Cyber-Espionage Report

Tackling Cyber-Espionage: 2 approaches

Investigative tiger teaming—the reactive approach

By John Grim,
Distinguished Architect,
Verizon Threat Research Advisory Center

Cyber-Espionage breaches, as compared to all breaches, take much longer to discover (from months to years) and contain (days to months), according to the Verizon Cyber-Espionage Report. Not only are Cyber-Espionage breaches difficult to detect and contain, they're also a challenge to investigate.

In addition to slow (or no) detection, Cyber-Espionage breaches appear to be underreported. Because threat actors target Credentials, as well as Secrets, Internal and Classified data—all nonregulated data types—the victims have no obligation to report breaches. This is in stark contrast to breaches with mandatory reporting requirements, such as for Personal, Payment, Medical and Bank data.

The evidence
As with any data breach, investigators rely on digital evidence to identify, collect, parse and analyze Cyber-Espionage breaches. Cyber-Espionage-compromised assets focus primarily on end-user devices and software, such as desktops, laptops, mobile devices, servers, web applications and databases. This means proof can be hidden in malcode and suspicious files; endpoint forensic data, including memory dumps (memdumps); disks; and logs. It may lie in network forensic data, such as packets, flow and logs, as well as internet backbone flow and clear, deep and dark web content. Evidence can be found in both information technology and operational technology environments.

The process
The overall Verizon Incident Preparedness and Response (VIPR) process consists of six incident response (IR) phases. An established, familiar IR process is critical to an effective and efficient IR plan. An established process gives IR stakeholders and tactical responders, including a Cyber-Espionage tiger team, a strategy to respond to and resolve data breaches. A tiger team is considered a highly skilled, multifunctional tactical response team.

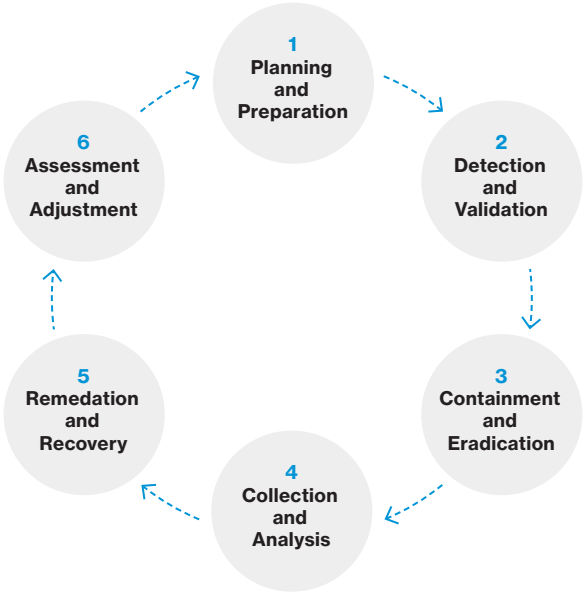

Figure 1: Reactive VIPR phases

VIPR phase 2 (Detection and Validation), phase 3 (Containment and Eradication) and phase 4 (Collection and Analysis) are the primary response and investigation phases for data breach and cybersecurity IR activities.

The team
Together with a solid IR plan, assembling a tiger team for Cyber-Espionage attacks is imperative to respond to breaches quickly. The team members should arm themselves with knowledge of the Cyber-Espionage tactics, techniques and procedures (TTPs); detection and response controls, such as the Center for Internet Security (CIS) Critical Security Controls (CSCs) (cisecurity.org/controls/cis-controls-list/); and evidence sources relevant to attacks.

The tiger team lead should be well versed in investigative response and familiar with team roles and responsibilities. Team members should include network investigators capable of examining packets, flow and logs; endpoint investigators

capable of analyzing memdumps, disk images and system logs; and malware examiners capable of sifting through malcode and suspicious files. Other members should include dark web hunters capable of reviewing clear, deep and dark web content, as well as threat intelligence analysts capable of providing insight into threat actor TTPs, indicators of attack (IoAs) and indicators of compromise (IoCs).

Attack detection
Key CIS CSCs to detect Cyber-Espionage attacks include:

- **Boundary Defense (CSC-12)** – Scan for unauthorized connection and deploy network-based intrusion detection system sensors
- **Implement a Security Awareness and Training Program (CSC-17)** – Train users to identify and report incidents
- **Malware Defenses (CSC-8)** – Centralize anti-malware logging
- **Account Monitoring and Control (CSC-16)** – Alert on account login behavior deviation
- **Maintenance, Monitoring and Analysis of Audit Logs (CSC-6)** – Regularly review logs
- **Data Protection (CSC-13)** – Monitor and block unauthorized network traffic

Investigative response
Key CIS CSCs to respond to and investigate Cyber-Espionage attacks include:

- **Boundary Defense (CSC-12)** – Configure monitoring systems to record network packets
- **Maintenance, Monitoring and Analysis of Audit Logs (CSC-6)** – Activate audit logging
- **Data Protection (CSC-13)** – Inventory sensitive information
- **Incident Response and Management (CSC-19)** – Document IR procedures

Tiger-team members should be qualified individually, based on experience, skill sets, training and certifications. They should also be trained as a team through data breach simulation exercises, Purple Team exercises – exercises involving both Red and Blue Teams – and proactive threat-hunting activities. This level of preparation can go a long way to effectively detect and respond to Cyber-Espionage attacks.

