Cybereason Exposes Campaign Targeting US Taxpayers with NetWire and Remcos Malware

cybereason.com/blog/cybereason-exposes-malware-targeting-us-taxpayers

Over the past year, the Cybereason Nocturnus Team has observed various trends among cyber criminals and nation-state groups leveraging various global events such as COVID-19 and other topical themes and trending issues as phishing content to lure their victims into installing their malware of choice.

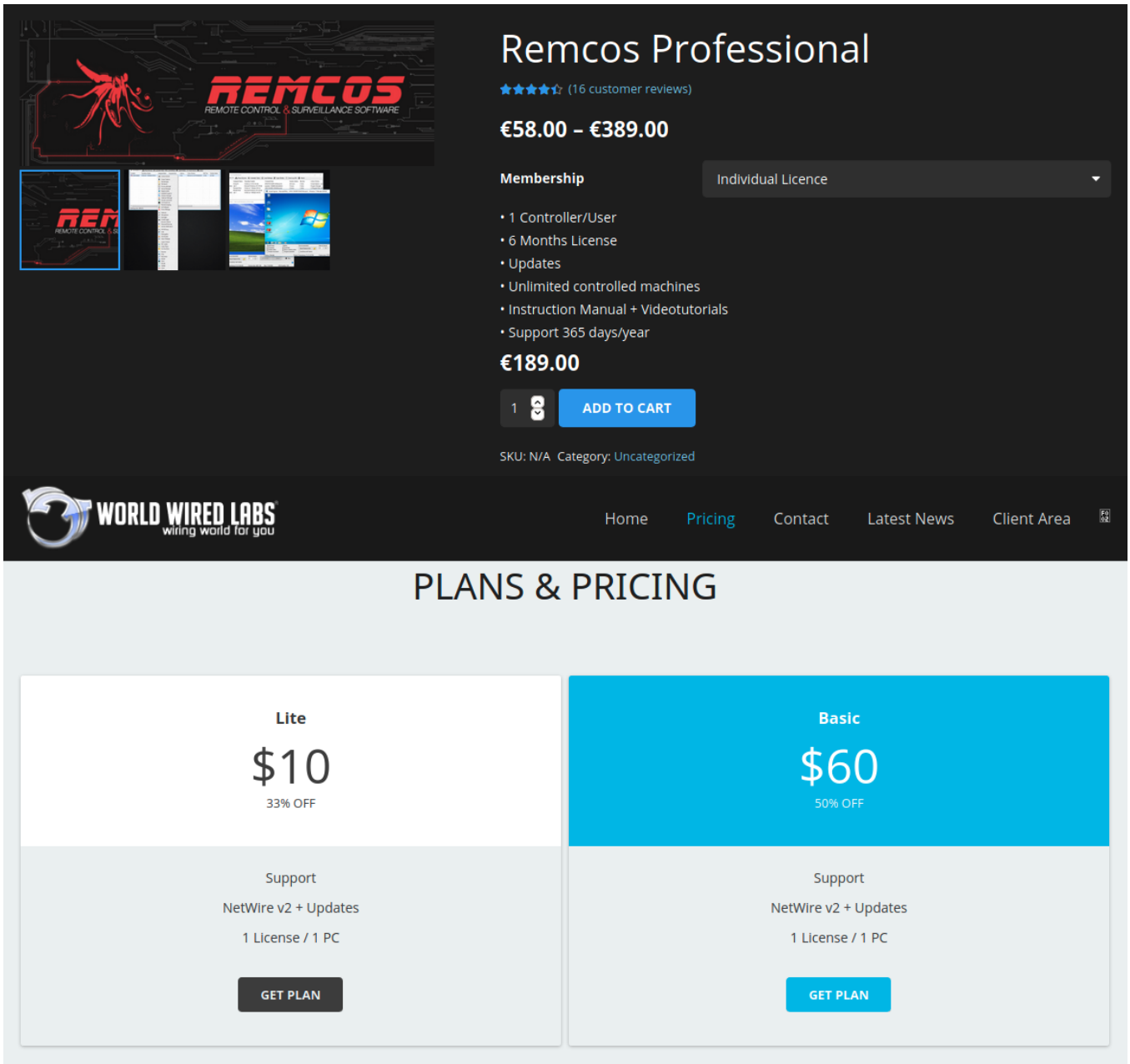
As the tax season is already here, Cybereason detected a new campaign targeting US taxpayers with documents that purport to contain tax-related content, ultimately delivering NetWire and Remcos - two powerful and popular RATs (remote access trojans) which can allow attackers to take control of the victims' machines and steal sensitive information.

