Targeted attacks are inevitable in organizations with sensitive data. Depending on the situation, a targeted attack may involve the theft of source code, negotiation data, or general business disruption. Companies need to be prepared to identify, respond, and mitigate a targeted attack with the same amount of effort that goes into implementing a disaster recovery plan. From decades of experience, the consultants at CrowdStrike have created the following checklists to help organizations prepare for and respond to targeted attacks.

BEFORE A TARGETED ATTACK:

- **Consolidate and Monitor Internet Egress Points:** All connections to the Internet from your corporate environment should be monitored to identify which information is leaving the environment. The less egress points to monitor, the easier it is to detect potentially malicious activity.
- **Leverage Host Based Detection:** As the workforce becomes more mobile, centralized network intrusion detection systems are not always in a position to inspect network traffic from a mobile workforce. Computers should utilize software, similar to the CrowdStrike Falcon platform, to detect tactics, techniques, and procedures from targeted attackers.
- **Implement a Tiered Active Directory Administration Model:** CrowdStrike recommends using at least three levels of administration to isolate credentials and prevent the compromise of critical credentials. These levels are Domain Admins, Server Admins, and Workstation Admins. No single account can access all systems. There are several ways to accomplish this depending upon your environment.
- **Minimize or Remove Local Administrative Privileges:** Users should not utilize accounts with Local Administrator privileges as this creates multiple ways for targeted attackers to move laterally and compromise credentials. CrowdStrike recommends disabling the Local Administrator Account. In an Active Directory Domain, the Local Administrator on workstations and servers should be disabled.
- **Implement Centralized and Time-Synchronized Logging:** DHCP, DNS, Active Directory, Server Event Logs, Firewall Logs, IDS, and Proxy Logs should all be stored in a protected centralized system that is time synchronized and easily searchable.
- **Have an Incident Response Services Retainer in Place:** Evaluate Incident Response firms in advance of when you may need their services, so that you have a plan in place if a targeted attack occurs.
- **Identify, Isolate, and Log Access to Critical Data:** Determine where your most sensitive data is located and implement logging and monitoring of access to it - NOW!
- **Patch, Patch, and Patch:** Patching operating systems and third party applications is one of the best ways to harden a network against a targeted attack. Critical security patches should be installed as soon as possible.
- **Subscribe to Cyber Intelligence Feeds:** Obtaining an understanding of who may be targeting you and the tactics they will likely use can help you to prioritize detection capabilities that will protect your sensitive data.
- **Review Reporting Requirements:** Identify which organizations and customers you have a responsibility to notify in the event of a security breach, and prepare documents and perform a legal review in advance.

RESPONDING TO A TARGETED ATTACK:

- **DO NOT DISCONNECT:** The majority of Targeted Attacks go on for months to years before being detected. When a compromised system is hastily disconnected, it is highly probable that the attacker will compromise additional systems to establish other forms of persistence that may go undetected. If a computer must be disconnected, ensure that a forensic image (to include a memory image) of the system is preserved prior to disconnecting power.
- **Preserve ALL Logs:** Validate that all centralized host-based and network-based logs are being preserved and that backups of critical servers are being maintained.
- **Establish Out-of-Band Communication Channels:** Assume that your network is completely compromised and the attacker can read email messages.
- **Contact an Incident Response Services Company:** This should be a company you already established a retainer with in the previous checklist.
- **Scope the Incident:** Conduct Network Forensics; Conduct Host Forensics to determine how many systems have been accessed or compromised and which data may have been accessed
- **Remediate the Attack:** Isolate Critical Systems; Block access to Command and Control Infrastructure; Remove and replace infected hosts; Perform Credential Resets where needed; Assess additional measures to harden the environment
- **Report:** Deliver required reporting per requirements and determine if media reporting is necessary.

Each environment is unique and will require additional items depending on the goals of the organization as well as the types of attacks that may be leveraged. CrowdStrike is available to help your organization prepare for a targeted attack, or to investigate one when it occurs.

Contact: Steven R. Chabinsky
General Counsel & Chief Risk Officer
Chabinsky@CrowdStrike.com
202.870.1442