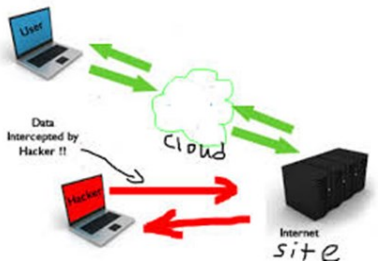
CYBER

common pattern of using legitimate tools to avoid detection.

Remote desktop
What better way to control a victim asset than full interactive GUI access, using a legitimate control channel that is built in to almost every version of Windows? Once attackers have valid credentials, terminal services, or RDP as it is commonly known, is the weapon of choice to gain interactive access to the assets. Since RDP sessions are encrypted, they're opaque to monitoring solutions (which in any case would not flag them as they are such a common legitimate administrative mechanism).

Central admin consoles
The modern attacker is lazy. Rather than spending time breaking into individual hosts, it's far less effort to break in to the system that controls them all in some way, and treat it as a mini legitimate botnet controller. ATM controllers, point-of-sales management systems, remote management tools like Ansible and Salt are all great targets as they give an attacker a "one shot, thousand kills" capability.

Network sniffing
While switched networks have made promiscuous mode sniffing less of an issue, attackers still gain tremendous value from setting up network sniffing on a high-traffic server to gain access to credentials of customers and other information. User segments are usually subjected to man-in the middle attacks like ARP spoofing, explained below.



ARP spoofing
It's been around for ages, but it's still used. Generating gratuitous fake ARP requests and replies can let attackers interject themselves in communications in switched networks in a classic man-in-the-middle attack. While these attacks have fallen out of favor somewhat, they're still not detected on many networks, and can be extremely damaging if an attacker finds the right hosts to poison.

Admin shares
While we've already spoken about file sharing, the built-in ADMIN$, C$ etc. shares deserve special mention, because they are used in practically every attack we have analyzed. The ADMIN$ share is the mainstay of PsExec style attacks, and gives complete access to the %SYSTEMROOT% folder. Meanwhile the per-partition hidden shares give complete read-write access to the entire hard drive of the remote system. What more would an attacker want? Once again, virtually undetectable as it has legit uses.

Token stealing
While a fairly recent technique in the public domain, stealing tokens from memory has become all the rage, and is used in almost every attack these days.

Tools such as ***Mimikatz*** and Windows Credential Editor can find service accounts in memory, create Kerberos tickets, and elevate an attacker from normal user to domain administrator in a few seconds.

Fully undetectable versions of these tools are easily available, while savvy hackers have implemented the functionality in PowerShell to avoid detection.

Port-scans
The simple port-scan is used to quickly identify services of interest — typically web applications, database servers and remote access functionality. While a full-blown port-scan is easily detected, "low and slow" scans get past practically any network monitoring system. Despite Nmap's plethora of features, attackers don't need to bother with bells and whistles like OS detection, or script scanning. Just simple TCP connects are sufficient for finding targets.

Pass-the-hash
Due to how the NTLM protocol works, attackers can use the encrypted hash of a password to authenticate to remote services without knowing what the plaintext password is.

After obtaining the password hashes, the attacker simply passes them on to other services, without having to undertake dictionary or brute-force attacks on the hash itself.

This technique has been superseded in many attacks by token stealing, but has still been used to devastating effect in recent breaches such as the Target Corporation attack.

Focus On...

Helping you bring your organization into focus.™

August 2019 • Volume 9, Issue 8

CYBER

Why Catching Lateral Movement Is Your Biggest Win

Wisdom states that 'prevention is better than cure'. Unfortunately, the attack surface of modern organizations is so large, that protection is akin to building a fence around a national border.

Our research shows that 80% of an attack is spent during lateral movement. The actual breach occurs fairly rapidly, and the final goal is quickly accomplished as well. It's moving from initial breach to the final goal that takes hackers time and resources. Even the savviest attacker is operating 'blind' once in the network. They may know where the assets are, but they have to move slowly and stealthily to get there. ***If you can catch them during this process, it's game over for the attacker.***

The Challenges

On average it takes months from initial compromise to a breach being discovered. Unfortunately, the volume of data is huge, and even the best predictive analytics solutions generate a huge number of false positives. This is because the volume and irrelevance of alerts leads security teams to disable or ignore these monitoring solutions.

Lateral Movement - Techniques, Tactics & Procedures

So how does an attacker move laterally on the network? The tools may change, but the basic strategy remains the same — Gain access to a lower protected, lower privileged asset, escalate privileges, and then start seeking out interesting targets on the network. After studying the specifics behind numerous breaches, these are some of the most common lateral movement techniques that we have observed.

File shares

Windows file shares is a backbone collaboration mechanism, file shares are used both on central file servers, as well as by individual users. They often contain customer databases, details of additional systems, operating procedures, and useful software. The built-in administrative shares for the hard-drive are also extremely useful to attackers with elevated privileges. ***These are legitimate traffic channels that go unpoliced by monitoring solutions.***

PowerShell

As sandboxing technology began catching malware without signatures, attackers moved to 'living off the land', or avoiding malware in their attacks and using built-in operating system capabilities to replicate malware functionality. The number one mechanism is PowerShell, Microsoft's object-oriented scripting facility is built-in to every modern version of Windows, and is extremely powerful — attackers have used it to steal in-memory credentials, modify system configuration and automate movement from one system to the next. ***Once again, it's legit, so it doesn't' get caught.***

PsExec

Own by Microsoft, PsExec and the entire Pstools suite lets administrators to remotely control Windows systems from the terminal. Attackers love PsExec for its ability to upload, execute and interact with an executable on a remote host. Since it works from a command line, it is easily scriptable, and doesn't alert the remote user to its operation. Since it's also a legitimate system administration tool, it is invariably not blacklisted or detected by antivirus solutions. You will observe this

Inside This Issue

Focus Audits will be closed on Monday, September 2, 2019 for the Labor Day Holiday.

FOCUS AUDITS™