COVID-19 and FMLA Campaigns used to install new IcedID banking malware

COVID-19 and FMLA Campaigns used to install new IcedID banking malware

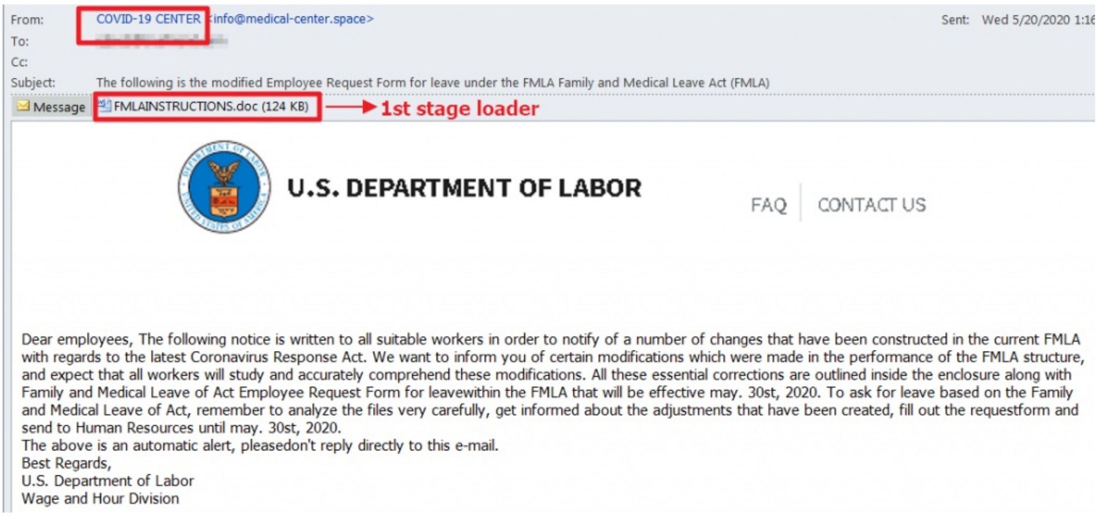
June 18, 2020
by **Paul Kimayong**

Juniper Threat Labs has been monitoring a campaign that pushes a new IcedID banking trojan. This new campaign changes tactics by injecting into msiexec.exe to conceal itself and use full steganography for downloading its modules and configurations. Previous versions of IcedID injected into svchost.exe and downloaded encrypted modules and config as ".dat" files. This campaign also takes advantage of the COVID-19 pandemic by using keywords such as COVID-19 and FMLA in email sender names and attachment names. IcedID is a banking malware that performs Man-in-the-Browser attacks to steal financial information.

In this blog, we will detail this campaign's infection chain and also touch on the network communications, including how quickly threat actors update and change their network communication.

1st Stage (Malicious Office Files)

The first stage of the infection chain starts with phishing emails with malicious attachments, such as below:



From: COVID-19 CENTER <info@medical-center.space> Sent: Wed 5/20/2020 1:16

To: [redacted]

Cc:

Subject: The following is the modified Employee Request Form for leave under the FMLA Family and Medical Leave Act (FMLA)

Message FMLAINSTRUCTIONS.doc (124 KB)

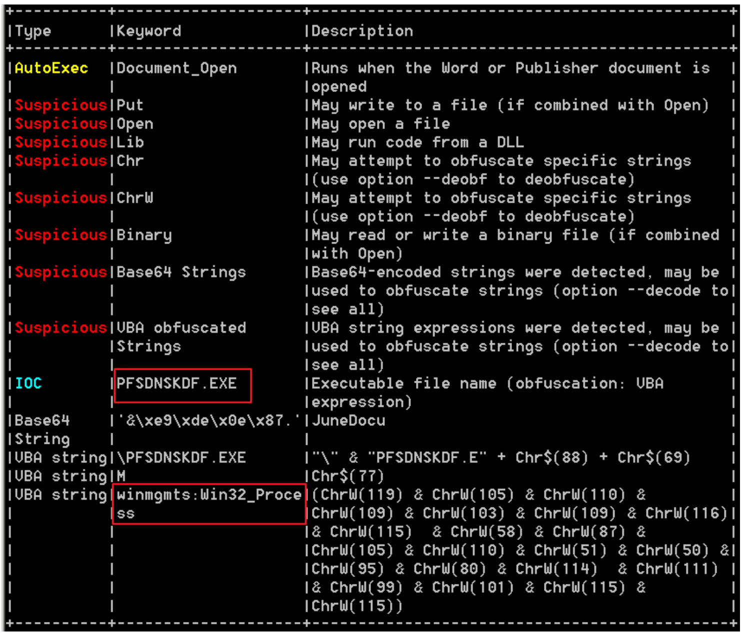
Dear employees, The following notice is written to all suitable workers in order to notify of a number of changes that have been constructed in the current FMLA with regards to the latest Coronavirus Response Act. We want to inform you of certain modifications which were made in the performance of the FMLA structure, and expect that all workers will study and accurately comprehend these modifications. All these essential corrections are outlined inside the enclosure along with Family and Medical Leave of Act Employee Request Form for leavewithin the FMLA that will be effective may. 30st, 2020. To ask for leave based on the Family and Medical Leave of Act, remember to analyze the files very carefully, get informed about the adjustments that have been created, fill out the requestform and send to Human Resources until may. 30st, 2020.
The above is an automatic alert, pleasedon't reply directly to this e-mail.
Best Regards,
U.S. Department of Labor
Wage and Hour Division

Sha256 of attachment: 822a8e3dfa14cd7aaac749dc0515c35cf20632717e191568ba5daf137db7ec17

The Word document has a malicious macro in it and, when opened by the victim, it will drop and execute a file in a specific folder.

