CHECK POINT RESEARCH

SECURING THE CLOUD, MOBILE, AND INTERNET OF THINGS

THE MOST VULNERABLE TARGETS IN CYBER SECURITY

2019 Security Report
Volume 03

VOLUME 03

2019 SECURITY REPORT

01	INTRODUCTION	3
02	CLOUD IS YOUR WEAKEST LINK	4
03	THE MOBILE WEAK SPOT	11
04	IoT'S WEAKNESS	14
05	CONCLUSION	16

INTRODUCTION

In the first installment of this 2019 Security Report we reviewed the latest trends and threats facing the IT security industry today. In the second installment, we took a deeper look at the cyber crime underworld to get a grasp on the democratization of cyber crime to understand how malware has shifted gears to a more stealth-like approach to infecting organizations.

In this third installment we focus on how threat actors are able to keep one step ahead by targeting the weakest points in an organization's IT infrastructure – the cloud, mobile and IoT. Indeed, these platforms offer a threat actor a much higher chance of success and fewer obstacles to overcome due to them being far less protected.

As a result, their profits can often be higher due to more private data stored on mobile devices and larger databases and resources held in the cloud. So with account takeovers becoming increasingly common, and the introduction of GDPR in 2018, potential data breaches and other attacks are simply too costly to ignore.

CLOUD IS YOUR WEAKEST LINK

Few are surprised by the popularity of the cloud. It offers flexible computing options at a fraction of the cost and time. Organizations can conveniently improve data storage and server processing or use Software-as-a-Service (SaaS) products.

Cloud computing has become an integral piece of today's IT infrastructure. Its 'try before you buy' and 'pay as you go' models provide organizations with the ability to test the technology, and integration with the cloud is fast and usually requires virtually no organizational down time.

However, much like other emerging technologies, the cloud can be abused. So it's imperative to know its vulnerabilities, especially the holes in security.

> ***91%*** *of organizations are concerned about cloud security.*
>
> Source: 2018 Cloud Security Report, Dome9

Cloud's Weakest Points

In brief, the main security challenges with the cloud and the services it provides include:

External Exposure – Cloud services are typically accessed from any location and any device. All that's needed is an internet connection. While ease of access can boost company agility, services running in the cloud versus those on premise are more likely to be breached.

Only Default Security – Typically, cloud services are provided with only basic security which allows unrestricted open internet file sharing. This vulnerability can open the door to any number of malware attacks.

Cloud services are vulnerable across three main attack vectors:

1. Account Hijacks – Gaining unauthorized access to an individual or organization's email or computer account for malicious purposes. In a Check Point survey, Account Hijacks were the biggest concern amongst customers and partners.

2. Malware Delivery – Propagation, especially through in-app file sharing services, such as Box or One Drive cloud apps, in order to commit a variety of cyber crimes.

3. Data Leaks – Whether intentionally or unintentionally, data leakage occurs with the seamlessness of sharing information with cloud services.

Due to the cloud's security challenges, the Check Point Incident Response team is seeing an increase in security breaches with cloud services, both with SaaS and Infrastructure-as-a-Service (IaaS) models.

> ***18%*** *of organizations experienced a cloud security incident in the past year.*
>
> Source: 2018 Cloud Security Report, Dome9

Despite the upward trend in security breaches with the cloud, however, 65% of IT professionals still underestimate the damage they can cause. The obvious concern is that organizations are not taking cloud security seriously enough. The breach of sensitive data held in the cloud is a huge risk for an organization, and threat actors know it. The rate of cyber attacks against cloud-based targets is growing, and with little sign it will slow down.

When asked why they may not be securing their cloud assets, a full 30% of survey respondents believe security is the responsibility of the cloud service provider. This negates recommendations that cloud security follow the Mutual Responsibility model shared by the cloud provider and the customer.

> ***65%*** *of IT professionals underestimate the damage caused by attacks on the cloud.*
>
> Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Whether an organization suffers a financial, informational or reputational loss, the overall effect of a cloud attack can be devastating to a business. To understand the potential damage of a cloud attack, let's take a closer look at Account Hijacks.

> ***1 in 3*** *IT Professionals still consider security to be the responsibility of the cloud service provider.*
>
> Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

> ***49%*** *of organizations are increasing their cloud security budget in the next year.*
>
> Source: 2018 Cloud Security Report, Dome9

How Do Account Hijacks Occur?

