Hillstone iNGFW White Paper: Intelligence Driven Defense

Introduction

Cyber-security has gone from a niche IT issue to a boardroom priority. Senior executives and boards of directors are no longer complacent about the risks posed by data breaches and cyber attacks. They know that a breach of confidential information can damage brand or reputation, trigger class-action lawsuits and cause costly downtime. They also know that data breaches are thrusting organizations into the media spotlight, as new regulations require public disclosure of security breaches - especially if cardholder data or personally identifiable information is exposed.

An unfortunate consequence of these disclosures is the embarrassing fact that most companies did not detect the breach on their own. According to several industry sources 69 percent of victim companies learned that they were compromised from a third party such as supplier, partner, customer or law enforcement. Implicitly, if you are a victim of an attack, you can assume that others – and not just the attackers – will also know about the incident. Another disquieting statistic is that it takes on average 205 days before a breach is discovered. That is a long time for the bad guys to be inside your network: performing reconnaissance, building backdoors, installing covert utilities, obtaining user credentials, and stealing your confidential data.

Organizations from all industries are targets of attack. Cyber threat actors are motivated by an ever-widening array of economic and political objectives. It can range from nuisance attacks (botnets and spam), to data theft for economic or political gain, to cyber crime for financial gain (e.g., credit card theft), to hacktivism (website defacements), to destructive attacks, which deleted data and destroy critical infrastructure.

Cost of a Data Breach

Regardless of the motivation, the cost to the victim company can be high. According to the Ponemon Institute's 2015 Cost of a Data Breach study, the average total cost of a data breach increased 23 percent over the past two years to $3.79 million. And, the average cost paid for each lost or stolen record containing sensitive and confidential information increased 6 percent, jumping from $145 in 2014 to $154 in 2015. The growing awareness of identity theft and consumers' concerns about the security of their personal data following a breach has contributed to the increase in lost business.

Attack Methodology

Over the last several years there has been a dramatic change in information security incidents. Superbly capable teams of attackers have expanded their intrusions at government and defense related industries to researchers, manufacturers, law firms, retail organizations, and just about every other enterprise imaginable. This class of threat has been given the moniker "Advanced Persistent Threat" or APT. Their success rate has been impressive. APT actors continually demonstrate the capability to compromise systems by using advanced tools, customized malware and "zero-day" exploits that easily evade anti-virus, firewalls, intrusion detection and other best practices. But, while attackers continue to adapt and become more sophisticated they all use a consistent and identifiable exploitation cycle. This cycle is called the Cyber Kill Chain and it consists of a series of steps that must be accomplished to successfully execute the adversary's mission. These steps include the following activity:

1. Initial Exploit

The initial exploit or reconnaissance phase is the "information gathering" phase. The attacker is looking for one or more vulnerabilities to penetrate the victim's network. They will often begin the process by scanning perimeter and internal network devices looking for weaknesses including: open ports, open services, vulnerable applications, vulnerable operating systems, weak protection of data in transit, and make and model of each piece of LAN/Wan equipment. Email addresses are highly prized because they can be used for spear phishing attacks. theHarvester is a very powerful tool to gather subdomain names, virtual hosts, employee names, open ports and banners from different public sources such as search engines or PGP key servers. It is particularly useful for email address discovery.

2. Delivery

Delivery is the phase where malware is surreptitiously installed on an end user's computer. Attackers often use several techniques to gain access to an organization. The most common method has been the use of social engineering to entice users to click on an attachment (or malicious link) in a spoofed email. When the victim clicks on the attachment their machine becomes compromised and the attacker gains access to the network. This is known as spear phishing.

As users have become more cautious about clicking on attachments attackers have shifted tactics. They are now placing malware on websites they know are used on a daily basis by the targeted organization. When the targeted users go to the compromised website malware is downloaded on their machines. Once installed, the malware collects usernames, passwords, browser cookies, and the computer name of the system being used. This is known as a watering hole attack.

3. Command & Control

To maintain a foothold in the compromised environment attackers deploy backdoors on several machines. Backdoors are used to communicate with the attacker's Command and Control (C2) infrastructure. It allows the attacker to remotely manipulate the victim's system, download the latest and greatest stealthy code, and exfiltrate stolen data.

