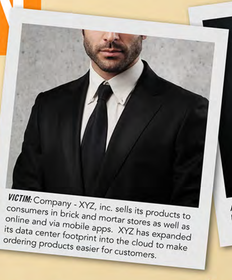
UNDERSTANDING THE CYBER KILL CHAIN

Today's attackers are a sophisticated lot, using advanced techniques to infiltrate a business environment. Lockheed Martin's team developed the Cyber Kill Chain to describe the different stages of an attack, from initial reconnaissance to objective completion.

Attackers will continue to infiltrate systems. The best opportunity to protect all types of sensitive data is to understand how attackers operate.

HOW AN ADVERSARY PROGRESSES THROUGH THE KILL CHAIN

The following fictitious case was created to map out an attack, categorizing each attack activity in the context of the Kill Chain.



VICTIM: Company - XYZ, inc. sells its products to consumers in brick and mortar stores as well as online and via mobile apps. XYZ has expanded its data center footprint into the cloud to make ordering products easier for customers.

ATTACKER: Hacker Group, EchoBravp (EB) has been tracking XYZ for quite a while

IDENTIFY & RECON | INITIAL ATTACK | COMMAND / CONTROL | DISCOVER / SPREAD | EXTRACT / EXFILTRATE

IMPACT
FINANCIAL LOSS
HARM TO BRAND
EMPLOYMENT CHANGES
SCRUTINY FROM REGULATORS

STEP ONE: IDENTIFY & RECON

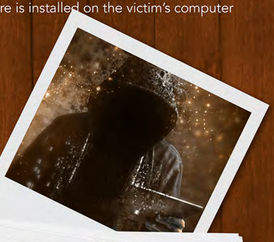
- EB begins by scanning the public-facing websites
- EB performs scans against the internal network looking for possible vulnerabilities, and/or holes in perimeter protection
- Extensive monitoring of employees, employees family, partners and suppliers social media networks
- Multiple potential entry points identified after several months of monitoring

STEP TWO: INITIAL ATTACK

- Using the information collected in the recon stage EB will be using several attacks vectors
- Malware via phishing emails and social engineering with the intent of an employee clicking a link that permits malware to enter the network
- Brute force attack to gain access to the XYZ network
- Using different IP addresses and a significant number of computers, EB hackers will kick off an automated dictionary attack
- After a few days – Success – malware is installed on the victim's computer

STEP THREE: COMMAND & CONTROL

- EB begins a "low and slow" in-depth recon against the internal network
- Disables several security controls on the infected machine
- Escalates privileges on victim's account and creates new user account with privileged access



STEP FOUR: DISCOVER AND SPREAD

- EB spreads malware across XYZ's environment through network shared, unsecured servers, USBs, and network devices
- Detailed map of network, security controls and new public cloud data center created
- EB waits, making detailed assets maps, noting employee patterns

One compromised account – in particular an IT admin account – can give an attacker full ability to do almost anything:
- *Propagate malware*
- *Disable or bypass controls*
- *Delete evident of presence*
- *Exhiltration entire virtual machines and data sets*
- *Suspect or delete workloads*

STEP FIVE: EXTRACT AND EXFILTRATE

- EB begins to siphon data out, moving targeted data to a remote server, taking additional steps to prevent a trace of the data's location
- After several months of siphoning data EB ends the campaign
- However makes several network modifications that will enable the group to return in the future
- XYZ's data is converted to cash – or Bitcoin – XYZ notified by government officials after data purchased by an undercover operative on the dark web

In this example, XYZ did not have the tools, technology, or expertise in place to detect EB's activities at any point across the Kill Chain. It's imperative that organizations approach securing their environment with the mindset of the attacker.

STOP ATTACKERS IN THEIR TRACKS

- Know your adversaries and their methods
- Detect threat activity earlier in the Kill Chain
- Disrupt the Kill Chain and stop the attack
- Extract actor presence and remove the threat

Cyber attacks are going to happen. Vulnerabilities and exploits are going to be identified. Having a solid security-in-depth strategy, coupled with the right tools and people that understand how to respond, can ultimately put you in a position to minimize your exposure and risk.

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides.

ALERT LOGIC.COM / U.S. 877.484.8383 / U.K. +44 (0) 203 011 5533

ALERT LOGIC®