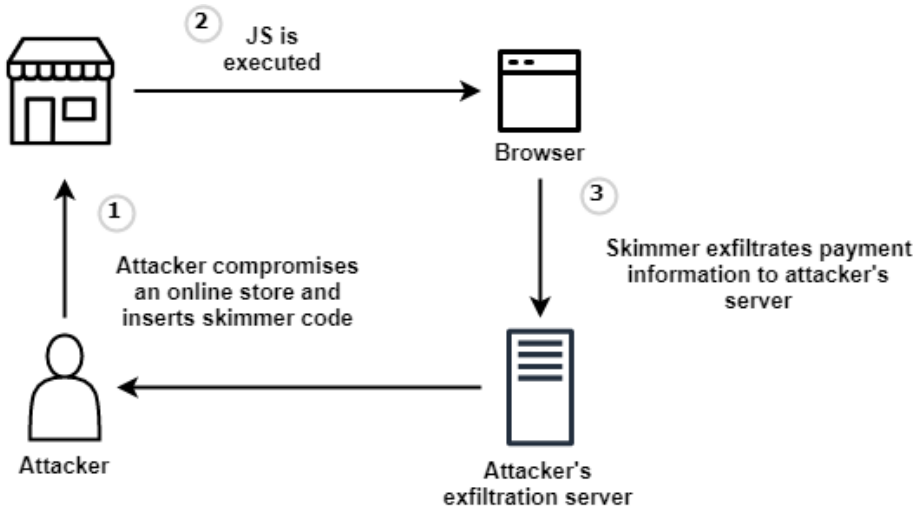

Figure 6.1: Simple example of formjacking attack flow

have been tied to the Magecart 6 group. Magecart 6 is also known as FIN6 [36]. FIN6 has a history of targeting systems with payment card data, including point-of-sale (POS) systems [37] and formjacking is only a part of their cybercrime operations.

In the case of the British Airways incident, the attackers showed a more sophisticated and well executed approach compared to the other Magecart groups. The attack was clearly highly targeted and they had done extra work to blend into the British Airways infrastructure. FIN6 has been seen to use this kind of highly targeted and selective approach before [38].

The attackers got access to the servers and modified one the JavaScript files loaded on the payment page. They added a couple of lines of code to the end of the file. The simple piece of code was especially crafted to fit to the site and was bound to run when the used released the press of the submit button. It then serialized the data in the form, turned it into a text-string and sent it within a POST request to an attacker controlled page. In order to blend in more, the exfiltration server domain name and URL were also chosen to represent a British Airways internal data processing application.

6.1.2 Taking up cloud as an attack vector

During 2019, there were for the first time Magecart type formjacking attacks that were targeting service providers' cloud platforms and other cloud assets to increase the reach of their attacks. Before this the attacks had been focusing individual targets including web-shops and other pages with payment

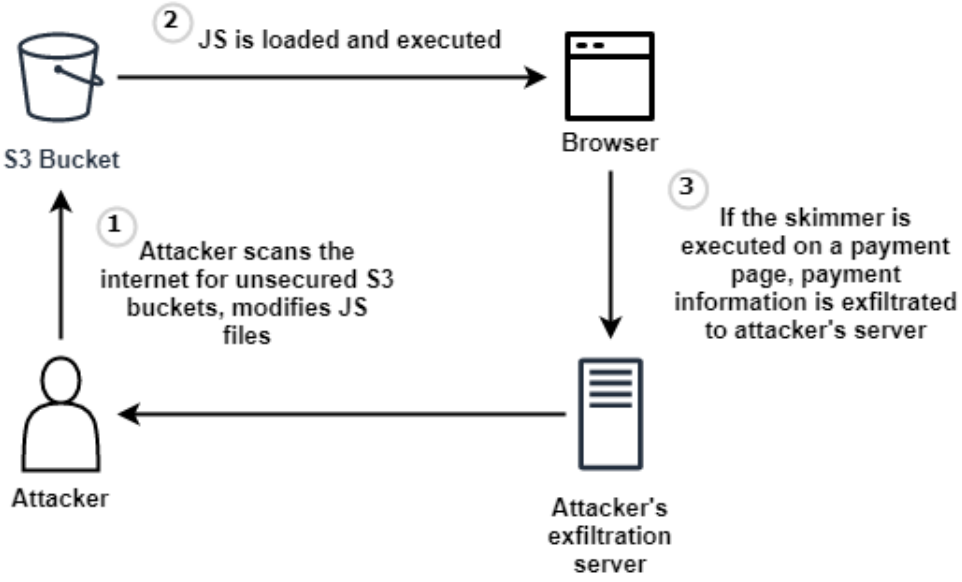

Figure 6.2: Magecart S3 bucket attack flow

processing functionality.

In July of 2019, RiskIQ published an article [20] on another Magecart campaign targeting misconfigured AWS S3 buckets. S3 is an object storage service that is used for application storage, data archiving, cloud storage etc. The attackers approach was to scan the internet for public unsecured S3 buckets, which can be accessed by anyone having an AWS account. They would then proceed to seek for JavaScript files in the bucket, download them, append the skimmer script and upload the modified JavaScript file back onto the S3 bucket (see figure 6.2). This tactic is based completely on the ease of execution and relying on the mass exploitation of S3 buckets regardless of the use of the bucket. Only a small percentage of the infected JavaScript files would manage to exfiltrate credit card information.

In October of 2019, Trend Micro published [39] their research on a Magecart campaign targeting Volusion, a e-commerse service provider. In the past Volusion has made it public [40] that they have moved their whole infrastructure to Google Cloud Platform (GCP), being one of the first to do so. This Magecart attack started by the attackers gaining access to the Volusion cloud infrastructure, although the details of this initial attack have not been made public. The attackers were able to inject malicious JavaScript to a code library Volusion provides to their client shops (see figure 6.3). Therefore by gaining access to the Volusion code library, the attackers were able

to infect a multitude of web shops. Trend Micro reported that 3126 individual web stores were impacted. The initial injected code part created a new script element and loaded another JavaScript file that was hosted on Google Storage. For added stealthiness the Google Storage bucket was named *volusionapi*. The attackers had clearly put extra effort in hiding the malicious loader code into the original code, integrating it into the execution flow of the program and using a style uniform to the other code. The skimmer's exfiltration server, where the script was sending the extracted credit card information, was also a Volusion domain look-a-like.

In fact, the Volusion attack was the third similar attack on e-commerce providers' cloud platforms. Previously a different Magecart actor named Mirrorthief executed similar attacks on two smaller providers, infecting 200+ online stores with skimmer malware[41, 42].

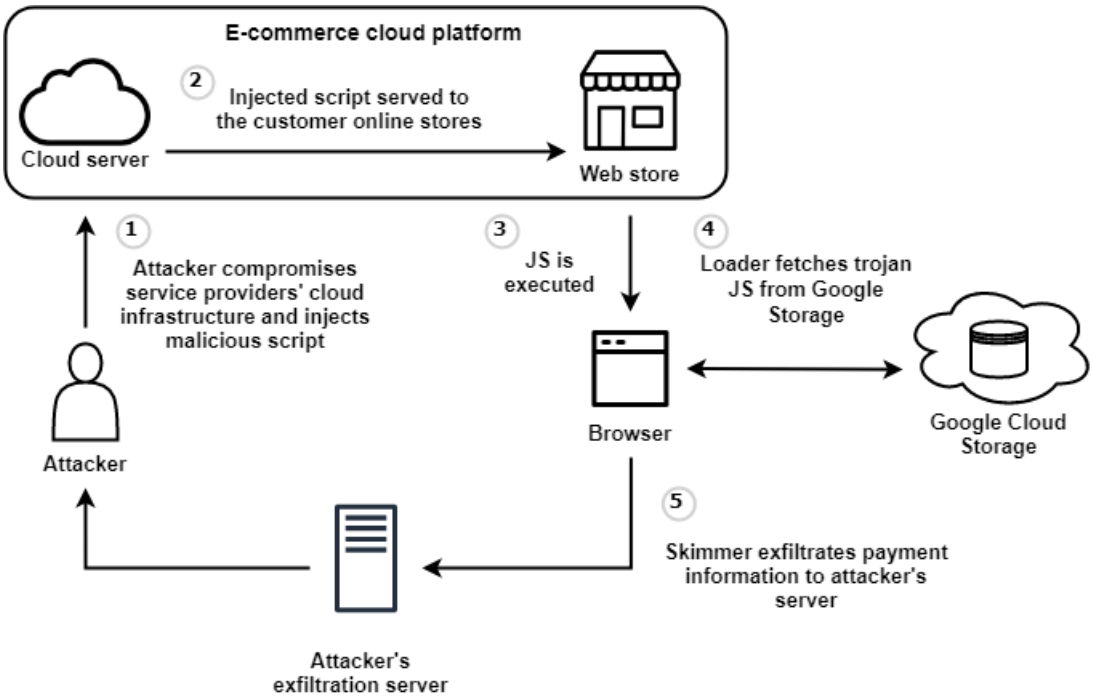

Figure 6.3: Magecart Volusion hack attack flow

To note, the attacks using misconfigured S3 buckets as the access vector are in principle very different style of attacks compared to the Volusion or British Airways hacks that have been attributed to the Magecart 6 group. Both Volusion and British Airways hack had a similar style of developing

custom code that fits the target infrastructure and does not stand out, where as in the S3 bucket attacks the attackers had not done any manual work to optimize the JavaScript payload to stay undetected. Instead the S3 attacks were automated in nature, did not do any target selection nor try to hide their actions. In their report Trend Micro presented [39] the evidence tying the Volusion attack to the attacks of British Airways and Newegg. They found clear similarities in the skimmer code: both skimmers were jQuery based scripts that serialized the data and sent it off to the exfiltration server by a POST request in a similar manner. The exfiltration server domain names were also similarly chosen to be close to the target's domain name, and were all registered through the same provider.

6.1.3 Trust abuse for Content Security Policy bypass

In June of 2020, Sansec Threat Research Team published an analysis [43] of a new Magecart style attack that runs almost entirely on Google's services. The malware uses Google Analytics to covertly exfiltrate the entered credit card details. It makes use of the implicit trust the site administrator has for Google combined with the lack of granularity provided by the Content Security Policy (CSP) rules. See figure 6.4 for an illustration of the attack flow.

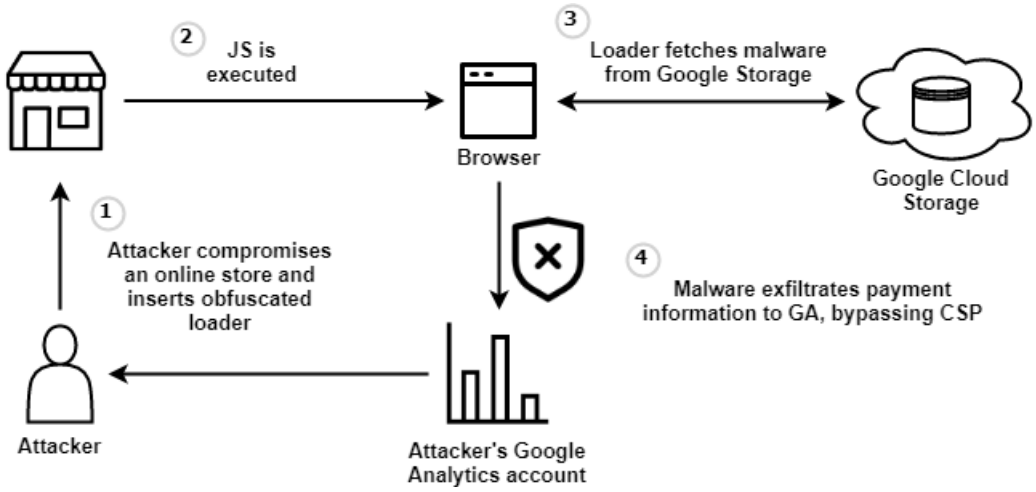

Figure 6.4: Magecart CSP bypass attack flow

The skimmer script is hosted on Google Storage and fetched by a small loader script. It takes advantage of the trust the site admin places on Google, in order to fly under the radar. The skimmer is able to completely bypass the CSP on the site if the site is using Google Analytics (GA). For the GA to

work the domain needs to be allowlisted in the CSP, which then also allows the attacker to connect to their own instance of GA for data exfiltration purposes.

Additionally the skimmer uses external service to obtain the IP address of the victim, and also includes a feature that disables the skimmer if the victim has developer tools window open in their browser.

CSP was designed to combat the problems of client side vulnerabilities, namely cross-site scripting (XSS). It has been considered a promising defence against the execution of malicious scripts, but does have it's problems [44]. CSP is a policy mechanism, that defines the allowed resources for the client side code, including allowlisted domains for script download and other communication. PerimeterX published an article [45] describing this method of using external third party services for data exfiltration, in order to bypass CSP. In the article they describe in detail the ways to exploit this vulnerability in CSP, that stems from the vagueness of the CSP rules. By default, CSP does not protect against compromised hosts that are trusted by the site and allowed in the CSP rules. Side product of the allowlisting is also the fact that any third party services used or otherwise trusted by the site administrator are also available for the attackers to use. PerimeterX shows the problem with CSP to be the lack of query string support, thus it cannot differentiate for example between Google Analytics tag IDs.

With the wide spread use of cloud services, and the selection of the available services offered by cloud providers, a domain or path based restrictions can become problematic. As a site uses a given cloud service providers service for the normal operation of the site, they must allowlist the needed actions for that to be possible. The side effect of that is that the attacker's code is allowed to connect to the same service.

6.1.4 Public repositories, steganography and new exfiltration methods

During 2020 multiple Magecart campaigns were found using steganography and favicon image files [46, 47]. The different campaigns hid their skimmer code inside image files and also used image files as packaging for their data exfiltration.

Later in July Sucuri published another report [48] where they disclosed a similar tactic in which the skimmer code was appended into and .png image. The attacker had created a full Magento beta version repository with the skimmer embedded into the image file, hoping unsuspecting developers to use the repository for setting up a Magento site.

The initial loader script was appended to Google Tag Manager inside a compromised Magento 2 site. The obfuscated script loaded a .PNG file from a directory in the same site and executed part of it. The loaded *google-tagmanager.png* file had the obfuscated JavaScript skimmer code appended into the binary. The JavaScript code fetched another image file *mage.png* from a public GitHub repository containing a beta version of Magento 2.4. This *mage.png* file included a encrypted exfiltration URL pointing to a URL impersonating a Google Fonts API service.

In September 2020 Malwarebytes reported[49] on yet another credit card skimmer variant that had changed the exfiltration infrastructure to use a instant messaging platform Telegram. This allowed the attackers to not reveal their IP addresses or domains if the skimmer would be analyzed. The skimmer would also perform anti-debugging checks to prevent analysis. The code activated when the user sent the purchase confirmation, copying the fields containing sensitive information and sending a POST-request to Telegram API that forwards the message into a chat. Similar to the Content Security Bypass attack abusing Google Analytics, the use of Telegram achieves some level of cover by using a legitimate and common service to exfiltrate the stolen data.

