

```
Parrot Terminal
File Edit View Search Terminal Help

after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-----

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

[*] 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:
192.168.64.2 - - [21/Apr/2025 18:50:31] "GET / HTTP/1.1" 200 -
192.168.64.2 - - [21/Apr/2025 18:50:32] "GET /favicon.ico HTTP/1.1" 404 -
192.168.64.2 - - [21/Apr/2025 18:57:38] "GET / HTTP/1.1" 200 -
```

Contributorship citations							
Citation: Sittikorn	(Citation: fb_arid_viper),(Citation: sentinelone_israel ha						
Citation: Drew Chu	(Citation: CrowdStrike-Android),,						
Citation: Cisco Tal	(Citation: blackberry_mobile_malware apt_esp),						
APT	(Citation: Trend Micro Bouncing Golf 2019),(Citation: Tr						
	(Citation: lookout_hornbill_sunbird_0221),,						
	(Citation: Lookout Dark Caracal Jan 2018),(Citation: Loc						
Citation: Microsoft	,,						
	(Citation: MoustachedBouncer ESET August 2023),						
The name StrongPit	,,(Citation: Bitdefender StrongPity June 2020),(Citation:						
Citation: Dragos Ti	(Citation: CYBERWARCON CHEMISTGAMES),(Citation: Le						
Citation: Microsoft	(Citation: MSTIC Octo Tempest Operations October 202						
Denise Ta	(Citation: Meta Adversarial Threat Report 2022),(Citatio						
Citation: SANS Win	(Citation: BlackBerry Bahamut),(Citation: Cyfirma Baha						

ApplicationsPlacesSystem

Parrot SecurityMalwareBazaar | DownloadVirusTotal - File - d49f1ffATT&CK Data & Tools | MEarth Lusca, TAG-22, Char

Parrot Terminal

FileEditViewSearchTerminalHelp

7) HTA Attack MethodOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

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 Templates2) Site Cloner3) Custom Import

99) Return to Webattack Menu

set:webattack>

DefensesCTIResourcesBenefactorsBlog

Search

ATT&CKcon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found [here](#)

ID: G1006

Associated Groups: TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Version: 2.0

Created: 01 July 2022

Last Modified: 16 September 2024

Version Permalink

Associated Group Descriptions

Name	Description
TAG-22	[2]

MenuEarth Lusca, TAG-22, ... | 1 mobile-attack-v16.1-g...Parrot Terminal

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
- 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>

ID: G1006

 Associated Groups: TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Version: 2.0

Created: 01 July 2022

Last Modified: 16 September 2024

[Version Permalink](#)

Associated Group Descriptions

Name	Description
TAG-22	[2]

Parrot Terminal

File Edit View Search Terminal Help

The Social-Engineer Toolkit is a product of TrustedSec. Learning Resources

MITRE ATT&CK

Visit: <https://www.trustedsec.com>

It's easy to update using the PenTesters Framework! 4 (PTF) 25 in McLean, VA. More details about tickets and our CFP can be found [here](#)

Visit <https://github.com/trustedsec/ptf> to update all your tools!

GROUPS

Home > Groups > Earth Lusca

Select from the menu:

Earth Lusca

Elderwood

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>

It's easy to update using the PenTesters Framework! 4 (PTF) 25 in McLean, VA. More details about tickets and our CFP can be found [here](#)

Visit <https://github.com/trustedsec/ptf> to update all your tools!

GROUPS

Home > Groups > Earth Lusca

Select from the menu:

Earth Lusca

Elderwood

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>

FIN6

FIN7

FIN8

Fox Kitten

GALLIUM

Menu Earth Lusca, TAG-22, ... | 1 mobile-attack-v16.1-g... Parrot Terminal

Earth Lusca

Earth Lusca is a suspected China-based cyber espionage group that has been active since at least April 2019. Earth Lusca has targeted organizations in Australia, China, Hong Kong, India, Japan, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, South Korea, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some Earth Lusca operations may be financially motivated.^[1]

Earth Lusca has used malware commonly used by other Chinese threat groups, including APT41 and the Winnti Group cluster, however security researchers assess Earth Lusca's techniques and infrastructure are separate.^[1]