- C:\1\Whole\PFSDNSKDF.EXE (Ee9fd78107cdcaffc274cf2484d6c74c56c7f3be39b1896894d9525506118d1e)

It achieves this by reading a binary embedded in it and using Windows Management Instrumentation (WMI) to execute the binary.



```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|Suspicious|Put                 |May write to a file (if combined with Open)  |
|Suspicious|Open                |May open a file                              |
|Suspicious|Lib                 |May run code from a DLL                      |
|Suspicious|Chr                 |May attempt to obfuscate specific strings    |
|          |                    |(use option --deobf to deobfuscate)          |
|Suspicious|ChrW                |May attempt to obfuscate specific strings    |
|          |                    |(use option --deobf to deobfuscate)          |
|Suspicious|Binary              |May read or write a binary file (if combined |
|          |                    |with Open)                                   |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|VBA obfuscated      |VBA string expressions were detected, may be |
|          |Strings             |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|IOC       |PFSDNSKDF.EXE       |Executable file name (obfuscation: VBA       |
|          |                    |expression)                                  |
|Base64    |'&\xe9\xde\x0e\x87.'|JuneDocu                                     |
|String    |                    |                                             |
|VBA string|\PFSDNSKDF.EXE      |"\" & "PFSDNSKDF.E" + Chr$(88) + Chr$(69)    |
|VBA string|M                   |Chr$(77)                                     |
|VBA string|winmgmts:Win32_Proce|(ChrW(119) & ChrW(105) & ChrW(110) &         |
|          |ss                  |ChrW(109) & ChrW(103) & ChrW(109) & ChrW(116)|
|          |                    |& ChrW(115)  & ChrW(58) & ChrW(87) &         |
|          |                    |ChrW(105) & ChrW(110) & ChrW(51) & ChrW(50) &|
|          |                    |ChrW(95) & ChrW(80) & ChrW(114)  & ChrW(111) |
|          |                    |& ChrW(99) & ChrW(101) & ChrW(115) &         |
|          |                    |ChrW(115))                                   |
+----------+--------------------+---------------------------------------------+
```

Olevba output of the malicious word document

2nd Stage Loader

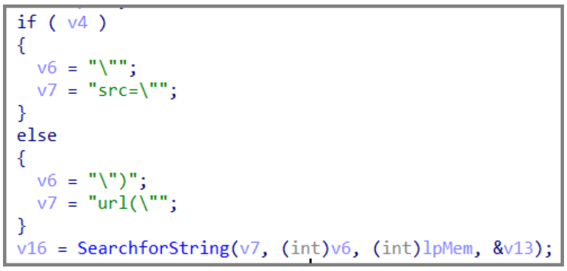
The file C:\1\Whole\PFSDNSKDF.EXE that was dropped by the malicious document is another loader whose purpose is to download another IcedID loader. It first unpacked itself by reading a binary file embedded in its resource, decrypting it and executing in memory. It will then loop on the following domains, using WinHTTP queries:

- support.apple.com

- www.intel.com
- help.twitter.com
- support.microsoft.com
- connuwedro[.]xyz
- support.oracle.com

All of the above queries are normal, except for **connuwedro[.]xyz.** It does this to evade detection by trying to blend to normal traffic.

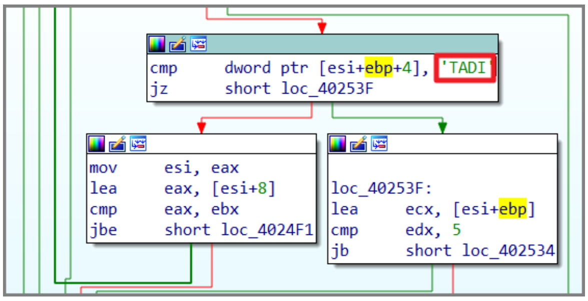
It is specifically looking for a response that is a PNG file and ignores responses with tags present in an html, such as the following:



```
if ( v4 )
{
  v6 = "\"";
  v7 = "src=\"";
}
else
{
  v6 = "\")";
  v7 = "url(\"";
}
v16 = SearchforString(v7, (int)v6, (int)lpMem, &v13);
```

Code Snippet for filtering out benign domains

It expects a PNG file as a response from connuwedro[.]xyz. To confirm this, it will specifically look for the DWord "IDAT", which is a tag found in any PNG files.



```
cmp     dword ptr [esi+ebp+4], 'TADI'
jz      short loc_40253F
```

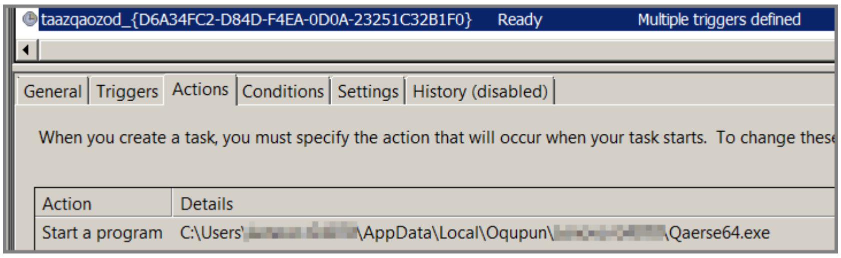
```
mov     esi, eax
lea     eax, [esi+8]
cmp     eax, ebx
jbe     short loc_4024F1
```

```
loc_40253F:
lea     ecx, [esi+ebp]
cmp     edx, 5
jb      short loc_402534
```

Code snippet for finding the 'IDAT' keyword on PNG file

It would then decrypt this PNG file using the RC4 algorithm and execute the embedded binary. It also includes checksum checking in the code to make sure that it is the correct file. This technique is also known as steganography.

The binary will be saved in the %APPDATA% folder and, for persistence, it creates a scheduled task that will execute every hour.



taazqaozod_{D6A34FC2-D84D-F4EA-0D0A-23251C32B1F0}   Ready   Multiple triggers defined

When you create a task, you must specify the action that will occur when your task starts. To change these

Action	Details
Start a program	C:\Users\[redacted]\AppData\Local\Oqupun\[redacted]\Qaerse64.exe

Task Job of 3rd stage loader

The hash of the binary is c35dd2a034376c5f0f22f0e708dc773af8ee5baf83e2a4749f6f9d374338cd8e and we designate it as the 3rd stage loader whose purpose is to download the IcedID main module.

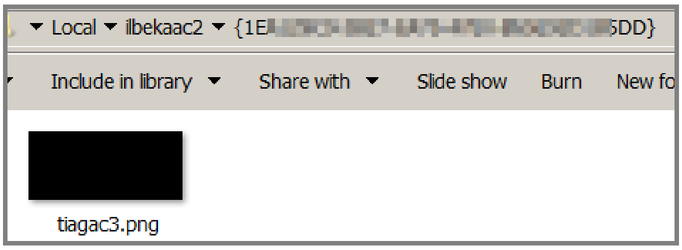
3rd Stage Loader and Main Module

This is the loader that will download the IcedID main module. Similar to the second stage, it applies the same technique of unpacking itself and using steganography. It unpacks an embedded binary in its resource and executes it. Once unpacked, it will download the IcedID main module as a PNG file from the following link:

- https://cucumberz99[.]club/image?id={01XXXXXXXXXXXXXXXXXXXXX}

This domain resolves to 31.24.224[.]12, during our analysis.

