# Must Have SOC Analysts customized cookbook

Leverage automation and threat intel data analysis for prioritizing detection

*Report customized for health sector*

This report aims at providing  statical analysis of TTPs (Tactics, Techniques and Procedures) used by threat actors targetting health sector in order to help SOC in operationalizing their mission.

While contextualising, gathering and analysing available data for a given sector, the overall objective is to introduce a different threat perspective for SOC teams - a perspective based on all known (and shared) threat actor behaviours. The main idea is to provide to SOC team a dedicated baseline to operationalize their efficiency in their daily job from collections to remediations.

The 1st chapter enumerates the threat actors based on MITRE data sources.
The 2nd chapter gives statistics about TTPs and data sources to collect in order to maximise detection capability (beware of bias).
The 3rd and last chapter gives detailed information on how to detect the most used techniques.
This report is AUTOMATICALLY generated based on MITRE ATT&CK and OSSEM data.

MITRE ATT&CK (https://attack.mitre.org) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world - by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

The OSSEM (Open Source Security Events Metadata / https://github.com/OTRF/OSSEM) is a community-led project that focuses primarily on the documentation and standardization of security event logs from diverse data sources and operating systems. Security events are documented in a dictionary format and can be used as a reference while mapping data sources to data analytics used to validate the detection of adversarial techniques. In addition, the project provides a common data model (CDM) that can be used for data engineers during data normalization procedures to allow security analysts to query and analyze data across diverse data sources. Finally, the project also provides documentation about the structure and relationships identified in specific data sources to facilitate the development of data analytics.

This is a beta version (work still in progress).
Good enough for now.
May this work be of help for you.

Feedbacks, contributions and enrichments are welcome :)
Thomas Billaut <thomas.billaut@protonmail.com>
https://github.com/tbillaut

# 1. Threat Groups

This chapter aims at giving the list of threat groups targetting the health sector.
Data are extracted from MITRE ATT&CK.
Information and citation links can be retrieved from MITRE ATTACK website (https://attack.mitre.org/groups).

## 1.1 Tonto Team

Alias : Tonto Team, Earth Akhlut, BRONZE HUNTLEY, CactusPete, Karma Panda

Tonto Team (https://attack.mitre.org/groups/G0131) is a suspected Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020 they expanded operations to include other Asian as well as Eastern European countries. Tonto Team (https://attack.mitre.org/groups/G0131) has targeted government, military, energy, mining, financial, education, healthcare, and technology organizations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).
Citation: Kaspersky CactusPete Aug 2020
Citation: ESET Exchange Mar 2021
Citation: FireEye Chinese Espionage October 2019
Citation: ARS Technica China Hack SK April 2017
Citation: Trend Micro HeartBeat Campaign January 2013
Citation: Talos Bisonal 10 Years March 2020

## 1.2 Fox Kitten

Alias : Fox Kitten, UNC757, PIONEER KITTEN, Parisite

Fox Kitten (https://attack.mitre.org/groups/G0117) is threat actor with a suspected nexus to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America. Fox Kitten (https://attack.mitre.org/groups/G0117) has targeted multiple industrial verticals including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering.
Citation: ClearkSky Fox Kitten February 2020
Citation: CrowdStrike PIONEER KITTEN August 2020
Citation: Dragos PARISITE
Citation: ClearSky Pay2Kitten December 2020

## 1.3 Operation Wocao

Alias : Operation Wocao

Operation Wocao (https://attack.mitre.org/groups/G0116) described activities carried out by a China-based cyber espionage adversary. Operation Wocao (https://attack.mitre.org/groups/G0116) targeted entities within the government, managed service providers, energy, health care, and technology sectors across several countries, including China, France, Germany, the United Kingdom, and the United States. Operation Wocao (https://attack.mitre.org/groups/G0116) used similar TTPs and tools to APT20, suggesting a possible overlap.
Citation: FoxIT Wocao December 2019

## 1.4 Whitefly

Alias : Whitefly

Whitefly (https://attack.mitre.org/groups/G0107) is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large

amounts of sensitive information. The group has been linked to an attack against Singapore's largest public health organization, SingHealth.
Citation: Symantec Whitefly March 2019

## 1.5 APT41

Alias : APT41, WICKED PANDA

APT41 (https://attack.mitre.org/groups/G0096) is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 (https://attack.mitre.org/groups/G0096) has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 (https://attack.mitre.org/groups/G0096) overlaps at least partially with public reporting on groups including BARIUM and Winnti Group (https://attack.mitre.org/groups/G0044).
Citation: FireEye APT41 Aug 2019
Citation: Group IB APT 41 June 2021

## 1.6 FIN4

Alias : FIN4

FIN4 (https://attack.mitre.org/groups/G0085) is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013.
Citation: FireEye Hacking FIN4 Dec 2014
Citation: FireEye FIN4 Stealing Insider NOV 2014

FIN4 (https://attack.mitre.org/groups/G0085) is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.
Citation: FireEye Hacking FIN4 Dec 2014
Citation: FireEye Hacking FIN4 Video Dec 2014

## 1.7 Tropic Trooper

Alias : Tropic Trooper, Pirate Panda, KeyBoy

Tropic Trooper (https://attack.mitre.org/groups/G0081) is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper (https://attack.mitre.org/groups/G0081) focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.
Citation: TrendMicro Tropic Trooper Mar 2018
Citation: Unit 42 Tropic Trooper Nov 2016
Citation: TrendMicro Tropic Trooper May 2020

## 1.8 Orangeworm

Alias : Orangeworm

Orangeworm (https://attack.mitre.org/groups/G0071) is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.
Citation: Symantec Orangeworm April 2018

## 1.9 Leviathan

Alias : Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope

Leviathan (https://attack.mitre.org/groups/G0065) is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company.
Citation: CISA AA21-200A APT40 July 2021

Active since at least 2009, Leviathan (https://attack.mitre.org/groups/G0065) has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across the US, Canada, Europe, the Middle East, and Southeast Asia.
Citation: CISA AA21-200A APT40 July 2021
Citation: Proofpoint Leviathan Oct 2017
Citation: FireEye Periscope March 2018

## 1.10 menuPass

Alias : menuPass, Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH

menuPass (https://attack.mitre.org/groups/G0045) is a threat group that has been active since at least 2006. Individual members of menuPass (https://attack.mitre.org/groups/G0045) are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.
Citation: DOJ APT10 Dec 2018
Citation: District Court of NY APT10 Indictment December 2018

menuPass (https://attack.mitre.org/groups/G0045) has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.
Citation: Palo Alto menuPass Feb 2017
Citation: Crowdstrike CrowdCast Oct 2013
Citation: FireEye Poison Ivy
Citation: PWC Cloud Hopper April 2017
Citation: FireEye APT10 April 2017
Citation: DOJ APT10 Dec 2018
Citation: District Court of NY APT10 Indictment December 2018

## 1.11 Deep Panda

Alias : Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine

Deep Panda (https://attack.mitre.org/groups/G0009) is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications.
Citation: Alperovitch 2014

The intrusion into healthcare company Anthem has been attributed to Deep Panda (https://attack.mitre.org/groups/G0009).
Citation: ThreatConnect Anthem

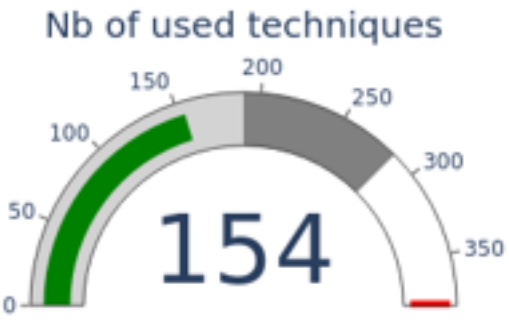
This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther.
Citation: RSA Shell Crew

Deep Panda (https://attack.mitre.org/groups/G0009) also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion.
Citation: Symantec Black Vine

Some analysts track Deep Panda (https://attack.mitre.org/groups/G0009) and APT19 (https://attack.mitre.org/groups/G0073) as the same group, but it is unclear from open source information if the groups are the same.
Citation: ICIT China's Espionage Jul 2016

# 2. What TTPs to prioritize for detection ?

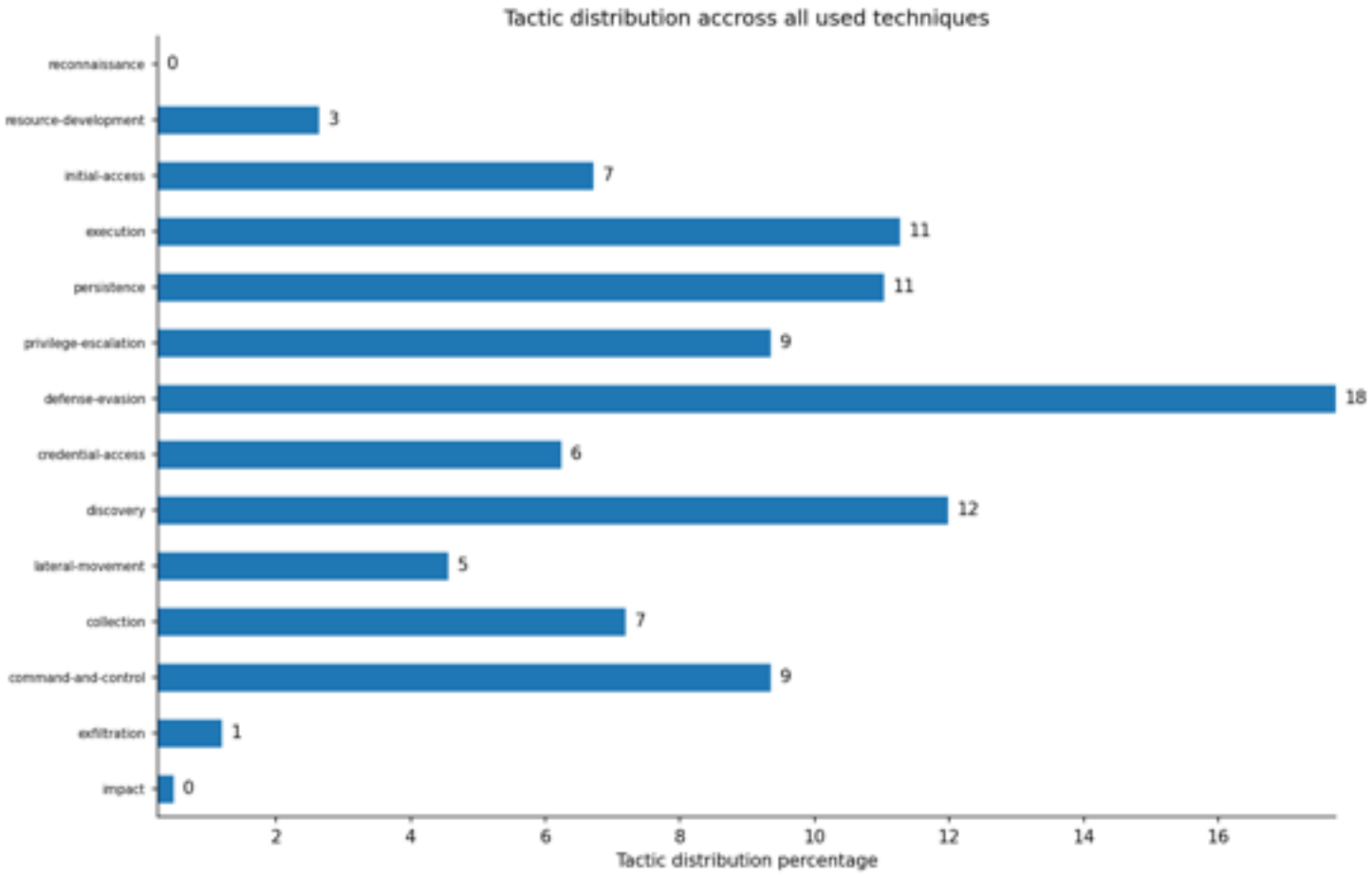
This chapter aims at providing some statistics about tactics and techniques used by the previous threat actors. While understanding most used and share techniques, SOC analysts should be able to focus on most used tactics and techniques. And possibly adopt a new perspective of the priority.



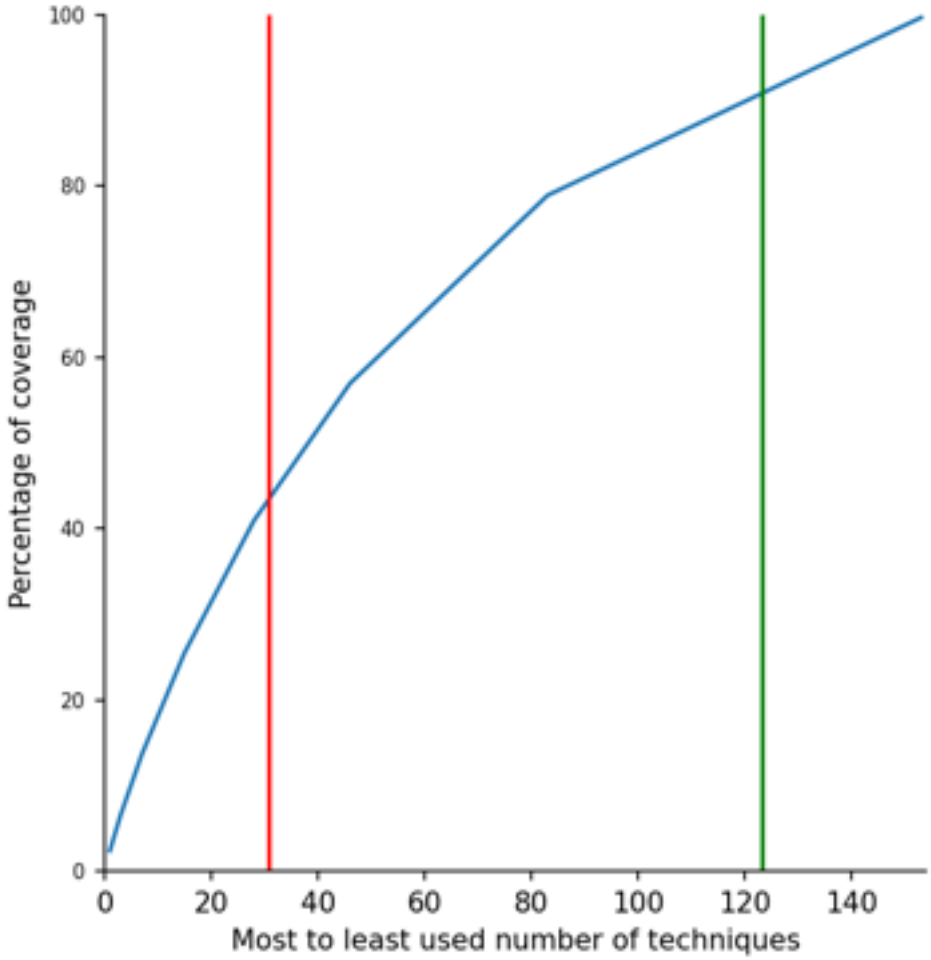
## 2.1 Tactics distribution

The following chart gives the tactics distribution of all used techniques used by the threat actors.
This representation may offer a new perpective for SOC teams concerning detection capabilities.



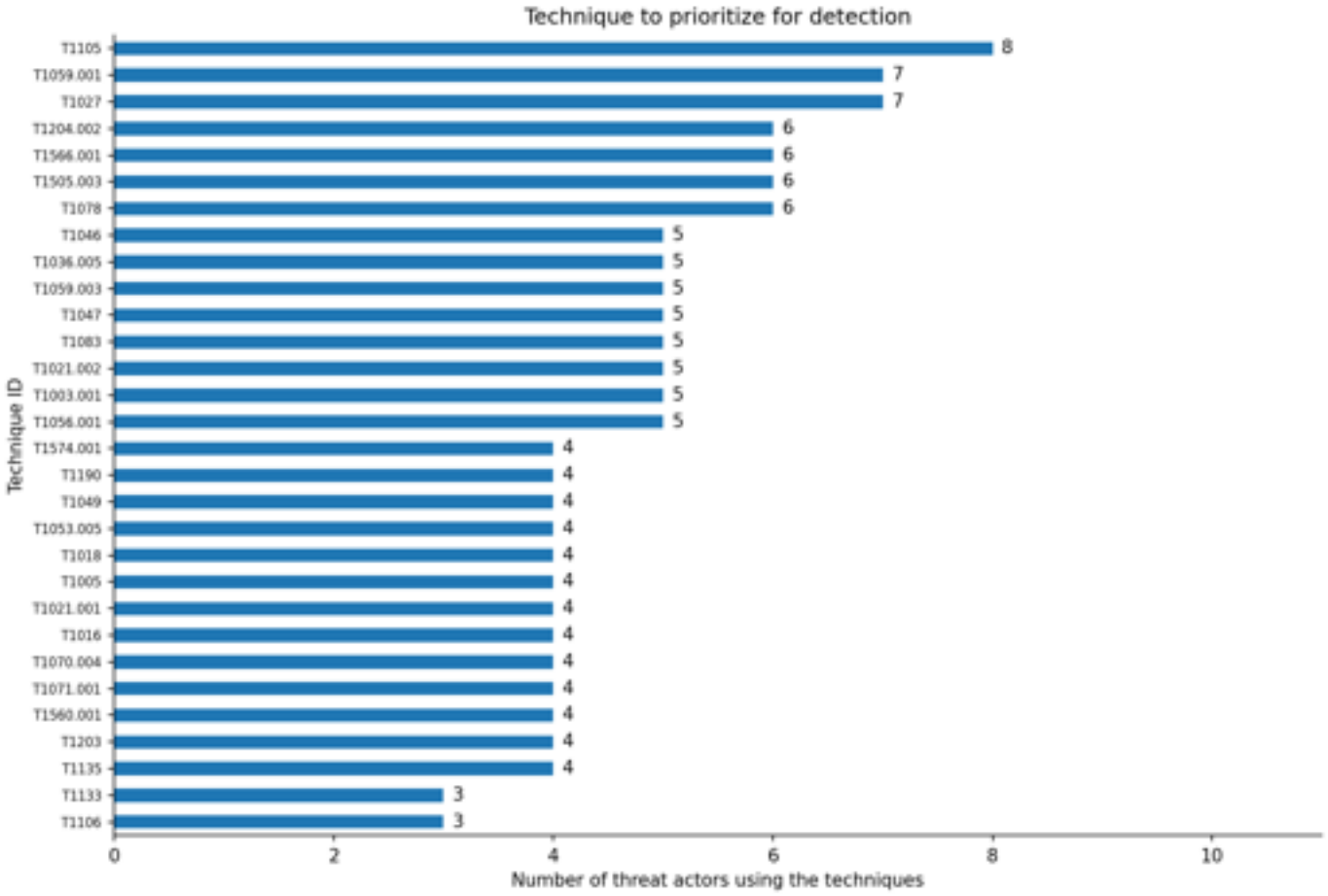

## 2.2 Technique distribution

The following graph gives the techniques distribution accross all of those threat actors.
It aims at understanding how many techniques need to be covered in order to have the suitable level of detection.
The profile can be compared to the pareto model where covering 20% of the most used techniques would covered 80% of the total of techniques used.
The red line gives the number of techniques corresponding to 20% of total techniques used.
The green line gives the number of techniques corresponding to 80% of total techniques used.



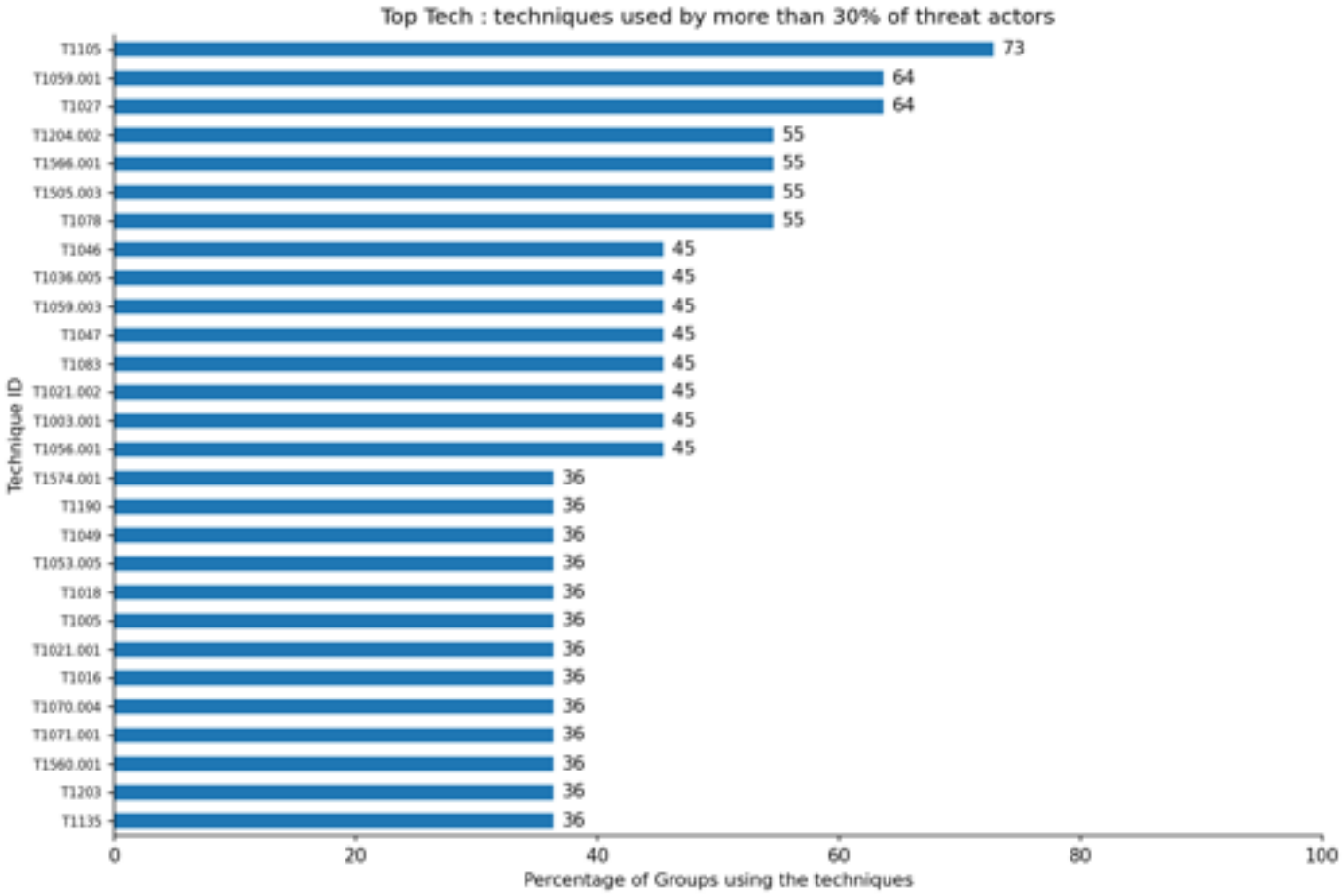

## 2.3 Top 30 most used techniques

The following graph gives the top 30 techniques that are most used by all of those threat actors.
For each most used technique, the number of group using this technique is given.