Threat hunting and Red Teaming—the proactive approach

**By Ashish Thapar,
Managing Principal, Asia-Pacific and Japan,
Verizon Threat Research Advisory Center**

While it's always better to be prepared for war, it's a known fact that wars are not won only on the battlefield. Significant effort is applied behind the scenes in planning, analyzing intelligence and preparing through training, testing and simulating. Similarly, rather than waiting for a Cyber-Espionage attack to occur (and taking a reactive investigative response approach), cyberdefenders and incident responders should plan and prepare for the next cybersecurity incident.

For cyberdefenders and incident responders, Cyber-Espionage threat actors pose a unique challenge—more so than other threat actors, including organized crime syndicates, hacktivists and even insider threats. 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 assets and data, and exit without being detected. Or, they stay back and maintain covert persistence for a long haul.

Countering this type of threat requires a significant level of insight, preparedness and cybersecurity maturity. Cyberdefenders can up their game by proactively hunting for undetected indications of Cyber-Espionage threat-actor activity. In turn, defenders can thwart further activity

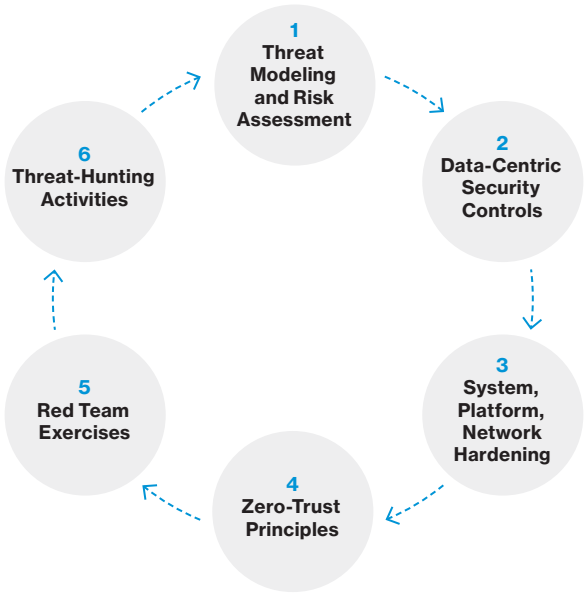

Figure 2: Proactive threat-hunting phases

and expel the bad actors. While this challenge may seem daunting, Cyber-Espionage threat hunting can be simplified by employing the VIPR phased proactive threat hunting.

The proactive approach to defending against Cyber-Espionage attacks typically starts with the data or information criticality, along with threats and vulnerabilities. From there, the process includes:

Threat modeling and risk assessment
Identify assets; ascertain those that need the most attention and determine the threat potentially targeting those critical assets. This would give rise to a prioritized set of security controls that need to be implemented to safeguard the critical assets first.

Data-centric security controls
Start with the data itself by examining the governance controls for securely handling information through people, processes and technology elements.

System, platform and network hardening
Implement robust protection controls to harden the systems, platforms (including containers and cloud-based systems) and network that may be used to access, process and manage sensitive or critical information.

Zero-trust principles
Implement "zero-trust" principles at all controls and checkpoints. The zero-trust principles would work to enforce controls so that no entity or network connection is trusted, and all access to critical resources (such as data, systems, applications or services) is duly verified. Implementing zero trust leverages controls such as network segmentation, multilayered protection and granular user-access control.

Red Team exercise
These assessments are covert in nature and are designed to test cyber defenders and incident responders. A typical Red Team exercise can include reconnaissance and initial vectors of compromise (including social engineering) to establish access or start from the assumed breach perspective, such as with a toehold on an employee laptop. For Cyber-Espionage breaches, the Red Team may then move through privilege escalation, maintaining persistent access (internally and externally), lateral movement, and finally, capturing the target information or meeting the objective.

Threat-hunting activities
To be effective and gain a significant advantage in detecting threat actors, implement key threat-hunting elements, such as:

1. Conducting a hypothesis-driven exercise
2. Proactively and reactively searching for threat-actor activities and TTPs
3. Effectively eliminating, or at least reducing, false negatives (i.e., indicators that signature-based detection approaches can overlook)
4. Assuming that threat actors are already present in the infrastructure
5. Placing a strong focus on IoAs combined with IoCs
6. Defining overall threat types and prioritizing the hunt for the most dangerous ones first

Visible and speedy detection techniques play a very important role in the never-ending battle against cyberattacks. For successful threat-hunting activities, it is imperative that detection measures be a combination of signature- and behavior-based techniques. For maximum impact on Cyber-Espionage threat actors, threat hunting must embrace behavior-based techniques and go above and beyond traditional defenses and monitoring.

More information:

- Cyber-Espionage Report: verizon.com/business/resources/reports/cyber-espionage-report/
- Verizon Threat Research Advisory Center (VTRAC) IR Hotline: +1.844.819.6071
- VTRAC services: enterprise.verizon.com/resources/reports/verizon-threat-research-advisory-center/

verizon