Malware Lateral Movement: A Primer

mandiant.com/resources/blog/malware-lateral-move

Chad Holmes

For all the talk about malware, a lot of discussion focuses on initial infection. Recently, the lateral spread of malware—so called east-west movement—has garnered more increasing interest. Here's some basics every security professional should know.

So, how is your day-to-day IT operations related to lateral spread?

During our incident response engagements conducted all over the world, we identify numerous trends related to how malicious actors, maintain persistence and move laterally within a compromised organization. After the initial host compromise, the malicious actors will typically focus their efforts on credential harvesting, internal reconnaissance and attacking other internal systems to get deeper inside your network.

They will utilize whatever is at their disposal to continue their quest for your data. This often includes leveraging built-in operating systems, and IT support tools and protocols that your organization actively relies on during its daily operations. For example, they will access and use tools like PowerShell, remote desktop protocol, Kerberos, remote scheduling tools, communication protocols and many others to move throughout your network.

Beyond just being resourceful, attackers often turn to these tools and protocols for another reason: Evasion. Tools like Powershell are often whitelisted, and their activity/logs are often not part of a security log review process. By leveraging already-existing tools and protocols, attackers avoid being detected on your network; a key aspect of longer term, persistent campaigns.

The key techniques used for lateral movement are:

1) Internal reconnaissance
Lets first take a look at the different techniques and tools that the malicious actor will use during their internal reconnaissance efforts. After they are able to gain access to an individual machine on your network, they will need to find out where they are located, what they can get access to and what firewalls or other devices that maybe between them and their goal. To do this, they may download other tools or they will use built-in windows or support tools, to reduce their risk of being detected.

Here is a brief list of some built-in tools, that they may leverage to do internal reconnaissance.

- Netstat – Built-in tool showing the machines current network connections. This can be used for identifying more critical assets or used for gaining knowledge of the network they are connected to.
- IPConfig/IFConfig – Built-in tools providing access to the network configuration and location information
- ARP cache – Provides information of the IP address to physical address. This information can be used for targeting individuals machines inside your network and/or used for evasion techniques.
- Local Routing table – This will display the current routes/communication paths for the connected host
- PowerShell – Powerful built-in Windows command line and scripting tool

They could also leverage tons of external custom tools and open source tools for port scanning, proxy connections and other techniques.

2) Credentials harvesting;
When it comes to massive compromise of an entire network, credentials are a main component. Out of all the incident response engagements that we conducted; 100% of them involved the threat actor compromising valid credentials during the attack. The malicious actor used any and all possible techniques to gain access to the local or domain level credentials.

Here are some of the techniques, we have seen;