The image will be saved in the following directory:

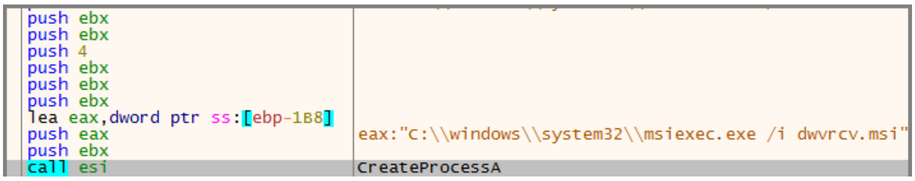


IcedID stored as PNG file

This image is stored at that specific location so that when the third stage loader starts, it does not need to download it again. The size of the image is more than 600KB and embedded in it is the encrypted IcedID main module. The encryption algorithm is RC4 and the keys are also embedded in the image at specific offset.

The decrypted code is not a complete PE image, as it does not contain any header. Most of its strings are also encrypted, which makes analysis even harder.

The first part of the shellcode is to spawn a suspended process of msiexec.exe.



```
push ebx
push ebx
push 4
push ebx
push ebx
lea eax,dword ptr ss:[ebp-1B8]
push eax                          eax:"C:\\windows\\system32\\msiexec.exe /i dwvrcv.msi"
push ebx
call esi                          CreateProcessA
```

Code snippet for injecting to msiexec.exe

It calls the following series of API calls to inject itself on the remote process before it exits:

ZwWriteVirtualMemory, ZwProtectVirtualMemory, ZwQueueApcThread, NtResumeThread.

Using **msiexec.exe /i {random name}.msi** is a simple technique to try to conceal itself and look like a normal installation of an msi application.

The code injected into an msiexec.exe sends a beacon signal to the CnC server and awaits commands. The commands include:

- Update the IcedID main module
- Update configurations
- Send bot logs to the server
- Execute a shellcode from the CnC server
- Collect system information
- Download and execute a file from the CnC server
- Execute a command and send results to the server

- Reboot the client machine
- Upload a file to the server
- Extract passwords stored in browsers and mail applications

Man-in-the-Browser

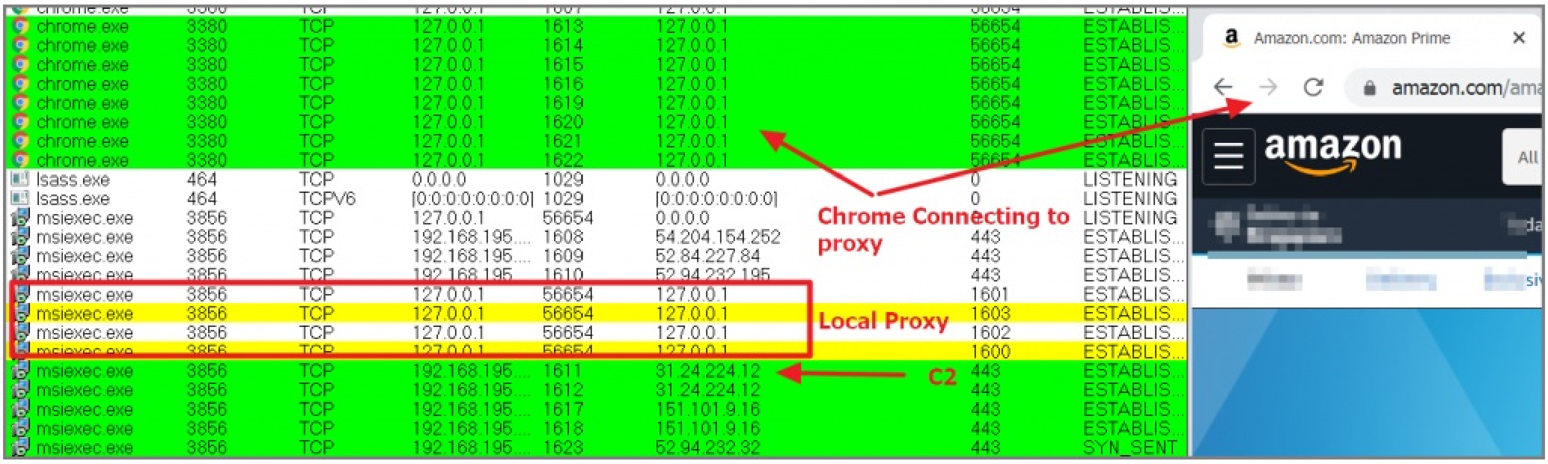
The IcedID core's main function is to steal financial data using webinjects. The IcedID main module, which is injected into msiexec process, watches for specific browser process names:

- Firefox.exe
- Chrome.exe
- Iexplore.exe

When it finds that a browser process is present, three things happen:

- It creates a local proxy that listens on 127.0.0.1:56654
- It hooks the following API on the browsers:
    - Chrome.exe and Iexplore.exe
        - CertGetCertificateChain
        - CertVerifyCertificateChainPolicy
        - connect
    - Firefox.exe
        - connect
        - SSL_AuthCertificateHook or function from the library SSL3.dll
- It generates a self-signed certificate in the %TEMP% folder

With these three things, all connections to the browser are proxied to msiexec.exe and it achieves full control of the browser.



```
chrome.exe    3380  TCP     127.0.0.1            1607   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1613   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1614   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1615   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1616   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1619   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1620   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1621   127.0.0.1             56654  ESTABLIS...
chrome.exe    3380  TCP     127.0.0.1            1622   127.0.0.1             56654  ESTABLIS...
lsass.exe     464   TCP     0.0.0.0              1029   0.0.0.0               0      LISTENING
lsass.exe     464   TCPV6   [0:0:0:0:0:0:0:0]    1029   [0:0:0:0:0:0:0:0]     0      LISTENING
msiexec.exe   3856  TCP     127.0.0.1            56654  0.0.0.0               0      LISTENING
msiexec.exe   3856  TCP     192.168.195....      1608   54.204.154.252        443    ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1609   52.84.227.84          443    ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1610   52.94.232.195         443    ESTABLIS...
msiexec.exe   3856  TCP     127.0.0.1            56654  127.0.0.1             1601   ESTABLIS...
msiexec.exe   3856  TCP     127.0.0.1            56654  127.0.0.1             1603   ESTABLIS...
msiexec.exe   3856  TCP     127.0.0.1            56654  127.0.0.1             1602   ESTABLIS...
msiexec.exe   3856  TCP     127.0.0.1            56654  127.0.0.1             1600   ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1611   31.24.224.12          443    ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1612   31.24.224.12          443    ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1617   151.101.9.16          443    ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1618   151.101.9.16          443    ESTABLIS...
msiexec.exe   3856  TCP     192.168.195....      1623   52.94.232.32          443    SYN_SENT
```