ID: G1006

 Associated Groups: TAG-22, Charcoal Typhoon, CHROMIUM, ControlIX

Version: 2.0

Created: 01 July 2022

Last Modified: 16 September 2024

[Version Permalink](#)

Associated Group Descriptions

Name	Description
TAG-22	[2]

```
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.

GROUP Visit: https://www.trustedsec.com

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

Ember Bear


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. 2025 in McLean, VA. More details about tickets and our CFP can be found [here](#)

ID: G1006

 Associated Groups: TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Version: 2.0

Created: 01 July 2022

Last Modified: 16 September 2024

[Version Permalink](#)

Associated Group Descriptions

Name	Description
TAG-22	[2]

ApplicationsPlacesSystem

Parrot Security

MalwareBazaar | Download

VirusTotal - File - d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

https://www.virustotal.com/gui/file/d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182/behavior

Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

Max size 650MB

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

Sign inSign up

Activity Summary

Download ArtifactsFull ReportsHelp

Processes Terminated

1816 - C:\Windows\system32\compattel\DiagTrackRunner.exe /UploadEtlFilesOnly

2416 - C:\Windows\System32\slui.exe -Embedding

3176 - taskhost.exe SYSTEM

3200 - C:\Windows\system32\sc.exe start w32time task_started

3332 - C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"

3420 - taskhost.exe \$(Arg0)

3584 - rundll32 C:\Windows\system32\GeneralTel.dll,RunInUserCxt PVzG3YkoJ02vQA80.1.1.2 {DFEB11F6-BC8D-4000-BD3D-6723866941B6} {D87FB157-A879-1F43-EA1E-5F4FE43DBD0A} IsAdmin WAMAccountCount

824 - C:\Windows\system32\DeviceDisplayObjectProvider.exe -Embedding

Services Opened

VaultSvc

wscsvc

Processes Tree

3640 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\AudioCapture.dll",#1

5768 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\HTCTL32.DLL",#1

↳ 6608 - C:\Windows\SysWOW64\WerFault.exe -u -p 5768 -s 732

2204 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\KBDTAM99.DLL",#1

↳ 5324 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\KBDTAM99.DLL",#1

Menu

VirusTotal - File - d49...

ApplicationsPlacesSystem

Parrot Security

MalwareBazaar | Download

VirusTotal - File - d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

https://www.virustotal.com/gui/file/d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182/behavior

Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

Max size 650MBd49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

Sign inSign up

Activity SummaryDownload ArtifactsFull ReportsHelp

Registry Keys Set

+ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000040064\VirtualDesktop

+ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000501C8\VirtualDesktop

+ HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries

+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter

+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\GrpConv

+ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\usbhub\hubg\EnableDiagnosticMode

+ \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\WritePermissionsCheck

+ \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41\BinFileVersion

+ \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41\BinProductVersion

+ \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41\BinaryType

Registry Keys Deleted

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\GrpConv

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TsUsbFlt\BootFlags

Process and service actions

Menu

VirusTotal - File - d49...

123

Activity Summary

Download Artifacts Full Reports Help

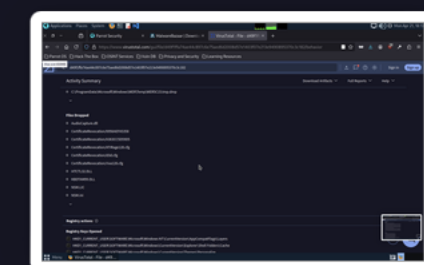
Registry Keys Set

- + HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000040064\VirtualDesktop
- + HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000501C8\VirtualDesktop
- + HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries
- + HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter
- + HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\GrpConv
- + HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\usbhub\hubg\EnableDiagnosticMode
- + \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\WritePermissionsCheck
- + \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41\BinFileVersion
- + \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41\BinProductVersion
- + \REGISTRY\A\{958c68f6-4084-23ae-cf40-19411e5ca9af}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41\BinaryType

Registry Keys Deleted

- + HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\GrpConv
- + HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TsUsbFlt\BootFlags

Process and service actions



Activity Summary

Download Artifacts Full Reports Help

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C15.tmp.dmp

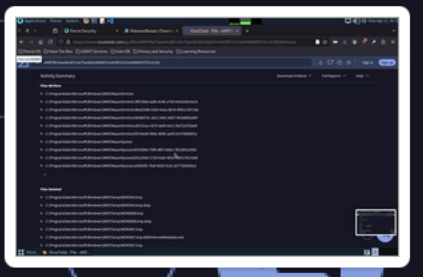
Files Dropped

- + AudioCapture.dll
- + CertificateRevocation/6956AEFA5358
- + CertificateRevocation/A363CC5D59D5
- + CertificateRevocation/ATIRage128.cfg
- + CertificateRevocation/d3d.cfg
- + CertificateRevocation/riva128.cfg
- + HTCTL32.DLL
- + KBDTAM99.DLL
- + NSM.LIC
- + NSM.ini

Registry actions

Registry Keys Opened

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize



Activity Summary

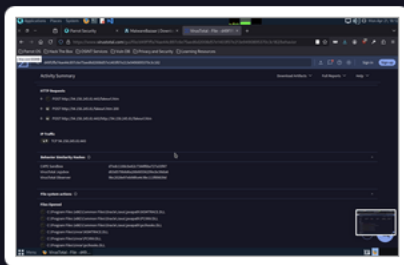
Download Artifacts Full Reports Help

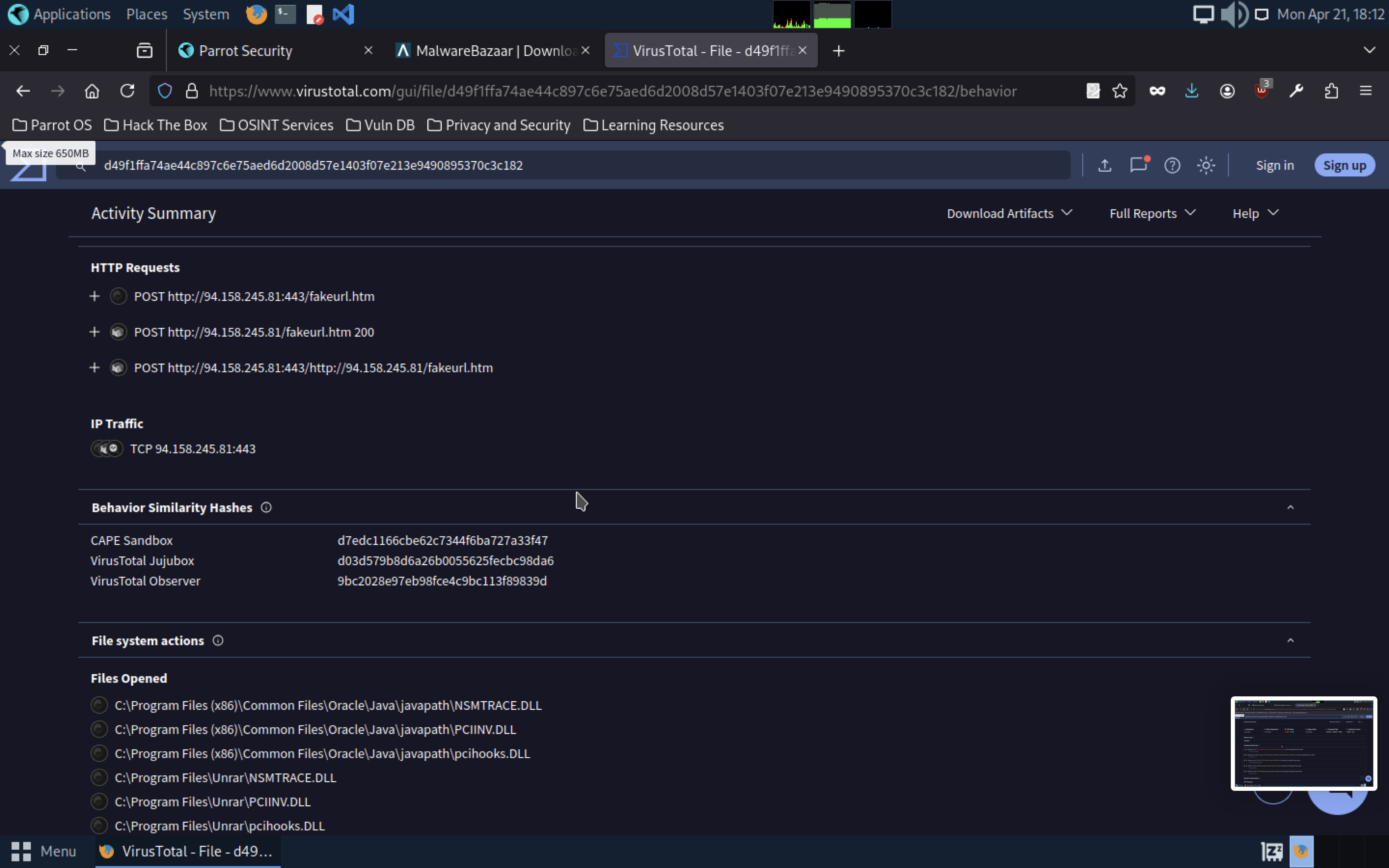
Files Written

- + C:\ProgramData\Microsoft\Windows\WER\ReportArchive
- + C:\ProgramData\Microsoft\Windows\WER\ReportArchive\3f67efe6-ea8b-4c4b-a75d-b9c0245c6a14
- + C:\ProgramData\Microsoft\Windows\WER\ReportArchive\46ed1568-9164-43aa-8674-3f9b1c997cbb
- + C:\ProgramData\Microsoft\Windows\WER\ReportArchive\8b9b6791-a811-445c-b057-f610dfd3a967
- + C:\ProgramData\Microsoft\Windows\WER\ReportArchive\af2c52aa-1879-4a00-8a11-f0e72c076a04
