Initial Access

This lesson is going to focus on the first stage in the MITRE ATT&CK framework, Initial Access (TA0001). These techniques are used to describe ways that adversaries could get their first foothold in a network, and at the time of writing there are currently 9 techniques:

- Drive-by Compromise
- Exploit public-facing application
- External remote services
- Hardware additions
- Phishing
- Replication through removable media
- Supply chain compromise
- Trusted relationship
- Valid accounts

Below we're going to take a deep dive on a few of these techniques, but feel free to click on the links above if you're interested in learning more about a technique that we don't cover here!

MITRE Technique T1566

By now you should already understand how important phishing is, and that it's the number one initial access method. We can see that this technique actually has three sub-techniques, which are shown below (well done MITRE!). These pages will include a description of the technique, mitigations, and how to improve detection.

Phishing

Sub-techniques (3)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

MITRE offers some great mitigations that we can use to reduce the risk from phishing emails, shown below (all of which we covered in the Phishing Analysis domain!)

Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.
Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
User Training	Users can be trained to identify social engineering techniques and phishing emails.

And at the bottom of the page we have some recommendations on how to better detect phishing activity within your environment.

Detection

Network intrusion detection systems and email gateways can be used to detect phishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

Because most common third-party services used for phishing via service leverage TLS encryption, SSL/TLS inspection is generally required to detect the initial communication/delivery. With SSL/TLS inspection intrusion detection signatures or other security gateway appliances may be able to detect malware.

Anti-virus can potentially detect malicious documents and files that are downloaded on the user's computer. Many possible detections of follow-on behavior may take place once User Execution occurs.

MITRE Technique T1133

External remote services can come in many forms, such as:

- **VPNs**
- **Remote Desktop Protocol** (RDP)
- **Secure Shell** (SSH)
- **Citrix**
- **amongst others**

For an adversary to use this tactic, it is highly likely that they will also use the Initial Access technique T1078 Valid Accounts, so they can log into these remote services (harvesting accounts from data breaches, phishing with credential harvesters, social engineering, and so on). An alternative is brute-forcing credentials to try and find a valid account, but this is extremely noisy and can easily be detected, and is therefore not typically used by advanced actors. Having access to valid accounts and remote services can also make for a good persistence mechanism, allowing the attacker to connect back to systems within the private network.

Looking at the Procedure Examples table for this technique we can see quite a few examples of actors and malware that have utilised this tactic historically. A small snippet of the table is shown below.

Procedure Examples

Name	Description
APT18	APT18 actors leverage legitimate credentials to log into external remote services.[18]
APT41	APT41 compromised an online billing/payment service using VPN access between a third-party service provider and the targeted payment services.[19]
Dragonfly 2.0	Dragonfly 2.0 used VPNs and Outlook Web Access (OWA) to maintain access to victim networks.[20][21]
FIN5	FIN5 has used legitimate VPN, Citrix, or VNC credentials to maintain access to a victim environment.[14][21][12]

MITRE offers some Mitigations that we can use to reduce the risk from Internet-facing remote services. Examples include disabling the service if it is not needed (this is very important!), and using two-factor authentication to prevent credential reuse attacks (where an attacker finds old credentials and tries them against other services in the hope that the user has used the same password in different places).

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.

And below that we have the Detection section which is short and sweet, and recommends monitoring usage of remote services and alerting on anomalous activity, such as an employee who works 9am – 5pm but is logging in to Remote Desktop Protocol at 3am.

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.

MITRE Technique T1091

Removable media is pretty self-explanatory, it's using devices such as USB pens or 'Rubber Duckies' to transport malware to a target system, provided we can get physical access (or we can convince someone with physical access to plug the device in!). This technique can be used to attack air-gapped systems which is when two networks are not connected, and therefore can't interact with each other.

Procedure Examples

Name	Description
Agent.btz	Agent.btz drops itself onto removable media devices and creates an autorun.inf file with an instruction to run that file. When the device is inserted into another system, it opens autorun.inf and loads the malware.[7]
APT28	APT28 uses a tool to infect connected USB devices and transmit itself to air-gapped computers when the infected USB device is inserted.[8]
CHOPSTICK	Part of APT28's operation involved using CHOPSTICK modules to copy itself to air-gapped machines and using files written to USB sticks to transfer data and command traffic.[9][10]
DarkHotel	DarkHotel's selective infector modifies executables stored on removable media as a method of spreading across computers.[11]
DustySky	DustySky searches for removable media and duplicates itself onto it.[12]

Below this we have the table for Mitigations to help protect the organization from this attack technique, and we have some pretty solid options, such as disabling AutoRun so that USB devices won't automatically run any files included on them, creating policies that state employees should simply not use USBs, and actually locking the system down so that it won't register USBs at all (we can also use USB port blockers which sit in the USB port and can't be removed without a special key).

Mitigations

Mitigation	Description
Disable or Remove Feature or Program	Disable Autorun if it is unnecessary.[7] Disallow or restrict removable media at an organizational policy level if it is not required for business operations.[8]
Limit Hardware Installation	Limit the use of USB devices and removable media within a network.

And finally we have a section on how we can detect activity related to removable media devices. Additionally to the below, we can actually monitor USB device usage using Windows Event logs, however this functionality is not enabled by default. If you want to read about how this can be done, check out this Tech Republic article.

Detection

Monitor file access on removable media. Detect processes that execute from removable media after it is mounted or when initiated by a user. If a remote access tool is used in this manner to move laterally, then additional actions are likely to occur after execution, such as opening network connections for Command and Control and system and network information Discovery.