

---

# INTRODUCING SOC COOKBOOK FOR MANUFACTURING

PROVIDING A CUSTOM COOKBOOK ON ADVERSARIES, TTPS AND STATISTICS TO MAXIMIZE  
DETECTION

THOMAS BILLAUT



---

# WHOAMI

FEEL FREE TO PING ME



@tbillaut



<https://fr.linkedin.com/in/thomasbillaut/>



Thomas.billaut@protonmail.com

---

## AGENDA

- Why, how, what
- Manufacturing sector threat actors
- Manufacturing sector TTP statistics
- Most used manufacturing sector techniques

---

## AGENDA

- Why, how, what
- Manufacturing sector threat actors
- Manufacturing sector TTP statistics
- Most used manufacturing sector techniques

---

# WHY, HOW, WHAT


## INTRODUCING SOC COOKBOOK FOR MANUFACTURING SECTOR

Today's SOC (Security Operational Center) activity is **overwhelming**.

Talented people, well defined process and governance are **not anymore** sufficient for keeping the adversary out of your enterprise.

**Automation** is a must have to make the job done at scale (on premise and cloud infrastructures).

And **threat intel** must be used daily for short/middle term prioritization.



This project aims at **helping SOC** teams while providing a custom cookbook on adversaries, TTPs and statistics to maximize detection.

Based on **MITRE ATT&CK** and **OSSEM** datasets, the main idea is to provide a dedicated baseline to operationalize SOC efficiency from collections to remediations. Note the approach is based on known and shared attacks. There are accordingly some **bias**.

The report is customized for the **manufacturing sector** and generated **automatically**

This presentation gives an **overview** of what can be found in the report. It is also an example of what can be done with the materials produced by this project.

Words and idea can change the world...

---

## AGENDA

- Why, how, what
- Manufacturing sector threat actors
- Manufacturing sector TTP statistics
- Most used manufacturing sector techniques

# MANUFACTURING SECTOR THREAT ACTORS

## [KNOW YOUR ENEMY](#)



Threat actors

### Fox Kitten

Alias : Fox Kitten, UNC757, PIONEER KITTEN, Parisite

Fox Kitten 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.

### APT-C-36

Alias : APT-C-36, Blind Eagle

APT-C-36 is a suspected South America espionage group that has been active since at least 2018.

### SilverTerrier

SilverTerrier is a Nigerian threat group that has been seen active since 2014

### APT19

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

APT19 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

Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open-source information if the groups are the same

### Leviathan

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

Leviathan 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.

### BRONZE BUTLER

Alias : BRONZE BUTLER, REDBALDKNIGHT, Tick

BRONZE BUTLER is a cyber espionage group with likely Chinese origins that has been active since at least 2008.

### menuPass

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

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass 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

### Threat Group-3390

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

Threat Group-3390 is a Chinese threat group that has extensively used strategic Web compromises to target victims.

### Axiom

Alias : Axiom, Group 72

Axiom 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 and Winnti Group but the two groups appear to be distinct based on differences in reporting on TTPs and targeting

### APT18

Alias : APT18, TG-0416, Dynamite Panda, Threat Group-0416

---

## AGENDA

- Why, how, what
- Manufacturing sector threat actors
- Manufacturing sector TTP statistics
- Most used manufacturing sector techniques