Key Points

- **Leveraging US Tax Season to lure victims:** Each year, by April 15th, all US citizens are expected to deliver their tax returns. Cybereason detected a phishing campaign targeting US taxpayers.
- **Delivering two types of commodity malware:** Two infamous remote access tools (RATs) are being used in this campaign, NetWire and Remcos, each manifesting as binaries delivered via malicious documents.
- **Evading heuristic and AV detection mechanisms:** The malicious documents that infect the user are roughly 7MB in size, which allows them to evade traditional AV mechanisms and heuristic detection.
- **Abuse of legitimate cloud services:** The infection chain uses cloud services such as "imgur" to store the Netwire and Remcos payloads, hidden in image files
- **Steganography:** Payloads are concealed and downloaded within image files, combined with the fact they are hosted on public cloud services makes them even harder to detect.
- **Exploiting legitimate OpenVPN clients:** As a part of the infection process, a legitimate OpenVPN client is downloaded and executed then sideloads a malicious DLL that drops NetWire/Remcos.

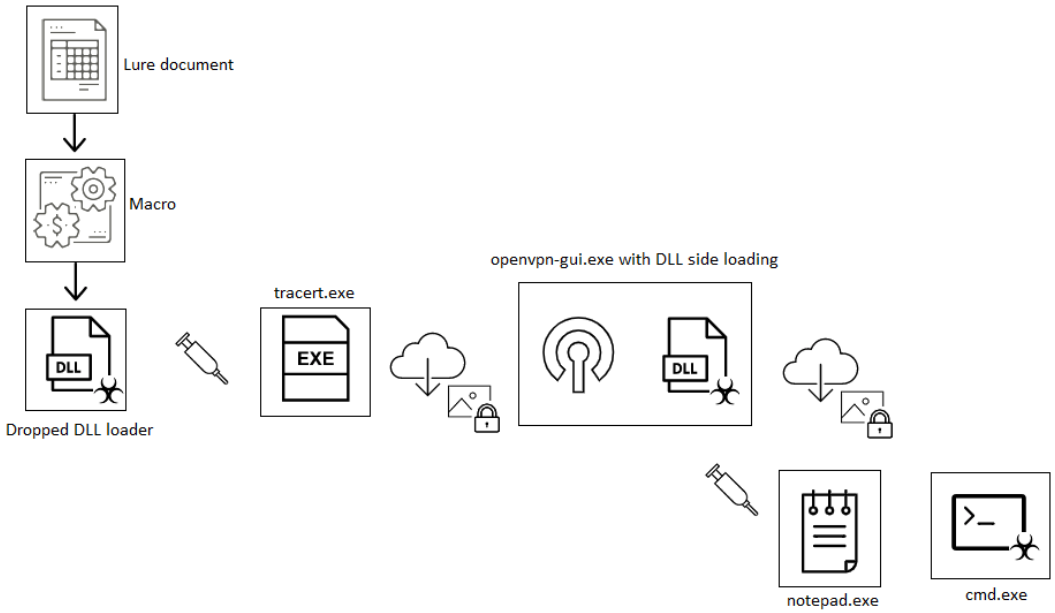
Background

The campaign bears resemblance to another campaign observed in April of 2020 which also delivered the NetWire RAT. Both NetWire and Remcos are commercial RATs that are available for purchase online for rather affordable prices of as little as US$10 per month. Both offer various licensing plans and following the Malware-as-a-Service (MaaS) model, offering their customers a subscription-based model with services such as 24/7 support and software updates:



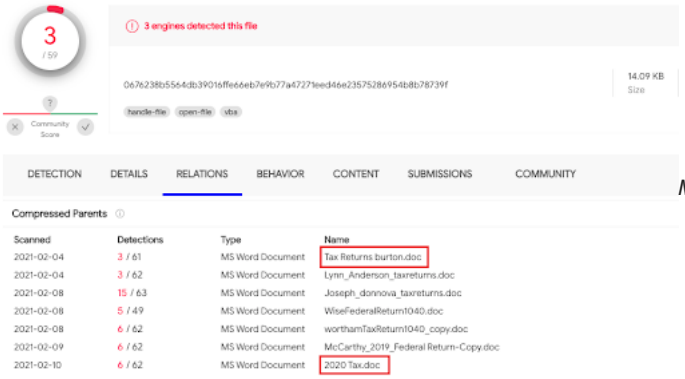
Remcos and NetWire as offered on their websites

campaign analysis



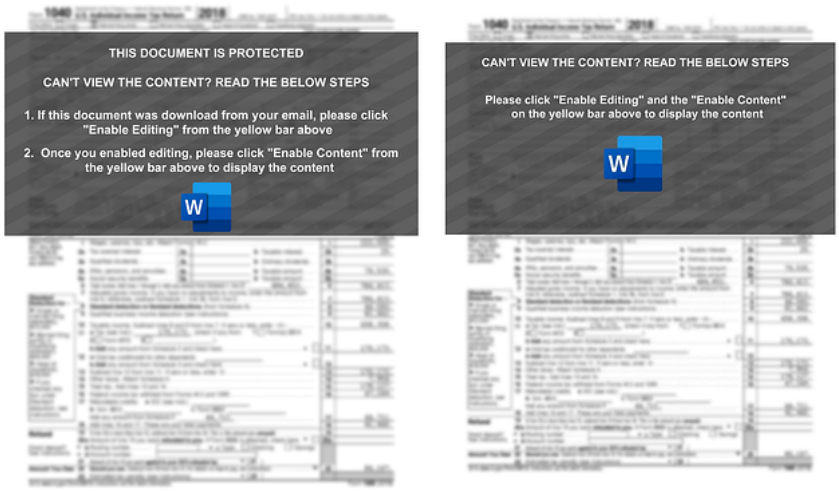
Infection Vector: Lure Documents Containing a Malicious Macro

The infection vector that lures the users into installing the malware is a tax return themed Word document containing a malicious macro:



Malicious documents submitted to VirusTotal

Once the document has been opened, the content in the background is allegedly blurred, and the “Enable Editing” and “Enable Content” prompts must be manually confirmed by the user:



Malicious documents content

This is a known social engineering method used to encourage the user to enable embedded macros to run on their machine. Once the malicious content is being executed, an embedded and heavily obfuscated macro is ran on the victim's machine:

```
Sub batteldevastations()
Dim credenzadetours As Boolean
Dim dysenterybareness As Boolean
Call aggroschests("exjsonp", "standardattachment", "Sid")
On Error Resume Next
dysenterybareness = Audrey.christening(26)
If dysenterybareness = False Then
Call aggroschests("Usernamebinarys", "openidlayer", "Sid")
Audrey.christening (42)
End If
End Sub
Private Sub Document_Open()
Audrey.disherisonGloucestershire ("Temp")
batteldevastations
End Sub
'START_MODULE
```

A part of the embedded macro obfuscated code

The above code partially shows that the payload is eventually dropped in the users "Temp" directory:

