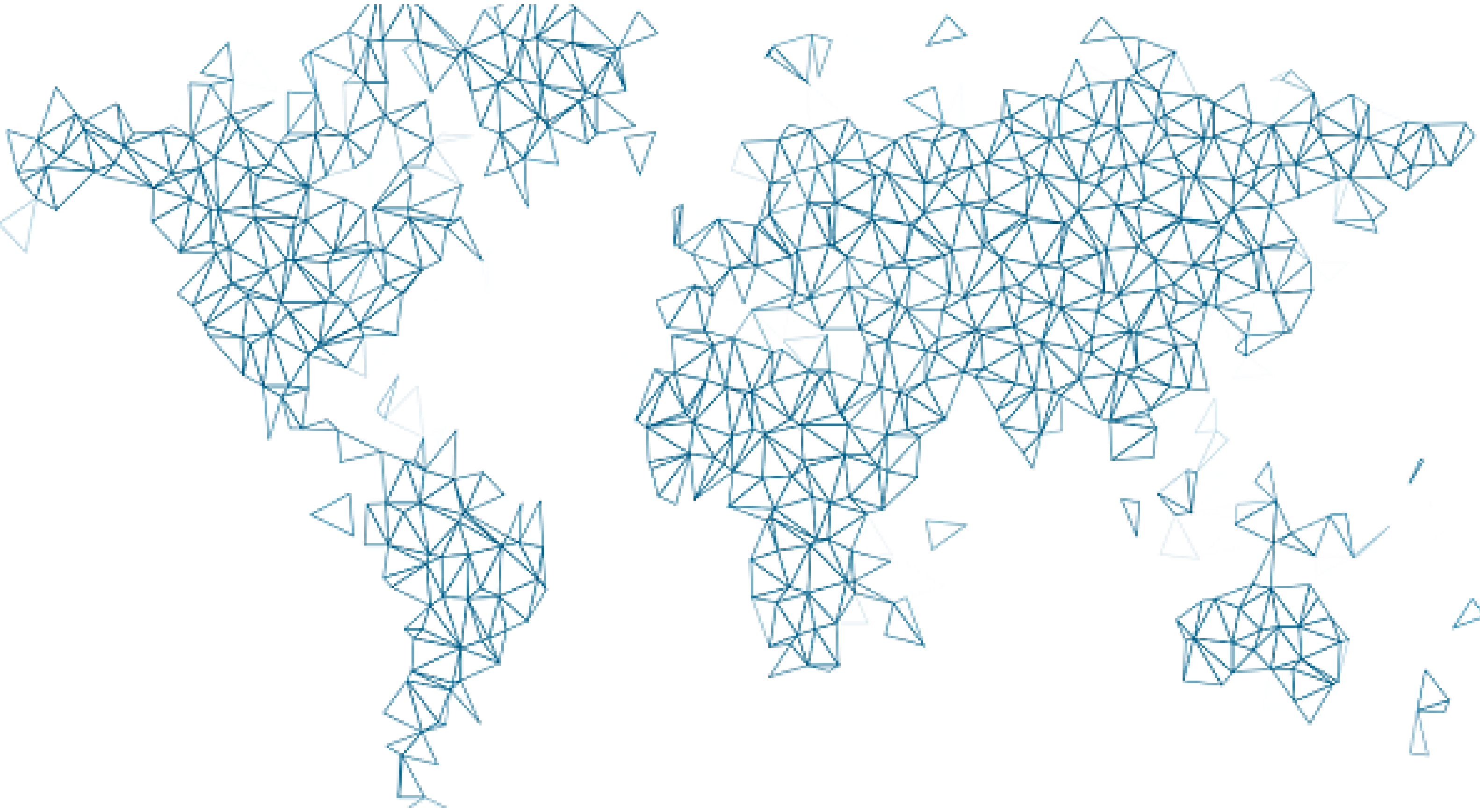
Must Have SOC Analysts customized cookbook

Leverage automation and threat intel data analysis for prioritizing detection



Report customized for defense sector

This report aims at providing statical analysis of TTPs (Tactics, Techniques and Procedures) used by threat actors targetting defense 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 defense 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 Transparent Tribe

Alias : Transparent Tribe, COPPER FIELDSTONE, APT36, Mythic Leopard, ProjectM

Transparent Tribe (https://attack.mitre.org/groups/G0134) is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India and Afghanistan.
Citation: Proofpoint Operation Transparent Tribe March 2016
Citation: Kaspersky Transparent Tribe August 2020
Citation: Talos Transparent Tribe May 2021

1.2 Ajax Security Team

Alias : Ajax Security Team, Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose

Ajax Security Team (https://attack.mitre.org/groups/G0130) is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team (https://attack.mitre.org/groups/G0130) transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
Citation: FireEye Operation Saffron Rose 2013

1.3 HAFNIUM

Alias : HAFNIUM, Operation Exchange Marauder

HAFNIUM (https://attack.mitre.org/groups/G0125) is a likely state-sponsored cyber espionage group operating out of China that has been active since at least January 2021. HAFNIUM (https://attack.mitre.org/groups/G0125) primarily targets entities in the US across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.
Citation: Microsoft HAFNIUM March 2020
Citation: Volexity Exchange Marauder March 2021

1.4 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

1.5 Sharpshooter

Alias : Sharpshooter

Operation Sharpshooter (https://attack.mitre.org/groups/G0104) is the name of a cyber espionage campaign discovered in October 2018 targeting nuclear, defense, energy, and financial companies. Though overlaps between this adversary and Lazarus Group (https://attack.mitre.org/groups/G0032) have been noted, definitive links have not been established.
Citation: McAfee Sharpshooter December 2018

1.6 Gallmaker

Alias : Gallmaker

Gallmaker (https://attack.mitre.org/groups/G0084) is a cyberespionage group that has targeted victims in the Middle East and has been active since at least December 2017. The group has mainly targeted victims in the defense, military, and government sectors.
Citation: Symantec Gallmaker Oct 2018

1.7 APT19

Alias : APT19, Codoso, C0d0so0, Codoso Team, Sunshop Group

APT19 (https://attack.mitre.org/groups/G0073) is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms.
Citation: FireEye APT19

Some analysts track APT19 (https://attack.mitre.org/groups/G0073) and Deep Panda (https://attack.mitre.org/groups/G0009) 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
Citation: FireEye APT Groups
Citation: Unit 42 C0d0so0 Jan 2016

1.8 Thrip

Alias : Thrip

Thrip (https://attack.mitre.org/groups/G0076) is an espionage group that has targeted satellite communications, telecoms, and defense contractor companies in the U.S. and Southeast Asia. The group uses custom malware as well as "living off the land" techniques.
Citation: Symantec Thrip June 2018

1.9 Elderwood

Alias : Elderwood, Elderwood Gang, Beijing Group, Sneaky Panda

Elderwood (https://attack.mitre.org/groups/G0066) is a suspected Chinese cyber espionage group that was reportedly responsible for the 2009 Google intrusion known as Operation Aurora.
Citation: Security Affairs Elderwood Sept 2012

The group has targeted defense organizations, supply chain manufacturers, human rights and nongovernmental organizations (NGOs), and IT service providers.
Citation: Symantec Elderwood Sept 2012
Citation: CSM Elderwood Sept 2012

1.10 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

1.11 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

1.12 Dragonfly

Alias : Dragonfly, TEMP.Isotope, DYMALLOY, Berserk Bear, TG-4192, Crouching Yeti, IRON LIBERTY, Energetic Bear

Dragonfly (https://attack.mitre.org/groups/G0035) is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16.
Citation: DOJ Russia Targeting Critical Infrastructure March 2022
Citation: UK GOV FSB Factsheet April 2022

Active since at least 2010, Dragonfly (https://attack.mitre.org/groups/G0035) has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.
Citation: Symantec Dragonfly
Citation: Secureworks IRON LIBERTY July 2019
Citation: Symantec Dragonfly Sept 2017
Citation: Fortune Dragonfly 2.0 Sept 2017

Citation: Gigamon Berserk Bear October 2021
Citation: CISA AA20-296A Berserk Bear December 2020
Citation: Symantec Dragonfly 2.0 October 2017

1.13 Threat Group-3390

Alias : Threat Group-3390, Earth Smilodon, TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse

[Threat Group-3390](https://attack.mitre.org/groups/G0027) is a Chinese threat group that has extensively used strategic Web compromises to target victims.
Citation: Dell TG-3390

The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, manufacturing and gambling/betting sectors.
Citation: SecureWorks BRONZE UNION June 2017
Citation: Securelist LuckyMouse June 2018
Citation: Trend Micro DRBControl February 2020

1.14 APT17

Alias : APT17, Deputy Dog

APT17 (https://attack.mitre.org/groups/G0025) is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.
Citation: FireEye APT17

1.15 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

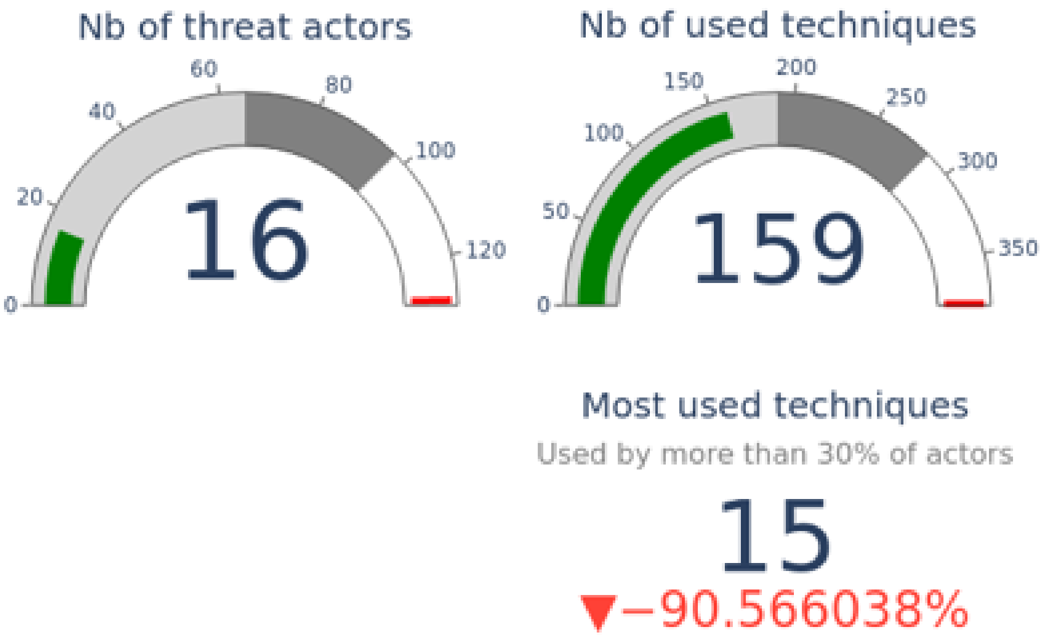
1.16 Axiom

Alias : Axiom, Group 72

Axiom (https://attack.mitre.org/groups/G0001) is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. Some reporting suggests a degree of overlap between Axiom (https://attack.mitre.org/groups/G0001) and Winnti Group (https://attack.mitre.org/groups/G0044) but the two groups appear to be distinct based on differences in reporting on TTPs and targeting.
Citation: Kaspersky Winnti April 2013
Citation: Kaspersky Winnti June 2015
Citation: Novetta Winnti April 2015

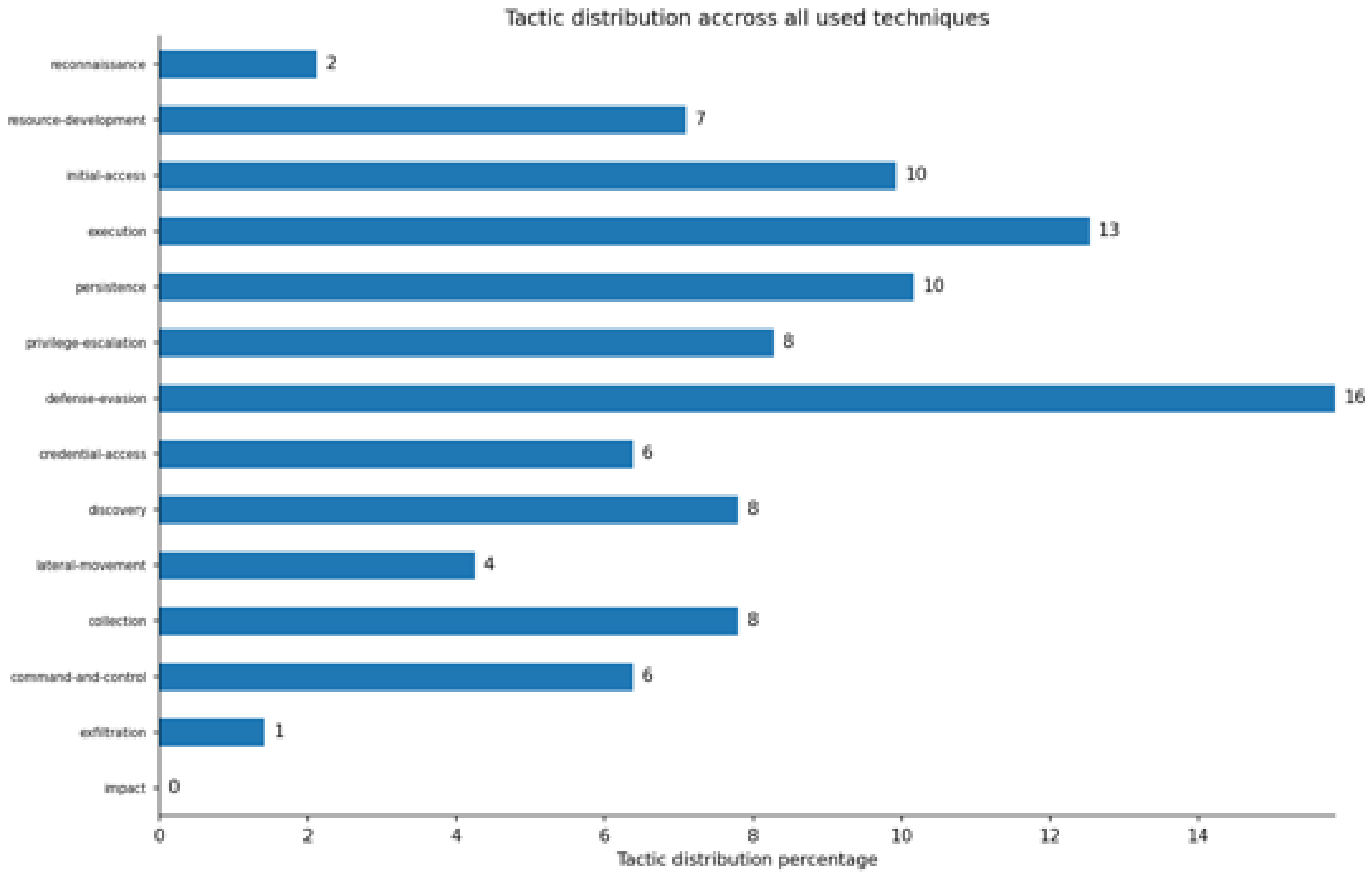
2. What TTPs to prioritize for detection ?

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

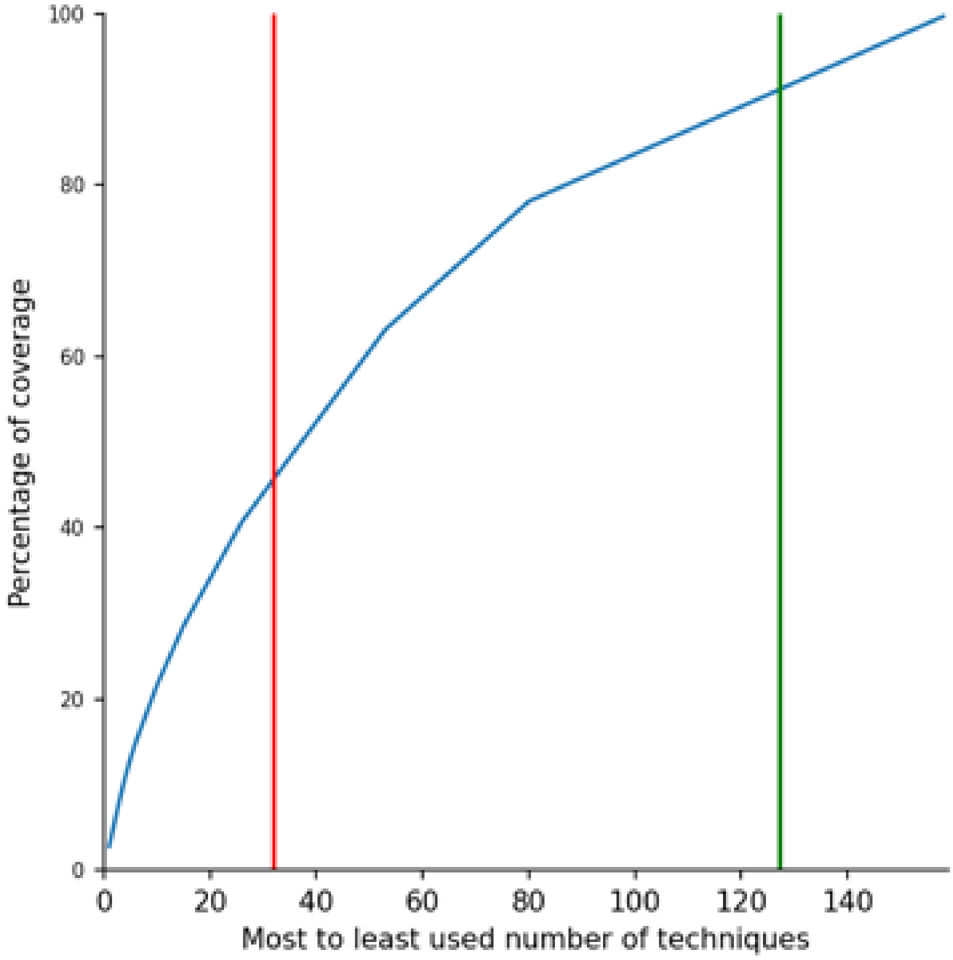
The following graph gives the techniques distribution accross all of those threat actors.

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.

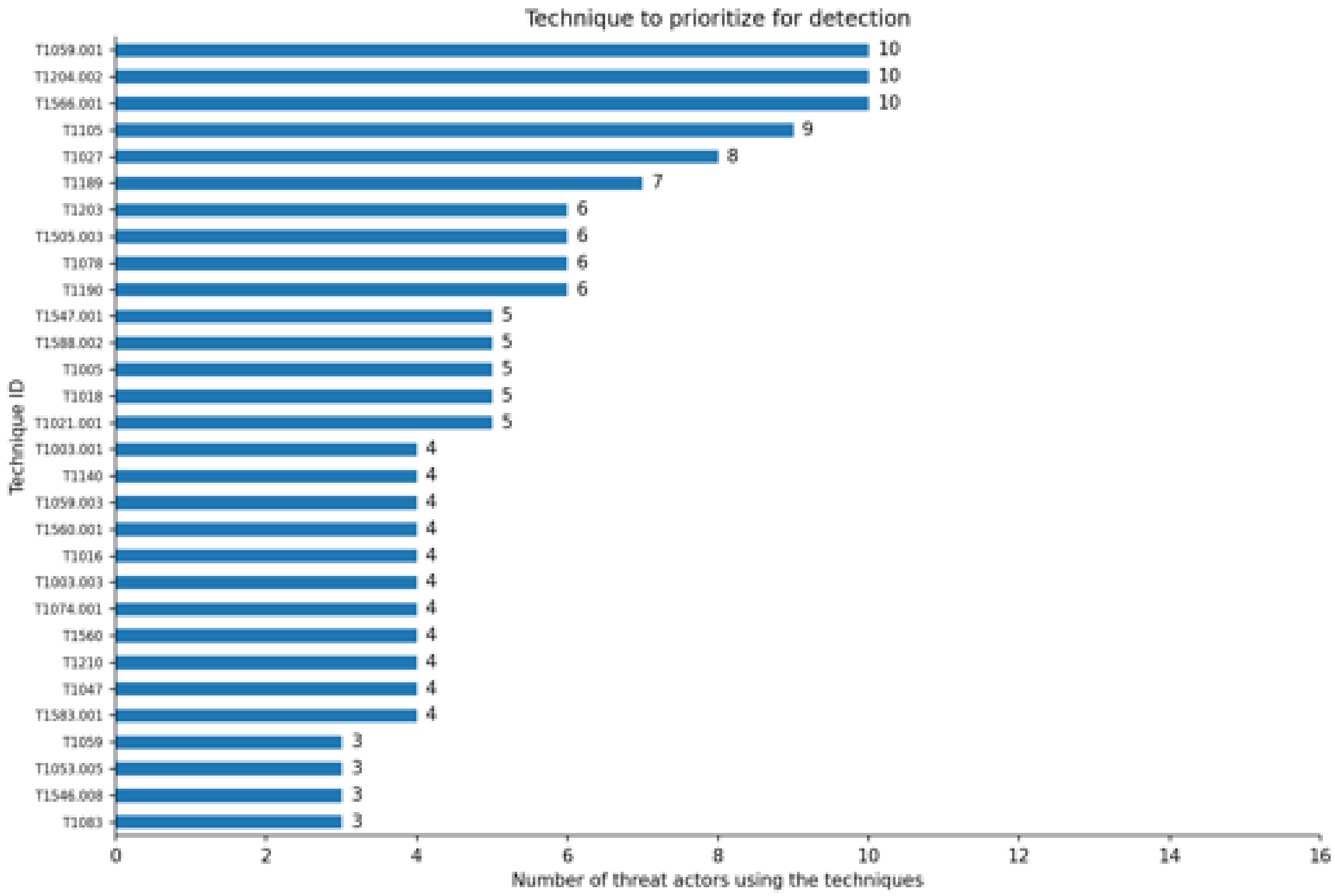
The green line gives the number of techniques corresponding to 80% of total techniques used.