TCPView results on a system infected with IcedID

It will monitor browser activity related to financial transactions and inject forms on the fly to try to steal credit card details. Among the banks and financial-related services it targets are the following:

- Amazon.com
- American Express
- AT&T
- Bank Of America
- Capital One
- Chase
- CIBC
- Comerica
- Dell
- Discover
- Dollar Bank

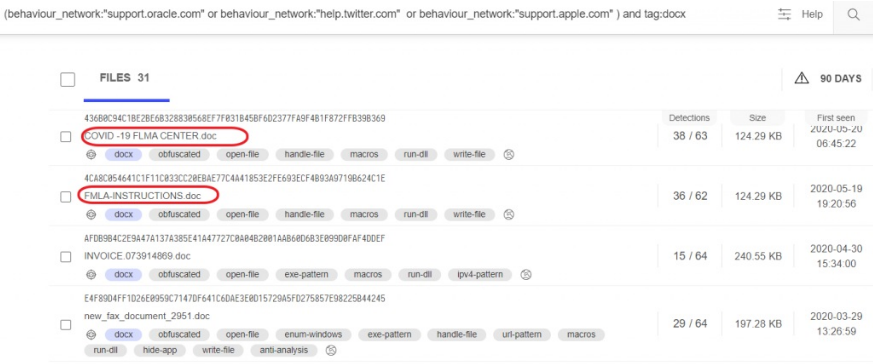
- eBay
- Erie Bank
- E-Trade
- Frost Bank
- Halifax UK
- Hancock Bank
- Huntington Bank
- J.P. Morgan
- Lloyds Bank
- M&T bank
- Centennial Bank
- PNC
- RBC
- Charles Schwab
- SunTrust Bank
- Synovus
- T-Mobile
- Union Bank
- USAA
- US Bank
- Verizon Wireless
- Wells Fargo

More details about the functionality of the main module have already been discussed by various security blogs. We link to these in the reference section.

Let's Go Hunt

1st Stage Loader

The vast majority of benign documents do not perform any network communication, even towards benign domains. The following network behavior could be used for finding other samples related to this campaign. With this, we have found other samples that are using COVID-19 and FMLA keywords. All of them have macros.

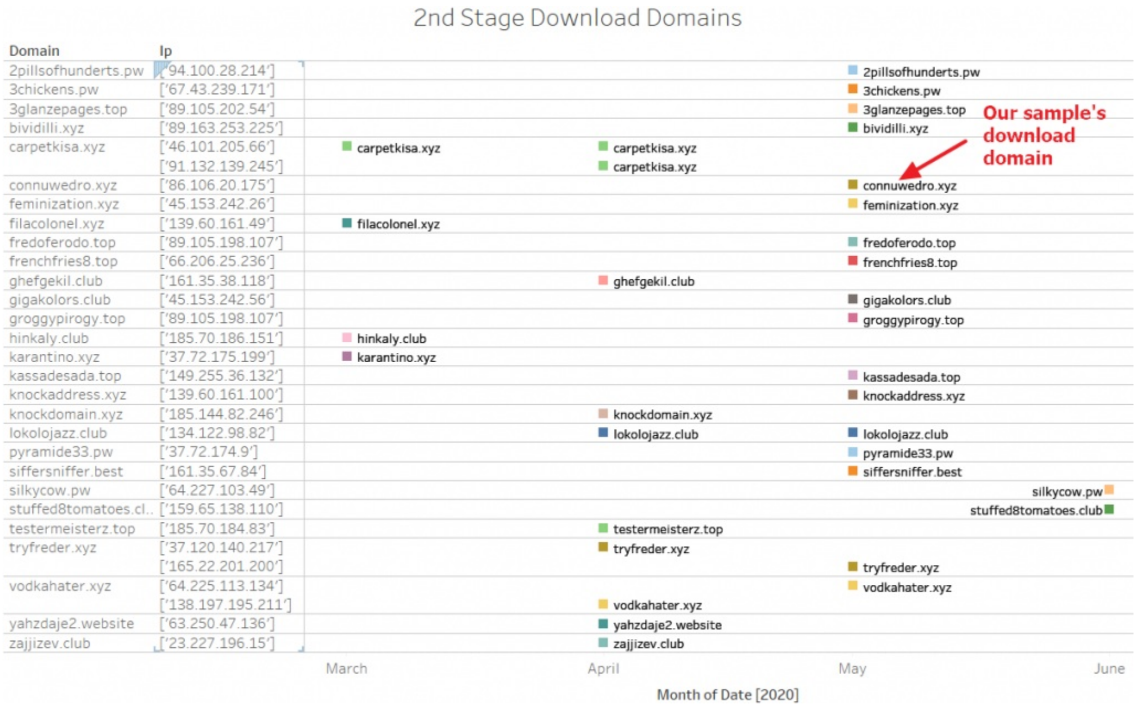


(behaviour_network:"support.oracle.com" or behaviour_network:"help.twitter.com" or behaviour_network:"support.apple.com") and tag:docx

	Detections	Size	First seen
436B0C94C1BE2BE6B328830568EF7F031B45BF6D2377FA9F4B1F872FFB39B369 COVID -19 FLMA CENTER.doc docx obfuscated open-file handle-file macros run-dll write-file	38 / 63	124.29 KB	2020-05-20 06:45:22
4CA8C054641C1F11C033CC20EBAE77C4A41853E2FE693ECF4B93A9719B624C1E FMLA-INSTRUCTIONS.doc docx obfuscated open-file handle-file macros run-dll write-file	36 / 62	124.29 KB	2020-05-19 19:20:56
AFDB9B4C2E9A47A137A385E41A47727C0A04B2001AAB60D6B3E099D0FAF4DDEF INVOICE.073914869.doc docx obfuscated open-file exe-pattern macros run-dll ipv4-pattern	15 / 64	240.55 KB	2020-04-30 15:34:00
E4F89D4FF1D26E0959C7147DF641C6DAE3E0D15729A5FD275857E98225B44245 new_fax_document_2951.doc docx obfuscated open-file enum-windows exe-pattern handle-file url-pattern macros run-dll hide-app write-file anti-analysis	29 / 64	197.28 KB	2020-03-29 13:26:59

VT search for finding related malware

For the second stage, we found 29 unique domains with varying IP resolutions.