# MANUFACTURING SECTOR TTP STATISTICS

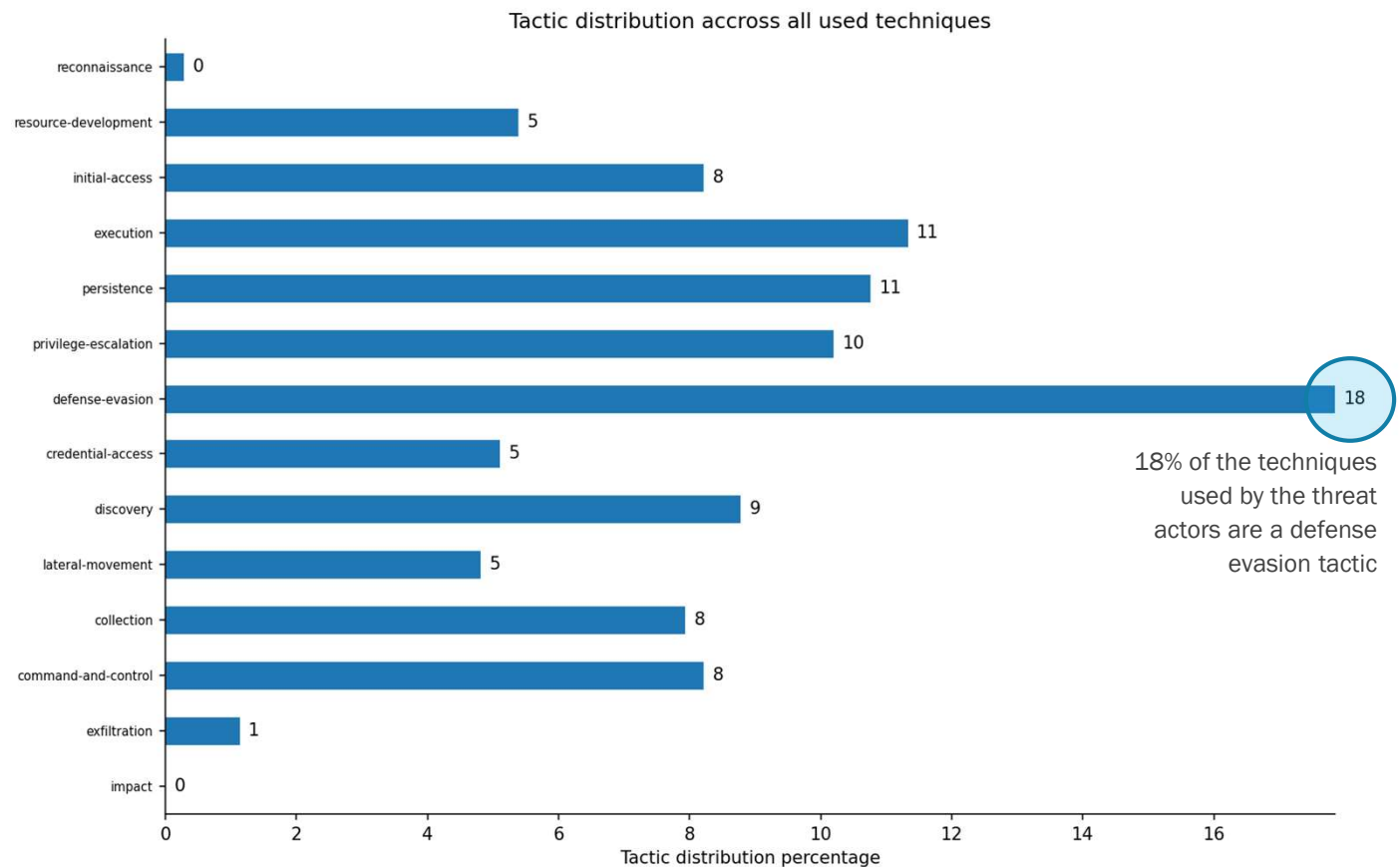
[UNDERSTAND YOUR ENEMY 1/4](#)