To take over an account, the attacker must first gain the victim's trust. The most common method to achieve trust is to use social engineering. Phishing attacks are the most common method for stealing log-in credentials from unsuspecting users.

Here's how it typically works. The cyber criminal sends an "urgent" email from Microsoft support or another service provider requesting a response from the victim. A click on a link in the email will allow the attackers to hijack the victim's account. We've all seen these phony emails, yet people still fall prey to the scheme.

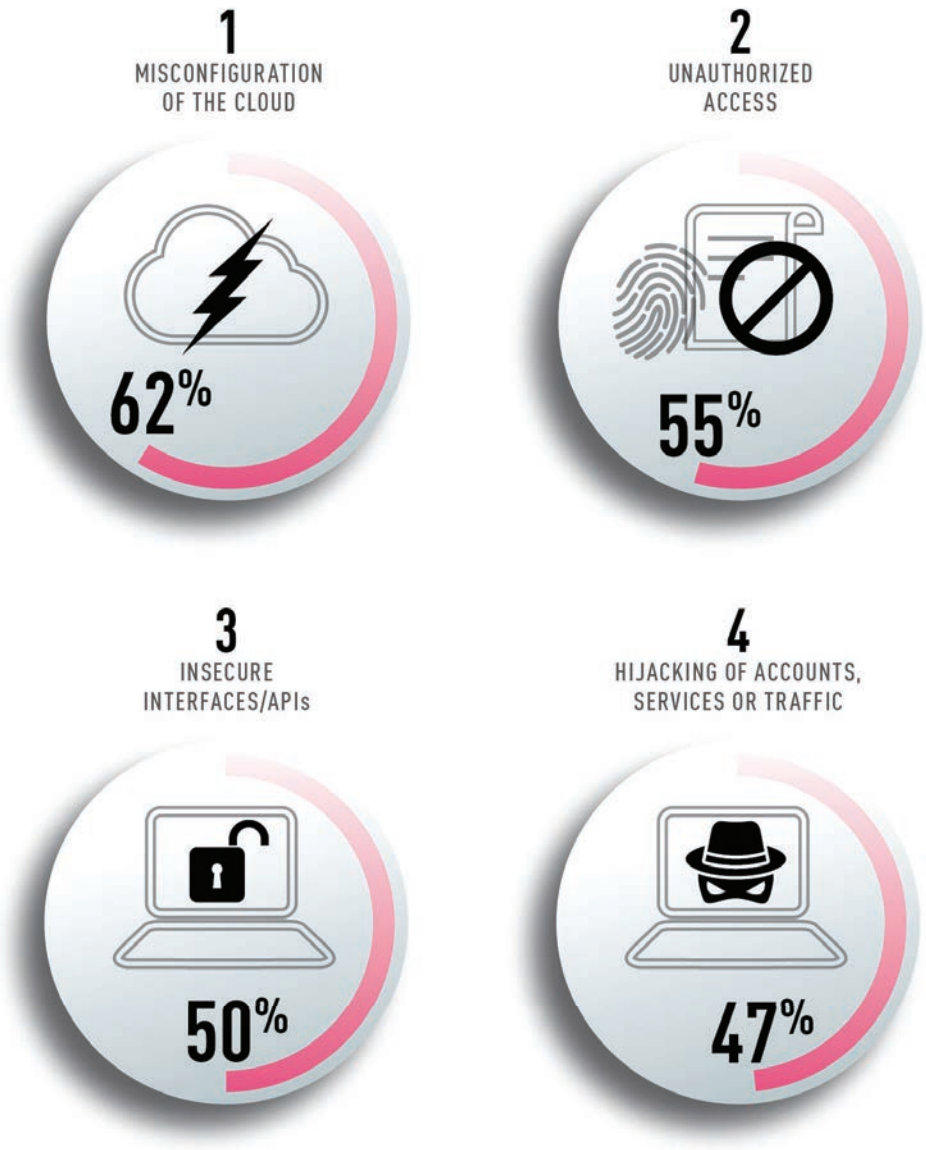
After proceeding to click on the link and enter their log-in credentials when prompted, the unsuspecting victim may also receive a push notification by SMS to his mobile device. This is mainly used to add an extra element of authenticity to the phishing scam, which the victim, having already trusted the initial source of the attack, will also likely approve and continue as instructed. Of course, as the victim unknowingly provides these sensitive log-in details to the attacker, the attacker uses them to gain access to the victim's SaaS account, for example, helping themselves to the private and confidential information stored there.