2.3 Top 30 most used techniques

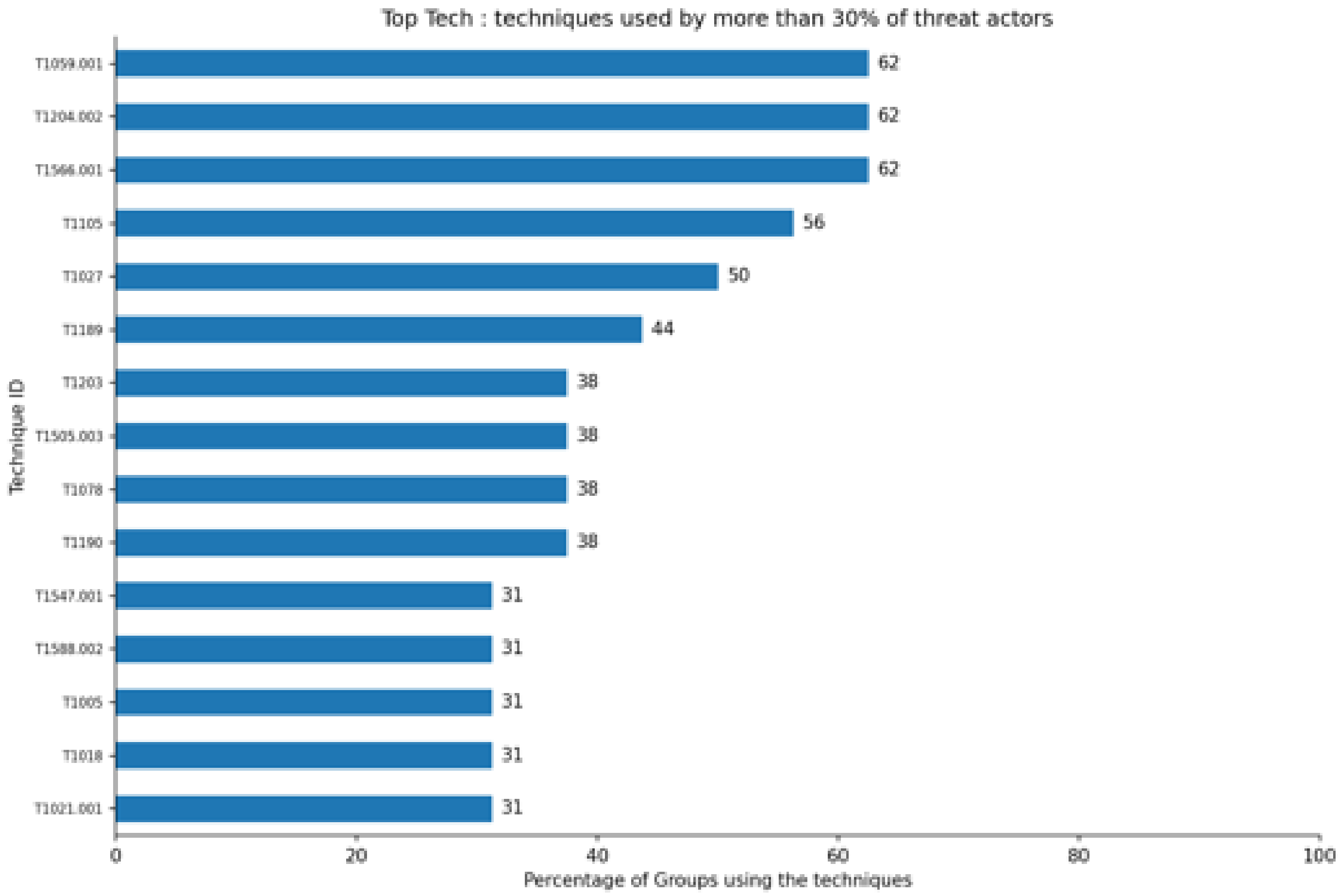
The following graph gives the top 30 techniques that are most used by all of those threat actors.

For each most used technique, the number of group using this technique is given.



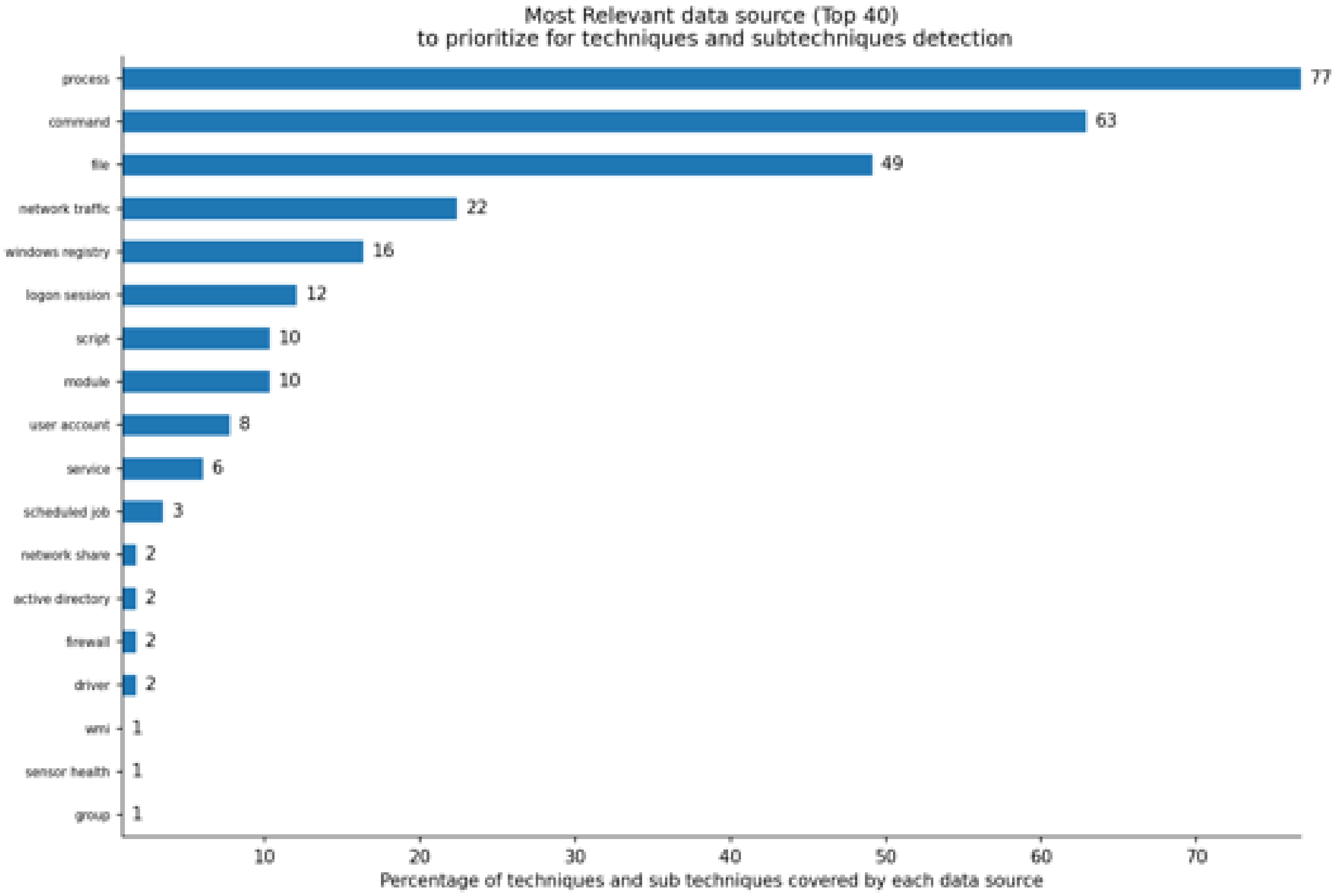
2.4 The Must be covered techniques

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.



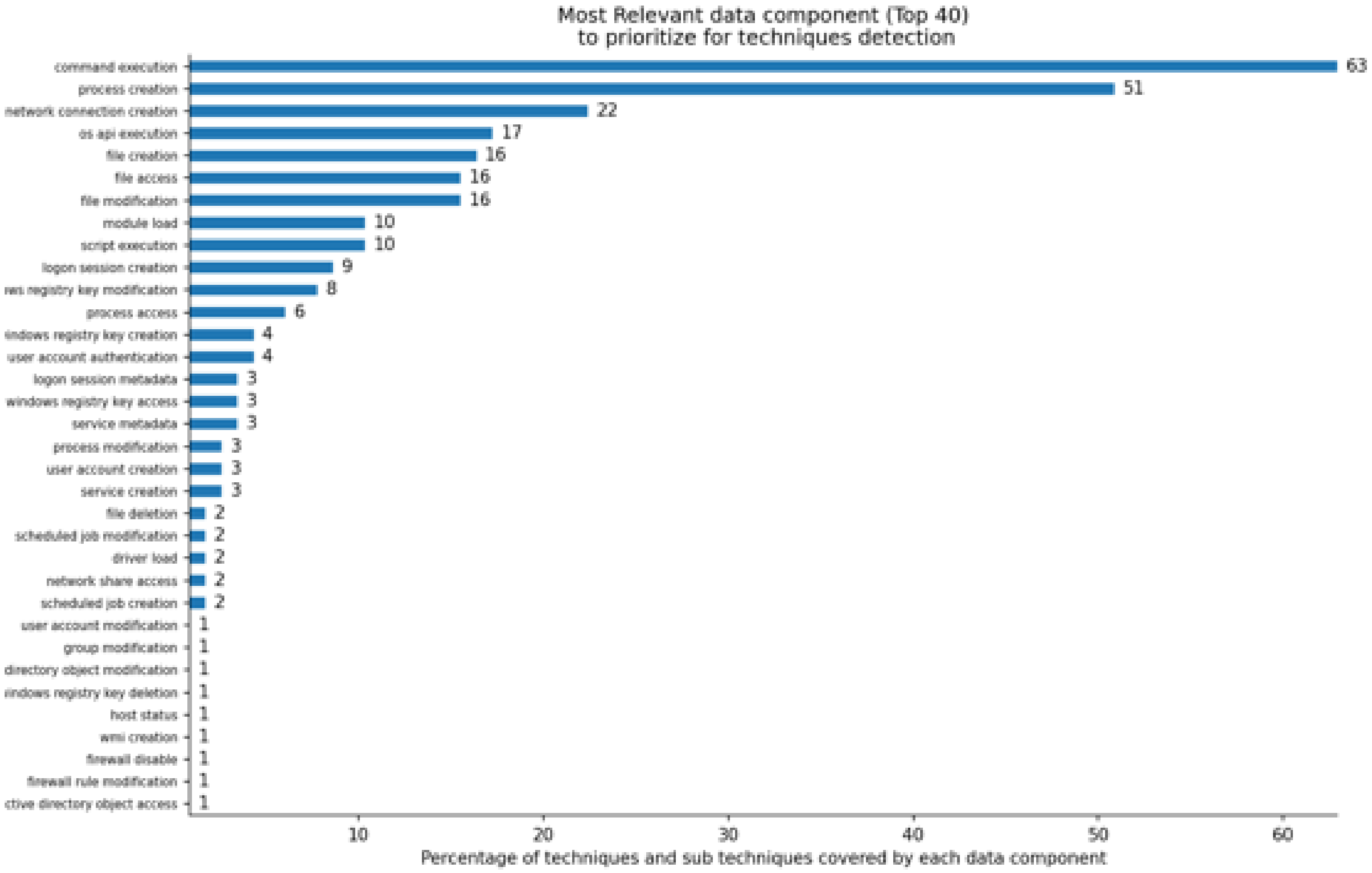
2.5 Top data source to collect for detections

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.



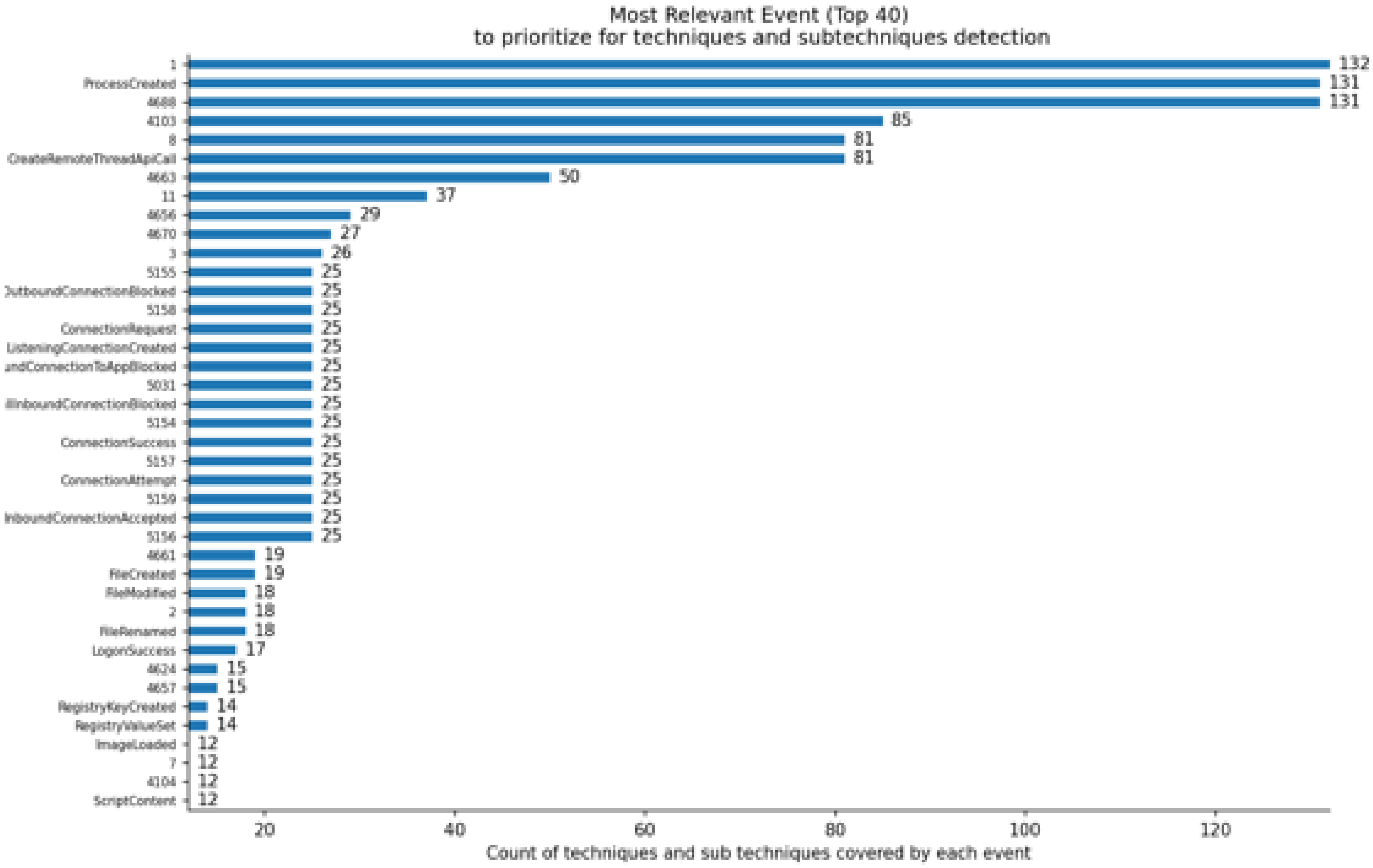
2.6 Top data component to collect for detections

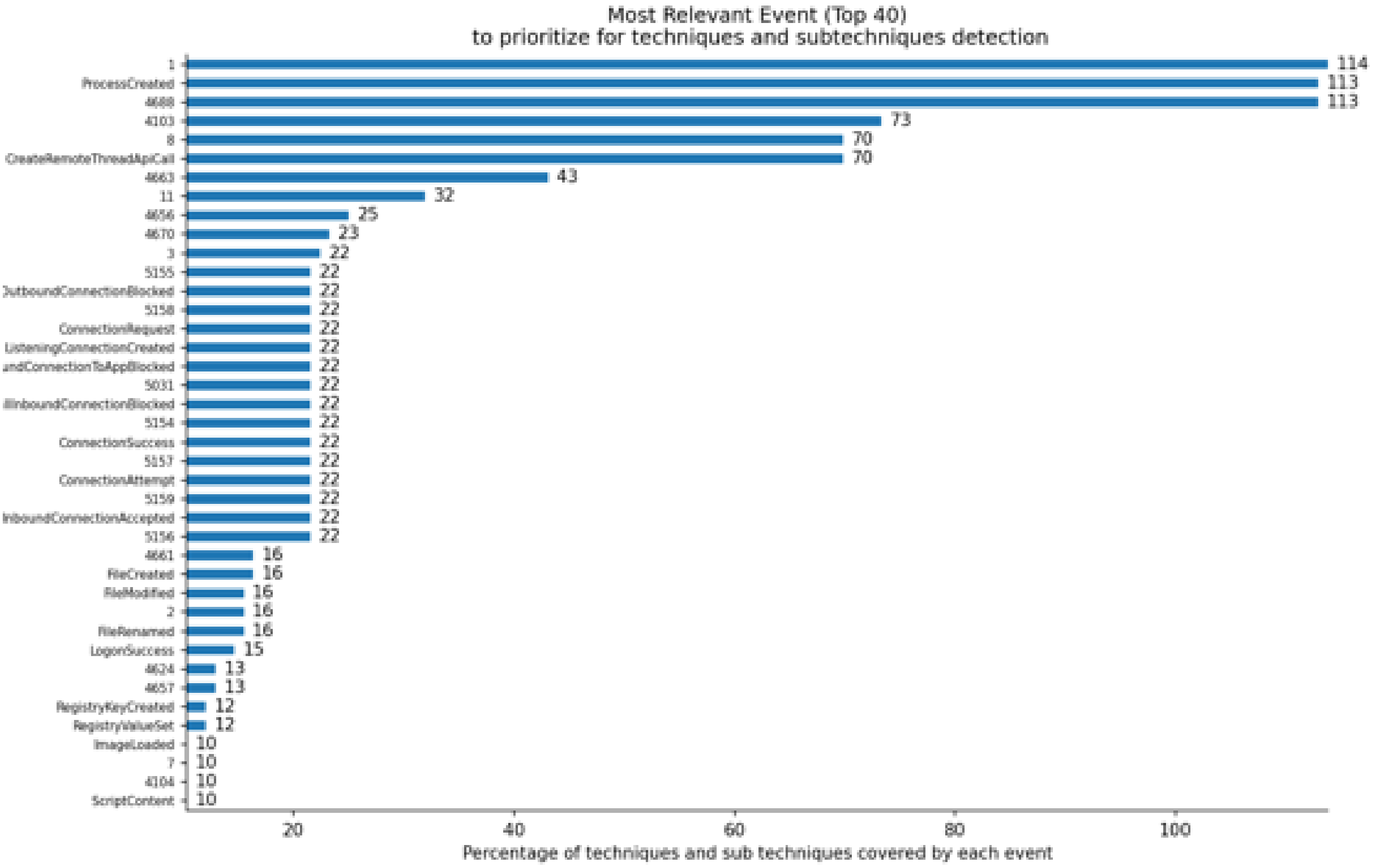
The following graph gives the top 40 data source to collect in order to be able to detect the techniques used by threat actors. Please see annexes for reference.



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
132
ProcessCreated
131
4688
131
4103
85
8
81
CreateRemoteThreadApiCall
81
4663
50
11
37
4656
29
4670
27
3
26
5155
25
OutboundConnectionBlocked
25
5158
25
ConnectionRequest
25
ListeningConnectionCreated
25
undConnectionToAppBlocked
25
5031
25
llInboundConnectionBlocked
25
5154
25
ConnectionSuccess
25
5157
25
ConnectionAttempt
25
5159
25
InboundConnectionAccepted
25
5156
25
4661
19
FileCreated
19
FileModified
18
2
18
FileRenamed
18
LogonSuccess
17
4624
15
4657
15
RegistryKeyCreated
14
RegistryValueSet
14
ImageLoaded
12
7
12
4104
12
ScriptContent
12
20
40
60
80
100
120
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
8
CreateRemoteThreadApiCall
4663
11
4656
4670
3
5155
OutboundConnectionBlocked
5158
ConnectionRequest
ListeningConnectionCreated
undConnectionToAppBlocked
5031
llInboundConnectionBlocked
5154
ConnectionSuccess
5157
ConnectionAttempt
5159
InboundConnectionAccepted
5156
4661
FileCreated
FileModified
2
FileRenamed
LogonSuccess
4624
4657
RegistryKeyCreated
RegistryValueSet
ImageLoaded
7
4104
ScriptContent
114
113
113
73
70
70
43
32
25
23
22
22
22
22
22
22
22
22
22
22
22
22
22
22
22
22
16
16
16
16
16
15
13
13
12
12
10
10
10
10
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 T1059.001

Used by group : HAFNIUM, Fox Kitten, Gallmaker, APT19, Thrip, Leviathan, menuPass, Dragonfly, Threat Group-3390, Deep Panda

Tactic : execution

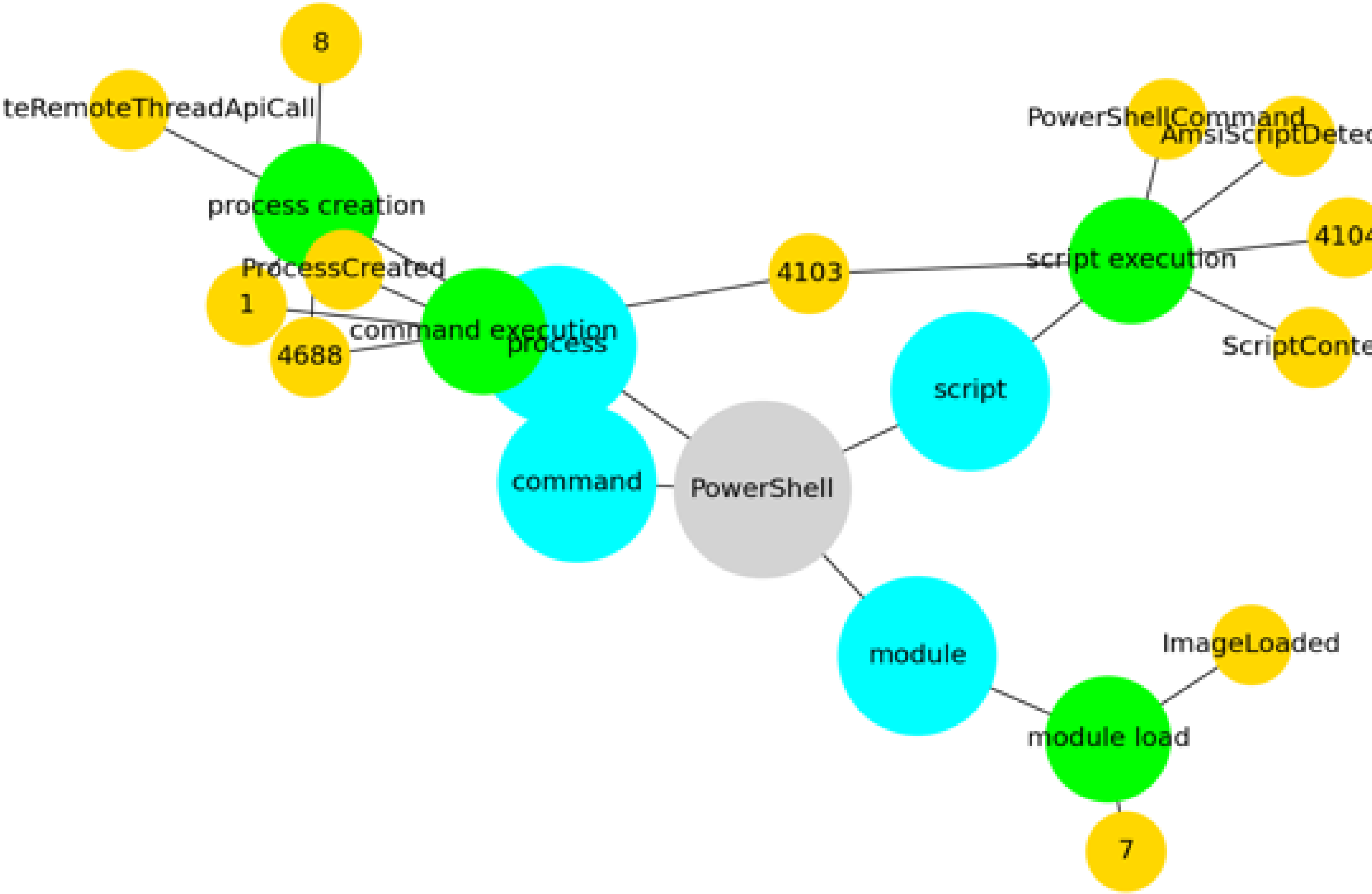
Technique : PowerShell

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)