136

Techniques have been used by the adversaries

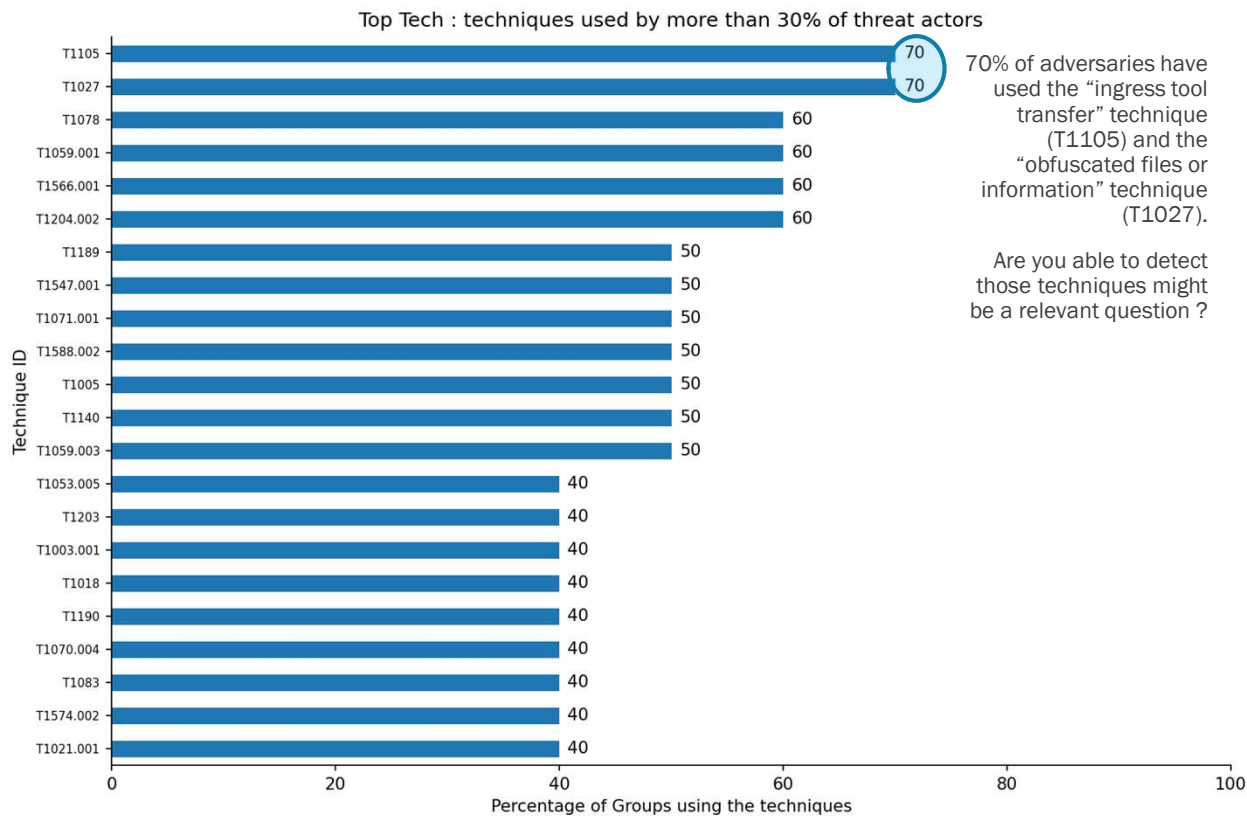
22

Techniques have been used by more than 30% of the adversaries



# MANUFACTURING SECTOR TTP STATISTICS

UNDERSTAND YOUR ENEMY AND THINK ABOUT DETECTION 2/4



**“KNOWLEDGE IS OF  
NO VALUE UNLESS  
YOU PUT IT INTO  
PERSPECTIVE.**

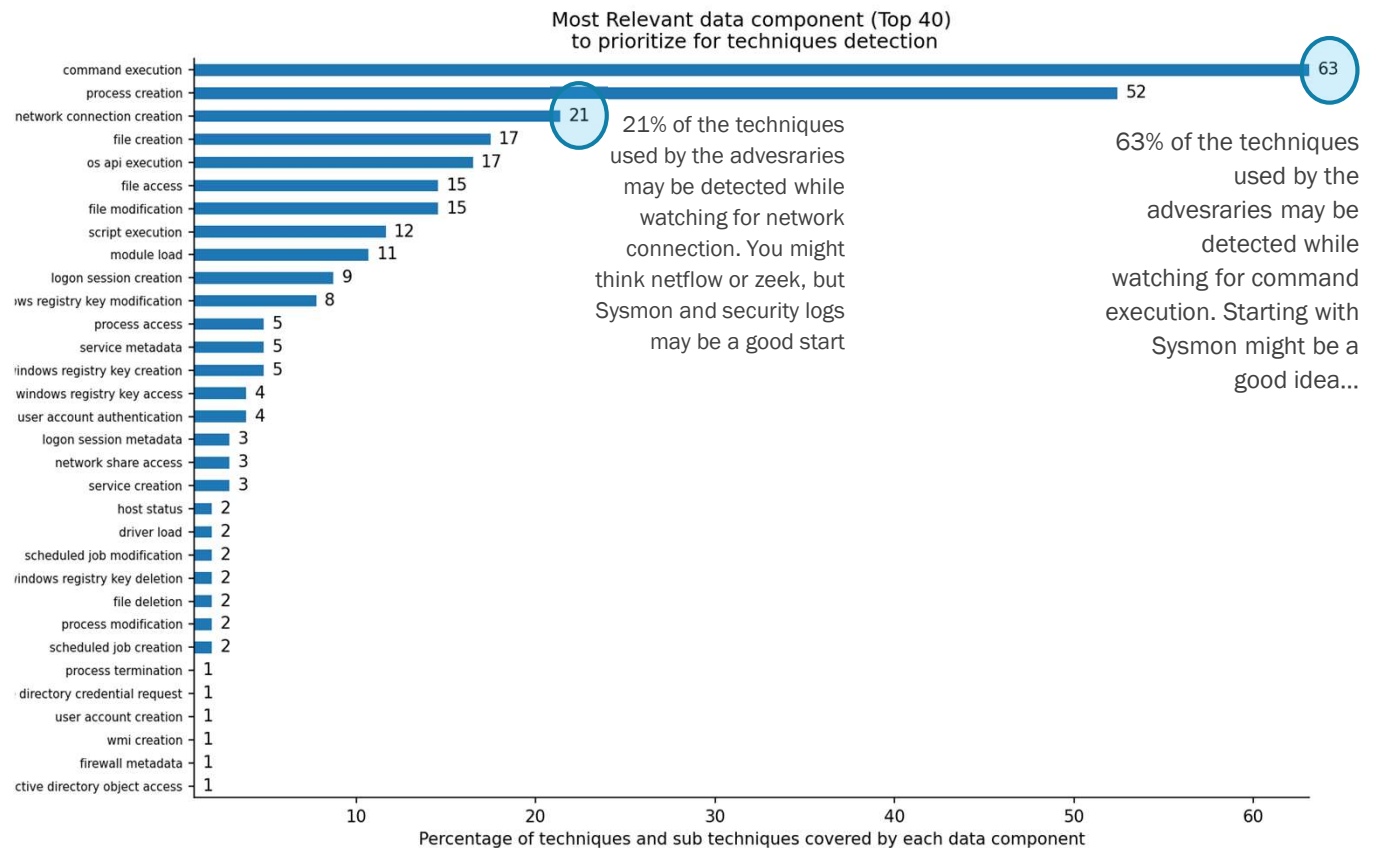
ANTON CHEKHOV

# MANUFACTURING SECTOR TTP STATISTICS

UNDERSTAND YOUR ENEMY AND THINK ABOUT COLLECTION 3/4

**“THE KEY IS NOT  
TO PRIORITIZE  
