CYBERTHREAT REPORT: RECONNAISSANCE 2.0

Attackers have developed an arsenal of tools and techniques to break into organizations' networks and steal valuable information. This report reveals the latest tactics threat actors use to stay under the radar while conducting internal reconnaissance. It also explains how automation has enabled amateur hackers to carry out advanced reconnaissance and accelerate their attacks.

Attackers in Search of Valuable Data

Targeted attacks often start with the weakest links in organizations' defenses: their endpoints. The initial step of a targeted attack can be as simple as convincing a user to open a email attachment. With 4 percent of users falling for any given phishing campaign[1] and attackers able to send an infinite number of phishing emails as well as execute countless other attacks – from zero-day exploits to social engineering attacks – intrusions can strike even the best-fortified organizations.

Once attackers have compromised an endpoint, they must establish a channel of communication to a command-and-control server. Next, they begin to explore their surroundings as they search for valuable assets. During the internal reconnaissance phase, they may pursue paths that lead to dead ends, but will continue trying new avenues until they achieve their objective.

To avoid detection, threat actors continually update their tools and methods. They take advantage of new techniques to determine the lay of the land and locate key assets, such as Active Directory® servers, file servers and databases.

For years, attackers have used a combination of port scanners, malware, hacking tools, and trial and error to map out targeted networks and expand their realm of access once they've gained a foothold in the network. Today, many attackers have increased their repertoires of internal reconnaissance techniques to include those shown in Figure 1.

Figure 1: Some internal reconnaissance techniques

These internal reconnaissance techniques allow threat actors to cloak their activities and speed up their attacks. So, how do they work? More importantly, can we detect and stop these attacks before the damage is done? We believe the answer is a resounding "yes."

Fileless Attacks

As security technologies get better at detecting malware, threat actors have turned to fileless attacks to compromise endpoints and conduct internal reconnaissance without raising alarms. Fileless attack techniques include the following:

- Memory-only malware
- Script-based malware and tools
- Embedding malicious code in benign files

Threat actors use fileless attacks because they are much more likely to succeed than traditional, file-based malware. In fact, according to a recent survey, 77 percent of successful attacks in 2017 were due to fileless attacks or exploits, while only 23 percent of compromises were attributed to file-based attacks.

__77%__ of successful attacks in 2017 were due to fileless attacks or exploits.

Fileless attacks can elude security controls because traditional antivirus software was designed to analyze files and look for attributes or functions of files to determine if they are malicious. However, with a fileless attack, there is no traditional file for antivirus to scan or analyze, enabling an attacker to circumvent static, disk-based detection.

Attackers can start with an exploit distributed through web or email traffic, such as a malicious Adobe® Flash® file, a macro in a spreadsheet or even a specially crafted JavaScript string, that takes advantage of an endpoint vulnerability to execute malicious code.

Attackers can then abuse built-in Windows® tools, such as PowerShell® and Windows Management Instrumentation, or use other tools, such as Metasploit®, to transfer malware from a remote location and load it into memory. The malware contents are never written to the disk but reside in volatile system areas, such as in-memory processes or service areas. Memory-only malware is especially effective on servers and network devices that are rebooted infrequently.

1. Verizon 2018 Data Breach Investigations Report

Attackers also use script-based malware, often in conjunction with memory-only malware, to execute commands on targeted machines. Because scripts are unstructured text files, security tools cannot easily use attack signatures to detect them. Attackers can easily modify parameters, names or the order of script code to thwart signature detection.

Lastly, attackers can embed malicious code in well-known files, especially free or open source apps that are not digitally signed. They can even inject code into running processes. If antivirus tools happen to detect malicious functions in these legitimate files, security analysts typically assume the alerts are false positives in favor of focusing on seemingly higher-priority threats. Once attackers have compromised an endpoint with a fileless attack, they can traverse the network to find and exfiltrate data.

__20%__ of all attacks in 2016 were fileless. Fileless attacks are expected to increase to __35%__ in 2018

Prepackaged exploit kits and frameworks have made fileless attacks easier than ever to deploy and more commonplace in today's threat landscape. Out of all attacks in 2016, 20 percent were fileless, and this figure is expected to increase to 35 percent in 2018.[2]

Living off the Land

Once attackers have exploited an endpoint – often with a fileless attack – they attempt to locate and steal, manipulate, or destroy data. Rather than drawing attention to themselves by installing malware or attack tools, stealthy attackers use existing applications already on victims' machines to perform reconnaissance. These applications are trusted and used for legitimate, day-to-day activities, so attackers can use them in multiple stages of the attack lifecycle, including internal reconnaissance, while evading detection.

Living off the land also consists of abusing well-known services, such as GitHub®, Pastebin, Twitter®, Box or even Microsoft® Office 365®. Attackers use these services to find sensitive data in online file sharing and email applications. They also use these services for command and control as well as data exfiltration.

