THE CASE FOR COMBATING CYBER ESPIONAGE

Introduction

Across industries and enterprises of all types, the specter of cyber espionage lurks behind every email and every cursor click. This year, Microsoft notified more than 600 organizations about 23,000 attempted espionage-related intrusions into systems.[1] The intruders aimed to obtain information stored in the cloud and are associated with nation-state operators.

The inherent and inescapable interconnectedness of the internet, organizations, and global commerce means that cyber criminals can break into almost anything, from anywhere. Cyber espionage is a concern for every company. Software vulnerabilities and built-in backdoors allow hackers to quickly access systems, upgrade privileges and launch invasive and insidious surveillance operations in minutes. Although the majority of enterprises are not direct targets, they can function as conduits for larger espionage endeavors.

Analysts warn that the most sophisticated of cyber spies may move into stealing encrypted data. Why encrypted data? To crack the code using the quantum computers of the future. Although quantum computers may be years away, they still represent a legitimate incentive for hackers to steal high-value data right now.[2]

[1] "Ignoring Sanctions...," The New York Times, David E. Sanger, 26 October 2021

[2] "Hackers Could Steal Encrypted Data Now...," ZDnet.com, Liam Tung, 30 November 2021

Case-in-Point: The SolarWinds Security Incident

In late 2020, security experts discovered a stealthy cyber attack that targeted a company producing network and applications monitoring software; SolarWinds. Intruders lingered within the system for months, and possibly years, ahead of executing the maneuvers that left the world taken-aback.

Criminals managed to insert malicious software into a software update, which was deployed to thousands of companies and government agencies across the globe. While the SolarWinds enterprise functioned as the conduit, the hackers' main interest was in gaining widespread access to a large number of enterprise networks simultaneously.

Enter the Spy

In the past, stakeholders have not recognized cyber espionage as an issue, as the threat may seem distant and "shrug" worthy. Any espionage prevention protocols have fallen to the security team in entirety. As a result, espionage prevention tactics tend to be bolted on to projects as an afterthought, rather than being built into corporate systems and processes.

> The security cameras will catch a thief who's after the goods in the vault, but how will you catch the nation-state threat actors monitoring your security cameras?

If physical security is on stakeholders' minds, cyber security should be as well. After all, these days, it's arguably easier to conduct a cyber break-in than a physical one. A few clicks, and the bad actor is in.

Your stolen data can be used for nefarious economic gain and for reputational damage. In 2018 and 2019, Apple, the repudiated tech giant, experienced two distinct incidents whereby employees allegedly stole trade secrets pertaining to the company's self-driving car project. In one case, 40GB of sensitive data was exfiltrated from the company. The suspected thief intended to pursue a job with electric vehicle startup Xiaopeng Motors. Many presumed that the stolen intellectual property would be used within this startup's work.

Avoiding Surveillance and Theft

A handful of spies operate legitimately within international intelligence communities. However, other, more sinister, cyber spies remain at-large due to breakdowns in international communications and lack of extradition agreements between nations. In yet other cases still, inadequate technical capabilities on the part of authorities unintentionally permit espionage to persist unchecked. "Considering the volume [of espionage and economic attacks] ...going on, how many times has the F.B.I. gotten them? Precious few," says Nicholas Eftimiades, a retired American intelligence officer. [3]

When it comes to the prevention of espionage, a single tactic, such as the use of anti-malware tools, isn't enough. Organizations need to take a layered security approach in order to prevent surreptitious surveillance. CISOs, cyber security professionals, and business stakeholders should consider:

1. Deploying client protections; sandboxing, CDR, anti-phishing, anti-ransomware. Also, leaders should protect cloud email applications with cloud-native APIs to prevent phishing and account takeover, and should deploy micro segmentation protections for cloud and devices, e.g. for VMs, apps, cloud workloads, endpoints, mobile, IoT devices.
2. Optimizing threat intelligence. Robust and real-time intelligence can alert you to new techniques and procedures that cyber criminals are acting on.
3. Transforming your employees into a critical line of defense. Social engineers or phishing emails can't always be caught via sophisticated filters and technologies. Sometimes, security comes down to your human helpers.

[3] "Spies for Hire..." The New York Times, Paul Mozur and Chris Buckley, 26 August 2021

4. Assessing whether or not your organization follows a zero-trust network access framework. Applying zero-trust means that a stolen password is less likely to result in complete business compromise.

5. While Bring Your Own Device (BYOD) policies can appear cost-effective in the short-term, in the long-run, they can actually harm an organization. As a security administrator, it's impossible to know who has had access to the device and which sites, apps or advertisements a person has clicked on (without invading privacy).

6. A managed detection and response (MDR) solution, which can discern indicators of network compromise and endpoint interruptions. Essential components of an MDR solution include intelligence and AI-based tools.

7. Understanding what legitimate executables and files should operate on your organization's devices and making sure that the security team receives alerts should any strange behavior manifest.

8. Safeguarding the hardware that your enterprise uses. If your organization operates from an office space, ensure that employees know not to leave laptops or other electronics unattended. It only takes a moment for a bad actor to walk off with a piece of hardware.

9. Regularly testing and updating your organization's incident response plan can help you mitigate espionage-based attacks with greater ease, should they occur.

10. Working with a trusted security vendor that can provide routinely updated technological controls can enable you to prevent cyber intrusions.

In addition, organizations must operate in an espionage prevention mindset. Is espionage discussed in your organization's annual reports? Is it something that your organization should consider talking about? Also, keep track of how many security incidents you've seen within the past 12 months, along with the nature of those incidents.

In Conclusion

Cyber espionage conducted by nation-states, enterprises, and private persons is a growing threat. Espionage activities can result in tremendous financial, reputational and legal consequences. Pursuing a prevention-first approach can keep your organization safer in the ever-evolving digital threat landscape. Simple strategies and tactics can mean the difference between effective data management and serious security interruptions.

For more information about shoring up your systems and preventing cyber espionage reach out to your local Check Point sales representative. To get timely insights into tech trends, business news and more, visit CyberTalk.org.

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

www.checkpoint.com