WHAT'S ON YOUR  
SCHEDULE, BUT TO  
SCHEDULE YOUR  
PRIORITIES**

STEPHEN COVEY

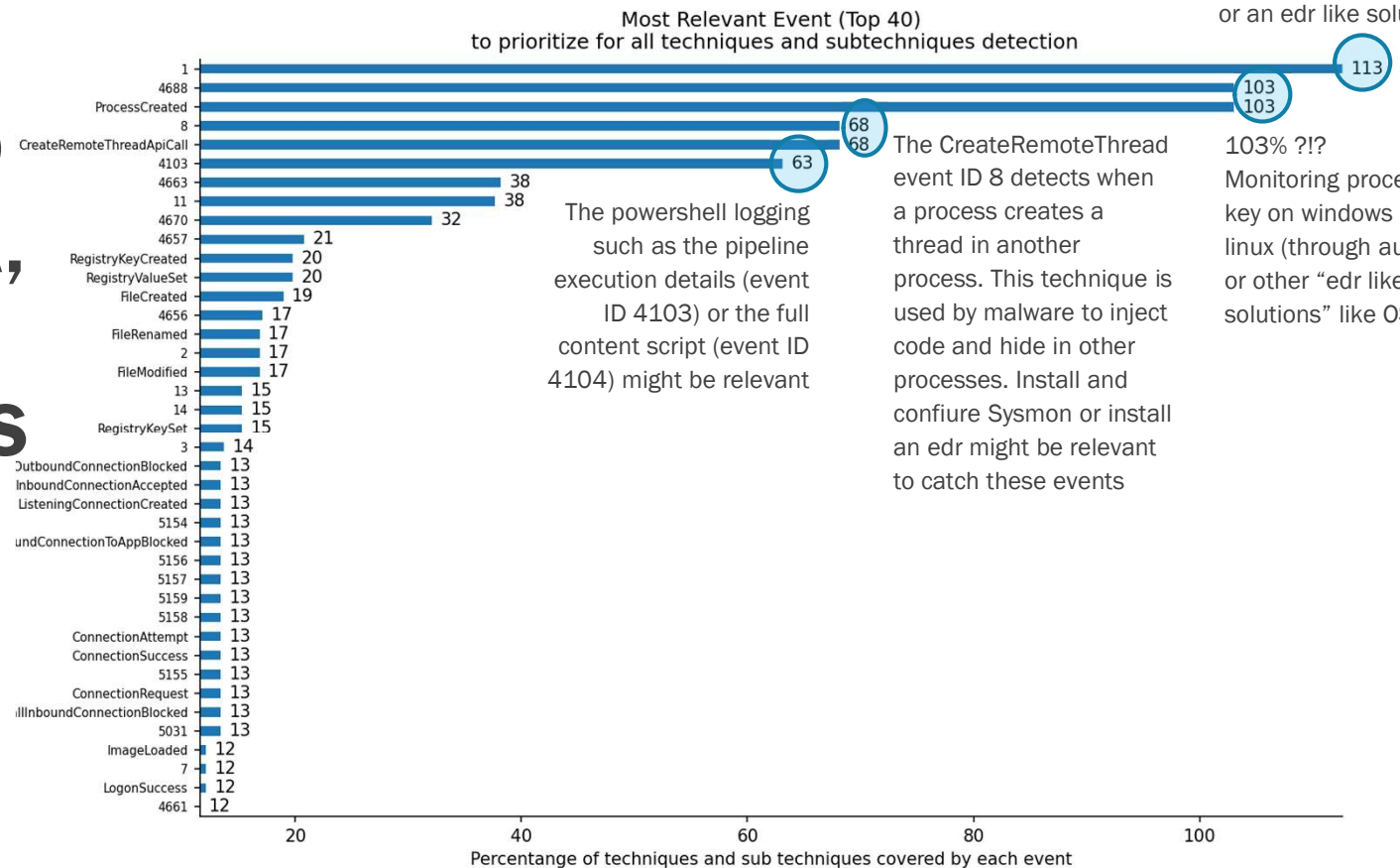


# MANUFACTURING SECTOR TTP STATISTICS

UNDERSTAND YOUR ENEMY AND THINK ABOUT IMPLEMENTATION 4/4

“IT'S IMPORTANT TO HAVE A SOUND IDEA, BUT THE REALLY IMPORTANT THING IS THE IMPLEMENTATION

WILBUR ROSS



---

## AGENDA

- Why, how, what
- Manufacturing sector threat actors
- Manufacturing sector TTP statistics
- Most used manufacturing sector techniques