- + C:\ProgramData\Microsoft\Windows\WER\ReportArchive\f07e9e00-f6bb-469b-ae95-6c974980bf1e
- + C:\ProgramData\Microsoft\Windows\WER\ReportQueue
- + C:\ProgramData\Microsoft\Windows\WER\ReportQueue\429334b0-76f9-4fd7-b8ba-7fb1d65a295b
- + C:\ProgramData\Microsoft\Windows\WER\ReportQueue\825c256d-1728-43a0-983e-c96517b218d6
- + C:\ProgramData\Microsoft\Windows\WER\ReportQueue\29493f2-7baf-4428-912e-d377204295a3

Files Deleted

- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER3543.tmp
- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER3543.tmp.dmp
- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DB.tmp
- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DB.tmp.dmp
- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER5407.tmp
- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER5407.tmp.WERInternalMetadata.xml
- + C:\ProgramData\Microsoft\Windows\WER\Temp\WER5967.tmp





ApplicationsPlacesSystem

Parrot Security

MalwareBazaar | Downloa

VirusTotal - File - d49f1ffa

Mon Apr 21, 18:12

https://www.virustotal.com/gui/file/d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182/behavior

Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

Max size 650MB

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

Sign in

Sign up

Activity Summary

Download ArtifactsFull ReportsHelp

Detections

NOT FOUND

Mitre Signatures

NOT FOUND

IDS Rules

1 HIGH4 LOW

Sigma Rules

NOT FOUND

Dropped Files

1 PE_EXE3 OTHER1 TEXT

Network comms

3 HTTP1 IP

Behavior Tags

persistence

Crowdsourced IDS rules

Matches rule **POLICY-OTHER HTTP request by IPv4 address attempt** at Snort registered user ruleset

↳ *policy-violation*

Matches rule **(http_inspect) HTTP start line or header line terminated by LF without a CR** at Snort registered user ruleset

↳ *unknown*

Matches rule **ET POLICY HTTP traffic on port 443 (POST)** at Proofpoint Emerging Threats Open

↳ *Potentially Bad Traffic*

Matches rule **ET INFO NetSupport Remote Admin Checkin** at Proofpoint Emerging Threats Open

↳ *Misc activity*

Matches rule **ET INFO NetSupport Remote Admin Response** at Proofpoint Emerging Threats Open

↳ *Misc activity*

Network Communication

HTTP Requests

Menu

VirusTotal - File - d49...

123

ApplicationsPlacesSystem

Parrot Security

MalwareBazaar | Downloa

VirusTotal - File - d49f1ffa

Mon Apr 21, 18:12

https://www.virustotal.com/gui/file/d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182/re

Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

Max size 650MB

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

Community Score

66

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182.zip

zipcontains-pe

Size

2.40 MB

Last Analysis Date

a moment ago

ZIP

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Bundled Files (33)

Scanned	Detections	File type	Name
2025-04-15	19 / 72	Win32 DLL	PCICL32.DLL
2025-04-21	18 / 72	Win32 EXE	client32.exe
2025-04-03	12 / 62	INI	NSM.LIC
2025-04-17	5 / 72	Win32 EXE	remcmdstub.exe
