Blue Team Level 1 Certification (Standard)

PHISHING ANALYSIS DOMAIN

✓ ~~PA1) Introduction to Emails and Phishing~~
7 Topics | 1 Quiz

✓ ~~PA2) Types of Phishing Emails~~
10 Topics | 2 Quizzes

✓ ~~PA3) Tactics and Techniques Used~~
12 Topics | 2 Quizzes

✓ ~~PA4) Investigating a Phishing Email~~
8 Topics | 2 Quizzes

✓ ~~PA5) Analysing URLs, Attachments, and Artifacts~~
8 Topics | 1 Quiz

○ PA6) Taking Defensive Actions
12 Topics | 1 Quiz

○ PA7) Report Writing
7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge
3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence
7 Topics

○ TI2) Threat Actors & APTs
6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence
7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns
6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics
5 Topics

○ DF2) Forensics Fundamentals
10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection
8 Topics | 1 Quiz

○ DF4) Windows Investigations
3 Topics | 3 Quizzes

○ DF5) Linux Investigations
4 Topics | 2 Quizzes

○ DF6) Volatility
3 Topics | 1 Quiz

○ DF7) Autopsy
4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM
7 Topics | 1 Quiz

○ SI2) Logging
6 Topics | 2 Quizzes

○ SI3) Aggregation
2 Topics | 1 Quiz

○ SI4) Correlation
6 Topics | 1 Quiz

○ SI5) Using Splunk
5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

Exfiltration

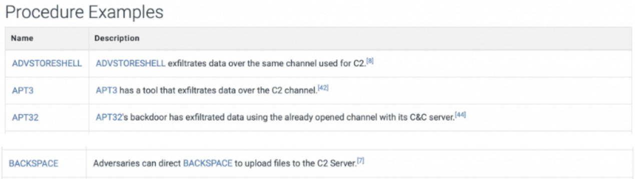
Blue Team Level 1 Certification (Standard) > IR6) MITRE ATT&CK > Exfiltration IN PROGRESS

At some point an adversary needs to fulfil their objectives, quite often this could be to steal valuable data. These actions are referred to as exfiltration and is the tenth phase within MITRE. The Exfiltration phase consists of techniques used to steal data from the compromised network and systems, and ways of avoiding detection when completing this. This can include the compression, encryption or encoding of files when removing them from the network and typically involves transferring it over a command-and-control communication channel. Exfiltration has 9 techniques at the time of writing. **We will be looking at the following:**

- Exfiltration Over C2 Channel
- Scheduled Transfer

MITRE Technique T1041

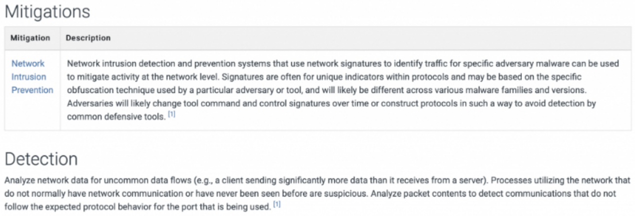
A previously explained adversaries may use existing command and control channels to exfiltrate data out of a network. Adversaries can extract data within beacons calling out to their C2 servers.



Procedure Examples

Name	Description
ADVSTORESHELL	ADVSTORESHELL exfiltrates data over the same channel used for C2.[8]
APT3	APT3 has a tool that exfiltrates data over the C2 channel.[42]
APT32	APT32's backdoor has exfiltrated data using the already opened channel with its C&C server.[44]
BACKSPACE	Adversaries can direct BACKSPACE to upload files to the C2 Server.[7]

A key way of checking for the exfiltration of files is to look for clients sending a significant amount of data out to a server. A NIDS (Network Intrusion Detection System) can also be utilised as rules can be created to alert on the 'magic bytes' of files. A rule can essentially be created to alert anytime a Microsoft Word file is seen been transferred over the network. Another method of detection is the initial detection of the C2 server itself, beacons will quite often call out to the external IP address at regular intervals with a slight "jitter" set by the adversary. Frequency analysis can be a common method of detecting this.



