Blue Team Level 1 Certification (Standard)
Introduction to BTL1
~~Welcome to Blue Team Level 1!~~
4 Topics
~~Lab and Forum Access~~
SECURITY FUNDAMENTALS DOMAIN
~~Introduction to Security Fundamentals~~
1 Topic
~~Soft Skills~~
7 Topics
~~Security Controls~~
5 Topics | 1 Quiz
~~Networking 101~~
6 Topics | 1 Quiz
~~Management Principles~~
4 Topics | 1 Quiz
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

Collection

This lesson is going to cover the ninth stage in the MITRE ATT&CK framework, Collection. These techniques are used to describe ways that adversaries will identify important files or information, collect them, and prepare them for data exfiltration. At the time of writing currently includes 16 top-level techniques. **We will be looking at the following:**

- Email Collection
- Audio Capture
- Screen Capture
- Data From Local System

MITRE Technique T1114

Collecting emails from a target system seems like a great idea – these emails could give an insight into business operations, provide a list of valid internal email addresses for future spear phishing attacks or sell them for money on underground markets, collect email attachments that could include sensitive data, and much more. When considering email collection there's three sub-technique that we need to consider:

Sub-techniques (3)

ID	Name
T1114.001	Local Email Collection
T1114.002	Remote Email Collection
T1114.003	Email Forwarding Rule

- Local Email Collection – Attackers may target emails on the local system to identify and collect sensitive information. Files containing email data can be acquired from a user's local system such as Outlook storage or cache files typically stored in `C:\Users\<username>\Documents\Outlook Files` or `C:\Users\<username>\AppData\Local\Microsoft\Outlook`.
- Remote Email Collection – Attackers may specifically target and pivot to an Exchange server or Office 365 to collect sensitive information. Using valid credentials the actor can interact directly with the Exchange server to poll information from within a network. The attack doesn't always have to occur from within a network, as internet facing Exchange services or Office 365 can be accessed to read, send, save and delete emails.
- Email Forwarding Rule – Adversaries may setup email forwarding rules to collect sensitive information. Any emails that are sent to a user will be silently auto-forwarded to an attacker-owned email address presenting a data leak that will continue to give the adversary access to email messages even if they have lost access to the network. This could result in sensitive data exposure which could also be used for social engineering and spear phishing attacks in the future.

Using multi-factor authentication (MFA) can prevent access to an account where a malicious actor has discovered the valid username and password combination. Although there are ways MFA can be bypassed it adds more work for the adversary and gives us more time to catch them. We could also consider encrypting our emails or sensitive documents and only share the decryption key with trusted parties via alternative communication methods. And finally enterprise-grade email solutions could have functionality to audit auto-forwarding rules to see if any have been created to send mail to non-domain mailboxes and generate an alert or report for further investigation.

Mitigations

Mitigation	Description
Audit	Enterprise email solutions have monitoring mechanisms that may include the ability to audit auto-forwarding rules on a regular basis. In an Exchange environment, Administrators can use Get-InboxRule to discover and remove potentially malicious auto-forwarding rules.[1]
Encrypt Sensitive Information	Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.
Multi-factor Authentication	Use of multi-factor authentication for public-facing webmail servers is a recommended best practice to minimize the usefulness of usernames and passwords to adversaries.

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
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

In regard to detecting this activity we have a number of options the we can choose from. Unusual processes accessing an email server or application could suggest an adversary is attempt to connect, or a user that works from 9 AM to 5 PM logging in at 1:30 AM on a Saturday and opening their email application is very unusual and is potentially a sign of malicious activity. Also monitor for unusual PowerShell, WMI, and CMD commands being executed from a user's account.

Detection

There are likely a variety of ways an adversary could collect email from a target, each with a different mechanism for detection.

File access of local system email files for Exfiltration, unusual processes connecting to an email server within a network, or unusual access patterns or authentication attempts on a public-facing webmail server may all be indicators of malicious activity.

Monitor processes and command-line arguments for actions that could be taken to gather local email files. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Detection is challenging because all messages forwarded because of an auto-forwarding rule have the same presentation as a manually forwarded message. It is also possible for the user to not be aware of the addition of such an auto-forwarding rule and not suspect that their account has been compromised; email-forwarding rules alone will not affect the normal usage patterns or operations of the email account.

MITRE Technique T1123

An attacker can utilise peripheral devices such as plugged-in microphones, headsets or webcams to collect audio from users that are interacting with the system. Recording of system audio can also result in the ability to capture conversations via Voice-over IP (VOIP) applications such as Skype, Webex, and Teams.

APT37 has been documented using audio capture software known as SOUNDWAVE to record microphone input from an infected system. The Bandook malware has modules that can allow the software to capture audio, the same with Cobian RAT, Attor, and Cadelspy.