# MOST USED MANUFACTURING SECTOR TECHNIQUES

## MOST WANTED : T1105 / INGRESS TOOL TRANSFER

### T1105

Used by 70% of the groups : Fox Kitten, APT-C-36, Leviathan, BRONZE BUTLER, menuPass, Threat Group-3390, APT18

Tactic : command-and-control

Technique : Ingress Tool Transfer

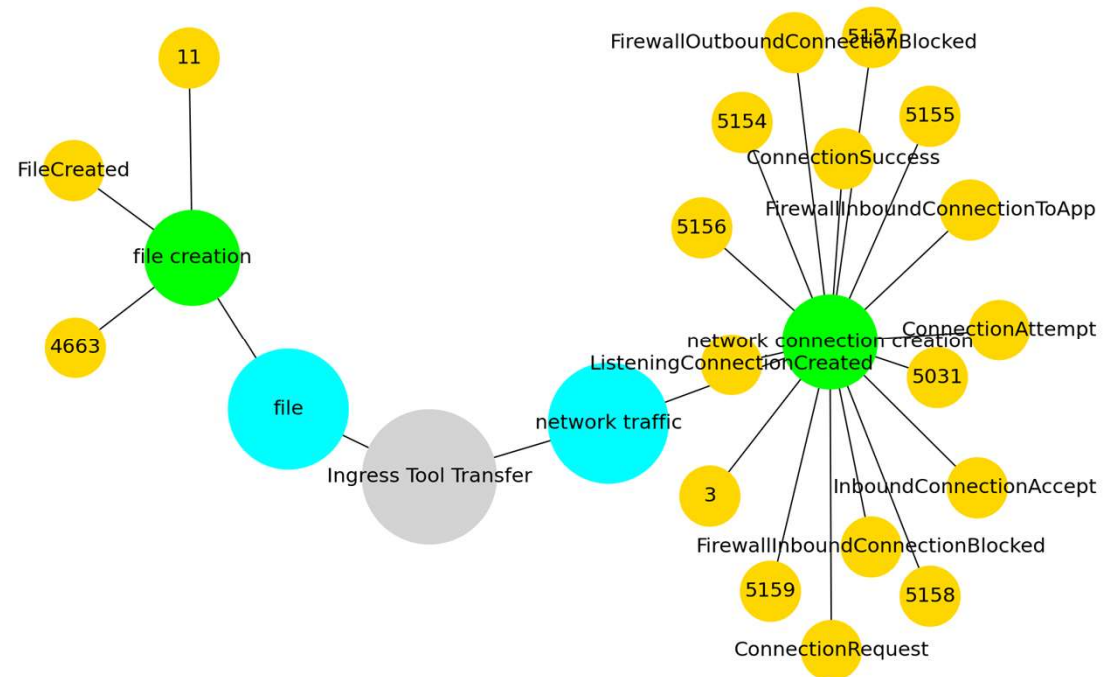
Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp.

Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. Lateral Tool).

TransferFiles can also be transferred using various Web Services as well as native or otherwise present tools on the victim system.

On Windows, adversaries may use various utilities to download tools, such as ``copy``, ``finger``, and PowerShell commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`.

On Linux and macOS systems, a variety of utilities also exist, such as ``curl``, ``scp``, ``sftp``, ``tftp``, ``rsync``, ``finger``, and ``wget``.



# MOST USED MANUFACTURING SECTOR TECHNIQUES

## MOST WANTED : T1027 / OBFUSCATED FILES OR INFORMATION

### T1027

Used by 70% of the groups : Fox Kitten, APT-C-36, APT19, Leviathan, menuPass, Threat Group-3390, APT18