WINWORD.EXE	936	WriteFile	C:\Users\Administrator\AppData\Local\Temp\Sid.dll
WINWORD.EXE	936	WriteFile	C:\Users\Administrator\AppData\Local\Temp\Sid.dll
WINWORD.EXE	936	WriteFile	C:\Users\Administrator\AppData\Local\Temp\Sid.dll
WINWORD.EXE	936	Process Create	C:\Windows\system32\notepad.exe
notepad.exe	584	Process Start	
WINWORD.EXE	936	RegSetValue	HKCU\Software\Microsoft\Office\14.0\Word\Security\Trusted Document...
WINWORD.EXE	936	RegSetValue	HKCU\Software\Microsoft\Office\14.0\Common\Licensing\C0AC079DA8...
WINWORD.EXE	936	RegSetValue	HKCU\Software\Microsoft\Office\14.0\Word\WordName

The DLL dropped by the macro code

Finally, the DLL is injected into notepad and continues the infection chain.

Loaders

The "sid.dll" loader that was dropped by the macro was observed to have at least two different variants: one is a loader for Remcos, and the other is a loader for NetWire. Looking at their exports, both loaders share the same "payload" exported method:

Name	Address	Ordinal
payload	100011B0	1
DllEntryPoint	**100015CD**	**[main entry]**

The loader's exported methods

Upon execution, the "payload" method starts decrypting data using a XOR key:

```
push    5
push    offset xor_key
push    16E4h
push    offset unk_74F38190
push    ebx
call    decrypt_data
push    5
push    offset xor_key
push    1Eh
push    offset unk_74F3DD38
mov     [esp+60h+var_2C], ebx
push    esi
mov     [esp+64h+var_28], 28AFh

add     ebx, 5B0Fh
call    decrypt_data
push    64h ; 'd'           ; dwBytes
push    40h ; '@'           ; uFlags
mov     [esp+58h+var_30], esi
```

Dat decryption methods of the NetWire loader

The first decrypted part is an additional executable code, and the second part is decrypting the URL the loader connects to in order to download the next execution stage:

```
movsx ecx,word ptr ds:[74F41054]
movzx edx,byte ptr ds:[74F41050]
cmp dword ptr ds:[74F4106C],ecx
mov ecx,FFFFFFDA
cmovl edx,ecx
add esi,4
mov byte ptr ds:[74F41050],dl
dec edi
jne sid.74F31020
pop esi
pop ebp
```

```
esi:"https://i.ibb.co/Y21YyRx/DUIJRm-Dz-RMa-Eu.jpg"
esi:"https://i.ibb.co/Y21YyRx/DUIJRm-Dz-RMa-Eu.jpg"
```

The decrypted initial C2 URL

Eventually, the malicious code is injected into "tracert.exe" that downloads the OpenVPN client along with a trojanized DLL file called "libcrypto-1_1.dll", which will be side-loaded to the OpenVPN client upon execution. A similar process, most likely by the same threat actor, was mentioned earlier this year and describes documents that date back to middle 2020. It then creates a persistence for the VPN client by creating automatic execution of a .lnk file (C:\Users\%username%\AppData\Local\Temp\openvpn-gui.lnk).

OpenVPN DLL Sideloading

The malicious code in the sideloaded DLL unpacks an additional DLL in-memory and injects it into “notepad.exe”. A secondary payload hidden in an image file is then downloaded from “imgur.com”, a well-known cloud image storage service. The decrypted payload can be either NetWire or Remcos:

Screenshot of an image concealing a malicious payload

Remcos

The features for the Remcos RAT can be found on its official website, and includes:

