Key features of today’s cybercrime landscape

Moneer Barazi

In recent years, cyber-attacks have become more frequent and more vicious. Attackers have honed their skills and their impact is becoming both deeper and broader as the cybercrime ecosystem grows. Moreover, malware often stays on the victim’s servers for weeks or months before being detected. Financial losses are only one category of the losses. Cyber attackers can and have led to wider disruption at unprecedented scale, as today they can grind fuel supplies to a halt, and stop electricity from reaching hospitals, potentially leading to loss of life. Governments, organizations, and individuals must adapt very quickly as time is of the essence and geopolitical interests are at stakes. It is no longer only about profit.

Attacks are becoming broader and more effective

Banks and other financial institutions are being attacked from multiple angles. A case in point is the carbanak attacks against 100 financial institutions. The mastermind behind the attack was arrested in 2018. Below is a brief description of how they worked.

“The organised crime group started its high-tech criminal activities in late 2013 by launching the Anunak malware campaign that targeted financial transfers and ATM networks of financial institutions around the world. By the following year, the same coders improved the Anunak malware into a more sophisticated version, known as Carbanak, which was used in until 2016. From then onwards, the crime syndicate focused their efforts into developing an even more sophisticated wave of attacks by using tailor-made malware based on the Cobalt Strike penetration testing software.”

Cloud is a tempting and rewarding target

Businesses in general are increasingly relying on the cloud. The cloud infrastructure, in turn, relies increasing on Linux which currently powers 90% of the cloud workload. Attackers have responded to this development by developing malware targeted at Linux operating system and the cloud in general, where they can find troves of data that they can use in different ways. Linux-based malware grew 40% year-

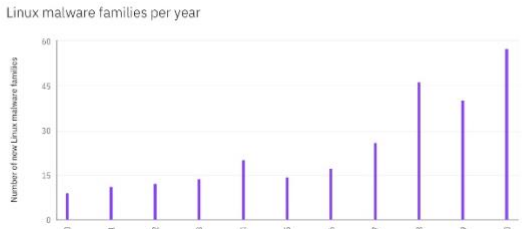


Figure 1: New Linux malware families discovered per year, 2010-2020 (Source: Intezer)

over-year from 2019 to 2020, and by 500% from 2010 to 2020 [1].

Companies should look beyond the direct cost of the attacks and look at the ripple effect

The recent attack on Colonial Pipelines has caused a disruption of oil supply to several parts of the United States for nearly a week. The cost of this disruption far exceeds the USD4.4 million ransom already paid (part of which has been recovered later) by the company. The outage led to chaos in the country, in addition to the lost revenue that Colonial Pipeline suffered from. Another example is when a cybercriminal attempted to poison the water supply in Florida. Fortunately, a proactive civil servant managed to step in and prevent the mass poisoning and save lives.

Those incidents, and several others, have far more serious ramifications that are seen outside of the cyber space. They impact people's lives materially outside of the virtual world. While those indirect consequences cannot be quantified with 100% accuracy, they need to be taken into consideration. Those consequences should offer another incentive for information security officers to be proactive, and CEOs and boards to invest in much needed layers of security.

Some VPNs are secretly (or explicitly) provided by Chinese companies

Research has shown that at least 101 VPN products (both cross-platform and mobile-only VPN products) are owned or operated by only 23 companies. Almost third of the popular mobile-only VPNs are Chinese which means that Chinese authorities can have access to sensitive information such as encryption keys, and details about users[2].

Motivations of attackers vary, but cybercrime is quite profitable. Proceeds are often reinvested.

The aim behind attacks can vary. In some cases, the goal is to achieve financial gains, either by demanding ransoms, or selling the data on markets on the dark web. In other cases, the aim is geopolitical. Attackers, often supported or tolerated by the host government, carry out attacks against adversary nations to achieve geopolitical gains. Examples of such nations include Iran, China, and Russia.

Attacks are becoming more sophisticated, targeted, widespread, and undetected

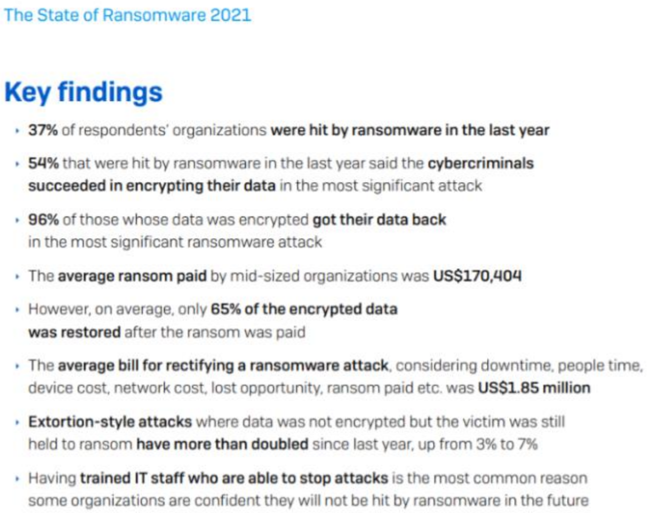
According to a report by European Union Agency for Cybersecurity (ENSIA), cyber-attacks are becoming more sophisticated, targeted, widespread, and undetected. Cyber attackers are working tirelessly to improve their capabilities, adapt to current layers of security, and wage better attacks.