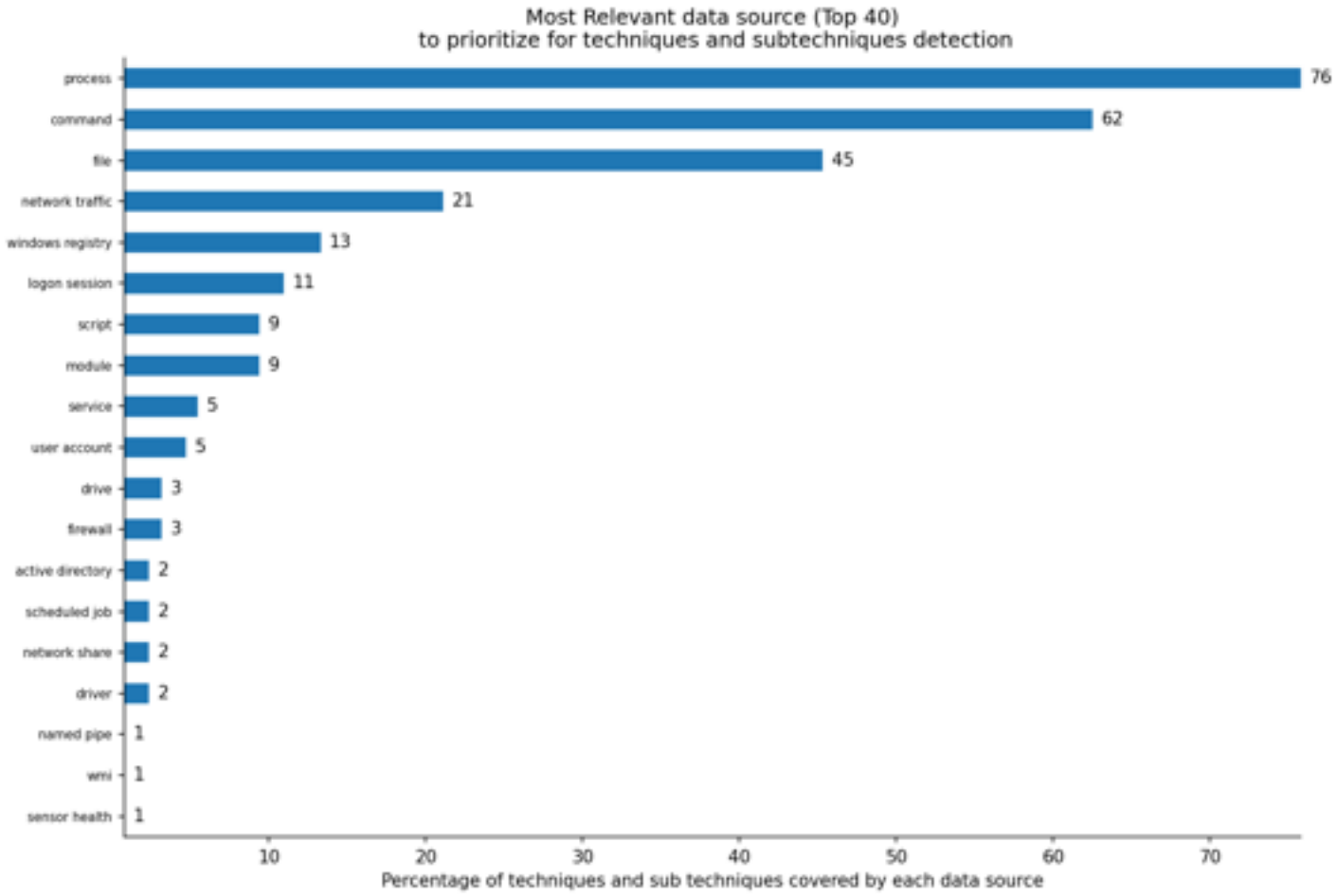

## 2.4 The Must be covered techniques

The following graph is just a focus of the previous one by giving the techniques that are used by almsot 30% of the threat actors. For each technique, the percentage of threat actors using this technique is given.



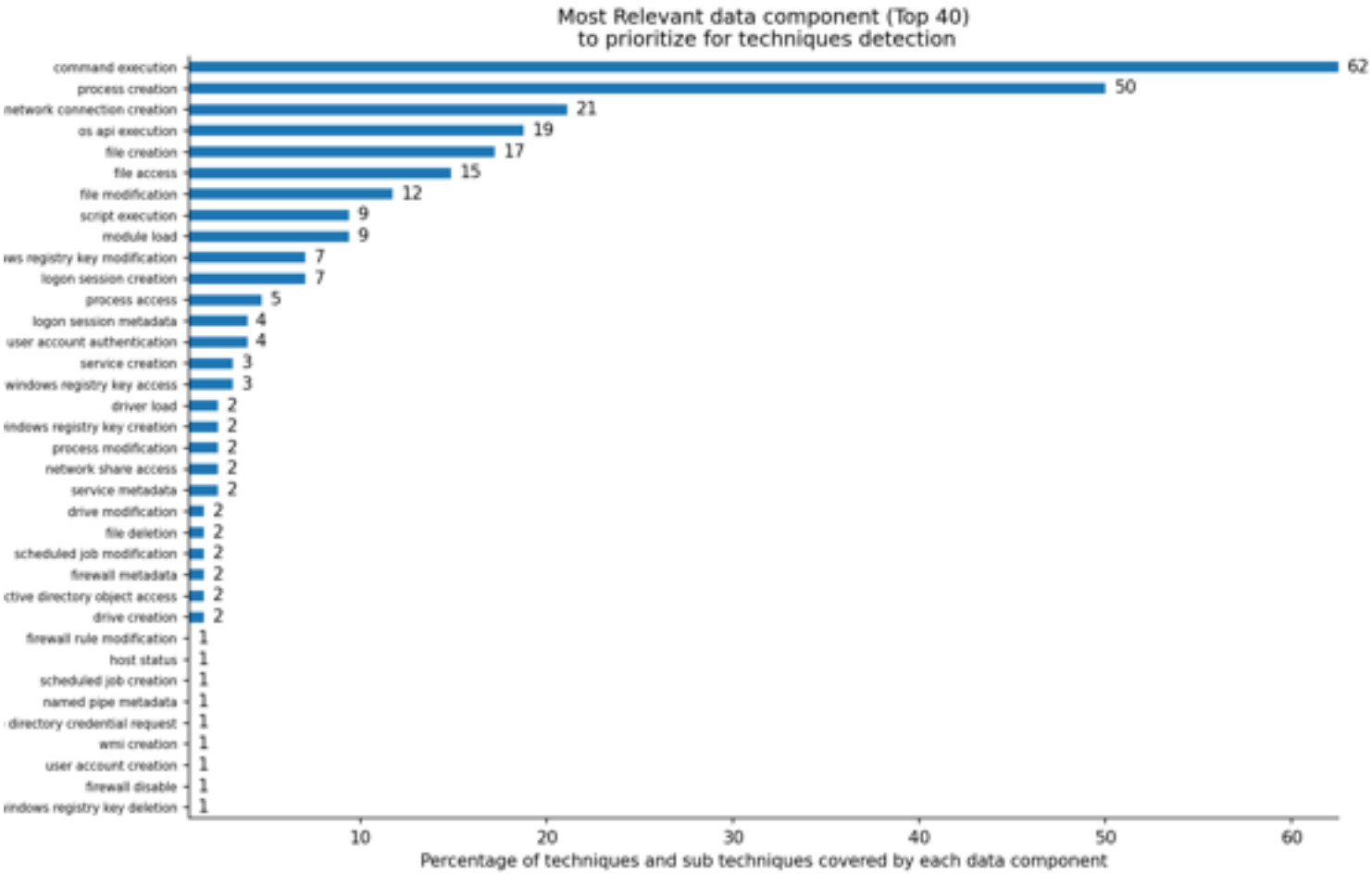

## 2.5 Top data source to collect for detections

The following graph gives the top 40 data source to collect in order to be able to detect the techniques used by threat actors.
Please see annexes for reference.



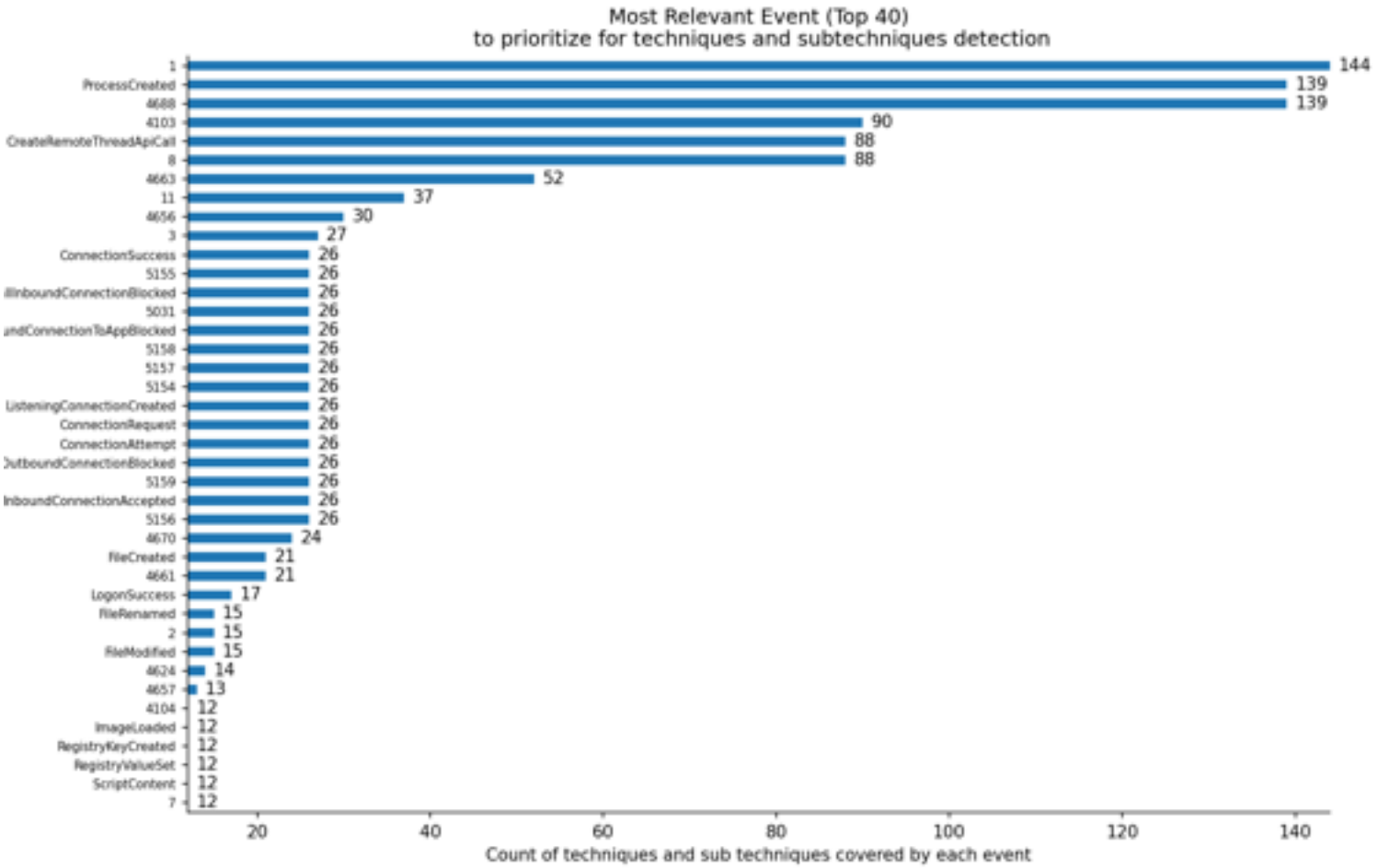

## 2.6 Top data component to collect for detections

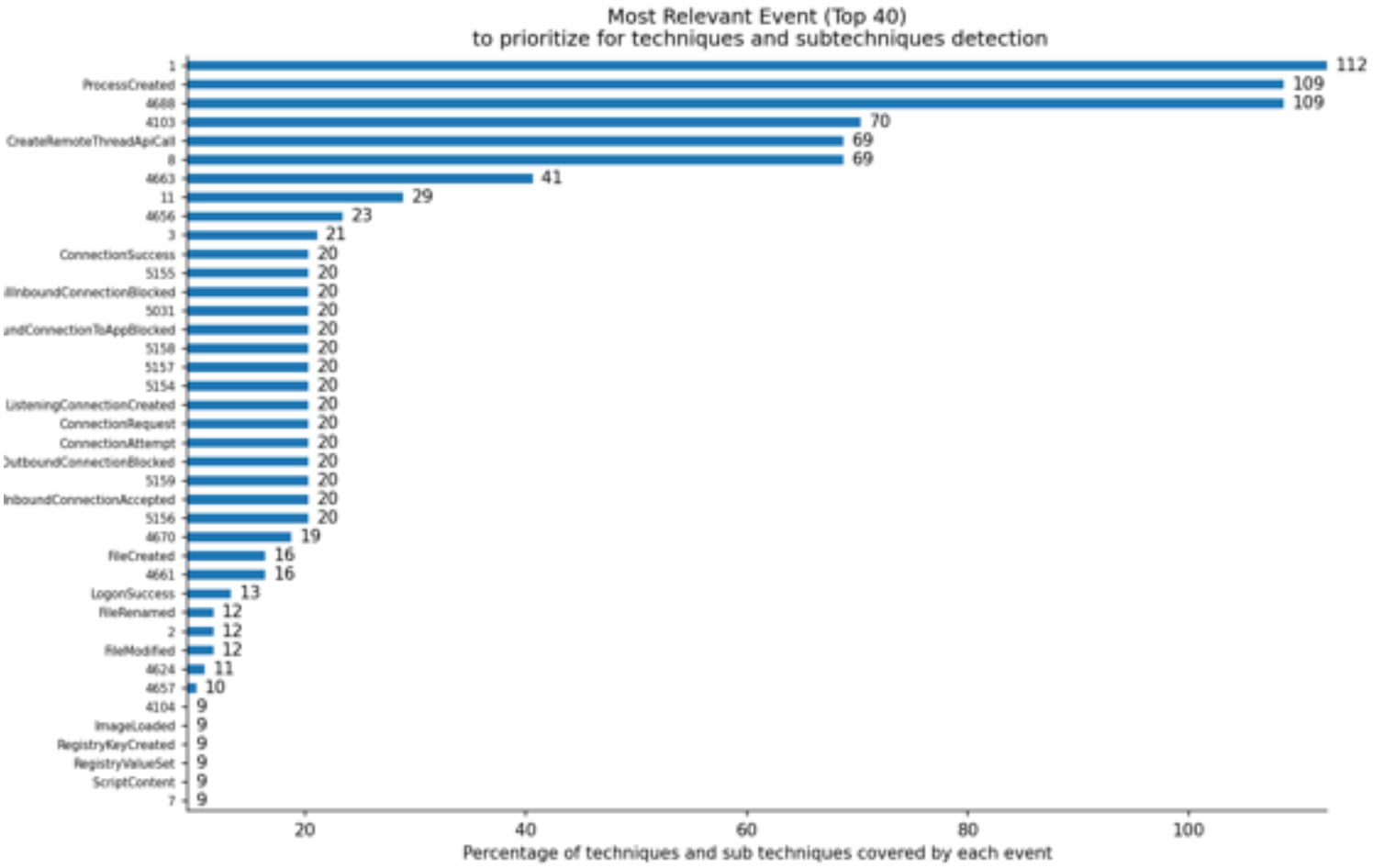
The following graph gives the top 40 data source to collect in order to be able to detect the techniques used by threat actors.
Please see annexes for reference.




## 2.7 Top event to collect for detections

The following graph gives the top 40 event to collect in order to be able to detect the techniques used by threat actors.
Please see annexes for reference.


Most Relevant Event (Top 40)
to prioritize for techniques and subtechniques detection
1
ProcessCreated
4688
4103
CreateRemoteThreadApiCall
8
4663
11
4656
3
ConnectionSuccess
5155
ilInboundConnectionBlocked
5031
andConnectionToAppBlocked
5158
5157
5154
ListeningConnectionCreated
ConnectionRequest
ConnectionAttempt
OutboundConnectionBlocked
5159
InboundConnectionAccepted
5156
4670
FileCreated
4661
LogonSuccess
FileRenamed
2
FileModified
4624
4657
4104
ImageLoaded
RegistryKeyCreated
RegistryValueSet
ScriptContent
7
144
139
139
90
88
88
52
37
30
27
26
26
26
26
26
26
26
26
26
26
26
26
26
26
24
21
21
17
15
15
15
14
13
12
12
12
12
12
12
20
40
60
80
100
120
140
Count of techniques and sub techniques covered by each event


Most Relevant Event (Top 40)
to prioritize for techniques and subtechniques detection
1
ProcessCreated
4688
4103
CreateRemoteThreadApiCall
8
4663
11
4656
3
ConnectionSuccess
5155
ilInboundConnectionBlocked
5031
andConnectionToAppBlocked
5158
5157
5154
ListeningConnectionCreated
ConnectionRequest
ConnectionAttempt
OutboundConnectionBlocked
5159
InboundConnectionAccepted
5156
4670
FileCreated
4661
LogonSuccess
FileRenamed
2
FileModified
4624
4657
4104
ImageLoaded
RegistryKeyCreated
RegistryValueSet
ScriptContent
7
112
109
109
70
69
69
41
29
23
21
20
20
20
20
20
20
20
20
20
20
20
20
20
20
19
16
16
13
12
12
12
11
10
9
9
9
9
9
9
20
40
60
80
100
Percentage of techniques and sub techniques covered by each event

# 3. How to detect most used techniques ?

This chapter aims at reviewing the most used techniques from most used to least used while providing more detailed information on the technique, the collection data required for detection and how to detect the technique.

## 3.1 T1105

Used by group : Tonto Team, Fox Kitten, Operation Wocao, Whitefly, APT41, Tropic Trooper, Leviathan, menuPass

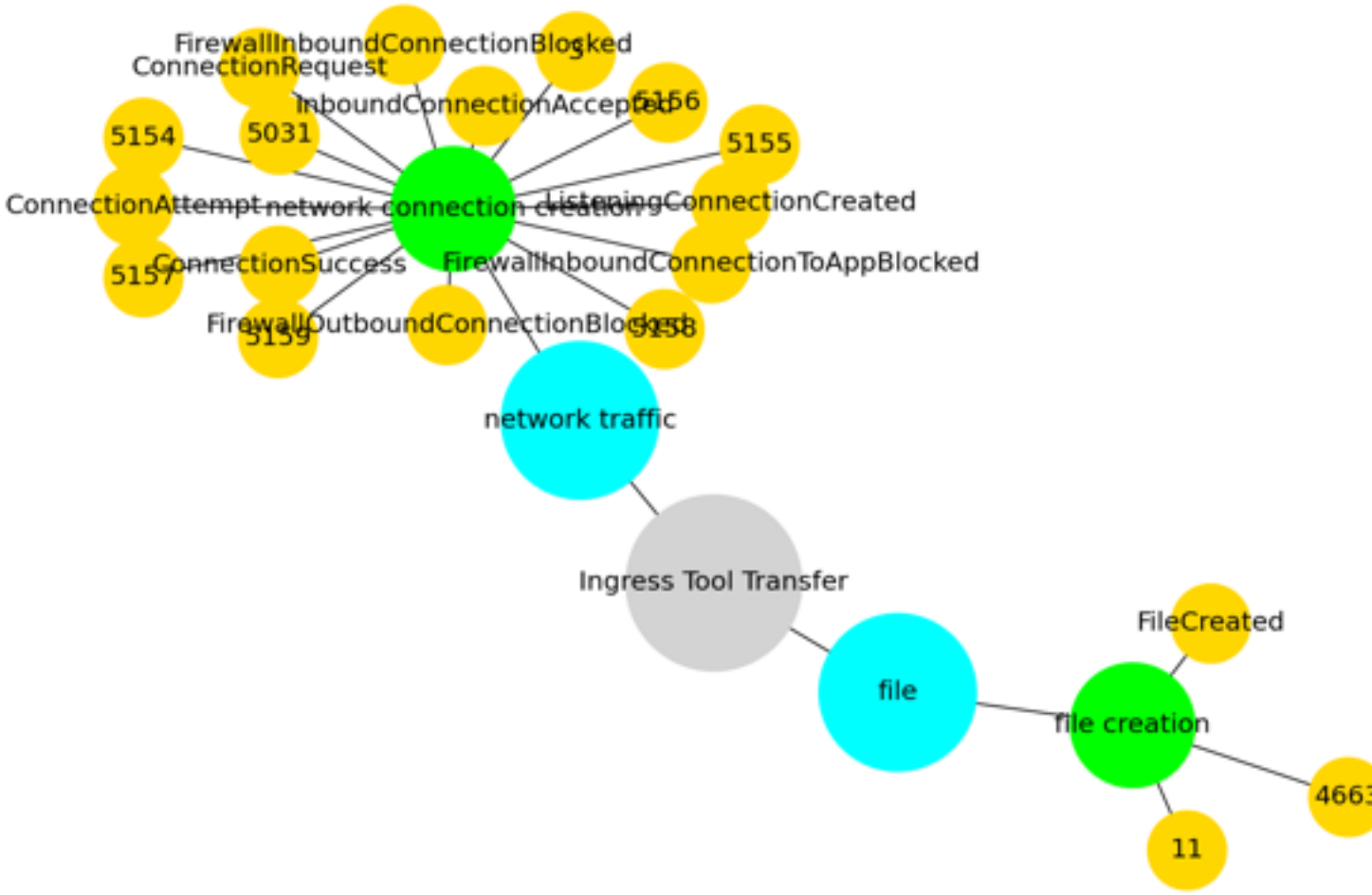
Tactic : command-and-control

Technique : Ingress Tool Transfer

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)).

Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016)

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as <code>IEX(New-Object Net.WebClient).downloadString()</code> and <code>Invoke-WebRequest</code>. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas)




## 3.2 T1059.001

Used by group : Tonto Team, Fox Kitten, Operation Wocao, APT41, Leviathan, menuPass, Deep Panda

Tactic : execution

Technique : PowerShell

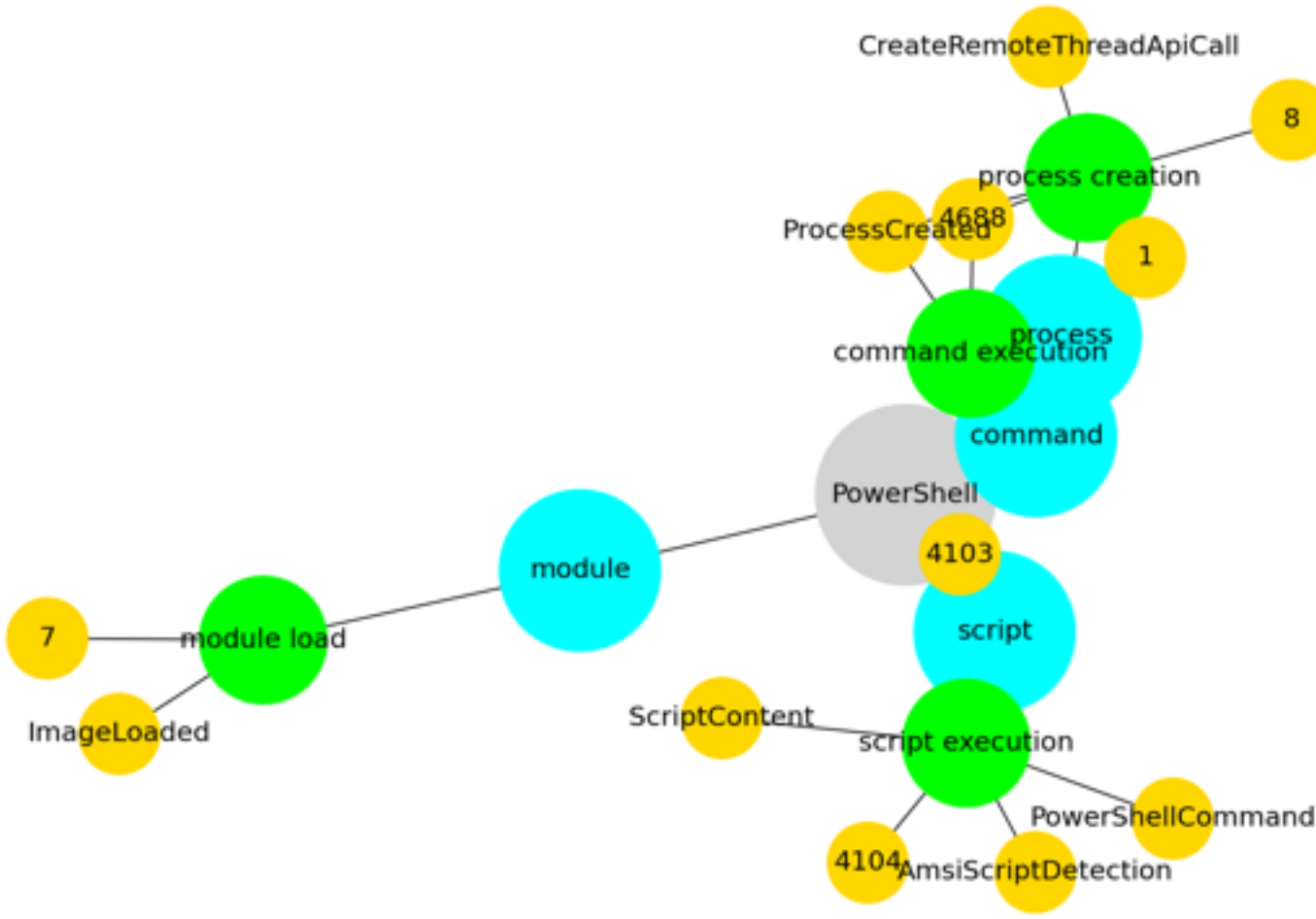
Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the <code>Start-Process</code> cmdlet which can be used to run an executable and the <code>Invoke-Command</code> cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory

without touching disk.

