Persistence

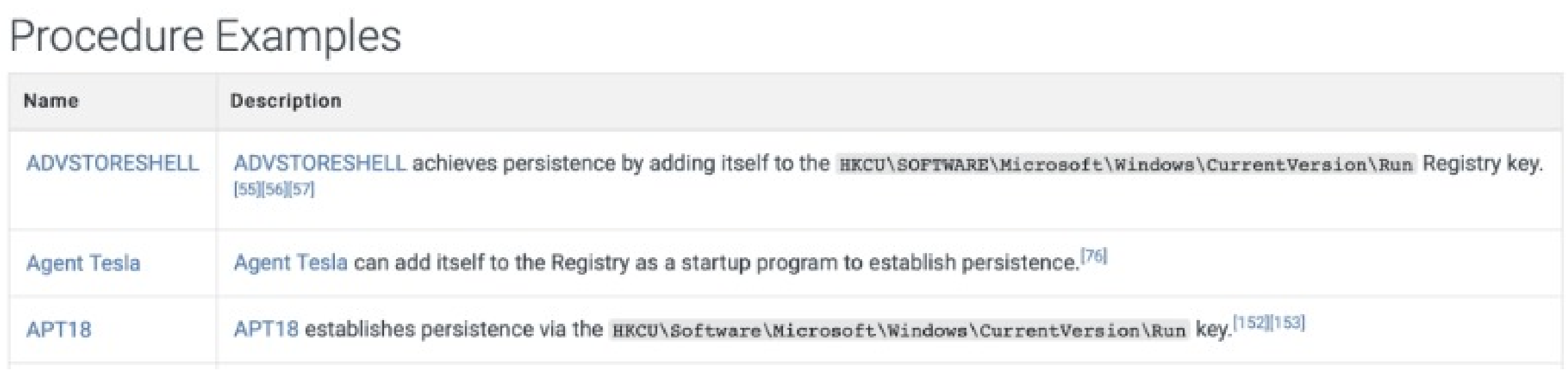
This lesson is going to cover the third stage in the MITRE ATT&CK framework, Persistence. Once an adversary has access to a system they need to attempt to maintain their foothold by hiding from the defenders and utilising multiple methods to regain access to the compromised host. At the time of writing there are currently 18 high-level techniques for this category. **We will be looking at the following:**

- Boot or Logon Autostart Execution
- External Remote Services

BOOT OR LOGON AUTOSTART EXECUTION

MITRE Technique T1547

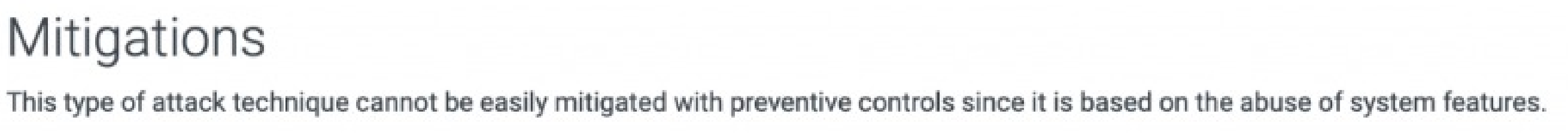
One way of adversaries achieving persistence is by adding a program to a start-up folder or referencing it with a registry run key. When an adversary, or anyone, adds an entry to the "run keys" this will cause the program referenced to be executed when any users logs into the host. Numerous advanced adversaries utilise this method of persistence when they have achieved initial access including APT18, 19 and 29.