3.2 T1204.002

Used by group : Transparent Tribe, Ajax Security Team, Sharpshooter, Gallmaker, APT19, Elderwood, Leviathan, menuPass, Dragonfly, Threat Group-3390

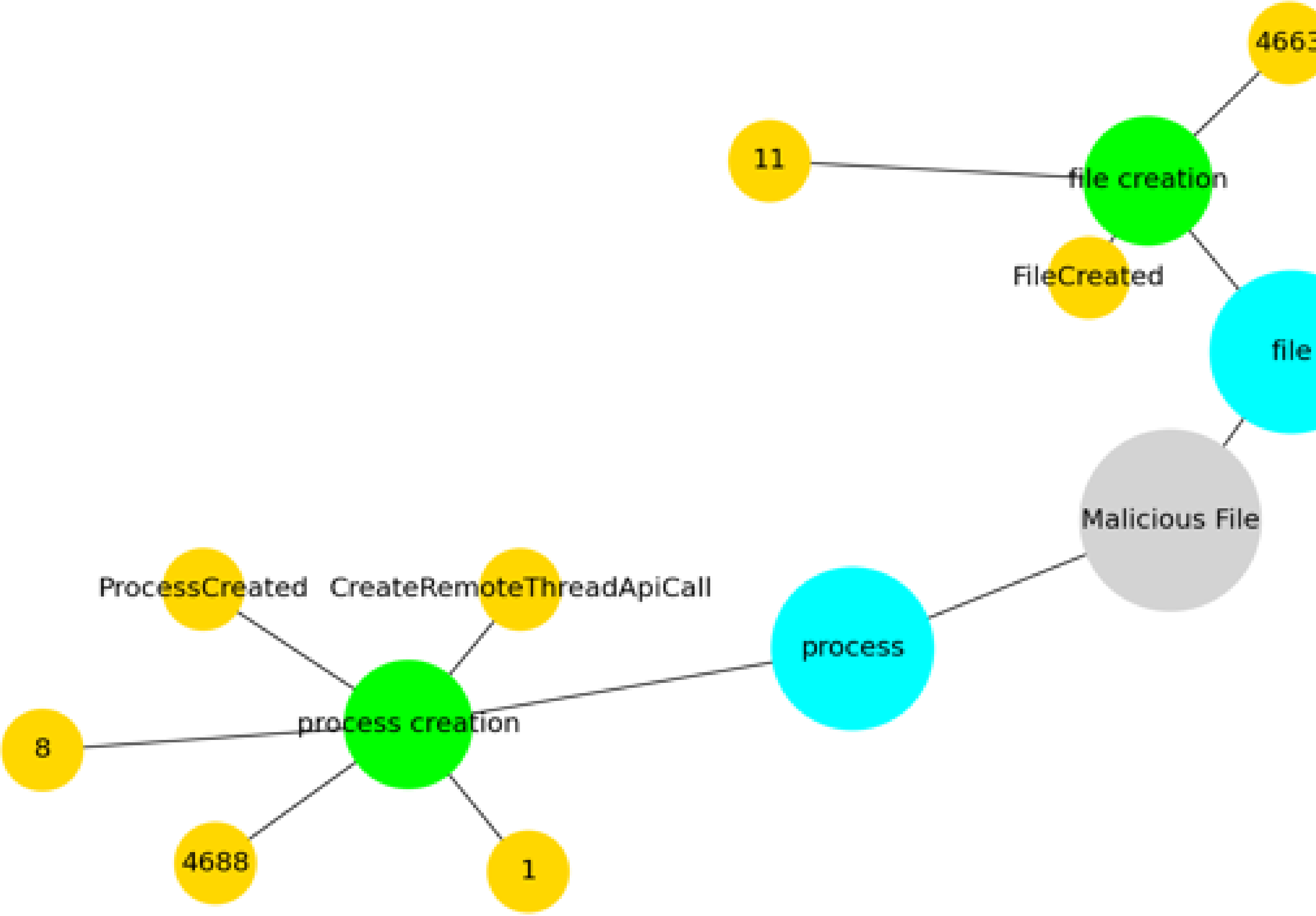
Tactic : execution

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).



3.3 T1566.001

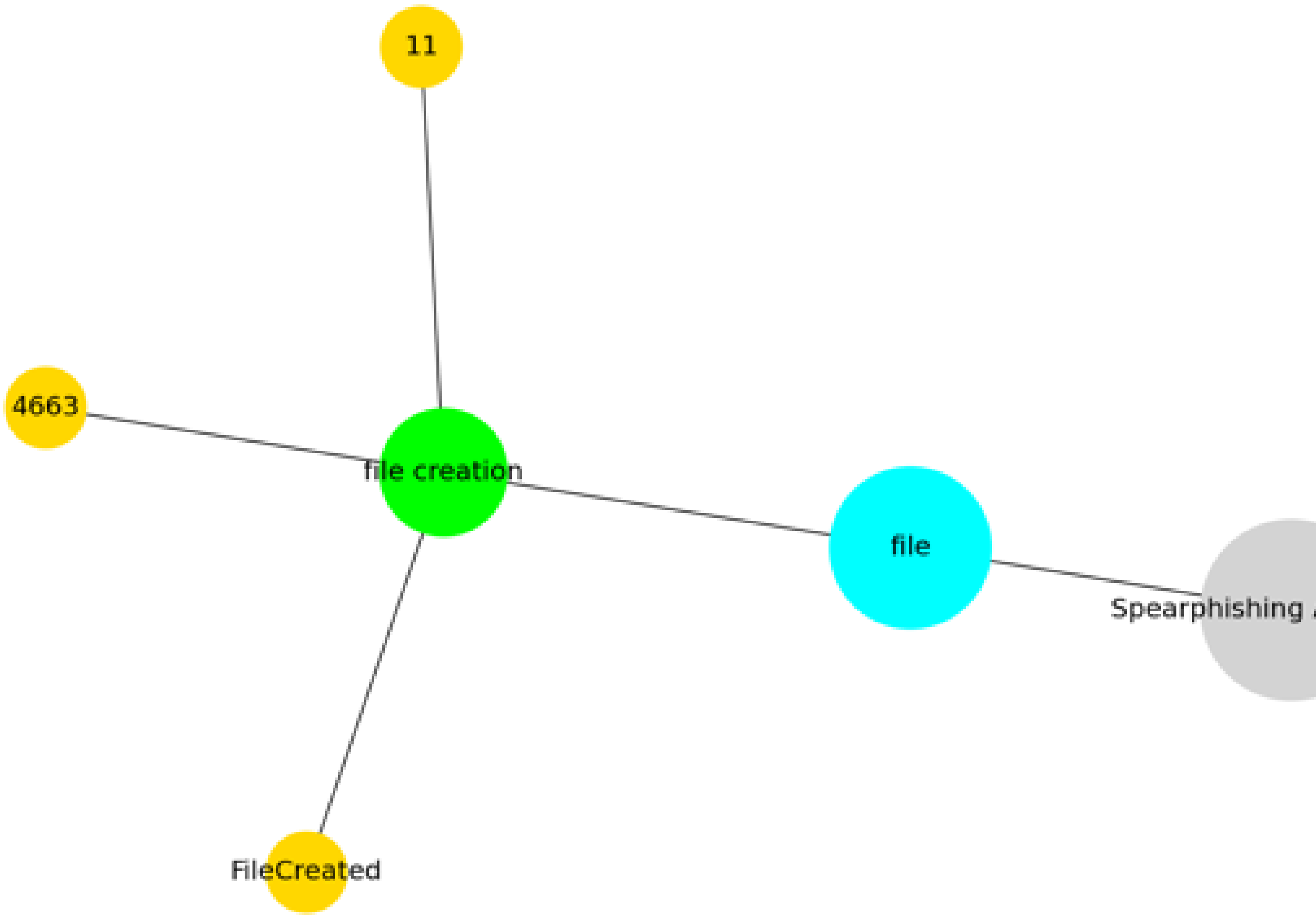
Used by group : Transparent Tribe, Ajax Security Team, Sharpshooter, Gallmaker, APT19, Elderwood, Leviathan, menuPass, Dragonfly, Threat Group-3390

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.



3.4 T1105

Used by group : Ajax Security Team, HAFNIUM, Fox Kitten, Sharpshooter, Elderwood, Leviathan, menuPass, Dragonfly, Threat Group-3390

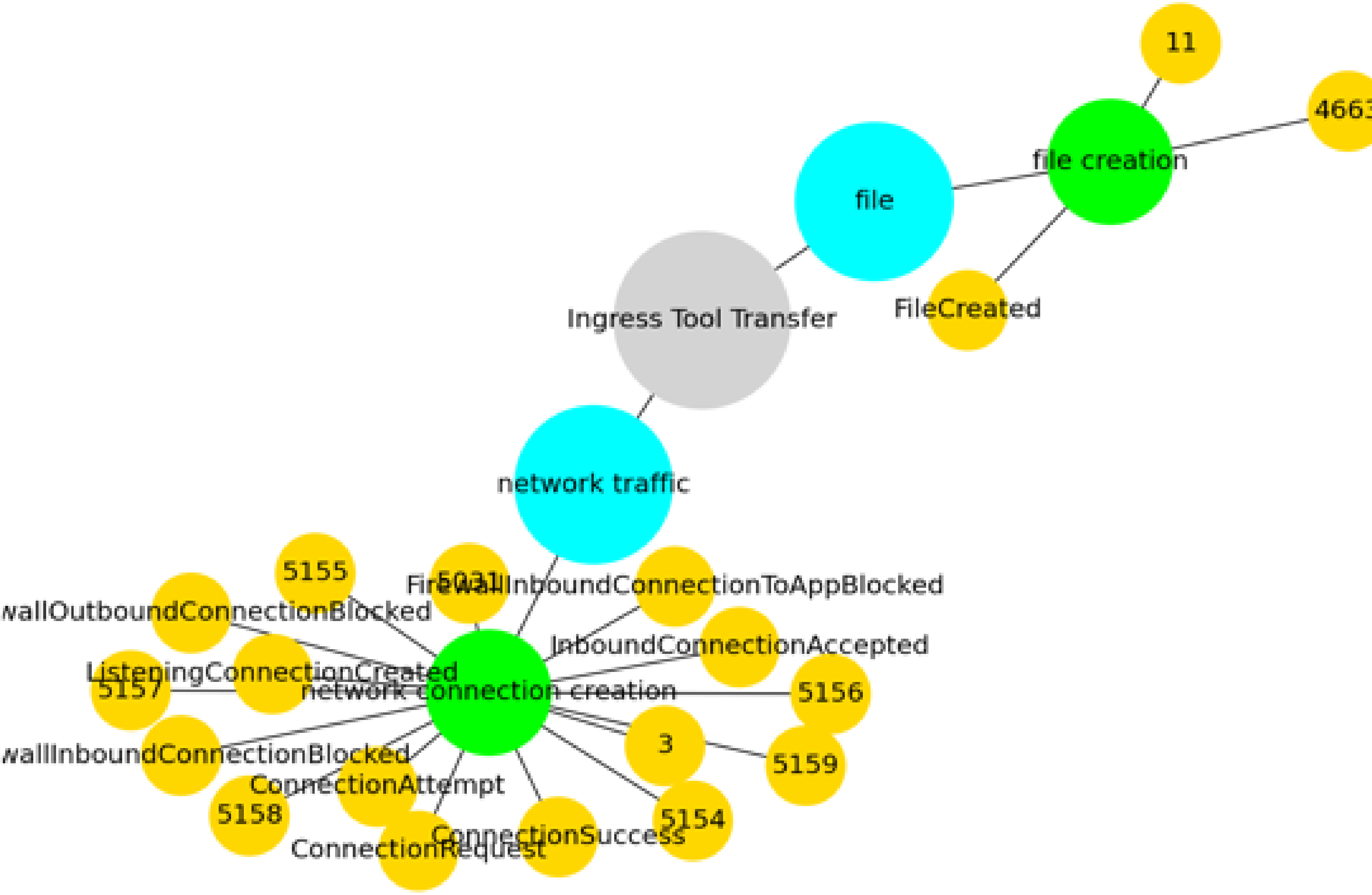
Tactic : command-and-control

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)


11
466
file creation
file
FileCreated
Ingress Tool Transfer
network traffic
5155
5031
FirewallInboundConnectionToAppBlocked
wallOutboundConnectionBlocked
InboundConnectionAccepted
ListeningConnectionCreated
5157
network connection creation
5156
3
5159
wallInboundConnectionBlocked
ConnectionAttempt
5158
5154
ConnectionSuccess
ConnectionRequest

3.5 T1027

Used by group : Transparent Tribe, Fox Kitten, Gallmaker, APT19, Elderwood, Leviathan, menuPass, Threat Group-3390

Tactic : defense-evasion

Technique : Obfuscated Files or Information

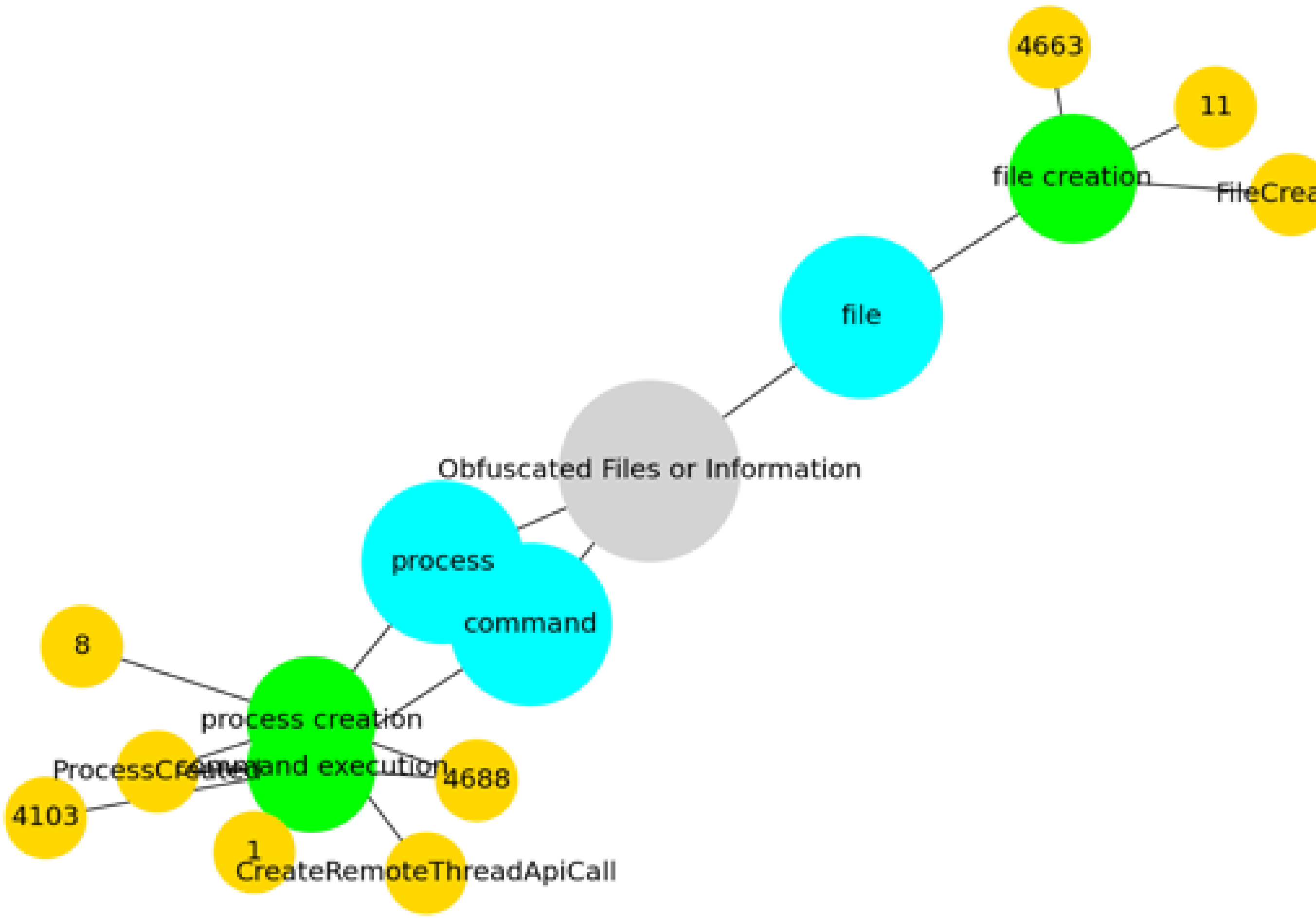
Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

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)



3.6 T1189

Used by group : Transparent Tribe, APT19, Elderwood, Leviathan, Dragonfly, Threat Group-3390, Axiom

Tactic : initial-access

Technique : Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001).

Multiple ways of delivering exploit code to a browser exist, including:

* A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
* Malicious ads are paid for and served through legitimate ad providers.
* Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

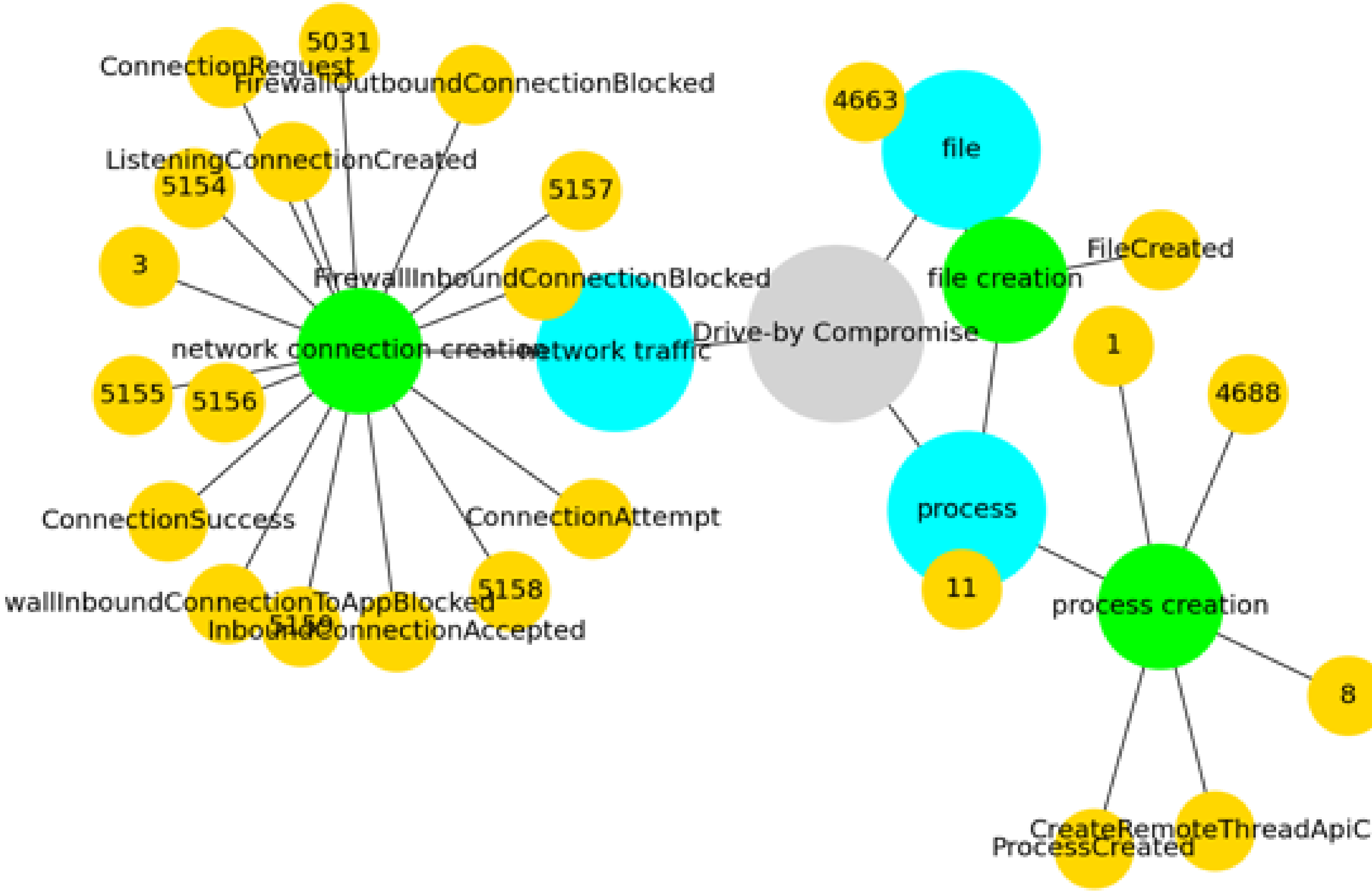
Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise)

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
    * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
    * In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)



3.7 T1203

Used by group : Transparent Tribe, Elderwood, Leviathan, Dragonfly, Threat Group-3390, Axiom

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.