A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the <code>powershell.exe</code> binary through interfaces to PowerShell's underlying <code>System.Management.Automation</code> assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)




## 3.3 T1027

Used by group : Fox Kitten, Operation Wocao, Whitefly, APT41, Tropic Trooper, Leviathan, menuPass

Tactic : defense-evasion

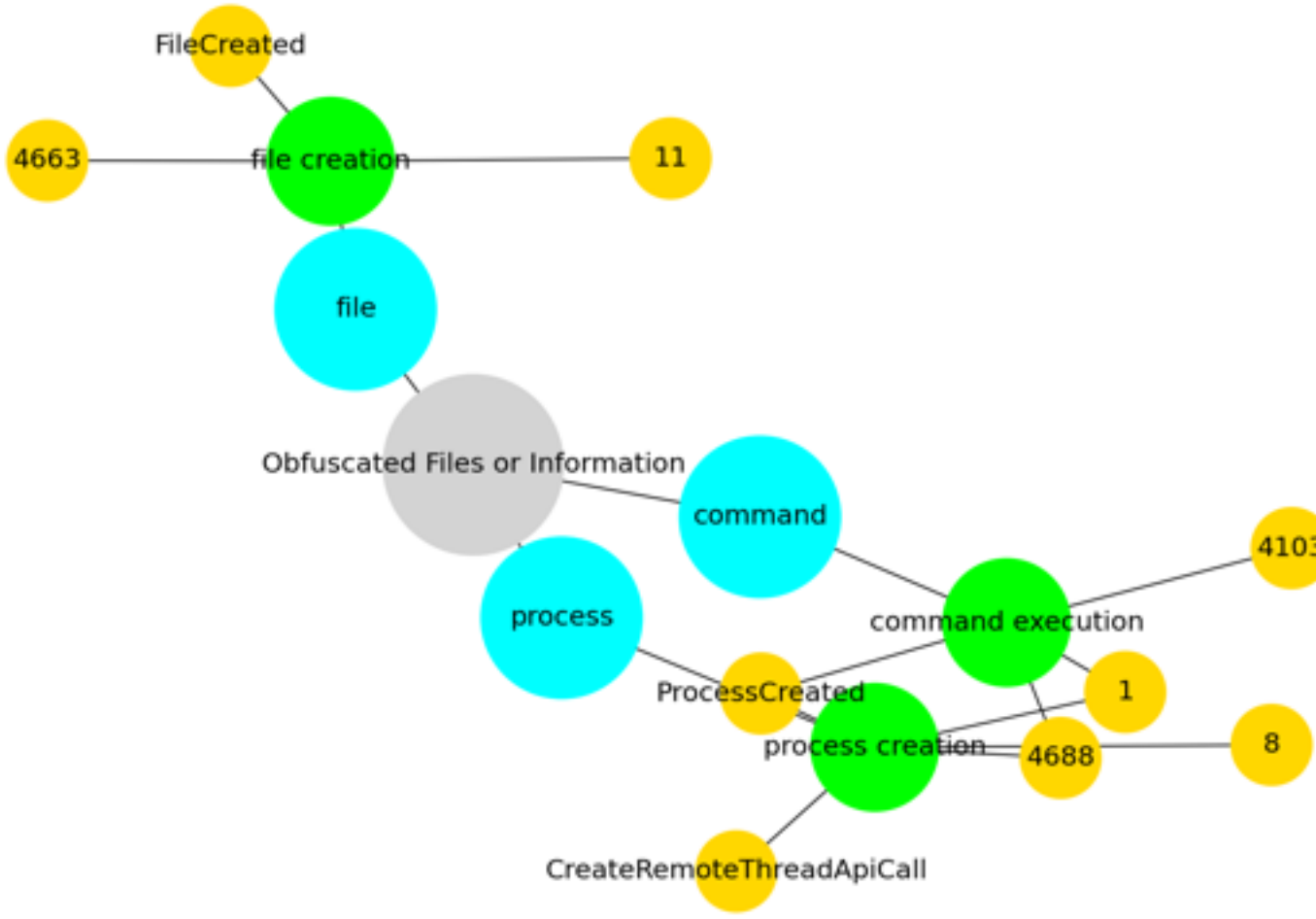
Technique : Obfuscated Files or Information

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also used compressed or archived scripts, such as JavaScript.

Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016)

Adversaries may also obfuscate commands executed from payloads or directly via a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)




## 3.4 T1204.002

Used by group : Tonto Team, Whitefly, FIN4, Tropic Trooper, Leviathan, menuPass

Tactic : execution

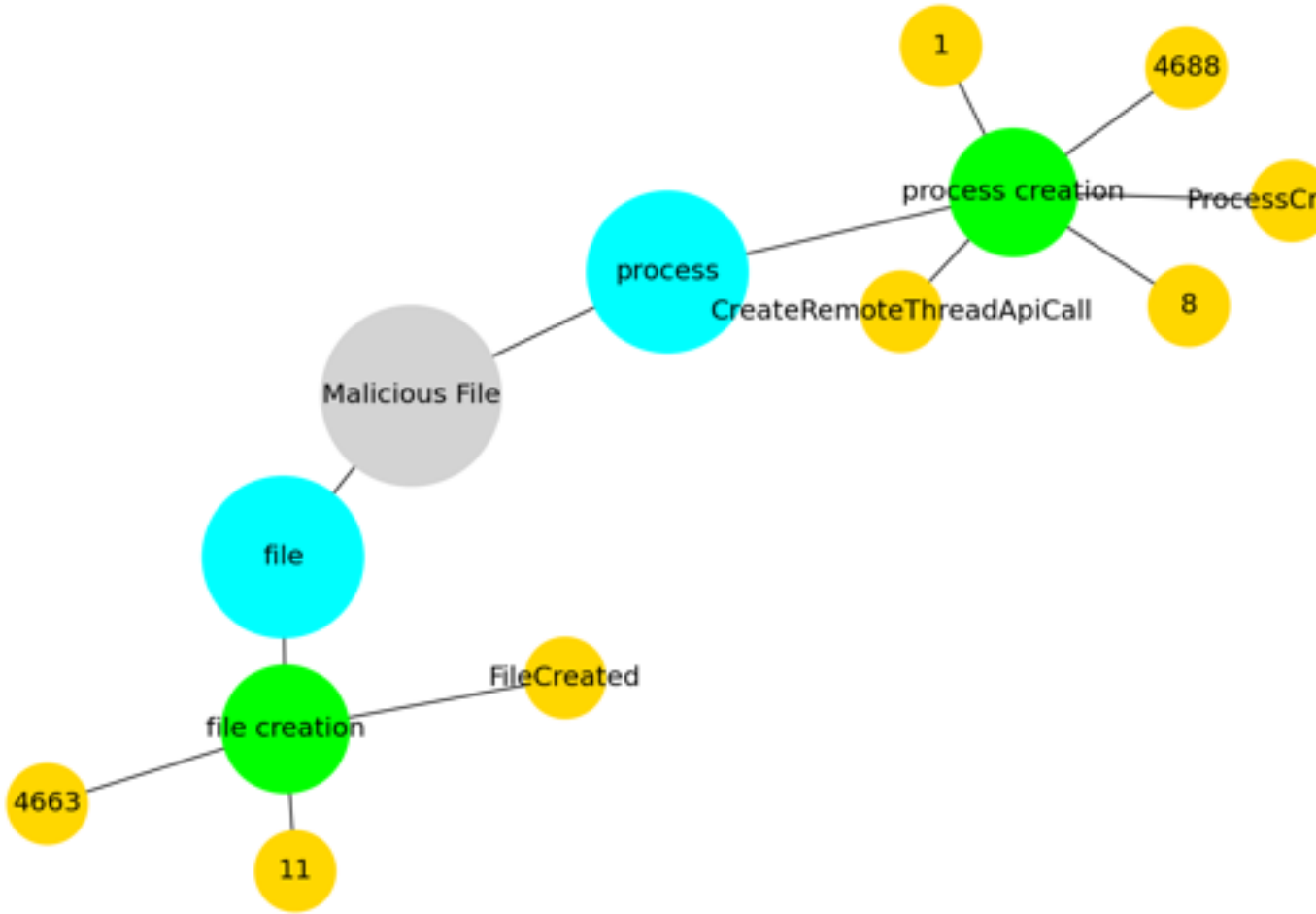
Technique : Malicious File

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.

Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying

instructions to a user on how to open it.(Citation: Password Protected Word Docs)

While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).




## 3.5 T1566.001

Used by group : Tonto Team, APT41, FIN4, Tropic Trooper, Leviathan, menuPass

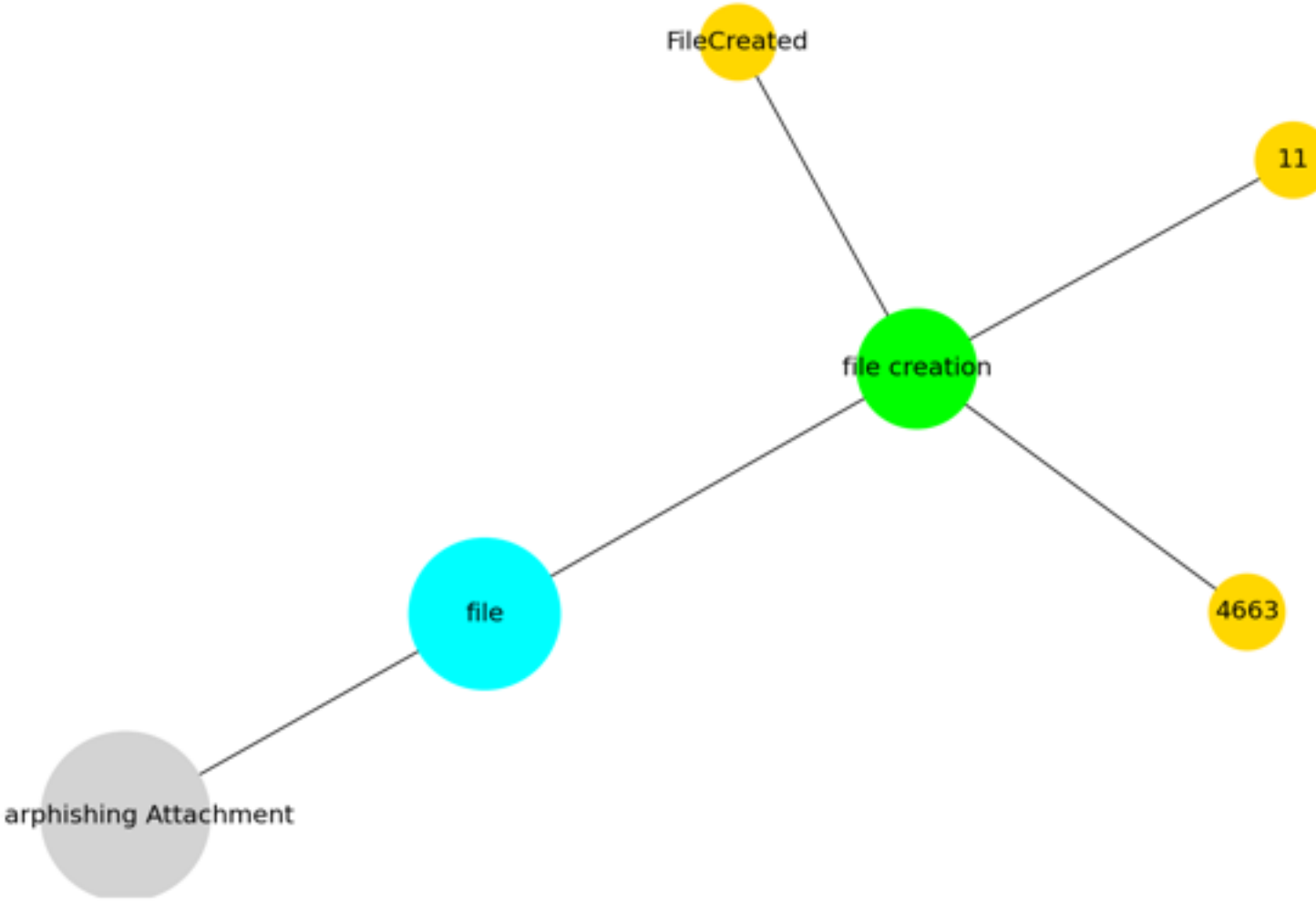
Tactic : initial-access

Technique : Spearphishing Attachment

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of

spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.




## 3.6 T1505.003

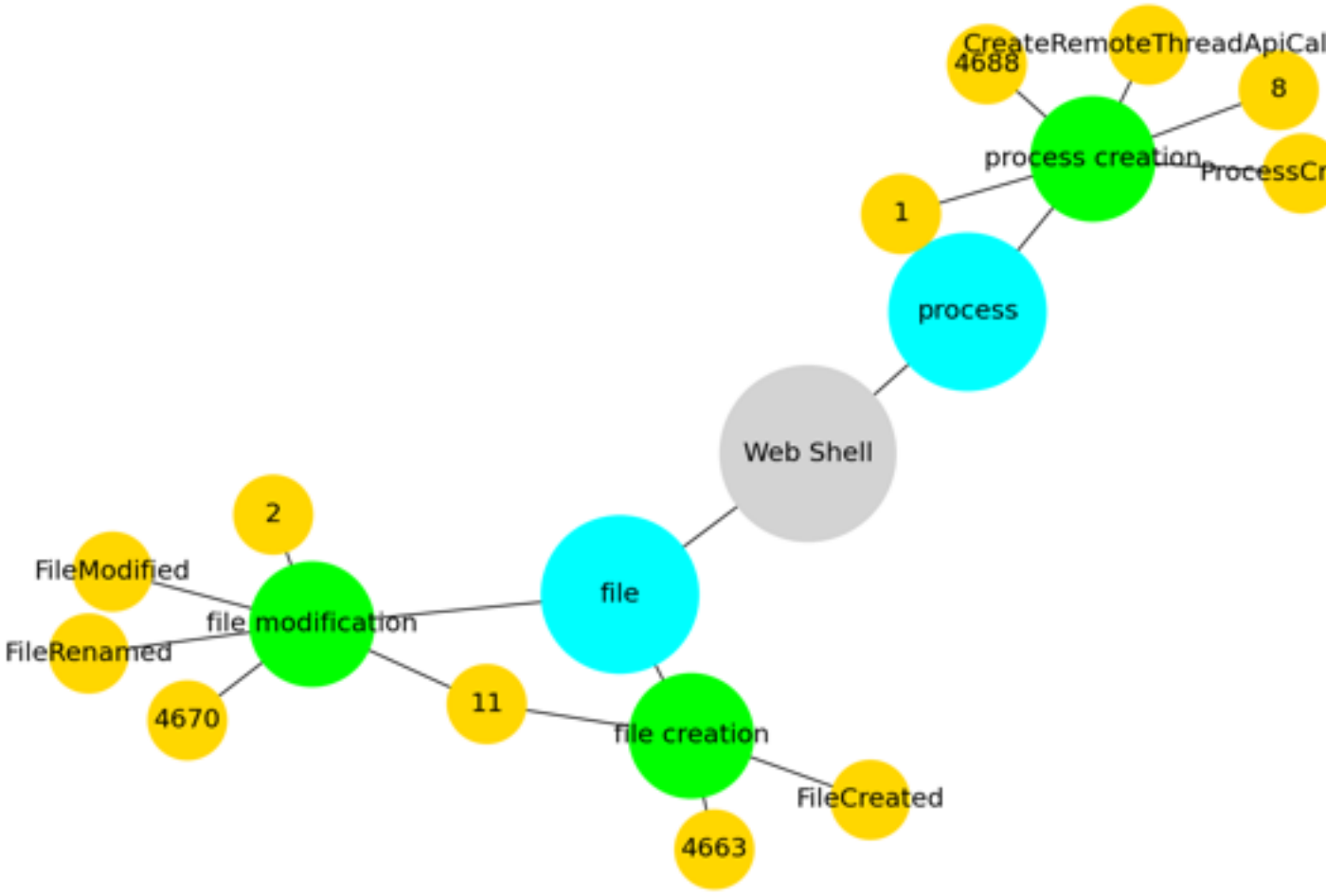
Used by group : Tonto Team, Fox Kitten, Operation Wocao, Tropic Trooper, Leviathan, Deep Panda

Tactic : persistence

Technique : Web Shell

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.

In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (ex: [China Chopper](https://attack.mitre.org/software/S0020) Web shell client).(Citation: Lee 2013)




## 3.7 T1078

Used by group : Fox Kitten, Operation Wocao, APT41, FIN4, Leviathan, menuPass

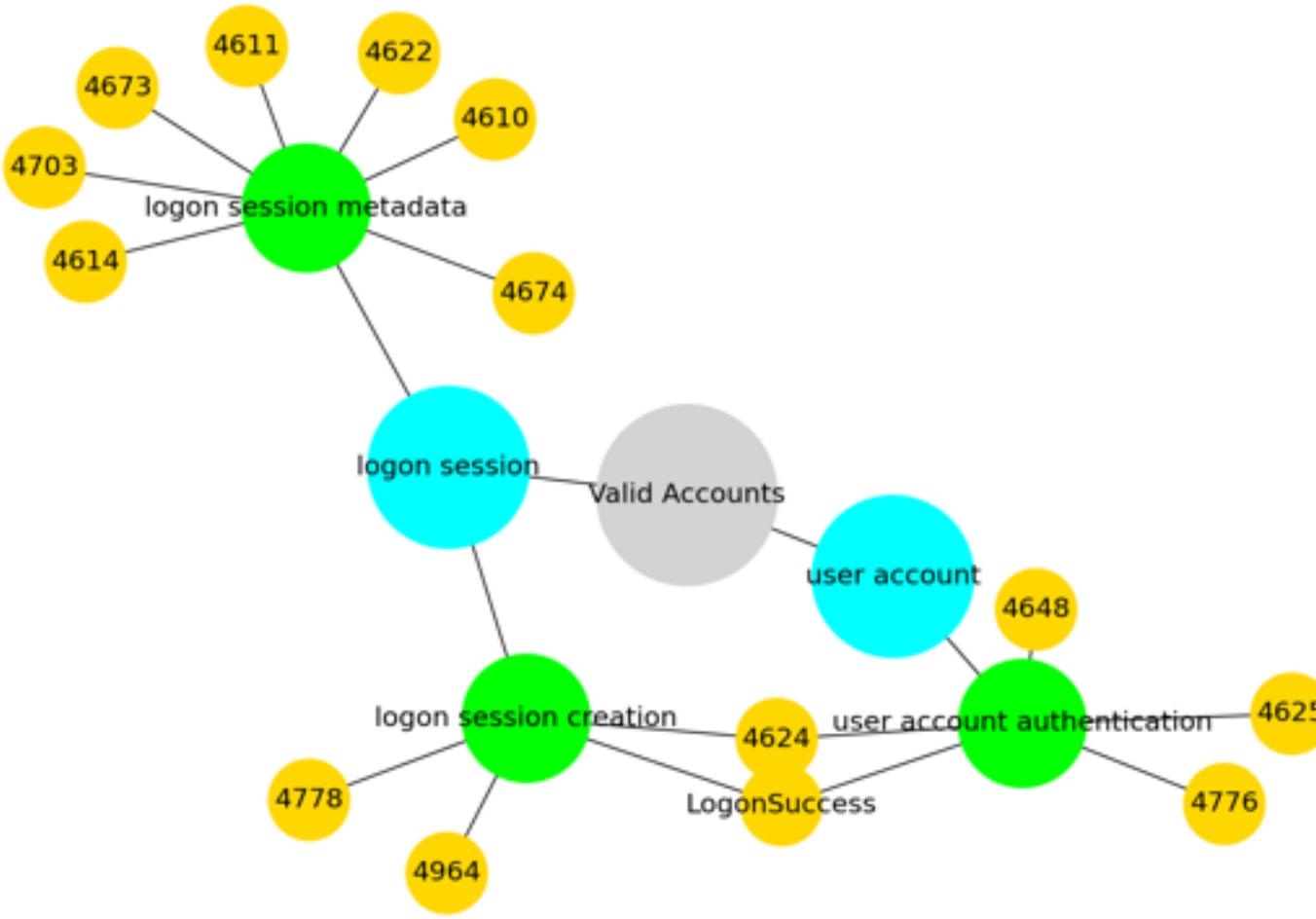
Tactic : defense-evasion, persistence, privilege-escalation, initial-access

Technique : Valid Accounts

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare)

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)




## 3.8 T1046

Used by group : Fox Kitten, Operation Wocao, APT41, Tropic Trooper, menuPass

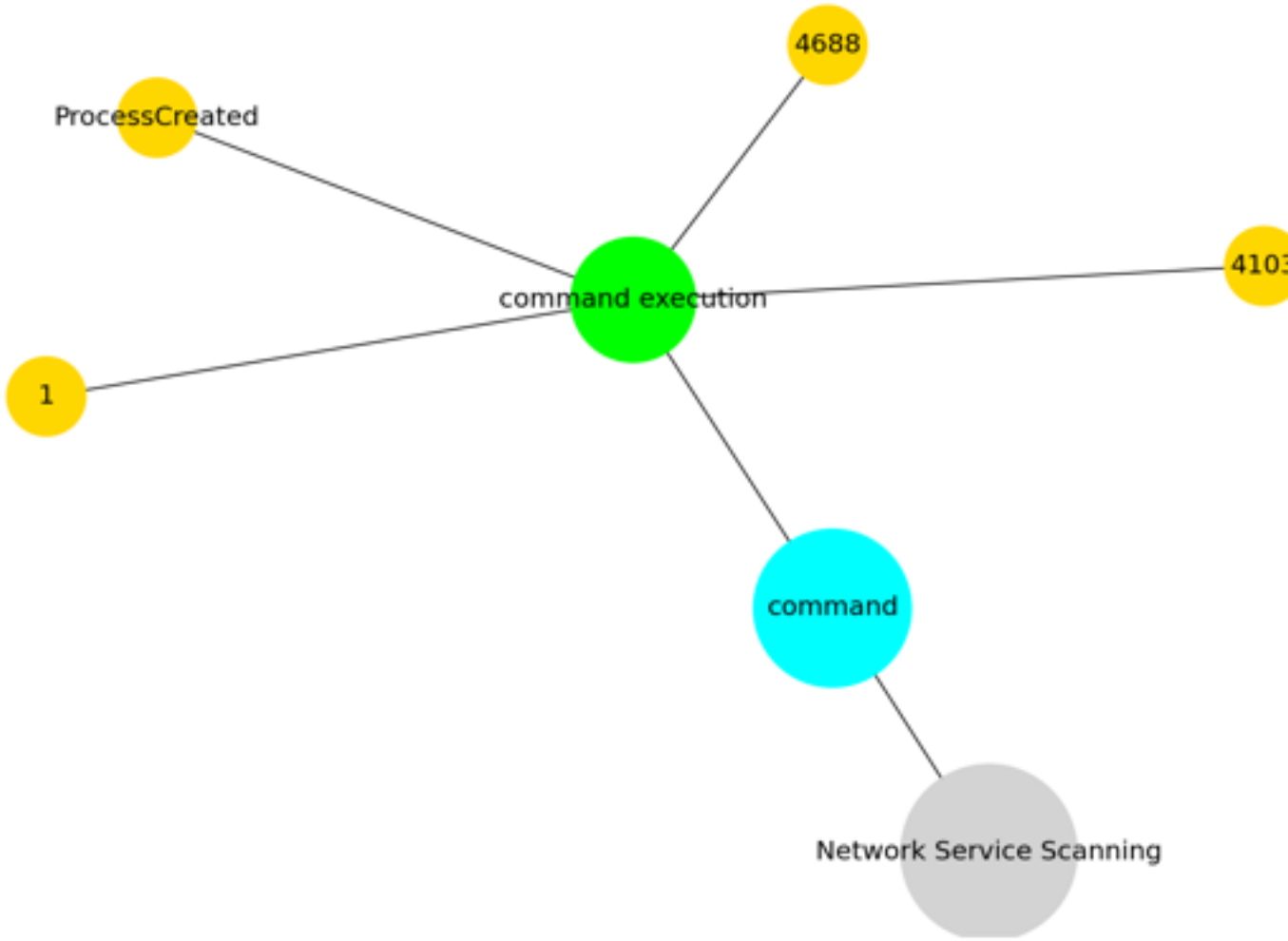
Tactic : discovery

Technique : Network Service Discovery

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021)

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well.

Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as <code>dns-sd -B _ssh._tcp .</code>) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)




## 3.9 T1036.005

Used by group : Fox Kitten, Whitefly, APT41, Tropic Trooper, menuPass

Tactic : defense-evasion

Technique : Match Legitimate Name or Location

Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also

be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster. Alternatively, a file or container image name given may be a close approximation to legitimate programs/images or something innocuous.

Adversaries may also use the same icon of the file they are trying to mimic.

## 3.10 T1059.003

Used by group : Fox Kitten, Operation Wocao, APT41, Tropic Trooper, menuPass

Tactic : execution

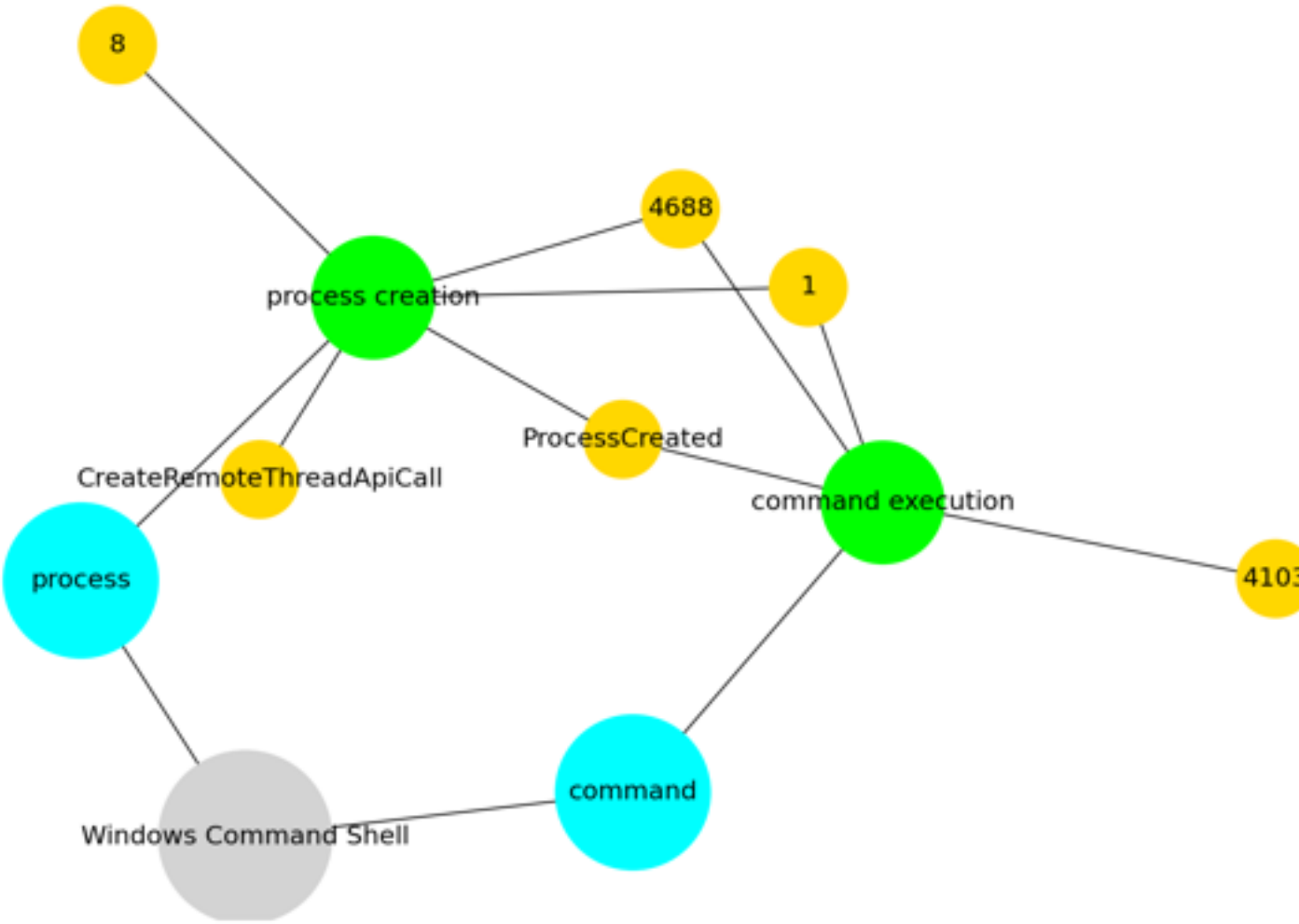
Technique : Windows Command Shell

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of

commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows)

Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.




## 3.11 T1047

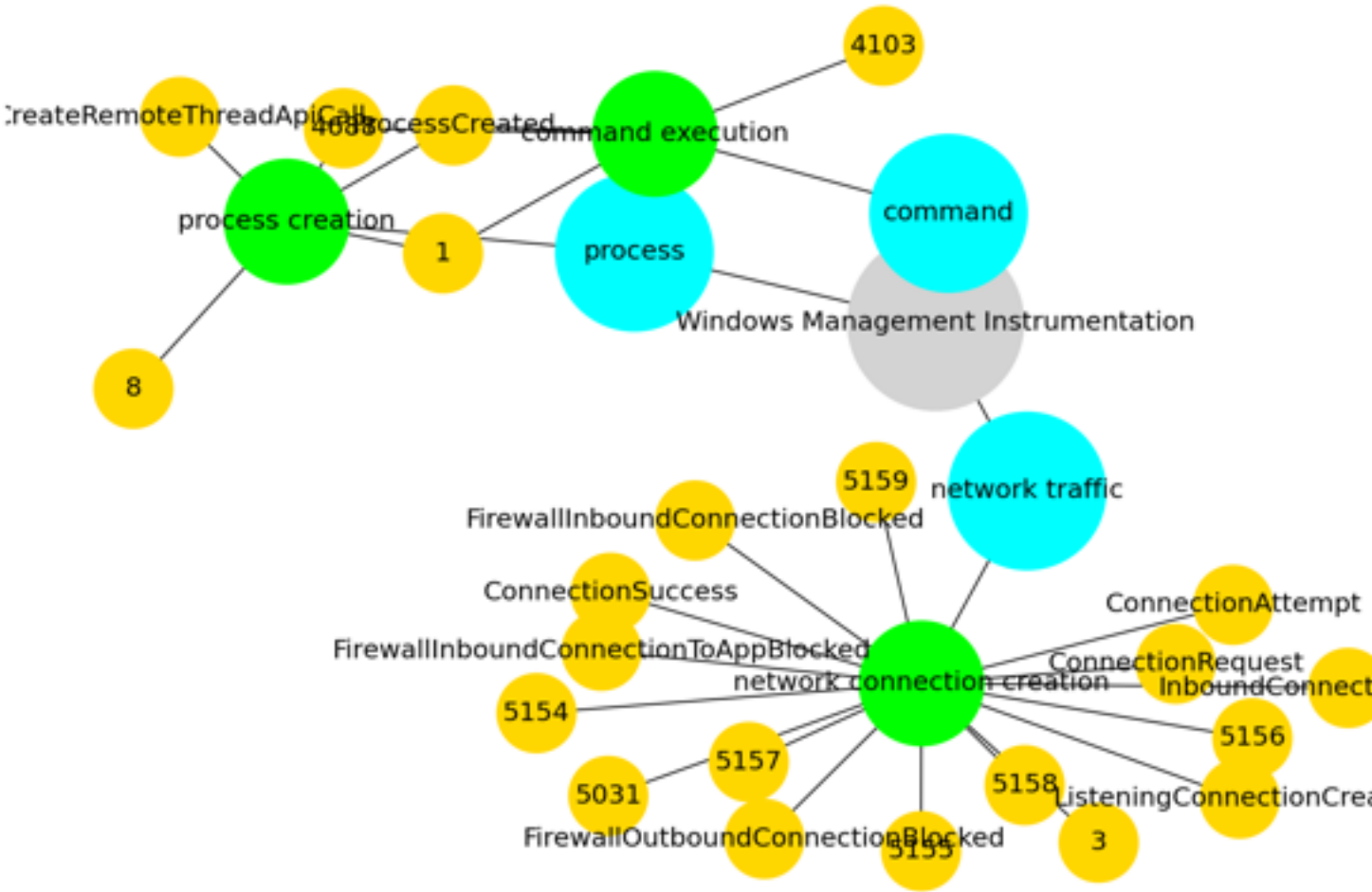
Used by group : Operation Wocao, APT41, Leviathan, menuPass, Deep Panda

Tactic : execution

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](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015)

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. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)



## 3.12 T1083

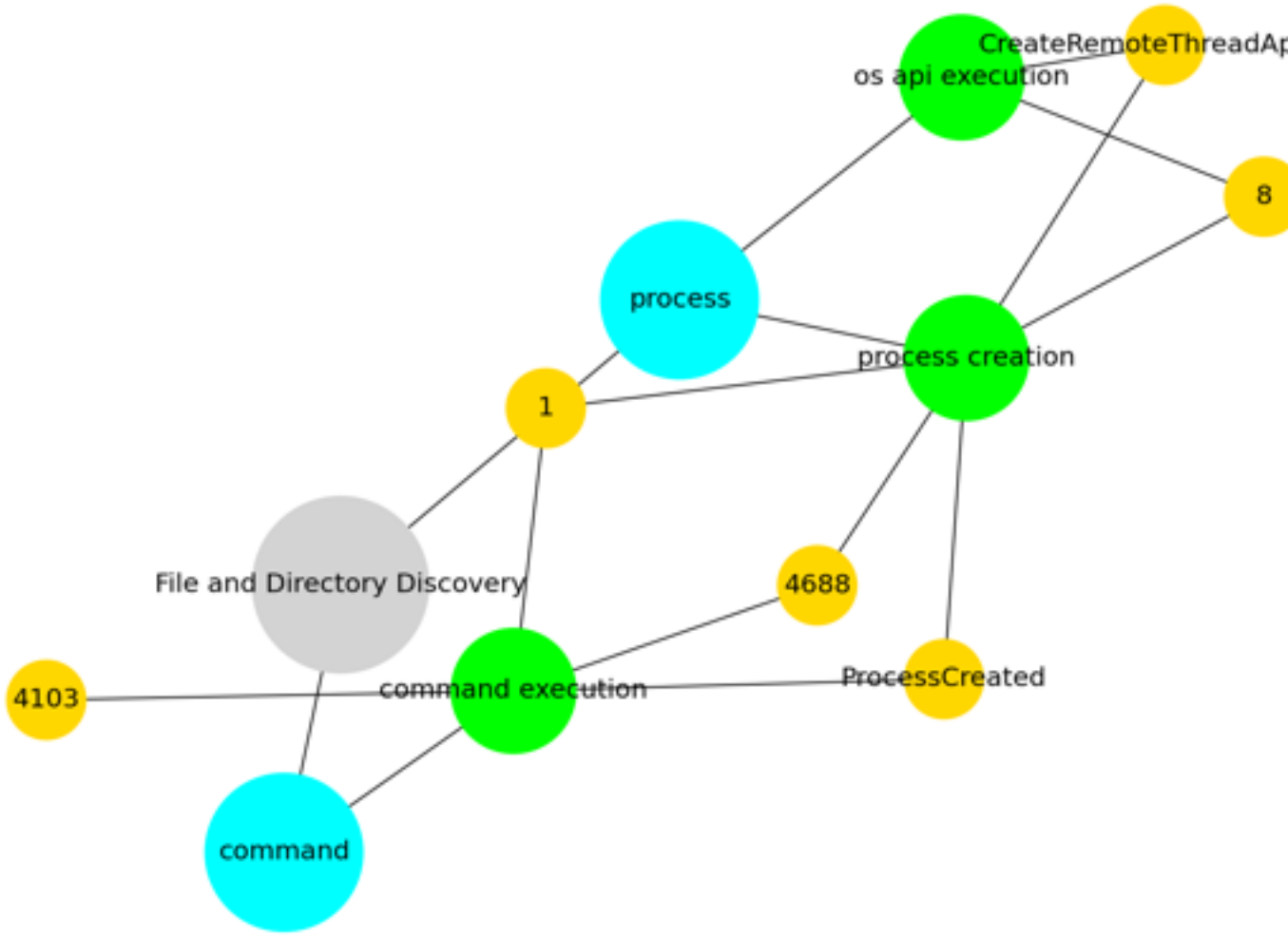
Used by group : Fox Kitten, Operation Wocao, APT41, Tropic Trooper, menuPass

Tactic : discovery

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](https://attack.mitre.org/techniques/T1083) 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 <code>dir</code>, <code>tree</code>, <code>ls</code>, <code>find</code>, and <code>locate</code>.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information.(Citation: US-CERT-TA18-106A)




## 3.13 T1021.002

Used by group : Fox Kitten, Operation Wocao, APT41, Orangeworm, Deep Panda

Tactic : lateral-movement

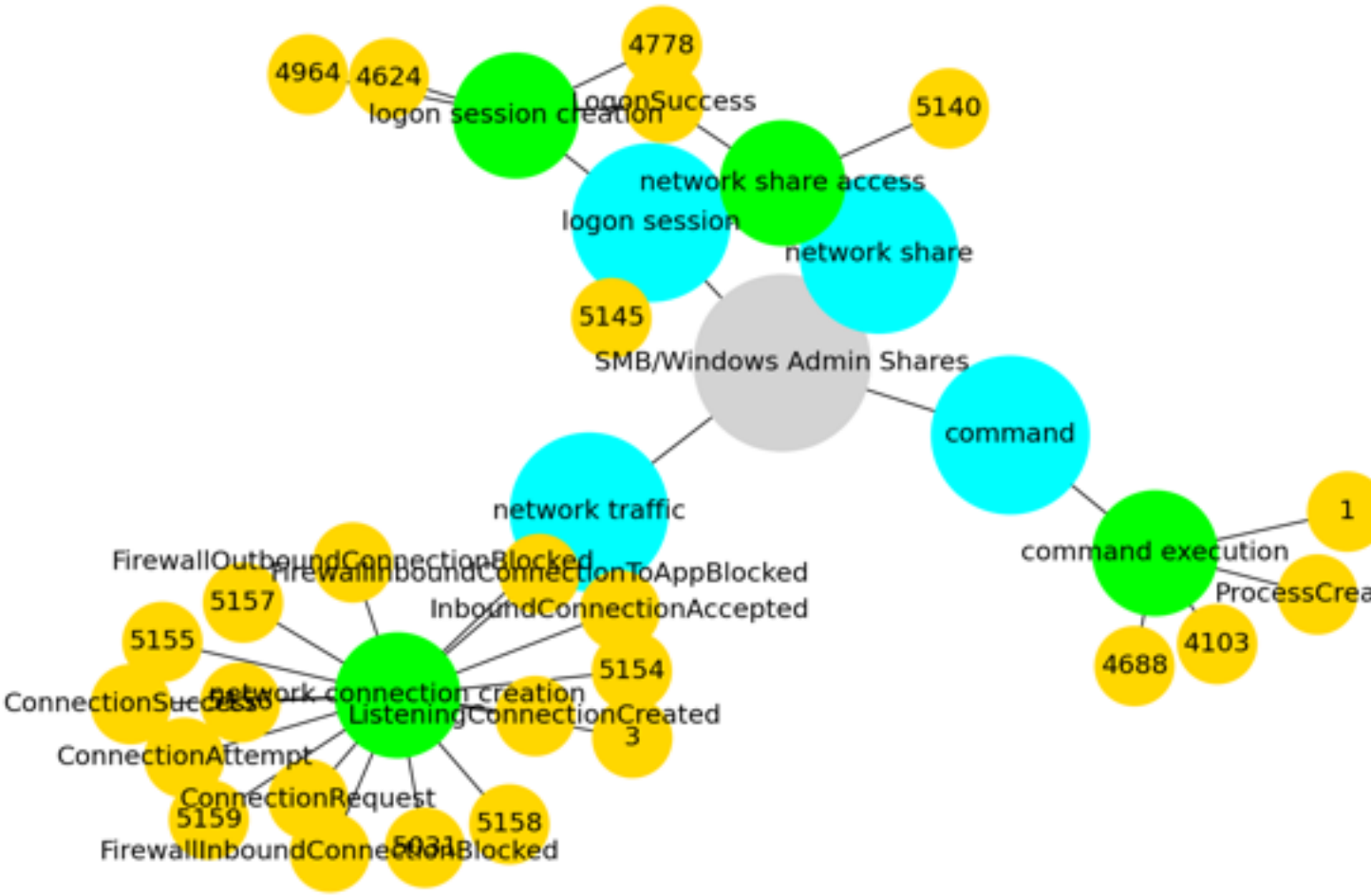
Technique : SMB/Windows Admin Shares

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.

SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy

and other administrative functions. Example network shares include `C$`, `ADMIN$`, and `IPC$`. Adversaries may use this technique in conjunction with administrator-level [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely access a networked system over SMB,(Citation: Wikipedia Server Message Block) to interact with systems using remote procedure calls (RPCs),(Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). Adversaries can also use NTLM hashes to access administrator shares on systems with [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) and certain configuration and patch levels.(Citation: Microsoft Admin Shares)




## 3.14 T1003.001

Used by group : Fox Kitten, Operation Wocao, Whitefly, APT41, Leviathan

Tactic : credential-access

Technique : LSASS Memory

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550).

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

* <code>procdump -ma lsass.exe lsass_dump</code>

Locally, mimikatz can be run using:

* <code>sekurlsa::Minidump lsassdump.dmp</code>
* <code>sekurlsa::logonPasswords</code>

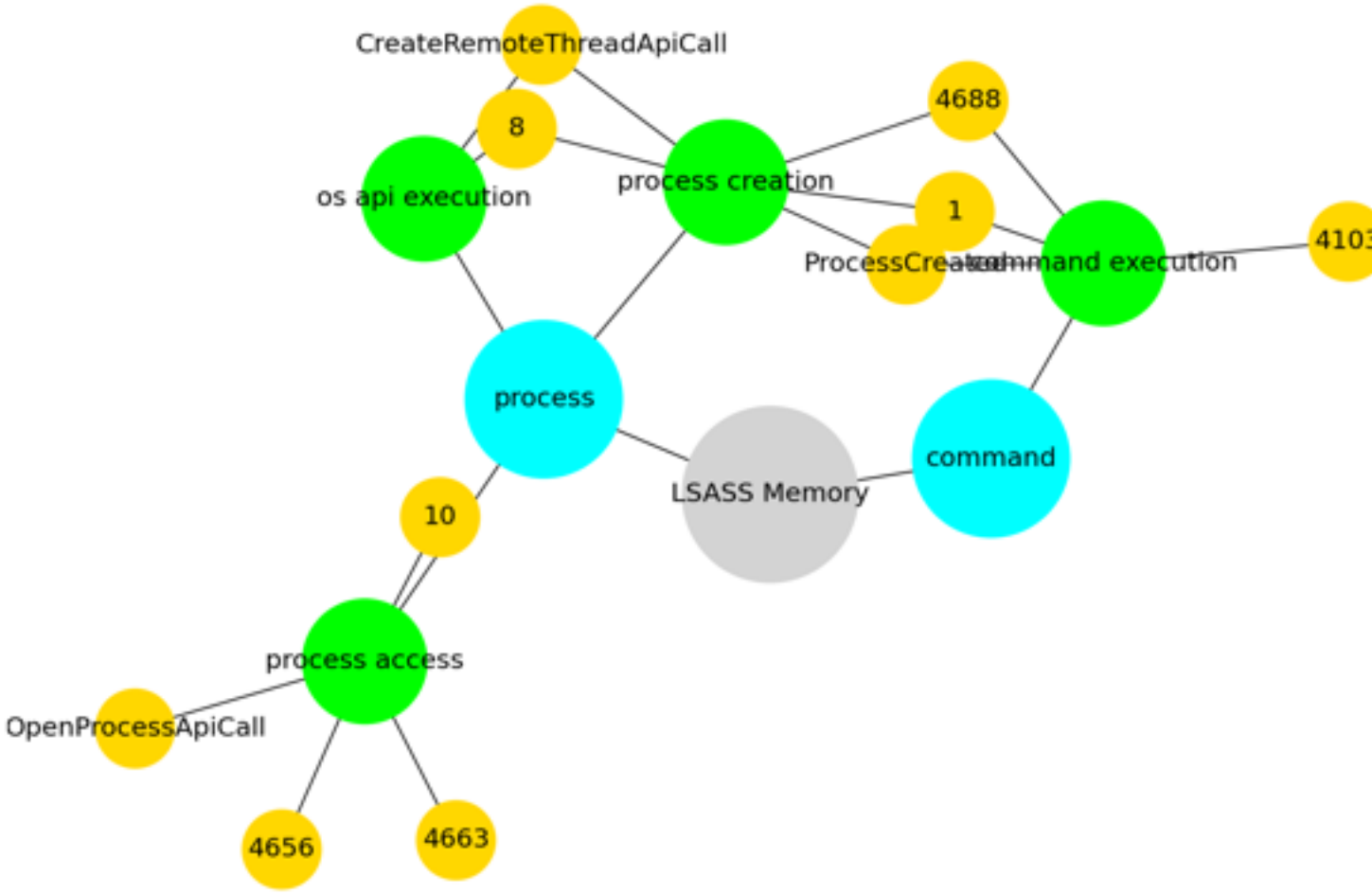
Built-in Windows tools such as comsvcs.dll can also be used:

* <code>rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full</code>(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector)

Windows Security Support Provider (SSP) DLLs are loaded into LSSAS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014)

The following SSPs can be used to access credentials:

* Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
* Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.(Citation: TechNet Blogs Credential Protection)
* Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
* CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)




## 3.15 T1056.001

Used by group : Tonto Team, Operation Wocao, APT41, FIN4, menuPass

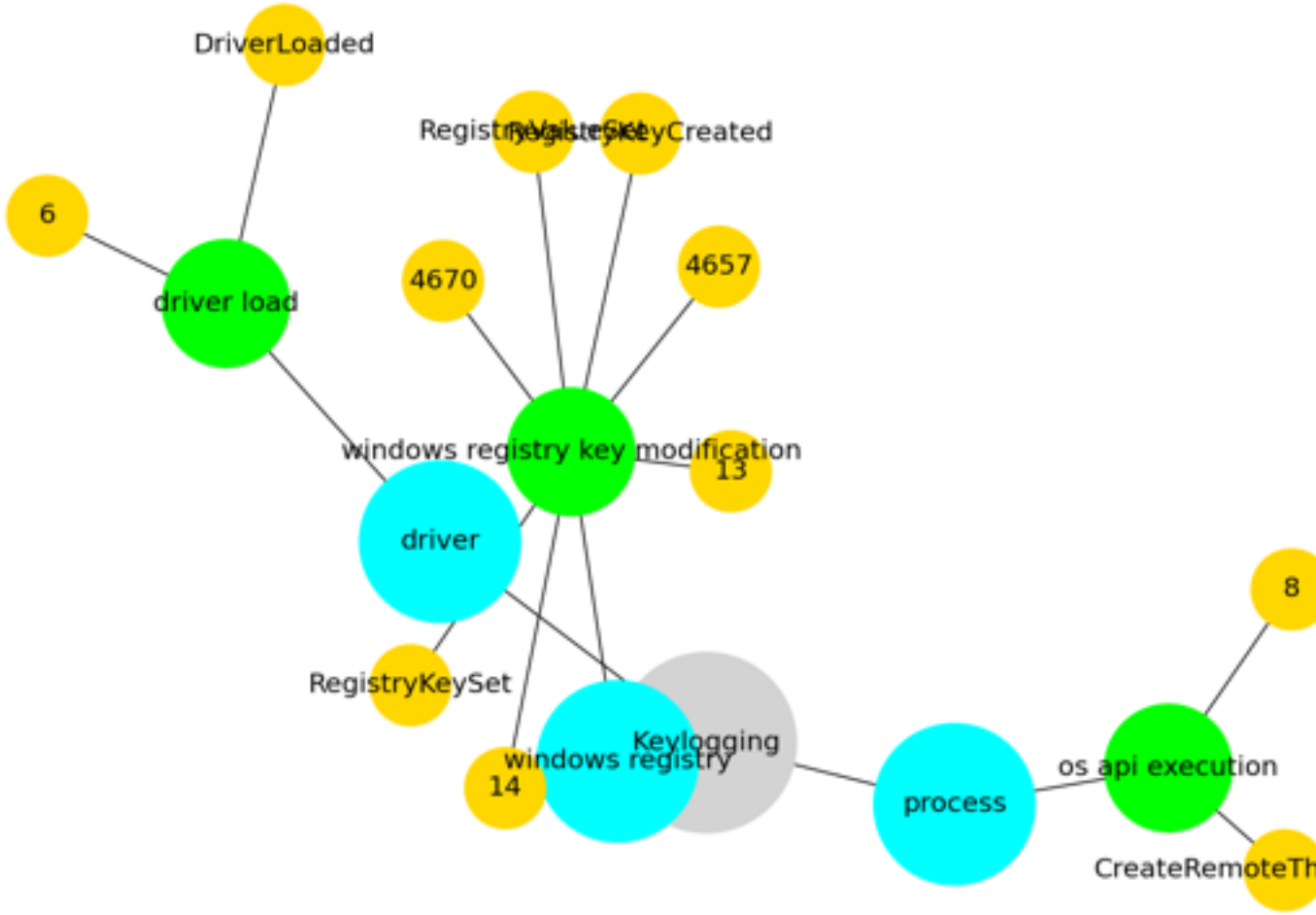
Tactic : collection, credential-access

Technique : Keylogging

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured.

Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include:

* Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data.
* Reading raw keystroke data from the hardware buffer.
* Windows Registry modifications.
* Custom drivers.
* [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)




## 3.16 T1574.001

Used by group : Tonto Team, Whitefly, APT41, menuPass

Tactic : persistence, privilege-escalation, defense-evasion

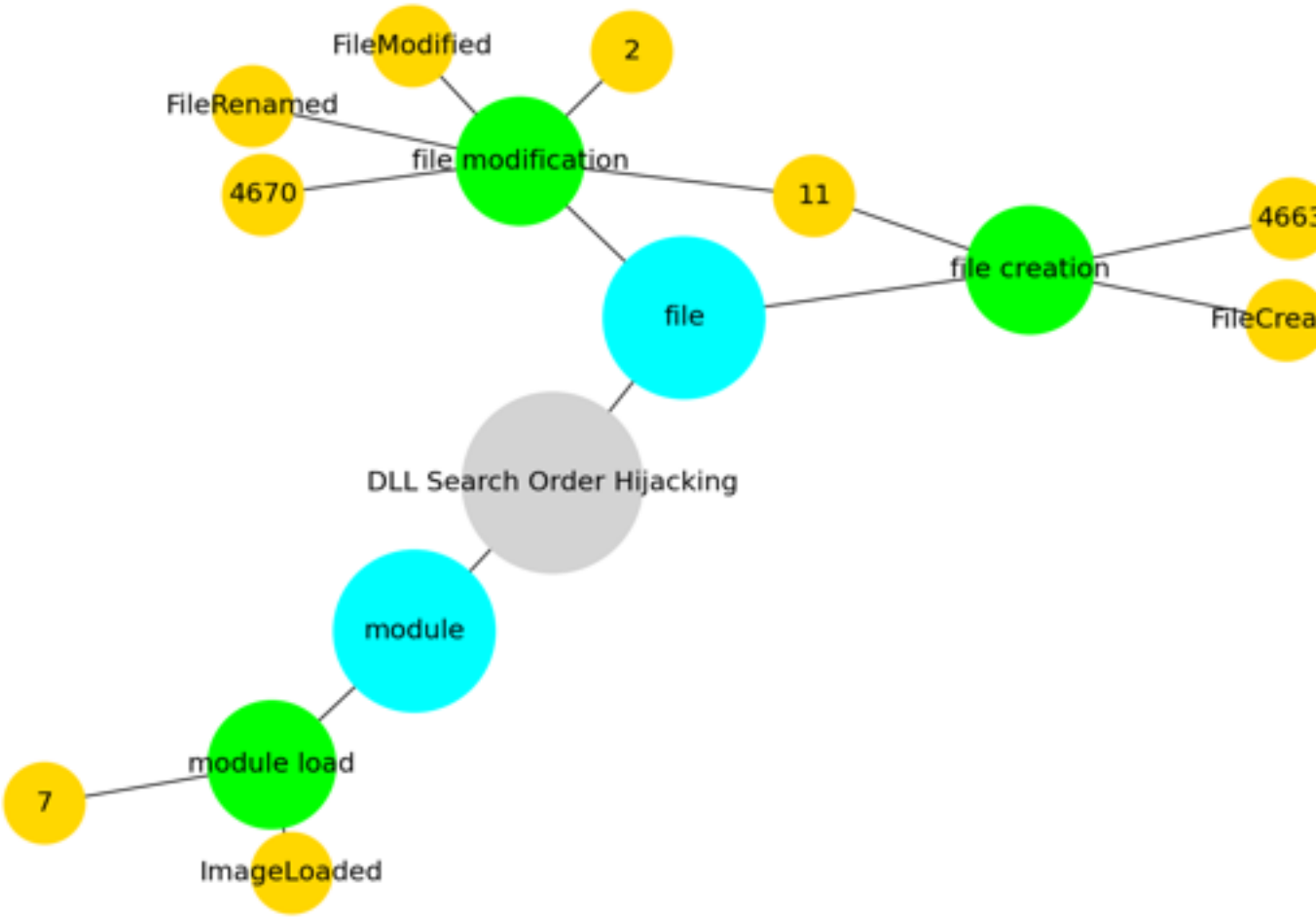
Technique : DLL Search Order Hijacking

Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft Dynamic Link Library Search Order)(Citation: FireEye Hijacking July 2010) Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution.

There are many ways an adversary can hijack DLL loads. Adversaries may plant trojan dynamic-link library files (DLLs) in a directory that will be searched before the location of a legitimate library that will be requested by a program, causing Windows to load their malicious library when it is called for by the victim program. Adversaries may also perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program.(Citation: FireEye fxsst June 2011) Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft Security Advisory 2269637)

Adversaries may also directly modify the search order via DLL redirection, which after being enabled (in the Registry and creation of a redirection file) may cause a program to load a different DLL.(Citation: Microsoft Dynamic-Link Library Redirection)(Citation: Microsoft Manifests)(Citation: FireEye DLL Search Order Hijacking)

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program. Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.




## 3.17 T1190

Used by group : Fox Kitten, Operation Wocao, APT41, menuPass

Tactic : initial-access

Technique : Exploit Public-Facing Application

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may include [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211).

If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies.

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

## 3.18 T1049

Used by group : Operation Wocao, APT41, Tropic Trooper, menuPass

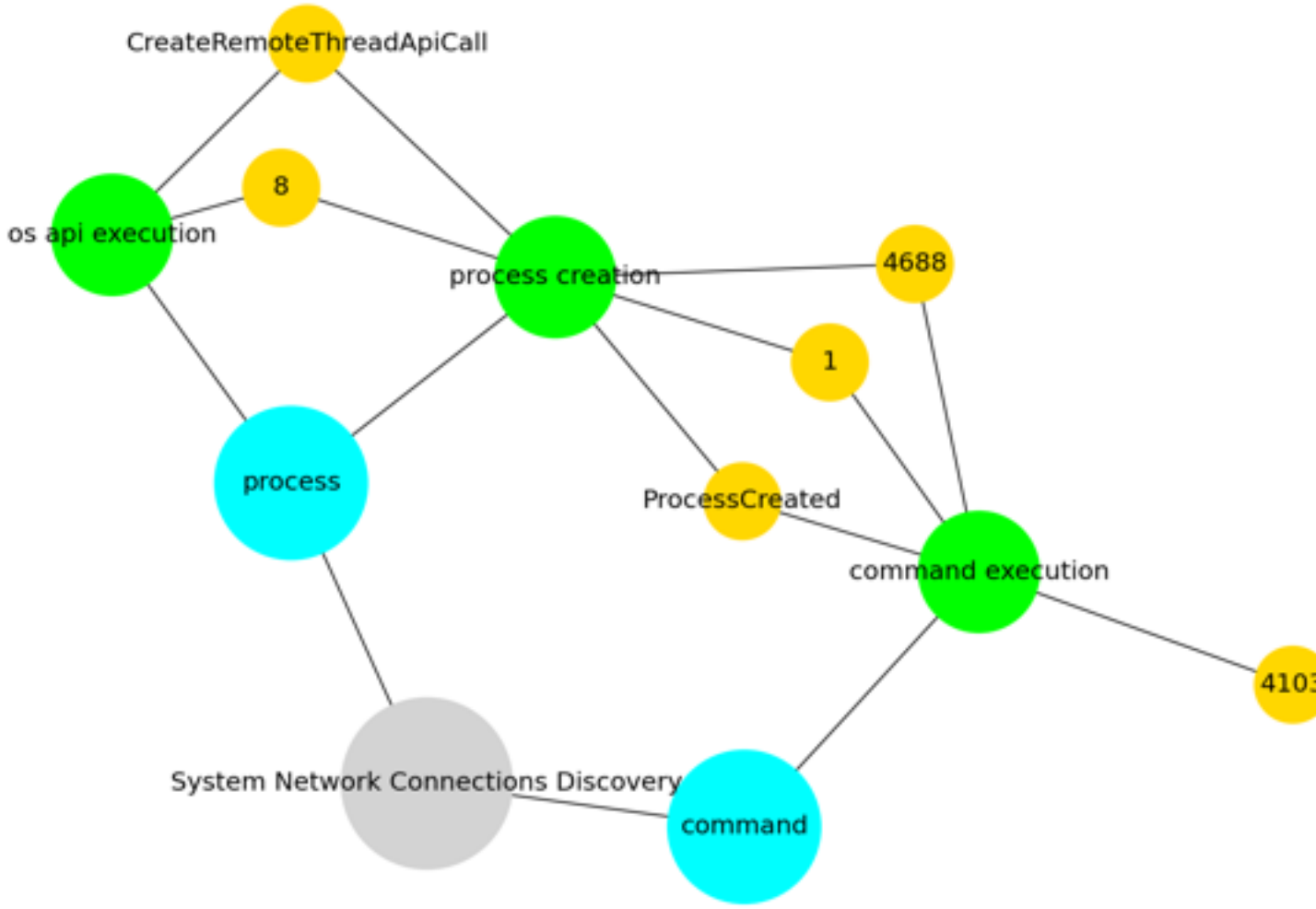
Tactic : discovery

Technique : System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services.

Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used.(Citation: US-CERT-TA18-106A)




## 3.19 T1053.005

Used by group : Fox Kitten, Operation Wocao, APT41, menuPass

Tactic : execution, persistence, privilege-escalation

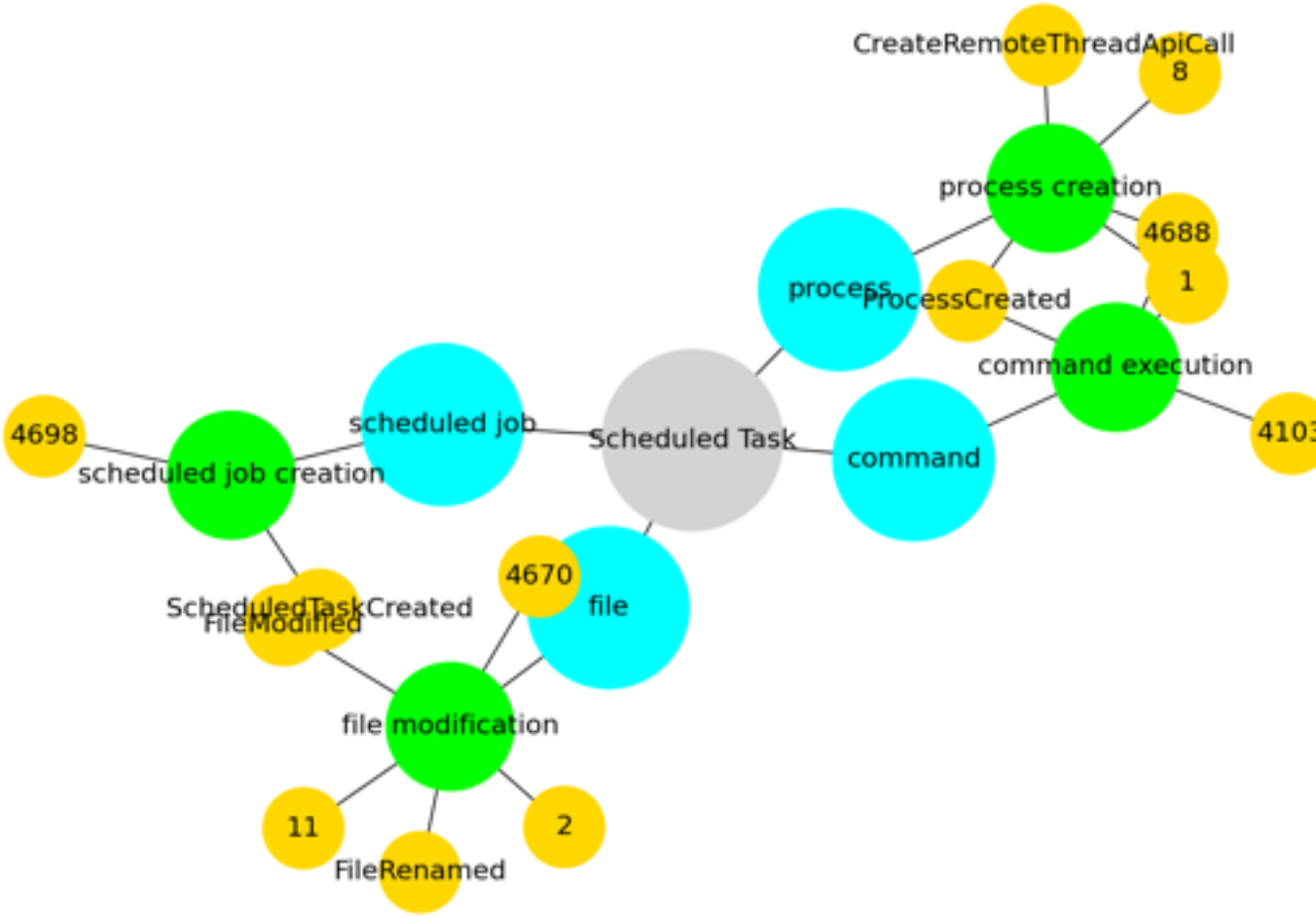
Technique : Scheduled Task

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task.

The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though <code>at.exe</code> can not access tasks created with

<code>schtasks</code> or the Control Panel.

An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent)




## 3.20 T1018

Used by group : Fox Kitten, Operation Wocao, menuPass, Deep Panda

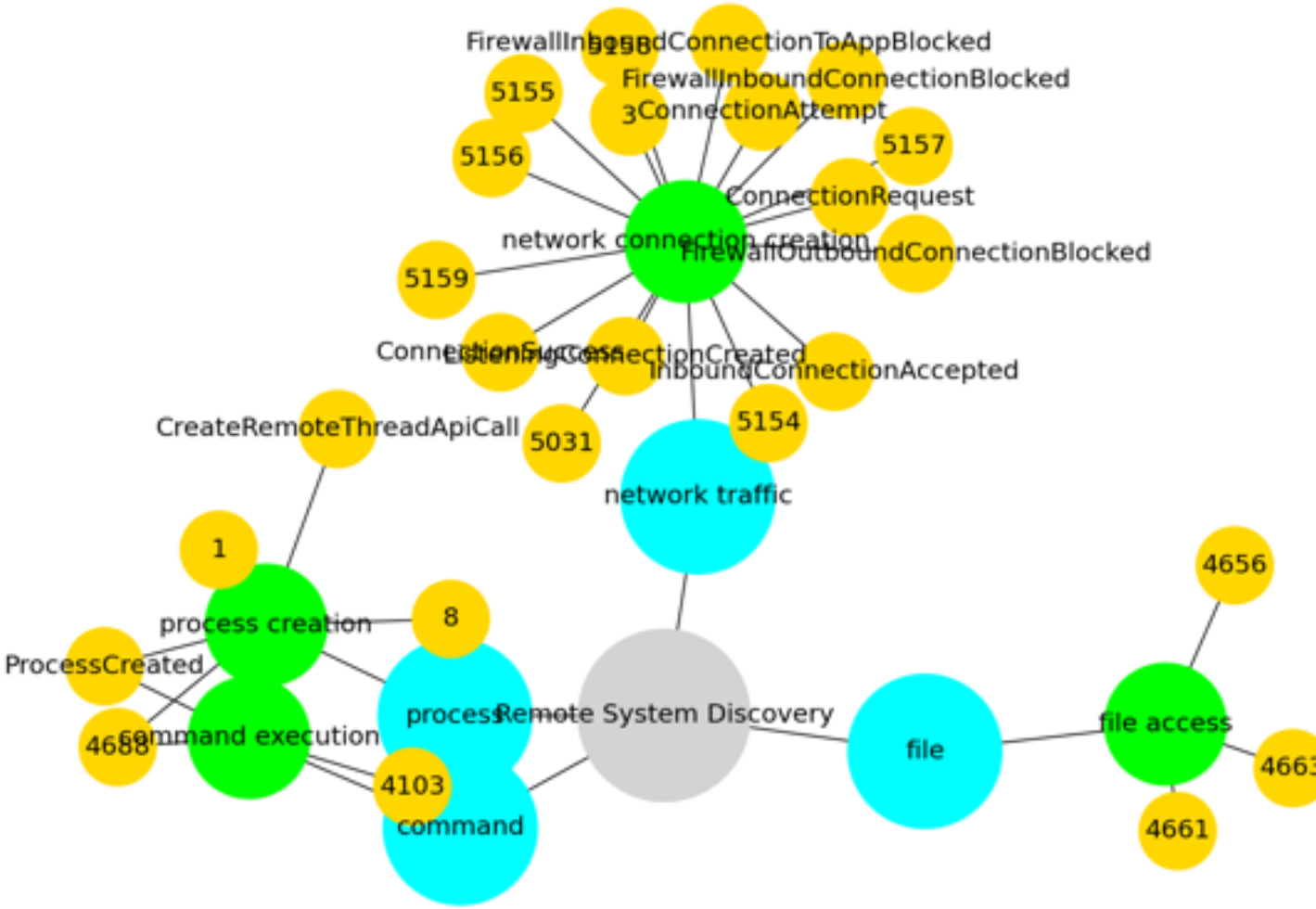
Tactic : discovery

Technique : Remote System Discovery

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or <code>net view</code> using [Net](https://attack.mitre.org/software/S0039).

Adversaries may also analyze data from local host files (ex: <code>C:\Windows\System32\Drivers\etc\hosts</code> or <code>/etc/hosts</code>) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment.

Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network.(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)




## 3.21 T1005

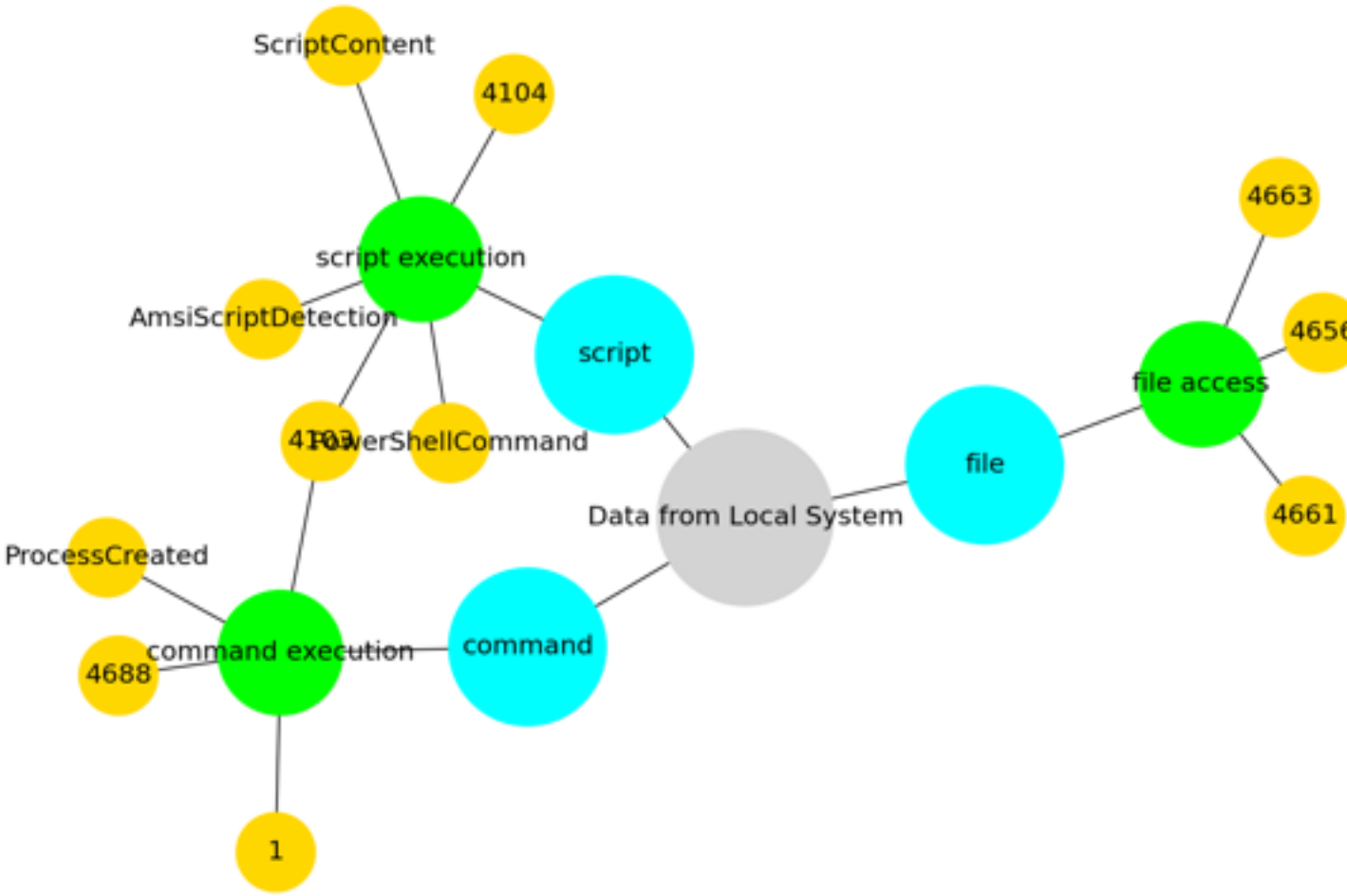
Used by group : Fox Kitten, Operation Wocao, APT41, menuPass

Tactic : collection

Technique : Data from Local System

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.

Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information. Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.



