

17
/ 63
Community Score

17/63 security vendors flagged this file as malicious

Reanalyze Similar More

65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c

65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c.zip

Size
2.19 KB

Last Analysis Date
2 minutes ago

ZIP

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.susparThreat categoriestrojanFamily labelssuspar

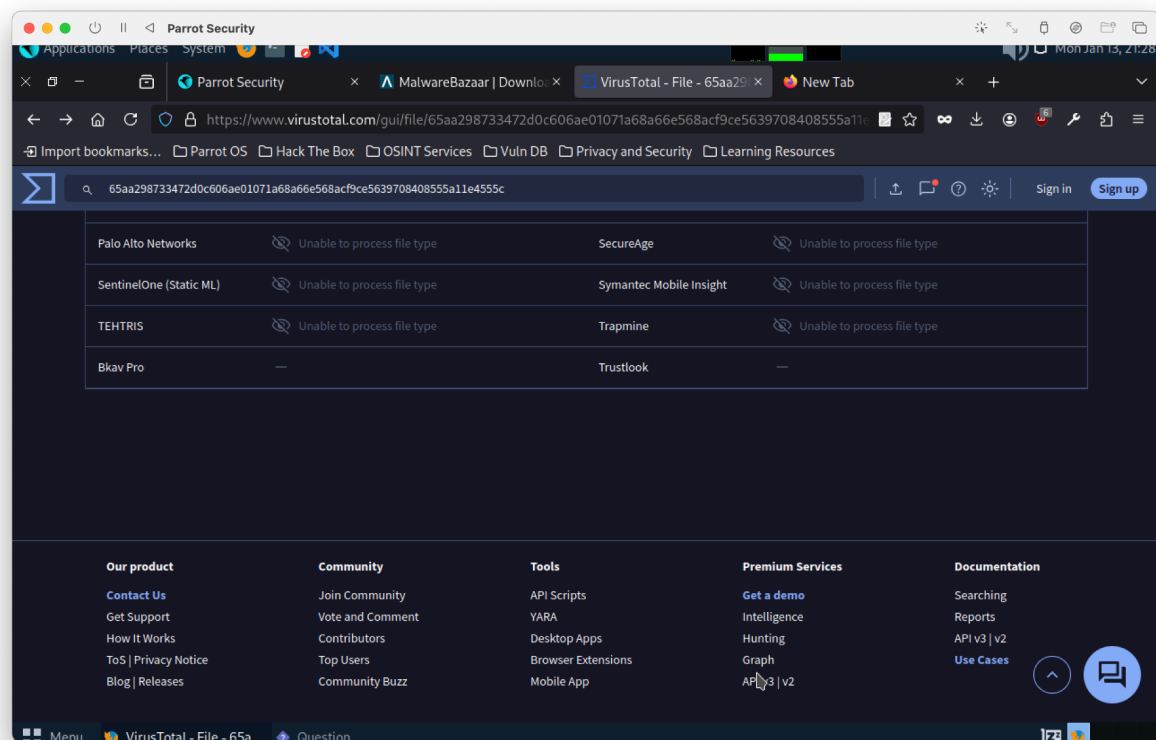
Security vendors' analysisDo you want to automate checks?

Alibaba	Trojan:Script/Generic.c77f2639	AliCloud	Trojan:Multi/Puwaders.C9nj
Avira (no cloud)	HEUR/Suspar.Gen	Cynet	Malicious (score: 70)

Popular threat labeltrojan.susparThreat categoriestrojanFamily labelssuspar

Security vendors' analysisDo you want to automate checks?

Alibaba	Trojan:Script/Generic.c77f2639	AliCloud	Trojan:Multi/Puwaders.C9nj
Avira (no cloud)	HEUR/Suspar.Gen	Cynet	Malicious (score: 70)
Google	Detected	Ikarus	Trojan-Downloader.JS.Agent
Kaspersky	HEUR:Trojan.Script.Generic	Kingsoft	Script.Trojan.Generic.a
NANO-Antivirus	Trojan.Script.Heuristic-js.iacgm	Skyhigh (SWG)	BehavesLike.Exploit.xc
Sophos	Mal/DrodZp-A	Symantec	Trojan.Gen.MBT
Tencent	Script.Trojan.Generic.Rgil	Trellix (ENS)	Artemis!A31034EB3C47
Varist	JS/Agent.CKJ4.genIEldorado	VirIT	Trojan.Win32.MSIL_Heur.A
WithSecure	Heuristic.HEUR/Suspar.Gen	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	ALYac	Undetected



VirusTotal Scan Analysis

VirusTotal is a tool that analyzes files using multiple antivirus engines to detect potential malware. The scan results indicate that **17 out of 63 security vendors flagged this file as malicious**, with various detections identifying it as a **Trojan**.

