ORACLE
Linux

Anatomy of a Cyber Attack

The Lifecycle of a Security Breach

ORACLE WHITE PAPER|DECEMBER 2017

ORACLE

Table of Content

Introduction

Security is everyone's job today, from consumers, to system administrators, to executives. If you are doing business, you need to elevate the priority of security across your organization and data center. Over the years, cybercriminals have gotten more advanced and better funded. They are entire teams of highly trained hackers, and they have built it into a very profitable business. Cybercrime is big business. In many cases, states have built their own cyberattack teams. These teams are no less important to their state strategies than their army or navy. And just like these cyber-attack teams are prepared to attack anyone, you too must be prepared to defend against anyone. Whether you know it or not, you are in a cyber war.

You need to be prepared.

We are at War

Cybercrime is the new buzzword. Hackers have become highly sophisticated and organized. They have become the new Mafia, and they are running it like an industry.

According to Breach Level Index database,[1] 1,792 data breaches were reported in 2016 resulting in theft of around 1.3 billion data records. Just to clarify, these are the data breaches publicly reported and don't include thousands of cyber-attack incidents and undiscovered data breaches.

Here are some examples of how hackers have industrialized cybercrime:[2]

- You can get someone's complete health insurance data by paying $1,250.
- For just $7/hour, you can unleash a Distributed Denial of Service attack on your competition.
- You can purchase US Fulz records (someone's identity, passport, SSN, and others). You can get all that for around $40.
- You can also get 10,000 fake Twitter followers for $15.
- And if you want access to a government server, that can be had for $6.

You're dealing with professional organizations that:

- Provide 24/7 customer service;
- Offer free trial attacks to demonstrate their prowess;
- Payment after the successful attack once you are satisfied with the results.

The cost of cybercrime in 2016 is estimated to be around $445 billion, and it is predicted to increase to around $2 Trillion globally by 2019.[3]

These estimates only include known attacks, not undetected cybercrime, industrial espionage, or state-sponsored attacks.

---

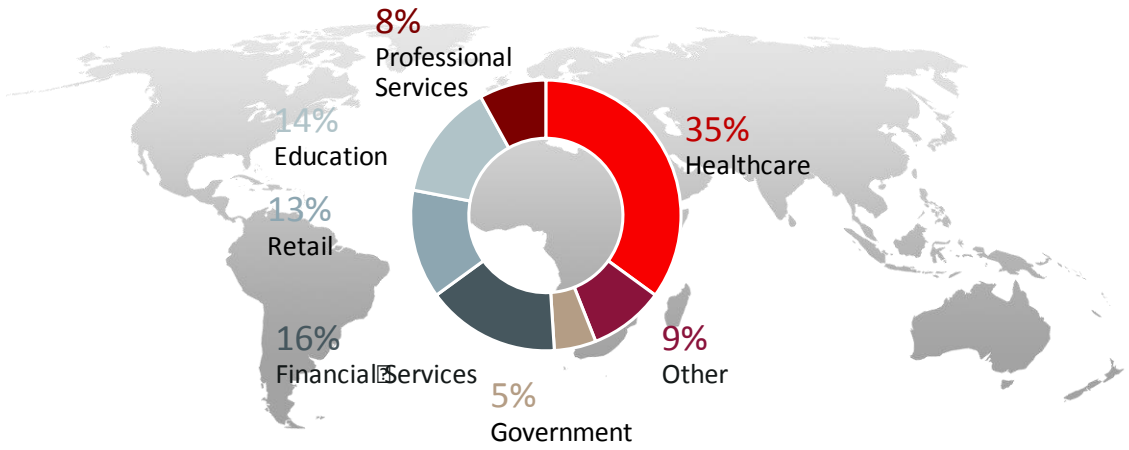
[1] http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf

[2] http://www.havocscope.com/black-market-prices/hackers/

[3] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4af445823bb0

No one is immune

In 2016, approximately 35% of all attacks occurred against the healthcare industry.[4] In the past financial services have been the biggest target. However, the financial services industry has gotten smarter and has hardened itself. In 2016, the most common type of incident was phishing/hacking/malware at 43%. It was the largest type of attack/incident in all sectors, except financial services.[5] Today, all business sectors must assume that they are at risk.



Even small companies can't assume they are safe. In 2016, 39% of all cyber-attacks occurred against companies with less than $100 million in revenue and an additional 33% occurred against companies that have revenue between $100 million and $500 million.

Ransomware is on the rise. In 2016, ransomware attacks rose 500%. It is to the point where it is being recommended as good practice to keep a bitcoin wallet to pay off the ransomware attackers. However, there is no guaranteeing that the attackers won't take the money and lose the encryption key.