## 3.22 T1021.001

Used by group : Fox Kitten, APT41, Leviathan, menuPass

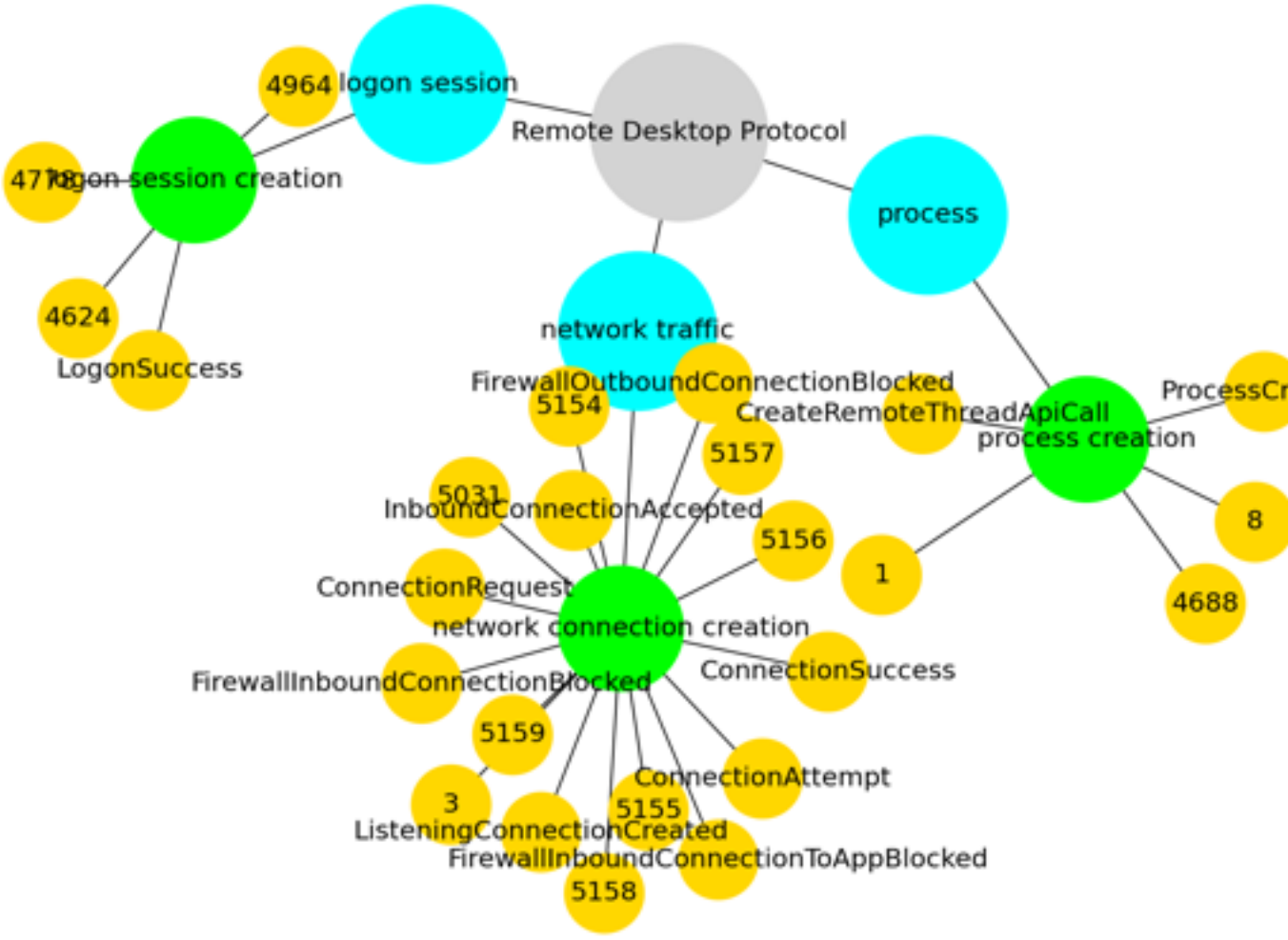
Tactic : lateral-movement

Technique : Remote Desktop Protocol

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)




## 3.23 T1016

Used by group : Operation Wocao, APT41, Tropic Trooper, menuPass

Tactic : discovery

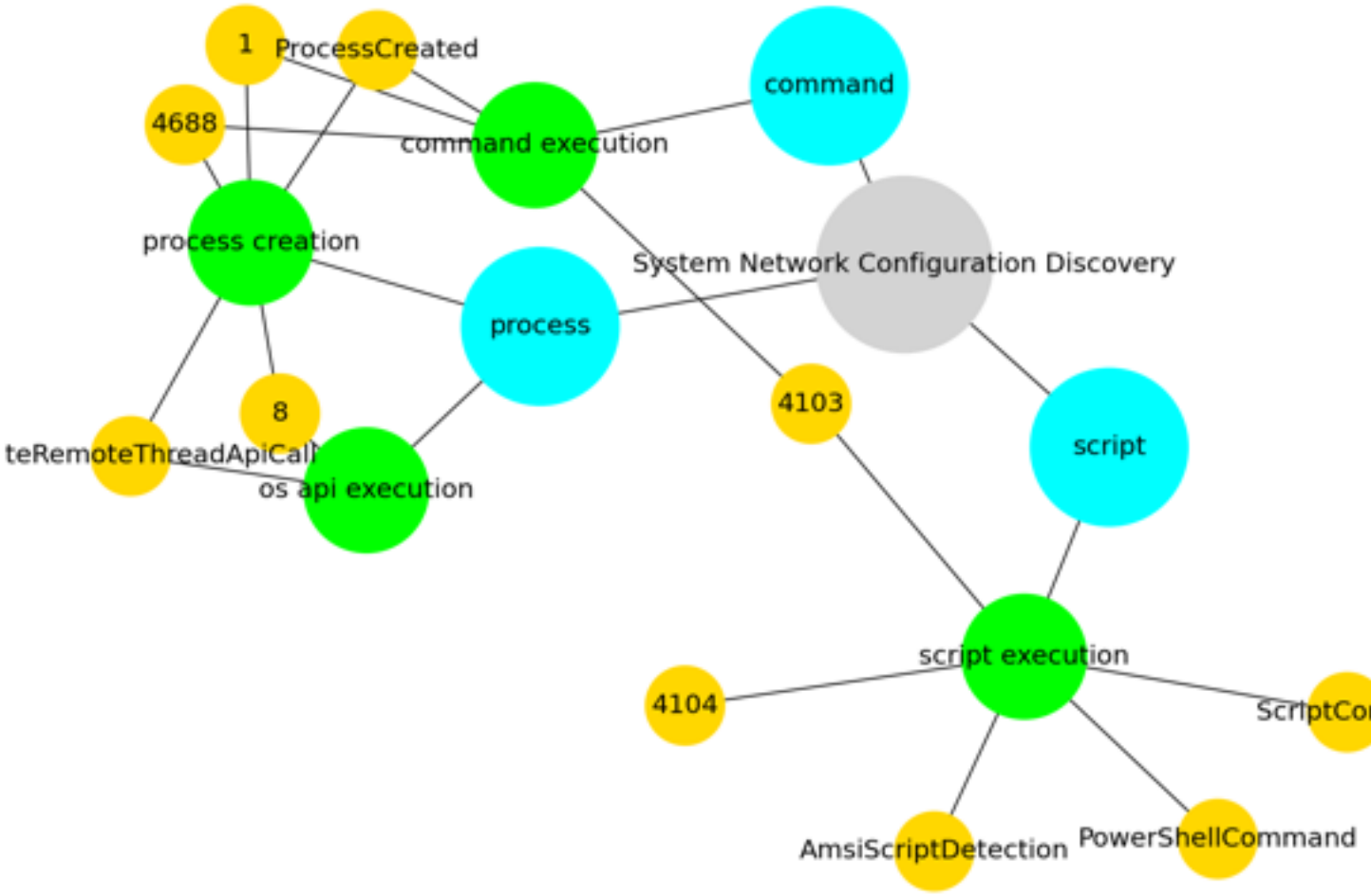
Technique : System Network Configuration Discovery

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103).

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes.(Citation:

US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion )

Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.




## 3.24 T1070.004

Used by group : Operation Wocao, APT41, Tropic Trooper, menuPass

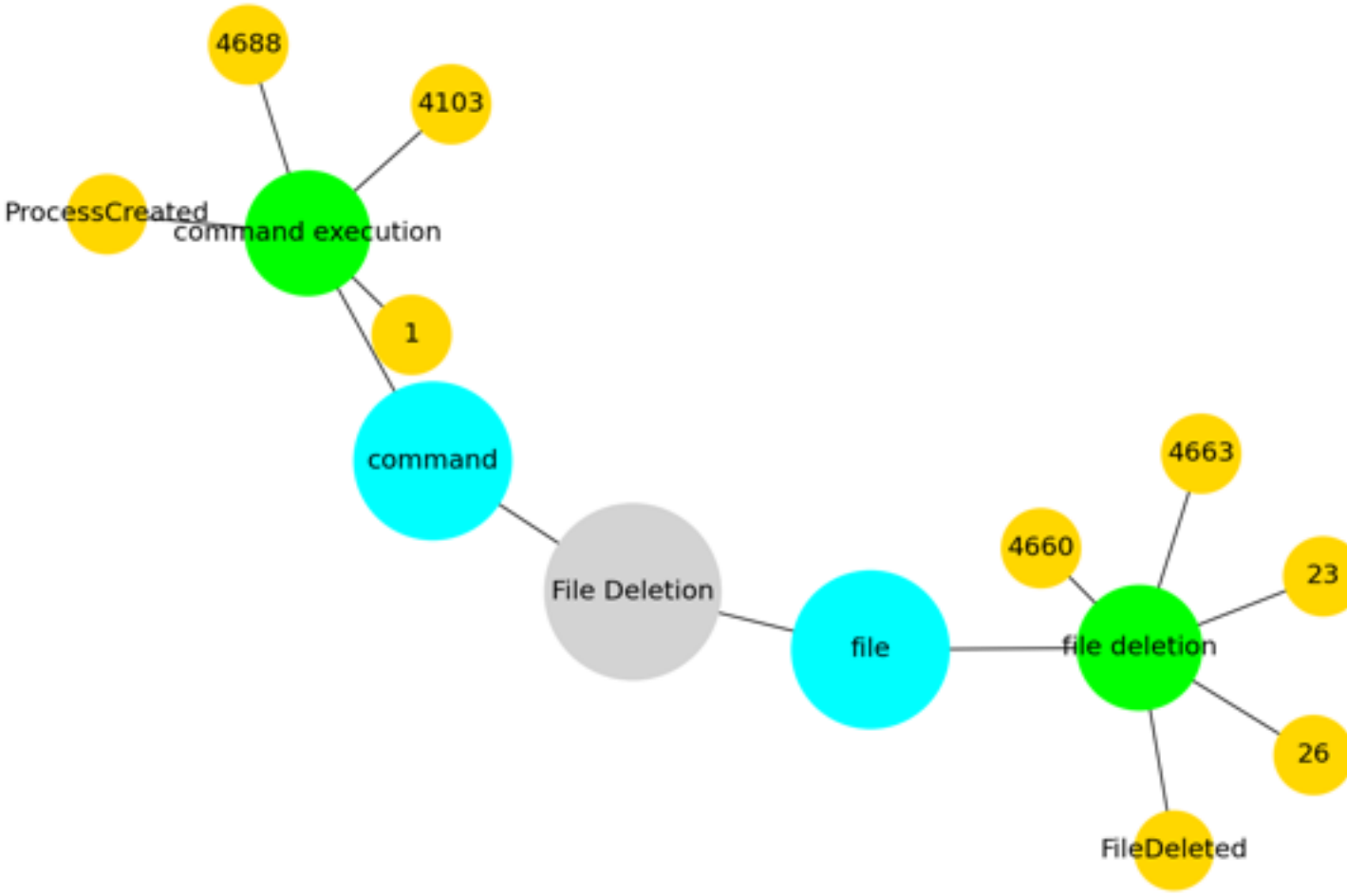
Tactic : defense-evasion

Technique : File Deletion

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) may leave traces to

indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) functions include <code>del</code> on Windows and <code>rm</code> or <code>unlink</code> on Linux and macOS.




## 3.25 T1071.001

Used by group : APT41, FIN4, Tropic Trooper, Orangeworm

Tactic : command-and-control

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.

## 3.26 T1560.001

Used by group : Fox Kitten, Operation Wocao, APT41, menuPass

Tactic : collection

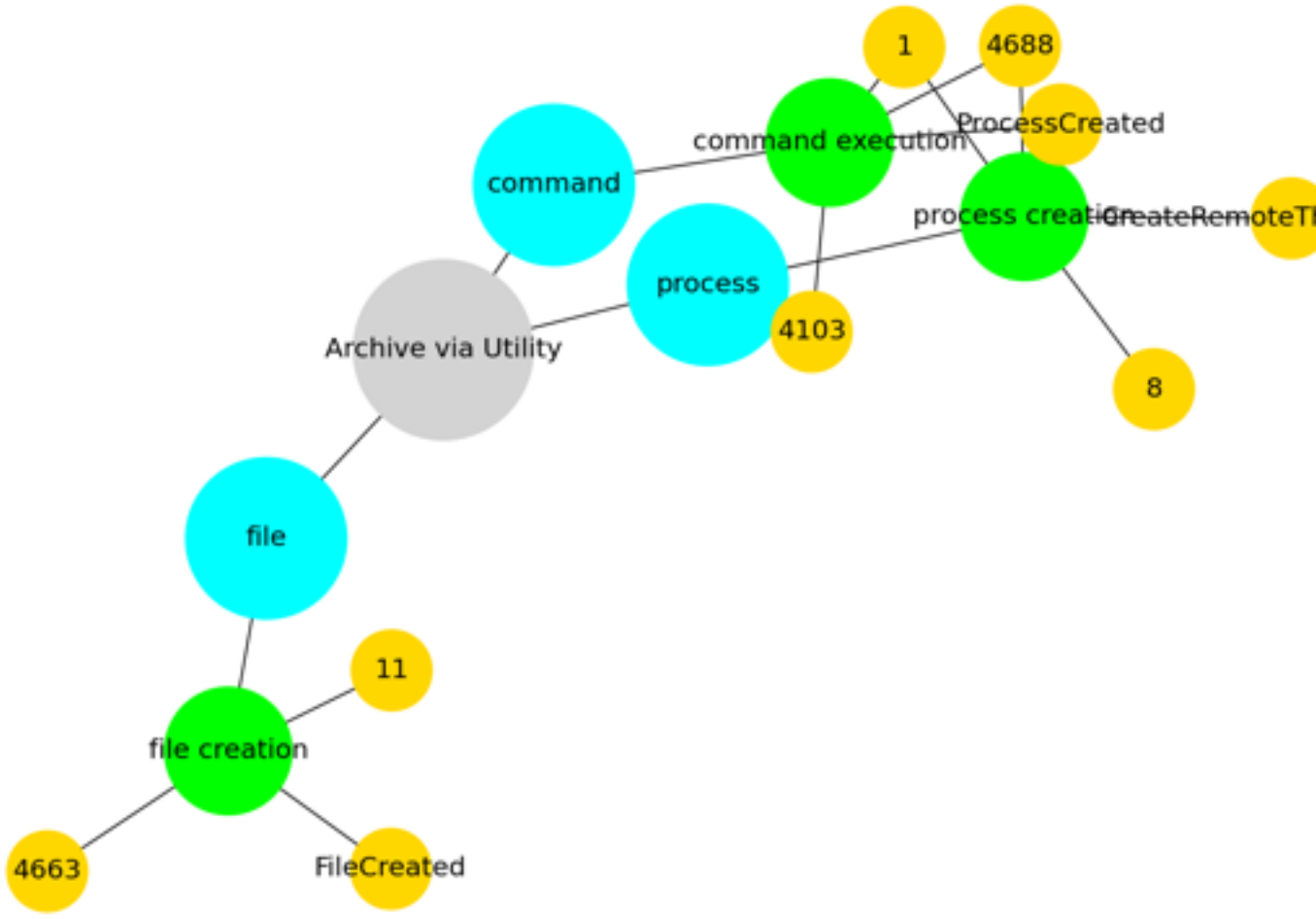
Technique : Archive via Utility

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to

compress, encrypt, or otherwise package data into a format that is easier/more secure to transport.

Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third party utilities may be preinstalled, such as <code>tar</code> on Linux and macOS or <code>zip</code> on Windows systems. On Windows, <code>diantz</code> or <code> makecab</code> may be used to package collected files into a cabinet (.cab) file. <code>diantz</code> may also be used to download and compress files from remote locations (i.e. [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002)).(Citation: diantz.exe_lolbas) Additionally, <code>xcopy</code> on Windows can copy files and directories with a variety of options.

Adversaries may use also third party utilities, such as 7-Zip, WinRAR, and WinZip, to perform similar activities.(Citation: 7zip Homepage)(Citation: WinRAR Homepage)(Citation: WinZip Homepage)




## 3.27 T1203

Used by group : Tonto Team, APT41, Tropic Trooper, Leviathan

Tactic : execution

Technique : Exploitation for Client Execution

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

### Browser-based Exploitation

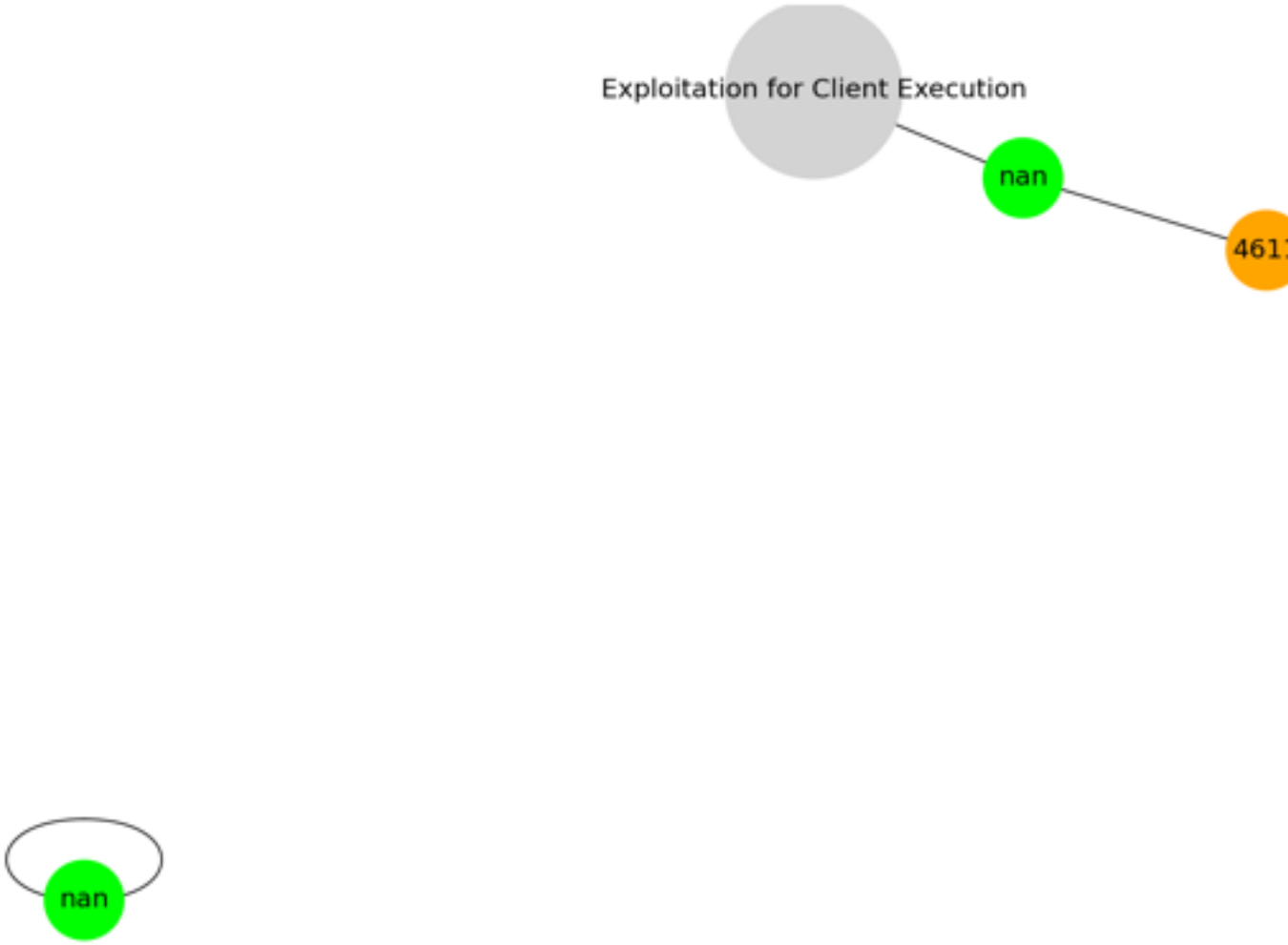
Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

### Office Applications

Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

### Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.




## 3.28 T1135

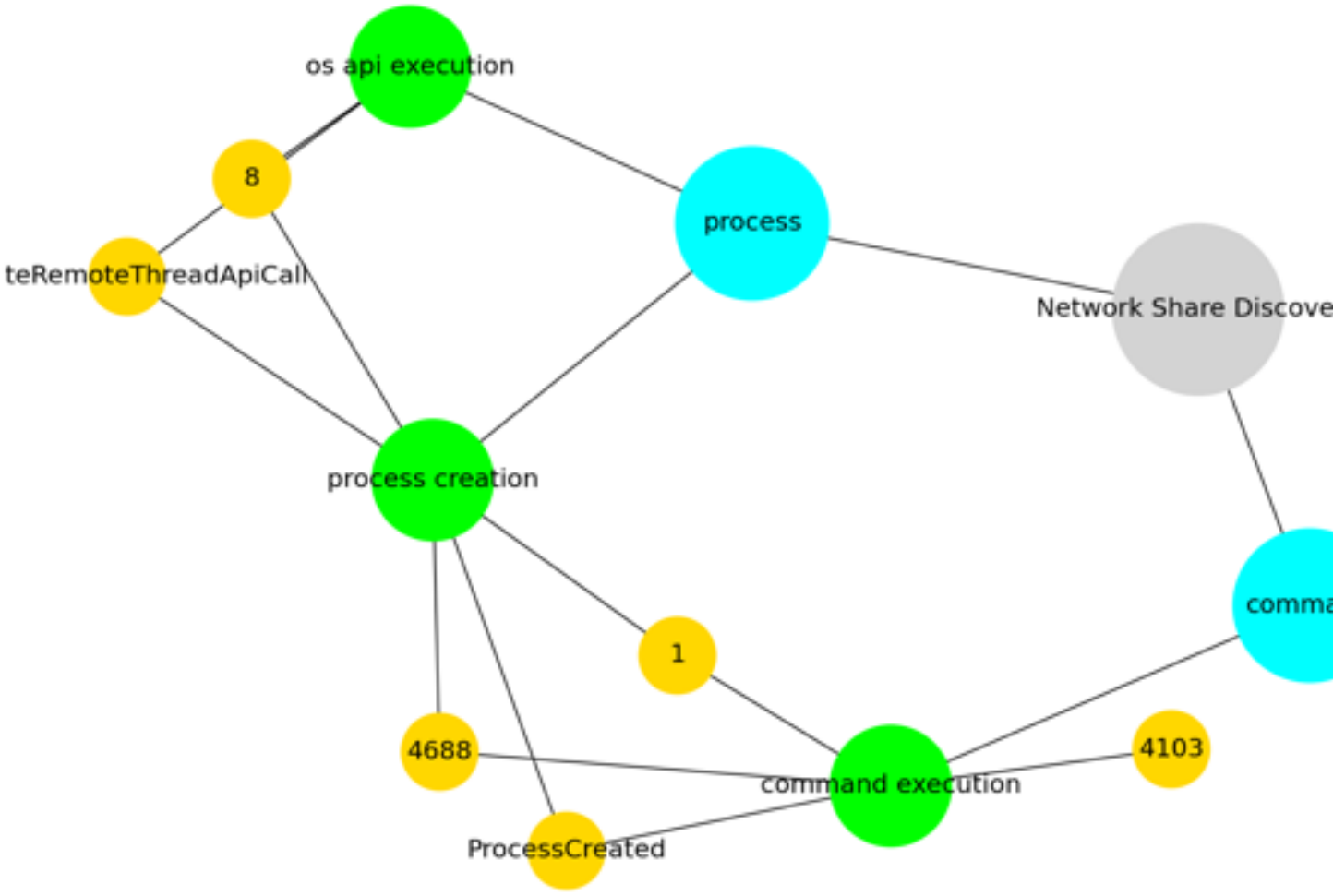
Used by group : Tonto Team, Operation Wocao, APT41, Tropic Trooper

Tactic : discovery

Technique : Network Share Discovery

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the <code>net view \\\\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>. For macOS, the <code>sharing -l</code> command lists all shared points used for smb services.