47% OF ORGANIZATIONS THINK ACCOUNT HIJACKS ARE THE BIGGEST THREAT TO THEIR CLOUD SECURITY.

Source: 2018 Cloud Security Report, Dome9

Figure 1: The Top 4 Security Threats Facing Public Cloud as Perceived by IT Professionals

Source: 2018 Cloud Security Report, Dome9



> ***62%*** *of IT Professionals are most concerned about Data Loss or Leakage.*
>
> Source: 2018 Cloud Security Report, Dome9

> ***67%*** *of those who experienced a cyber attack rated its impact as medium or high.*
>
> Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

New Threats Transition to the Cloud

Along with a wide range of benefits, the cloud infrastructure introduces a new, fertile and attractive environment for attackers who crave the enormous amount of available computing resources and sensitive data it holds. Indeed, 2018 has brought us various sophisticated techniques and tools exploited against cloud storage services.

Several cloud-based attacks, mainly those involving data exfiltration and information disclosure, derived from poor security practices. Credentials left available on public source code repositories or the use of weak passwords are just some examples of how threat actors gained access and control over unprotected resources hosted in the cloud.

Another rising threat taking the cloud environment by storm are cryptominers, targeting the cloud infrastructure in order to exploit the vast computational power it presents and generate huge profits for cyber criminals.

Application Programming Interfaces (APIs) that are used to manage, interact and extract information from services have also been a target for threat actors. The fact that cloud APIs are accessible via the Internet has opened a window for threat actors to take advantage and gain considerable access to cloud applications.

As time passes, threats to the cloud will continue to evolve. Attackers will continue to develop more and more tools for their cloud playground, pushing the limits of the public cloud services. Indeed, as new cloud exploitations emerge, there is no doubt that the next attack is already taking place.

This introduces a whole new environment in which victims are exposed to more attack vectors that could be exploited by threat actors trying to find the weakest link that leads to a person or organization's data.

Required Prevention Solutions

In order to prevent such phishing attacks, an in-depth security solution is needed to detect such phishing attempts. A trusted prevention solution can scan the content of emails, evaluate the trustworthiness of the sender, and maintain specially researched keywords and a list of other such variables.

Whereas many solutions perform such scanning detections on traffic received from outside of an organization's network, what they fail to detect, however, is traffic already received from within the network. In fact, it's vital for a solution to scan internal emails from within an organization as phishing scams can be easily spread from an already compromised account.

A solution that performs internal scans must also work in harmony with the existing security of the cloud provider and perform security checks from within the email cloud service. This is something that is not currently done by most of the current solutions available in the cyber security product solutions market. Such security features that come with the cloud service itself are often shut down.

Before a prevention solution is adopted, it's vital to ensure your IT environment is clean. This can be accomplished by your cloud security solution's anomaly monitoring that monitors and detects anomalies such as forwarding rules, i.e., a compromised account sending malicious emails to external users.

In order to prevent account takeovers, any device granted access to the SaaS platform must be clean and compliant with the security policy of the company to prevent devices with malware or OS exploits from logging in.

Of course, detection by itself is never sufficient. Prevention is preferred so your cloud security solution protects the last line of defense in your network security architecture. By applying identity protections, your solution can prevent unauthorized access to accounts. Such identity protections must be able to deflect phishing attempts and yet still be easy to deploy with zero friction to users.

MOBILE'S WEAK SPOT

Mobile security is a major security concern these days — and for good reason. Nearly all employees now routinely access corporate data from smartphones, and the challenge is to keep sensitive information out of the wrong hands.

The main security challenge with mobile devices is that they are easy to overlook. Today's smartphones are mobile computers that have been pressed into action by businesses throughout the world. This has made network security a bigger and more diverse challenge. The use of mobile devices and apps has also added a new range of attack vectors and additional security challenges for IT.