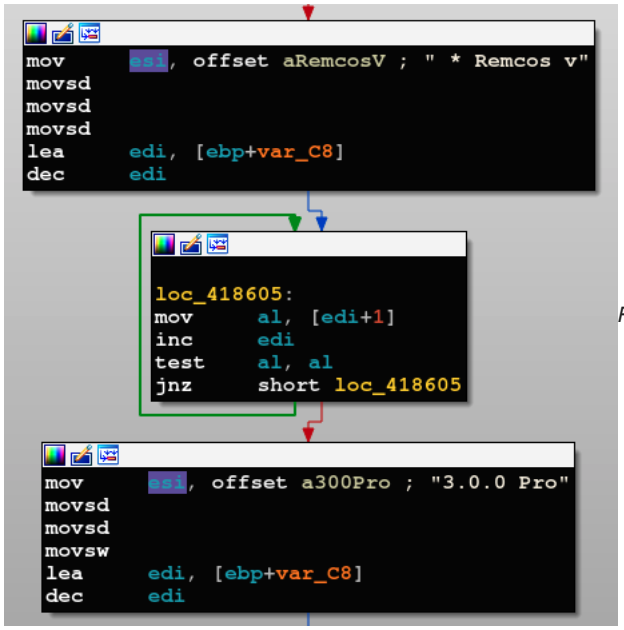
• Remote execution of shell commands on the infected machine

• Downloading and execution of additional payloads

• Screen capture

• Clipboard data management

The version that is used in this campaign is 3.0.0 professional, which also offers support and software updates:



Remcos variant as seen in its code

netwire

NetWire has been active for years, and in 2019 a new version was spotted in the wild. Some of the most notable features of NetWire include:

• Downloading and execution of additional payloads

• File and system managers

• Screen capture

• Browser credentials and history theft

• Gathering information about the victim’s system

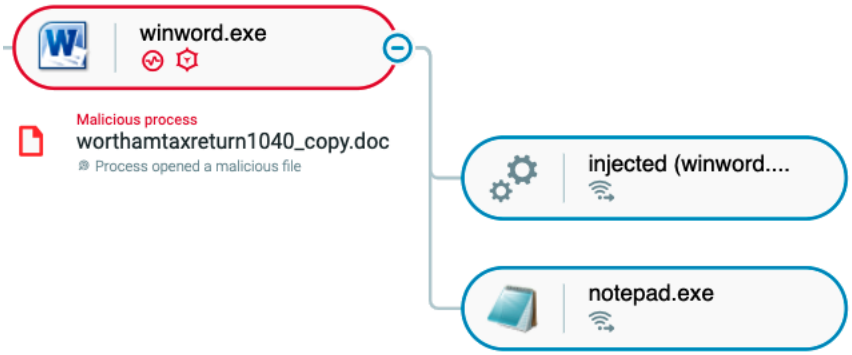
Similar to Remcos, the NetWire malware also contains indicative hardcoded strings:

```
loc_40C9CB:
lea     ebx, [esp+22Ch+var_210]
mov     [esp+22Ch+lpValueName], offset aNetwire ; "NetWire"
mov     [esp+22Ch+var_228], offset aSoftware ; "SOFTWARE\\"
mov     [esp+22Ch+Stream], 80000001h ; HKEY
call    sub_415BC0
mov     [esp+22Ch+var_228], 204h ; DWORD
mov     [esp+22Ch+Stream], ebx ; LPSTR
call    sub_40B740
test    al, al
jz      short loc_40CA0F
```