Key Findings from the Scan

- Detection Rate:**
 - 17 security vendors detected the file as a **Trojan** or **malicious script**.
 - Common threat labels include **Trojan.Suspar**, **Trojan.Script.Generic**, and **HEUR.Suspar.Gen**.
- Threat Classification:**
 - The file is categorized as a **Trojan**, a type of malware that disguises itself as a legitimate file to gain access to systems.
 - Different vendors flagged it with unique identifiers, such as **Trojan:Multi/Puwaders.C9nj** and **JS/Agent.CKJ4.gen**.
- Security Vendor Analysis:**
 - Multiple well-known cybersecurity companies, including **Kaspersky**, **Avira**, **Alibaba**, and **Sophos**, identified it as a threat.

- Some engines labeled it as "**Heuristic**", meaning it was detected based on suspicious behavior rather than a known signature.

What Does This Mean?

- Since multiple antivirus engines detected this file as malicious, it is likely a **Trojan** that could be used for **data theft, remote access, or system compromise**.
- The **ZIP file** format suggests it may contain a **malicious script or executable** that could harm the system when extracted and executed.

Recommended Actions

1. **Do Not Open or Execute the File** – If this file is on your system, delete it immediately.
2. **Run a Full System Scan** – Use a reputable antivirus program to check for any infections.
3. **Check for Suspicious Activity** – Look for unusual system behavior, unauthorized access, or unexpected network connections.
4. **Update Security Software** – Ensure your antivirus and security software are up to date to prevent future threats.

```
Parrot Terminal
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
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!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the "Social-Engineer" Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>
```

```
The Social-Engineer Toolkit is a product of TrustedSec.
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learn
Visit: https://www.trustedsec.com
65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Popular threat label: trojan-suspai Threat categories: trojan
Security vendors' analysis
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
```

File Edit View Search Terminal Help

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 settings 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 powershell exploitation through the browser.

- | | | |
|---------------------------------------|---------------------------------|---------------|
| 1) Java Applet Attack Method | Detected | Ikarus |
| 2) Metasploit Browser Exploit Method | | |
| 3) Credential Harvester Attack Method | Script.Generic | Kingsoft |
| 4) Tabnabbing Attack Method | | |
| 5) Web Jacking Attack Method | Trojan.Script.Heuristic.js.acgm | Skyhigh (SWG) |
| 6) Multi-Attack Web Method | | |
| 7) HTA Attack Method | Mal/DroDZp-A | Symantec |

99) Return to Main Menu

set:webattack>3

```
Parrot Terminal
File Edit View Search Terminal Help
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3

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
```

```
File Edit View Search Terminal Help
SET → https://www.virustotal.com/gui/file/65aa298733472d0c606ae01071a68a66e568ac9...
[+] to harvest credentials or parameters from a website as well as place them in
to a report

-----
--- * 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.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.64.
2]:192.168.64.2
```


File Edit View Search Terminal Help

https://www.virustotal.com/gui/file/65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c

**** Important Information ****

65aa298733472d0c606ae01071a68a66e568acf9ce5639708408555a11e4555c

or templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.

Popular threat label Trojan:AutoSpam Threat categories trojan

you can configure this option under:

Security vendors' analysis

/etc/setoolkit/set.config

Alibaba Trojan:Script.Generic.c77f2639 AliCloud

Avira (no cloud) Cynet

Ikarus

Kaspersky HEUR:Trojan.Script.Generic Kingsoft

Skyhigh (SWG)

Symantec

Trellix (ENS)

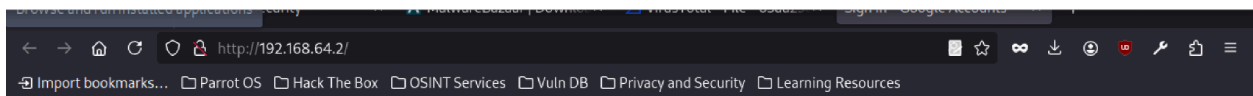
VirIT

1. Java Required

2. Google


3. Twitter

et:webattack> Select a template:2



Google

Sign in with your Google Account



[Need help?](#)

[Create an account](#)