Tactic : defense-evasion

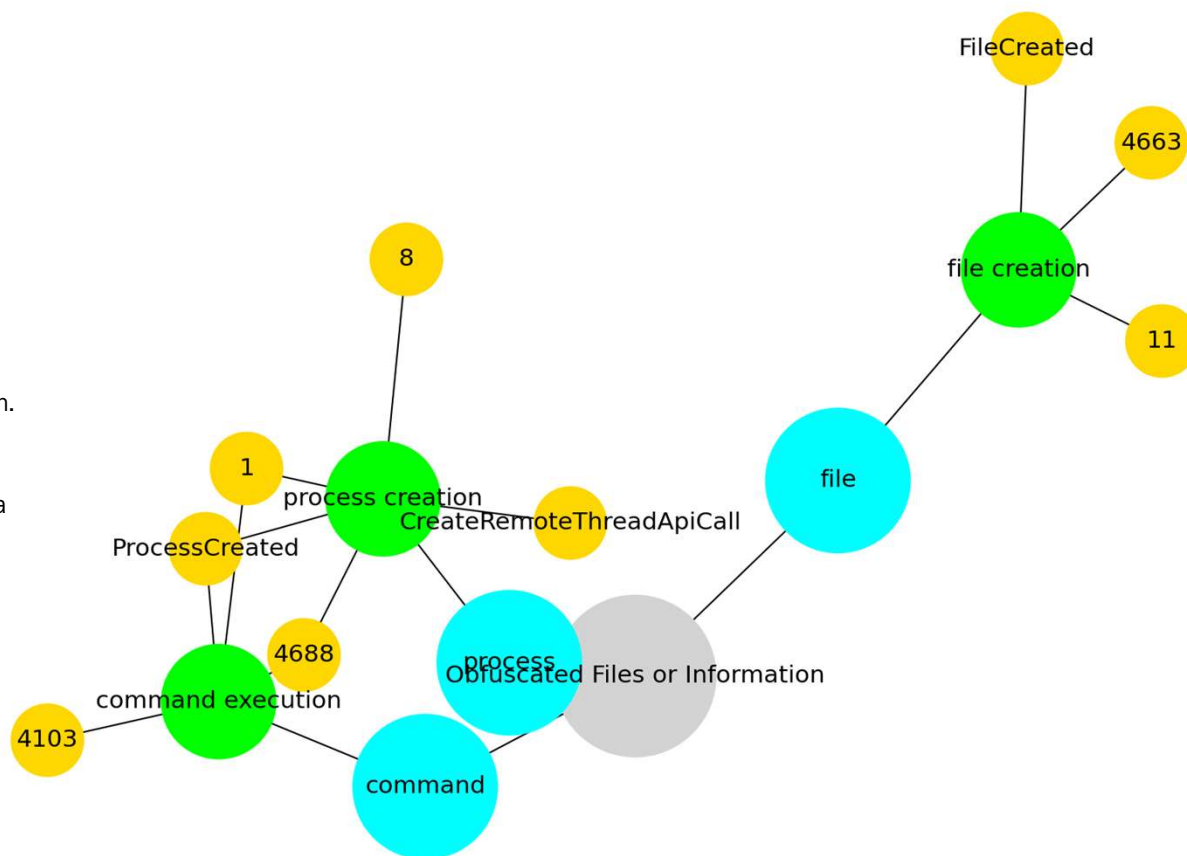
Technique : Obfuscated Files or Information

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 for User Execution. The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. Adversaries may also use compressed or archived scripts, such as JavaScript.

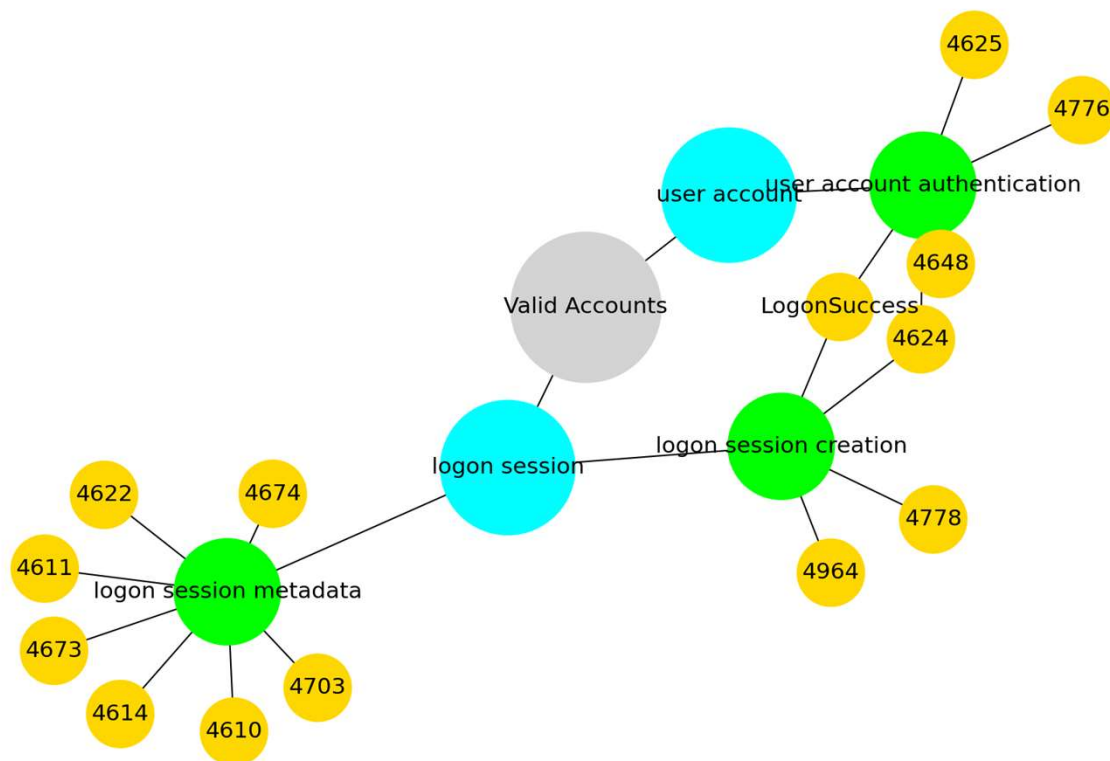
Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.