The proliferation of personal smartphones and tablets in the workplace exposes your company to increased risks. While a breach of personally identifiable information or payment card data is certainly a top concern for many businesses, there are other risks that organizations need to consider. Chief among these are the cost of breaches and responding to incidents, the potential damage to brand reputation, and a loss of competitive advantage if valuable trade secrets or intellectual property become public knowledge.

Mobile systems, the networks they connect to, and the applications they run can all be exploited to steal sensitive information such as documents, calendar appointments, email messages, texts, and attachments. As Check Point Research illustrated via announcements of threat actors taking advantage of the World Cup last year to spy on government agencies through malicious mobile applications, cyber criminals can use the smartphone in other ways. A device's microphone and camera can be used to spy on their targets, and then send recordings to a secret remote server. They can also capture user names and passwords as users log in to corporate systems containing sensitive data.

With this in mind, let us take a closer look at the four major threats to mobile security in today's corporate environment.

> *59% of IT Professionals do not use Mobile Threat Defense.*
>
> Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Trojans and Malware

Social engineering scams remain astonishingly effective. In fact, trickery is just as troubling on the mobile front as it is on desktops.

Many mobile users are unaware of the dangers and they are far too trusting when clicking on links they receive via SMS or social media apps such as WhatsApp. This can often lead to the device getting infected by a wide array of mobile malware.

Trojans, for example, carried within an app or installed through an unsecured network connection, infect a device with malicious code that may conduct surveillance by eavesdropping and recording conversations, extracting call logs, tracking locations, logging keyboard activity, and collecting passwords.

> *Only 9% of IT Professionals Consider Threats on Mobile a Significant Risk.*
>
> Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Fake Apps

Malicious apps can take control of mobile devices and although the app may not appear to be malicious, users may not notice or understand the permissions they grant during installation. What's more, even popular apps can be reverse-engineered and injected with malicious code, and then uploaded to an app store under a different name.

Criminals can also create seemingly authentic copies of apps that include similar icons, descriptions, screenshots, and even user reviews. But, of course, they don't work as intended. Instead, victims receive a malicious payload, such as a

subscription to an expensive texting service or a stealthy surveillance tool. Indeed, malicious apps can enable a host of activities, such as remotely seizing control of the device's camera and microphone to spy on users and their surroundings. Such were the apps the Check Point Research team came across on multiple occasions throughout 2018, proving just how prevalent these highly invasive apps are.

Man-in-the-Middle Attacks

Man-in-the-Middle attacks can eavesdrop, intercept and alter traffic between two devices. You believe you're interacting with a known and trusted entity, but in fact an attacker is copying credentials, snooping on instant messages, or stealing sensitive information. The familiar alert and warning signs on PCs and laptops are far more subtle and easily overlooked on mobile devices. Small screen sizes can also hide web addresses, making it harder to validate the address the browser is pointing to.

Public Wi-Fi hotspots, which are convenient for internet access, are easy to fake. An attacker can create a spoofed Wi-Fi network, or eavesdrop and alter a legitimate network's encrypted communications by using spoofed certificates or downgrading the communication link so that it is no longer encrypted. The attacker can then intercept communications, alter data in transit or install a Trojan.

System Vulnerabilities

Each version of an operating system for a mobile device offers vulnerabilities that cyber criminals can use to launch attacks. Unfortunately, as new versions are notoriously late to market, critical security updates might not make it through testing for weeks or even months, leaving users exposed.

Android is particularly vulnerable. The thousands of different types of Android smartphones and tablets are not updated consistently and at the same time. Most devices are still using older Android versions in which vulnerabilities have not been patched.

Apple's iOS, on the other hand, is less vulnerable because Apple makes only a handful of different devices and consistently prompts users to update them. However, the number of attacks carried out on Apple's iOS is increasing due to the more sophisticated types of attacks that are carried out on this operating system.

IoT'S WEAK SPOT

There is no doubt that today's world is becoming ever more interconnected, so much so that we should perhaps no longer talk so much about the Internet of Things (IoT) but rather the Internet of Everything. Whether it is agriculture, manufacturing or healthcare, almost every industry is embracing the proliferation of smart devices available to them to get deeper insights and more data to aid them in their work.

