Cyber-Espionage Report

Article

Fine-tuning your plan to address the most complex of threats

New research shows Cyber-Espionage is real, and a strong defense demands a unique mix of security capabilities.

By David Grady,
Chief Cybersecurity Evangelist,
Verizon Business Group

Cyber-Espionage is more than just the stuff of Hollywood movies and feverish online conspiracy theories. According to a new report from the Verizon Threat Research Advisory Center (VTRAC), Cyber-Espionage is a very real threat to a large number of industries, and it requires a specialized approach to defend against. "We've conducted all sorts of investigations into cybersecurity incidents and data breaches over the years," the Verizon Cyber-Espionage Report (CER) says. "None have been more challenging or perplexing than Cyber-Espionage."

The new report analyzes seven years (2014 to 2020) of data breach content collected by Verizon for its annual Data Breach Investigations Report (DBIR)—a report considered by many to be the gold standard in cybercrime research. The CER focuses on the unique nature of Cyber-Espionage, from the perpetrators and the actions they take to the specific capabilities security teams need to detect and defend against cyberspies.

Further, the CER makes one thing very clear: Unlike opportunistic threat actors who often attack indiscriminately (frequently motivated by financial gain), Cyber-Espionage threat actors—motivated by the goal of stealing secrets and other highly sensitive information—are patient and determined.

"Through advanced techniques and a specific focus, these determined threat actors seek to swiftly and stealthily gain access to heavily defended environments. Depending on their goals, they move laterally through the network, obtain targeted access and data, and exit without being detected. Or, they stay back and maintain covert persistence," the report advises.

Some industries are more prone to attack.

While no industry is immune to Cyber-Espionage, some have bigger targets on their backs, according to the report. State-affiliated or Nation-state threat actors are more likely to attempt to steal valuable secrets and internal data from Manufacturing, Information, Scientific and Technical Services, and Professional than from other industries.

Energy companies and utilities (Mining + Utilities)—part of any country's critical infrastructure—are also frequently attacked. And research from educational institutions is considered to be of high value to threat actors. The Public Administration sector (Public) is, of course, under constant threat of Cyber-Espionage attacks.

Capabilities and controls make the difference.

To help security teams in targeted industries (and any industry with sensitive, proprietary or classified data to protect) bolster their defenses, Verizon's new report maps insights and takeaways from hundreds of Cyber-Espionage breaches. It details well-established security controls that can strengthen the confidentiality and integrity of company secrets and sensitive systems. For example:

- Social engineering, or phishing, is a common method cyberspies use to gain access into sensitive systems. The CER explores how and why security awareness training can make a difference
- The report also describes how effective boundary defenses (such as network segmentation) and stronger access management capabilities (e.g., access granted on a need-to-know basis) can mitigate Cyber-Espionage attacks

verizon

- Because cyberspies tend to operate in a "low and slow" manner, detecting their unauthorized presence in an IT environment in a timely manner is crucial to minimize the damage that these threat actors can cause, according to the report. In the majority of Cyber-Espionage attacks, the bad guys often attack laptops, desktops and mobile devices. They can fly under the radar, undetected for months and sometimes even longer. A robust Managed Detection and Response (MDR) offering can smoke out indicators of compromise on the network and at the endpoint. Essential components of MDR include security information and event management (SIEM) technologies; security orchestration, automation and response (SOAR); threat intelligence; user and entity behavioral analytics (UEBA); and threat hunting capabilities, as well as integrations with endpoint detection and response (EDR), network detection and response (NDR), and deception technologies
- Data leakage prevention (DLP) can flag sensitive data being snuck out the back door
- Optimizing cyberthreat intel to help recognize indicators of compromise (IOCs); leveraging tactics, techniques and procedures (TTPs); and implementing a strong incident response plan are also important strategies for combating Cyber-Espionage

A formidable foe

Still, not all cyberspies are the same, so the security efforts to defend against them should be purpose-built as well. The CER offers a deep dive into seven industries particularly prone to Cyber-Espionage attacks, pointing out the actions taken by cyberspies against unique assets, thus allowing defenders to optimize their defenses and their detection and response efforts. These seven industries include Public, Manufacturing, Professional, Information, Mining + Utilities, Education and Financial.

As the CER points out, "if your industry isn't featured within this report, you're not off the hook. Cyber-Espionage threat actors may still be targeting your assets and data—you may just not have visibility into those attacks. If you've got sensitive, classified, proprietary or internal secrets that you'd like to keep from getting into the wrong hands ... read on."

Depending on the type of organization being targeted, the report states, Cyber-Espionage threat actors use different techniques to achieve their goals. "To stay ahead of cyber defenders and incident responders, Cyber-Espionage threat actors adjust their TTPs to embrace new technology, while keeping their tried-and-true TTPs operational."

With Verizon's new CER, the playing field should get more even.

Learn more:

To read Verizon's CER, visit verizon.com/cyberespionage
To learn more about how Verizon's security services can help you combat this unique threat, visit enterprise.verizon.com/products/security/threat-intelligence-solutions/

verizon