## 3.29 T1133

Used by group : Operation Wocao, APT41, Leviathan

Tactic : persistence, initial-access

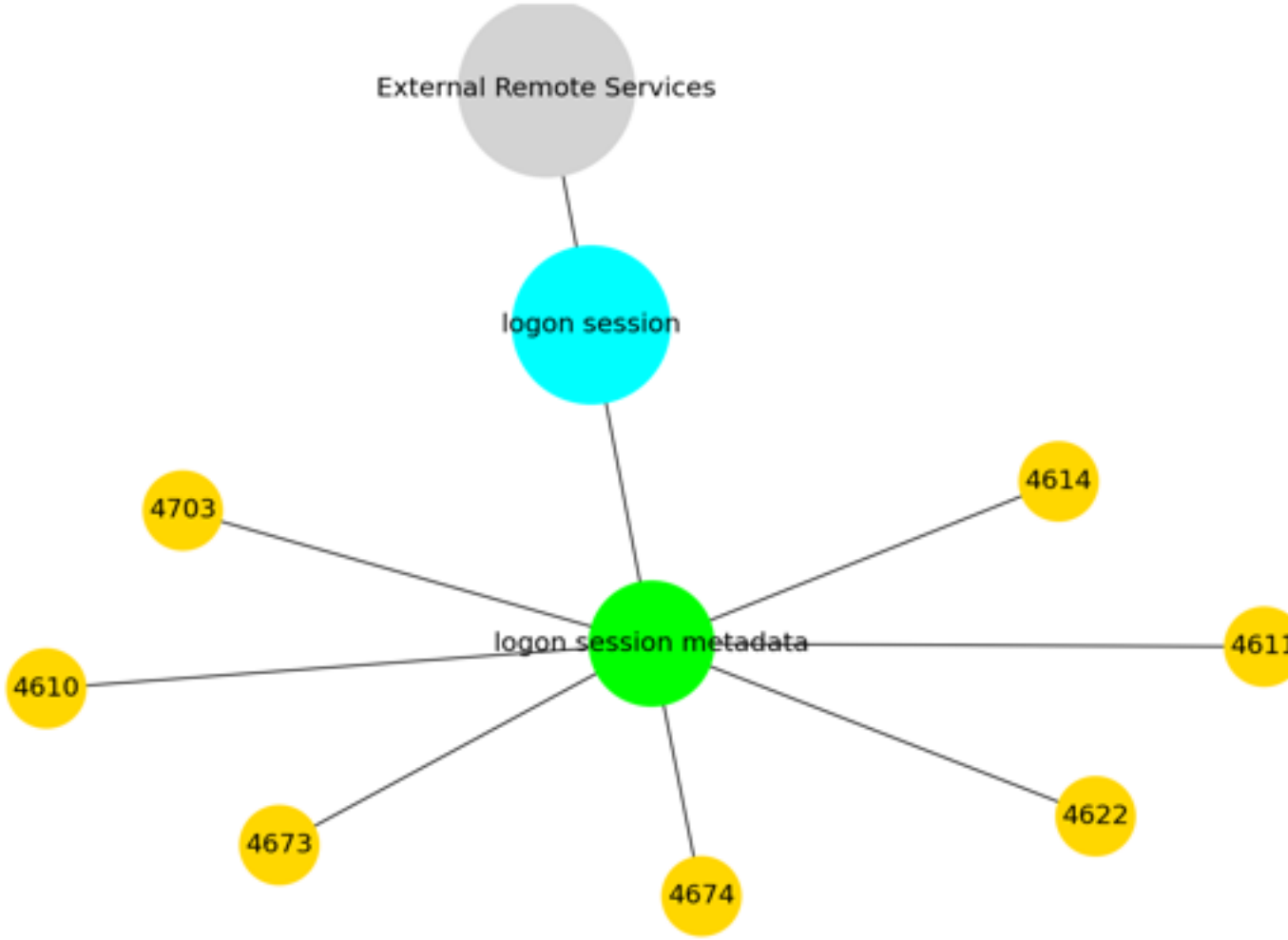
Technique : External Remote Services

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop)

Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be

obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)




## 3.30 T1106

Used by group : Operation Wocao, Tropic Trooper, menuPass

Tactic : execution

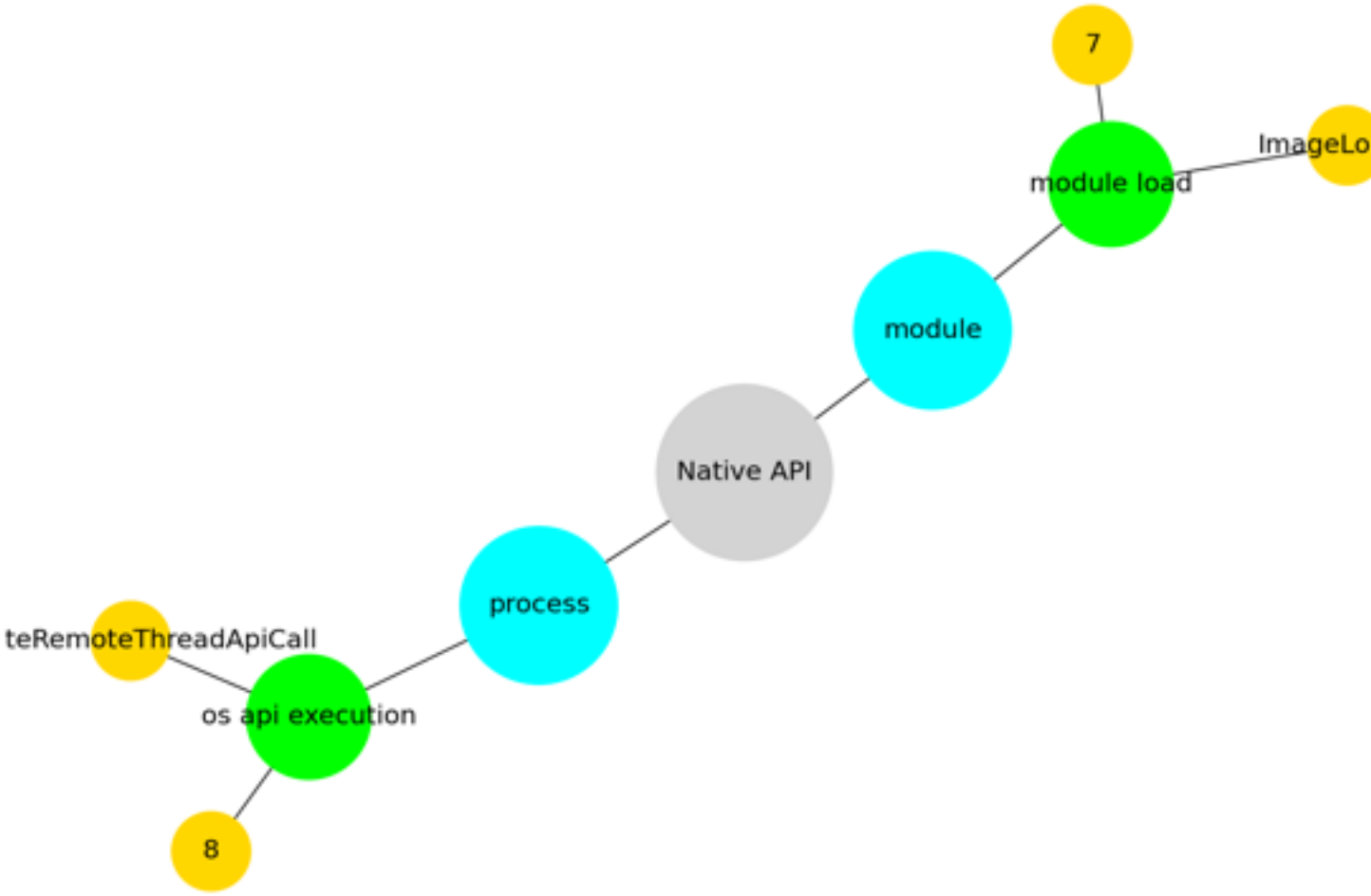
Technique : Native API

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

Native API functions (such as <code>NtCreateProcess</code>) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API <code>CreateProcess()</code> or GNU <code>fork()</code> will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC)

Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation)

Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).


7
ImageLo
module load
module
Native API
process
teRemoteThreadApiCall
os api execution
8

# 4. Annexes

< To be corrected or added in future releases >

## 4.1 List of all techniques used

| technique_id | tactic | technique | group |
|---|---|---|---|
| T1105 | command-and-control | Ingress Tool Transfer | Tonto Team, Fox Kitten, Operation Wocao, Whitefly, APT41, Tropic Trooper, Leviathan, menuPass |
| T1059.001 | execution | PowerShell | Tonto Team, Fox Kitten, Operation Wocao, APT41, Leviathan, menuPass, Deep Panda |
| T1027 | defense-evasion | Obfuscated Files or Information | Fox Kitten, Operation Wocao, Whitefly, APT41, Tropic Trooper, Leviathan, menuPass |
| T1204.002 | execution | Malicious File | Tonto Team, Whitefly, FIN4, Tropic Trooper, Leviathan, menuPass |
| T1566.001 | initial-access | Spearphishing Attachment | Tonto Team, APT41, FIN4, Tropic Trooper, Leviathan, menuPass |
| T1505.003 | persistence | Web Shell | Tonto Team, Fox Kitten, Operation Wocao, Tropic Trooper, Leviathan, Deep Panda |
| T1078 | defense-evasion, persistence, privilege-escalation, initial-access | Valid Accounts | Fox Kitten, Operation Wocao, APT41, FIN4, Leviathan, menuPass |
| T1046 | discovery | Network Service Discovery | Fox Kitten, Operation Wocao, APT41, Tropic Trooper, menuPass |
| T1036.005 | defense-evasion | Match Legitimate Name or Location | Fox Kitten, Whitefly, APT41, Tropic Trooper, menuPass |
| T1059.003 | execution | Windows Command Shell | Fox Kitten, Operation Wocao, APT41, Tropic Trooper, menuPass |
| T1047 | execution | Windows Management Instrumentation | Operation Wocao, APT41, Leviathan, menuPass, Deep Panda |
| T1083 | discovery | File and Directory Discovery | Fox Kitten, Operation Wocao, APT41, Tropic Trooper, menuPass |
| T1021.002 | lateral-movement | SMB/Windows Admin Shares | Fox Kitten, Operation Wocao, APT41, Orangeworm, Deep Panda |
| T1003.001 | credential-access | LSASS Memory | Fox Kitten, Operation Wocao, Whitefly, APT41, Leviathan |
| T1056.001 | collection, credential-access | Keylogging | Tonto Team, Operation Wocao, APT41, FIN4, menuPass |
| T1574.001 | persistence, privilege-escalation, defense-evasion | DLL Search Order Hijacking | Tonto Team, Whitefly, APT41, menuPass |
| T1190 | initial-access | Exploit Public-Facing Application | Fox Kitten, Operation Wocao, APT41, menuPass |
| T1049 | discovery | System Network Connections Discovery | Operation Wocao, APT41, Tropic Trooper, menuPass |
| T1053.005 | execution, persistence, privilege-escalation | Scheduled Task | Fox Kitten, Operation Wocao, APT41, menuPass |
| T1018 | discovery | Remote System Discovery | Fox Kitten, Operation Wocao, menuPass, Deep Panda |
| T1005 | collection | Data from Local System | Fox Kitten, Operation Wocao, APT41, menuPass |
| T1021.001 | lateral-movement | Remote Desktop Protocol | Fox Kitten, APT41, Leviathan, menuPass |
| T1016 | discovery | System Network Configuration Discovery | Operation Wocao, APT41, Tropic Trooper, menuPass |
| T1070.004 | defense-evasion | File Deletion | Operation Wocao, APT41, Tropic Trooper, menuPass |
| T1071.001 | command-and-control | Web Protocols | APT41, FIN4, Tropic Trooper, Orangeworm |
| T1560.001 | collection | Archive via Utility | Fox Kitten, Operation Wocao, APT41, menuPass |
| T1203 | execution | Exploitation for Client Execution | Tonto Team, APT41, Tropic Trooper, Leviathan |
| T1135 | discovery | Network Share Discovery | Tonto Team, Operation Wocao, APT41, Tropic Trooper |
| T1133 | persistence, initial-access | External Remote Services | Operation Wocao, APT41, Leviathan |
| T1106 | execution | Native API | Operation Wocao, Tropic Trooper, menuPass |
| T1090.003 | command-and-control | Multi-hop Proxy | Operation Wocao, FIN4, Leviathan |
| T1210 | lateral-movement | Exploitation of Remote Services | Tonto Team, Fox Kitten, menuPass |
| T1119 | collection | Automated Collection | Operation Wocao, Tropic Trooper, menuPass |
| T1074.001 | collection | Local Data Staging | Operation Wocao, Leviathan, menuPass |
| T1547.001 | persistence, privilege-escalation | Registry Run Keys / Startup Folder | APT41, Tropic Trooper, Leviathan |
| T1090 | command-and-control | Proxy | Fox Kitten, Operation Wocao, APT41 |
| T1057 | discovery | Process Discovery | Operation Wocao, Tropic Trooper, Deep Panda |
| T1553.002 | defense-evasion | Code Signing | APT41, Leviathan, menuPass |
| T1140 | defense-evasion | Deobfuscate/Decode Files or Information | Tropic Trooper, Leviathan, menuPass |
| T1546.008 | privilege-escalation, persistence | Accessibility Features | Fox Kitten, APT41, Deep Panda |
| T1033 | discovery | System Owner/User Discovery | Operation Wocao, APT41, Tropic Trooper |

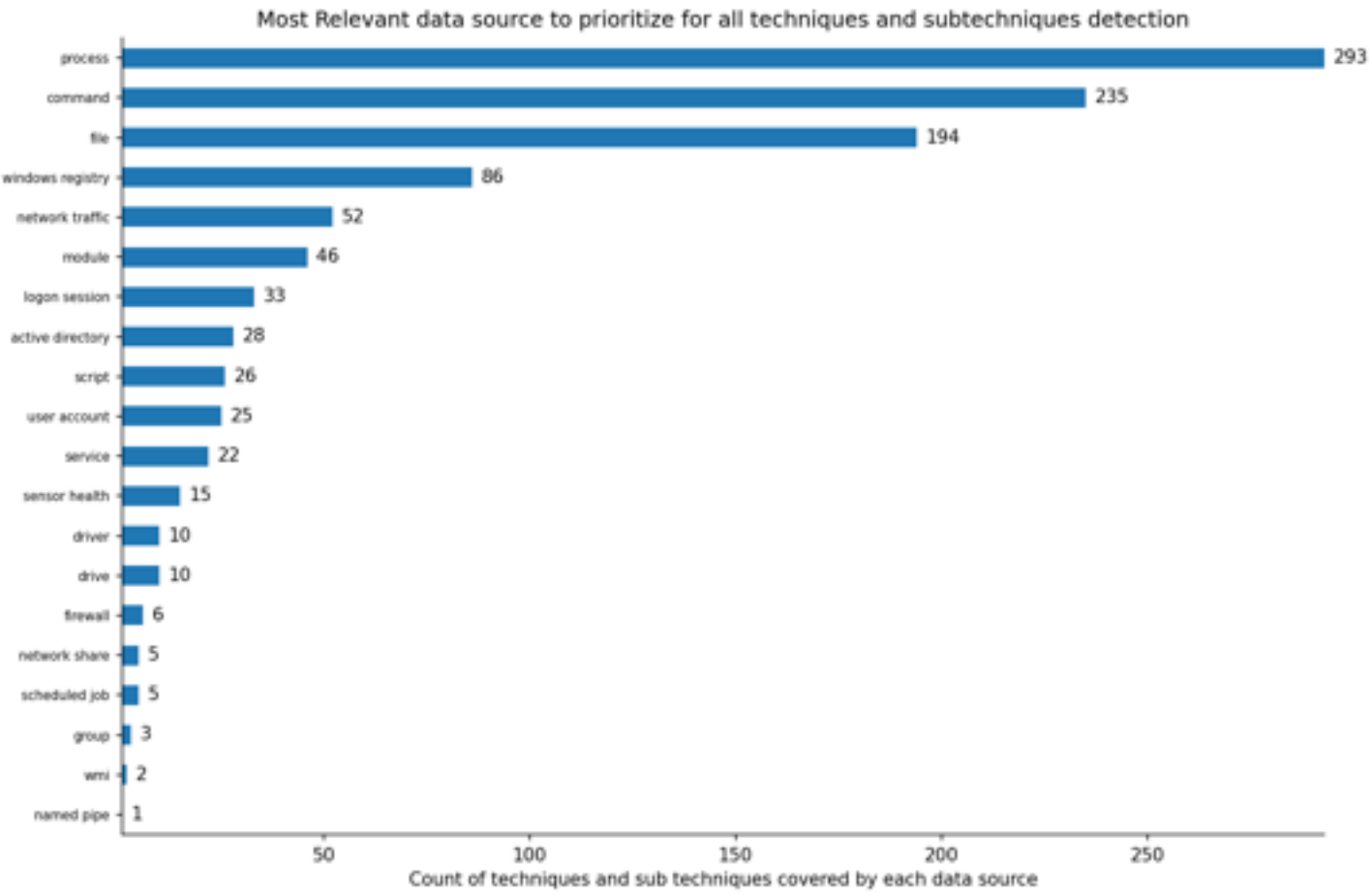
| | | | |
|---|---|---|---|
| T1059.005 | execution | Visual Basic | Operation Wocao, FIN4, Leviathan |
| T1588.002 | resource-development | Tool | Whitefly, APT41, menuPass |
| T1087.002 | discovery | Domain Account | Fox Kitten, Operation Wocao, menuPass |
| T1574.002 | persistence, privilege-escalation, defense-evasion | DLL Side-Loading | APT41, Tropic Trooper, menuPass |
| T1021.004 | lateral-movement | SSH | Fox Kitten, Leviathan, menuPass |
| T1583.001 | resource-development | Domains | Leviathan, menuPass |
| T1074.002 | collection | Remote Data Staging | Leviathan, menuPass |
| T1518 | discovery | Software Discovery | Operation Wocao, Tropic Trooper |
| T1070.001 | defense-evasion | Clear Windows Event Logs | Operation Wocao, APT41 |
| T1112 | defense-evasion | Modify Registry | Operation Wocao, APT41 |
| T1027.003 | defense-evasion | Steganography | Tropic Trooper, Leviathan |
| T1197 | defense-evasion, persistence | BITS Jobs | APT41, Leviathan |
| T1543.003 | persistence, privilege-escalation | Windows Service | APT41, Tropic Trooper |
| T1082 | discovery | System Information Discovery | Operation Wocao, Tropic Trooper |
| T1071.004 | command-and-control | DNS | APT41, Tropic Trooper |
| T1055 | defense-evasion, privilege-escalation | Process Injection | Operation Wocao, APT41 |
| T1070.003 | defense-evasion | Clear Command History | APT41, menuPass |
| T1055.001 | defense-evasion, privilege-escalation | Dynamic-link Library Injection | Tropic Trooper, Leviathan |
| T1041 | exfiltration | Exfiltration Over C2 Channel | Operation Wocao, Leviathan |
| T1560 | collection | Archive Collected Data | Leviathan, menuPass |
| T1090.002 | command-and-control | External Proxy | Tonto Team, menuPass |
| T1078.003 | defense-evasion, persistence, privilege-escalation, initial-access | Local Accounts | Operation Wocao, Tropic Trooper |
| T1036.004 | defense-evasion | Masquerade Task or Service | Fox Kitten, APT41 |
| T1012 | discovery | Query Registry | Fox Kitten, Operation Wocao |
| T1069.001 | discovery | Local Groups | Tonto Team, Operation Wocao |
| T1059.006 | execution | Python | Tonto Team, Operation Wocao |
| T1068 | privilege-escalation | Exploitation for Privilege Escalation | Tonto Team, Whitefly |
| T1003 | credential-access | OS Credential Dumping | Tonto Team, Leviathan |
| T1555.005 | credential-access | Password Managers | Fox Kitten, Operation Wocao |
| T1585.001 | resource-development | Social Media Accounts | Fox Kitten, Leviathan |
| T1572 | command-and-control | Protocol Tunneling | Fox Kitten, Leviathan |
| T1003.003 | credential-access | NTDS | Fox Kitten, menuPass |
| T1136.001 | persistence | Local Account | Fox Kitten, APT41 |
| T1059 | execution | Command and Scripting Interpreter | Fox Kitten, Whitefly |
| T1039 | collection | Data from Network Shared Drive | Fox Kitten, menuPass |
| T1566.002 | initial-access | Spearphishing Link | FIN4, Leviathan |
| T1027.005 | defense-evasion | Indicator Removal from Tools | Operation Wocao, Deep Panda |
| T1518.001 | discovery | Security Software Discovery | Operation Wocao, Tropic Trooper |
| T1218.010 | defense-evasion | Regsvr32 | Leviathan, Deep Panda |
| T1569.002 | execution | Service Execution | Operation Wocao, APT41 |
| T1573.002 | command-and-control | Asymmetric Cryptography | Operation Wocao, Tropic Trooper |
| T1204.001 | execution | Malicious Link | FIN4, Leviathan |
| T1132.001 | command-and-control | Standard Encoding | Tropic Trooper |
| T1052.001 | exfiltration | Exfiltration over USB | Tropic Trooper |
| T1573 | command-and-control | Encrypted Channel | Tropic Trooper |
| T1547.009 | persistence, privilege-escalation | Shortcut Modification | Leviathan |
| T1056.002 | collection, credential-access | GUI Input Capture | FIN4 |
| T1546.003 | privilege-escalation, persistence | Windows Management Instrumentation Event Subscription | Leviathan |
| T1114.002 | collection | Remote Email Collection | FIN4 |
| T1567.002 | exfiltration | Exfiltration to Cloud Storage | Leviathan |