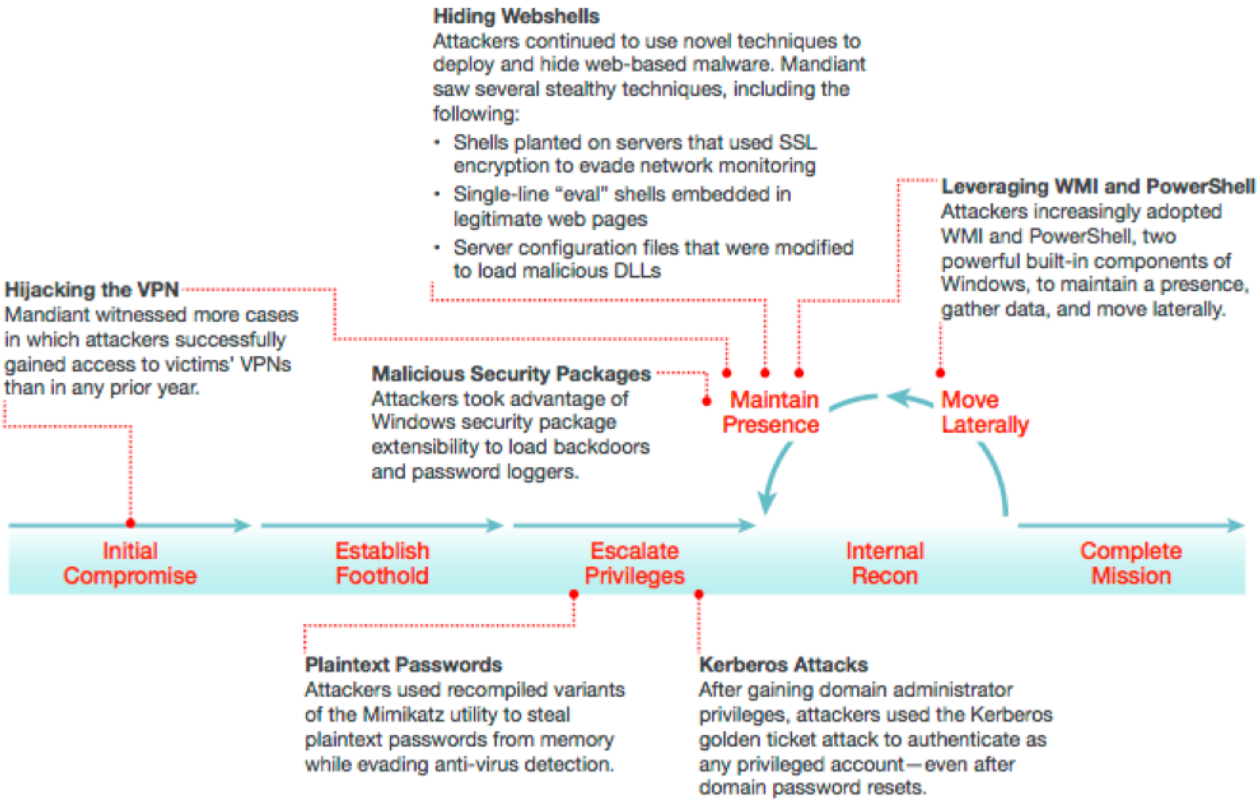
- Stealing of NTLM hashes and then performing a technique called “pass the hash”, which allows the malicious actor to successfully authenticate to other machines with these hashes.
- Stealing of plaintext passwords from the memory of the machine using tools like Mimikatz and using these passwords to authenticate to other machines.
- In this process, an intruder that has compromised a domain controller can generate a Kerberos ticket-granting ticket for any user. This golden ticket can be generated offline, remain valid for an indefinite lifespan, and be used to impersonate any account—even after a password reset.
- Utilizing open source keylogging tools to capture passwords
- Utilizing certificate capture tools like Mimikatz to harvest authentication certificates from compromised machines

3) Pivoting attacks to compromise other hosts
It varies on the motives of the malicious actor but most of the time, it is not the “patient zero” machine that was the goal. Instead, they are looking to use the information that was gathered in the previous steps to gain deeper access to your network, bypassing existing security controls and exfiltrating your data.

During this phase, the malicious actor will again utilize the built-in system or IT support tools to help them spread laterally. Here are a few example techniques used to do so:

- Using built-in system tools like Remote Desktop Protocol (RDP), AT, PsExec, VBScript and using open source tools like Metasploit. While these tools have been used a lot in the past for things like remote scheduling, exploiting, evasion or remote access and authentication, they tend to leave behind more forensic artifacts. As a result, we have seen a move to newer techniques.
- Some of the newer techniques that we have seen includes leveraging the built-in Windows tool PowerShell and WMI (Windows Management Instrumentation). Attackers can use PowerShell and WMI to connect to remote systems, modify the registry, access event logs, and even execute commands on remote machines.

As you can see, it is important to understand the techniques used by malicious actors to do internal reconnaissance, credential harvesting and pivoting attacks towards other machines inside your network.



Bottom line is a lot of the tools that malicious actors will utilize are tools that your IT support staff also uses or installs by default. Reducing business risk and improving security starts with controlling your internal environment and making people realize that security is everyone's problem.

What can you do to detect and contain the threat actors creeping around in the dark space of your network?

First, you need to be able to shine a light into that dark space and get visibility into what you are missing. Below are some recommendations that will help you do just that:

- Gathering Threat Intelligence about the tools, tactics and procedures of the malicious actors and their campaigns
- Have a threat analytics platform to identify and consolidate the information that will give your analyst the ability to do more proactive hunting for these types of techniques
- Proactively perform forensics and sweeping of endpoints for indicators of compromise
- Harden the devices that are on your network by removing any non-required applications or services and preforming proactive application and system configuration management and logging
- Implement tighter controls and proactive monitoring of credentials and applications, utilizing whitelisting and multifactor authentication methods.
- Perform data exfiltration identification and monitoring by utilizing full packet analysis and monitoring tools.

Armed with this information, you will hopefully be able to empower your IT staff to detect these types of actives, and see a little deeper into the dark spaces on your network where traditional tools fall short.

For more technical details of the different techniques covered please review the 2015 M-Trends report located*here*

Have questions? Let's talk.