Adversaries may also obfuscate commands executed from payloads or directly via a Command and Scripting Interpreter. Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms.



# MOST USED MANUFACTURING SECTOR TECHNIQUES

2<sup>ND</sup> MOST WANTED : T1078 / VALID ACCOUNTS



## T1078

Used by 60% of the groups : Fox Kitten, Leviathan, menuPass, Threat Group-3390, APT18, Axiom

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

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.

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.



# MOST USED MANUFACTURING SECTOR TECHNIQUES

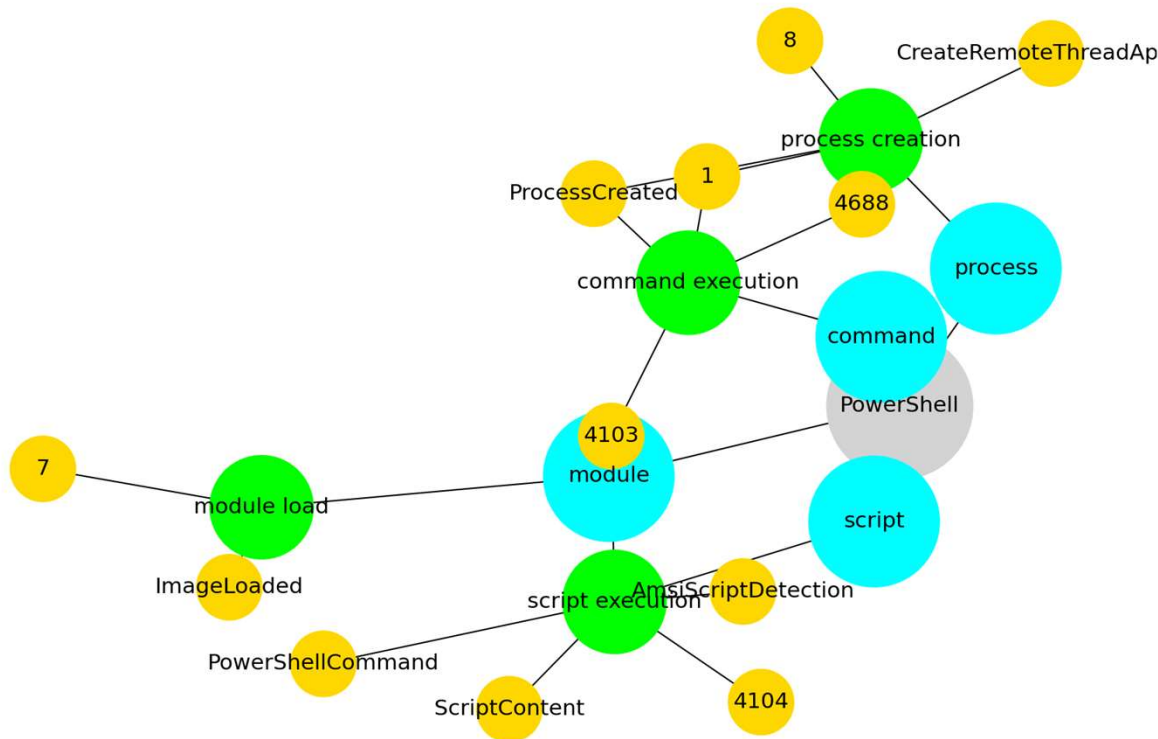
2<sup>ND</sup> MOST WANTED : T1059.001 / POWERSHELL

**T1059,001**

Used by 60% of the groups : Fox Kitten, APT19, Leviathan, BRONZE BUTLER, menuPass, Threat Group-3390

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. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` 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, PowerSploit, PoshC2, and PSAttack

PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).