2025-04-21	4 / 60	INI	client32.ini
2025-04-15	2 / 72	Win32 DLL	pcicapi.dll
2025-04-15	1 / 72	Win32 DLL	AudioCapture.dll
2025-03-28	1 / 73	Win32 DLL	HTCTL32.DLL
2025-04-15	1 / 72	Win32 DLL	PCICHEK.DLL
2025-04-21	1 / 71	Win32 DLL	ifsutilx.dll

Menu

VirusTotal - File - d49...

ApplicationsPlacesSystem

Mon Apr 21, 18:12

Parrot SecurityMalwareBazaar | DownloadVirusTotal - File - d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

https://www.virustotal.com/gui/file/d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182/details

Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

Max size 650MB

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

Latest Contents Modification2025-04-21 12:44:48

Names

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182.zip

Bundle Info

Warnings

Contains one or more Windows executables.

Contents Metadata

Contained Files38

Uncompressed Size5.21 MB

Earliest Content Modification2007-07-06 12:07:32

Latest Content Modification2025-04-21 12:44:48

Contained Files By Type

UNKNOWN15

PORTABLE EXECUTABLE23

Contained Files By Extension

LIC1

INF1

EXE2

INI3

DLL4

CFG6

DLL17

Sign inSign up

Menu

VirusTotal - File - d49...

123

Antiy-AVL	❗ RiskWare[RemoteAdmin]/Win32.NetSup	Avast	❗ Other:Malware-gen [Trj]
AVG	❗ Other:Malware-gen [Trj]	DrWeb	❗ Trojan.RA.587
Elastic	❗ Malicious (moderate Confidence)	ESET-NOD32	❗ Multiple Detections
Fortinet	❗ W32/PossibleThreat	Google	❗ Detected
Gridinsoft (no cloud)	❗ Trojan.Win32.Downloader.ddlc	Jiangmin	❗ RemoteAdmin.NetSup.ai
K7AntiVirus	❗ Riskware (00584baa1)	K7GW	❗ Riskware (00584baa1)
Kaspersky	❗ Not-a-virus:HEUR:RemoteAdmin.Win32....	Lionic	❗ Riskware.Win32.NetSup.1lc
MaxSecure	❗ Trojan.Malware.74404514.susgen	Panda	❗ PUP/RnkBend
Rising	❗ PUF.RemoteAdmin!1.E606 (CLASSIC)	Skyhigh (SWG)	❗ PUP-NetSupport
Sophos	❗ Mal/NetSupRat-A	Tencent	❗ Malware.Win32.Gencirc.11ce8752
Trellix (ENS)	❗ Generic Trojan.a	TrendMicro	❗ PUA.Win32.NetSupportManager.E
TrendMicro-HouseCall	❗ PUA.Win32.NetSupportManager.E	Varist	❗ W32/RemoteAdmin.BURT-5818
VBA32	❗ Trojan.Tiggre	Webroot	❗ W32.Remoteadmin.Netsupport
Zillya	❗ Tool.NetSup.Win32.153	ZoneAlarm by Check Point	❗ Mal/NetSupRat-A

28

/ 66

Community Score

28/66 security vendors flagged this file as malicious

Reanalyze

Similar

More

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182

d49f1ffa74ae44c897c6e75aed6d2008d57e1403f07e213e9490895370c3c182.zip

zipcontains-pe

Size

2.40 MB

Last Analysis Date

a moment ago

ZIP

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

Popular threat label

hacktool.netsup/netsupport

Threat categories

hacktool

trojan

pua

Family labels

netsup

netsupport

netsupportmanager

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	RiskWare[RemoteAdmin]/Win32.NetSup	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	DrWeb	Trojan.RA.587
Elastic	Malicious (moderate Confidence)	ESET-NOD32	Multiple Detections
Fortinet	W32/PossibleThreat	Google	Detected