To survey the network, shrewd attackers take advantage of networking apps, such as Ping, NetStat and IpConfig, as well as remote desktop tools and admin utilities. If attackers happen to compromise IT administrators' machines, they've hit the "living off the land" jackpot and can usually commandeer multiple apps – and credentials – that can help them achieve their underhanded goals.

Security teams cannot easily uninstall all these applications. Compounding security risks, attackers living off the land can often bypass traditional antivirus software and application whitelisting tools because attackers have not installed new files on the system. As a result, there are no signatures for antivirus tools to detect and few traces of activities that can be used for forensics.

Abusing Backups

Many organizations invest inordinate amounts of resources in protecting their sensitive applications. They deploy firewalls, strong authentication, threat prevention, endpoint protection and more to safeguard their apps and data. However, these security-conscious organizations do not typically extend cybersecurity best practices to backup servers. They often consider password protection and regular patching to be sufficient security controls. As a result, backup servers can provide easily accessible treasure troves of data to unscrupulous hackers.

As a case in point, "Phineas Fisher," the self-proclaimed hacker of Milan-based IT company HackingTeam, reported that he had used backup servers to obtain access to several virtual machines, including HackingTeam's Exchange Mail Server. In his "Hack Back" guide, Fisher claimed, "Their insecure backups were the vulnerability that opened their doors." The HackingTeam attack was not the first to exploit unprotected backup systems, but it did raise awareness among the black hat community about using backup systems and services to locate and steal data.

Because backup servers contain prior versions of active data, they should be protected with the same level of security as active servers and applications. Organizations should implement the Zero Trust model, using network segmentation and granular firewall policies to limit access to

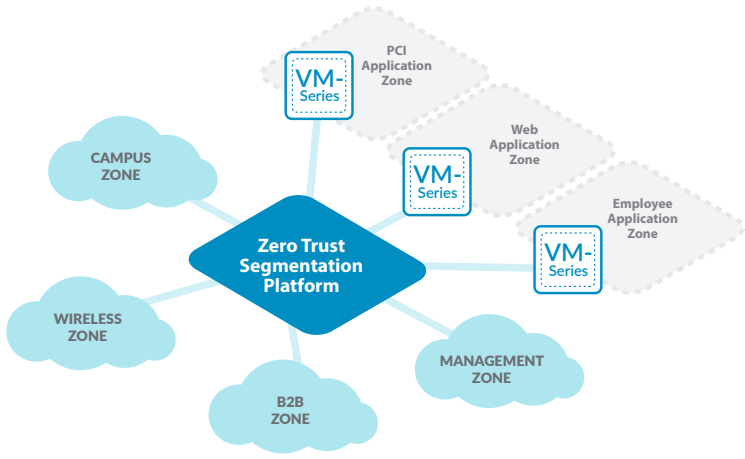

Figure 2: Zero trust model

2. The 2017 State of Endpoint Security Risk, Ponemon Institute

authorized users. They should also implement multi-factor authentication to prevent attackers from accessing backup data with stolen credentials. Lastly, organizations should monitor access to backup data to detect unusual activities, such as a user downloading a large volume of data, or a user downloading data without uploading or syncing any data.

Automation

In the past, only the most sophisticated cybercriminals and state-sponsored attackers could carry out targeted attacks. Now, even the most novice-level hacker can carry out multi-stage attacks using a combination of attack tools, scripts and information sharing. Automation also enables attackers to perform reconnaissance more quickly than ever.

Penetration-testing tools, such as Metasploit and PowerShell Empire, have simplified targeted attacks. Although these tools are not necessarily new – Metasploit was first introduced in 2003 – they have added features over time to exploit systems, discover new vulnerabilities, and assist white hat or black hat hackers through every step of an attack. With many of these tools boasting active online communities, they are continually being enhanced to include new features and exploits.

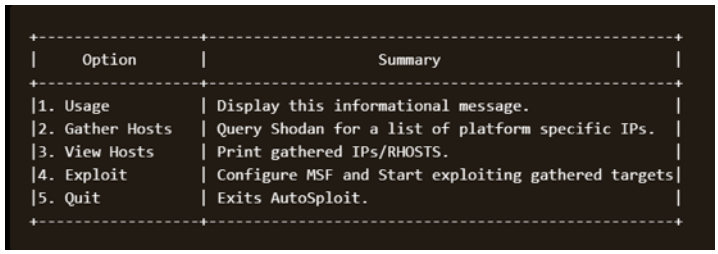

Figure 3: AutoSploit simplifies reconnaissance and system exploitation

More recently, developers have added graphical user interfaces and included exploit recommendations with their tools, making "pen" testing and hacking easier than ever. Developers have also included integrated scripts that enable even the most novice-level pen testers and hackers to carry out their attacks. For example, AutoSploit, introduced in early 2018, automates many of the manual steps of an attack, allowing virtually any attacker to execute a multi-stage assault. AutoSploit combines Metasploit and Shodan®, a search engine for internet-connected devices, allowing attackers to locate and exploit systems, such as insecure IoT devices.