3.8 T1505.003

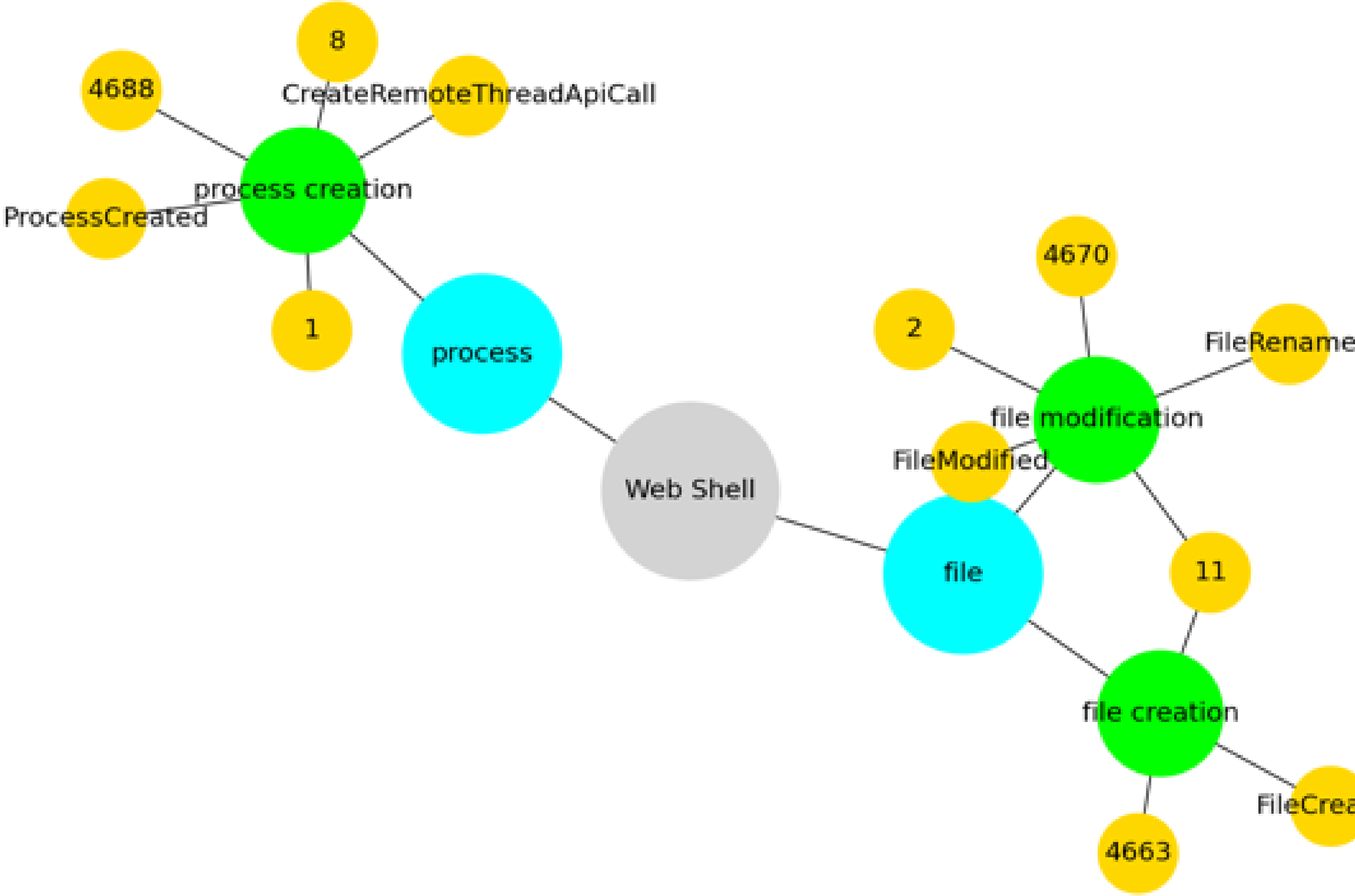
Used by group : HAFNIUM, Fox Kitten, Leviathan, Dragonfly, Threat Group-3390, Deep Panda

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)



3.9 T1078

Used by group : Fox Kitten, Leviathan, menuPass, Dragonfly, Threat Group-3390, Axiom

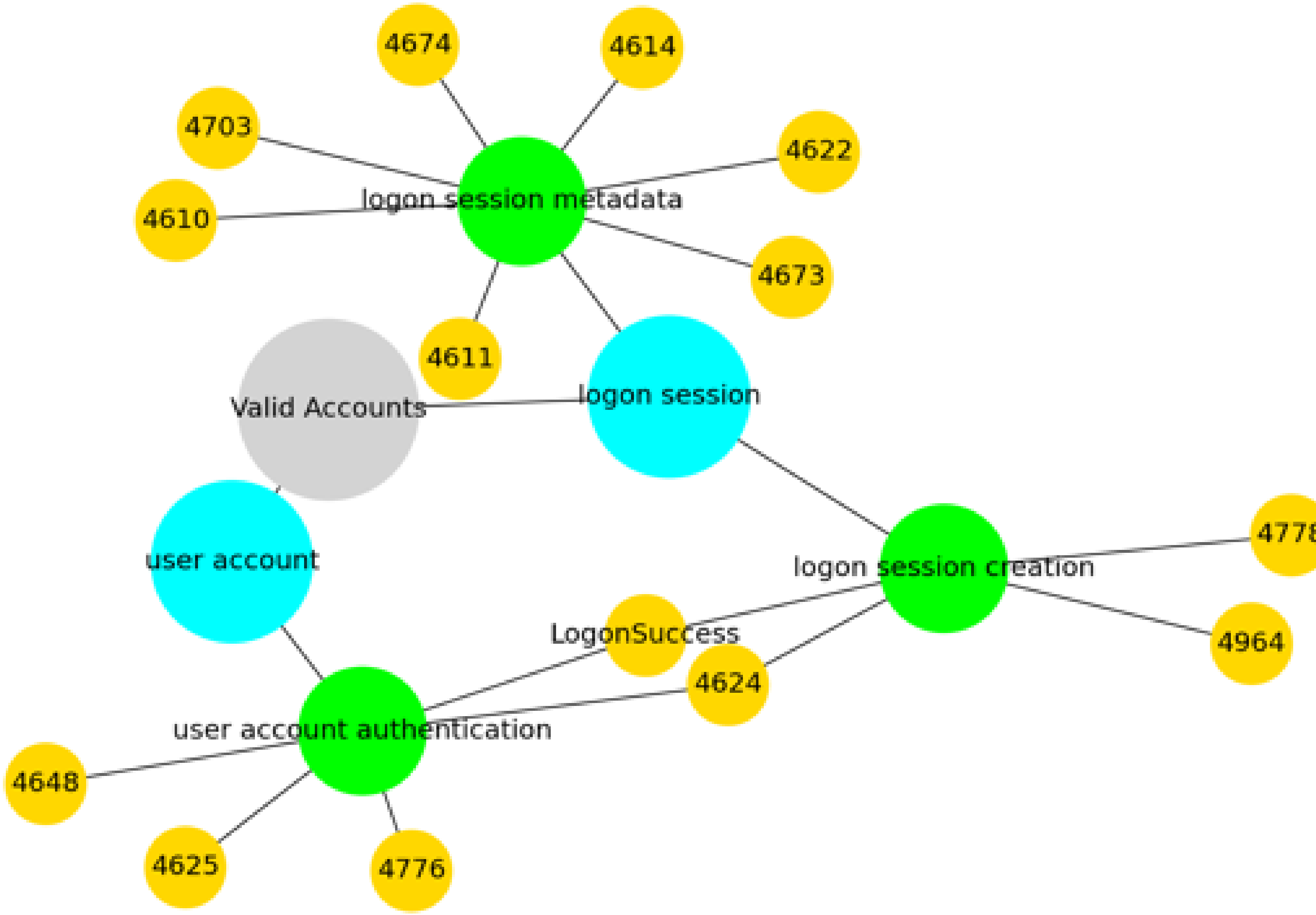
Tactic : defense-evasion, persistence, privilege-escalation, initial-access

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)



3.10 T1190

Used by group : HAFNIUM, Fox Kitten, menuPass, Dragonfly, Threat Group-3390, Axiom

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)

3.11 T1547.001

Used by group : Sharpshooter, APT19, Leviathan, Dragonfly, Threat Group-3390

Tactic : persistence, privilege-escalation

Technique : Registry Run Keys / Startup Folder

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level.

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is <code>C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs\Startup</code>. The startup folder path for all users is <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp</code>.

The following run keys are created by default on Windows systems:

* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run</code>
* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>
* <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</code>
* <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>

Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</code> is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: <code>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)

The following Registry keys can be used to set startup folder items for persistence:

* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>
* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
* <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
* <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>

The following Registry keys can control automatic startup of services during boot:

* <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
* <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices</code>
* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices</code>

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

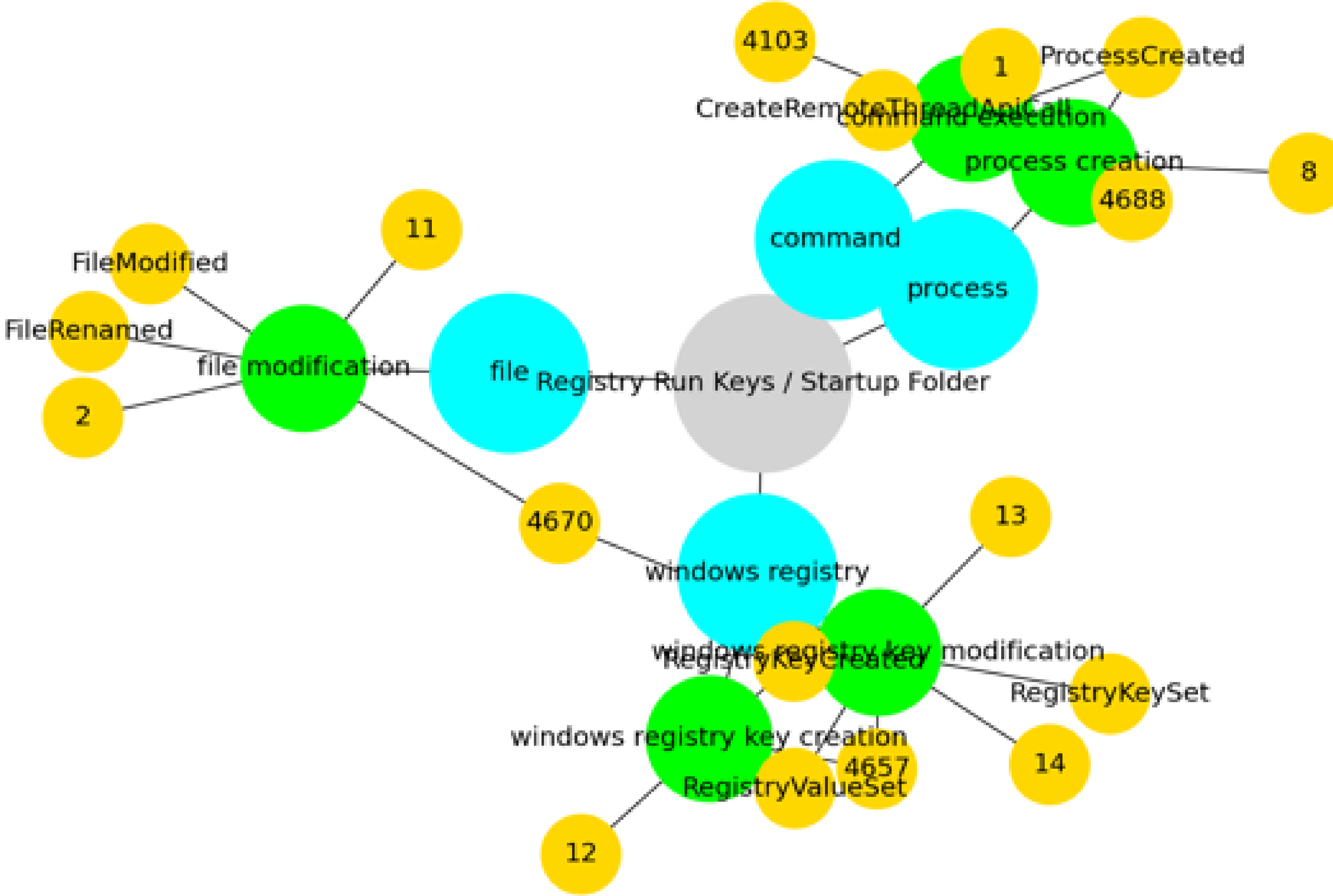
* <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>
* <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>

The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit</code> and <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell</code> subkeys can automatically launch programs.

Programs listed in the load value of the registry key <code>HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> run when any user logs on.

By default, the multistring <code>BootExecute</code> value of the registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> is set to <code>autocheck autochk *</code>. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.



3.12 T1588.002

Used by group : APT19, Thrip, menuPass, Dragonfly, Threat Group-3390

Tactic : resource-development

Technique : Tool

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Tool acquisition can involve the procurement of commercial software licenses, including for red teaming tools such as [Cobalt Strike](https://attack.mitre.org/software/S0154). Commercial software may be obtained through purchase, stealing licenses (or licensed copies of the software), or cracking trial versions.(Citation: Recorded Future Beacon 2019)

Adversaries may obtain tools to support their operations, including to support execution of post-compromise behaviors. In addition to freely downloading or purchasing software, adversaries may steal software and/or software licenses from third-party entities (including other adversaries).

3.13 T1005

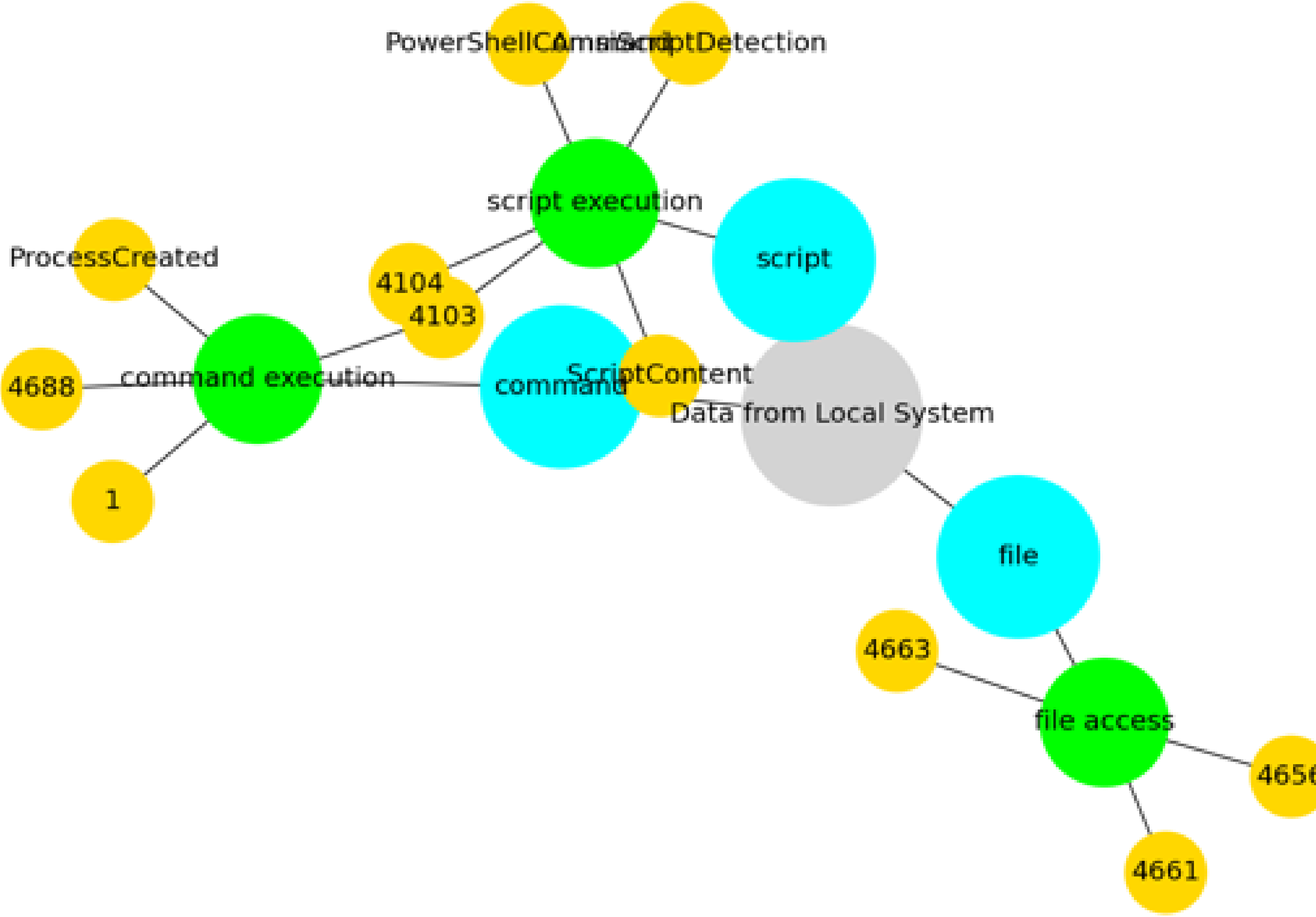
Used by group : Fox Kitten, menuPass, Dragonfly, Threat Group-3390, Axiom

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.



3.14 T1018

Used by group : Fox Kitten, menuPass, Dragonfly, Threat Group-3390, Deep Panda

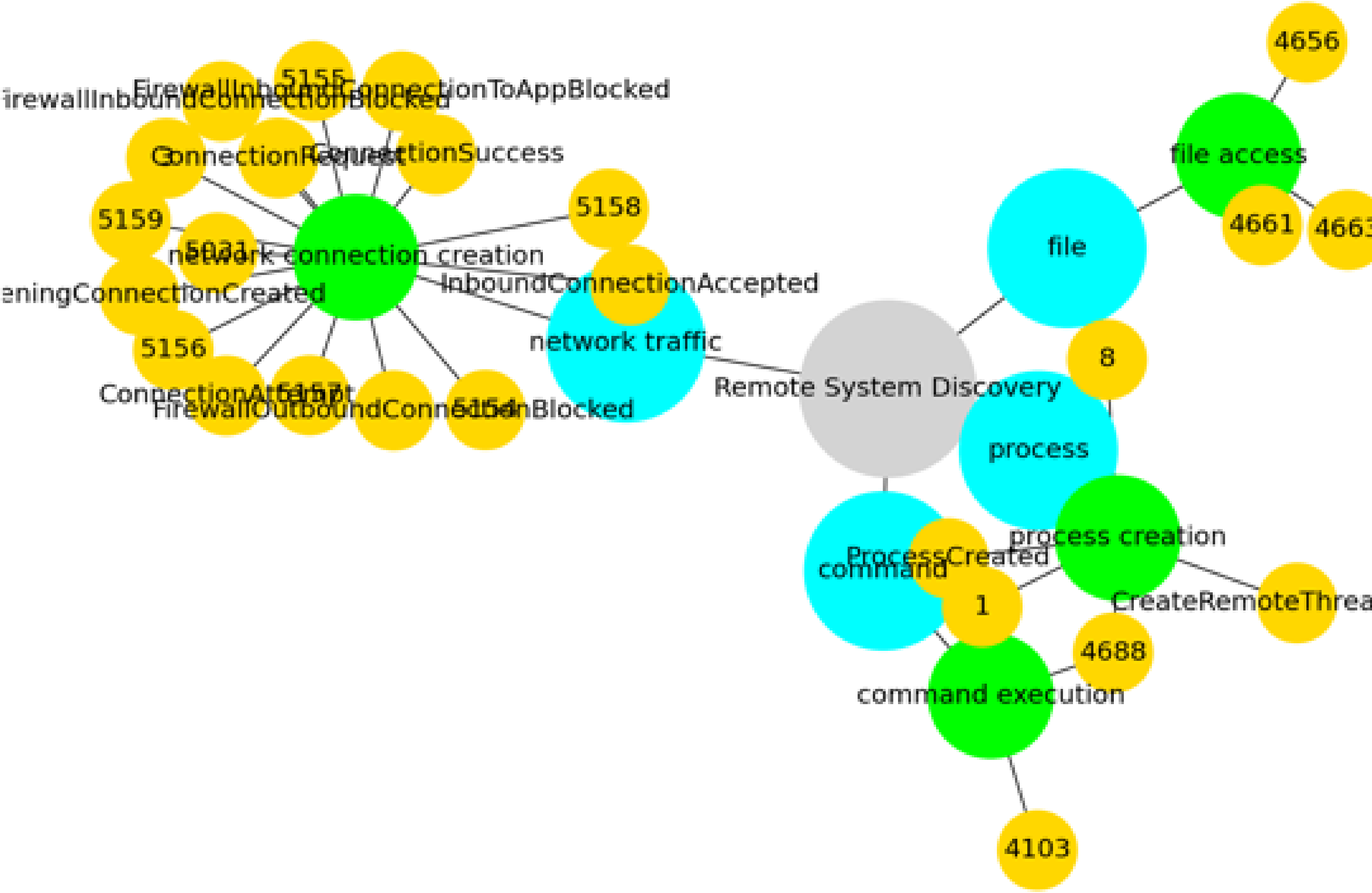
Tactic : discovery

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)



3.15 T1021.001

Used by group : Fox Kitten, Leviathan, menuPass, Dragonfly, Axiom

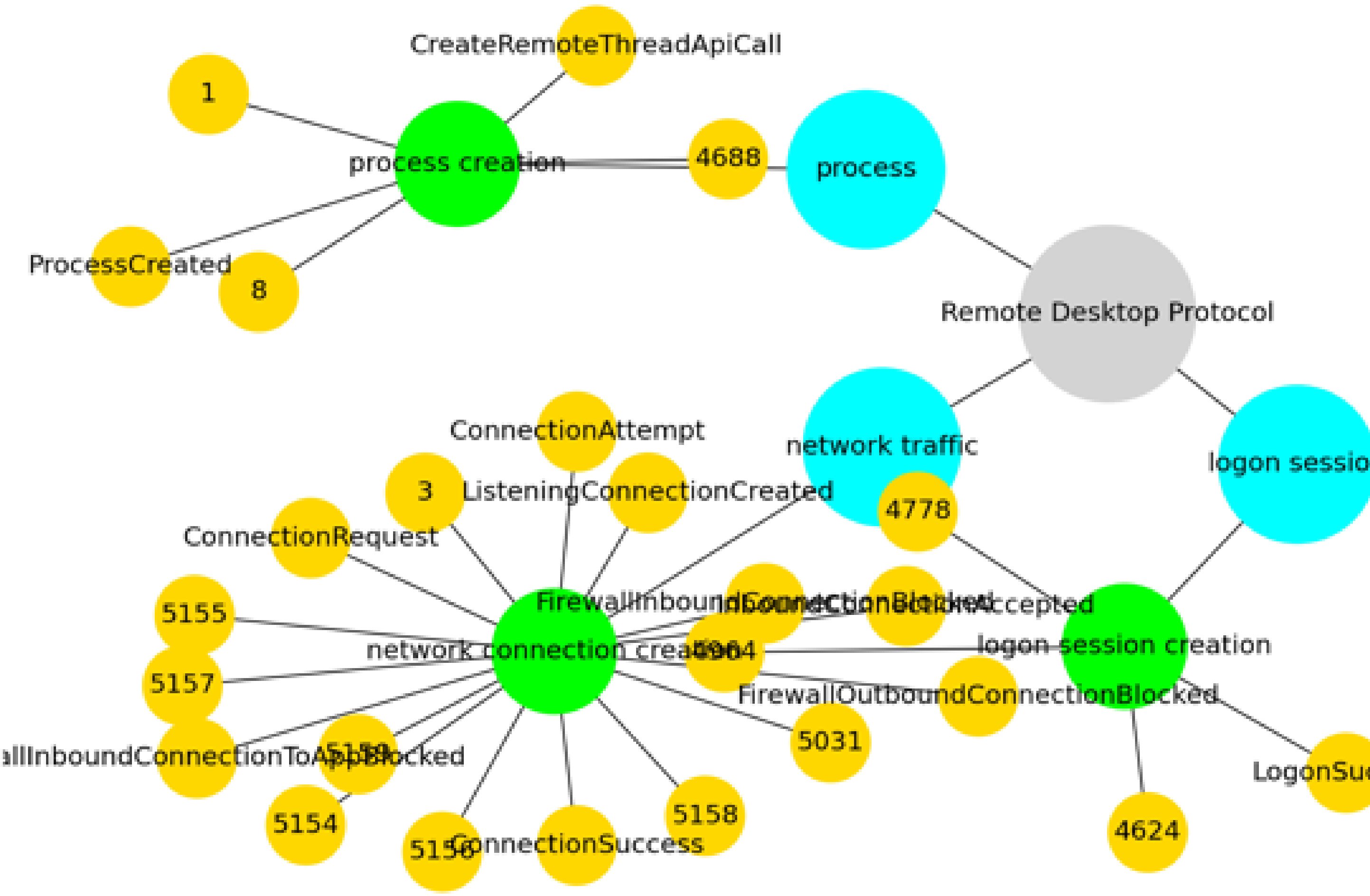
Tactic : lateral-movement

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)