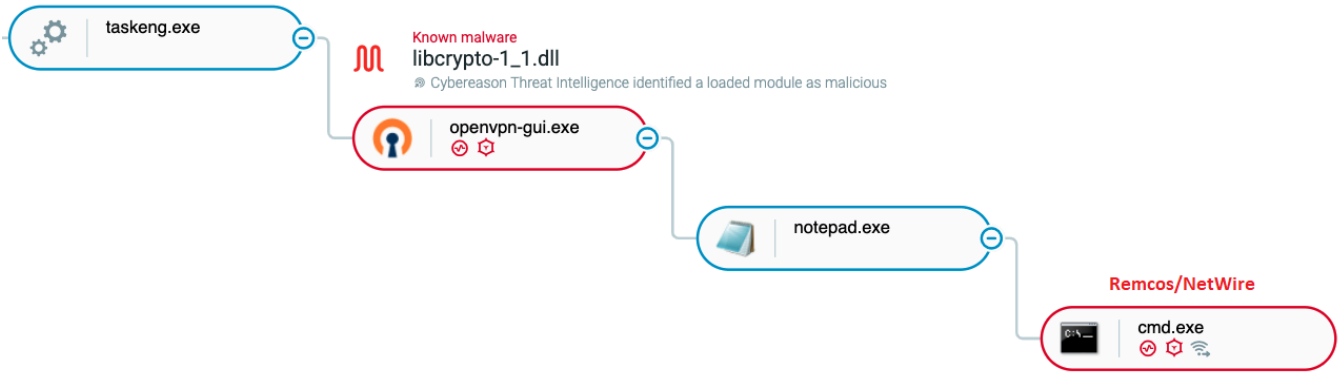
NetWire hardcoded strings

Cybereason Detection and Prevention

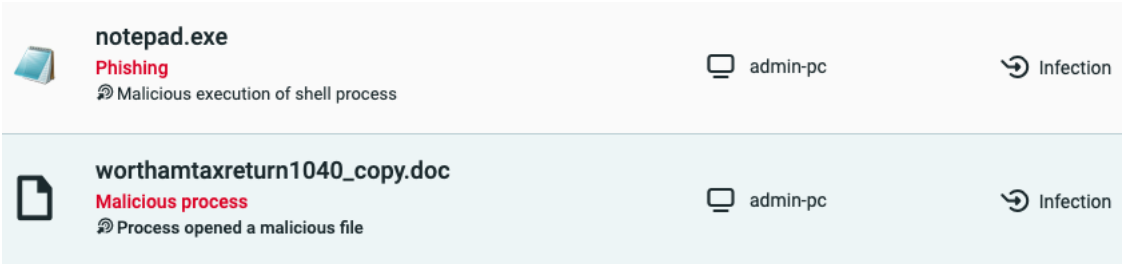
The Cybereason Defense Platform detects the execution of a malicious Word document used in the operation:



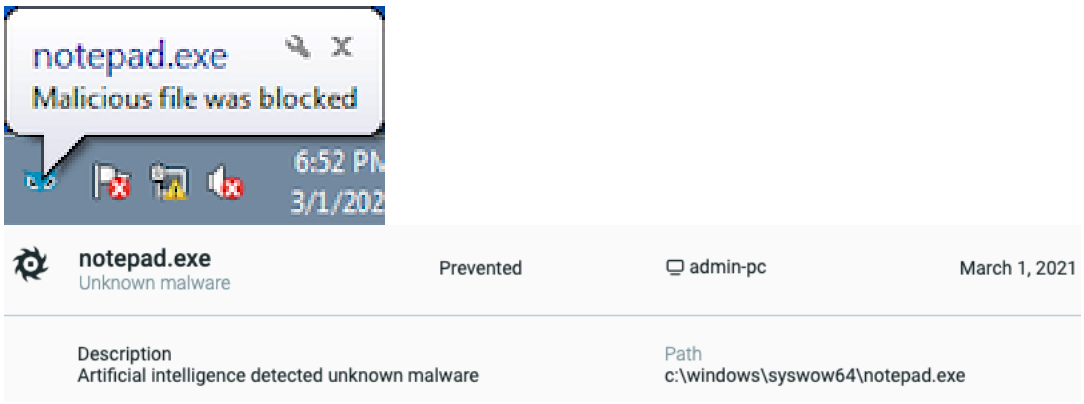
Once persistence is created in the first stage, the second stage of the attack is also detected, monitoring Remcos/NetWire injected into cmd.exe:



Corresponding Malops(™) are then triggered:



When the malicious sideloaded DLL is loaded by “openvpn-gui” in Prevention Mode, the Cybereason Defense Platform also detects the code injection into “notepad.exe” and prevents it from executing further:



Conclusion

Social engineering via phishing has been, and continues to be, the preferred infection method among cyber criminals and nation-state threat actors alike. In order to succeed, the threat actor must choose an interesting theme that is likely to lure its victim into opening the weaponized document or link.