Procedure Examples

Name	Description
APT37	APT37 has used an audio capturing utility known as SOUNDWAVE that captures microphone input.[33]
Attor	Attor's has a plugin that is capable of recording audio using available input sound devices.[30]
Bandook	Bandook has modules that are capable of capturing audio.[24]
Cadelspy	Cadelspy has the ability to record audio from the compromised host.[31]
Cobian RAT	Cobian RAT has a feature to perform voice recording on the victim's machine.[19]

It is not possible to complete mitigate this technique because using system audio is practically a necessity. Focusing on detection we can monitor API calls that are related to audio capture, but this would generate a high volume of false positives because it could be legitimate activity. Process monitoring should be conducted to identify any unusual processes are attempting to access the microphone on a system along with file creation that is likely audio-related.

Mitigations

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

Detection

Detection of this technique may be difficult due to the various APIs that may be used. Telemetry data regarding API use may not be useful depending on how a system is normally used, but may provide context to other potentially malicious activity occurring on a system.

Behavior that could indicate technique use include an unknown or unusual process accessing APIs associated with devices or software that interact with the microphone, recording devices, or recording software, and a process periodically writing files to disk that contain audio data.

MITRE Technique T1133

Taking screen captures from the system can help to gather information over a long period of time, and this technique will typically be deployed soon after a system has been compromised, giving it a good chance of collecting valuable information or build up a profile of the user's day-to-day habits. Taking a screenshot can also be achieved through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture` (but this isn't standard behaviour, so we can monitor on these commands!).

The first entry in the Procedure Examples table for this technique is the famous Agent Tesla remote access trojan (RAT). This tool has the ability to take screenshots at regular intervals which could disclose information from open documents or web browsing activity. APT28 and APT39 have been known to collect screenshots during their cyber operations as an information collection technique. Aria-body, a malicious program, also has the ability to capture screenshots.

Procedure Examples

Name	Description
Agent Tesla	Agent Tesla can capture screenshots of the victim's desktop.[67][68][69][70][71]
APT28	APT28 has used tools to take screenshots from victims.[111][27][53]
APT39	APT39 has used a screen capture utility to take screenshots on a compromised host.[121]
Aria-body	Aria-body has the ability to capture screenshots on compromised hosts.[107]

Mitigating these actions isn't feasible as it can be used for legitimate purposes, and instead we should focus on detection. We can monitor for unusual API calls that are related with taking screenshots, but this could still generate a large number of false positives. We should find ways to link this with other activity to reduce the number of false positives and build a stronger detection capability.

Mitigations

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

Detection

Monitoring for screen capture behavior will depend on the method used to obtain data from the operating system and write output files. Detection methods could include collecting information from unusual processes using API calls used to obtain image data, and monitoring for image files written to disk. The sensor data may need to be correlated with other events to identify malicious activity, depending on the legitimacy of this behavior within a given network environment.

MITRE Technique T1005

Attackers may search through any attached local or networked drives to find files of interest and sensitive data prior to Exfiltration. This can be anything from local databases to coding projects, sensitive documents to user's files. Identifying such files can be achieved by using an interpreter such as the CMD on Windows systems, making use of commands such as **`find`**, **`tree`**, **`locate`**, and **`dir`**. Alternatively attackers can make use of tools that can perform Automated Collection on the local system.

The Procedure Examples table for this technique has a lot of generic entries because almost every threat actor is going to want to identify and exfiltrate interesting files from a compromised system. We can see that APT28 has previously exfiltrated internal documents from systems under their control and using Forfiles to prepare files for exfiltration. GravityRAT (remote access trojan) is known to steal files with specific file extensions which are typically widely used within businesses and enterprises. The same goes for Inception which looks for files with specific extensions and sends them back to the attacker.

Procedure Examples

Name	Description
APT1	APT1 has collected files from a local victim.[51]
APT28	APT28 has retrieved internal documents from machines inside victim environments, including by using Forfiles to stage documents before.[5][59]
APT3	APT3 will identify Microsoft Office documents on the victim's computer.[50]
GravityRAT	GravityRAT steals files with the following extensions: .docx, .doc, .pptx, .ppt, .xlsx, .xls, .rtf, and .pdf.[18]
Inception	Inception used a file hunting plugin to collect .txt, .pdf, .xls or .doc files from the infected host.[67]

It's hard to differentiate between legitimate and malicious activity because it won't immediately look any different than expected user activity accessing and changing user-generated files on their systems. To detect this activity we should monitor for excessive usage of commands in CMD and PowerShell that may represent a malicious actor preparing files for exfiltration.

Mitigations

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

Detection

Monitor processes and command-line arguments for actions that could be taken to collect files from a system. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Previous Topic
Mark Complete
Next Topic
Back to Lesson