SECURITY IN CONTEXT

LATERAL MOVEMENT:
How Do Threat Actors Move Deeper Into Your Network?

LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Enterprises consider advanced persistent threats (APTs) to be high-priority threats due to the risks they pose against confidential data. The impact of APT campaigns to an organization or business includes data or intellectual property theft, damage to business reputation or image, and/or sabotage.[1]

Phases of a Targeted Attack

In an APT campaign, attackers begin by obtaining data on the target organization such as its network environment and the organizational structure. The gathered data is then used for social engineering ploys in order to gain entry into the network. Attackers can use compromised email accounts or popular web-based email accounts to send contextually relevant email. This is done to trick employees into opening the email, which can carry exploits and malicious attachments or links.

Once threat actors gain access to the network, they establish and strive to sustain communication with the compromised computer. Threat actors then need to gain more privileges by getting login credentials from the network that has access to valuable information. However, note that threat actors may also gather information (e.g. documents found in desktops, network access for shared drives etc.) via regular user accounts. Once identified, the target data will be made ready for exfiltration.

Gaining Persistence across the Network

Lateral movement usually involves activities related to reconnaissance, credentials stealing, and infiltrating other computers.

When communication with the compromised systems and C&C (command and control) servers is established, threat actors need to sustain persistent access across the network. To do so, they have to move laterally within the network and gain higher privileges through the use of different tools. This, in turn, enables threat actors to have access to servers, which contain valuable information—the company "crown jewels."[2]

"An APT attack is not a one-time process. Threat actors continuously look for new targets to expand their control over the targeted organization. They also change their plans and adopt different techniques and tools depending on the information they collected."

— Spencer Hsieh, threat researcher

Apart from servers, threat actors may be also interested in endpoint systems. For instance, confidential documents such as Microsoft Word, Microsoft Excel and Microsoft PowerPoint files are stored in personal computers.

As threat actors move deeper into the network, their movements and methods become difficult to detect especially when they utilize Windows features and tools typically used by IT administrators. Gaining administrative privileges also makes threat actors' activities undetected or even untraceable.

[1] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apt-primer.pdf

[2] http://about-threats.trendmicro.com/us/threat-intelligence/targeted-attacks/annotations-from-the-labs/inside-the-network-time-for-persistence

Deeper and Deeper into the Network

Reconnaissance

In order to move laterally within the breached network and remain persistent without being detected, attackers obtain information like network hierarchy, services used in the servers, and operating systems.

Attackers also check the host naming conventions to easily identify which specific assets to target. They can utilize this information to map the network and acquire intelligence about their next move.

Some of the tools used in this activity include netstat, a command-line tool that can get network connection information via active connections and open ports. This may be used for identifying running services or internal servers accessed by the compromised computer. Port scanning tools check open network ports in order for attackers to make a tunnel connection between the compromised system and his system. Port forwarding tools like ZXPortMap and ZXProxy (aka AProxy) are used to create a tunnel connection to bypass firewall protection.[3]

Stealing Credentials

Once threat actors identify other “territories” they need to access, the next step is to gather login credentials.

Cracking and Stealing Passwords

To access these “territories,” attackers use keyloggers, ARP spoofing and hooking tools among others to obtain credentials. Hooking tools basically hook functions related to password authentication while ARP spoofing tools sniff conversations between two systems or more in a network packet though spoofed ARP to steal credentials. Pwdump is another tool for getting password hashes from the Windows registry. Other tools used are Windows Credential Editor (WCE), Mapiget , Lslsass, Gsecdump and CacheDump.

[3] http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/

Pass the Hash

Attackers can also use a technique called “pass the hash” which involves the use of a hash instead of a plaintext password in order to authenticate and gain higher access. They can also use a brute force attack, which is simply guessing passwords through a predefined set of passwords.

Using the gathered information, threat actors can now move to new territories within the network and widen their control. These activities may go unnoticed by IT administrators since they only check failed logins without tracking the successful ones.

Infiltrating Other Computers

Using stolen credentials, threat actors can now remotely access desktops. Accessing desktops in this manner is not unusual for IT support staff. As a result, remote access will not be readily associated to an ongoing attack. Moreover, attackers may also gather domain credentials to log in systems, servers, and switches.