Mitigations

Mitigation	Description
Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. [1]

Detection

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. [1]

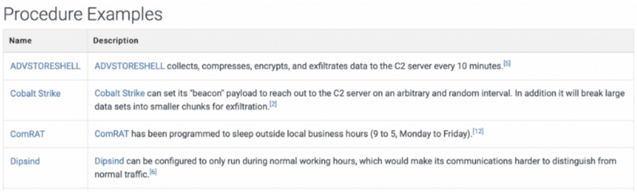
MITRE Technique T1029

Adversaries may schedule data exfiltration to occur only at specific times in an attempt to evade Network Intrusion Detection and Prevention Systems (NIDS/NIPS) or security analysts and ensure that they can exfiltrate as much data as possible before being discovered.

The ADVSTORESHELL malware will collect data, compress it, encrypt it, and upload it to the command-and-control server every 10 minutes. While this may be fairly easy to detect due to the short timeframe between uploads, this will ensure that a lot of data can be retrieved from the system quickly. Cobalt Strike, the popular offensive security

○ IR1) Introduction to Incident Response
● 8 Topics | 1 Quiz
○ IR2) Preparation Phase
● 10 Topics | 2 Quizzes
○ IR3) Detection and Analysis Phase
● 7 Topics | 4 Quizzes
○ IR4) Containment, Eradication, and Recovery Phase
● 5 Topics | 1 Quiz
○ IR5) Lessons Learned and Reporting
● 7 Topics
○ IR6) MITRE ATT&CK
● 13 Topics | 2 Quizzes
○ Section Introduction, ATT&CK
○ Initial Access
○ Execution
○ Persistence
○ Privilege Escalation
○ Defense Evasion
○ Credential Access
○ Discovery
○ Lateral Movement
○ Collection
○ Command and Control
○ Exfiltration
○ Impact
Activity) ATT&CK Navigator
Activity) End of Section Review, ATT&CK
BTL1 EXAM
○ Exam Preparation
○ Using RDP and SSH
○ How to Start Your Exam

platform can set the beacon payload (code that attempts to connect to the C2 server) to use a random interval to make it harder to spot. This tool can also break large files into smaller chunks to allow for more subtle transfer out of the network. Then both ComRAT and Dipsind can be set to only operate during standard business hours (9-5) to help it blend in with normal traffic.

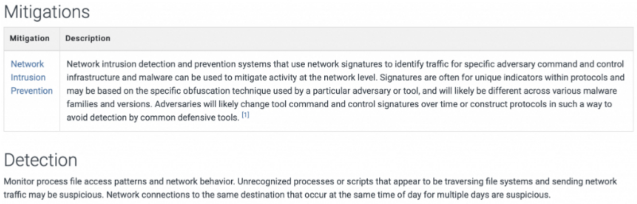


Procedure Examples

Name	Description
ADVSTORESHELL	ADVSTORESHELL collects, compresses, encrypts, and exfiltrates data to the C2 server every 10 minutes.[5]
Cobalt Strike	Cobalt Strike can set its "beacon" payload to reach out to the C2 server on an arbitrary and random interval. In addition it will break large data sets into smaller chunks for exfiltration.[2]
ComRAT	ComRAT has been programmed to sleep outside local business hours (9 to 5, Monday to Friday).[12]
Dipsind	Dipsind can be configured to only run during normal working hours, which would make its communications harder to distinguish from normal traffic.[6]

A pretty essential mitigation is suggested, which is the use of NIDS/NIPS tools such as Snort and Bro/Zeek to detect, alert, and respond to suspicious or malicious activity over the network.

To detect this technique we should monitor for unusual processes that are accessing files and making network connections, as this could represent an adversary exfiltration data. Looking for network connections with large packets could assist with file upload detection.



Mitigations

Mitigation	Description
Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. [1]

Detection

Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious. Network connections to the same destination that occur at the same time of day for multiple days are suspicious.

< Previous Topic   Mark Complete ✓   Next Topic >
Back to Lesson