Domain	Ip
2pillsofhunderts.pw	['94.100.28.214']
3chickens.pw	['67.43.239.171']
3glanzepages.top	['89.105.202.54']
bividilli.xyz	['89.163.253.225']
carpetkisa.xyz	['46.101.205.66'] ['91.132.139.245']
connuwedro.xyz	['86.106.20.175']
feminization.xyz	['45.153.242.26']
filacolonel.xyz	['139.60.161.49']
fredoferodo.top	['89.105.198.107']
frenchfries8.top	['66.206.25.236']
ghefgekil.club	['161.35.38.118']
gigakolors.club	['45.153.242.56']
groggypirogy.top	['89.105.198.107']
hinkaly.club	['185.70.186.151']
karantino.xyz	['37.72.175.199']
kassadesada.top	['149.255.36.132']
knockaddress.xyz	['139.60.161.100']
knockdomain.xyz	['185.144.82.246']
lokolojazz.club	['134.122.98.82']
pyramide33.pw	['37.72.174.9']
siffersniffer.best	['161.35.67.84']
silkycow.pw	['64.227.103.49']
stuffed8tomatoes.cl..	['159.65.138.110']
testermeisterz.top	['185.70.184.83']
tryfreder.xyz	['37.120.140.217'] ['165.22.201.200']
vodkahater.xyz	['64.225.113.134'] ['138.197.195.211']
yahzdaje2.website	['63.250.47.136']
zajjizev.club	['23.227.196.15']

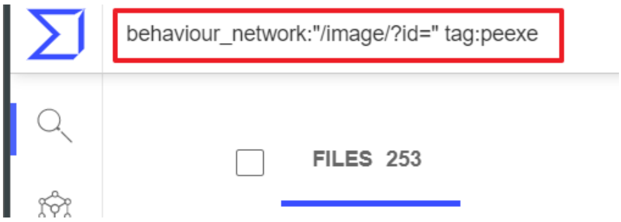
Our sample's download domain

Download Domains for Third Stage

3rd Stage and Main Module

The network communication of this IcedID is unique, as it follows this specific format:

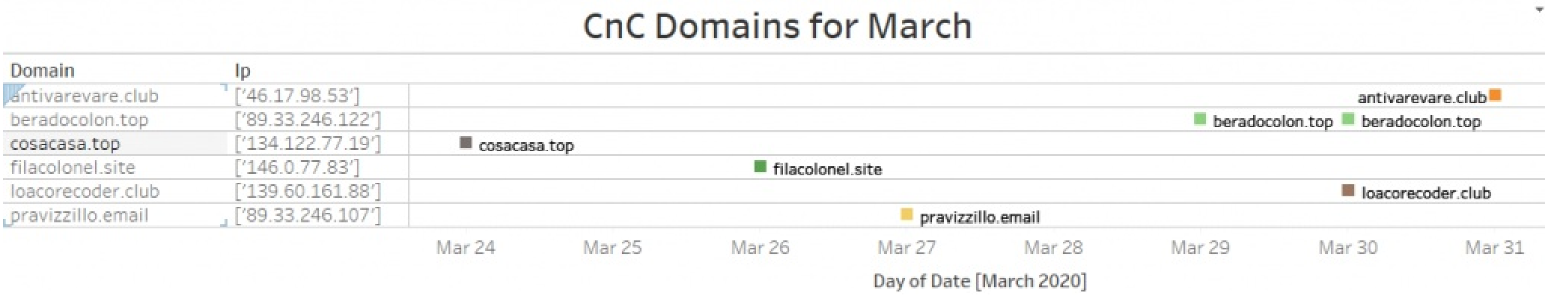
- {cnc_domain}**/image/?id=01**XXXXXXXXXXXXXXXXXXXXXX



behaviour_network:"/image/?id=" tag:peexe

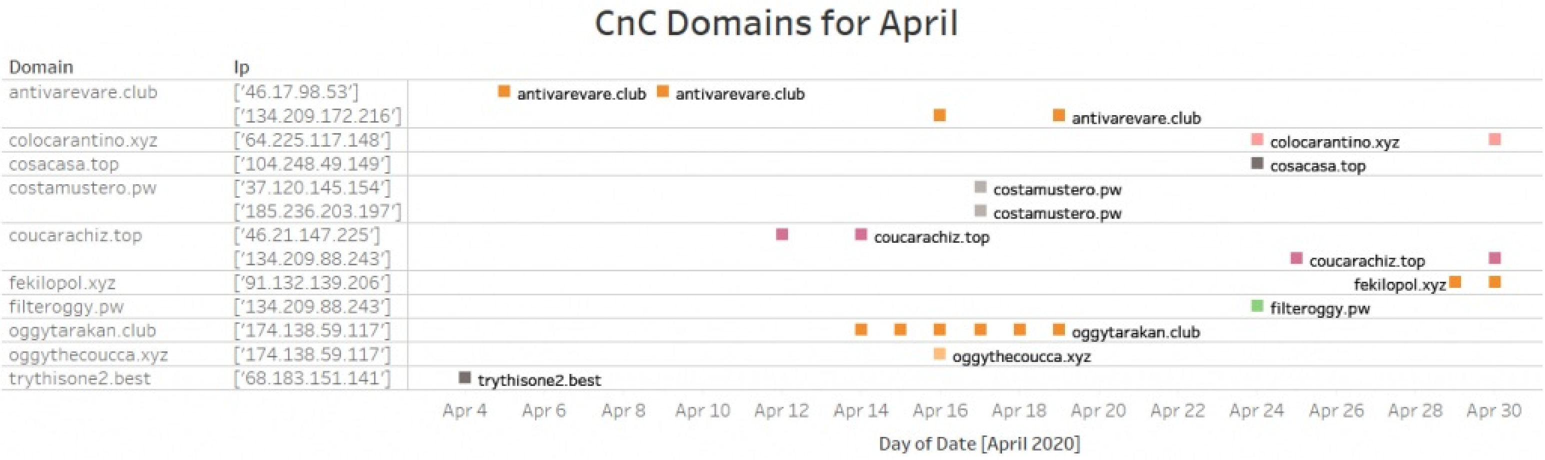
VT Query for hunting third stage loaded

Using VTs behavior search module, we are able to find approximately 250 unique samples. Out of these samples, we identified 62 unique C2 domains. The complete list of hashes and domains will be listed in the IOC section of this blog. The following data shows how quickly IcedID threat actors update or change their CnC.