IoT devices make our lives easier. Smart home technology, for example, can help users improve energy efficiency by enabling them to turn on (and off) lights and appliances with the tap of a touchscreen. Some connected devices, such as smart medical equipment and alarm systems, can even help save lives.

Take medical devices, for example. This subset of IoT belonging specifically to healthcare and its supporting technologies, the Internet of Medical Things, is made up of smart, connected devices that automatically collect, process, and digitally relay information from the physical world through a shared network infrastructure.

Networked medical devices give healthcare professionals the ability to be much more accurate with their treatment regimens, far more efficient in administering care, and way quicker collecting and responding to biomedical information.

> *There will be an estimated **125 million** Healthcare IoT devices in 2019.*
>
> Source:Statistica.com, Estimated Healthcare IoT Device Installations

As a result, IoMT technologies are currently exploding, both in terms of their popularity and capabilities. Put simply, IoMT is redefining the practice of medicine. And while this new frontier of medicine is very exciting and hugely promising, it is not without its problems.

There are also serious security risks associated with IoT technology. As the IoT ecosystem expands, so does the attack surface for cyber criminals. In other words, the more we rely on connected technology in our day-to-day lives, the more vulnerable we are to the cyber threats that are increasingly tailored to exploit vulnerabilities and security design flaws in IoT devices.

This presents a daunting challenge for cybersecurity professionals. They must not only protect their own devices, but they must also defend against threats targeting external machines that might connect to their IT networks as a whole.

The current IoT landscape then can be compared to the early days of the internet, when viruses, worms, and email spam plagued users. Many companies raced to join the internet 'gold rush' without necessarily considering the importance of internet security.

The Security Issues

While the concerns regarding medical IoT devices may be more particular, the major malfunction with IoT device security as a whole lies in the fact that they are usually poorly coded. This is mainly due to the device manufacturers' pursuit of profitability over user security. So when insecure devices are connected to the open internet, they become the route for a disaster waiting to happen.

For example, cyber criminals can hack insecure security cameras or other smart devices and use them to access the rest of an organization's corporate or individual's home network. Alternatively, thousands of these insecure IoT devices can be combined to form a zombie botnet army to launch devastating DDoS attacks.

In addition, IoT devices themselves can be exploited to give threat actors unauthorized entry, as illustrated by Check Point's research into LG automatic vacuum cleaners that showed how a hacker could take over the device's camera to spy on users. However it is often forgotten that the data collected by these devices is usually stored in the cloud. In this respect, as shown by recent research into drones, an attack on the IoT-Cloud infrastructure could leave photos and film footage taken by the drone devices exposed to theft. This is just one example of how sensitive data stored in the cloud could be breached, though with so much data collected by IoT devices as a whole, organizations should be extremely cautious about how that data is stored.

Another hurdle IT professionals face with regard to network compliance is the sheer lack of regulation surrounding the entire IoT ecosystem. Though there may soon be IoT regulations in the state of California, which is leading the way in the area of IoT regulations, it is currently the responsibility of IT professionals to audit devices for compliance. Regardless of these regulations, there will continue to be millions of devices still in use from before these new requirements come into force, which will still have a large potential for exploiting the weaknesses in these outdated devices.

CONCLUSION: NEXT STEPS

The cloud environment has changed the way companies manage, store and share their data, applications, and workloads. Along with a wide range of benefits, though, the cloud infrastructure also introduces a new, fertile and attractive environment for attackers who crave the enormous amount of available computing resources and sensitive data it holds.

While we consider the cloud to be an organization's weakest link, threats posed to them via their employee's mobile and IoT devices are also to be taken seriously as one of many attack vectors from which sensitive data can be stolen or leveraged to launch an attack.

In the next and final installment of this 2019 Security Report, we will be providing some recommendations on how organizations can prevent these invasive and damaging attacks from occurring. Considering the direction the threat landscape has taken so far, we will also be making some predictions about what we can expect to see in the year ahead.

Check Point
SOFTWARE TECHNOLOGIES LTD

cp<r>
CHECK POINT RESEARCH

WORLDWIDE HEADQUARTERS

5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. HEADQUARTERS

959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391 | 650-628-2000 | Fax: 650-654-4233

UNDER ATTACK?

Contact our Incident Response Team:
emergency-response@checkpoint.com

checkpoint.com