Procedure Examples

Name	Description
ADVSTORESHELL	ADVSTORESHELL achieves persistence by adding itself to the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` Registry key.[55][56][57]
Agent Tesla	Agent Tesla can add itself to the Registry as a startup program to establish persistence.[76]
APT18	APT18 establishes persistence via the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` key.[152][153]

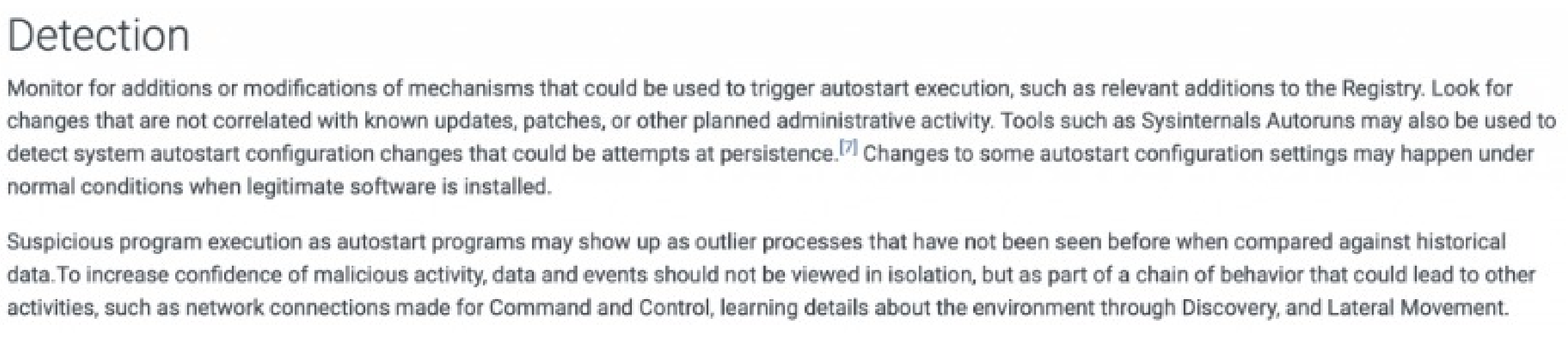
When considering Mitigation, MITRE states that this can be very hard to detect as legitimate programs will be assigned to be executed when the system is starting up.



Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

While it is hard to prevent completely, there are a lot of different ways we can detect the presence of malicious executable at system launch. Firstly we can audit the Windows Registry to identify if there are any suspicious entries. This can be quite a daunting task unless you are very familiar with the Registry and what should, and shouldn't, be in there. Sysinternals Autoruns is a tool that can help identify autostart configurations to uncover potentially malicious files that will be run every time a system is rebooted. Adversaries may use executables stored in run keys that are launched when the system starts as a solid persistence method, and these executables may actually initiate a connection back out to a command-and-control (C2) server. Monitoring this autorun's behaviour may actually aid an investigation.



Detection

Monitor for additions or modifications of mechanisms that could be used to trigger autostart execution, such as relevant additions to the Registry. Look for changes that are not correlated with known updates, patches, or other planned administrative activity. Tools such as Sysinternals Autoruns may also be used to detect system autostart configuration changes that could be attempts at persistence.[7] Changes to some autostart configuration settings may happen under normal conditions when legitimate software is installed.