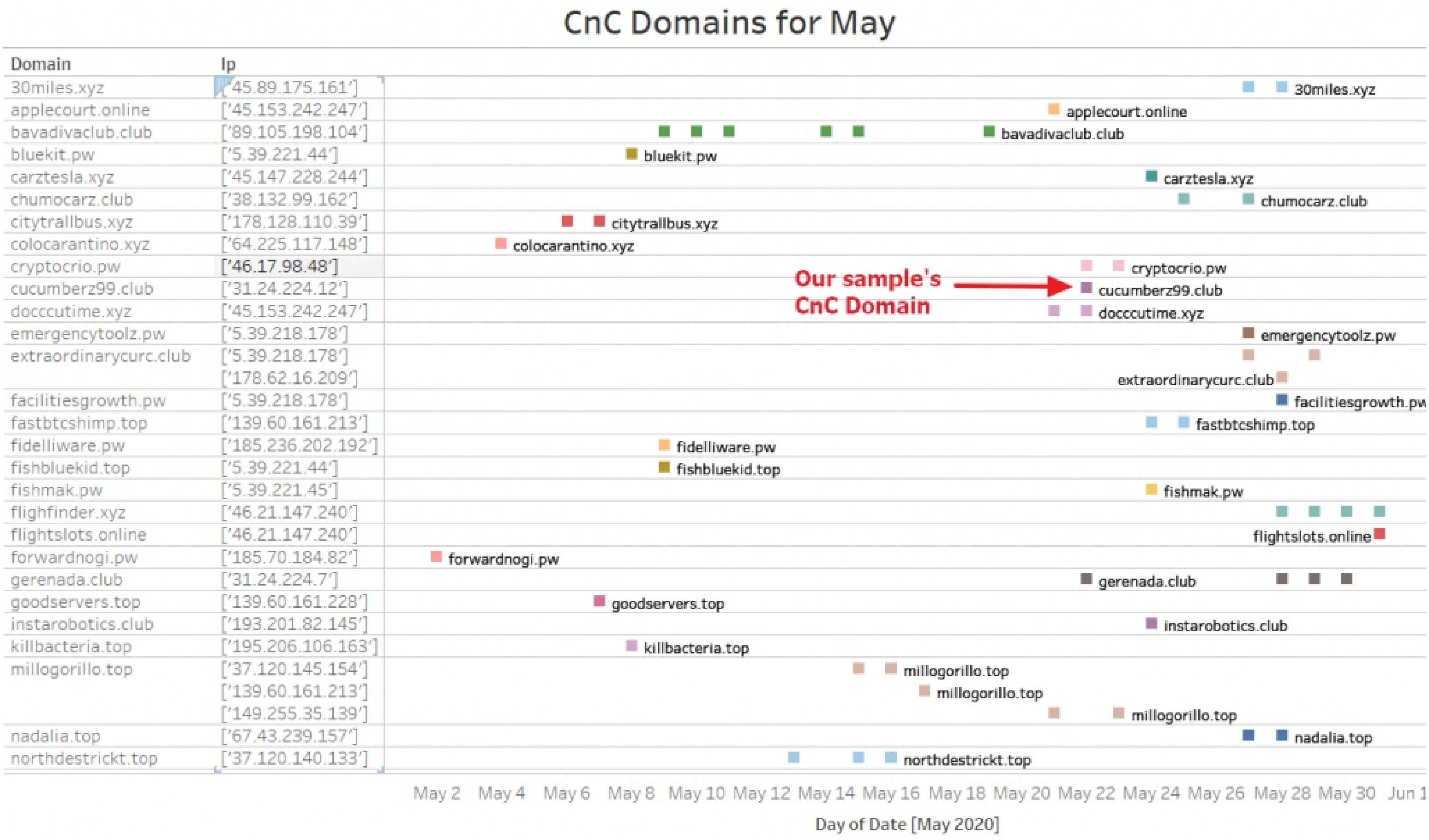
Domain	Ip
antivarevare.club	['46.17.98.53']
beradocolon.top	['89.33.246.122']
cosacasa.top	['134.122.77.19']
filacolonel.site	['146.0.77.83']
loacorecoder.club	['139.60.161.88']
pravizzillo.email	['89.33.246.107']

CnC Domains for March



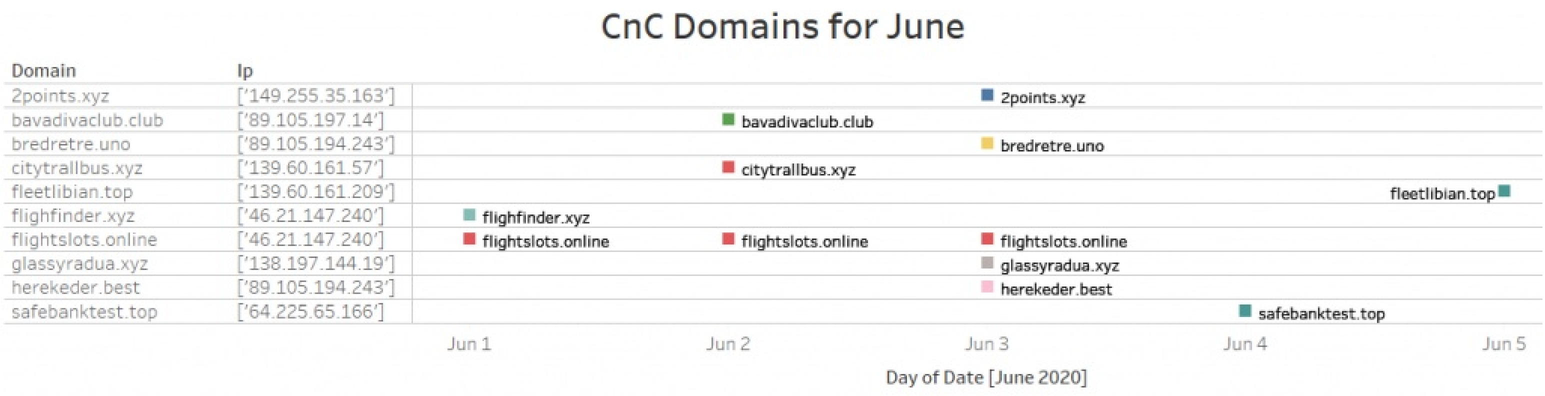
Domain	Ip
antivarevare.club	['46.17.98.53'] ['134.209.172.216']
colocarantino.xyz	['64.225.117.148']
cosacasa.top	['104.248.49.149']
costamustero.pw	['37.120.145.154'] ['185.236.203.197']
coucarachiz.top	['46.21.147.225'] ['134.209.88.243']
fekilopol.xyz	['91.132.139.206']
filteroggy.pw	['134.209.88.243']
oggytarakan.club	['174.138.59.117']
oggythecoucca.xyz	['174.138.59.117']
trythisone2.best	['68.183.151.141']