3.16 T1003.001

Used by group : HAFNIUM, Fox Kitten, Leviathan, Threat Group-3390

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>

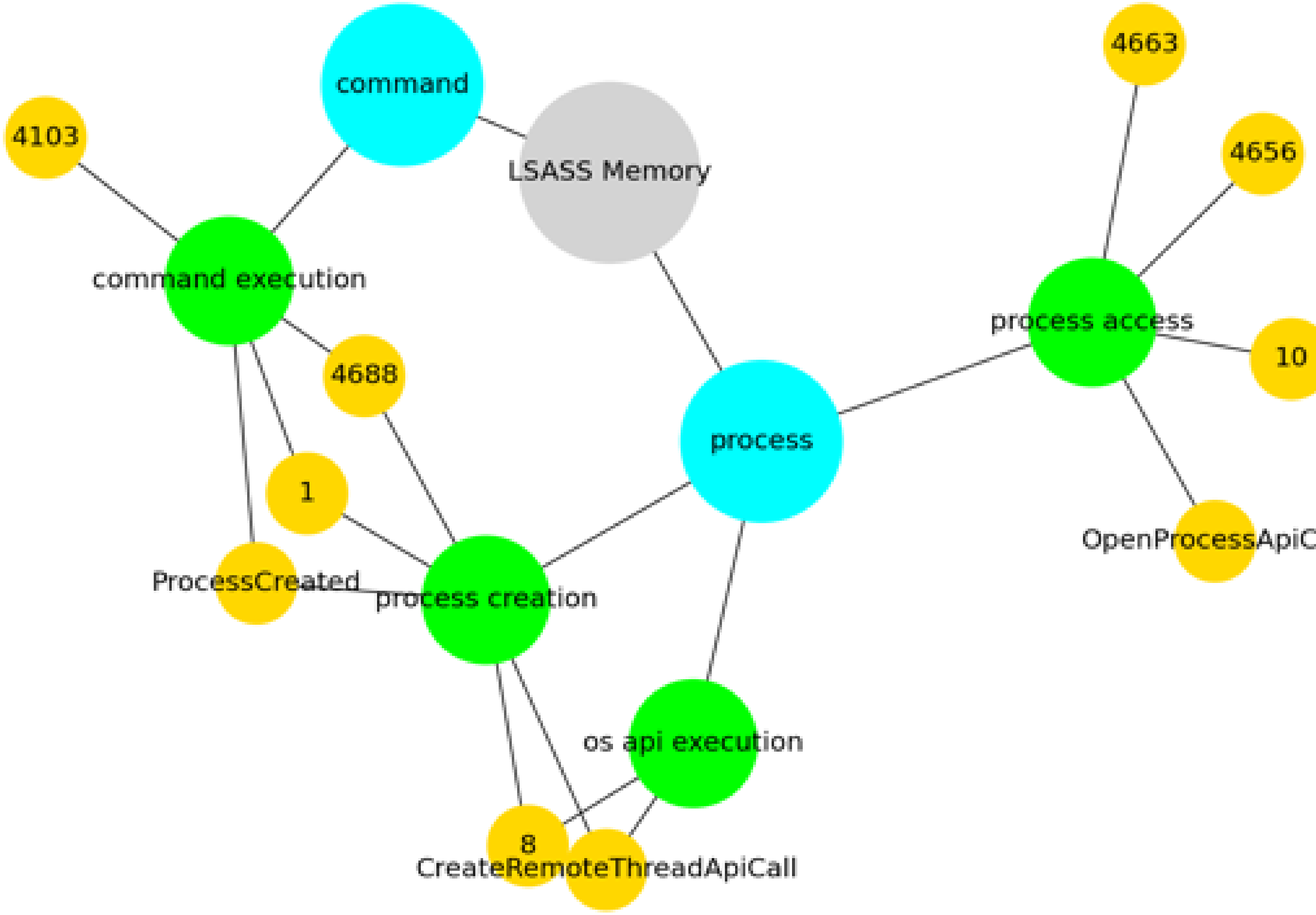
Built-in Windows tools such as comsvcs.dll can also be used:

* <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)



3.17 T1140

Used by group : APT19, Leviathan, menuPass, Threat Group-3390

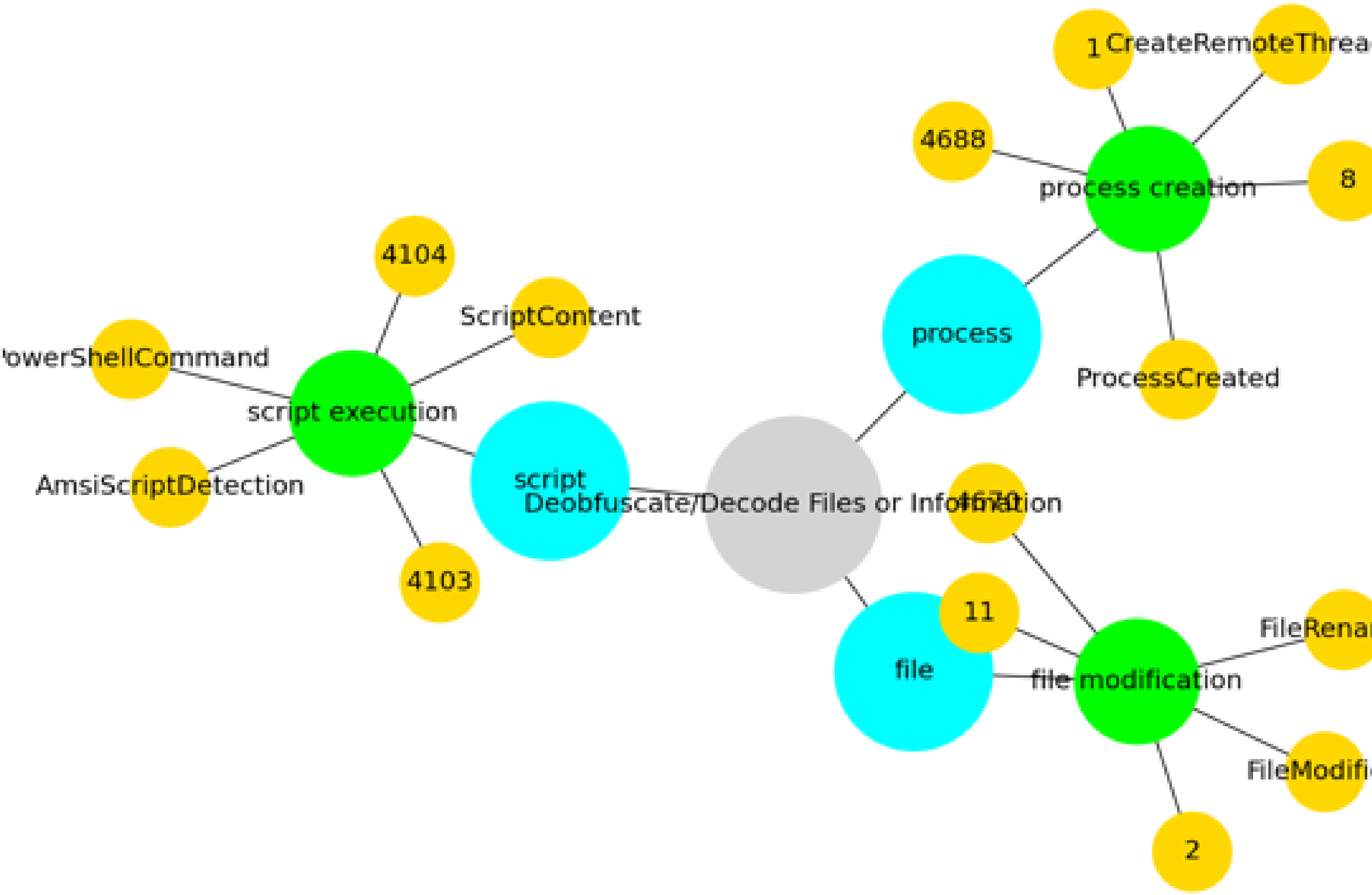
Tactic : defense-evasion

Technique : Deobfuscate/Decode Files or Information

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) 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.

One such example is use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file. (Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows <code>copy /b</code> command to reassemble binary fragments into a malicious payload. (Citation: Carbon Black Obfuscation Sept 2016)

Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)



3.18 T1059.003

Used by group : Fox Kitten, menuPass, Dragonfly, Threat Group-3390

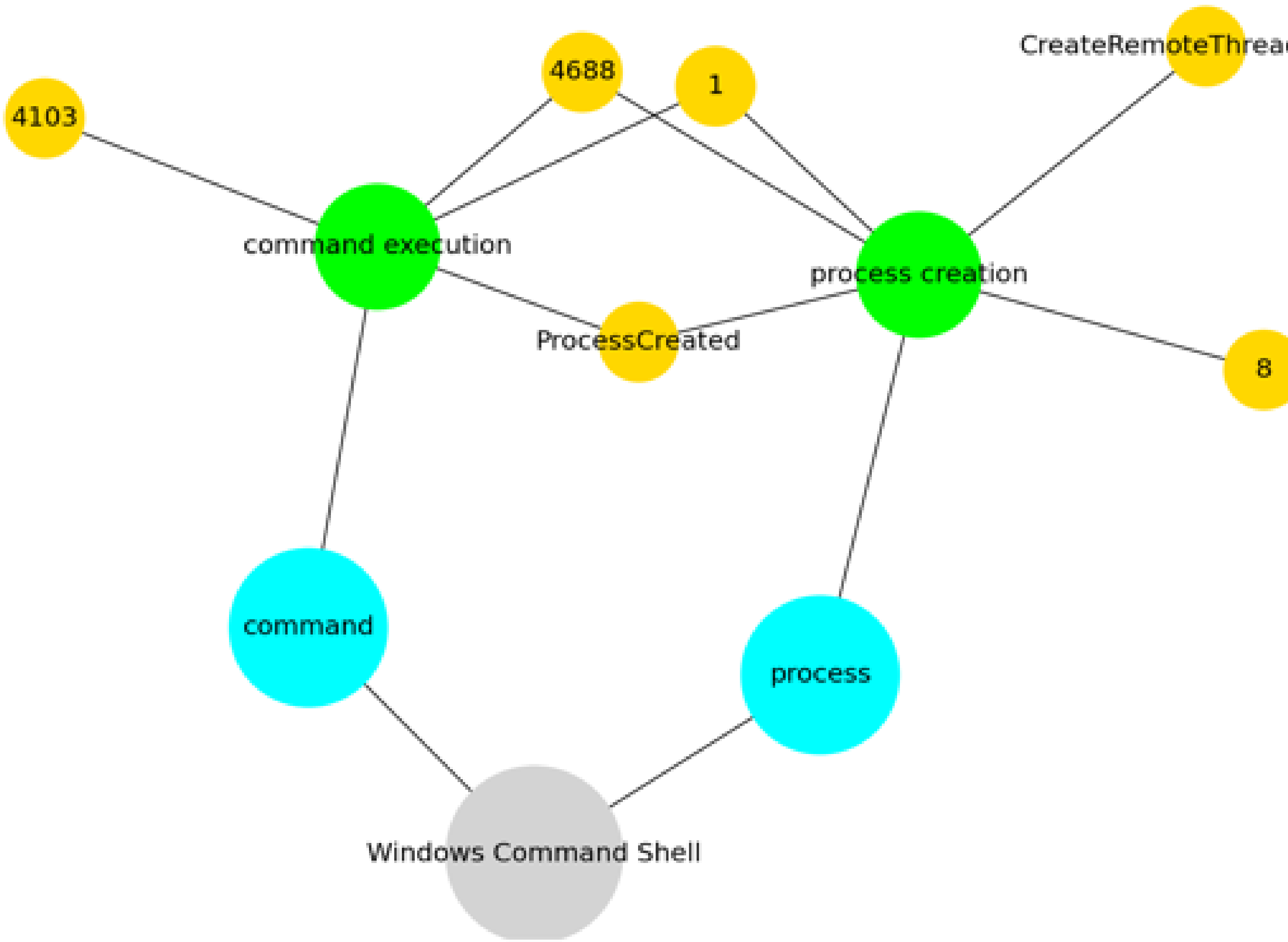
Tactic : execution

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.



3.19 T1560.001

Used by group : HAFNIUM, Fox Kitten, Gallmaker, menuPass

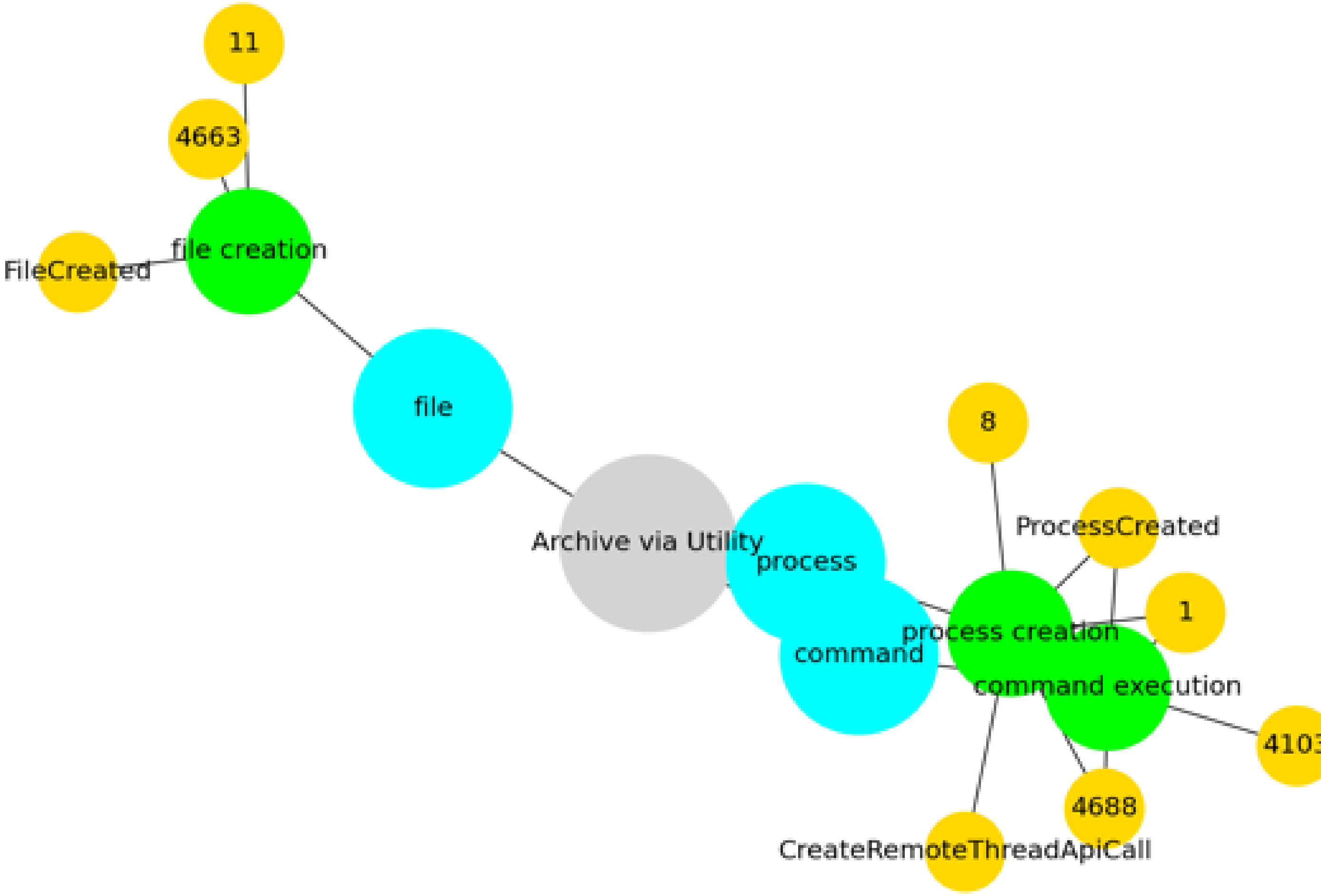
Tactic : collection

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)



3.20 T1016

Used by group : APT19, menuPass, Dragonfly, Threat Group-3390

Tactic : discovery

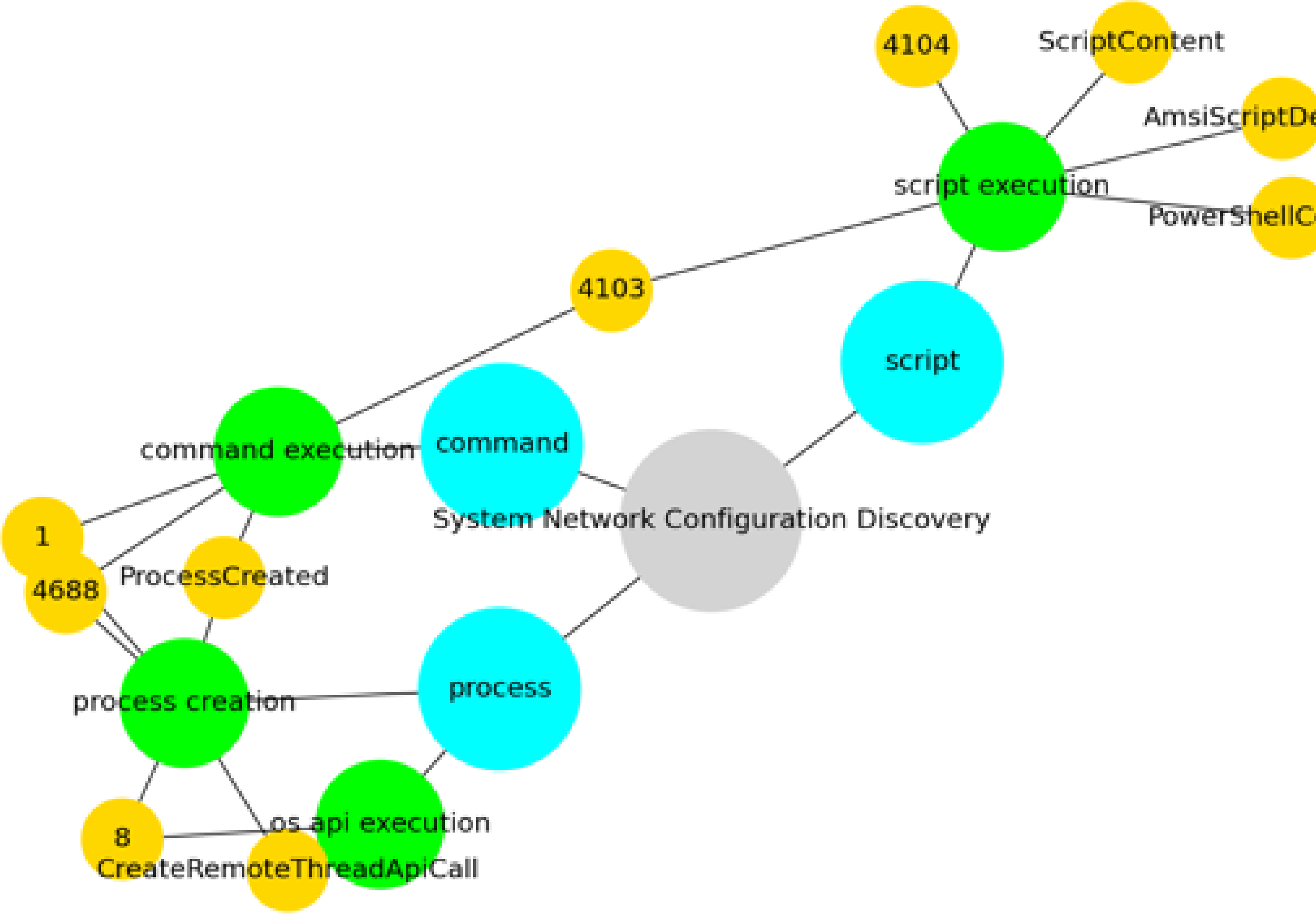
Technique : System Network Configuration Discovery

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.



3.21 T1003.003

Used by group : HAFNIUM, Fox Kitten, menuPass, Dragonfly

Tactic : credential-access

Technique : NTDS

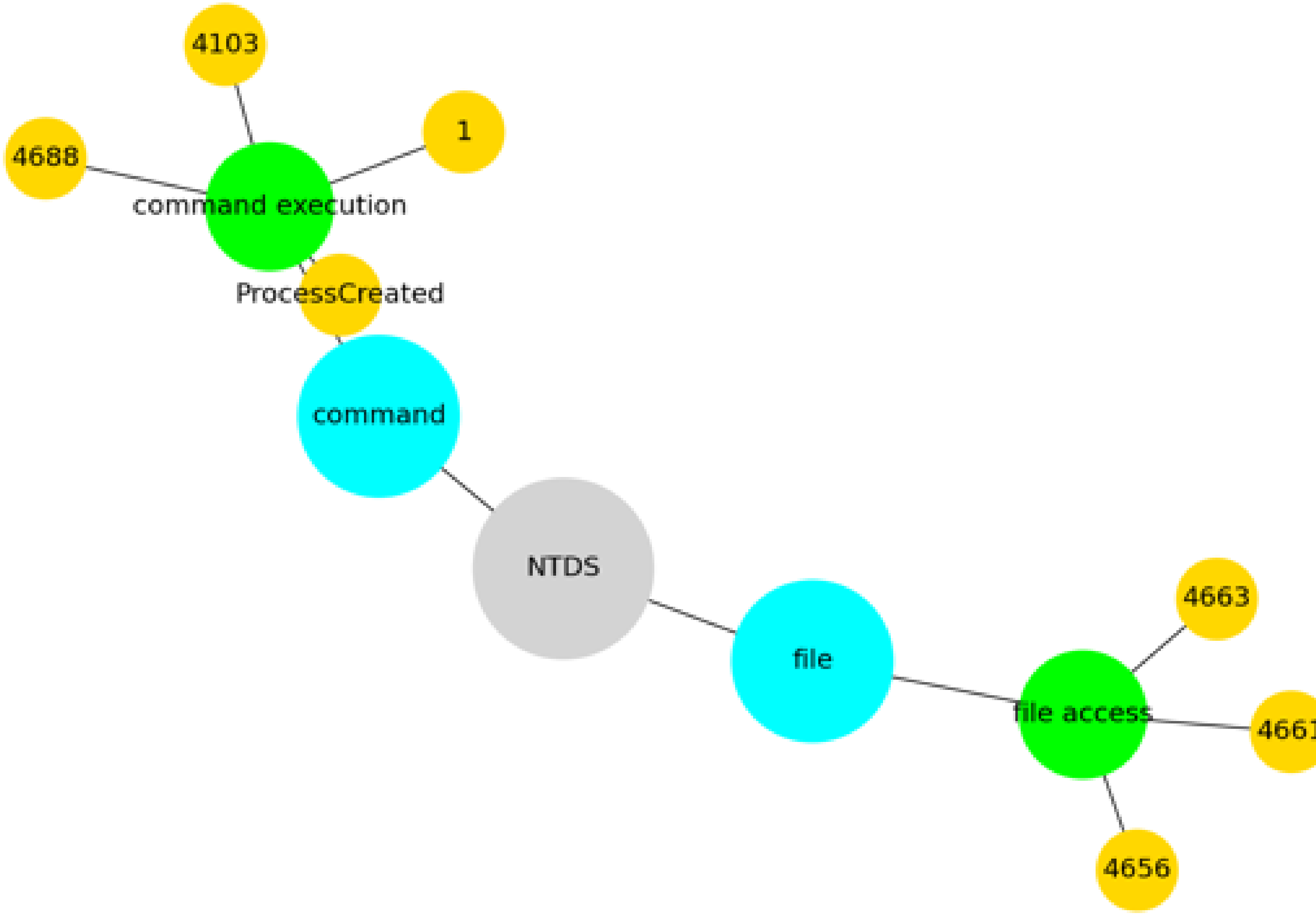
Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights. By default, the NTDS file

(NTDS.dit) is located in <code>%SystemRoot%\NTDS\Ntds.dit</code> of a domain controller.(Citation: Wikipedia Active Directory)

In addition to looking for NTDS files on active Domain Controllers, adversaries may search for backups that contain the same or similar information.(Citation: Metcalf 2015)

The following tools and techniques can be used to enumerate the NTDS file and the contents of the entire Active Directory hashes.