# MOST USED MANUFACTURING SECTOR TECHNIQUES

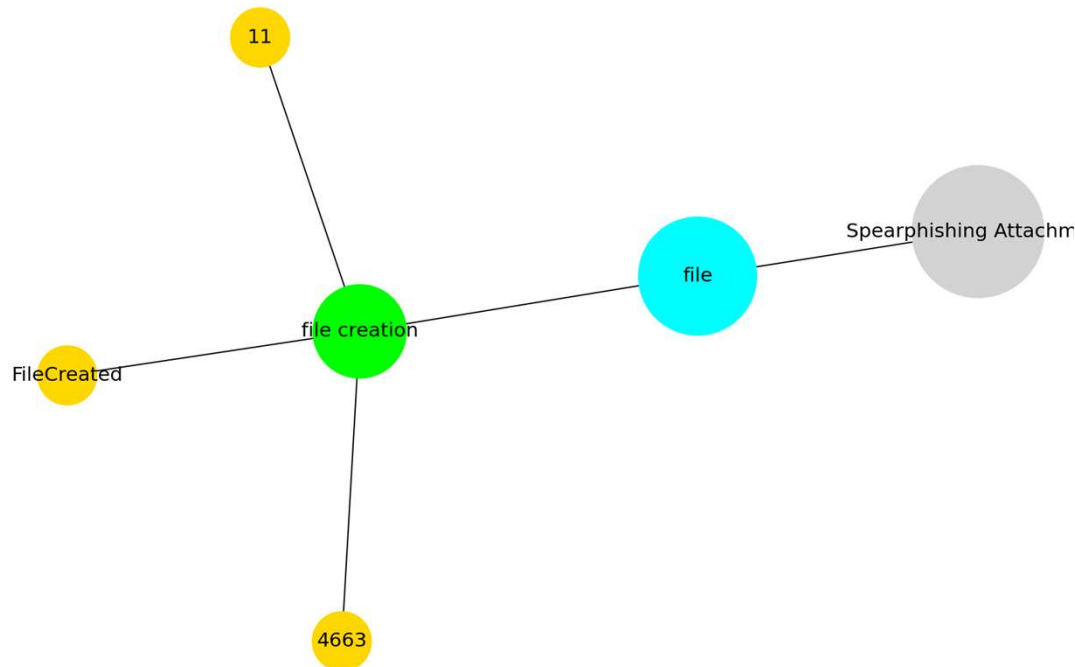
2<sup>ND</sup> MOST WANTED : T1566.001 / SPEARPHISHING ATTACHMENT

Used by 60% of the groups : APT-C-36, APT19, Leviathan, BRONZE

BUTLER, menuPass, 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 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.

# MOST USED MANUFACTURING SECTOR TECHNIQUES

2<sup>ND</sup> MOST WANTED : T1204.002 / MALICIOUS FILE

## T1204.002

Used by 60% of the groups : APT-C-36, APT19, Leviathan, BRONZE BUTLER, menuPass, Threat Group-3390

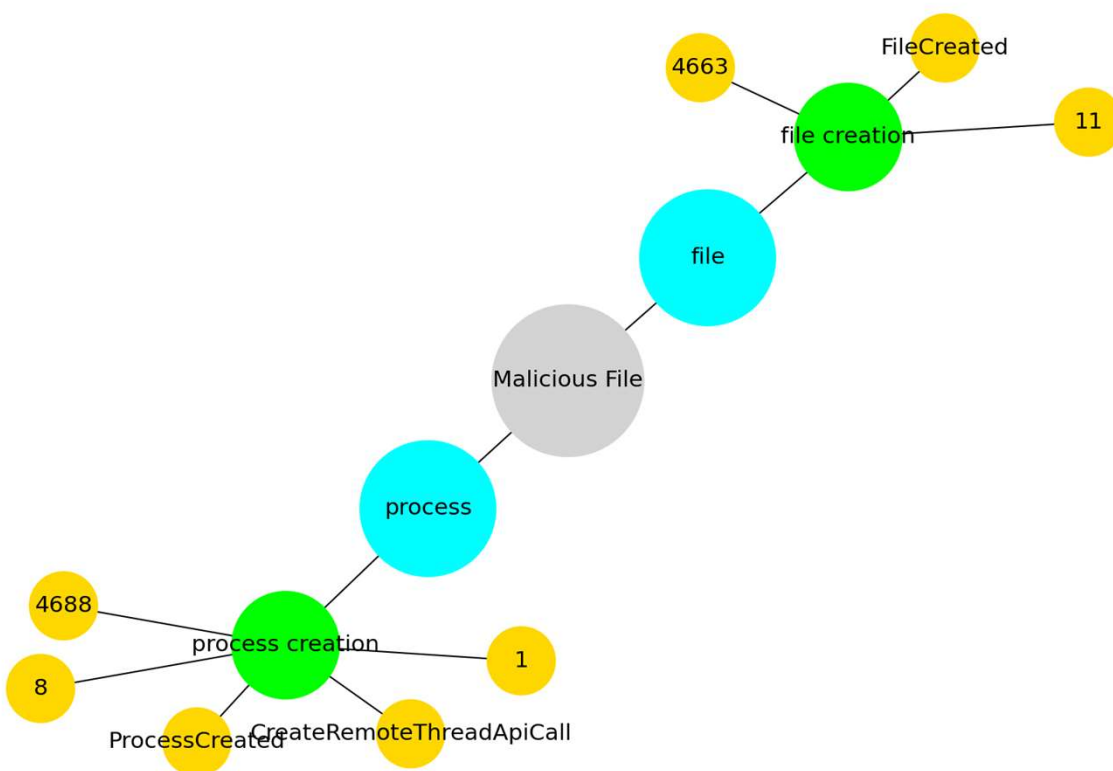
Tactic : execution

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. 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 and Obfuscated Files or Information 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.

While Malicious File 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.



---

# THANKS



@tbillaut



<https://fr.linkedin.com/in/thomasbillaut/>



Thomas.billaut@protonmail.com



# APPENDICES