4. Monetization

Not every attack is designed to exfiltrate data. Very often the attacker's sole motive is to turn the victim machine into a "bot" or zombie for financial gain. When the appropriate malware is installed the attacker can use an army of bots (botnets) to send spam, viruses, spyware, or steal credit card numbers, bank credentials and/or commit click fraud. It is not

uncommon for hackers to rent an army of botnets to commit these crimes.

5. Internal Recon

Once the attacker is inside an endpoint he needs to find the applications and servers that contain the data he intends to steal. He also needs to find servers that can be used as staging platforms to aggregate the stolen data and park his toolkits and utilities. Typically, they will use network scans and traffic captures to find this information.

6. Lateral Movement

Today's intruders access the majority of compromised systems with valid credentials. They often target domain controllers to obtain user accounts and corresponding password hashes en masse. Widely available credential-stealing tools have made harvesting passwords and escalating privileges in a Windows environment very easy. "Pass-the-hash" is a tried and true technique that is especially effective where groups of servers share the same administrator passwords.

Mimikatz is another popular tool that can snare plaintext Windows passwords that the operating system maintains in memory to support various forms of single sign-on. This tool is especially effective on shared servers that receive many interactive logon sessions.

Windows Management Instrumentation (WMI) and PowerShell are increasingly being used to move laterally in a Windows environment because they do not leave a footprint. Attackers use WMI to connect to remote systems, modify registry files, access event logs, and most importantly, execute commands. Aside from an initial logon event, remote WMI commands leave little evidence on the accessed system.

PowerShell can execute in memory without ever touching the disk on the accessed system. It leaves no footprint. Attackers are using the remote commands in PowerShell and in-memory scripts to move laterally and harvest credentials.

7. Data Exfiltration

Attackers often use staging servers to aggregate the data they intend to steal. They encrypt, compress and password protect the aggregated data. When it is time to transmit the data the attacker will obfuscate the transmission. For example, they may open hundreds of connections to legitimate websites to obscure the C2 site. Or, they may use domain-generating algorithms to change the location of the C2 domain each time a connection is established. And, in most cases, attackers will use legitimate user credentials so they blend in with typical user activity.

Threat Data ≠ Threat Intelligence

The Cyber Kill Chain is part of a "cyber threat intelligence" model for the identification and prevention of cyber intrusions. The adversary must progress successfully through each stage of the chain before it can achieve its desired objective. A single mitigation disrupts the chain and the adversary. Through an intelligence-driven response the defender can achieve an advantage over the aggressor for APT caliber adversaries.

Today, however, the term "cyber threat intelligence" is often misused. In many cases it is used to describe raw information such as a list of attacks. An undeniable truth is that IT administrators already have too much unvetted data causing too many false alarms. What they need is predictive, accurate insights into the real threats relevant to them;

delivered at a speed and in a format that enables an efficient, effective response. In other words, they need actionable intelligence to verify, mitigate and prevent future attacks.

The Hillstone Advantage

The cyber kill chain is part of the Intelligence Driven Defense model built into Hillstone's Intelligent Next Generation Firewall (iNGFW). It provides an instantaneous visualization of where an adversary is within the kill chain framework. It enables the administrator to determine both the strategy and the tactics used by the attacker within minutes rather than the hours or days typically required for advanced forensic analysis.

But just knowing where an attacker is inside the kill chain is not enough. The system should provide near instantaneous detection and response to prevent the attacker from gaining a foothold within the network. In this regard Hillstone leverages an important fact. According Verison's Data Breach Investigations Report most unknown malware is simply a variant of "known" malware. It is this fact that allows Hillstone to detect malware before it can do damage.

Advanced Threat Detection

Hillstone has built a proprietary engine that has analyzed close to a million "known" malware samples. Each sample has been classified and characterized based on multiple dimensions that describe its actions, assets and attributes.

When new malware is encountered (in an actual deployment) it is also analyzed, characterized and classified. Then it is compared to the database of known malware samples that have already been analyzed. The closer the unknown sample matches a known sample - the higher the confidence that it is a variant of a known malware sample. This process is called "statistical clustering" and it provides a very accurate method for identifying new malware.