6.1.5 Magecart TTPs

Main notable attacker techniques

- Cloud storage misconfiguration abuse in order to add malicious code
- Use of cloud storage for hosting skimmers
- Use of PaaS platform to host attack infrastructure
- Use of SaaS applications for data exfiltration
- Bypass cross-site scripting protections by using SaaS applications for exfiltration
- Cloud supply chain compromise for malware delivery
- Domain impersonation
- Code obfuscation and anti debugging techniques
- Software vulnerability exploitation for initial access
- Steganography

6.2 TeamTNT cryptojackers

Cryptojacking is a common form of resource hijacking [50]. Research has shown that at least 23% of companies maintaining cloud infrastruture have experienced cryptojacking attacks [51]. Performing resource hijacking attacks against cloud instances purposes has been a very popular attacking technique for cyber criminals for multiple reasons. Firstly especially IaaS service model gives the attacker access to nearly unlimited resources to use for mining cryptocurrency. Secondly, the ease of execution: finding and abusing misconfigured systems in the cloud has been easy and setting up cryptojacking software trivial.

TeamTNT has been one of the most active threat actors in the field of cryptojacking, especially in attacks abusing misconfigured Docker daemons and Kubernetes clusters [21]. Over the last couple of years they have had a multitude of campaigns with ever evolving methods. In this section we cover the most interesting of the TeamTNT's cryptojacking malware variants.

6.2.1 Graboid: first of its kind

In October 2019, Unit42 reported [52] on a new kind of cryptojacking attack: a cryptojacking worm targeting misconfigured, unsecured Docker instances, with publicly accessible APIs that do not require authentication.

Graboid worm has not been clearly attributed to the TeamTNT group that this case study is focusing on, but because Graboid is the first of it's kind, acting as a predecessor to TeamTNT's malware variants, we decided to include it in the case study.

Graboid was the first worm observed to abuse Docker daemons. It uses a prepared malicious docker image in the Docker Hub container image library. Using a ready-to-deploy malicious image helped to streamline the process of exploitation. The worm deploys XMRig, a known Monero cryptominer binary. Although coming up with a new way of propagation, the techniques used are simple and the whole process of running the cryptojacking operations is clearly unrefined and lacks efficiency. The Unit 42 research concludes that the worm-like propagation combined with C2 supplied scripts underline a possible threat of deploying a more destructive malware, for example ransomware. Notably the worm itself does not perform any scanning activities to find new vulnerable hosts to spread to, but relies on the provided list of vulnerable hosts.

Graboid notable details

- Begins the attack by deploying a masqueraded malicious Docker image from Docker Hub
- Entry point script downloads 4 shell scripts from the C2 and executes them
  - *live.sh:* Reports system information to the C2
  - *worm.sh:* Downloads IP list of vulnerable Docker APIs, uses Docker CLI to propagate
  - *cleanxmr.sh:* Picks random IP from the list, stops miners on the target
  - *xmr.sh:* Picks random IP from the list, deploys masqueraded image containing XMRig binary

6.2.2 TeamTNT's initial worm: Covid-19

In May 2020, Trend Micro reported [53] on the first found TeamTNT cryptojacking worms targeting cloud instances. As with Graboid before, the worm takes advantage of misconfigured Docker APIs. Comparing to the Graboid worm, the TeamTNT's Covid-19 comes with considerably more functionality and capabilities, although the reporting does not specify how well the capabilities were utilized.

Covid-19 notable details

- Scanning script *mxutzh.sh* scans for vulnerable Docker instances and deploys an Alpine Linux container
- Container entry command downloads and executes a dropper scripts that downloads and executes the different parts:
  - *clean.sh*: seeks and removes competing miners including Kinsing
  - *dns*: The Kaiten/Tsunami DDoS bot
  - *lan.ssh.kinsing.sh*: script for lateral movement via SSH
  - *NarrenKappe.sh*: Firewall configuration and data exfiltration script
  - *setup.basics.sh*: Utility installer script
  - *setup.mytoys.sh*: Script that prepares log cleaner and *punk.py* post-exploitation tool used for lateral movement

Reconnaissance	Script scans for open default Docker API ports	T1595
Initial Access	Exposed Docker daemon allowing anonymous access	T1190
Execution	Use Docker daemon to deploy Alpine Linux image Entrypoint script dropper downloads & executes components	T1059.004 T1610
Defence Evasion	Modify firewall to open needed ports Clear logs	T1562.004 T1070.002
Discovery	System Information Discovery	T1082
Lateral movement	Scripted SSH bruteforce (punk.py & lan.ssh.kinsing.sh)	T1110.003
Exfiltration	Automated exfiltration of system details and sensitive information	T1020 T1041
Impact	Cryptojacking operations Victim used as a part of DDos botnet	T1496

Table 6.1: Covid-19 variant TTPs

- *setup.xmrig.curl.sh*: Script to prepare the cryptominer
- *sysinfo*: Binary for system information gathering and exfiltration

Notably contrary to the Graboid worm, this TeamTNT worm does not use a malicious image hosted on Docker, but deploys a benign container and relies entirely for self hosted files and C2 server to supply the scripts used for malicious activity.

6.2.3 TeamTNT adds AWS credential theft

In August 2020, Cado Security reported [54] on a shift in the TeamTNT campaign. The cryptojacking worm targeting unsecured Docker APIs had started to collect and exfiltrate AWS credentials. This is the first time a cloud cryptojacker has been observed to also target and steal cloud platform credentials. This is a very simple process as normally credentials are stored in a cleartext file on the filesystem. Also as mentioned in the Cado Security report, the TeamTNT malware has copied some new techniques from competitor(Kinsing), e.g., disabling Alibaba cloud security tooling. This variant seems to be a refined version of the Covid-19 worm, with added functionality.

Reconnaissance	Script scans for open default Docker API ports	T1595
Initial Access	Exposed Docker daemon allowing anonymous access	T1190
Execution	Use Docker daemon to deploy Alpine Linux image Entrypoint script dropper downloads & executes components	T1059.004 T1610
Persistence	Installs Diamorphine rootkit and Tsunami IRC Backdoor	T1014
Defence Evasion	Diamorphine rootkit Disables Alibaba Cloud security tooling C2 server domain name masqueraded as Docker domain Clear logs	T1014 T1562 T1036.005 T1070.002
Discovery	Gathers AWS credentials for exfiltration Gathers local account credentials	T1087.004 T1087.001
Lateral movement	Scripted SSH bruteforce (punk.py)	T1110.003
Exfiltration	Automated exfiltration of AWS credentials	T1020 T1041
Impact	Cryptojacking operations	T1496

Table 6.2: AWS stealer variant TTPs

AWS credential stealer notable details

- Seeks for AWS credentials in the home directories and sends them unencrypted to the C2
- If found, removes Alibaba Cloud Security tooling
- Installs Diamorphine rootkit

6.2.4 AVScan: refined malicious Docker images

In August 2020, Aquasec reported[55] on a new TeamTNT campaign using Docker Hub for hosting a multitude of malicious images. The Docker Hub account found by Aquasec had varying images uploaded over the span of four months. Aquasec divided the images in three different categories depending on the level of sophistication. The first images were simple images with embedded cryptojacking malware. The second set additionally included tool for Docker escapes aimed for privilege escalation, based on an open-source tool that uses common Docker escape techniques. The third and most sophisticated group of Docker images, included three images which had incorporated detection evasion techniques to hide command and control communication and new persistence methods. The Aquasec report included an in-depth

analysis of the *AVscan* image. See figure 6.5 for view of AVScan TTPs.

AVscan variant notable details

- *AVscan.sh*: Image entrypoint, starts the processes
- *Carray.sh*:script seeks & removes competing miners and deletes itself after
- *Cron.sh*: Sets a cron job downloader for *minion.sh* over Tor
  - *minion.sh*: hides & executes base64 snippet scripts, functionality includes:
    * (/usr/bin/hid) tries to stealthily mount /proc/PID into /usr/foo
    * (/usr/bin/pu) is a lateral movement SSH script
    * (/tmp/.logs.c) login/logout log cleaner
    * deactivates CPU intensive programs
    * acts as a dropper for three additional scripts (user.sh, sbs.sh, sxc.sh)

Scripts downloaded & executed by *minion.sh*:

- *user.sh*: Prepares the victim environment, gathers information
- *sbs.sh*:
  - Creates a bind shell for remote access (/usr/bin/bioset)
  - Collects and sends base64 encoded system information to C2
  - Cleans command history etc
- *sxc.sh*:
  - Downloads XMRig (cryptominer) and optimizes it's operation
  - Logs and sends mining process information to C2
  - Removes system logs, command history
  - Disables network configuration, monitoring and security tooling
  - Disables security scanners including Alibaba's Aliyun

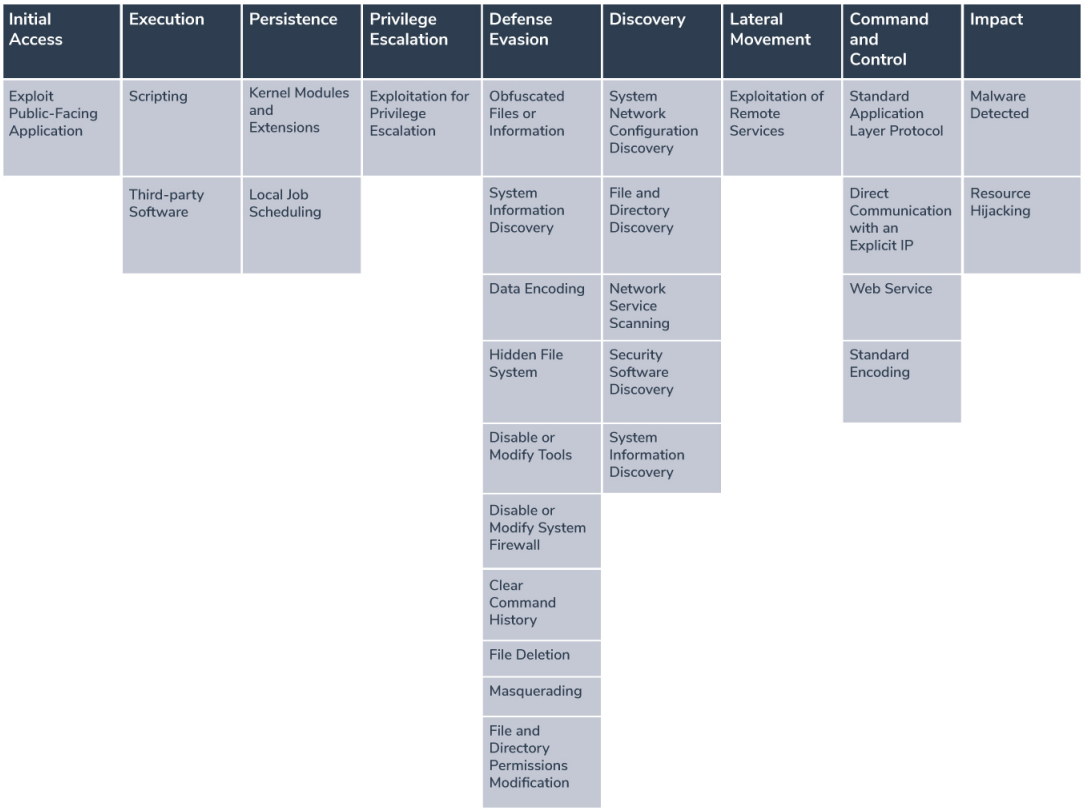

Figure 6.5: AVScan variant TTPs [55]

6.2.5 Cetus: chained binary delivery

In August 2020, Unit42 reported [56] on another TeamTNT worm exploiting unsecured Docker instances. Malware campaign named Cetus masquerades itself as an UI management tool Portainer, a tool commonly used in Docker environments. It starts a disguised XMRig miner and starts the network scanning in order to spread.

Cetus variant notable details

- Copies *Portainer*(Cetus) and *docker-cache*(XMRig) from the container running the scanning
- Obtains persistence through .bash_aliases

Interesting details of the Cetus worm based on the Unit42 report include the fact that it does not rely on malicious images hosted on Docker Hub, but uses a benign Ubuntu image and copies the malicious binaries over from

the previously infected container. This means that it does not rely on C2 infrastructure to provide the malicious binaries. Additionally the *docker-cache*(XMRig) cryptominer is highly obfuscated to evade security tooling, while Cetus itself is not obfuscated at all and does not use anti-debugging techniques. Cetus also uses an unique naming convention for the containers it creates, this is possibly done in order to better monitor the mining operation.

6.2.6 Weave Persistent: 3rd party software as backdoor

In September 2020, Intezer reported[57] on new TeamTNT attacks using never before seen technique of abusing legitimate third party software as backdoor. The attack employs Weave Scope, a legitimate open source container management tool, to establish a persistence on the host. It allow the attackers to directly run system commands on the containers directly via HTTP without installing any malicious backdoors or beacons.

Weave Persistent variant notable details

- Abuses exposed unsecured Docker API to deploy a new privileged Ubuntu container, with the host filesystem mounted to the container and as an entrypoint command start cryptominers on the container
- Attempts privilege escalation by creating a local privileged account *hilde* on the host and connect via SSH
- Installs Weave Scope on the host for persistence

This attack was the first observed attack by TeamTNT that tries to gain root access on the host. If the Docker daemon is run as root, it gives the attacker an opportunity for an easy container escape and privilege escalation. Notably this attack was also among the first times a cloud targeted attack has utilized legitimate admin tooling in their attacks and practically obtaining a backdoor to the system.

6.2.7 Still alive: two part attacks

In September 2020, Aquasec reported [58] on new TeamTNT activity. New malware variant with the name 'Still alive' was found after the researchers found a new TeamTNT Docker Hub account. This variant incorporated many new attack techniques and post-exploitation tools. They noted that it seemed that TeamTNT were experimenting with a variety of open source

attack tools and new attack vectors. The attack is split in two parts, using the initial Docker instance as a scanning and attacking platform to further attack vulnerable Redis instances.

Still alive -variant notable details
1st part: scanning/spreading

- Abuses exposed unsecured Docker API to deploy a malicious container from Docker Hub
- The entrypoint script uses Shodan to search for vulnerable Redis hosts and attack them using open source tool called *hackredis*

2st part: cryptojacking

- Prepares the environment, disables security tooling, removes cryptominers
- Clones the XMRig miner from Github, and if not available, from a S3 bucket
- Downloads previously known malicious TeamTNT binaries (e.g. DDoS tools) from a S3 bucket
- Downloads more cryptominers and tools from other possibly compromised domains and IPs

Notably, in another Docker image found under the same user was found ZIP-files containing *mimipenguid* and *mimipy*, tools for scraping the memory for user credentials. See figure 6.6 for the variant's TTPs.

6.2.8 Black-T: memory scraping

In October 2020, Unit42 reported [59] on a new shift in the TeamTNT cryptojacking malware TTPs. The new malware variant, bearing the name Black-T, added new focus on scanning capabilities, memory scraping functionality and fighting competing cryptojacking malware.