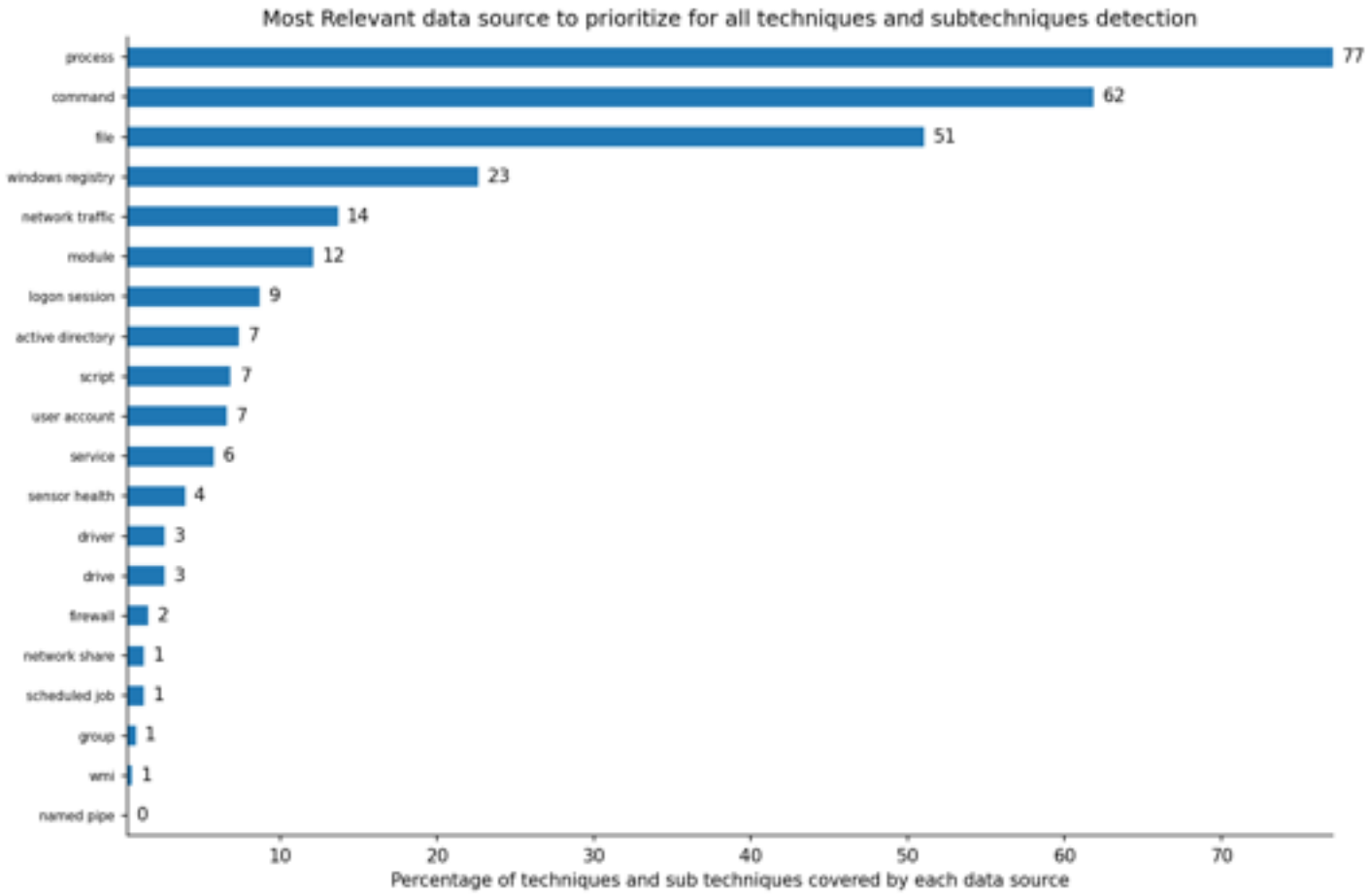
| | | | |
|---|---|---|---|
| T1547.004 | persistence, privilege-escalation | Winlogon Helper DLL | Tropic Trooper |
| T1036 | defense-evasion | Masquerading | menuPass |
| T1221 | defense-evasion | Template Injection | Tropic Trooper |
| T1564.001 | defense-evasion | Hidden Files and Directories | Tropic Trooper |
| T1199 | initial-access | Trusted Relationship | menuPass |
| T1091 | lateral-movement, initial-access | Replication Through Removable Media | Tropic Trooper |
| T1218.004 | defense-evasion | InstallUtil | menuPass |
| T1189 | initial-access | Drive-by Compromise | Leviathan |
| T1568.001 | command-and-control | Fast Flux DNS | menuPass |
| T1003.004 | credential-access | LSA Secrets | menuPass |
| T1003.002 | credential-access | Security Account Manager | menuPass |
| T1036.003 | defense-evasion | Rename System Utilities | menuPass |
| T1102.003 | command-and-control | One-Way Communication | Leviathan |
| T1585.002 | resource-development | Email Accounts | Leviathan |
| T1020 | exfiltration | Automated Exfiltration | Tropic Trooper |
| T1586.001 | resource-development | Social Media Accounts | Leviathan |
| T1559.002 | execution | Dynamic Data Exchange | Leviathan |
| T1586.002 | resource-development | Email Accounts | Leviathan |
| T1055.012 | defense-evasion, privilege-escalation | Process Hollowing | menuPass |
| T1589.001 | reconnaissance | Credentials | Leviathan |
| T1534 | lateral-movement | Internal Spearphishing | Leviathan |
| T1027.001 | defense-evasion | Binary Padding | Leviathan |
| T1095 | command-and-control | Non-Application Layer Protocol | Operation Wocao |
| T1564.008 | defense-evasion | Email Hiding Rules | FIN4 |
| T1008 | command-and-control | Fallback Channels | APT41 |
| T1124 | discovery | System Time Discovery | Operation Wocao |
| T1552.004 | credential-access | Private Keys | Operation Wocao |
| T1558.003 | credential-access | Kerberoasting | Operation Wocao |
| T1003.006 | credential-access | DCSync | Operation Wocao |
| T1562.004 | defense-evasion | Disable or Modify System Firewall | Operation Wocao |
| T1570 | lateral-movement | Lateral Tool Transfer | Operation Wocao |
| T1078.002 | defense-evasion, persistence, privilege-escalation, initial-access | Domain Accounts | Operation Wocao |
| T1090.001 | command-and-control | Internal Proxy | Operation Wocao |
| T1102 | command-and-control | Web Service | Fox Kitten |
| T1110 | credential-access | Brute Force | Fox Kitten |
| T1217 | discovery | Browser Bookmark Discovery | Fox Kitten |
| T1213 | collection | Data from Information Repositories | Fox Kitten |
| T1530 | collection | Data from Cloud Storage Object | Fox Kitten |
| T1552.001 | credential-access | Credentials In Files | Fox Kitten |
| T1021.005 | lateral-movement | VNC | Fox Kitten |
| T1087.001 | discovery | Local Account | Fox Kitten |
| T1585 | resource-development | Establish Accounts | Fox Kitten |
| T1120 | discovery | Peripheral Device Discovery | Operation Wocao |
| T1115 | collection | Clipboard Data | Operation Wocao |
| T1111 | credential-access | Multi-Factor Authentication Interception | Operation Wocao |
| T1110.002 | credential-access | Password Cracking | APT41 |
| T1014 | defense-evasion | Rootkit | APT41 |
| T1104 | command-and-control | Multi-Stage Channels | APT41 |
| T1486 | impact | Data Encrypted for Impact | APT41 |
| T1496 | impact | Resource Hijacking | APT41 |

| | | | |
|---|---|---|---|
| T1542.003 | persistence, defense-evasion | Bootkit | APT41 |
| T1218.011 | defense-evasion | Rundll32 | APT41 |
| T1218.001 | defense-evasion | Compiled HTML File | APT41 |
| T1059.004 | execution | Unix Shell | APT41 |
| T1007 | discovery | System Service Discovery | Operation Wocao |
| T1568.002 | command-and-control | Domain Generation Algorithms | APT41 |
| T1195.002 | initial-access | Compromise Software Supply Chain | APT41 |
| T1574.006 | persistence, privilege-escalation, defense-evasion | Dynamic Linker Hijacking | APT41 |
| T1102.001 | command-and-control | Dead Drop Resolver | APT41 |
| T1071.002 | command-and-control | File Transfer Protocols | APT41 |
| T1480.001 | defense-evasion | Environmental Keying | APT41 |
| T1001 | command-and-control | Data Obfuscation | Operation Wocao |
| T1564.003 | defense-evasion | Hidden Window | Deep Panda |

## 4.2 Data sources reference for covering all mitre technique

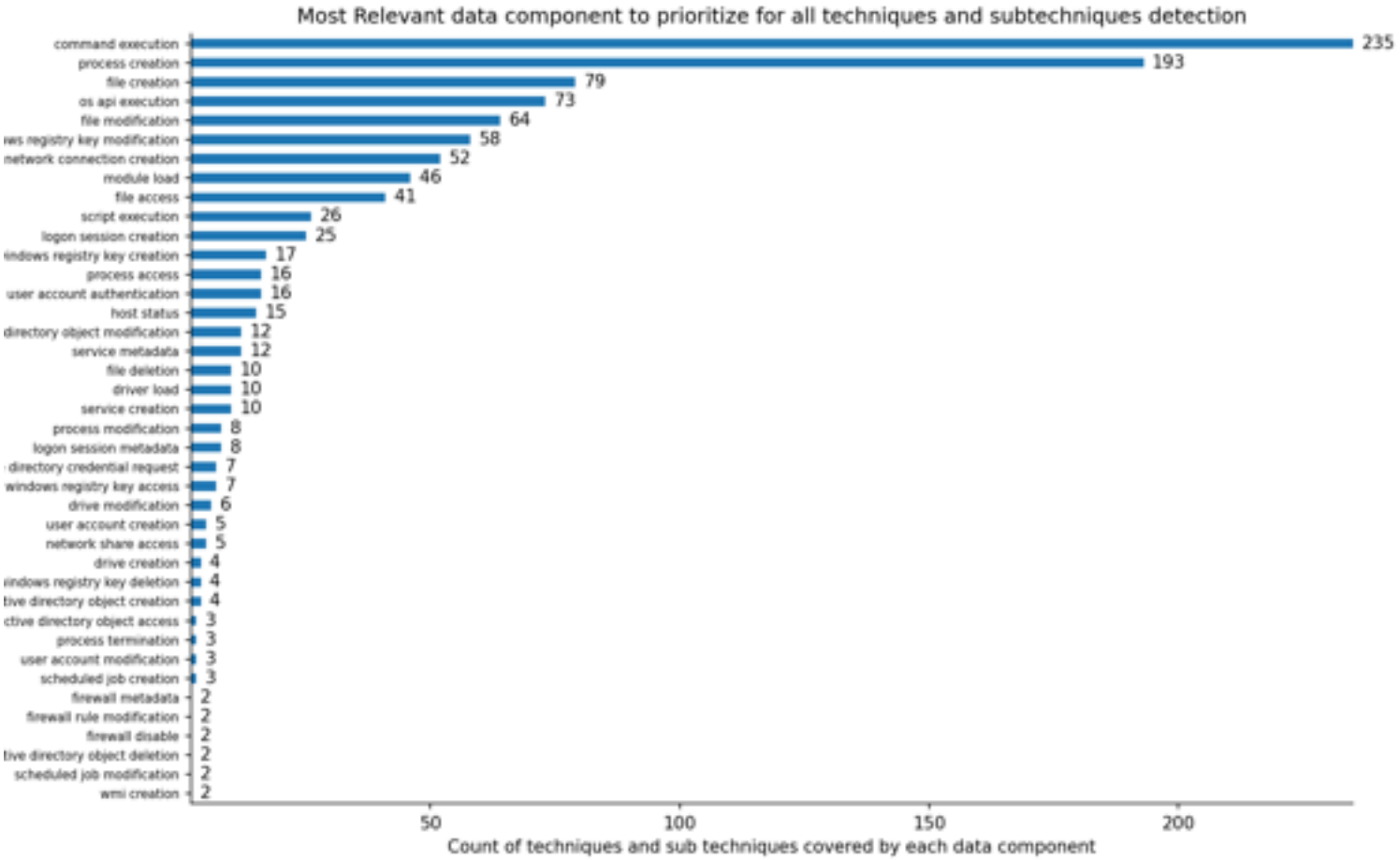
< To be corrected or added in future releases >

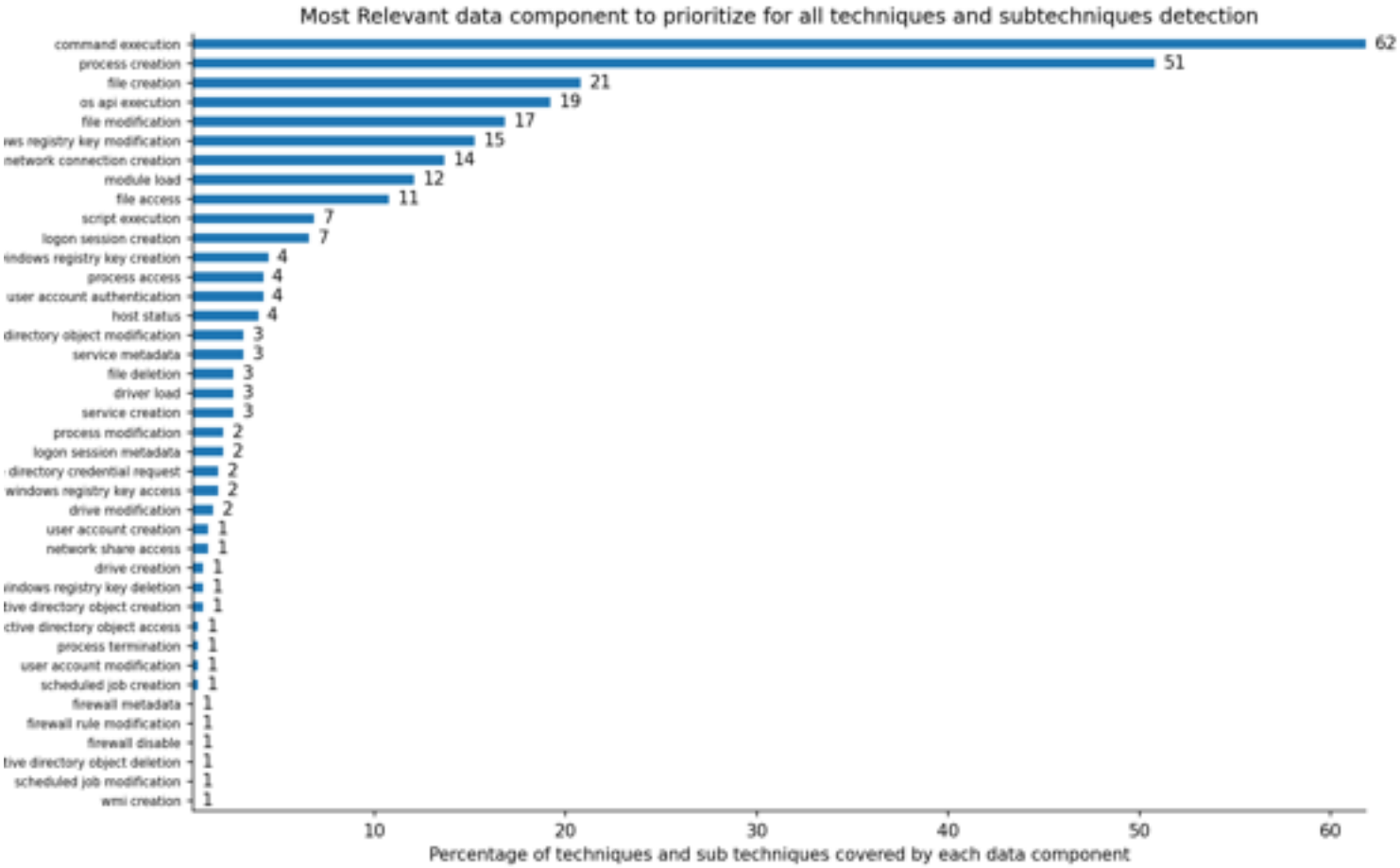





## 4.3 Data component reference for covering all mitre technique

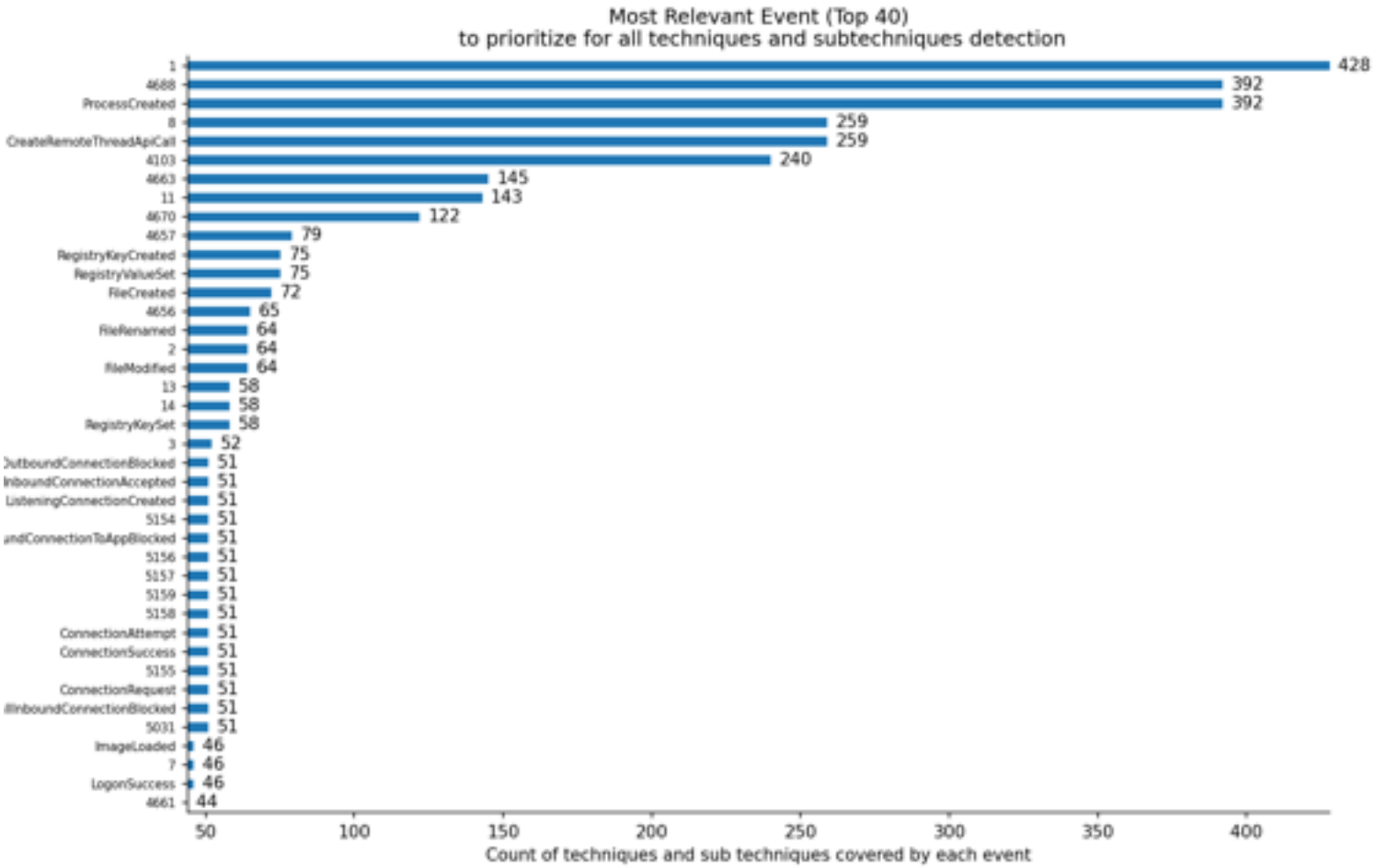
< To be corrected or added in future releases >

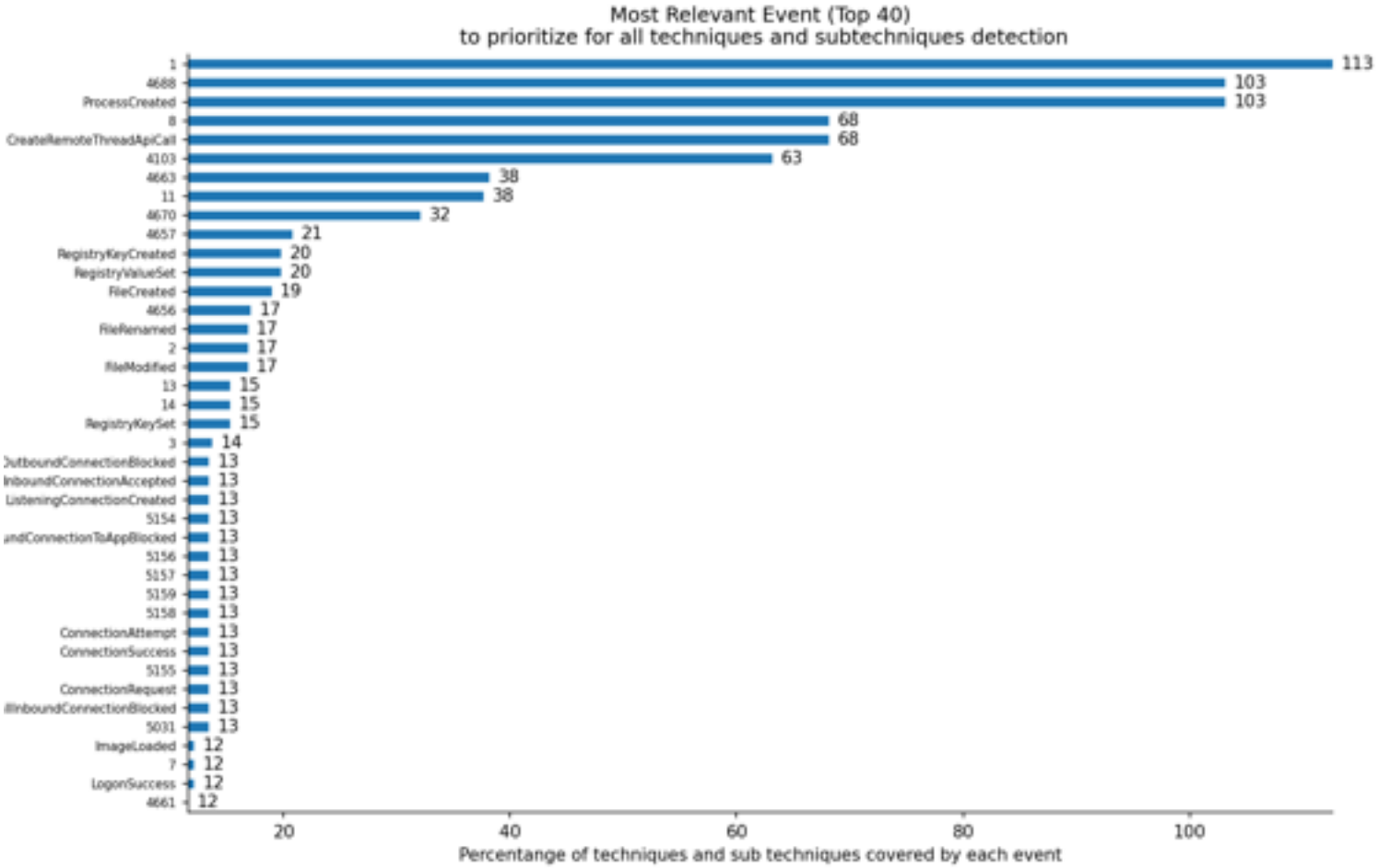

Most Relevant data component to prioritize for all techniques and subtechniques detection
command execution 235
process creation 193
file creation 79
os api execution 73
file modification 64
ws registry key modification 58
network connection creation 52
module load 46
file access 41
script execution 26
logon session creation 25
indows registry key creation 17
process access 16
user account authentication 16
host status 15
directory object modification 12
service metadata 12
file deletion 10
driver load 10
service creation 10
process modification 8
logon session metadata 8
directory credential request 7
windows registry key access 7
drive modification 6
user account creation 5
network share access 5
drive creation 4
indows registry key deletion 4
tive directory object creation 4
ctive directory object access 3
process termination 3
user account modification 3
scheduled job creation 3
firewall metadata 2
firewall rule modification 2
firewall disable 2
tive directory object deletion 2
scheduled job modification 2
wmi creation 2
50
100
150
200
Count of techniques and sub techniques covered by each data component




## 4.4 Event reference for covering all mitre technique

< To be corrected or added in future releases >


Most Relevant Event (Top 40)
to prioritize for all techniques and subtechniques detection
1
4688
ProcessCreated
8
CreateRemoteThreadApiCall
4103
4663
11
4670
4657
RegistryKeyCreated
RegistryValueSet
FileCreated
4656
FileRenamed
2
fileModified
13
14
RegistryKeySet
3
OutboundConnectionBlocked
InboundConnectionAccepted
ListeningConnectionCreated
5154
andConnectionToAppBlocked
5156
5157
5159
5158
ConnectionAttempt
ConnectionSuccess
5155
ConnectionRequest
llInboundConnectionBlocked
5031
ImageLoaded
7
LogonSuccess
4661
428
392
392
259
259
240
145
143
122
79
75
75
72
65
64
64
64
58
58
58
52
51
51
51
51
51
51
51
51
51
51
51
51
51
51
51
46
46
46
44
50
100
150
200
250
300
350
400
Count of techniques and sub techniques covered by each event


Most Relevant Event (Top 40)
to prioritize for all techniques and subtechniques detection
1
4688
ProcessCreated
8
CreateRemoteThreadApiCall
4103
4663
11
4670
4657
RegistryKeyCreated
RegistryValueSet
FileCreated
4656
FileRenamed
2
fileModified
13
14
RegistryKeySet
3
utboundConnectionBlocked
nboundConnectionAccepted
ListeningConnectionCreated
5154
ndConnectionToAppBlocked
5156
5157
5159
5158
ConnectionAttempt
ConnectionSuccess
5155
ConnectionRequest
llInboundConnectionBlocked
5031
ImageLoaded
7
LogonSuccess
4661
113
103
103
68
68
63
38
38
32
21
20
20
19
17
17
17
17
15
15
15
14
13
13
13
13
13
13
13
13
13
13
13
13
13
13
13
12
12
12
12
20
40
60
80
100
Percentange of techniques and sub techniques covered by each event