Statistical clustering has several advantages. First, it is a very fast method of identifying malware before it can do significant damage. Second, Hillstone can provide a complete description of the attack as well as the criticality of the attack (critical, high, medium, low) based on the malware it most closely resembles. And finally, Hillstone provides a degree of certainty or confidence based on how closely the unknown malware matches a known malware sample.

Hillstone is constantly refining its Advanced Threat Detection model. All newly discovered malware is uploaded to Hillstone's cloud security analytics platform. There, in conjunction with security experts, an in-depth analysis is done to fine tune the Advanced Threat Detection engine. In addition, a signature is created for the unknown malware. This signature is downloaded to all iNGFW customers and installed in their blacklist.

Abnormal Behavior Detection

Not every malware infection can be detected by Hillstone's firewall. Laptops often become infected outside of the protection of the corporate network. For this reason Hillstone has developed a sophisticated analysis tool that uses machine learning to determine if network behavior is outside normal parameters. Hillstone's Abnormal Behavior engine continuously monitors the network to learn what normal network traffic looks like for that particular day, time, and month; and it will alert when network activity exceeds calculated thresholds. It uses a 50+ dimensional array to calculate normal

network traffic from layer L4-L7. In addition, it has been trained with real hacking tools to insure that it will readily recognize malicious activity. These techniques limit false positives and provide the user with multiple opportunities to stop an attack.

Rich Forensic Analysis

Hillstone delivers a whole new way of seeing and analyzing attacks. Every action taken by the malicious code is automatically linked to steps in the "kill chain." It is complemented with rich forensic information that enables the security analyst to determine the origin of the attack, the severity of the attack, and the methodology employed. Hillstone also provides packet capture files, which when combined with syslog and traffic logs provides the administrator with a wealth of information. In addition, user data such as websites visited, applications used, and the risk level of the applications bring the exploits into sharp focus. And finally, Hillstone identifies the exact firewall policy that allowed the attacker to get through the firewall. Clicking on the policy number takes the administrator to the policy so he can examine and change the policy on the spot.

This last point is important. Many organizations have firewalls with years or even decades of configuration changes, with ports left open, IP addresses left unblocked and rules created without any documentation. When IT administrators find themselves victims of an attack they often have difficulty tracing it to the firewall policy that created the vulnerability. This is a bigger problem than most people realize. Gartner estimates that 95 percent of datacenter breaches are caused by misconfigured firewalls.

Knowing that you are under attack is the first (and most important) step to mitigating an attack. Hillstone's dashboard provides a "network risk index" which graphically displays the overall security health of the network. Next to this graphic are the numbers of hosts that are at risk of an infection sorted by criticality. With one quick glance the administrator can assess his security posture and with one click he can see which hosts are at risk.

Preemptive Mitigation

Beside the obvious ability to make a policy change to prevent an attack Hillstone has built-in several automatic mitigation features. These features consists of pre-defined templates that automatically slow-down or block an attack if suspicious behavior is detected. The intent of these templates is to buy time so that the administrator can examine the forensic information and make an informed decision about the authenticity of the attack.

Several options are available to the administrator. He can modify the templates to limit the bandwidth or the number of sessions available to the attacker. He can also adjust the constraints he places on network resources based on the type of attack and the confidence level. In cases where the attack is critical and the confidence level is high the mitigation can include a complete blockage of all network resources. And, if a template does not exist or is not active, the administrator can quickly setup a temporary mitigation for that event.

SUMMARY

Data breaches are a new business reality. Protecting corporate data is no longer just an IT challenge; it is fundamentally a business challenge. With the influx of new threats and the changes in regulatory requirements, an organization's security needs are continually evolving. Legacy signature-based security methods are no longer adequate against todays advanced attacks. Enterprises must employ world-class security that provides insight into the strategy and the tactics of the attacker so that appropriate mitigation steps can be deployed.

There is a world of difference between basic threat data and actionable cyber threat intelligence. Separating the two can mean the difference between preventing an attack and responding to one. Hillstone delivers actionable threat intelligence that provides real-time attack visualization and forensic analysis that allow security teams to rapidly achieve "intelligence driven defense." This new way of looking at attacks enables security personnel to completely reconstruct and validate even the most complex attacks in just minutes rather than the hours or days required with basic threat data.