Later AT&T Cybersecurity identified [60] the Black-T to be using a Golang based memory loader tool Ezuri. It acts as the malware loader, allowing the payload to be executed directly in memory without writing it to the disk.

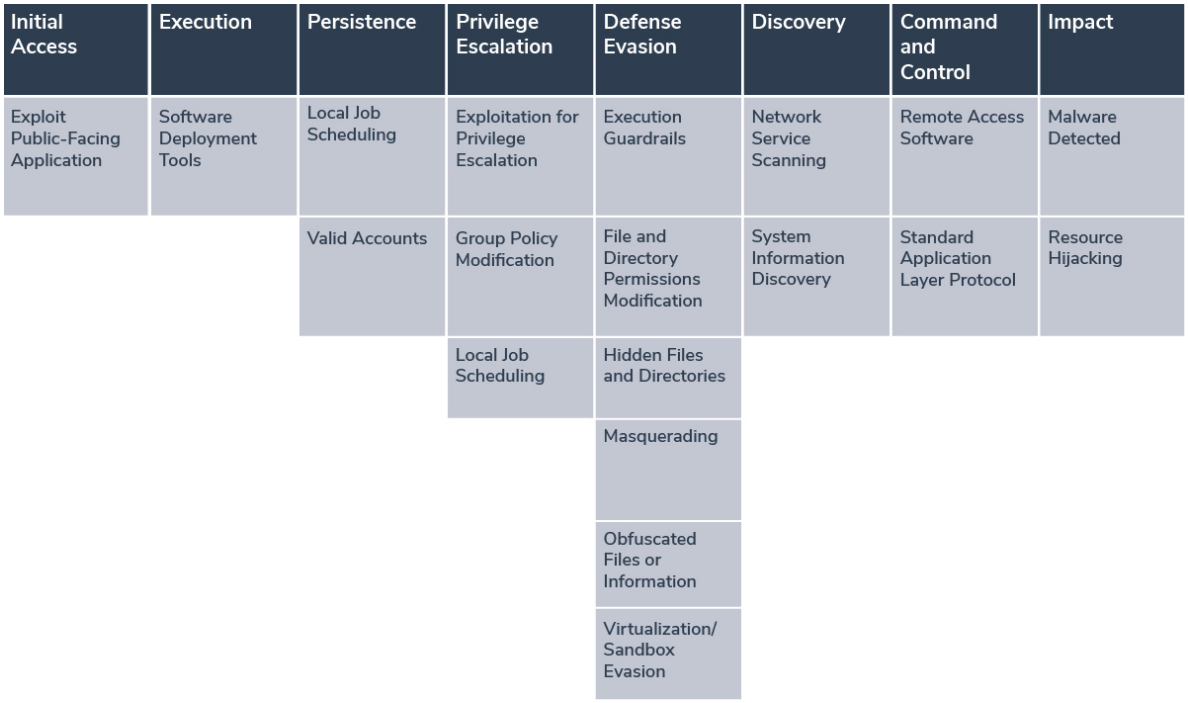

Figure 6.6: Still alive variant TTPs[58]

Black-T variant notable details

- Targets multiple competing cryptojackers removing the competition
- Uses multiple network scanning tools
- Compresses and exfiltrates cron files, files from /root/ and /home/*/, including AWS credentials and SSH keys
- Introduced new post-exploitation operations:
  - Password scraping using *mimipy* and *mimipenquin*, *NIX versions of the Windows Mimikatz tool
  - Infects all running containers

6.2.9 TNTbotinger: IRC DDoS bot

In December 2020, Trend Micro published a report[61] analysing a new TeamTNT cryptojacking malware variant. This new variant features a new

encrypted binary containing a IRC bot with C2 and DDos capabilities. The Internet Relay Chat(IRC) bot includes commands for various denial-of-service attacks using TCP and UDP messages (including SYN, SYN-ACK and ACK) as well as options for running system commands on the target.

6.2.10 Hildegard: turn to Kubernetes

In February 2021, Unit42 reported[62] on a TeamTNT campaign that shifted to target Kubernetes clusters. As before with Docker, the new variant takes advantage of misconfigured Kubelets that are exposed to the public and allow anonymous access. It has also taken on new techniques for command and control, persistence and evasion.

Hildegard variant notable details

- Begins by exploiting misconfigured Kubelet and searches for the containers in the nodes
- Establishes reverse shell connection using *tmate*, a terminal multiplexer, used to share terminal connections over SSH
- Uses library injection to hide malicious processes from monitoring tools
- Deploys encrypted IRC agent for secondary C2 directly from the cryptomining containers
- Modifies DNS configuration to avoid detection by DNS monitoring tools
- Generally deletes all scripts and command histories after execution
- Searches for cloud credentials, tokens, SSH keys etc.
- Gathers system information, scans the internal network for other kubelets
- Uses found unsecured kubelets for lateral movement

Interestingly the malware downloads adversarial tools(Peirates, BOtB) used for cloud enumeration and lateral movement, but does not seem to utilize them for pivoting further in the environments. Similarly the gathered credentials were not observed to be used. See figure 6.7 for the variant's TTPs.

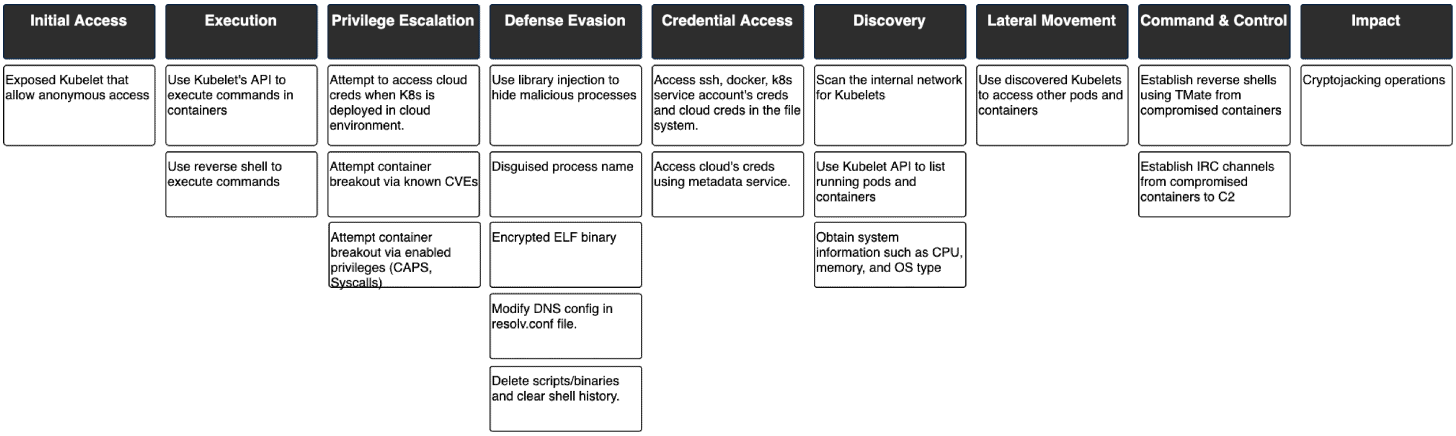

Figure 6.7: Hildegard variant TTPs[62]

6.2.11 Dockgeddon: Docker Hub images with account takeover

In May 2021, Lacework Labs published a report [63] detailing more TeamTNT's malicious cryptojacking Docker images found on Docker Hub. They note that the images are hosted on Docker Hub accounts taken over from another user. This account take over was possible since the same username was found to have a Github account that hosted a publicly available configuration file in which their Docker Hub secrets were. Generally the images use similar techniques seen in previous campaigns. The malicious images included *dockgeddon*, *docker*, *tornadopw* and more, with *dockgeddon* being the main image with spreading capabilities and a *Tsunami* IRC bot.

6.2.12 Chimaera campaign: Adding cloud environment enumeration

In June 2021, Unit42 published a report [64] on the TeamTNT's newest advances in cloud enumeration and exploitation in their cryptojacking campaigns. The report details scripts found in a TeamTNT malware repository called Chimaera. The scripts have added the functionality to use the obtained AWS cloud credentials to discover other permissions, configurations and assets in the environment using the AWS API.

Chimaera repository notable details

- *grab_aws-data.sh:* Using AWS CLI attempts to identify all IAM permissions, EC2 instances, S3 buckets, Cloudtrail configurations and CloufFormation operations the accessed AWS credentials have access to
- *search.sh:* Performs extensive credential scraping in the system, including 16 different applications including AWS, S3, Docker, Github, Google Cloud etc.
- Includes lateral movement scripts related to Weaveworks (*setup_scope.sh*) and Project Jupyter (*spread_jupyter_tmp.sh*)
- Includes pointers to using local Docker image or images (cf. hosted on Docker Hub)
- Includes open source container and cloud penetration tool Peirates, which allows attacker to perform actions against AWS and Kubernetes instances, finding exloitable misconfigurations within the systems

Later AT&T Alien Labs published a report [65] further analysing the campaign after it had been operational for some time. The actions performed by the active campaign differ from the tools and scripts found in the repository.

Chimaera campaign notable details

- Uses a new open source credential stealer component *Lazagne*
- Includes a Windows component with a cryptominer that uses startup folder for persistence

The Chimaera repository enumeration scripts are the first known instance of a similar attack targeting any other Identity and Access Management(IAM) credentials than AWS. In their report Unit 42 note that it is only a matter of time before the attackers deploy similar attacks targeting Google Cloud environments. Additionally Chimaera is the first time the attackers have developed deeper cloud enumeration capabilities, and the presence of related adversarial tooling points to them extending lateral movement activities in the future.

6.2.13 TeamTNT malware variants and TTPs overview

TeamTNT campaigns have included a extensive list of variants, with differing functionality and capabilities. The variants discussed in the case study

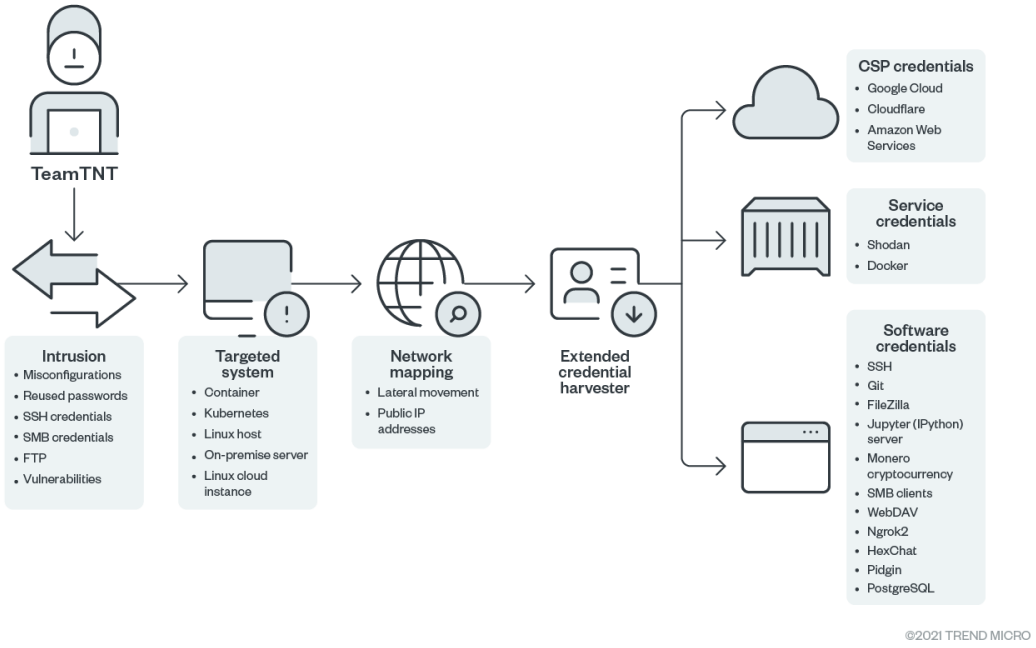

Figure 6.8: TeamTNT cloud credential harvesting attack flow [66]

include the most interesting specimens, but the list is not an exhaustive and does not include all observed malware variants. The described TeamTNT activity took place between May 2020 and September 2021. Figure 6.8 illustrates the general attack flow the later malware variants used in order to harvest credentials from the attacked systems. Table 6.3 presents the most interesting TeamTNT malware variants with their respective new functionality.

Covid-19	Initial cryptojacking campaign with DDos bot
AWS stealer	Worm, Cloud and local credential harvesting
AVScan	Malicious Docker images, new evasion techniques
Cetus	Benign image, chained binary delivery from previous victim
Weave Persistent	Installs 3rd party software on the host for persistence
Still alive	Two part attack, targeting Redis, S3 for binary delivery
Black-T	New scanning and memory scraping capabilities
TNTBotinger	Added IRC bot with C2 and DDos capabilities
Hildegard	Target Kubernetes, new evasion techniques, multiple C2 channels
Dockgeddon	Malicious images on a compromised Docker Hub account
Chimaera	Cloud environment enumeration

Table 6.3: TeamTNT variants with most notable new functionality

6.3 Phishing in the cloud

Phishing scams has been common for a long time, but the attacks still remain a relevant threat to organizations. In this section we will present common techniques threat actors are using when attacking organizations using cloud services. Because of the nature of the attacks, unlike in previous sections, we do not focus on a singular threat actor, but present a broader evolution of important phishing techniques regarding the cloud. We divide it in two main sections, OAuth phishing/abuse and more traditional email phishing.

6.3.1 Consent phishing and OAuth application abuse

The emergence of cloud services has enabled a completely new type of phishing: consent phishing. We will cover consent phishing by presenting a timeline of reported interesting attack techniques in use and some steps in prevention evolution by the service providers.

6.3.1.1 Reports on OAuth abuse

In May 2017, Google Gmail users were targeted [67] by a spammer with an OAuth consent phishing attack. The attacker had created an application with the name *Google Docs*, impersonating a legitimate Google application. The phishing email was in the for of a document sharing notification, where a contact known to the victim was sharing a document on *Google Docs*. The link redirected the user to the legitimate Google OAuth consent screen (see figure 6.9) with the application asking for full access to the victims email

and contacts. The spam email spread in a worm-like fashion, using the access to the victim's contact list and propagating using the victim's email. It is noteworthy that as designed, this attack was able to bypass all email security checks by Google, including SPF and DKIM(reputation and spoofing checks). Later Proofpoint reported [68] on the issue pointing out that after the incident Google introduced OAuth client name validations to mitigate the issue of app name impersonation using IDN homograph attacks [69].