Typical Attack Vectors

Generally, cyberattacks fall into just a handful of attack vectors. As we've said, social engineering attacks (i.e. phishing, hacking and malware) make up the largest single attack vector at 43%. Of course, vulnerability exploitation (exploiting a bug in software or firmware that hasn't been patched) is still a common attack vector. Typical examples of these in recent history include such widespread attacks as Heartbleed, ShellShock, and DirtyCOW. Stolen credentials are often used to gain access to systems, and then from there gain access to higher privileged credentials that eventually lead to the data the attacker is after. This was used in an insurance company breach in 2014. Login credentials were obtained and then used to gain access to higher privileged systems in the datacenter,

[4] https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/
[5] https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/

which was then used to steal 80 million Social Security numbers.[6] Another recent attack of a financial services company left 143 million Social Security numbers exposed.[7]

Malware/ransomware implant themselves into vulnerable systems and then spread across connected networks. The worst example of this most recently was the WannaCrypt exploit that infected systems on a network without any action taken by anyone on the network. Finally, there are Denial of Service attacks and Distributed Denial of Service attacks (DoS and DDoS). With these attacks a person, group, organization or enterprise is prevented from doing business by flooding their websites and services with artificial network traffic either from within their network or from outside their network. An example of a particularly bad DDoS attack was the Dyn DDoS attack. Dyn, one of the largest name service providers on the Internet, was attacked by the Mirai botnet (a type of software robot that infests a device and then awaits orders) via 10's of millions of Wifi-based "smart" devices around the world that had been infected.

Not Just a Single Attack Vector

If you dig into any of the examples mentioned above, you'll notice something they all have in common. They don't rely on one attack vector. In fact, combinations of the above attack vectors are combined together to build the most effective attack possible. For example, with the Dyn attack, a combination of stolen credentials and malware were used.

How did they do it? The attackers got the system administrator password (known as "root" password in UNIX and Linux) for the operating system that was being flashed into 10's of millions of Wifi-based smart devices (e.g. security cameras, light systems, baby monitors, etc.). The password was the same for every single device being put out by a single manufacturer. They were then able to gain access to these devices and install the Mirai botnet malware. When instructed, these devices would then send traffic to the targeted company/datacenter. This caused the datacenter to be flooded with traffic, exceeding its capacity, and effectively taking it offline for a couple of hours while

Dyn engineers worked to mitigate the attack. The attackers tried again a few hours later. This time it was more than just one datacenter. Dyn countered this second attack more quickly, and a third attack failed completely.[8] While Dyn was quick to counter the threat, and was successively more effective at mitigating the attacks, the impact was that dozens of the Internet's largest websites couldn't be accessed by many of their users effectively taking the sites offline.[9]

Looking to the Future

As technologies such as IOT and cloud gain market acceptance, they accelerate the growth of the number of users, devices and machines, network traffic and data. This will lead to more attack vectors, more infected devices, larger attacks and a significant increase in the amount of data stolen. New attack vectors like cloud jail-breaking will rise in use. Cloud jail-breaking is when an attacker legitimately or illegitimately gains access to a virtual machine in a cloud environment and uses that environment to break into or snoop on neighboring virtual machines, or utilizes the virtual machine to gain access to the underlying infrastructure. This potentially gives them access to all the infrastructure and access to all virtual machines in the cloud.

All of this leads us to the conclusion that **we are at war.**

You need to make cybersecurity and defenses your top strategic concern.

---

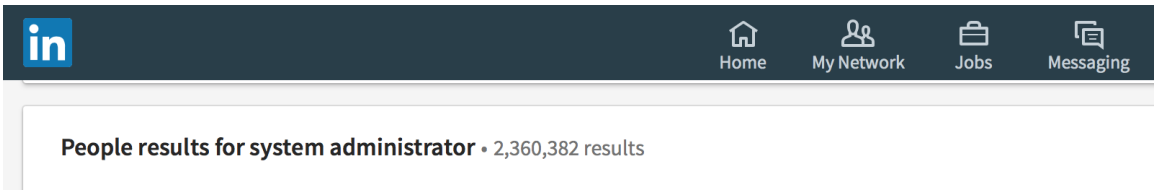
[6] https://krebsonsecurity.com/tag/wellpoint-breach/
[7] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
[8] https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
[9] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

Anatomy of a Typical Attack

Let's look at how a typical attack plays out. We're going walk through a theoretical attack and use a real-world example of an attack to show you how the theory is executed in reality.

Reconnaissance

Every attacker will start by trying to understand your business to gain as much detailed information as possible about your organization and network, as well as identify online behavior of system administrators and other key employees. The employee names and positions are found simply enough through common searches such as a search for "system administrator" on social networking sites like LinkedIn.



This gives a wealth of knowledge about people quickly and even access to contacting them directly.

Once the targets are identified, the attacker moves on to the next step.

Enumeration

Once the attacker has sufficient information, they trick your administrators into exposing sensitive information or downloading malicious software.