CnC Domains for April



Domain	Ip
30miles.xyz	['45.89.175.161']
applecourt.online	['45.153.242.247']
bavadivaclub.club	['89.105.198.104']
bluekit.pw	['5.39.221.44']
carztesla.xyz	['45.147.228.244']
chumocarz.club	['38.132.99.162']
citytrallbus.xyz	['178.128.110.39']
colocarantino.xyz	['64.225.117.148']
cryptocrio.pw	['46.17.98.48']
cucumberz99.club	['31.24.224.12']
docccutime.xyz	['45.153.242.247']
emergencytoolz.pw	['5.39.218.178']
extraordinarycurc.club	['5.39.218.178'] ['178.62.16.209']
facilitiesgrowth.pw	['5.39.218.178']
fastbtcshimp.top	['139.60.161.213']
fidelliware.pw	['185.236.202.192']
fishbluekid.top	['5.39.221.44']
fishmak.pw	['5.39.221.45']
flighfinder.xyz	['46.21.147.240']
flightslots.online	['46.21.147.240']
forwardnogi.pw	['185.70.184.82']
gerenada.club	['31.24.224.7']
goodservers.top	['139.60.161.228']
instarobotics.club	['193.201.82.145']
killbacteria.top	['195.206.106.163']
millogorillo.top	['37.120.145.154'] ['139.60.161.213'] ['149.255.35.139']
nadalia.top	['67.43.239.157']
northdestrickt.top	['37.120.140.133']

CnC Domains for May



Domain	Ip
2points.xyz	['149.255.35.163']
bavadivaclub.club	['89.105.197.14']
bredretre.uno	['89.105.194.243']
citytrallbus.xyz	['139.60.161.57']
fleetlibian.top	['139.60.161.209']
flighfinder.xyz	['46.21.147.240']
flightslots.online	['46.21.147.240']
glassyradua.xyz	['138.197.144.19']
herekeder.best	['89.105.194.243']
safebanktest.top	['64.225.65.166']

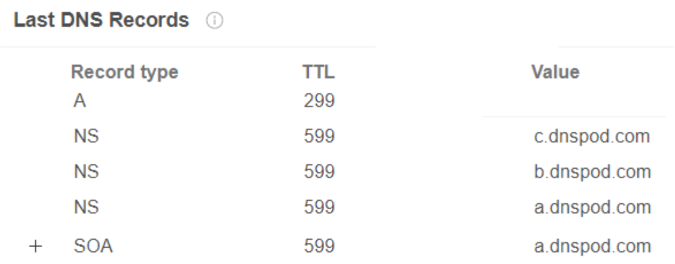
CnC Domains for June

A commonality among these download and CnC domains is that they only use the following TLDS:

- .xyz
- .club
- .top
- .pw
- .online

- .email
- .best
- .bid
- .site
- .uno

All of these domains also use the Nameserver **dnspod.com**



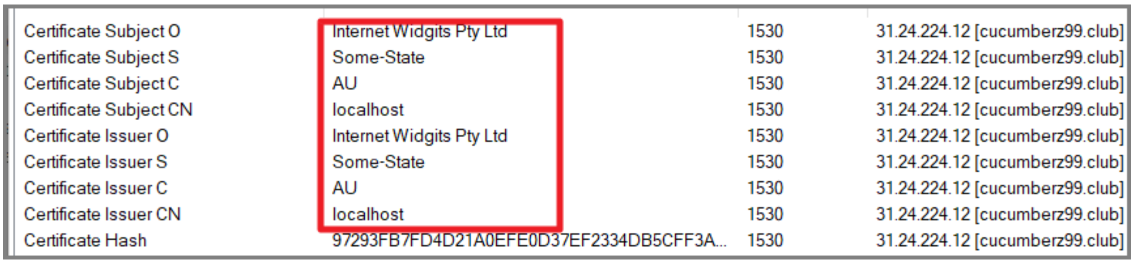
Last DNS Records

	Record type	TTL	Value
	A	299	
	NS	599	c.dnspod.com
	NS	599	b.dnspod.com
	NS	599	a.dnspod.com
+	SOA	599	a.dnspod.com

Nameserver information of IcedID download and CnC domains

Self-signed certificates

IcedID uses TLS in all of its communication but the certificate is self-signed. They can be spotted, as they use this kind of a self-signed certificate. The keyword “Internet Widgits Pty Ltd” is also being used by Trickbot, another banking malware, and it is believed that Trickbot and IcedID are cousins.



Certificate Subject O	Internet Widgits Pty Ltd	1530	31.24.224.12 [cucumberz99.club]
Certificate Subject S	Some-State	1530	31.24.224.12 [cucumberz99.club]
Certificate Subject C	AU	1530	31.24.224.12 [cucumberz99.club]
Certificate Subject CN	localhost	1530	31.24.224.12 [cucumberz99.club]
Certificate Issuer O	Internet Widgits Pty Ltd	1530	31.24.224.12 [cucumberz99.club]
Certificate Issuer S	Some-State	1530	31.24.224.12 [cucumberz99.club]
Certificate Issuer C	AU	1530	31.24.224.12 [cucumberz99.club]
Certificate Issuer CN	localhost	1530	31.24.224.12 [cucumberz99.club]
Certificate Hash	97293FB7FD4D21A0EFE0D37EF2334DB5CFF3A...	1530	31.24.224.12 [cucumberz99.club]