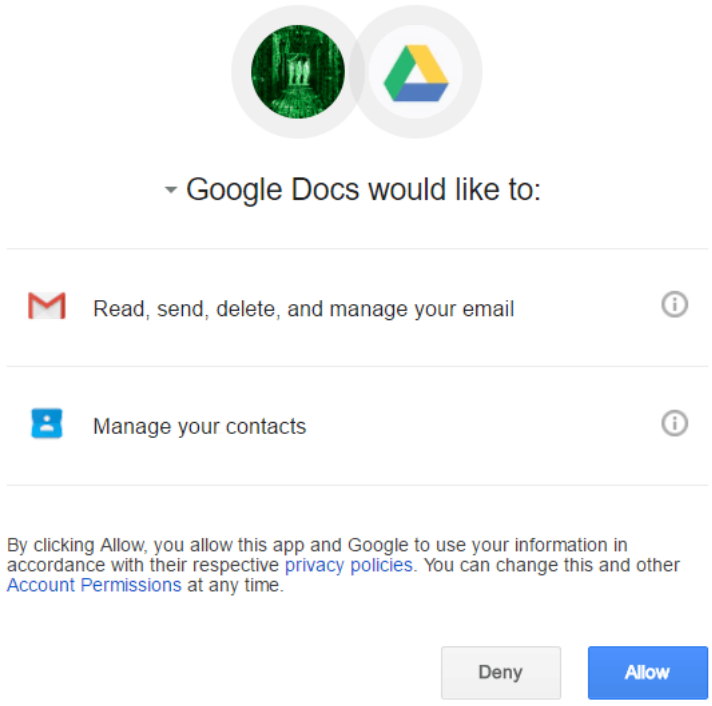

Figure 6.9: 2017 Google Docs worm consent prompt[67]

During 2019, Google updated [70] their OAuth application policies, adding new stricter restricted scopes for OAuth applications, requiring application reviews for larger applications. Also introducing a warning prompt for unverified small applications requiring restricted scopes.

In September 2020, Proofpoint published a report [71] on a threat actor phishing for OAuth access tokens. The phishing came in a form of messages with links taking them to the legitimate Microsoft third-party application consent page. The phishing emails impersonated Mexican tax authorities, Netflix and Amazon. In order to seem less suspicious, the application was only requesting for read-only access to the victims O365 account. This can

also help them stay under the radar of an organizations' security audits of the third party applications. Proofpoint had tracked the actor since the beginning of 2020 and suspected their activity to have started already in August of 2019.

In October 2020, Microsoft's response to fight malicious OAuth applications: publisher verification[72] and app consent policies became available. The aim of publisher verification is to allow legitimate developers to add verified identity to their application to prove the app source to be authentic. The new updates also included a change so that end users would not be able to consent to new multi-tenant apps registered after November 8th 2020. App consent policies also gave admins more control on what applications the end users can give permissions to, limiting them for example to only verified applications.

In November 2020, Phishlabs reported [12] on a phishing technique abusing Microsoft Office Add-Ins feature [73]. The attack came in a form of internal SharePoint or OneDrive file-share email, using targeted brand impersonation and spoofed sender information. The email contained a link to a legitimate Microsoft domain. This link would point the victim to Microsoft login page and after login the attacker's application would request full permissions to the victims Office 365 account (see figure 6.10). The add-in was created using previously compromised organizations development credentials. Microsoft allows Office 365 apps and add-ins to be installed via side loading, meaning the attacker can completely avoid any app review process and directly contact the victims with a valid consent grant link, hosting the malicious applications or add-ins on their own infrastructure. This attack worked because by default any user can grant permissions for add-ins to access their outlook application. Phishlabs also note that the impact of this attack also extends to the compromise of systems leveraging Office 365 accounts for Single-Sign-On purposes, such as SAML or OAuth.

In November 2020, Proofpoint observed [74] an attacker to use an legitimate application as a means of persistence. The attacker had previously compromised the user account, and later on authorized an email application that was also used by some other users in the same organization. This email application had an feature that allows the attacker to add an external email account to the users account, giving the attacker full remote access to the victims mailbox. Using such legitimate application for persistence in this way will likely stay undetected.

Proofpoint report [23] on OAuth application abuse, published in May 2021, points out that although Microsoft's efforts in securing OAuth applications did reduced the quantity of rogue applications it did not completely solve the issue. The publisher verification process proved to be rigorous

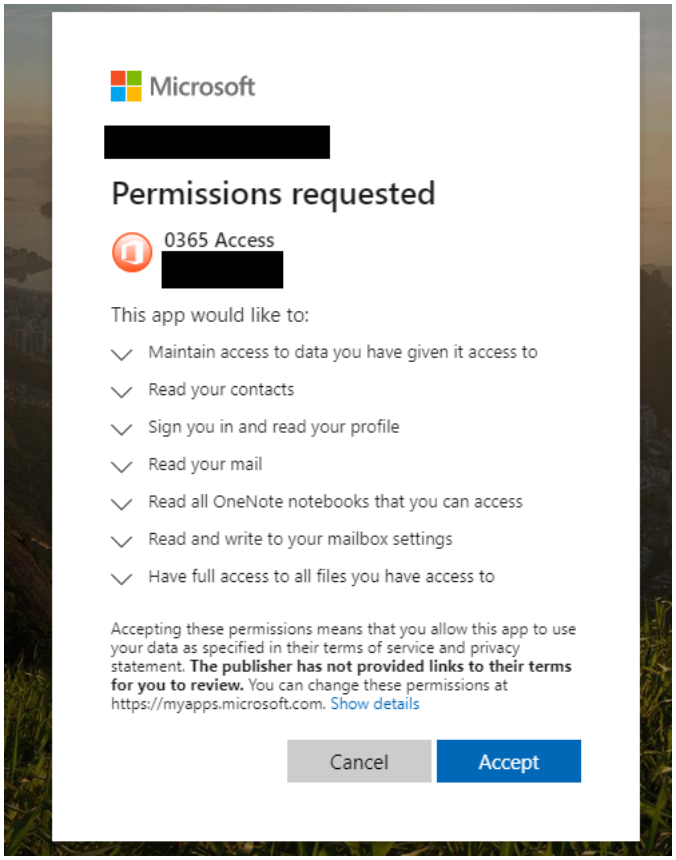

Figure 6.10: Microsoft Office 3rd party application consent prompt[12]

enough to keep malicious actors from obtaining the verification by applying for the verification, but it did not stop the attackers from circumventing the issue altogether by account compromise. Now attackers had started to gain access to a verified organization and create the malicious phishing application from within, gaining the verified status for their application.

6.3.1.2 OAuth phishing and abuse TTPs

Most notable attacker actions

- Spearphishing with links including lures with current topics
- Stealing application access tokens with malicious OAuth applications
- Self-propagation using access to email and contacts

- Application impersonation (homoglyphs, logo and domain)
- Spoofed sender information
- Using compromised accounts to create verified rogue OAuth applications
- Installing or using legitimate 3rd party application functionality for persistence and data exfiltration

6.3.2 Email phishing in the cloud

In this section we go through the evolution of cloud usage/abuse in traditional email phishing. It will not be a fully comprehensive list of all the techniques used by phishing actors but we try to cover the most important techniques.

Email is still a major channel for malware delivery in the cloud and credential phishing is still one of the major threats to companies' security. Over the years spam has grown from harmless advertising to be a considerable threat to security and that has also reflected in the defensive posture of email cloud providers. Email services like Microsoft Office 365 email services now also come with cloud-based email filtering systems to try to protect their customers. But again, where companies move to the cloud, the attackers follow. The multitude of cloud services on offer have given the attackers more tools for crafting new malicious emails that can be difficult to recognise to be malicious.

6.3.2.1 Reports on phishing in the cloud

In June 2016, Avanan reported [75] on Cerber ransomware campaign where the malware was delivered in mass to Office 365 users. The phishing emails were delivered roughly to a million Office 365 users, bypassing all built-in Office 365 security tooling by sending the emails from a private Office 365 email account. When opened, malicious .dotm file asks the user to enable macros in the document and if enabled, it continues to encrypt the victim's files.

In February 2019, Akamai reported [76, 77] on a phishing campaign using Google Translate to deceive the victims. The email came in the form of a Google sign-in notification, with a link loading a phishing page through Google Translate. This allowed the phishing page to seem like it was hosted on a legitimate Google domain, but actually load content from a malicious domain. The attack was optimized to work best on mobile devices, as the Google Translate page when viewed on mobile browsers displays the actual

URL the content is from on a very small line below the Google Translate URL on top (see figure 6.11). After the credentials were submitted, they would be emailed to the attacker. If the first phishing attack was to succeed, the victim was sent another phishing email with a link to a phishing page impersonating older Facebook login page.

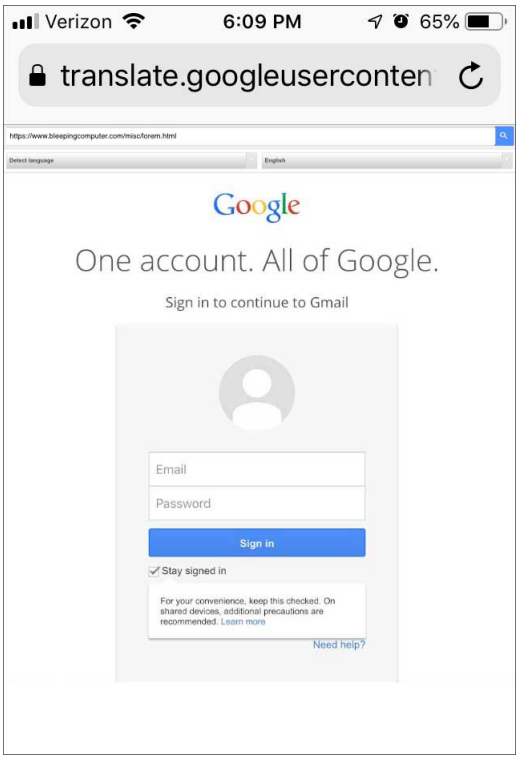

Figure 6.11: Phishing page camouflaged using Google Translate service, viewed on a mobile browser[77]

In June 2019, Kaspersky reported [78] on how spammers utilize Google services. Since Google or any other service provider do not want to hinder the flow of their own applications' traffic, they are unlikely to flag notifications from their own services as spam. This fact is leveraged by spammers to get their email messages to the victims' inboxes. In the Kaspersky report they show how spammers use the location and topic fields on a Google Calendar invitation to share malicious links with the victim. This works because by design, everyone can invite anyone else to a meeting with the meeting invite including a topic and other fields. Similarly Google Photos and Google Analytics are used to share images or analytics files along with phishing links

with an unsuspecting recipient. Google Drive and Google Storage are often used as the hosting for initial phishing pages and files. In some cases these Google cloud hosted files include a secondary link to the actual phishing page or malware.

In August 2019, Cofense reported [79, 80] on a new technique used by Trickbot banking trojan operators. The phishing email contained a link to a Google Docs document, a fake Google 404 page with another link to a file hosted on Google Docs. This downloaded document was an executable masqueraded as a PDF, containing the Trickbot malware that would run and obtain persistence if the file was opened.

In September 2019, Confense reported [81] on a phishing campaign using Captchas in order to bypass secure email gateways. As security products develop their capabilities, the attackers have to come up with new ways of evading them. In this case the phishing threat actors incorporated the use of Captchas to evade automated URL analysis done by the secure email gateway. The phishing emails were sent from a compromised account in the form of a voicemail notification. The email included a link that would take the user to a Captcha screen and after completion a fake Office 365 login screen would be shown. Both the Captcha and the phishing page were hosted on a Microsoft domain, allowing the attacker to benefit from the positive reputation of the domain and the SSL certificate.

In February 2020, Cofense reported [82] on phishing operation utilizing Google Forms for credential harvesting. The attacker had access to a compromised email account and used it to bypass basic email security checks including DKIM and SPF. By using a legitimate compromised account, the attackers were also able to bypass popular email gateways. The phishing emails came in the form of Office 365 update email, with a link to a form hosted by Google. After the victim enters the credentials the data is transferred to the attackers Google Drive.

In July 2020, Checkpoint published a report [83] detailing techniques used by phishing campaigns in the wild. On the earlier campaign the attackers hosted their phishing pages on Google Cloud Storage and on a later one, the attackers started using Google Cloud Functions to hide their own domains even better as it allowed the content to be loaded directly from Google Cloud Functions. The researchers were able to tie multiple different campaigns together as domains used for hosting phishing pages resolved to the same Ukrainian IP address. The report details some development in the phishing campaigns over the years. The attackers had started by hosting their phishing pages on their own infrastructure directly, then moved to Azure Storage and later to Google Cloud Storage.

In September 2020, Armorblox published a report [84] on a highly tar-

geted phishing operation that performed real-time Active Directory authentication. The phishing email came with an attachment containing HTML and opened a web page impersonating O365 login form. After entering the credentials, the attacker used Office 365 authentication API to check the validity of the credentials, then forward the victim either to the real O365 login page or to Zoom home page, depending on the result. The usage of authentication API gives the attacker immediate information on the validity of the credentials and a possibility to serve different content based on the result of the authentication query. The phishing emails were sent using Amazon Simple Email Service. The use of Amazon SES helped the attacker to avoid DKIM/SPF failures and to bypass spam filters.

In January 2021, Abnormal Security reported[85] on an operation in which BEC scammers were using a loopholes in Microsoft 365 read-receipt and out-of-office (OOO) reply functionality. In the case of the read-receipt attack, the attacker manipulates the Disposition-Notification-To email header in order to make Microsoft 365 to send a read-receipt notification message to the sender. This allows the attacker to get their message to the inbox of the target, even if the actual message sent by the attacker is blocked by the email security gateway. The out-of-office attack worked by the attacker impersonating an employee that had their OOO-reply enabled, sending them a message with a modified Reply-to email header field that points to another employee of the organization. The reply message was then sent by the original recipient and thus it would likely not be blocked. In both of these attacks the attacker successfully bypasses the email security systems by bouncing messages from inside the target organization.

In April 2021, Group-IB published a report [86, 87] showing the newest trends in phishing data exfiltration. The report revealed that cybercriminals have been increasingly incorporating the usage of legitimate services into their operations. They found that phishing attacks had started to use Google Forms and private Telegram bots for data exfiltration. They also note that there exists cybercrime-as-a-service type platforms for sale on the darknet, that utilize Telegram bots to automate the phishing process. The research concentrated on analyzing phishing-kits, tools for building and operating phishing pages, and the way they are used. The majority of the phishing kits still use email as the data exfiltration method, but new methods are emerging. The phishing kits use Google Forms by sending a POST request with the base64 encoded data to a hardcoded Google Forms URL.

In May 2021, Kaspersky published a report [88] on a phishing campaign using Google Docs to deceive the victim. The email came with a supposed link to a file. The supposed file that appears to be an office document on Microsoft OneDrive showing a screen with a button to open the document.

The opened screen was actually a Google Docs presentation showing a slide that opened automatically in full screen view mode. The button on slide had an embedded link and when clicking on it the user was redirected to a phishing login page impersonating Office 365. This phishing page was hosted on Amazon AWS.

In August 2021, Perception Point published a report [89] showcasing a new novel phishing operation using Salesforce for phishing email delivery. The reported operation used Salesforce Mass Email service to deliver emails to the victims, abusing the fact that Salesforce is commonly used by organizations. Salesforce recommends for the customer organizations to allowlist their whole IP range and since the organization is expecting only benign traffic from the application already used by the them, the attackers can use this as an open attack avenue. Mass Email also allows the attacker to create personalized emails, making the phishing email even more credible. In this case the attacker impersonated the Israeli Postal service and within the email, they provided a link to a spoofed Israeli postal service website asking for the victim's credit card information. The attackers had also obtained a SSL certificate for their phishing site.