There are many ways that this could be done. An email could be sent to the employees that looks official asking them to take some action such as downloading a new tool, or changing a password on a website.

In the case of one large insurance provider, an email was sent to employees that looked like an official email, asking them to click on a link. The link looked legitimate. However, it was actually not a link to their site, but to a site that had a similar looking name. This technique is known as typosquatting, and it is a type of spear-phishing that takes advantage of the fact that our brains pattern match and make quick assessments. The websites look similar enough that unless you look carefully at it, it makes the link look legitimate. This particular attack was more sophisticated. The attackers built an entire website made to look like the target site and prompted victims to login, giving the attackers access to their login credentials. It included a spoofed VPN service that allowed the attackers to gain VPN level access to the corporate network. And it prompted the victims to download software/malware that infected the user's systems, giving them inside access to the network.

The attack managed to successfully spear five technology employees, including a system administrator, and gain access to the entire IT system of the corporation.

Penetration

Once they have gained the access to your network, the attacker now looks to penetrate your network and systems. This can come in many forms. Malware or ransomware could log keystrokes, waiting for you to type in a password, or it could become a worm that looks for vulnerable systems and begins to spread throughout your network. If the

attacker gained access through user credentials, they can plant a worm and leave. They intend to keep the attack going for as long as possible. This can be for months or even years.

They are looking for your data. It may be that they want Personally Identifiable Information (PII) or they may want your business data. Either way, their next step will be to look for vulnerable credential servers like your Active Directory servers. Exploiting your credential servers gives them broader access to your network and services.

Then they establish “Command and Control”. Once in your network, they will attempt to take control of your network. The attacker will surreptitiously hijack as many of your systems as possible. This will give them the ability to control as much of your network as possible and give them high availability of their attack. Once they’ve established a foothold, they can then send requests back to a command server and begin to act on the commands given.

At this point, they begin their data collection. This may include your credentials from your credential servers, emails, and business data, PII, or transaction data from your databases.

Exfiltration

Of course, the point of all this effort, if it isn’t to actively destroy your network, is to get your data out of your network and back to the attackers. So the next step is to send that data back to them.

They’ll likely encrypt the data to prevent your Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) from detecting and/or blocking the data from being exfiltrated out of your datacenters. They use your own servers to prevent detection.

Your data will be sent via one or more anonymizing routers throughout the Internet so that you can’t track where the data is going.

Sanitation

This is the last step in the process. The attackers will remove all evidence that they were in your network and systems. This is to make a clean getaway but also allowing them to come back in next week, month, or year and attack you again.

Defending Your Data Center

You must do more than protect your network to defend your data center. Defense in depth, or building layers of protection, is a must. There are three Pillars of Protection” that support each layer and assist in making your data center secure. These are “People”, “Platform” and “Data.”

The first pillar is people. People are the Achilles’ Heel of Cybersecurity.[10] People have been and continue to be the single largest source of cybersecurity incidents. While, some may be “bad actors”, generally, they cause incidents by making simple mistakes that result in exposure to cyberattack or information leaks.

The second pillar of protection is the platform. This is the physical and virtual machines in your datacenter or your virtual machines in the cloud. While people are the root cause for the plurality of incidents, vulnerable systems are still a large portion of successful attacks. Hackers are quick to exploit vulnerabilities. If your systems aren’t patched or patched quickly enough you are exposed. A survey of Oracle customers showed that 74% of organizations take more than three months (could be one year, five years, or never) to patch their systems.

[10] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-internet-of-things.pdf

The third pillar is your data. You must protect your data. In 2016, the average cost per record of data stolen was $158.[11] The cost per record by industry ranged from $88/record for government (public sector data) to $355 per record in the healthcare industry. The means that the cost of stolen data to the healthcare industry in 2016 was over $325,000 per minute.[12]

In our next white paper, “Pillars of Protection: A New View of Enterprise Security,” we’ll address the pillars and the unique advantages Oracle Linux provides in assisting you in protecting all three pillars in your data center.

Conclusion

We are at war with cybercriminals. You need to make cybersecurity and defenses your top strategic concern. Defending your datacenter is crucial for the survival of your business. Ask your Oracle representative about the Oracle Linux Risk Assessment Program and how we can help you protect your data center and your data from cyberattacks. Learn more about how to protect your data center and/or your cloud deployments and the unique advantages that Oracle Linux provides in “Pillars of Protection: A New View of Enterprise Security” white paper.

[11] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report

[12] 1,378,509,261 records in 2016; 2622/minute; 35% are healthcare; 2622*.35 = 917.7 records/minute*$355/record = $325,783.5/minute

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/Linux
facebook.com/OracleLinux
twitter.com/OracleLinux
oracle.com/Linux

Integrated Cloud Applications & Platform Services