[1] https://securityintelligence.com/posts/2021-x-force-threat-intelligence-index-reveals-linux-malware-spoofed-brands-covid-19/

[2] https://vpnpro.com/wp-content/uploads/Infographic-VPNpro-97-VPN-products-run-by-just-23-companies.pdf

To pay or not to pay, that is the question

Whenever a company is attacked by a ransomware, its leaders must make the decision about whether to pay to retrieve its data from the attackers or simply refuse to meet the demands. In theory, no company wants to make the ransom payment and succumb to demands of criminals. However, in reality it is not that simple, and companies do need to consider trade-offs. The Colonial Pipeline case shows the amount of disruption and delays that can happen when critical systems are infiltrated. Thus, companies need to consider various *what-ifs* before making the decision. They need to think about the sensitivity of the data and the consequences of exposure. **Yet, research shows that even when companies do pay, in more than 90% of the cases attackers do not return the data.** Even those who get it back, they do not get it back in full.



The State of Ransomware 2021

Key findings

- **37%** of respondents' organizations **were hit by ransomware in the last year**
- **54%** that were hit by ransomware in the last year said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- **96%** of those whose data was encrypted **got their data back** in the most significant ransomware attack
- The **average ransom paid** by mid-sized organizations was **US$170,404**
- However, on average, only **65% of the encrypted data was restored** after the ransom was paid
- The **average bill for rectifying a ransomware attack**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was **US$1.85 million**
- **Extortion-style attacks** where data was not encrypted but the victim was still held to ransom **have more than doubled** since last year, up from 3% to 7%
- Having **trained IT staff who are able to stop attacks** is the most common reason some organizations are confident they will not be hit by ransomware in the future

Recommendations for banks to improve cyber security

1- Companies can replace passwords with **biometric sensors**.

2- Companies can (and should) **examine their legacy systems** for potential vulnerabilities.

3- Companies **should mitigate the risk of human error** by offering their employees training to identify potential threats early on. Moreover, they should **curtail unnecessary authorizations and access** to their systems.

4- Ethical hacking. Companies **can offer incentives to ethical hackers** who can identify weak spots and vulnerabilities in their systems.

5- Banks should **extend the focus of their cyber security efforts to include their suppliers** and other stakeholders. Attacks through third party service providers are becoming more frequent and common. Toyota managed to avoid much of the impact of the current shortage of microchips by having close oversight and good relationships with their suppliers. Banks can achieve cyber resilience in the same way. In other words, banks should **adopt an ecosystem approach to cyber security**. Secure organizations are usually embedded in secure ecosystems.

6- Banks should **ensure that the configuration of their cloud services are secure**, as attackers can gain access through misconfigured cloud servers and infrastructure. According to IBM, remote exploitation of cloud environments was the most common infection vector observed, accounting for 45% of cloud-related cybersecurity events examined, and threat actors took advantage of misconfigured cloud servers to siphon over 1 billion records from compromised cloud environments in 2019.

7- **Preparedness (both mental and physical) is crucial.** Banks and financial institutions can **conduct simulation drills** where they simulate potential expected and unexpected security events to assess their defenses and preparedness. For example, investment banks in the US have mirrored military “war games” and gamified cyber security to train their staff on responding to threats.

8- Every organization is different. **Different kinds of assets require different kinds of investigative tools**.

9- Banks can carry out **awareness campaigns** about potential scams and phishing attempts targeted to older less tech-savvy generations. Even today, scammers are able to steal money from victims by pretending to be from Microsoft or any other trustworthy organization. Banks should help vulnerable clients with this increasingly common phenomenon.

10- Banks should be aware of the **negative transfer** attack. The hacker initiates a transfer of -100 (for example) from his account to the account of the victim. This would lead to the hackers account gaining 100 and the victim’s losing 100.

11- **Partnerships and alliances are crucial**. Financial institutions, among other, stand to benefit from cooperating with various stakeholders on reporting and dealing with cyber-crime. As cyber criminals become more organized, a more harmonized response from various actors with different capabilities is needed. In the past, major organization such as Wells Fargo, Visa, MasterCard, Citigroup, and others have launched **“cyber war rooms”** to coordinate threat intelligence and response. Norwegian banks can do the same.

12- **Within the bounds of the law, hacked institutions can hack their attackers back**. This is a controversial step that can be considered only if the law allows it.

13- **Expenditure on cyber security may be associated with diminishing returns after a certain point. Banks should not only consider the amount they are spending on cyber security but also the efficiency of that spending**. Research has shown that higher spending does not necessarily correlate with better protection.