In August 2021, Microsoft published a security report [90] detailing a large scale phising operation that was abusing open redirect links and Captchas. The emails originated from a large selection of domains including compromised, domains from different country code top-level domains (ccTLDs) and attacker-owned domains using domain generated algorithms. The emails were impersonating known large service providers and invited the victim to open a link to check related information. The links were using open redirect with a legitimate domain that would likely be one to be trusted by the victim (see figure 6.12). Open redirection functionality can be used for legitimate traffic redirection by the organizations, but in this case it allowed the attacker to redirect the traffic to their malicious phishing pages. Initially the link redirected the victims to a Google reCAPTCHA challenge to avoid automated URL analysis and after completion it would redirect the user to a phishing page impersonating different login pages. The recipient's email address was also prefilled into the login form. The automated form fill was actuated by adding victim information in the PHP parameters of the link, that would then render in the phishing page. In some cases the phishing pages also had extra details to tie the phishing page to the organization of the victim. After the login form, the user was shown a legitimate Sophos cloud success screen.

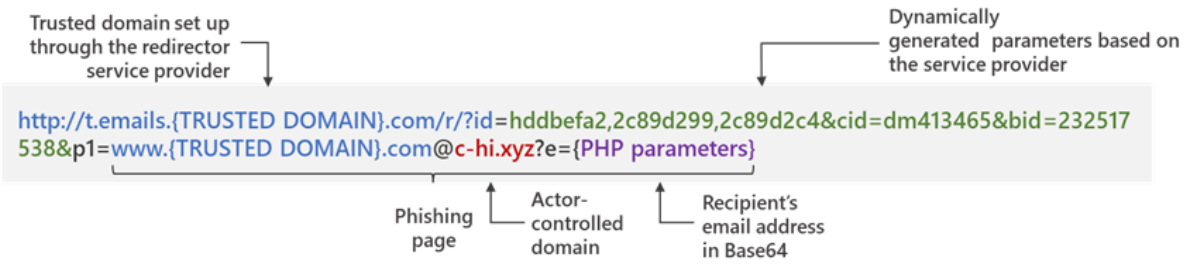

Figure 6.12: Open redirect phishing URL[90]

6.3.2.2 Case example: BEC phishing operation

In June 2021, Microsoft 365 Defender researchers published a report [16] on the details of a large BEC operation. The attackers started the operation with a phishing email containing a voice message lure and an additional HTML document attachment. The email was sent from an external cloud provider's address space. The HTML document contained JavaScript code that dynamically decoded a page mimicking Microsoft login page, which had the username field already provided. After the user provided their password, the JavaScript exfiltrated the credentials to the attackers server with a POST request, while the HTML page shows an animation and ends up with a message for a deleted or moved file.

The timeline showed that soon after receiving the phishing emails, new email forwarding rules were created. Creating email forwarding rules is a common and persistent data exfiltration method, used especially in BEC attacks [91]. The mailbox rules were set to forward potential financial emails using keywords including invoice, payment and statement. Another rule also deleted the forwarded emails to evade detection.

The research also showed that the attackers had automated the process using virtual machines (VM) hosted by another cloud provider. They had assigned a different VM for each step of the process and running the tasks out of sync time wise. This result in all the actions being done from a different IP address at different times, making connecting the dots more difficult for the defenders. The automation dealt separately with adding the forwarding rules, monitoring the accessed mailboxes, managing the forwarded emails and figuring out the most lucrative targets from gathered data. To further blend into the email traffic, the attackers had also set up multiple DNS records to mimic the legitimate corporate domains. After identifying and choosing the targets, the attackers had also tried to use a tool to pull the emails from

the target's mailbox, using a POP3/IMAP client. Over the last couple of years, using legacy protocols e.g. POP3/IMAP has been a common method to effectively bypass the multi-factor authentication (MFA) [92].

This report points out how wide the defence approach has to be in order to be able to effectively identify and defend against these types of operations. Singular events can be distributed and cues to tie the different actions together are few.

6.3.2.3 Email phishing TTPs relating to the cloud

Most notable phishing methods

- Using SaaS applications to deliver emails or notifications including phishing links to other users of the same service
- Using a SaaS service to masquerade a phishing page content to be from a reputable source like a cloud service provider
- Using a fake cloud hosting 404-page with a link to a file download to deceive the victim to download a malicious document instead of viewing it in the browser
- Using Captchas to bypass secure email gateways
- Cloud service provider logo, domain and login page impersonation
- Hosting phishing pages on a cloud hosting provider, phishing for credentials for the same hosting providers services
- Using access to a compromised email account to send emails, bypassing security checks
- Using SaaS services for phishing data and credential gathering
- Using Function-as-a-Service(FaaS) offerings to run phishing operation, hiding infrastructure and gaining legitimacy
- Using an cloud authentication API to check credentials submitted to phishing page in real time
- Using SaaS service functionality loopholes to deceive, and bypass email security gateways
- Using SaaS services and applications for phishing page data exfiltration

- Using open redirection to create malicious phishing links with legitimate domain

Other actions related to the phishing operations

- Creating new email forwarding rules for persistence and data exfiltration, additional rules to evade detection
- Automating different parts of the operation using cloud VMs
- Pull email data using legacy protocols including POP3/IMAP, effectively bypassing MFA

Chapter 7

Discussion

In this chapter we will discuss cloud environments as targets of an attack, dissect the findings from the case studies, highlight the evolution in the TTPs and implications of that evolution. By identifying the prevalent TTPs of the threat actors we aim to identify the weak points or problematic areas in the cloud.

7.1 Cloud environments as targets

As discussed in the previous chapters, cloud services offer a great deal of opportunities for organizations to operate, but many of the very same benefits also work in favor of cybercriminals using the cloud or attacking organizations utilizing the cloud.

Cloud adoption has meant that the corporate IT environments are getting increasingly complex. Businesses are adding cloud elements to their systems and integrating cloud and on-premise systems together, increasing the amount of systems and assets to manage. Cloud usage has also dictated changes in the asset management structure of the cloud client organizations. All new asset acquisitions do not need to go through the IT department, as developers and other staff can easily spin up servers as needed. This change in asset management means that the attackers have a better chance of finding unmanaged or unsecured cloud network assets. As an example of this, the case study on TeamTNT cryptojacking shows how misconfigured Docker daemons are a viable target.

Cloud offers cloud customers easily scalable environments with near unlimited computational resources and from the point of view of cryptojacker operators, this appears very lucrative. As executed by the TeamTNT cryptojacking operators, who focus on exploiting wormable vulnerabilities and

misconfigurations. Cloud customers' cloud asset deployments are based on the tools and default configurations offered by the cloud srevice providers, thus deployed assets in different customers' environments can share common problems. The TeamTNT operations are a good example of how the use of client run containerization on the cloud has had the effect of producing easily exploitable uniform misconfigurations across clients.

On the other hand, the organizations' use of SaaS and PaaS offerings has changed the landscape of exploitable vulnerabilities from the attacker's point of view. Critical vulnerabilities are rarely found in the major cloud platforms (of course there are exceptions [93]). The difference is that generally the cloud platform vulnerabilities are either unpublished zero-days that are not known to the general public, or published vulnerabilities known to the vendor, also known as n-days, that have been fixed by the service provider. The centralized manner in which cloud platforms work mean that they do not always have the same patch gap problem as on-premise systems might have, relying on the IT personnel to keep the systems up to date. Once a security patch or mitigation has been implemented and updated to the platform, the issue has been mitigated. This does not apply in the same way to the cloud applications used by the customer on their endpoints or other systems. These applications often have automatic updates enabled by default, but are still vulnerable to patch-gap issues if misconfigured.

Although infrastructure and platform software updates are the responsibility of the service provider, this also implies a trust relationship the cloud customer has with the service provider. In the case of the Magecart Volusion attack [39], the targeted attack on the service providers systems allowed the attackers to inject malicious code to the trusted libraries that were then distributed to the Volusion customers.

Cloud systems are inherently highly connected systems and can provide great opportunities for lateral movement inside the given platform or across to other connected cloud platforms. As an example, the EA data breach [94] where the attackers purchased a Slack (a communication and collaboration platform) cookie off an online marketplace, used it to get access to the company's cloud systems and started a virtual machine for better visibility and exfiltrated source code data. One often discussed topic regarding cloud connectedness is the weakness to Server-Side-Request-Forgery(SSRF) vulnerabilities, that in the case of AWS cloud environment might allow the attacker to query the metadata instance for valuable information, including AWS IAM role credentials.

Cloud applications can be used by organizations as if they were an internal applications, but in reality much of the underlying infrastructure and security is handled by the service provider and the same service is used by other

organizations and users. As seen in the phishing case study section, this can cause interesting insider threat style scenarios, where the attacker is able to bypass security controls by using the same service as the target. By using the services' own features for connecting to the victims, the attacker is able to use the allowlisted application traffic as a way to bypass defences. The fact that these types of attacks are often mitigated by changes that would affect the usability of the application, the service providers are not keen on restricting the features by default.

The wide adoption of public cloud for infrastructure hosting has also brought a change in the hosting systems. 90 percent of the public cloud infrastructure is run on Linux [95] and this has an effect on the interests of the malware writers and cybercriminals accordingly. Malware is being adapted to work on Linux and part of the new malware is directly targeting Linux systems. Previously known malware families including Trickbot [96] and RansomEXX [97] have added Linux variants. Advanced malware has been directly targeting Linux systems[98] and botnet and worm-like malware have taken Linux as their primary target, as seen in section 6.2 as well as in other examples [99, 100].

7.1.1 How attackers relate to the cloud

In chapter 6 we presented the reported actions of a couple of threat actors that have taken on the cloud as an attack target and in the case of phishing we showed a broader overview on the evolution of the techniques along with another detailed well-reported attack. In the case studies the attackers had different end goals for their operations, aiming for different methods of monetization. This is interesting since, for the cybercriminals to move to a new domain like the cloud in this case, there needs to be a new, more lucrative target. Monetarily motivated cybercriminals can of course be seen to have a fairly straightforward goal of turning their operations into money, as effectively, securely and easily as possible. These three factors will help in dissecting the attacks further.

As seen in the case studies cybercriminal operations can differ largely in how these operations relate to the cloud. The variety of threat actors use the cloud for different means: For example phishing campaigns use the cloud for credibility, agility and evasion; formjacking operators use the cloud for the great reach it offers; and cryptojackers for abusing the uniform exploitability and resource availability.

As much as attackers see cloud as a target, it also provides them operational tools. Those operational capabilities can be divided into four main categories:

- malware hosting platform
- malware delivery channel
- phishing platform
- command, control and exfiltration channel

The case studies show how this thinking has been adopted by the cybercriminals. Phishing operations utilize cloud hosting and cloud applications widely for all the aforementioned categories of operational abuse. Attackers have found cloud to be a great tool for evading automated analysis tools and keeping their own infrastructure (e.g., domains and IP addresses) hidden.

The development of attacker tactics and techniques has also shown a change in how the cybercriminals relate to the cloud. In the case studies, many of the earlier attacks on the cloud mostly see cloud as an extension to the attack surface: Magecart abusing misconfigured S3 buckets and cryptojackers misconfigured Docker instances. Many of the recent attacks have shown that the attackers adopted more of the cloud services as tools for their attacks: Magecart using Google Analytics to bypass Content Security Policy restrictions and cryptojackers using the AWS Command Line Interface (AWS CLI) tools to enumerate the cloud environments for IAM configurations, EC2 instances, among others. This type of service abuse can also be difficult to detect from the defender's perspective, as attackers are using legitimate administration tools (e.g. AWS CLI) the context of the tool usage becomes a considerable factor.

On the cloud control plane, attacker techniques are blending in with normal activity. In the limited environment of control APIs, the attackers are forced to use the same tools to create and modify cloud resources as used by the legitimate users and administrators. This means threat detection in the cloud is based more on the telemetry and logging of actions. The defenders have a great view in to the actions of the attackers, but only if they are able to detect them from the flow of normal actions.

7.2 TTP evolution

Attack tactic and technique evolution is largely dictated by the changes in the attacked platform, it's features, issues and defences built against the attacks. In practice it means that the evolution of attacks against different platforms (or different platform types) vary. Attacks targeting a specific platform or abusing a specific feature of a platform are more probable to get a prompt

defensive response, thus causing a need to evolve the attack techniques. On the contrary, attacks abusing broader problems are less likely to be mitigated in a short period of time and thus attack technique evolution might not be as swift, or the attack technique development might be further weighted towards improving the impact or reach of the attack. This dichotomy in the evolution of the attacks was clearly visible in the case studies: attacks abusing misconfigurations continue to abuse the same initial access vectors, but have developed further post-exploitation and evasion capabilities, whereas attacks focusing on specific service providers' environments have needed to evolve more.

7.2.1 Attacks on SaaS environments

As discussed in the previous sections, cloud and specifically SaaS and PaaS environments have a different attack surface compared to traditional on premise solutions. This can be seen especially when examining threats including phishing. Attackers have adapted to use the cloud against itself, abusing the features for delivery, defence evasion and exfiltration.

In our case studies the reporting on phishing attacks and attack techniques shows how the attackers have been able to find new ways to better their phishing attacks. Most of the earlier attacks starting from 2016 focus on using cloud services to aid in the delivery of the phishing emails or to help with masquerading the phishing page to seem legitimate. These techniques include for example the usage of Google Translate for masquerading the phishing page as a Google-hosted legitimate login form, or bypassing security gateways and filters by using cloud applications to send notifications to the user.

Consent phishing emerged as new popular phishing method in early 2017. This method was earlier used by threat actor APT28 already since 2015 [101]. Since the beginning of OAuth phishing attacks, the attackers made use of techniques similar to traditional phishing: rotating application names and hosts to prevent blocks, masquerading application names, using unicode characters and creating believable social engineering pretexts to fool their victims.

These attacks slowed down in late 2020 after Microsoft released the published verification system. But as noted by Proofpoint [23], the threat was not fully mitigated, the attackers just made a shift in their tactics. As initially attackers could create malicious application freely, in practice they now needed to gain the publisher verification approval to continue their attacks. Because account compromises are so common in organizations [74], circum-

venting the publisher verification system was feasible. Attackers can then use the compromised account to create application in the tenant that already has the publisher verification and are then able to conduct the OAuth phishing operations again, this time armed with a verified publisher mark on the consent prompt.

Abuse of OAuth applications has been a common initial access vector, but applications have also been commonly abused for gaining persistence. These methods for gaining persistence include:

- authorizing another application that allows external API usage for access
- updating certificates
- stealing client secrets to generate access tokens
- gain access by application configuration changes
- adding reply URL to gain application token

To mitigate part of the most common persistence methods, Microsoft made changes to the external forwarding defaults in order to combat data theft and persistence through email forwarding, as usage of forwarding rules were a common technique used by attackers [91].