In the campaign, we have demonstrated how cybercriminals are leveraging the US tax season to infect American taxpayers with the Remcos and NetWire remote access trojans, granting the malware operators full access and control over the victims' machines. The sensitive information collected from the victims can be used by the attackers to carry out financial fraud or can be traded in the underground communities.

Cybereason also noticed efforts by the threat actor designed the campaign to stay under the radar, using various techniques such as steganography, storing payloads on legitimate cloud-based services, and exploiting DLL sideloading against a legitimate software.

Looking for the IOCs? Click on the chatbot displayed in lower-right of your screen.

MITRE ATT&CK BREAKDOWN

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command & Control
Native API	Hijack Execution Flow: DLL sideloading	Process Injection	Deobfuscate/Decode Files or Information	OS Credential Dumping	System Time Discovery	Credential API Hooking	Ingress Tool Transfer
Exploitation for Client Execution	Event Triggered Execution: Application Shimming		Obfuscated Files or Information		Account Discovery	Input Capture: Credential API Hooking	Encrypted Channel
Command and Scripting Interpreter	Create or Modify System Process: Windows Service		Masquerading		System Service Discovery	Screen Capture	Remote Access Software
Scheduled Task/Job			Virtualization/Sandbox Evasion		File and Directory Discovery	Video Capture	Non-Application Layer Protocol
System Services: Service Execution			Obfuscated Files or Information: Steganography		System Information Discovery	Clipboard Data	Application Layer Protocol

	Obfuscated Files or Information: Software Packing	**Software Discovery: Security Software Discovery**
		Process Discovery
		System Network Configuration Discovery

NetWire and Remcos Malware | Indicator's of Compromise

Files

SHA1	SHA256	Type
5e4577a28a42c29cbc10fe738652666e5363da1d	0676238b5564db39016ffe66eb7e9b77a47271eed46e23575286954b8b78739f	VBA
1e17bf14f3ca714cefecc3c4b053bba23466b669	db0a8b2e977f64d6ee08775c832dabd4e5e005047275f87efb6be1d8ff4e142e	Malicious document
eac9b14781aec888b2008ee4f569265d30bbc231	1d44fe1b97e1de15c6b0d33630ce501ccecccd792a5e200979bd987fc7aea549	Malicious document
597f31535e717ce873d789e208c1cb0adcdd2f0d	5a25eb67f9800dc9151847eca2a5a8e1ea8e9ae2f1a17d0f4cfa1e9da3c6c23c	Malicious document
80b46bd974c1392cc6d3ea27d12093ae7537be50	95725086d5d56e7015c0aaa405640eefb5d4d62d9614dce331880753266ffb51	Malicious document
f0ac8d48ba43de1fc566d53597b2005496a3fcad	a15f82c78c11b0a317ca1fb07fab110354e197af8036f6e915e031007647bdf4	Malicious document
9bdfa52764d858b5f074a63ff7911a42dc12be93	5917635fc380adf07c49e632ae844225e7ff06a66fca5b20434c64cda0c875b5	Malicious document
fa5322d971210ed9627833b0c1beb6aa03cd1f84	cce9d7a318c1a8ed40dd0d3a858600424f34dfe8e0b5c91ffefeb58b495c70cb	Malicious document
f4e0104333250e0c2a688a7eb9772228ef5eb377 ccb5903ae3706e133420936ca6ab32ccb216480c fb78e2ef5010e62d18825e2e2eeacf3edbf0e0c1	26074ef98027d222d6cff9fae12df04cd0beb8966da16c0a915326759a6f4de7 23b0da3674d5c4d611e5d1660dfccf192c7a51a061e4e135bdd292d50b981ef8 9b67fd995fb48fe19efb7d5610e1e5906e5d7c56ec02b59081e8a9d9875101ba	Remcos loader
5581ee470231d0a2a3f4a4778343e29423a91be0 bc24701afa14f10f07ac01444c9abad6aaa346fd 8dfb536a399adc93484e4d68d953c2f9e87811b0	09054f1dafb72ef8930a4366ca27e26b9d30b503ce35256435b1296fee8d0cbc f7f721266f0e31b107b782bb5f5672eda5262c6c8654c75ad573ae2845f3c889 919b49583e0e3c8865f2c33d0ba566b4caf83c96a155f341ac46e6cfdb4daa39	NetWire loader
23376196f17eb5319ed663f1133447cf6f1f9441 6c6e6c382e39c18a0f83fe09824a96239da43c34 b3768b81cfa8813f1692963ea7308a19e213819a	f72ad2afb781f309d6155817fbf7f013123fa8cc475e527c22d564ba130be2f4 ae73d880e9b48c7714448fc3f1bf5e5836dfa6cf297d2e77bef045e980a7adff 6f248f6dd7ac467f8c9e39c7dda64825147df54cb2ae6a44e0d3c5e7530a3890	NetWire infection OpenVPN sideloaded DLL