* Volume Shadow Copy
* secretsdump.py
* Using the in-built Windows tool, ntdsutil.exe
* Invoke-NinjaCopy



3.22 T1074.001

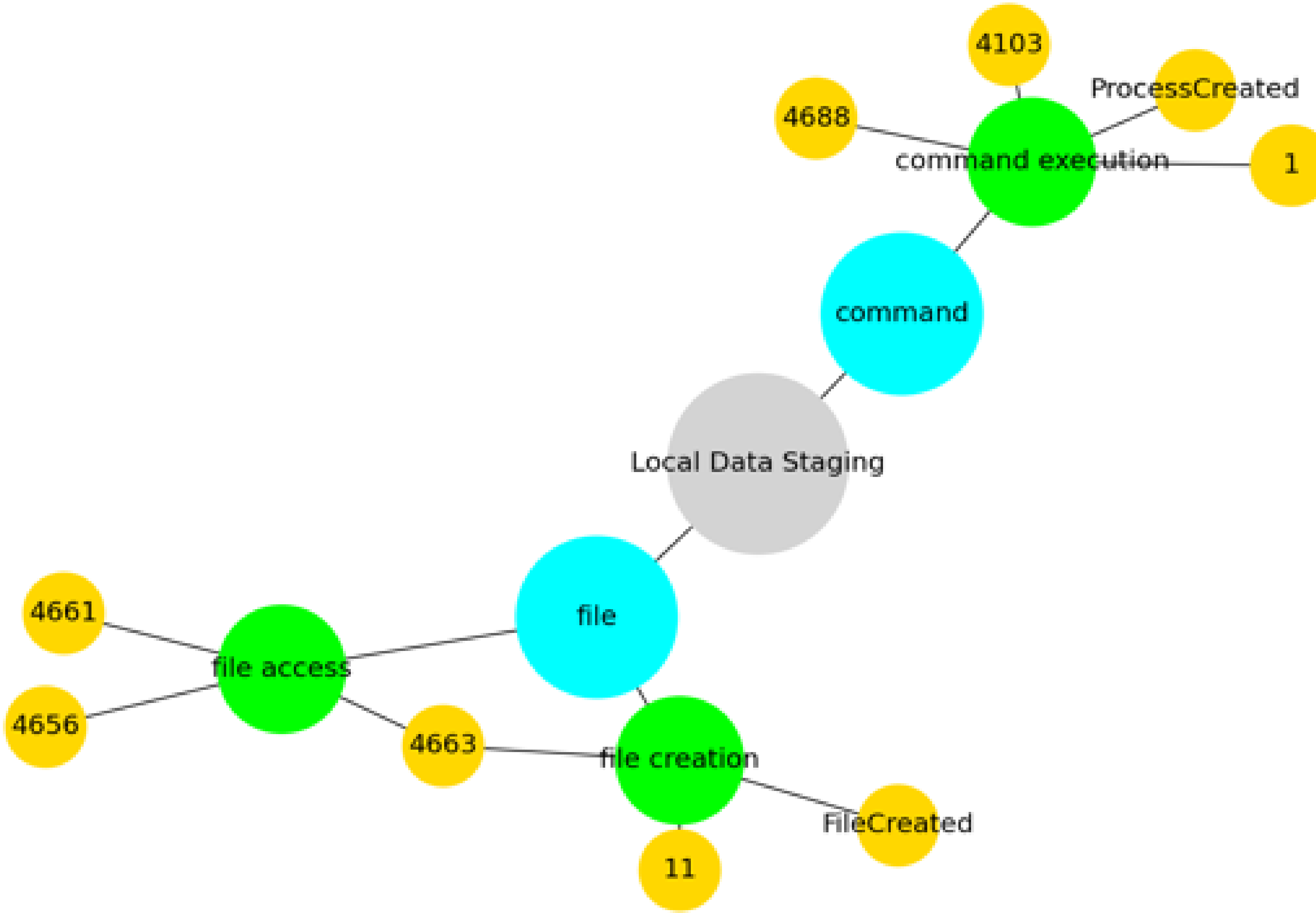
Used by group : Leviathan, menuPass, Dragonfly, Threat Group-3390

Tactic : collection

Technique : Local Data Staging

Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.

Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry.(Citation: Prevailion DarkWatchman 2021)



3.23 T1560

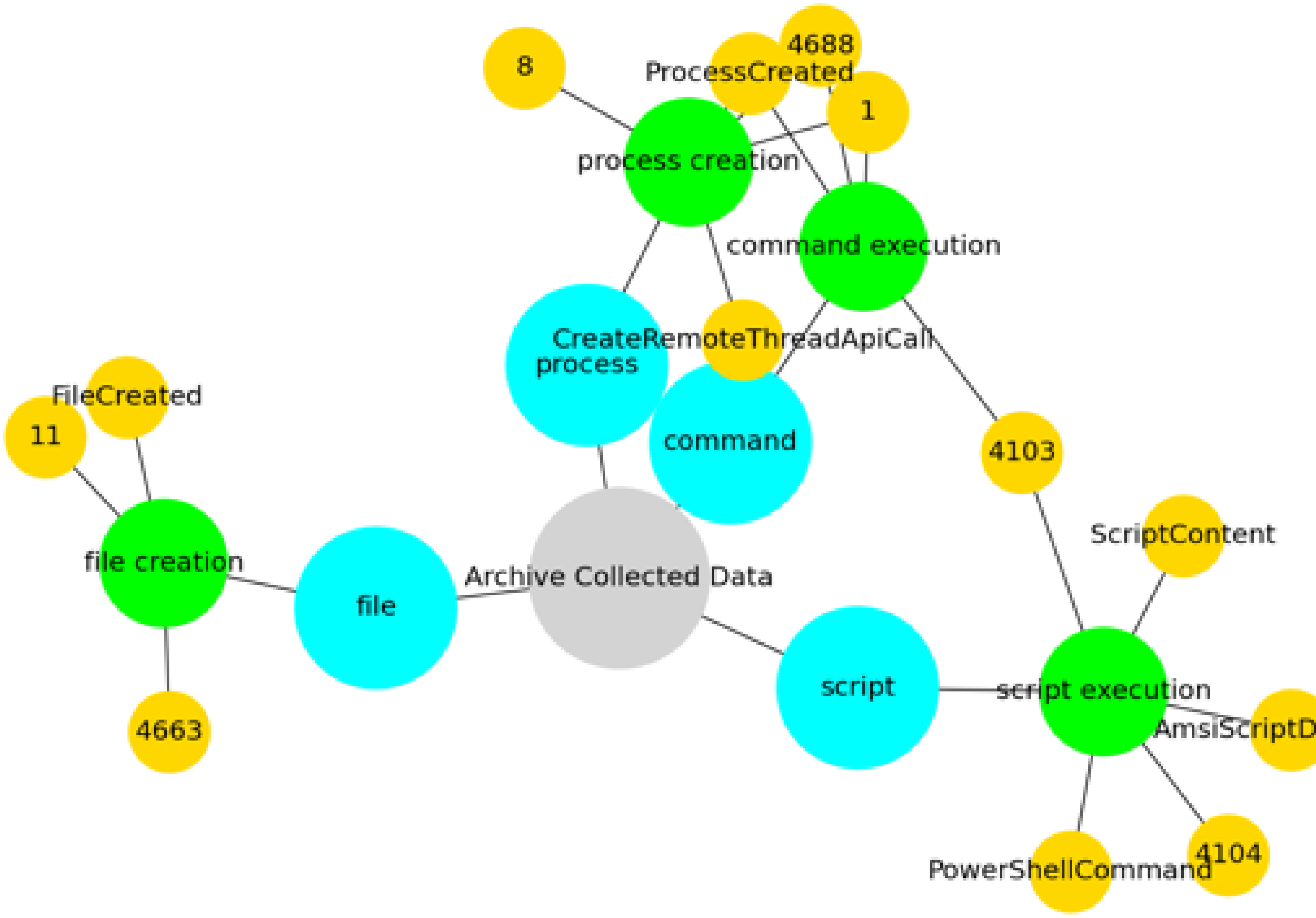
Used by group : Leviathan, menuPass, Dragonfly, Axiom

Tactic : collection

Technique : Archive Collected Data

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.



3.24 T1210

Used by group : Fox Kitten, menuPass, Dragonfly, Threat Group-3390

Tactic : lateral-movement

Technique : Exploitation of Remote Services

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. 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. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169)

Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

3.25 T1047

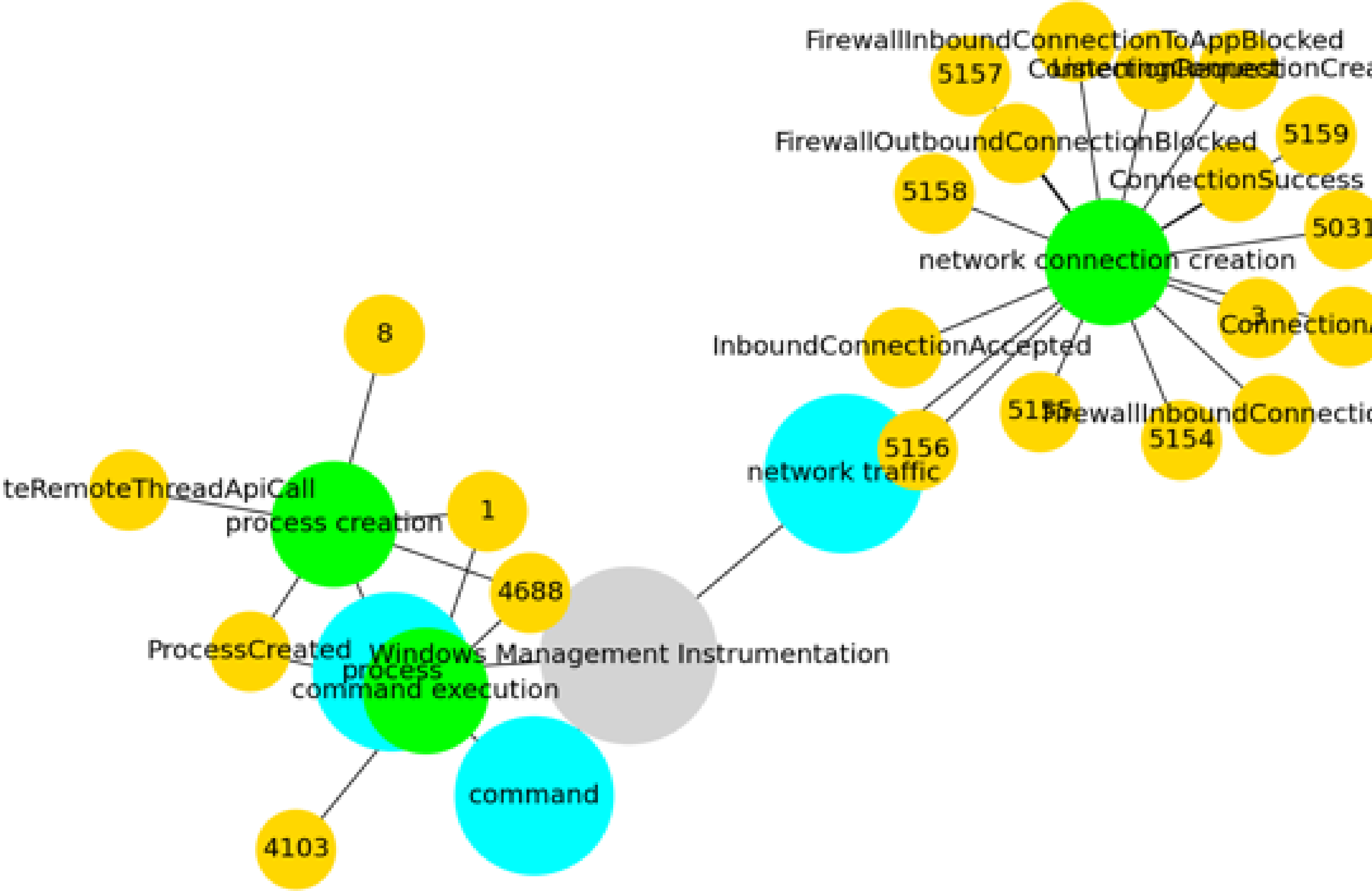
Used by group : Leviathan, menuPass, Threat Group-3390, Deep Panda

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)



3.26 T1583.001

Used by group : Transparent Tribe, Leviathan, menuPass, Dragonfly

Tactic : resource-development

Technique : Domains

Adversaries may purchase domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

Adversaries can use purchased domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries can also use internationalized domain names (IDNs) to create visually similar lookalike domains for use in operations.(Citation: CISA IDN ST05-016)

Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

3.27 T1059

Used by group : Fox Kitten, APT19, Dragonfly

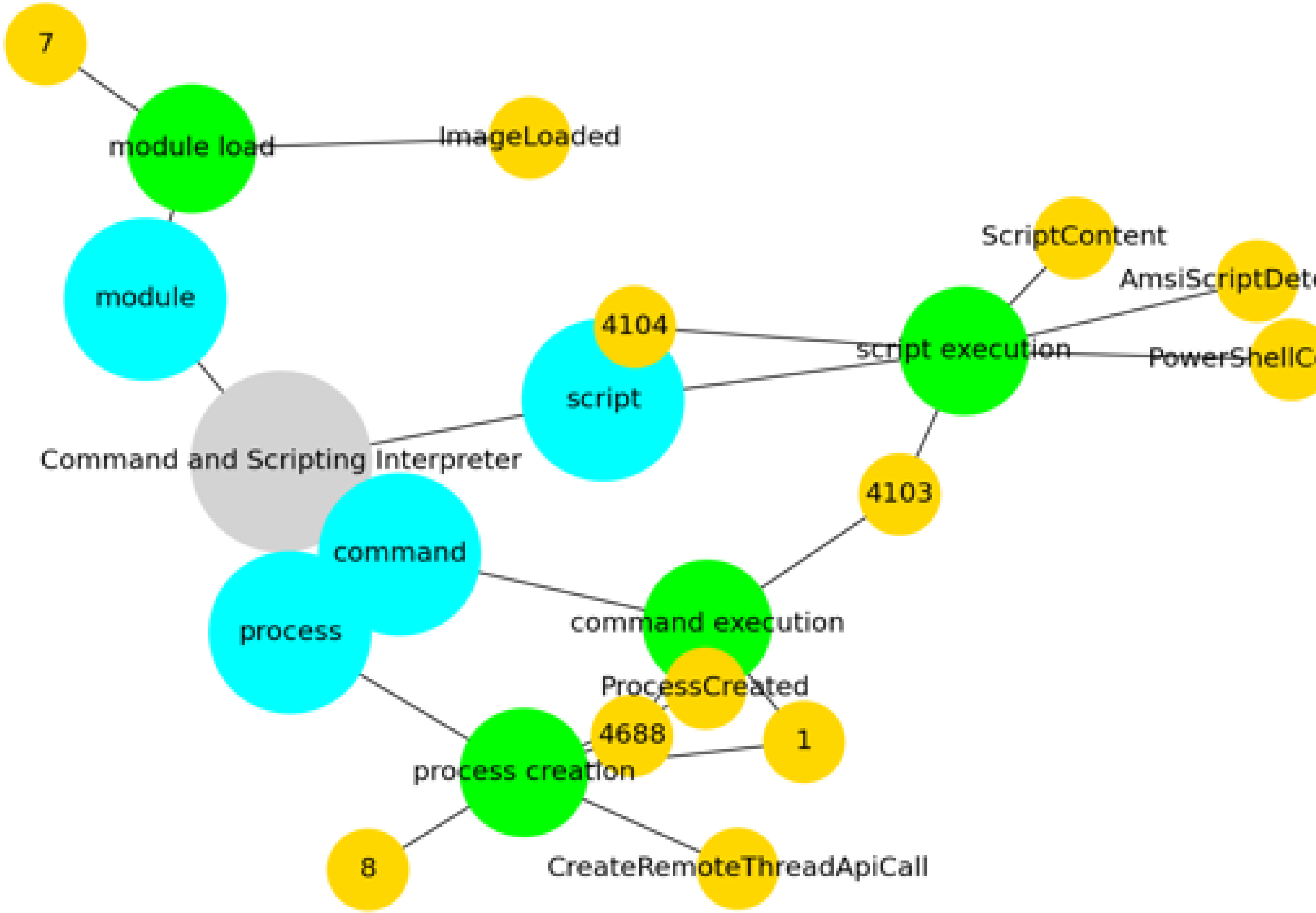
Tactic : execution

Technique : Command and Scripting Interpreter

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).

There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)



3.28 T1053.005

Used by group : Fox Kitten, menuPass, Dragonfly

Tactic : execution, persistence, privilege-escalation

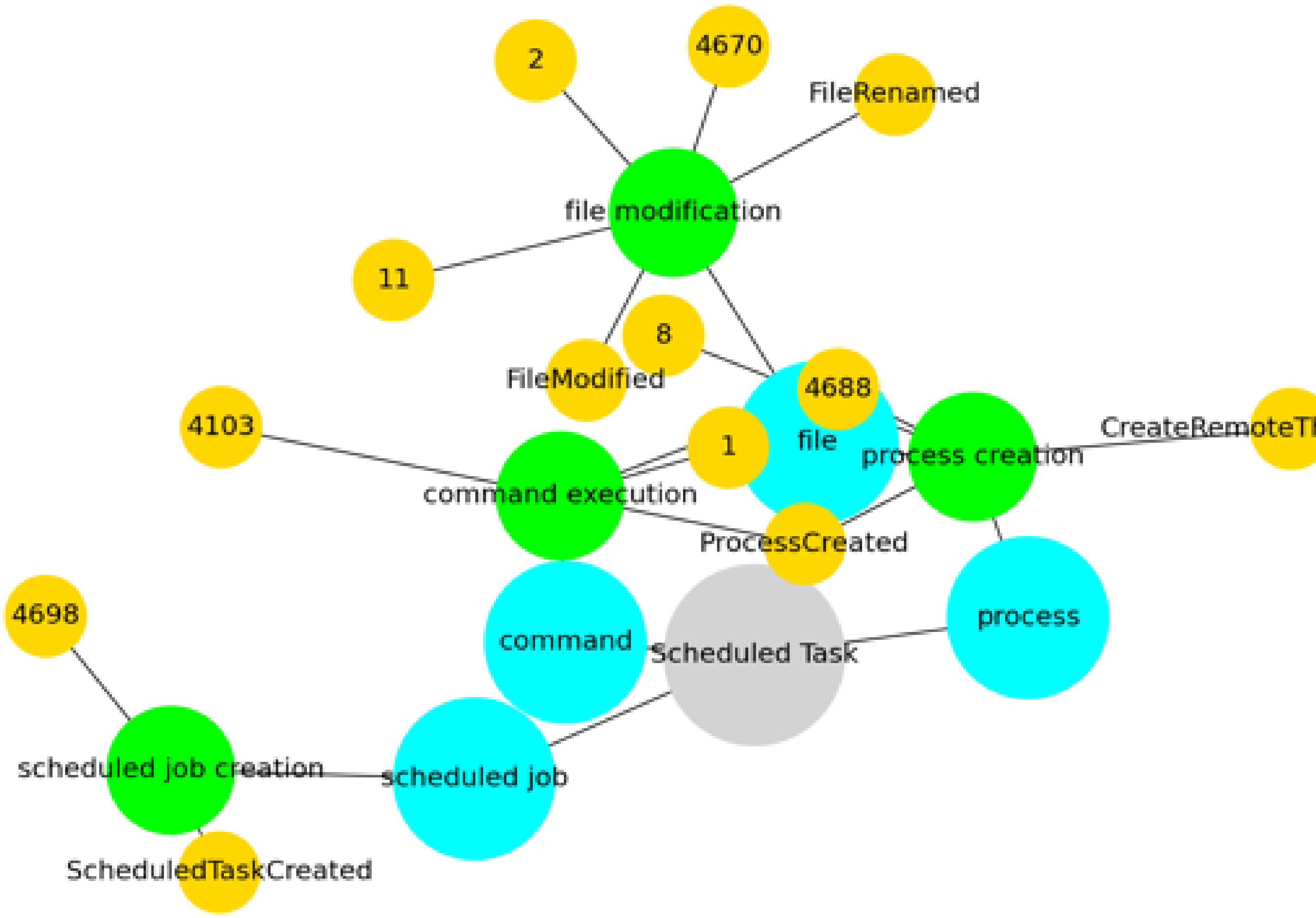
Technique : Scheduled Task

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)