Traditional email phishing attacks also show a trend in their evolution. Many of the earlier reports on email-based phishing attacks mention techniques used for email delivery and phishing page or malware hosting, whereas more recent attacks include a broader range of tactics and techniques including usage of cloud applications for credential exfiltration, evasion among others. The attacks have proven the cloud service usage to be an attractive and effective way of operating for phishing campaigns. As an example how some aspects of cloud service usage provide considerable advantages for the attacker: a phishing email delivered from a Microsoft cloud email application, with a link to a phishing page hosted on the Microsoft cloud, having a Microsoft CA signed SSL certificate, asking for Microsoft cloud credentials.

The earliest attack report included in the case study, a report [75] from 2016 by Avanan, details the Cerber ransomware delivery campaign using a private Office 365 account to bypass the built-in security tooling. Similarly, five years later in 2021, Perception Point reported [89] on a phishing campaign using Salesforce Mass Email service to deliver personalized phishing emails, bypassing the security controls. The report even noted that most email

security services have Salesforce set as a trusted safe source and thus were unable to detect the phishing emails. This example shows how surprisingly slow the service providers have been to react to the known possibility of abuse of their services.

Reports of spammers abusing Google services have also been published years before the Cerber campaigns [102]. In 2021, Google added a feature to block other users in Google Drive [103], after years of spam campaigns abusing the lack of power the users had on their Google Drive [104, 102, 105, 106]. The attackers have used a variety of techniques to contact their targets: adding to a Team Drive, using mentions, sharing files directly etc. The pattern is clear: using the applications for sharing or contacting the targets, which often bypasses anti-spam security features. The Google update gave the end user the option to block singular users from contacting them, but it failed to tackle the problem of phishing delivery through the service.

Other major cloud related tactics phishing operations have adopted is to use cloud services for command and control as well as evasion. The use of cloud hosting offers credibility, blends into the network traffic, takes away the need to maintain dedicated malware hosting infrastructure and offers tools to evade automated analysis attempts. Hosting phishing pages and malware on cloud service providers hosting services renders domain reputation based URL rating almost useless. In order to evade automated analysis, attackers have incorporated the use of captchas and nested links leading to the actual malware. As Netskope report shows, the percentage of malware delivered using cloud hosting has been growing year by year with the latest statistics reporting it reaching up to 68% [5].

During 2020, attackers started to utilize cloud services also for data gathering and exfiltration. Cofense reporting [82] on a phishing campaign using Google Forms and Group-IB report [86, 87] pointed out the trend of phishing kits utilizing Telegram and Google Forms for data exfiltration. Similar to phishing, the use of common services affords less obvious outgoing connections to blend into the network traffic, makes attribution more difficult, and lessens the burden of infrastructure management.

7.2.2 Attacks on IaaS and containers

Containerization is a major tool for cloud infrastructure, offering an agile, scalable and lightweight solution for managing cloud assets. For the ease of deployment and agility, it also carries the common misconfiguration and shadow IT deployment problems. This has been seen to be a largely exploited issue, from singular attacks to hijack organizations cloud infrastructure to full fledged worms. Cryptojacking has been one of the most prevalent attack

types seen on cloud containers.

Misconfiguration abuse for cryptojacking has been a common occurrence in the past years and moving to the cloud was the obvious course of evolution. At least since 2017, malicious Docker images impersonating popular projects (e.g., Cron, Tomcat) and running cryptojacking software have been found on Docker Hub [107]. Automated attacks scanning the internet for misconfigured Docker and Kubernetes instances date back at least to 2017, with reports on large companies getting breached [108, 109].

In 2019, the attacks moved from automated scanning to independent worms. Since then the attacker techniques have changed to best suit the worm functionality. The earliest detected worms focused on exploiting misconfigured Docker instances, later expanding to Kubernetes.

TeamTNT has progressed their cryptojacking operations considerably over time. They have shown to be very capable of quickly taking up new techniques and to find new avenues of exploitation. The main development has been putting additional effort into evasion and post-exploitation capabilities. One combining factor on all the campaigns is that the initial access vectors did not change, even after the operations have been running for multiple years: exploiting misconfigured public-facing applications has continued to be an effective way of entry into the environments. Misconfigured Docker APIs were their main target in the past, but later on they expanded to attack misconfigured Kubernetes instances as well. By default Docker API is not bound to a public facing interface, but often users want to be able to access the Docker instance remotely and attach it to a public interface exposing it to the internet. Unfortunately it is easy to find guides on how to bind your Docker API to a public-facing interface, but some do not even mention the need of authentication.

The current progress is clearly pointing towards advancing the capabilities for lateral movement and utilizing all found credentials to spread wider in the compromised infrastructure. Earlier campaigns do not focus on exfiltrating sensitive data or credentials, but have a set focus on cryptojacking with some DDoS capabilities. The following campaigns began to look for AWS credentials, but were not directly using them, merely exfiltrating to the C2 server. At this point they also incorporated further post-exploitation capabilities trying out different open-source attack tools.

TeamTNT malware have not yet been reported to be utilizing cloud service credentials other than the found AWS credentials. At the time of writing this thesis, there have been no attacks on any other cloud platforms directly linked to TeamTNT activity. Taken that TeamTNT has almost exclusively focused on cryptojacking operations, it could be expected that they would

expand their operations to other platforms in the future, especially now after having possibly acquired credentials for those platforms. Another possibility is that TeamTNT has been acting as an initial access broker (IAB), selling the working credentials to other criminals.

The exploitation of misconfigured container management systems has been heavily concentrated to resource hijacking [21], but vulnerable APIs pose a larger threat in certain environments. Cryptojacking can be considered a fairly minor threat as it generally does not pose a similar destructive risk as ransomware or other attacks with a serious impact.

Supply chain attacks and cloud compromise for payload delivery. As cryptojacker operators saw the opportunity for misconfiguration abuse, similar ways of abusing access to misconfigured cloud storage systems were also taken up by other types of cybercriminals. Magecart groups and similar attackers have been seen to use different attack methodologies ranging from highly targeted attacks [33] to high volume attacks targeting vulnerable Magento stores [110]. During 2019, different Magecart groups took these same attack methodologies to the cloud, attacking misconfigured AWS S3 buckets with high volume [20] and cloud service providers like Volusion [39] with a targeted supply chain attack.

Supply chain attacks have emerged as a considerable threat in recent years as multiple high-profile supply chain attacks have dominated the news cycles. Cloud service providers' offerings are becoming increasingly popular and companies are relying on service providers to keep their systems and applications running. This centralizing development means that service providers have become the higher value targets. As seen in the Magecart case study, by compromising the cloud infrastructure of the managed service provider(MSP) Volusion, the attackers were able to inject code into libraries served to all of their customers and stay under the radar, abusing the trust the Volusion customers placed on the service provider. Similarly ransomware operators have been heavily targeting MSPs already for years [111, 112].

Many common technology stacks used in for example cloud containers rely on open source software packages. These software packages can sometimes depend on a single person to patch vulnerabilities and maintain the code base. These packages have been seen to be a target for delivering malware [113] and the cloud supply chain can be vulnerable to these kinds of attacks.

Software vulnerability exploitation has also been a viable method of entry into cloud environments. As more of the organizations' infrastructure is in the cloud, new software is also being built to be cloud compatible and is

often meant to be run in containers. For the IT team updating the software, it can still pose some of the same issues as updating on-premise software. In June 2021, a report [114] on a new malware targeting Kubernetes systems through Windows containers was published by Unit 42. It described a new malware exploiting n-day vulnerablities in common web applications to gain initial access to a Windows container. The malware attempts to escape the container and spread in the Kubernetes cluster. This new malware displays how exploiting publicly known vulnerabilities is still a viable initial access vector into IaaS environments and has the possibility to compromise the cloud environment when combined with container escape capabilities. In 2021, the IBM Security X-Force Cloud Threat Report [115] noted the exploitation of software vulnerabilities running on IaaS systems as one of the most common initial access vectors for attackers.

7.3 Security problems in the cloud

As seen in the previous sections, moving to the cloud has changed the threat landscape organizations face. Some of the major changes are caused by the changes in the infrastructure and network schemes. Using externally managed SaaS solutions has relieved the organizations' IT teams from some of the software update burden, but as attackers are using the same services, it has offered new avenues for social engineering attacks, and more covert ways of malware delivery and data exfiltration. The malicious use of cloud services is clearly a trend in cybercriminal operations and it has proven to be problematic for the defenders. Connections to previously trusted domains of cloud service providers are used for malware delivery, C2 connections, and data exfiltration. The lack of granularity in certain defense mechanisms is causing problems when combined with cloud services, as seen in the example of Magecart using Google Analytics in order to bypass CSP limitations.

Cloud is being used as attacker infrastructure. Service providers have an important role in the fight against the malicious use of their services. In their research into criminal cloud hosting usage, Liao et al. [116] note the importance of the service provider to step in aggressively to detect and remove the malicious content, as third parties without full visibility to the repositories and their usage have limited possibilities to detect malicious repositories. Tajalizadehkhoob et al. [117] research into hosting providers role shows that the cybercriminals do not seem to prefer providers that react slower to malicious hosting, but pricing and storage space are much more important factors for the attackers. This might mean that the level of effort taken for

the attackers to rebuild their infrastructure on another cloud account after a take-down is so low, that the risk of take-down is not as relevant. This is also pointed out by a Kaspersky report on the evolution of Russian cybercrime [118]. Indeed as mentioned by Liao et al. [116], service providers are reluctant to conduct active inspections of customer data because of privacy and ethical concerns. The ease with which cybercriminals are able to set up supporting cloud infrastructure for their attacks enables their campaigns to be more agile, less affected by take-downs, and more difficult to track based on IoCs including IP addresses and domains.

Cloud services are a tool for phishing and malware delivery. Service providers are facing a problem with the abuse of their services as seen in the case studies. For example Google's services have been used extensively to aid in the delivery of spam and phishing messages. Still, the effective mitigations to many of the delivery techniques have been lacking or inadequate, since the service providers do not want to impair the ease of use of their own services. The long list (see section 6.3.2.3) of examples of attacker techniques related to phishing using cloud indicates the scale of the problem cloud service providers face.

Misconfigurations have continued being a major issue in the cloud. Threat actors like TeamTNT have continued their operations of abusing misconfigured systems for resource hijacking. Cloud role and access control misconfigurations are still key to escalating the damage caused by account compromises. The issue of misconfigurations in managed services has been pointed out to be largely due to the usage of default security profiles and configurations provided by the service provider [119]. The slowness of the cultural shift to tackle the problem of shadow IT is still resulting in misconfigurations and mismanaged assets.

Similar to the issue of using cloud services for phishing delivery, offering lax default configurations has been an issue relating to the ease-of-use for cloud customers. Service providers prefer their offerings to have a lower entry barrier, but with the side effect of causing the cloud instances to have unsecure initial configurations. Accurics Cloud Cyber Resilience report [120] points out that 22.5% of cloud violations in their customers' environments were due to unsecure configurations of managed services with majority of them being caused by the use of default security profile and permission configurations. Some of the configuration changes are slow to take effect. As an example, legacy protocols such as POP and IMAP have been extensively used for MFA bypass [92]. Still, at the time of this writing both are enabled by default for all users in Microsoft Exchange Online [121]. To combat

the abuse Microsoft released *security defaults* [122] to harden the systems, including blocking legacy authentication, and for tenants created after October 22nd 2019 *security defaults* are enabled by default.

Problems are underlined by the issue of misplaced trust. The change from an internally-hosted infrastructure where services used by the company are trusted by default and the traffic inside the on-premise network is benign by default, to a hybrid or a fully cloud based infrastructure means the attitude towards trust needs to change. Many of the problems seen in the case studies boil down to adapting to the culture change needed to secure the systems. The consequences of opening an unauthenticated Docker API in an internal network differ largely from a cloud hosted publicly accessible instance. Security of internal file sharing is not the same anymore when attackers use the same services to distribute malware. Phishing emails are bypassing security checks as they are being sent using functionality offered by high reputation cloud service providers. Practically almost all of the different attack types discussed in this thesis are in one way or another benefiting from two main issues of trust: the trust users and organizations place on the service providers, and the slow process of acclimation to an environment where services, users and entities cannot be trusted.

7.4 Expectations for the future

In this section we will briefly present some of our expectations for the general direction of cybercriminal activity in the cloud environments based on what this research has shown.

The attacks against cloud environments as well as attacks abusing cloud services have been constantly changing. The attacks will likely continue to evolve following the development of these services and environments. Every time a threat actor finds a new way of abusing a service or functionality, others copy the same techniques to better their attacks. These shifts in the attack patterns are dictated by what techniques require the lowest effort, yield the highest gains, and have the lowest risks involved. Less technically advanced attackers will likely continue to operate with a more opportunistic approach, exploiting misconfigurations and phishing for access, whereas more advanced attackers might opt for targeted attacks in the cloud supply chains or more complex hybrid environments with faulty integrations.

As is the case with other vulnerability exploitation [123], vulnerabilities affecting cloud deployments will likely be exploited increasingly quickly after being published by the vendors or exposed otherwise. In the case of

OMIGOD vulnerability [124] vulnerabilities affecting Microsoft Azure VMs, threat actors were observed actively exploiting the vulnerabilities only two days after they were disclosed by Microsoft.

More complete exploitation. In their 2021 H1 cloud threat report [125] Palo Alto noted that they observed for the first time a decline in cryptojacking attacks in the cloud since beginning to track the activity in 2018. Observing the evolution of the cryptojacking malware, for example in the TeamTNT campaigns detailed before, we can see how malware has become more automated and is expecting to encounter other similar malware. This evolution points to the saturation of the cryptojacking attacks (at least in the case of misconfigured Docker instances), and thus the decline in the volume of the attacks is expected as it becomes less lucrative because of competition. But as competition grows and the amount of vulnerable Docker instances goes down there is further incentive for the malware to extract the maximum benefit from the target. Developing more automated credential scraping and lateral movement capabilities makes sense.

Unit 42 report [126] also pointed out how IAM misconfigurations give a multitude of possibilities for the attackers to further compromise the vulnerable AWS environments. The scale of the infrastructure is making it difficult to keep the systems consistently secure. The later TeamTNT campaigns have already included wide cloud enumeration, thus an automated extended use of the found data, credentials and vulnerable IAM configurations is something that could be expected in the future.

More use of open-source attack tooling. As seen in the case of TeamTNT cryptojacking attacks, over time the campaigns evolved to have more capabilities in enumerating and pivoting in the cloud environments after initial access. These actions were largely supported by available attack tools designed for cloud environment enumeration and pivoting. In IaaS environments especially, the usage of attack tools help the attackers to automate the attack flow and speed up the process of spreading. In environments similar to those targeted by TeamTNT, the amount of misconfigured systems, permissions and network segments caused by shadow IT offer an easy path of exploitation for the attackers.

In the future, the usage of attack tools might also extend to SaaS environments. An example of a SaaS attack tool is a Google Apps Script document enumeration spider tool PaperChaser [127]. In his DEF CON 29 talk [128], Matthew Bryant, the developer of PaperChaser, explained the implications of sharing files with links as opposed to sharing them with users or groups directly. The spider takes advantage of the link sharing to find all accessible

but not searchable documents.

