APT28 SKINNYBOY: Cheat Sheet

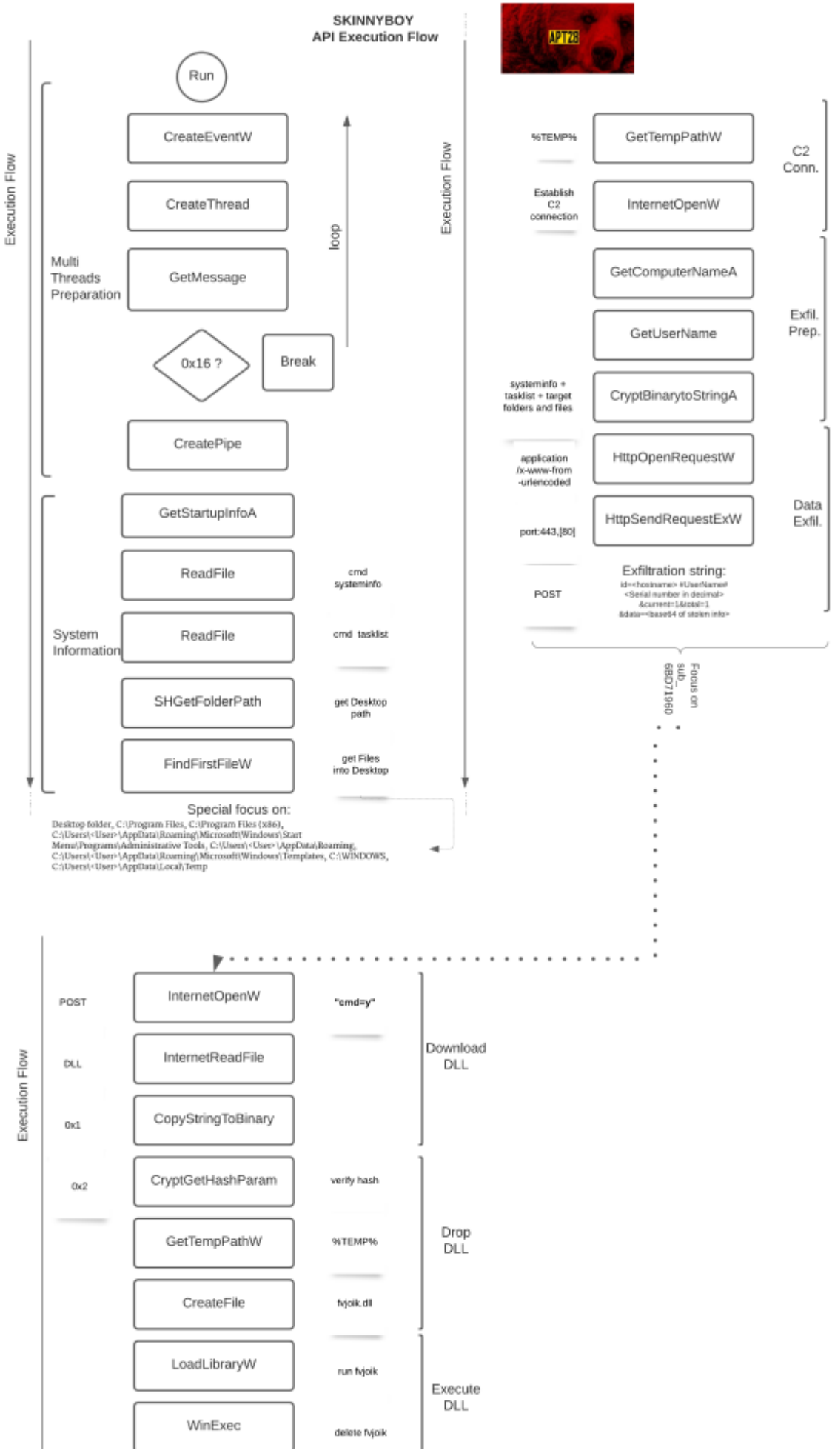
marcoramilli.com/2021/12/30/apt28-skinnyboy-cheat-sheet

December 30, 2021

APT28, also known as Sofacy Group is an (in)famous threat actor. It is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations and it has been characterized as an advanced persistent threat over the past years from many security organizations. In this post I share my cheat sheet on one of their last backdoors named **SkinnyBoy** (report Cluster25 here).

The intent of such a sheet is to offer the main SkinnyBoy functionalities mapped by API call blocks. It might help you in the following ways:

- To learn how the current CONTI ransomware works (if you had no chance to reverse it)
- To extract behavioural models for your Manchine Learning engine
- To synthetize API call signatures for your dynamic detection engine
- Extract behavioural patterns for your SIEM (for example if you use WinAPIOverride to log specific API calls into a syslog-flow to filluP your SIEM)


SKINNYBOY
API Execution Flow
APT28
Execution Flow
Run
CreateEventW
CreateThread
Multi Threads Preparation
GetMessage
loop
0x16 ?
Break
CreatePipe
GetStartupInfoA
ReadFile
cmd systeminfo
System Information
ReadFile
cmd tasklist
SHGetFolderPath
get Desktop path
FindFirstFileW
get Files into Desktop
Special focus on:
Desktop folder, C:\Program Files, C:\Program Files (x86), C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools, C:\Users\<User>\AppData\Roaming, C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Templates, C:\WINDOWS, C:\Users\<User>\AppData\Local\Temp
Execution Flow
%TEMP%
GetTempPathW
C2 Conn.
Establish C2 connection
InternetOpenW
GetComputerNameA
GetUserName
Exfil. Prep.
systeminfo + tasklist + target folders and files
CryptBinarytoStringA
application /x-www-from -urlencoded
HttpOpenRequestW
port:443,[80]
HttpSendRequestExW
Data Exfil.
POST
Exfiltration string:
id=<hostname> #UserName# <Serial number in decimal> &current=1&total=1 &data=<base64 of stolen info>
Focus on sub_68B071960
Execution Flow
POST
InternetOpenW
"cmd=y"
DLL
InternetReadFile
Download DLL
0x1
CopyStringToBinary
0x2
CryptGetHashParam
verify hash
GetTempPathW
%TEMP%
Drop DLL
CreateFile
fvjoik.dll
LoadLibraryW
run fvjoik
WinExec
delete fvjoik
Execute DLL

APT28 SKINNYBODY Cheat Sheet

The Execution flow is represented by the long up-to-down raws and it runs from left to right. The main API calls are included into rectangles while the conditional jumps are mapped into diamonds. Next to specific rectangles (API Calls) a little note is giving further details on the analyzed step. Square brackets wraps API calls into blocks so that you might easily read the six logic CONTI steps, that are: Preparation, System Information, Find and Delete Shadow Copies, Looking for External Targets (shared folders), Encryption Preparation (ransom note included) and Encryption Execution.