3.29 T1546.008

Used by group : Fox Kitten, Deep Panda, Axiom

Tactic : privilege-escalation, persistence

Technique : Accessibility Features

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

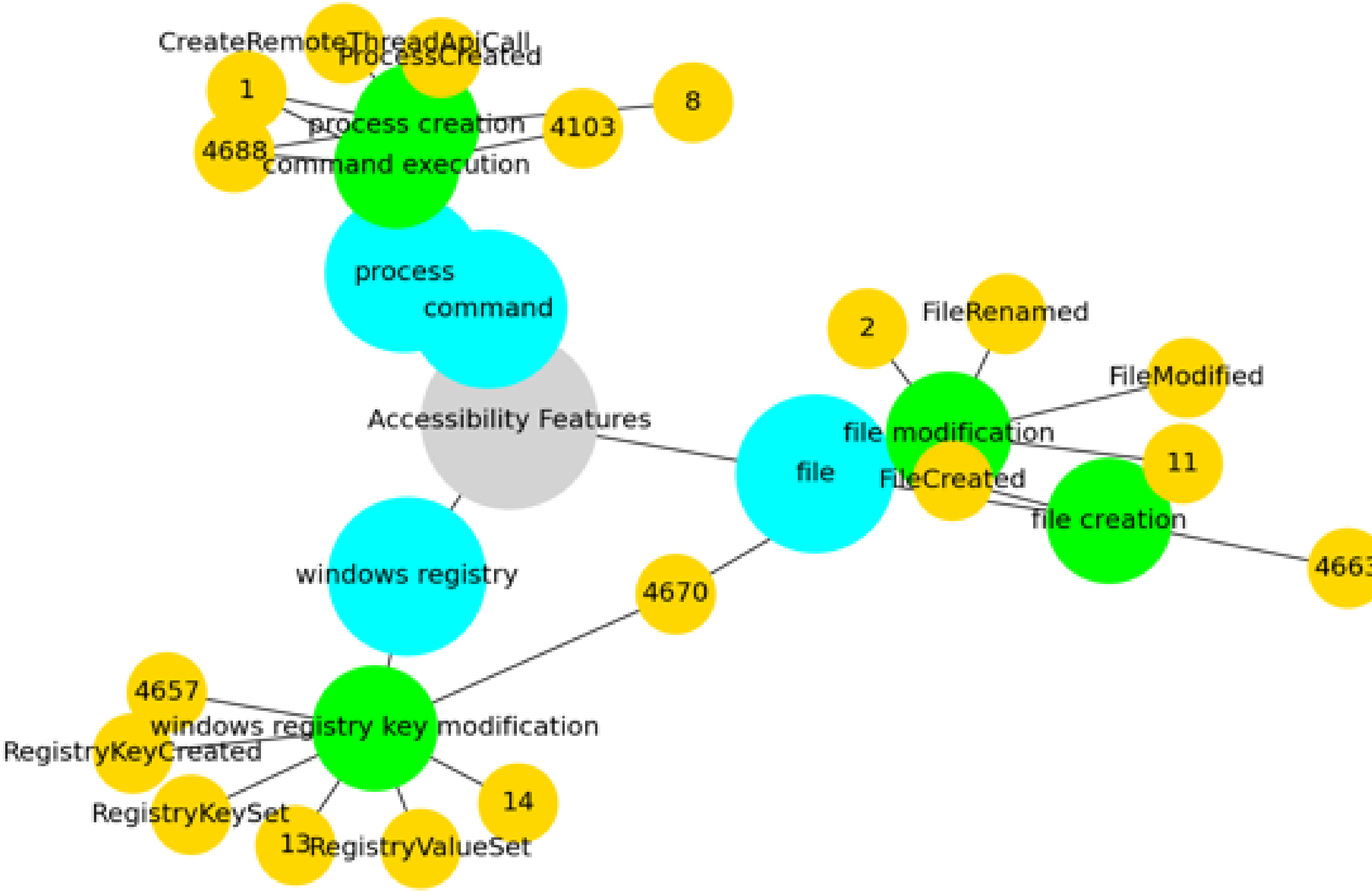
Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in <code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012) debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)(Citation: Narrator Accessibility Abuse)

* On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code>
* Magnifier: <code>C:\Windows\System32\Magnify.exe</code>
* Narrator: <code>C:\Windows\System32\Narrator.exe</code>
* Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code>
* App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>



3.30 T1083

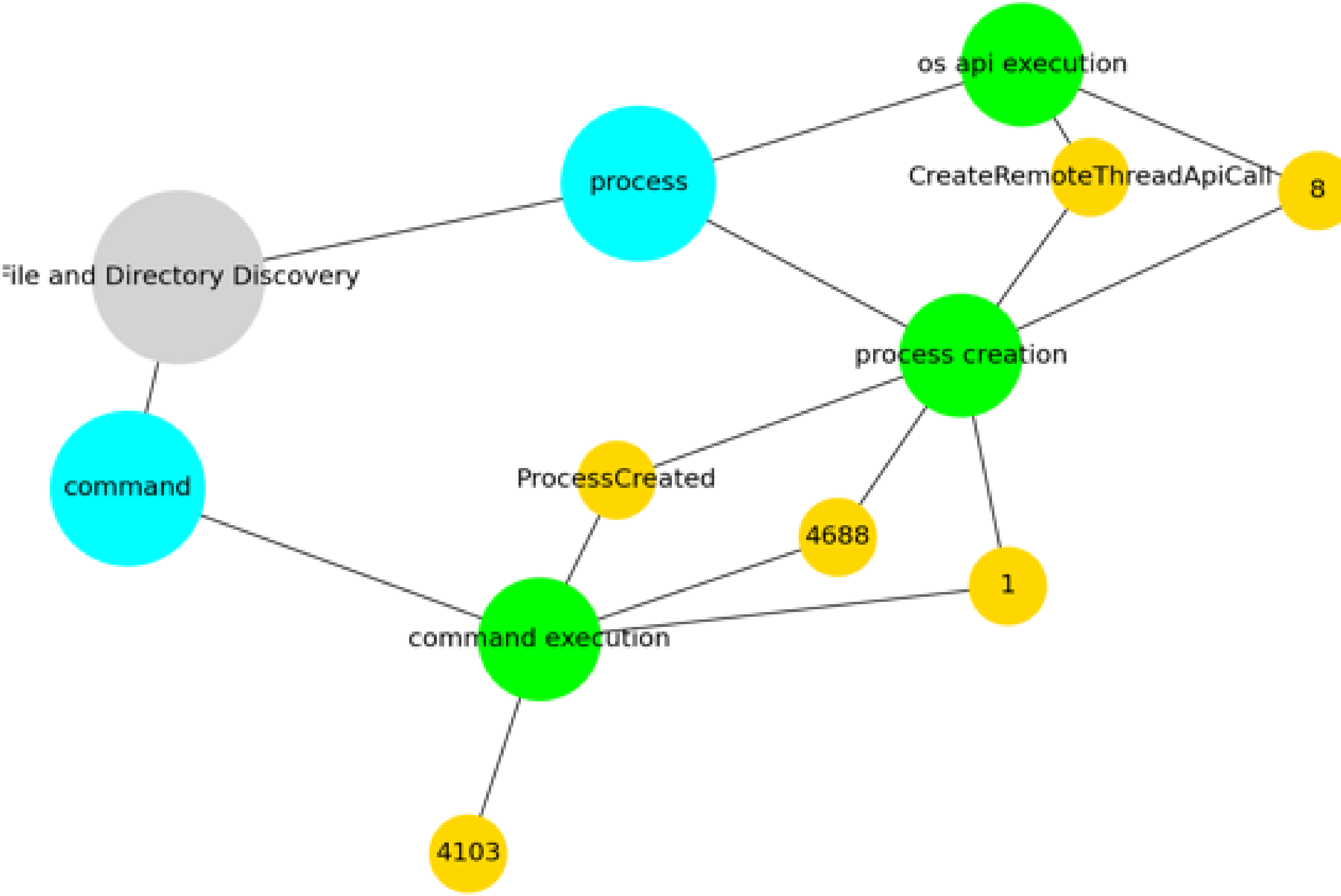
Used by group : Fox Kitten, menuPass, Dragonfly

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)



4. Annexes

< To be corrected or added in future releases >

4.1 List of all techniques used

technique_id	tactic	technique	group
T1059.001	execution	PowerShell	HAFNIUM, Fox Kitten, Gallmaker, APT19, Thrip, Leviathan, menuPass, Dragonfly, Threat Group-3390, Deep Panda
T1204.002	execution	Malicious File	Transparent Tribe, Ajax Security Team, Sharpshooter, Gallmaker, APT19, Elderwood, Leviathan, menuPass, Dragonfly, Threat Group-3390
T1566.001	initial-access	Spearphishing Attachment	Transparent Tribe, Ajax Security Team, Sharpshooter, Gallmaker, APT19, Elderwood, Leviathan, menuPass, Dragonfly, Threat Group-3390
T1105	command-and-control	Ingress Tool Transfer	Ajax Security Team, HAFNIUM, Fox Kitten, Sharpshooter, Elderwood, Leviathan, menuPass, Dragonfly, Threat Group-3390
T1027	defense-evasion	Obfuscated Files or Information	Transparent Tribe, Fox Kitten, Gallmaker, APT19, Elderwood, Leviathan, menuPass, Threat Group-3390
T1189	initial-access	Drive-by Compromise	Transparent Tribe, APT19, Elderwood, Leviathan, Dragonfly, Threat Group-3390, Axiom
T1203	execution	Exploitation for Client Execution	Transparent Tribe, Elderwood, Leviathan, Dragonfly, Threat Group-3390, Axiom
T1505.003	persistence	Web Shell	HAFNIUM, Fox Kitten, Leviathan, Dragonfly, Threat Group-3390, Deep Panda
T1078	defense-evasion, persistence, privilege-escalation, initial-access	Valid Accounts	Fox Kitten, Leviathan, menuPass, Dragonfly, Threat Group-3390, Axiom
T1190	initial-access	Exploit Public-Facing Application	HAFNIUM, Fox Kitten, menuPass, Dragonfly, Threat Group-3390, Axiom
T1547.001	persistence, privilege-escalation	Registry Run Keys / Startup Folder	Sharpshooter, APT19, Leviathan, Dragonfly, Threat Group-3390
T1588.002	resource-development	Tool	APT19, Thrip, menuPass, Dragonfly, Threat Group-3390
T1005	collection	Data from Local System	Fox Kitten, menuPass, Dragonfly, Threat Group-3390, Axiom
T1018	discovery	Remote System Discovery	Fox Kitten, menuPass, Dragonfly, Threat Group-3390, Deep Panda
T1021.001	lateral-movement	Remote Desktop Protocol	Fox Kitten, Leviathan, menuPass, Dragonfly, Axiom
T1003.001	credential-access	LSASS Memory	HAFNIUM, Fox Kitten, Leviathan, Threat Group-3390
T1140	defense-evasion	Deobfuscate/Decode Files or Information	APT19, Leviathan, menuPass, Threat Group-3390
T1059.003	execution	Windows Command Shell	Fox Kitten, menuPass, Dragonfly, Threat Group-3390
T1560.001	collection	Archive via Utility	HAFNIUM, Fox Kitten, Gallmaker, menuPass
T1016	discovery	System Network Configuration Discovery	APT19, menuPass, Dragonfly, Threat Group-3390
T1003.003	credential-access	NTDS	HAFNIUM, Fox Kitten, menuPass, Dragonfly
T1074.001	collection	Local Data Staging	Leviathan, menuPass, Dragonfly, Threat Group-3390
T1560	collection	Archive Collected Data	Leviathan, menuPass, Dragonfly, Axiom
T1210	lateral-movement	Exploitation of Remote Services	Fox Kitten, menuPass, Dragonfly, Threat Group-3390
T1047	execution	Windows Management Instrumentation	Leviathan, menuPass, Threat Group-3390, Deep Panda
T1583.001	resource-development	Domains	Transparent Tribe, Leviathan, menuPass, Dragonfly
T1059	execution	Command and Scripting Interpreter	Fox Kitten, APT19, Dragonfly
T1053.005	execution, persistence, privilege-escalation	Scheduled Task	Fox Kitten, menuPass, Dragonfly
T1546.008	privilege-escalation, persistence	Accessibility Features	Fox Kitten, Deep Panda, Axiom
T1083	discovery	File and Directory Discovery	Fox Kitten, menuPass, Dragonfly
T1608.004	resource-development	Drive-by Target	Transparent Tribe, Dragonfly, Threat Group-3390
T1046	discovery	Network Service Discovery	Fox Kitten, menuPass, Threat Group-3390
T1012	discovery	Query Registry	Fox Kitten, Dragonfly, Threat Group-3390
T1559.002	execution	Dynamic Data Exchange	Sharpshooter, Gallmaker, Leviathan
T1021.004	lateral-movement	SSH	Fox Kitten, Leviathan, menuPass
T1218.010	defense-evasion	Regsvr32	APT19, Leviathan, Deep Panda
T1033	discovery	System Owner/User Discovery	APT19, Dragonfly, Threat Group-3390
T1074.002	collection	Remote Data Staging	Leviathan, menuPass, Threat Group-3390

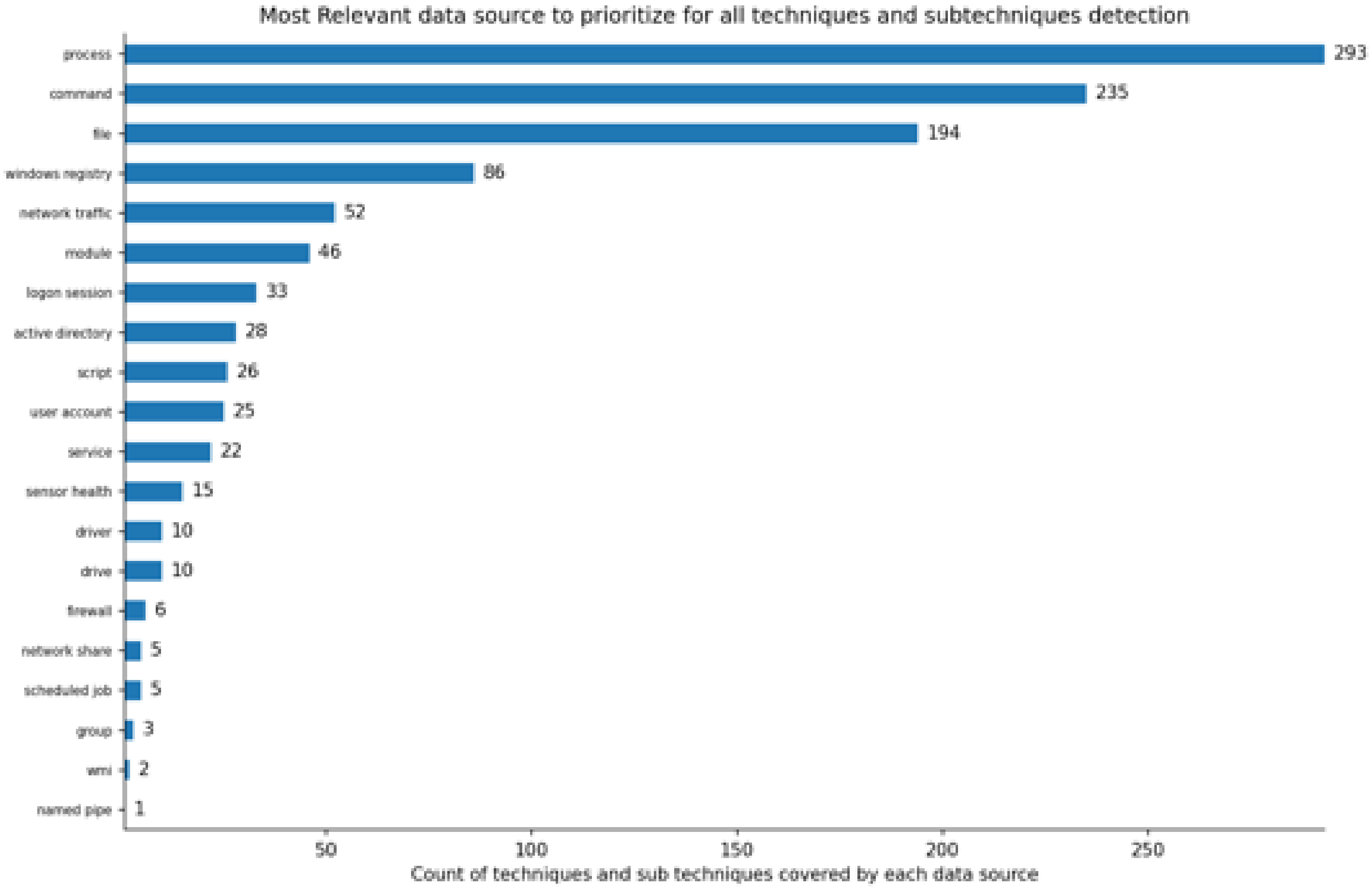
T1133	persistence, initial-access	External Remote Services	Leviathan, Dragonfly, Threat Group-3390
T1003.004	credential-access	LSA Secrets	menuPass, Dragonfly, Threat Group-3390
T1003.002	credential-access	Security Account Manager	menuPass, Dragonfly, Threat Group-3390
T1070.004	defense-evasion	File Deletion	menuPass, Dragonfly, Threat Group-3390
T1574.002	persistence, privilege-escalation, defense-evasion	DLL Side-Loading	APT19, menuPass, Threat Group-3390
T1112	defense-evasion	Modify Registry	APT19, Dragonfly, Threat Group-3390
T1583.003	resource-development	Virtual Private Server	HAFNIUM, Dragonfly, Axiom
T1087.002	discovery	Domain Account	Fox Kitten, menuPass, Dragonfly
T1567.002	exfiltration	Exfiltration to Cloud Storage	HAFNIUM, Leviathan, Threat Group-3390
T1204.001	execution	Malicious Link	Transparent Tribe, Elderwood, Leviathan
T1059.005	execution	Visual Basic	Transparent Tribe, Sharpshooter, Leviathan
T1566.002	initial-access	Spearphishing Link	Transparent Tribe, Elderwood, Leviathan
T1071.001	command-and-control	Web Protocols	HAFNIUM, APT19, Threat Group-3390
T1056.001	collection, credential-access	Keylogging	Ajax Security Team, menuPass, Threat Group-3390
T1036.005	defense-evasion	Match Legitimate Name or Location	Transparent Tribe, Fox Kitten, menuPass
T1027.002	defense-evasion	Software Packing	Elderwood, Threat Group-3390
T1106	execution	Native API	Sharpshooter, menuPass
T1583.006	resource-development	Web Services	HAFNIUM, APT17
T1564.003	defense-evasion	Hidden Window	APT19, Deep Panda
T1543.003	persistence, privilege-escalation	Windows Service	APT19, Threat Group-3390
T1055.012	defense-evasion, privilege-escalation	Process Hollowing	menuPass, Threat Group-3390
T1087.001	discovery	Local Account	Fox Kitten, Threat Group-3390
T1553.002	defense-evasion	Code Signing	Leviathan, menuPass
T1195.002	initial-access	Compromise Software Supply Chain	Dragonfly, Threat Group-3390
T1003	credential-access	OS Credential Dumping	Leviathan, Axiom
T1574.001	persistence, privilege-escalation, defense-evasion	DLL Search Order Hijacking	menuPass, Threat Group-3390
T1036	defense-evasion	Masquerading	menuPass, Dragonfly
T1049	discovery	System Network Connections Discovery	menuPass, Threat Group-3390
T1119	collection	Automated Collection	menuPass, Threat Group-3390
T1547.009	persistence, privilege-escalation	Shortcut Modification	Leviathan, Dragonfly
T1199	initial-access	Trusted Relationship	menuPass, Threat Group-3390
T1132.001	command-and-control	Standard Encoding	HAFNIUM, APT19
T1218.011	defense-evasion	Rundll32	HAFNIUM, APT19
T1585.001	resource-development	Social Media Accounts	Fox Kitten, Leviathan
T1110	credential-access	Brute Force	Fox Kitten, Dragonfly
T1585	resource-development	Establish Accounts	Fox Kitten, APT17
T1136.001	persistence	Local Account	Fox Kitten, Dragonfly
T1555.005	credential-access	Password Managers	Fox Kitten, Threat Group-3390
T1572	command-and-control	Protocol Tunneling	Fox Kitten, Leviathan
T1114.002	collection	Remote Email Collection	HAFNIUM, Dragonfly
T1021.002	lateral-movement	SMB/Windows Admin Shares	Fox Kitten, Deep Panda
T1039	collection	Data from Network Shared Drive	Fox Kitten, menuPass
T1566	initial-access	Phishing	Axiom
T1564.002	defense-evasion	Hidden Users	Dragonfly
T1562.004	defense-evasion	Disable or Modify System Firewall	Dragonfly
T1069.002	discovery	Domain Groups	Dragonfly
T1584.005	resource-development	Botnet	Axiom
T1059.006	execution	Python	Dragonfly
T1583.002	resource-development	DNS Server	Axiom
T1591.002	reconnaissance	Business Relationships	Dragonfly