More feature and allowlist abuse. The usage of cloud service features and the corresponding allowlisting was present in all of the different types of cybercrime examined in the case studies. The problem of feature and allowed traffic abuse is inherently going against the ease-of-use and agility, that are some of the main selling points of cloud services. By using the same services and features the targeted organizations use, the attackers have a greater chance of blending in and bypassing restrictions. Cloud platform security is inherently different from on-premise networks and partially forces the attackers to abuse legitimate features. Especially in SaaS environments the service functionality offers the attackers tools for attacks, meanwhile detection and defences placed in these services can rely heavily on the service provider, who is not inclined to limit the functionality for the sake of security.

More attacks on the cloud supply chains. Cloud supply chains have suffered attacks affecting large user bases and it is a trend that is not necessarily easily fixed. The way technology stacks commonly deployed in the cloud have nested dependencies on open source packages maintained by few people means scrutinising the code base is expensive. Furthermore the safety of the supply chain for a given package can depend on the security posture of a singular developer.

Similarly managed service providers have been a target for ransomware threat actors and more. These types of organizations and businesses that have a trust relationship with a multitude of companies will likely be a highly valued target also in the future.

Chapter 8

Conclusions

8.1 Summary

In this thesis we presented the current state of cybercriminal activity in cloud environments, with emphasis on the TTP evolution. We did this by reviewing reports on threat actor activity, news on attacks and attack techniques in a form of case studies.

The case studies provided an overview of the attack technique evolution in the specific niches of cybercrime. The research showed a clear trend towards a more diverse and widespread use of cloud services as tools for attacks. In many cases earlier attacks showed a simpler approach of using cloud hosting or cloud based email services for malware distribution, whilst recent attacks introduced a significant amount of different techniques used for defence evasion, data exfiltration etc. Cybercriminals have embraced cloud services as a new set of tools for malicious activity using cloud applications for malware hosting and delivery, IaaS services to host their infrastructure and cloud native benign third party applications for persistence.

Threat actors like Magecart groups and TeamTNT have found success in starting to target cloud instances by abusing common misconfigurations and benefiting from the connectivity and resource availability that the cloud offers. Both groups have demonstrated highly effective techniques abusing the cloud for great reach. On IaaS environments and containers cryptojacking has been common occurrence, and while threat actors have found new applications to target, misconfiguration abuse has continued being the initial access method of choice. Magecart and other actors have also targeted cloud supply chains in order to maximize the reach and impact of their attacks. As the cloud is inherently more centralized and applications are built on a multitude of nested dependencies, supply chain attacks are a high impact

target.

Attacks on SaaS environments have focused on different forms of phishing. Consent phishing emerged as a new popular phishing method and has then been targeted by new defence mechanisms by the service providers. Traditional email phishing has seen an ever growing variety of services and functionality used to bypass security checks and automated analysis technologies. The use of cloud service providers own offerings against their customers has proven to be effective as service providers are hesitant to limit the use of their services and are careful not to impair the ease-of-use the services aim to offer.

Issues causing the attacker actions to be successful are centered around the ease with which cybercriminals are able to use cloud services for their operations. They enable a variety of operational benefits for the attackers. Other aspects of the issues are caused by the complexity, shadow IT and need for cultural change in how security is managed. In general, misconfigurations, cloud application vulnerabilities and misplaced trust on the used services have been some of the most common causes for security incidents.

This thesis gives an overview of the state of cybercriminal tactics, techniques and procedures in the cloud environments. The primary purpose of the study was to compile information of observed attacker actions to be then be utilized for securing organizations. The provided overview on the evolution of the attacker methods gives defenders more tools to know what to expect in the future.

8.2 Limitations and future research

The research was conducted using publicly available reporting and material. This limited the study depth, especially regarding the details of post-compromise actions taken by the threat actors. Thus the study was not able to fully map the post compromise TTPs of attackers in all scenarios. The sensitive nature of certain types of incidents limits the research if insider knowledge is not available. The differences in attacked platforms and types of attacks also dictated the level of available details, as some environments (e.g., containers in IaaS environments) were attacked largely in an automated manner, honeypot deploying studies were a viable option and therefore the sensitivity problem was averted.

Meaningful future research could focus on targeting the threat actor post-compromise actions and evolution specifically, comprising of TTPs for persistence, privilege escalation, defence evasion, discovery and lateral movement. Especially cloud-to-cloud and on-premise-to-cloud lateral movement

is an area of interest, as integrations are generally more complex and these interfaces are a likely target for attacks.

Bibliography

[1] The MITRE Corporation, "Mimikatz," Referenced: 29.10.2021. [Online]. Available: https://attack.mitre.org/software/S0002/

[2] The MITRE Corporation , "Steal or Forge Kerberos Tickets: Kerberoasting," Referenced: 29.10.2021. [Online]. Available: https://attack.mitre.org/techniques/T1558/003/

[3] N. Jones, "How the cloud has changed detection," 3/2020. [Online]. Available: https://www.f-secure.com/en/consulting/our-thinking/how-the-cloud-has-changed-detection

[4] Netskope Threat Labs , "Cloud and Threat Report - 2021 February Edition," 2/2021. [Online]. Available: https://resources.netskope.com/cloud-threat-report/cloud-and-threat-report-february-2021

[5] Netskope Threat Labs, "Cloud and Threat Report - 2021 July Edition," 7/2021. [Online]. Available: https://go.netskope.com/rs/665-KFP-612/images/2021-07-Cloud%20and%20Threat%20Report-RR-474-1.pdf

[6] C. Kim, B. Newberger, and B. Shack, "Computer Crimes," 2012. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-7

[7] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*. IEEE, 2012, pp. 198–205.

[8] CloudPassage, "Shared Responsibility Model Explained," 8/2021. [Online]. Available: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

[9] Microsoft, "Shared responsibility in the cloud," 2021. [Online]. Available: https://docs.microsoft.com/vi-VN/azure/security/fundamentals/shared-responsibility

[10] Goyal, Sumit, "Public vs private vs hybrid vs community-cloud computing: a critical review," *International Journal of Computer Network and Information Security*, vol. 6, no. 3, p. 20, 2014.

[11] D. Hardt *et al.*, "The OAuth 2.0 authorization framework," 2012.

[12] J. Ellis, "Phishing Campaign Uses Malicious Office 365 App," 11/2020. [Online]. Available: https://www.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset/

[13] IBM Security X-Force® Incident Response and Intelligence Services (IRIS), "Cloud Threat Landscape Report 2020," 6/2020. [Online]. Available: https://www.ibm.com/downloads/cas/Z81AVOY7

[14] P. Mansfield, "Shady deals: The destructive relationship between network access sellers and ransomware groups," 10/2020. [Online]. Available: https://www.accenture.com/us-en/blogs/cyber-defense/destructive-relationship-between-network-access-sellers-and-ransomware-groups

[15] CISA, "Brute Force Attacks Conducted by Cyber Actors," 3/2018. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/TA18-086A

[16] Microsoft 365 Defender Research Team, "Behind the scenes of business email compromise: Using cross-domain threat data to disrupt a large BEC campaign," 6/2021. [Online]. Available: https://www.microsoft.com/security/blog/2021/06/14/behind-the-scenes-of-business-email-compromise-using-cross-domain-threat-data-to-disrupt-a-large-bec-infrastructure/

[17] J. Hutchings, "Introducing new ways to keep your code secure," 5/2019. [Online]. Available: https://github.blog/2019-05-23-introducing-new-ways-to-keep-your-code-secure/

[18] Trend Micro, "Data on 123 Million US Households Exposed Due to Misconfigured AWS S3 Bucket," 12/2017. [Online]. Available: https://www.trendmicro.com/vinfo/pl/security/news/virtualization-and-cloud/data-on-123-million-us-households-exposed-due-to-misconfigured-aws-s3-bucket

[19] D. Fiser and A. Oliveira, "ESG Research Report: The Maturation of Cloud-native Security," 7/2021. [Online]. Available: https://www.esg-global.com/research/esg-research-report-the-maturation-of-cloud-native-security

[20] Y. Klijnsma, "Spray and Pray: Magecart Campaign Breaches Websites En Masse Via Misconfigured Amazon S3 Buckets," 7/2019. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets/

[21] A. Sasson, "Docker Honeypot Reveals Cryptojacking as Most Common Cloud Threat," 5/2021. [Online]. Available: https://unit42.paloaltonetworks.com/docker-honeypot/

[22] M. Vergelis, "How spammers use Google services," 6/2019. [Online]. Available: https://www.kaspersky.com/blog/spam-through-google-services/27228/

[23] A. Friedman and I. Clarke, "How Attackers Use Compromised Accounts to Create and Distribute Malicious OAuth Apps," 5/2021. [Online]. Available: https://www.proofpoint.com/us/blog/email-and-cloud-threats/how-attackers-use-compromised-accounts-create-and-distribute-malicious

[24] OWASP Foundation Inc., "OWASP Top Ten," 2021. [Online]. Available: https://owasp.org/www-project-top-ten/

[25] CISA, "Alert (AA21-209A) Top Routinely Exploited Vulnerabilities," 7/2021. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa21-209a

[26] A. Zahravi, K. Choubey, P. Girnus, and W. G. Sanchez, "FormBook Adds Latest Office 365 0-Day Vulnerability (CVE-2021-40444) to Its Arsenal," 9/2021. [Online]. Available: https://www.trendmicro.com/en_us/research/21/i/formbook-adds-latest-office-365-0-day-vulnerability-cve-2021-404.html

[27] Identity Theft Resource Center, "ITRC's 2021 Q3 Data Breach Analysis," 10/2021. [Online]. Available: https://notified.idtheftcenter.org/s/2021-q3-data-breach-analysis

[28] A. Sharma, "GitHub Actions being actively abused to mine cryptocurrency on GitHub servers," 4/2021. [Online]. Available:

https://www.bleepingcomputer.com/news/security/github-actions-being-actively-abused-to-mine-cryptocurrency-on-github-servers/

[29] Trend Micro, "Business Email Compromise (BEC)." [Online]. Available: https://www.trendmicro.com/vinfo/hk/security/definition/business-email-compromise-(bec)

[30] Federal Bureau of Investigation, "Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion," 4/2020. [Online]. Available: https://www.ic3.gov/Media/Y2020/PSA200406

[31] Trend Micro, "Trend Micro Cloud App Security Threat Report 2020," 3/2020. [Online]. Available: https://www.trendmicro.com/vinfo/hk/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-threat-report-2020

[32] Y. Rogoza, "Credit Card numbers leak in Magento," 2/2014. [Online]. Available: https://www.atwix.com/magento/credit-card-numbers-leak/

[33] Y. Klijnsma, "Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims," 9/2018. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[34] Y. Klijnsma, "Another Victim of the Magecart Assault Emerges: Newegg," 9/2018. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-newegg/

[35] J. Leyden, "JavaScript sniffer slingers duke it out to control vulnerable websites," 4/2019. [Online]. Available: https://portswigger.net/daily-swig/javascript-sniffer-slingers-duke-it-out-to-control-vulnerable-websites

[36] The MITRE Corporation, "FIN6," 2020. [Online]. Available: https://attack.mitre.org/groups/G0037/

[37] FireEye Threat Intelligence, "FOLLOW THE MONEY: DISSECTING THE OPERATIONS OF THE CYBER CRIME GROUP FIN6," 4/2016. [Online]. Available: https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

[38] O. Villadsen, "More_eggs, Anyone? Threat Actor ITG08 Strikes Again," 8/2019. [Online]. Available: https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/

[39] J. C. Chen, "Magecart Card Skimmers Injected Into Online Shops," 10/2019. [Online]. Available: https://www.trendmicro.com/en_us/research/19/j/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops.html

[40] Volusion, "Volusion Is First Ecommerce Platform to Migrate To Google Cloud," 5/2018. [Online]. Available: https://www.prnewswire.com/news-releases/volusion-is-first-ecommerce-platform-to-migrate-to-google-cloud-300644928.html

[41] J. C. Chen, "Magecart Targets Hotel Booking Websites on Mobile," 9/2019. [Online]. Available: https://www.trendmicro.com/en_us/research/19/i/magecart-skimming-attack-targets-mobile-users-of-hotel-chain-booking-websites.html

[42] J. C. Chen, "Mirrorthief Hits Campus Online Stores Using Magecart," 9/2019. [Online]. Available: https://www.trendmicro.com/en_us/research/19/e/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada.html

[43] Sansec Threat Research, "Digital skimmer runs entirely on Google, defeats CSP," 6/2020. [Online]. Available: https://sansec.io/research/skimming-google-defeats-csp

[44] L. Weichselbaum, M. Spagnuolo, S. Lekies, and A. Janc, "CSP is dead, long live CSP! On the insecurity of whitelists and the future of content security policy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1376–1387.

[45] A. Shaked, "Exfiltrating User's Private Data Using Google Analytics to Bypass CSP," 6/2020. [Online]. Available: https://www.perimeterx.com/tech-blog/2020/bypassing-csp-exflitrate-data/

[46] J. Segura, "Credit card skimmer masquerades as favicon," 5/2020. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/05/credit-card-skimmer-masquerades-as-favicon/

[47] J. Segura, "Web skimmer hides within EXIF metadata, exfiltrates credit cards via image files," 6/2020. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/06/web-skimmer-hides-within-exif-metadata-exfiltrates-credit-cards-via-image-files/

[48] D. Sinegubko, "Skimmers in Images & GitHub Repos," 7/2020. [Online]. Available: https://blog.sucuri.net/2020/07/skimmers-in-images-github-repos.html

[49] J. Segura, "New web skimmer steals credit card data, sends to crooks via Telegram," 9/2020. [Online]. Available: https://blog.malwarebytes.com/web-threats/2020/09/web-skimmer-steals-credit-card-data-via-telegram/

[50] The MITRE Corporation, "Resource Hijacking," Referenced 29.10.2021. [Online]. Available: https://attack.mitre.org/techniques/T1496/

[51] Palo Alto Networks Unit 42, "Highlights from the Unit 42 Cloud Threat Report, 2H 2020," 10/2020. [Online]. Available: https://unit42.paloaltonetworks.com/highlight-cloud-threat-report-IAM/

[52] J. Chen, "Graboid: First-Ever Cryptojacking Worm Found in Images on Docker Hub," 10/2019. [Online]. Available: https://unit42.paloaltonetworks.com/graboid-first-ever-cryptojacking-worm-found-in-images-on-docker-hub/

[53] Trend Micro Incorporated, "Coinminer, DDoS Bot Attack Docker Daemon Ports," 5/2020. [Online]. Available: https://www.trendmicro.com/vinfo/hk-en/security/news/virtualization-and-cloud/coinminer-ddos-bot-attack-docker-daemon-ports

[54] C. Doman, "Team TNT – The First Crypto-Mining Worm to Steal AWS Credentials," 8/2020. [Online]. Available: https://www.cadosecurity.com/post/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials

[55] R. Kol, "Deep Analysis of TeamTNT Techniques Using Container Images to Attack," 8/2020. [Online]. Available: https://blog.aquasec.com/container-security-tnt-container-attack

