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

Impact

This lesson is going to cover the fourth stage in the MITRE ATT&CK framework, Impact. These techniques are used to describe the actions that adversaries may use to disrupt availability or compromise integrity by manipulating business and operational processes, such as tampering or destroying data. At the time of writing currently includes 13 top-level techniques. **We will be looking at the following:**

- Account Access Removal
- Defacement (2 sub-techniques)
- Data Encrypted For Impact

MITRE Technique T1531

Adversaries may want to prevent access to accounts as an anti-forensic technique or simply to disrupt business operations. This can be achieved by completing any of the following:

- **Deleting Accounts**
- **Locking Accounts**
- **Changing Passwords**

From an adversaries perspective these actions are extremely noisy and Windows has a number of logs that would alert the security team to this activity, so it would likely occur once the attacker has finished all intended objectives.

Under the Procedure Examples heading we have one entry for this technique, where it was used by LockerGoga, a ransomware strain. As well as encrypting files, it also changed account passwords and logged them out so recovery of systems was even harder.

Procedure Examples

Name	Description
LockerGoga	LockerGoga has been observed changing account passwords and logging off current users.[1][2]

For this technique the Mitigation section is extremely short because this technique is a legitimate system functionality that is being abused, and therefore there is no real way to prevent this. Administrative controls should be in place to limit the number of user accounts that have administrator or domain administrator account access and can modify or delete user accounts.

Mitigations

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

MITRE offers some incredible advice for detecting this technique, and even kindly provides us with the Windows event IDs that we need to monitor. We actually covered these events in an activity within IR3) Detection and Analysis! As mentioned below, especially in larger environments, users will become locked out for legitimate reasons, such as simply forgetting their password after changing it. Events for changing or reseting a password can also legitimately be created by non-malicious users, so other methods should be considered when writing detection rules, such as event volume (1-5 login failures is likely legitimate, over 9000 is not) and comparing to a baseline of 'standard' activity.

Detection

Use process monitoring to monitor the execution and command line parameters of binaries involved in deleting accounts or changing passwords, such as use of Net. Windows event logs may also designate activity associated with an adversary's attempt to remove access to an account:

- Event ID 4723 - An attempt was made to change an account's password
- Event ID 4724 - An attempt was made to reset an account's password
- Event ID 4726 - A user account was deleted
- Event ID 4740 - A user account was locked out

Alerting on Net and these Event IDs may generate a high degree of false positives, so compare against baseline knowledge for how systems are typically used and correlate modification events with other indications of malicious activity where possible.

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

MITRE Technique T1491

Adversaries may modify content available internally or externally to an enterprise network, such as editing desktop wallpapers to include an offensive image or ransom message, or modifying a company's primary website reducing legitimate operation to show a public message. But why would anyone do this? It's incredibly noisy, and if the defenders haven't identified the malicious actor by this point, they definitely know something is wrong now. Reasons for conducting defacement actions include:

- **Delivering messaging,** typically associated with hacktivists promoting socially or politically-motivated messages
- **Intimidation,** to assist with blackmail attempts towards the compromised organisation,
- **Claiming credit for an intrusion,** potentially for socially-motivated reasons such as showing off to friends or demonstrating technical capability to the organisation and others

This technique is split into two sub-techniques, internal and external.

Sub-techniques (2)

ID	Name
T1491.001	Internal Defacement
T1491.002	External Defacement

- Internal Defacement –
- External Defacement –

Arguably the easiest and most effective methods to combat internal and external defacement is to revert to the latest backup that doesn't show any malicious modification. This is easer said than done, as efforts need to be made to protect the backups themselves too as adversaries may target these to prevent recovery. The time between the latest backup being taken and recovery being applied will result in a period of lost data, so frequent backups are essential to reduce the impact of restoration.

Mitigations

Mitigation	Description
Data Backup	Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.[1] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

MITRE suggests that organisations monitor for changes to their website, protect the web server with a web application firewall (WAF), and filter and drop malicious traffic associated with remote-to-local (R2L) attacks including SQL inception, cross-site scripting, and others. If an attacker is able to access a web server from within the network then they may be able to circumvent the WAF by connecting directly to the system using remote tools such as Remote Desktop Protocol or Secure Shell, so file changes on the server should be monitored for unexpected changes.

Detection

Monitor internal and external websites for unplanned content changes. Monitor application logs for abnormal behavior that may indicate attempted or successful exploitation. Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection. Web Application Firewalls may detect improper inputs attempting exploitation.

MITRE Technique T1486

Data encryption. What comes to mind straight away? **Ransomware.** Adversaries can work to encrypt files and data and withholding the decryption key so that there is no way of reversing the encryption. This is typically deployed to try and receive a ransom payment, at which point the adversary may or may not provide the decryption key. If the actor isn't trying to extort money and simply wants to trash a system they can work to encrypt critical system files or the Master Boot Record to cripple system functionality. Because ransomware or encryption action will only affect the local system the adversary needs to identify ways for it to spread, such as utilising wormable vulnerabilities (WannaCry used a flaw in SMB, a file sharing protocol, that allowed it to spread rapidly) or access to valid accounts.

The Procedure Examples table has a ton of interesting entries, including some high-profile ransomware strains such as Ryuk, Shamoon, and WannaCry. We can see that they all sound similar, but if you take a deeper dive by clicking on the ransomware names you'll find out the cool details that separate them (go on, take a look!)

Ryuk	Ryuk has used a combination of symmetric (AES) and asymmetric (RSA) encryption to encrypt files. Files have been encrypted with their own AES key and given a file extension of .RYK. Encrypted directories have had a ransom note of RyukReadMe.txt written to the directory.[19]
SamSam	SamSam encrypts victim files using RSA-2048 encryption and demands a ransom be paid in Bitcoin to decrypt those files.[11]
Shamoon	Shamoon has an operational mode for encrypting data instead of overwriting it.[6][7]
SynAck	SynAck encrypts the victims machine followed by asking the victim to pay a ransom. [16]
TA505	TA505 has used a wide variety of ransomware, such as Locky, Jaff, Bart, Philadelphia, and GlobeImposter, to encrypt victim files and demand a ransom payment.[20]
WannaCry	WannaCry encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files.[8][21][9]
Xbash	Xbash has maliciously encrypted victim's database systems and demanded a cryptocurrency ransom be paid.[15]

For the Mitigations table we're presented with the sample suggestion as Defacement, reminding organisations to keep regular backups and ensure that they are appropriately protected to prevent tampering or destruction.

Mitigations

Mitigation	Description
Data Backup	Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.[3] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

For Detection the suggestions include monitor specific command-line usages such as vssadmin, wbadmin, bcdedit, all of which can be used to encrypt data. We can also monitor for a large number of file modifications within a short timeframe which could be evidence of ransomware actively encrypting files.

Detection

Use process monitoring to monitor the execution and command line parameters of of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit. Monitor for the creation of suspicious files as well as unusual file modification activity. In particular, look for large quantities of file modifications in user directories.

In some cases, monitoring for unusual kernel driver installation activity can aid in detection.

Previous Topic

Mark Complete

Back to Lesson