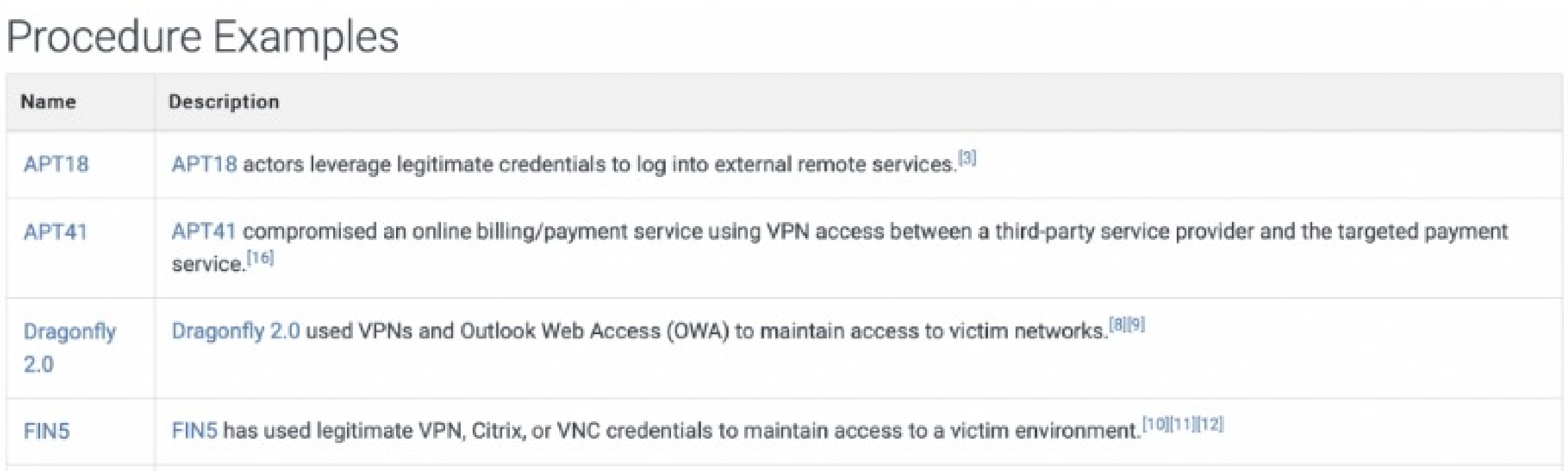
Suspicious program execution as autostart programs may show up as outlier processes that have not been seen before when compared against historical data.To increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

EXTERNAL REMOTE SERVICES

MITRE Technique T1133

If a system has internet-facing remote services such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) then if an attacker collects credentials belonging to valid accounts then they could ensure persistence by re-connecting to the compromised system using one of many remote services that may be present on the system. Alternatively if the organisation is utilising a VPN to allow remote workers to connect into a corporate network, an attacker could attempt to collect valid VPN credentials and then connect into the private network from anywhere. This is typically seen as a strong persistence method as provided the attacker isn't logging in at unusual hours, the traffic and logs generated from this activity will not look out of place, providing an element of stealth.

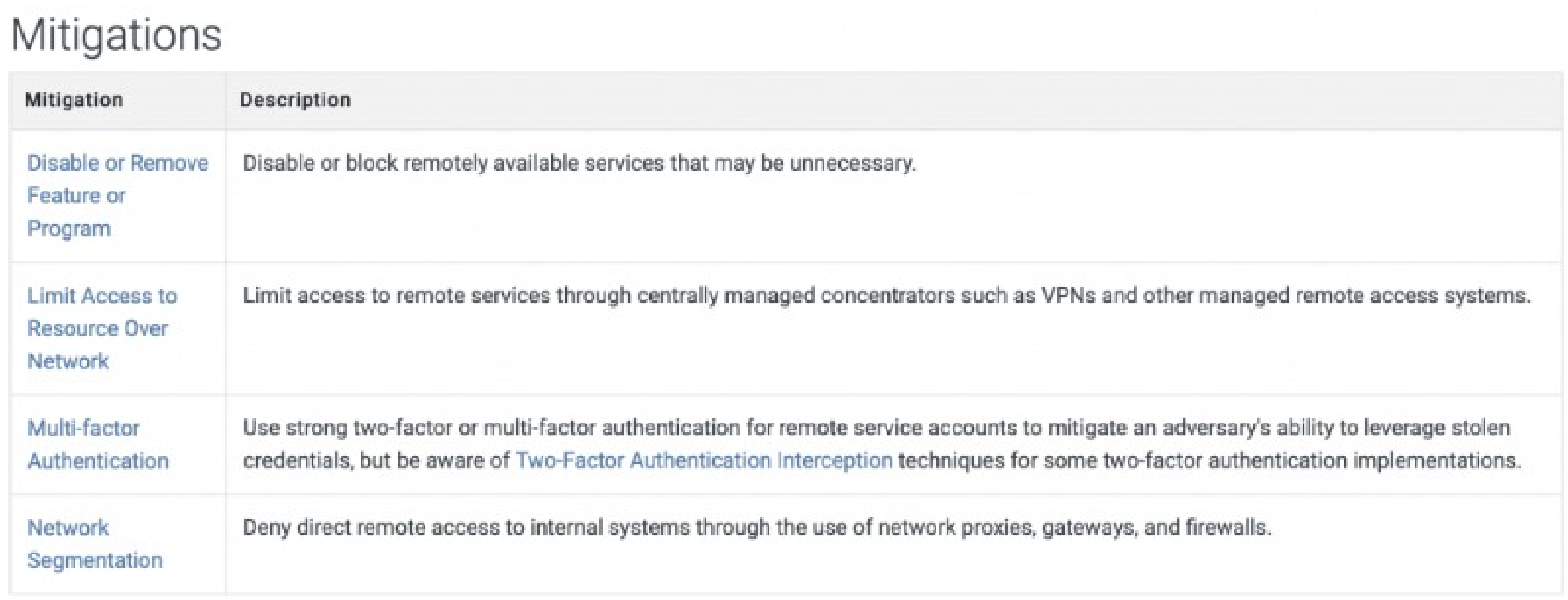
Looking at historic examples of adversaries using this technique we can see that APT18, APT41, Dragonfly 2.0 and FIN5 have all reused valid credentials to maintain access to a target network using remote services such as VPNs and Outlook Web Access.