[56] A. Sasson, "Cetus: Cryptojacking Worm Targeting Docker Daemons," 8/2020. [Online]. Available: https://unit42.paloaltonetworks.com/cetus-cryptojacking-worm/

[57] N. Fishbein, "Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks," 9/2020. [Online]. Available: https://www.intezer.com/blog/cloud-security/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/

[58] A. Morag, "Threat Alert: TeamTNT is Back and Attacking Vulnerable Redis Servers," 9/2020. [Online]. Available: https://blog.aquasec.com/container-attacks-on-redis-servers

[59] N. Quist, "Black-T: New Cryptojacking Variant from TeamTNT," 10/2020. [Online]. Available: https://unit42.paloaltonetworks.com/black-t-cryptojacking-variant/

[60] O. Caspi, "Malware using new Ezuri memory loader," 1/2021. [Online]. Available: https://cybersecurity.att.com/blogs/labs-research/malware-using-new-ezuri-memory-loader

[61] D. Fiser, "TeamTNT Now Deploying DDoS-Capable IRC Bot TNTbotinger," 12/2020. [Online]. Available: https://www.trendmicro.com/en_nz/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html

[62] J. Chen, A. Sasson, and A. Zelivansky, "Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes," 2/2021. [Online]. Available: https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

[63] Lacework Labs, "Taking TeamTNT's Docker Images Offline," 5/2021. [Online]. Available: https://www.lacework.com/blog/taking-teamtnt-docker-images-offline/

[64] N. Quist, "TeamTNT Actively Enumerating Cloud Environments to Infiltrate Organizations," 6/2021. [Online]. Available: https://unit42.paloaltonetworks.com/teamtnt-operations-cloud-environments/

[65] O. Caspi, "TeamTNT with new campaign aka "Chimaera"," 9/2021. [Online]. Available: https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera

[66] D. Fiser and A. Oliveira, "TeamTNT's Extended Credential Harvester Targets Cloud Services, Other Software," 5/2021. [Online]. Available: https://www.trendmicro.com/en_us/research/21/e/teamtnt-extended-credential-harvester-targets-cloud-services-other-software.html

[67] M. Mimoso, "1 Million Gmail Users Impacted by Google Docs Phishing Attack," 5/2017. [Online]. Available: https://threatpost.com/1-million-gmail-users-impacted-by-google-docs-phishing-attack/125436/

[68] Proofpoint staff, "Silver lining: Google OAuth worm leads to Proofpoint discovery and Google mitigation," 7/2017. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/google-oauth-worm-leads-proofpoint-discovery

[69] J. Umawing, "Out of character: Homograph attacks explained," 1/2018. [Online]. Available: https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained

[70] T. Potasinski, "Google OAuth Updates: 2019 Timeline and Everything Else You Need to Know," 12/2018. [Online]. Available: https://www.nylas.com/blog/google-oauth-updates-2019-timeline-and-everything-else-you-need-to-know/

[71] Proofpoint, "TA2552 Uses OAuth Access Token Phishing to Exploit Read-Only Risks," 9/2020. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/ta2552-uses-oauth-access-token-phishing-exploit-read-only-risks

[72] A. Simons, "Publisher verification and app consent policies are now generally available," 10/2020. [Online]. Available: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/publisher-verification-and-app-consent-policies-are-now/bap/1257374

[73] Microsoft, "Add-ins for Outlook in Exchange Online," 2021. [Online]. Available: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/add-ins-for-outlook/add-ins-for-outlook

[74] I. Clarke and A. Friedman, "OAuth Abuse: Think Solarwinds/Solorigate Campaign With Focus On Cloud Applications," 3/2021. [Online]. Available: https://www.proofpoint.com/us/blog/cloud-security/oauth-abuse-think-solarwindssolorigate-campaign-focus-cloud-applications

[75] M. Landewe, "Widespread Attack on Office 365 Corporate Users with Zero-day Ransomware Virus," 6/2016. [Online]. Available: https://www.avanan.com/blog/attack-on-office-365-corporate-users-with-zero-day-ransomware-virus

[76] L. Cashdollar, "Phishing Attacks Against Facebook and Google via Google Translate," 2/2019. [Online]. Available: https://www.akamai.com/blog/security/phishing-attacks-against-facebook-google-via-google-translate

[77] L. Abrams, "New Phishing Attack Uses Google Translate as Camouflage," 2/2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-google-translate-as-camouflage/

[78] M. Vergelis, "How spammers use Google services," 6/2019. [Online]. Available: https://www.kaspersky.com/blog/spam-through-google-services/27228/

[79] T. Tulachan, "Trickbot Is Using Google Docs to Trick Proofpoint's Gateway," 8/2019. [Online]. Available: https://cofense.com/trickbot-using-google-docs-trick-proofpoints-gateway/

[80] S. Gatlan, "TrickBot Bypasses Secure Email Gateway Using Google Docs Phishing," 8/2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/trickbot-bypasses-secure-email-gateway-using-google-docs-phishing/

[81] F. Rodrigues, "New Phishing Campaign Uses Captcha to Bypass Email Gateway," 9/2019. [Online]. Available: https://cofense.com/new-phishing-campaign-uses-captcha-bypass-email-gateway/

[82] K. Mahdavi, "Phishers Are Using Google Forms to Bypass Popular Email Gateways," 2/2020. [Online]. Available: https://cofense.com/phishers-using-google-forms-bypass-popular-email-gateways/

[83] Check Point Software Technologies Ltd., "How scammers are hiding their phishing trips in public clouds," 7/2020. [Online]. Available: https://blog.checkpoint.com/2020/07/21/how-scammers-are-hiding-their-phishing-trips-in-public-clouds/

[84] Team Armorblox, "Blox Tales 15: Credential Phishing Attack Performs Real-Time Active Directory Authentication," 10/2020. [Online]. Available: https://www.armorblox.com/blog/blox-tales-credential-phishing-attack-performs-real-time-active-directory-authentication/

[85] Abnormal Security, "Scammers Target Microsoft 365 Read Receipt and Out of Office Reply Loophole for BEC Attacks," 1/2021. [Online]. Available: https://abnormalsecurity.com/blog/scammers-target-microsoft-365-read-receipt-and-out-of-office-reply-loophole-for-bec-attacks/

[86] I. Ilascu, "Google Forms and Telegram abused to collect phished credentials," 4/2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/google-forms-and-telegram-abused-to-collect-phished-credentials/

[87] Y. Kargalev, "Send to saved messages: cybercriminals use Telegram bots and Google Forms to automate phishing," 4/2021. [Online]. Available: https://www.group-ib.com/media/phishing-automation/

[88] R. Dedenok, "Google Docs used for Office 365 credential phishing," 5/2021. [Online]. Available: https://www.kaspersky.com/blog/office-365-phishing-via-gdocs/39828/

[89] M. Slavoutsky and S. Golderman, "Attackers Are Using Salesforce's Mass Email Service to Perpetrate Phishing Attacks," 8/2021. [Online]. Available: https://perception-point.io/attackers-are-using-salesforces-mass-email-service-to-perpetrate-phishing-attacks/

[90] Microsoft 365 Defender Threat Intelligence Team, "Widespread credential phishing campaign abuses open redirector links," 8/2021. [Online]. Available: https://www.microsoft.com/security/blog/2021/08/26/widespread-credential-phishing-campaign-abuses-open-redirector-links/

[91] S. Gatlan, "FBI warns of BEC scammers using email auto-forwarding in attacks," 12/2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/fbi-warns-of-bec-scammers-using-email-auto-forwarding-in-attacks/

[92] Proofpoint Information Protection Research Team, "loud attacks leverage credential dumps, phishing, and legacy email protocols to bypass MFA and breach cloud accounts worldwide," 3/2019. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/threat-actors-leverage-credential-dumps-phishing-and-legacy-email-protocols

[93] N. Ohfeld and S. Tzadik, "ChaosDB: How we hacked thousands of Azure customers' databases," 8/2021. [Online]. Available: https://www.wiz.io/blog/chaosdb-how-we-hacked-thousands-of-azure-customers-databases

[94] J. Cox, "How Hackers Used Slack to Break into EA Games," 6/2021. [Online]. Available: https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack

[95] F. Khwaja, "Why Linux Runs 90 percent of the Public Cloud Workload," 3/2020. [Online]. Available: https://www.quickstart.com/blog/why-linux-runs-90-percent-of-the-public-cloud-workload/

[96] L. Abrams, "Linux warning: TrickBot malware is now infecting your systems," 7/2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/linux-warning-trickbot-malware-is-now-infecting-your-systems/

[97] F. Sinitsyn and V. Kuskov, "RansomEXX Trojan attacks Linux systems," 11/2020. [Online]. Available: https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

[98] M.-E. M.Léveillé and I. Sanmillan, "A Wild Kobalos Appears: Tricksy Linux malware goes after HPCs," 1/2021. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf

[99] A. Burt, "Gitpaste-12: a new worming botnet with reverse shell capability spreading via GitHub and Pastebin," 11/2020. [Online]. Available: https://blogs.juniper.net/en-us/threat-research/gitpaste-12

[100] L. O'Donnell, "Linux Devices Under Attack by New FreakOut Malware," 1/2021. [Online]. Available: https://threatpost.com/linux-attack-freakout-malware/163137/

[101] F. Hacquebord, "Two Years of Pawn Storm Examining an Increasingly Relevant Threat," 4/2017. [Online]. Available: https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf

[102] F. Allego, "Spammers Leverage Different Google Services for Phishing Attack," 8/2014. [Online]. Available: https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/print/spam/3525/spammers-leverage-different-google-services-for-phishing-attack

[103] Google, "Block shares from another user in Google Drive," 7/2021. [Online]. Available: https://workspaceupdates.googleblog.com/2021/07/block-shares-from-user-google-drive.html

[104] A. Orlowski, "OK Google: A stranger with stash of pirated films is spamming my Google Team Drive," 12/2017. [Online].

Available: https://www.theregister.com/2017/12/07/googles_team_drive_unwanted_drive/

[105] C. Summerson, "Google Drive Has a Serious Spam Problem, But Google Says a Fix is Coming," 1/2019. [Online]. Available: https://www.howtogeek.com/400511/google-drive-has-a-serious-spam-problem-and-google-doesnt-seem-to-care/

[106] J. Temperton, "A new scam uses Google Drive to send out a deluge of dodgy links," 10/2020. [Online]. Available: https://www.wired.co.uk/article/google-drive-spam-comments-phishing

[107] D. Maciejak, "Yet Another Crypto Mining Botnet?" 5/2018. [Online]. Available: https://www.fortinet.com/blog/threat-research/yet-another-crypto-mining-botnet

[108] W. Ashford, "Unprotected Kubernetes consoles expose firms to cryptojacking," 2/2018. [Online]. Available: https://www.computerweekly.com/news/252435544/Unprotected-Kubernetes-consoles-expose-firms-to-cryptojacking

[109] RedLock CSI Team, "Lessons from the Cryptojacking Attack at Tesla," 2/2018. [Online]. Available: https://redlock.io/blog/cryptojacking-tesla

[110] Sansec Threat Research. (9/2020) Cardbleed: 3% of Magento install base hacked. [Online]. Available: https://sansec.io/research/cardbleed

[111] H. Kass, "DHS Memo: Hackers Exploiting MSPs to Attack Customer' Networks," 10/2018. [Online]. Available: https://www.msspalert.com/cybersecurity-news/dhs-warning-msps-csps/

[112] B. Krebs, "Ransomware at IT Services Provider Synoptek," 12/2019. [Online]. Available: https://krebsonsecurity.com/2019/12/ransomware-at-it-services-provider-synoptek/

[113] L. Abrams, "Popular NPM library hijacked to install password-stealers, miners," 10/2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/

[114] D. Prizmant, "Siloscape: First Known Malware Targeting Windows Containers to Compromise Cloud Environments," 6/2021. [Online]. Available: https://unit42.paloaltonetworks.com/siloscape/

[115] IBM Security X-Force Threat Intelligence, "2021 IBM Security X-Force Cloud Threat Landscape Report," 9/2021. [Online]. Available: https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775

[116] X. Liao, S. Alrwais, K. Yuan, L. Xing, X. Wang, S. Hao, and R. Beyah, "Cloud repository as a malicious service: challenge, identification and implication," *Cybersecurity*, vol. 1, no. 1, pp. 1–18, 2018.

[117] S. Tajalizadehkhoob, C. Gañán, A. Noroozian, and M. v. Eeten, "The role of hosting providers in fighting command and control infrastructure of financial malware," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 575–586.

[118] R. Sabitov, "Russian-speaking cybercrime evolution: What changed from 2016 to 2021," 10/2021. [Online]. Available: https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

[119] Accurics Ltd., "Top 4 Cloud Security Pitfalls & Misconfigurations," 8/2021. [Online]. Available: https://www.accurics.com/wp-content/uploads/2021/08/WP-Top-4-Cloud-Security-Pitfalls-_-Misconfigurations-vF.pdf

[120] Accurics Inc., "Cloud Cyber Resilience Report," 2/2021. [Online]. Available: https://start.accurics.com/CloudCyberResilienceReportEvolvingRisks_LP-Reg.html

[121] Microsoft, "POP3 and IMAP4 in Exchange Online," 2021, Referenced: 29.10.2021. [Online]. Available: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/pop3-and-imap4/pop3-and-imap4

[122] M. Azure, "What are security defaults?" 2021, Referenced: 29.10.2021. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

[123] J. Chen, "The State of Exploit Development: 80% of Exploits Publish Faster than CVEs," 8/2020. [Online]. Available: https://unit42.paloaltonetworks.com/state-of-exploit-development/

[124] S. Gatlan, "OMIGOD: Microsoft Azure VMs exploited to drop Mirai, miners," 9/2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/omigod-microsoft-azure-vms-exploited-to-drop-mirai-miners/

[125] Unit 42, "Highlights from the Unit 42 Cloud Threat Report, 2H 2020," 4/2021. [Online]. Available: https://unit42.paloaltonetworks.com/highlights-cloud-threat-report-1h-2021/

[126] J. Chen, "Unit 42 Cloud Threat Report: Misconfigured IAM Roles Lead to Thousands of Compromised Cloud Workloads," 10/2021. [Online]. Available: https://unit42.paloaltonetworks.com/iam-roles-compromised-workloads/

[127] "PaperChaser," 2021. [Online]. Available: https://github.com/mandatoryprogrammer/PaperChaser

[128] "DEF CON 29 - Matthew Bryant - Hacking G Suite: The Power of Dark Apps Script Magic," 2021. [Online]. Available: https://www.youtube.com/watch?v=6AsVUS79gLw&ab_channel=DEFCONConference

Appendix A

Other concepts

Credential stuffing	Also known as password spraying, an automated attack making login requests using lists of credentials
BEC	Business Email Compromise, email based fraud attack
Formjacking	Also known as web skimming, an attack where injected code extracts user input field contents
Rootkit	A type of malware used for remote access, often with evasion capabilities
Honeypot	Isolated and monitored asset, used as a dummy target to gather data on attacks