Although cyberwarfare experts may prefer stealthy, manual attacks, attack automation brings advanced attacks in reach of less-sophisticated attackers. It also allows attackers to detect and exploit newly announced vulnerabilities very quickly, requiring organizations to patch systems just as rapidly. With attackers increasingly using automation, security teams must fortify their defenses and automate detection to outpace attacks.

Protecting Your Organization From Reconnaissance

Internal network reconnaissance is a key component of most targeted attacks, but it is also when attackers are the most exposed. For threat actors, initial intrusion is often just the first step. Once they have penetrated a network, they must take thousands of individual actions as they explore the network and move laterally until they access targeted data. If defenders can gather and analyze the signals such universal attacker activity gives off, they can get ahead of the threat actors.

With the right technology, we believe security teams can prevent successful cyberattacks. By automatically profiling user and device behavior, security teams can detect unusual behavior indicative of internal reconnaissance and the other phases of a targeted attack. Security teams only need to detect one of the many actions threat actors take in order to identify them, lock them out of the network and disrupt the attack.

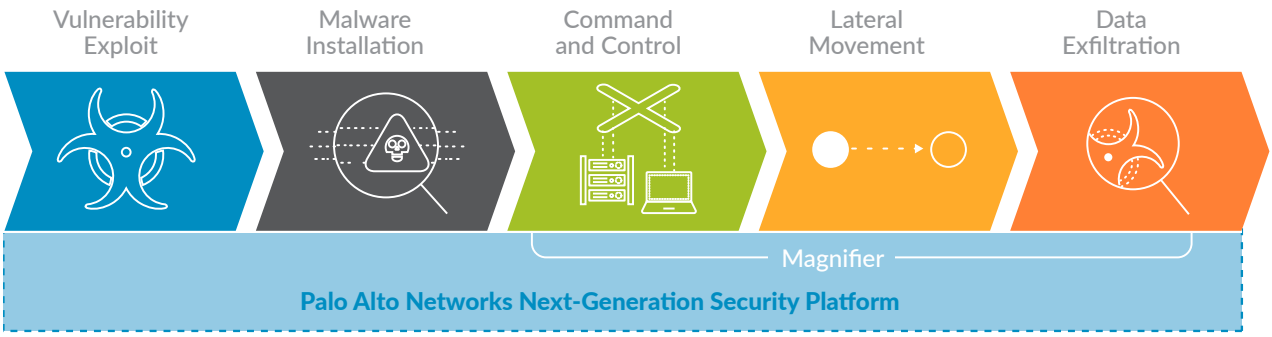

Figure 4: Palo Alto Networks prevents threats across the attack lifecycle

Stopping Attacks With Magnifier Behavioral Analytics

Magnifier™ behavioral analytics, the first app on the Palo Alto Networks® Application Framework, empowers security teams to find and stop advanced attacks. By analyzing rich network, endpoint and cloud data with machine learning, Magnifier accurately identifies behavioral anomalies indicative of attacks.

Magnifier detects internal reconnaissance even when threat actors don't use malware because it focuses on changes in network behavior. As a result, Magnifier can catch attackers living off the land, abusing backups or conducting automated reconnaissance. Magnifier can also detect attackers using fileless attacks and scripts to move from one host to another within the network.

Magnifier focuses on network-based attack behaviors and, using Magnifier Pathfinder endpoint analysis, can determine which endpoint processes are responsible for attacks. This integrated endpoint analysis helps security analysts identify which apps or tools, such as PowerShell or WMI, were used for attacks. Magnifier can also scan corporate devices and uncover rare processes. If Magnifier detects pen testing or hacking tools on a host, security teams can investigate further to determine if the host has been compromised.

Magnifier is a key element of the Palo Alto Networks Security Operating Platform. Our platform empowers customers to prevent successful cyberattacks by harnessing analytics to automate detection and enforcement. Data collection and analysis are tightly integrated across our platform as well as our partners' products to maximize security efficacy and IT efficiency.

Figure 5: Palo Alto Networks Security Operating Platform

Staying Ahead of Attackers

Cyberattack methods continually change. It is only a matter of time before attackers come up with new ways to speed up their attacks and hide their activities from security tools. Today's reconnaissance techniques – like living off the land, fileless attacks, abusing backups and automation – are dangerous, but attackers will eventually replace them with new attack methods. However, attackers will still need to gather information about their environments before they can locate and steal data. By profiling the network behavior of users and devices, security teams can detect internal reconnaissance even if attackers change their tools and techniques in the future.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cyberthreat report-reconnaissance2-wp-072418