435820a063f5d400bcd044194fab148968a07df7 d6123fb3b43ec3a64cb39ab1925539de1dc406e9 155b7a512175f802512d800dbe13e884c95d349f	8c74479d1b4d88b2f43b0e3589fbd4e7ffa0141c57011a2528205005ec657a86 b16cd6ed20daf9cba1a6f68dcc2f6ab48ce1cef89148fb03f74760c84ca885f1 aa5c12465da1126efb8af40ad4377f2951df27adfd6bfdd9929f49eefb844632	Remcos infection OpenVPN sideloaded DLL
826be84ef36bc065c4feaecaef0841fd7a2035a9 d6cf40cf57e0af9de9ea4406ea048724972a6bce e681ea9f3a49bae13c375389eab45e34a9f4082f 92ebe3ab3f4fa88d612365a954dd663522a8c45d	9a9975b28796eb5b5057a515cc49e4cd911ce734f80c4880f1455669cb14276e 5926c6d07e78b5b48f18ff008d474e46b42a93c20302f391e90343f57e7aa02a 56ef472cd74cd04afd42083c1d836767e7d4a48b991379420cda9317bf789a4a 131990449868578b35f7f649aa62bf2fc5b553a12874ee3f893d02d8673582f1	NetWire injected payload
df12d7fcc43da256a11c80d7f581bb5b845e8fac f1049602ae147dbc3efb428da789619ca8f42fb4 5cd11dde693f760b468a58a0db912cf5807ffbad	ca1ca8bf30feda8853391fb59ded4e46265165f738a867ff20667bad0579f4ea 04e0218dcad6ef6788eee1b1665bb413a7947844c01e9a157aa7c123f1cdced6 c604b7babe96d2d853dcf89b5a4e5737c077d372ee48279ecbeede3a041129da	Remcos injected payload

Remcos

C2 IPs

74.118.138[.]161

45.61.136[.]57

104.168.148[.]85

C2 Domains

petebots[.]cloud

www.designitwithmary[.]com

www.sophosmail[.]club

C2 URLs

https://i.imgur[.]com/6T75Qws.png

https://i.imgur[.]com/HUTEMgu.png

NetWire

C2 IPs

23.106.124[.]111

188.165.245[.]148

C2 Domains

eventsbypearce[.]host

escusemoisco[.]com

C2 URLs

https://i.imgur[.]com/Uef1u8s.png

https://i.ibb[.]co/djCM4KB/a-Ic-Xr-TDjs-A.jpg

About the Author

Daniel Frank

Daniel Frank is a senior Malware Researcher at Cybereason. Prior to Cybereason, Frank was a Malware Researcher in F5 Networks and RSA Security. His core roles as a Malware Researcher include researching emerging threats, reverse-engineering malware and developing security-driven code. Frank has a BSc degree in information systems.

All Posts by Daniel Frank