Procedure Examples

Name	Description
APT18	APT18 actors leverage legitimate credentials to log into external remote services.[3]
APT41	APT41 compromised an online billing/payment service using VPN access between a third-party service provider and the targeted payment service.[16]
Dragonfly 2.0	Dragonfly 2.0 used VPNs and Outlook Web Access (OWA) to maintain access to victim networks.[8][9]
FIN5	FIN5 has used legitimate VPN, Citrix, or VNC credentials to maintain access to a victim environment.[10][11][12]

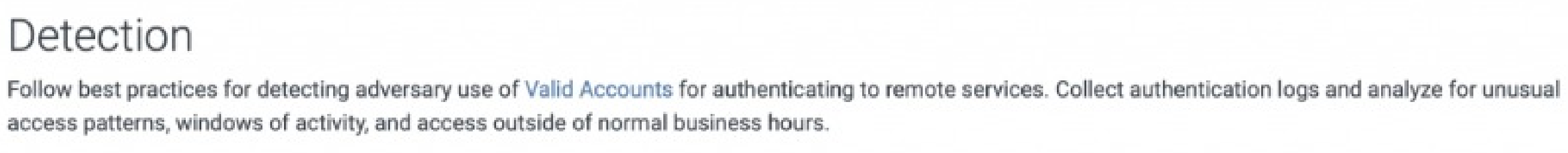
When it comes to mitigating persistence attempts using this technique we have a number of options. Firstly we can disable or block any remote services that are open to the internet. If a system doesn't need someone in a remote location to connect using RDP or SSH, these services should not be open or listening. Alternatively these services should only be listening for connection requests coming from inside of the network, vastly reducing the amount of systems that can try to connect via these methods (compared to the entire internet). Multi-factor authentication (MFA) should also be deployed where appropriate to prevent password spraying or password reuse and add another control that attackers would need to defeat. And finally, using VLANs and firewalls to properly segment a network and limit which systems can communicate with each other can be a very effective method at isolating an intruder.



Mitigations

Mitigation	Description
Disable or Remove Feature or Program	Disable or block remotely available services that may be unnecessary.
Limit Access to Resource Over Network	Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems.
Multi-factor Authentication	Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Two-Factor Authentication Interception techniques for some two-factor authentication implementations.
Network Segmentation	Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.

When it comes to detecting this activity we should be collecting logs regarding login attempts, successes, and failures. Rules should be created that look for activity outside of standard office hours which is more than likely malicious activity.



Detection

Follow best practices for detecting adversary use of Valid Accounts for authenticating to remote services. Collect authentication logs and analyze for unusual access patterns, windows of activity, and access outside of normal business hours.