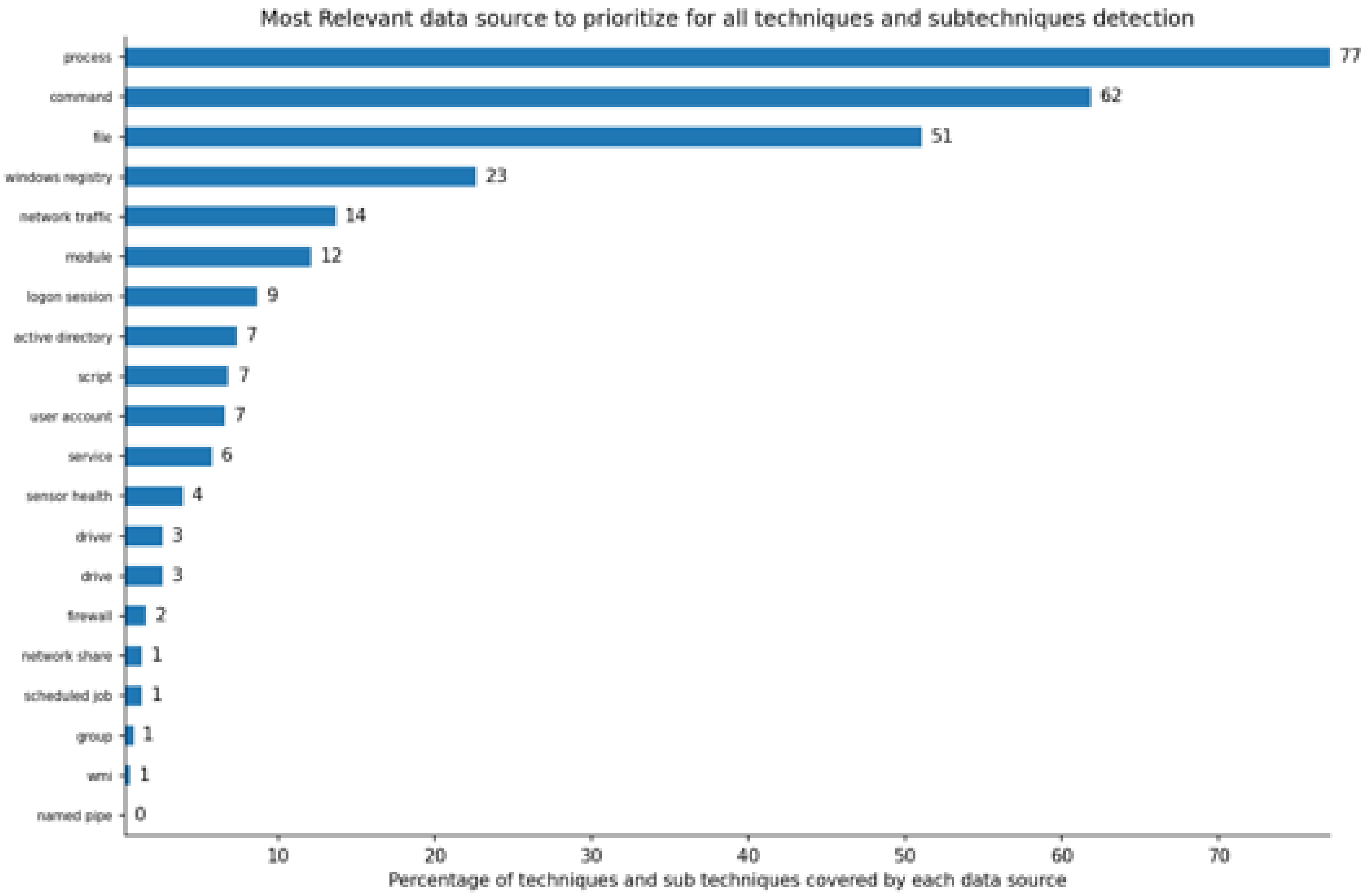
T1584.004	resource-development	Server	Dragonfly
T1563.002	lateral-movement	RDP Hijacking	Axiom
T1001.002	command-and-control	Steganography	Axiom
T1595.002	reconnaissance	Vulnerability Scanning	Dragonfly
T1598.003	reconnaissance	Spearphishing Link	Dragonfly
T1598.002	reconnaissance	Spearphishing Attachment	Dragonfly
T1070.001	defense-evasion	Clear Windows Event Logs	Dragonfly
T1110.002	credential-access	Password Cracking	Dragonfly
T1027.005	defense-evasion	Indicator Removal from Tools	Deep Panda
T1548.002	privilege-escalation, defense-evasion	Bypass User Account Control	Threat Group-3390
T1068	privilege-escalation	Exploitation for Privilege Escalation	Threat Group-3390
T1070.005	defense-evasion	Network Share Connection Removal	Threat Group-3390
T1021.006	lateral-movement	Windows Remote Management	Threat Group-3390
T1560.002	collection	Archive via Library	Threat Group-3390
T1562.002	defense-evasion	Disable Windows Event Logging	Threat Group-3390
T1030	exfiltration	Data Transfer Size Limits	Threat Group-3390
T1608.002	resource-development	Upload Tool	Threat Group-3390
T0817	initial-access-ics	Drive-by Compromise	Dragonfly
T1053.002	execution, persistence, privilege-escalation	At	Threat Group-3390
T0862	initial-access-ics	Supply Chain Compromise	Dragonfly
T1057	discovery	Process Discovery	Deep Panda
T1071	command-and-control	Application Layer Protocol	Dragonfly
T1098	persistence	Account Manipulation	Dragonfly
T1113	collection	Screen Capture	Dragonfly
T1135	discovery	Network Share Discovery	Dragonfly
T1187	credential-access	Forced Authentication	Dragonfly
T1221	defense-evasion	Template Injection	Dragonfly
T1608.001	resource-development	Upload Malware	Threat Group-3390
T1534	lateral-movement	Internal Spearphishing	Leviathan
T1218.004	defense-evasion	InstallUtil	menuPass
T1078.003	defense-evasion, persistence, privilege-escalation, initial-access	Local Accounts	HAFNIUM
T1048.003	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	Thrip
T1592.004	reconnaissance	Client Configurations	HAFNIUM
T1082	discovery	System Information Discovery	APT19
T1584.001	resource-development	Domains	Transparent Tribe
T1590.005	reconnaissance	IP Addresses	HAFNIUM
T1590	reconnaissance	Gather Victim Network Information	HAFNIUM
T1589.002	reconnaissance	Email Addresses	HAFNIUM
T1055	defense-evasion, privilege-escalation	Process Injection	Sharpshooter
T1136.002	persistence	Domain Account	HAFNIUM
T1070.003	defense-evasion	Clear Command History	menuPass
T1095	command-and-control	Non-Application Layer Protocol	HAFNIUM
T1090	command-and-control	Proxy	Fox Kitten
T1102	command-and-control	Web Service	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
T1036.004	defense-evasion	Masquerade Task or Service	Fox Kitten
T1219	command-and-control	Remote Access Software	Thrip

T1589.001	reconnaissance	Credentials	Leviathan
T1586.002	resource-development	Email Accounts	Leviathan
T1586.001	resource-development	Social Media Accounts	Leviathan
T1036.003	defense-evasion	Rename System Utilities	menuPass
T1568	command-and-control	Dynamic Resolution	Transparent Tribe
T1568.001	command-and-control	Fast Flux DNS	menuPass
T1090.002	command-and-control	External Proxy	menuPass
T1041	exfiltration	Exfiltration Over C2 Channel	Leviathan
T1564.001	defense-evasion	Hidden Files and Directories	Transparent Tribe
T1197	defense-evasion, persistence	BITS Jobs	Leviathan
T1021.005	lateral-movement	VNC	Fox Kitten
T1055.001	defense-evasion, privilege-escalation	Dynamic-link Library Injection	Leviathan
T1546.003	privilege-escalation, persistence	Windows Management Instrumentation Event Subscription	Leviathan
T1027.001	defense-evasion	Binary Padding	Leviathan
T1027.003	defense-evasion	Steganography	Leviathan
T1566.003	initial-access	Spearphishing via Service	Ajax Security Team
T1555.003	credential-access	Credentials from Web Browsers	Ajax Security Team
T1102.003	command-and-control	One-Way Communication	Leviathan
T1090.003	command-and-control	Multi-hop Proxy	Leviathan
T1585.002	resource-development	Email Accounts	Leviathan
T1553	defense-evasion	Subvert Trust Controls	Axiom

4.2 Data sources reference for covering all mitre technique

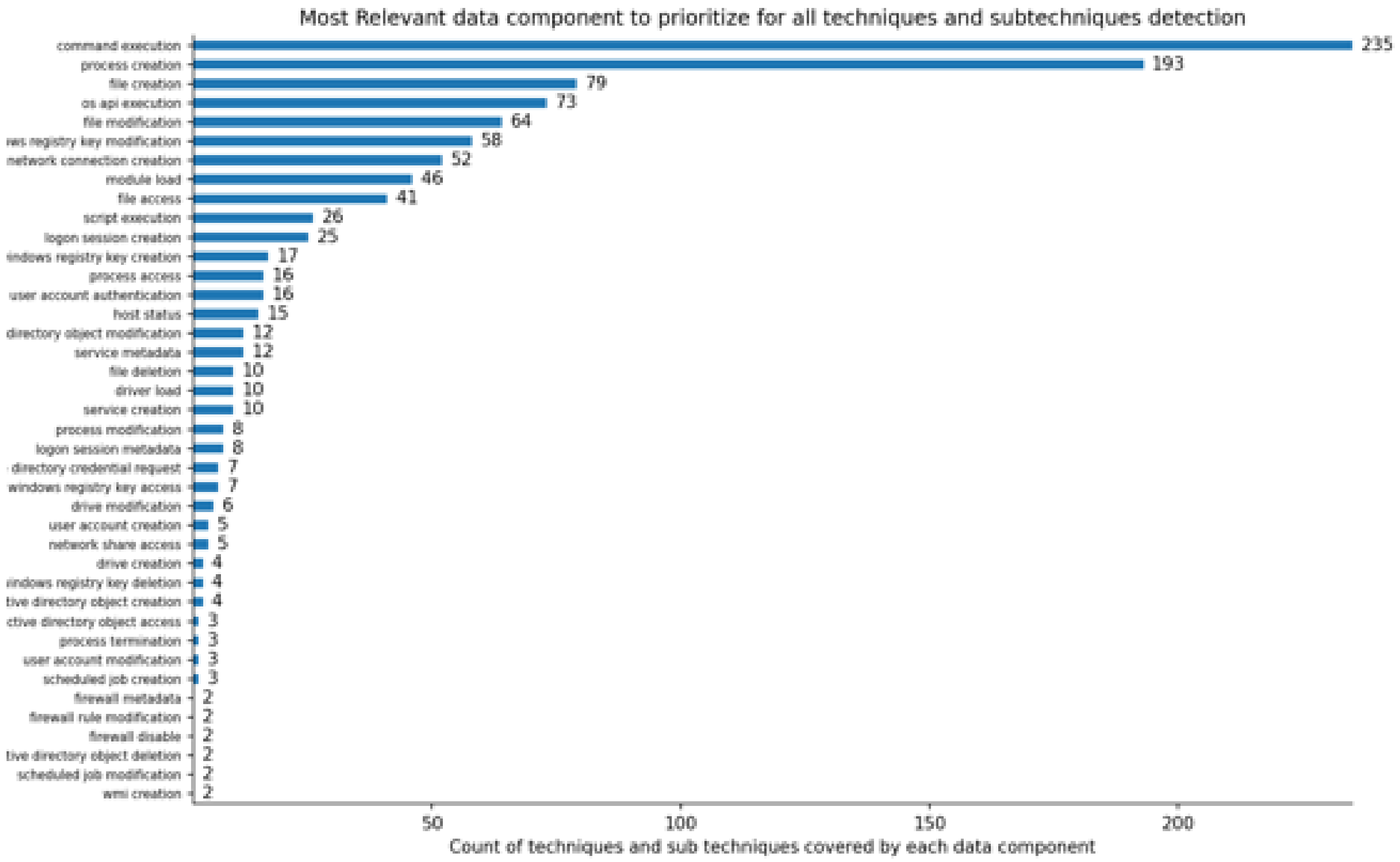
< To be corrected or added in future releases >

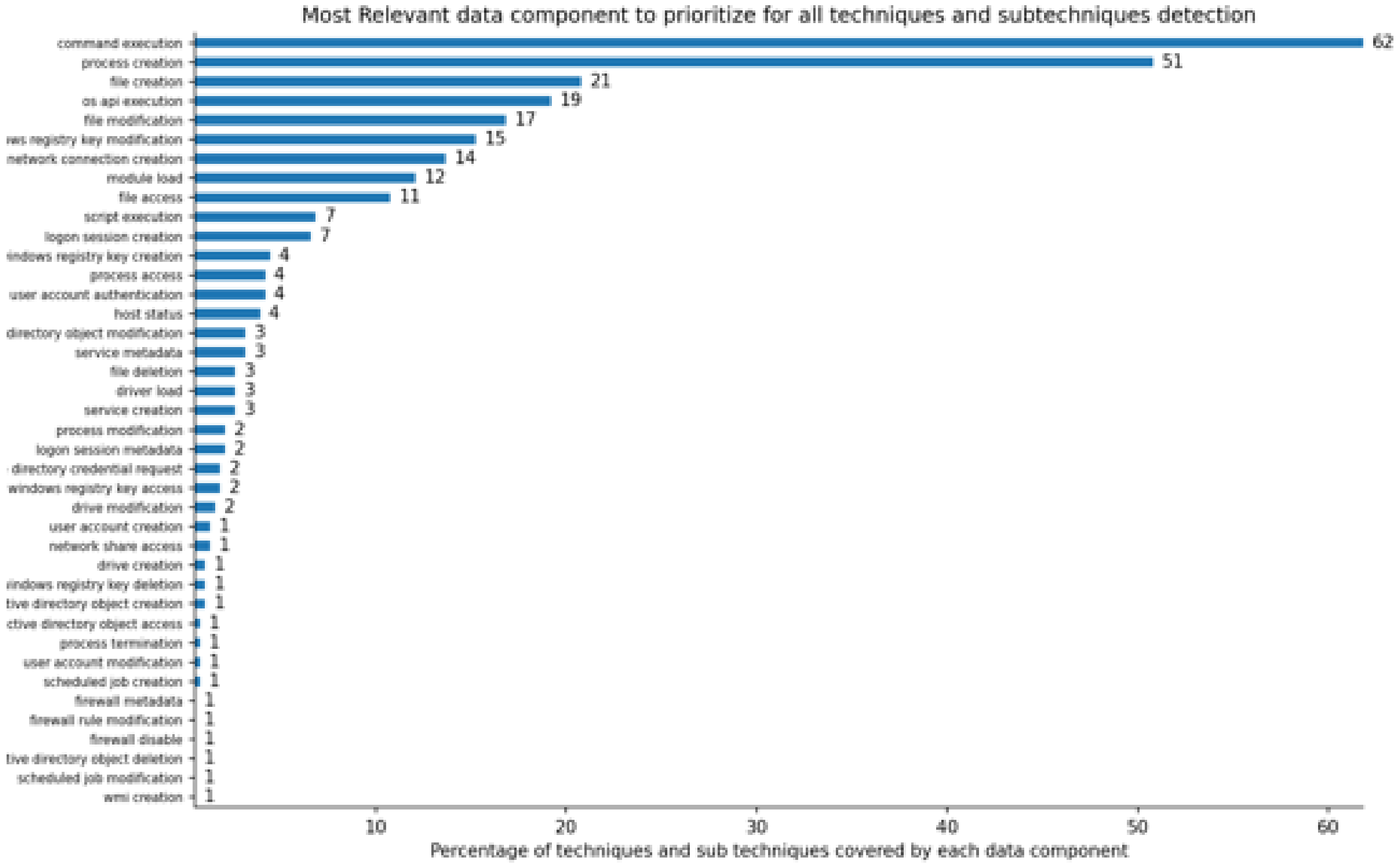

Most Relevant data source to prioritize for all techniques and subtechniques detection
process 293
command 235
file 194
windows registry 86
network traffic 52
module 46
logon session 33
active directory 28
script 26
user account 25
service 22
sensor health 15
driver 10
drive 10
firewall 6
network share 5
scheduled job 5
group 3
wmi 2
named pipe 1
50
100
150
200
250
Count of techniques and sub techniques covered by each data source



4.3 Data component reference for covering all mitre technique

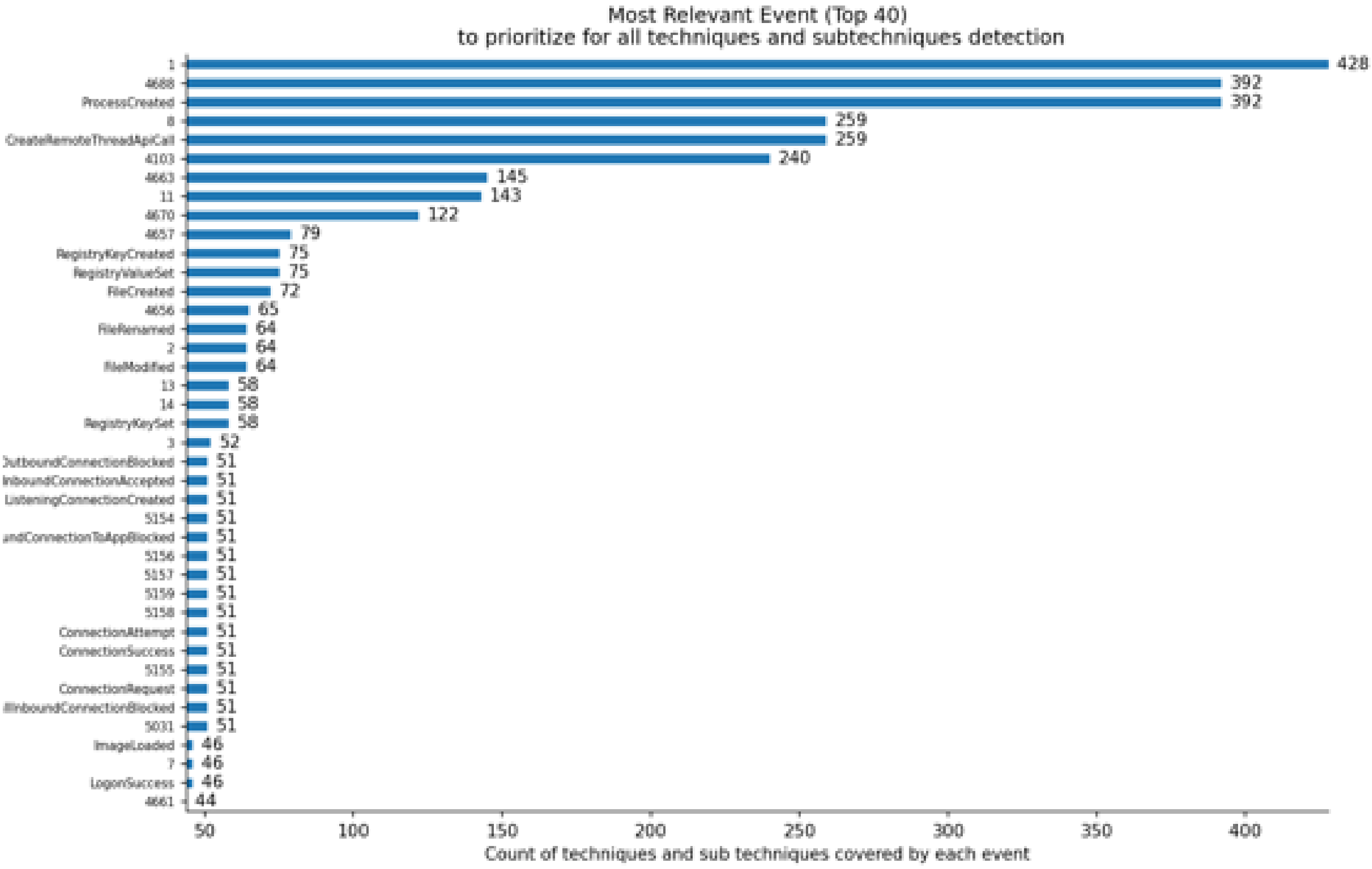
< To be corrected or added in future releases >

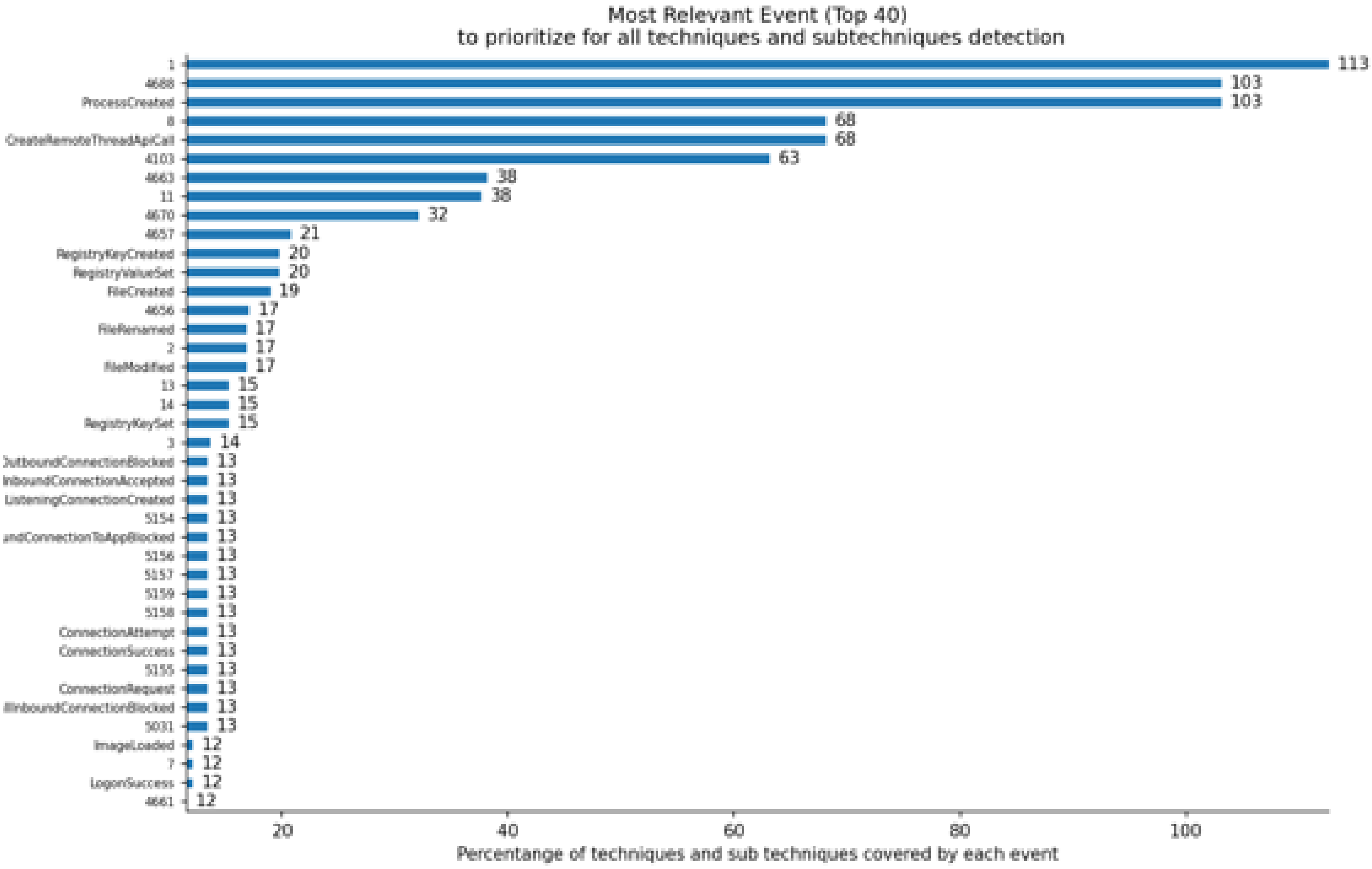

Most Relevant data component to prioritize for all techniques and subtechniques detection
command execution 235
process creation 193
file creation 79
os api execution 73
file modification 64
ws registry key modification 58
network connection creation 52
module load 46
file access 41
script execution 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
428
4688
392
ProcessCreated
392
8
259
CreateRemoteThreadApiCall
259
4103
240
4663
145
11
143
4670
122
4657
79
RegistryKeyCreated
75
RegistryValueSet
75
FileCreated
72
4656
65
FileRenamed
64
2
64
FileModified
64
13
58
14
58
RegistryKeySet
58
3
52
OutboundConnectionBlocked
51
InboundConnectionAccepted
51
ListeningConnectionCreated
51
5154
51
undConnectionToAppBlocked
51
5156
51
5157
51
5159
51
5158
51
ConnectionAttempt
51
ConnectionSuccess
51
5155
51
ConnectionRequest
51
llInboundConnectionBlocked
51
5031
51
ImageLoaded
46
7
46
LogonSuccess
46
4661
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
113
4688
103
ProcessCreated
103
8
68
CreateRemoteThreadApiCall
68
4103
63
4663
38
11
38
4670
32
4657
21
RegistryKeyCreated
20
RegistryValueSet
20
FileCreated
19
4656
17
FileRenamed
17
2
17
FileModified
17
13
15
14
15
RegistryKeySet
15
3
14
utboundConnectionBlocked
13
InboundConnectionAccepted
13
ListeningConnectionCreated
13
5154
13
undConnectionToAppBlocked
13
5156
13
5157
13
5159
13
5158
13
ConnectionAttempt
13
ConnectionSuccess
13
5155
13
ConnectionRequest
13
InboundConnectionBlocked
13
5031
13
ImageLoaded
12
7
12
LogonSuccess
12
4661
12
20
40
60
80
100
Percentange of techniques and sub techniques covered by each event