One Google Account for everything Google



```
192.168.64.2 - - [13/Jan/2025 22:27:45] "GET / HTTP/1.1" 200 -
192.168.64.2 - - [13/Jan/2025 22:27:46] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDh
tUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAAAAUy4_
qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=somthing
POSSIBLE PASSWORD FIELD FOUND: Passwd=somthing
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.64.2 - - [13/Jan/2025 22:28:48] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

Introduction

The Social-Engineer Toolkit (SET) is a comprehensive penetration testing framework designed to simulate various social engineering attacks. This report details the process of creating a phishing template targeting Google's login page using SEToolkit in Parrot OS. The objective is to demonstrate how to set up a phishing attack for educational and ethical hacking purposes.

Objective

The primary goal of this exercise is to understand the steps involved in creating a phishing template using SEToolkit. This knowledge is crucial for cybersecurity professionals to identify and mitigate potential phishing attacks.

Tools and Environment

- Operating System: Parrot OS
- Tool: Social-Engineer Toolkit (SET)
- Target: Google's login page

Steps to Create a Phishing Template

1. Launching SEToolkit
 - Open the terminal in Parrot OS.
 - Type `setoolkit` or `set` to launch the Social-Engineer Toolkit.
2. Main Menu
 - The main menu of SEToolkit provides various options. Select 1) `Social-Engineering Attacks` to proceed.
3. Selecting Website Attack Vectors
 - In the Social-Engineering Attacks menu, choose 2) `Website Attack Vectors`. This menu focuses on web-based attack methods.
4. Choosing Web Templates
 - Within the Website Attack Vectors menu, select 1) `Web Templates`. This option allows the import of pre-defined web applications that can be utilized within the attack.
5. Selecting the Google Template

- From the list of pre-defined templates, select the Google template. This template will be used to create a phishing page that mimics Google's login page.
6. Configuring the Phishing Attack
 - SEToolkit will prompt for configuration details:
 - IP Address: Enter the IP address where the phishing page will be hosted.
 - Redirect URL: Specify the URL to which victims will be redirected after entering their credentials.
 7. Launching the Attack
 - Once configured, SEToolkit will host the phishing page on the specified IP address. The attack is now live, and any victim who visits the URL will see a legitimate-looking Google login page.
 8. Capturing Credentials
 - When a victim enters their credentials on the phishing page, SEToolkit captures the information and stores it for the attacker to review.

Detailed Explanation of the Process

1. Web Attack Methods
 - The Web Attack Methods menu provides different methods for web-based attacks, including Web Templates, Site Cloner, and Custom Import. The Web Templates option is selected to use pre-defined templates.
2. Web Attack Vectors
 - The Web Attack Vectors menu includes various attack methods such as Java Applet Attack, Metasploit Browser Exploit, Credential Harvester, Tabnabbing, Web Jacking, Multi-Attack, and HTA Attack. The Web Templates option is chosen to utilize pre-defined templates.
3. Main Menu
 - The main menu of SEToolkit provides an overview of the tool's capabilities and options for different types of attacks and configurations.
4. Social-Engineering Attacks Menu
 - The Social-Engineering Attacks menu includes options for Spear-Phishing Attack Vectors, Website Attack Vectors, Infectious Media Generator, Create a Payload and Listener, Mass Mailer Attack, Arduino-Based Attack Vector, Wireless Access Point Attack Vector, QRCode Generator Attack Vector, Powershell Attack Vectors, and Third Party Modules.

Conclusion

The process of creating a phishing template using SEToolkit in Parrot OS involves navigating through various menus and selecting appropriate options to configure and launch the attack. The toolkit provides a user-friendly interface for setting up phishing pages, making it a powerful tool for penetration testers and security professionals.

- APT18 is a threat group active since at least 2009.
- Targets various industries including technology, manufacturing, human rights groups, government, and medical.
- Also known as TG-0416, Dynamite Panda, and Threat Group-0416.

Associated Groups

- TG-0416: Another name for APT18.
- Dynamite Panda: Another name for APT18.
- Threat Group-0416: Another name for APT18.

Techniques Used

- Application Layer Protocol: Uses HTTP and DNS for command and control (C2) communications.
- Boot or Logon Autostart Execution: Establishes persistence via registry run keys.
- Command and Scripting Interpreter: Uses `cmd.exe` to execute commands.
- External Remote Services: Leverages legitimate credentials to log into external remote services.
- File and Directory Discovery: Lists file information for specific directories.
- Indicator Removal: Deletes tools and batch files from victim systems.
- Ingress Tool Transfer: Uploads files to the victim's machine.
- Obfuscated Files or Information: Obfuscates strings in the payload.
- Scheduled Task/Job: Uses the native `at` Windows task scheduler tool.
- System Information Discovery: Collects system information from the victim's machine.
- Valid Accounts: Leverages legitimate credentials for external remote services.

Software

- `cmd`: Used for various command and scripting interpreter tasks.
- gh0st RAT: A remote access tool with multiple capabilities including keylogging and screen capture.

- hcdLoader: Used for command and scripting interpreter tasks and creating or modifying system processes.
- HTTPBrowser: Used for various tasks including DNS and web protocols, keylogging, and file discovery.
- Pisloader: Used for DNS protocols, file discovery, and system information discovery.

References

- Various articles and reports detailing the techniques and tools used by APT18, including the use of `at.exe` for lateral movement, DNS requests for command and control, and detection and response strategies in Exchange environments.