Remote control tools enable attackers to access other desktops in the network and perform actions like executing programs, scheduling tasks, and managing data collections on other systems. Tools and techniques used for this purpose include remote desktop tools, PsExec, and Windows Management Instrumentation (WMI). Note that these tools are not the only mechanisms used by threat actors in lateral movement.

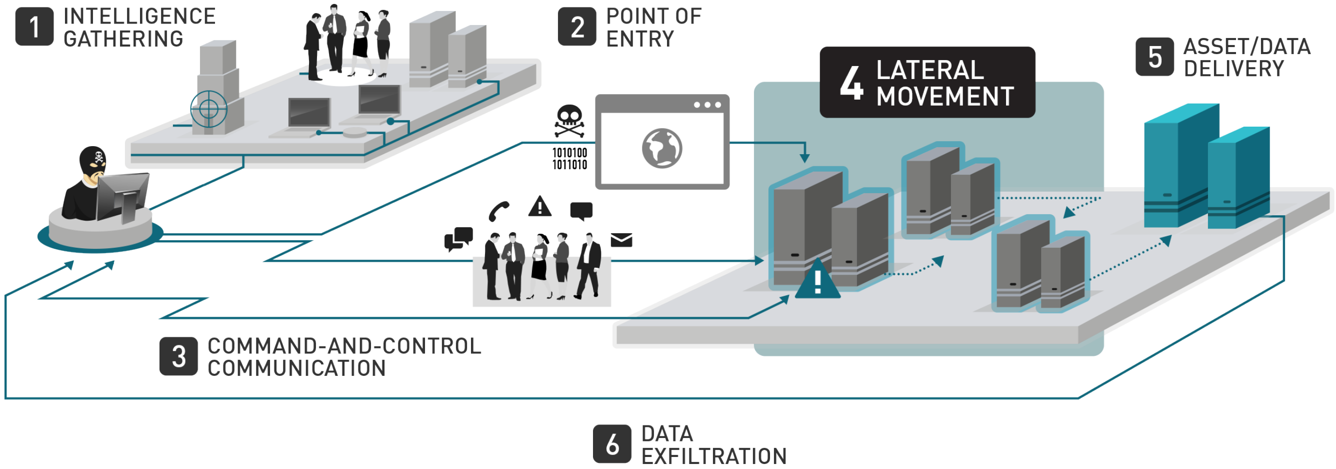

Figure 1. Six Stages of an APT attack

Develop Threat Intelligence

While lateral movement is arduous to detect, related activities can be detected via monitoring tools and a strong in-depth defense strategy. Enterprises need to build external and local threat intelligence, which can help determine indicators and APT-related activities.

IT administrators must also be knowledgeable on how their network infrastructure looks like at the baseline, which can be used as a point of comparison to help identify if the organization has been compromised. The presence of tools that have the same function as the tools discussed above should also trigger an investigation on how it is being used in the network. Moreover, a centralized location for all those who log in a system is a reliable way to detect any unauthorized access.

Since blacklisting and traditional AV signature-based solutions won't mitigate the risks of targeted attacks at this particular stage, enterprises need a robust security technology that can provide real-time local and global intelligence.[4] This can help IT administrators understand the nature of the attack they are dealing with. It also supports threat intelligence initiatives with its network-wide security event collection and analysis, which can enable IT administrators to perform remediation and containment plans.

> "An astute IT administrator or team who knows what is on their network may be able to detect lateral movement if they have monitoring tools installed in the proper locations."
>
> — Jim Gogolinski, senior threat researcher

These remediation plans should include an advanced threat detection which can determine any malicious content and communications. Such a plan should also include detecting behavior indicative of advanced malware and threat actor activity, threat tracking, analysis, and action that provides real-time threat visibility and in-depth analysis.

Enterprises need Custom Defense, an advanced threat protection platform that can perform network-wide monitoring to detect zero-day malware, malicious communications, and attacker behaviors that are invisible to standard security defenses.

Such security platform uses multiple detection engines and customer-defined sandboxes that better reflect an organization's real-life environment and allow them to determine whether they have been breached. Sandbox simulation gives them the power to block spearphishing and social engineering exploits commonly used by attackers in the initial phase of a targeted attack.

[4] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_custom-defense-against-targeted-attacks.pdf

TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS[SM]

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

TREND MICRO™

Securing Your Journey
to the Cloud

TrendLabs
Global Technical Support & R&D Center of TREND MICRO