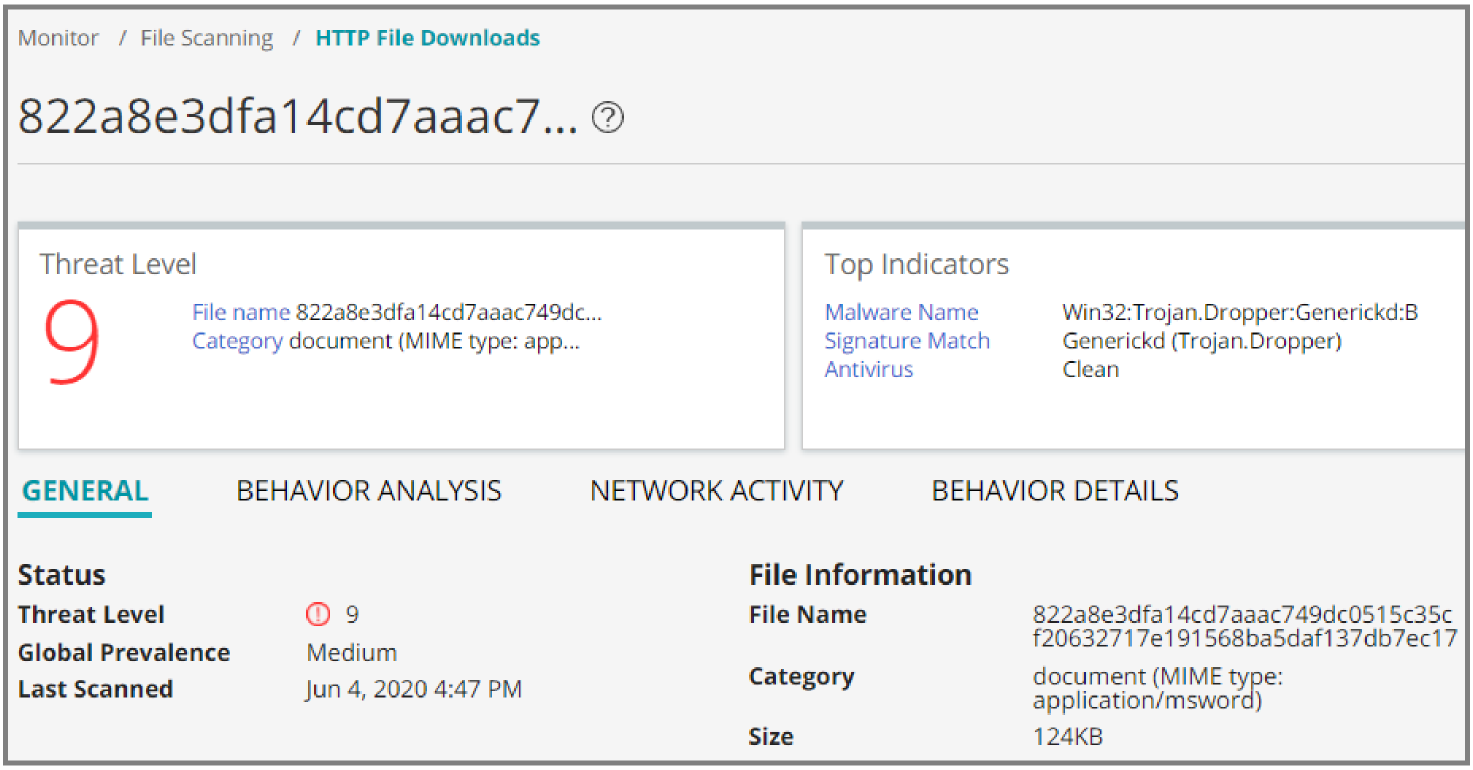
Network Miner output of IcedID certificate

Conclusion

IcedID is a very complex malware and there is no doubt the threat actors behind this are very much capable with constant updates to their arsenal. In summary, this latest IcedID Campaign focused on evasion by implementing the following:

- Signed Binary Proxy Execution using msiexec
- Full steganography
- HTTPS communication
- String encryption
- Blend communication with normal traffic

Juniper Advanced Threat Prevention (ATP) products detect this malware.



Monitor / File Scanning / **HTTP File Downloads**

822a8e3dfa14cd7aaac7... ?

Threat Level

9

File name 822a8e3dfa14cd7aaac749dc...
Category document (MIME type: app...

Top Indicators

Malware Name	Win32:Trojan.Dropper:Generickd:B
Signature Match	Generickd (Trojan.Dropper)
Antivirus	Clean

Status

Threat Level	ⓘ 9
Global Prevalence	Medium
Last Scanned	Jun 4, 2020 4:47 PM

File Information

File Name	822a8e3dfa14cd7aaac749dc0515c35cf20632717e191568ba5daf137db7ec17
Category	document (MIME type: application/msword)
Size	124KB

Juniper ATP detection

IOC

1st stage malicious documents

- 822a8e3dfa14cd7aaac749dc0515c35cf20632717e191568ba5daf137db7ec17
- 74d6e374d7958e70c6733b6c17e2f0d79b629e172aaf385c142c76678647f3b8
- 436b0c94c1be2be6b328830568ef7f031b45bf6d2377fa9f4b1f872ffb39b369
- 4ca8c054641c1f11c033cc20ebae77c4a41853e2fe693ecf4b93a9719b624c1e
- afdb9b4c2e9a47a137a385e41a47727c0a04b2001aab60d6b3e099d0faf4ddef
- e4f89d4ff1d26e0959c7147df641c6dae3e0d15729a5fd275857e98225b44245
- 3ff97578adea9f45bccea091234c5ccee6a12b3c52e7e29195a45e3c191aa926
- e15744eb13666670ad3cf256c31df57a01c40f355a0f8a592294187d4fedc257
- 454ff6a5ebf01fc7d9c1ced5b081d582d11119ab9b49fc06ccaf22b1b0259c23
- 54197c58c9693580c8ca961d8ff326cbad7688b23627114f7437c59fede46e82
- f1bf5ef89f644b1558dd54e68148e60310d537ca45c2daae2b410c30540d7de6
- e48e4e74dc7e67523878a2cf68b2ce72b5e5c999897e075d6b993e41c81f4174
- ef2ab4bc4ee63dd1b9f04a56fe727a87f56ddd476bc1cd72c78f4d31abff322a
- fd1173670139581345909 1b6d07878c52b448a4d9a5825517a0308fbfe6fa070
- 9979063dae01bdfffd946ed012e69fabb82be3795323a52b06532b42b0f59609
- 09c3ada49c47af20854d87fbb76a24263d759f93f8de7e5af88549111ce55dda
- 10ab8bfff505a3add9537bf742ede32f985e9f1ecc3a8afca99005b7255bca1b
- a6e0690db18e89187c2a9b0924585264606482dfdd9ac97c744bb649615ced65
- 1e988d02dedc8307c518e6bc2c6f8be14e4f0cd941972622deebcd90a6f09013
- f4fecef8cd7c7688d98ff168e137c70d98f01866114e552ede71aa28e2088018
- b0dc0a79862585b381afb61b05640276d51001961ddf9608703195bc183f1f06
- 8664c34e72bc78098668331faa8f5113ad798a29c085662a0a9d83c4598843b2
- 404650dbf9d8d4fcf844f529b042b895979f3a87334fb97925805c8072725ea8
- f5d8de500a504f6493af21ac67f50f5a4de5d6371e36c3a2251ac098f256187b
- 385a41aaa192a8cd56bc35b1841a8e4a31f4cae1d5b68542ae7584b6420d363e
- 55e1ba8683bb6b1d2a4f8b16b16ede25943d66e5884c9793f8c078614d12d9c4
- dea7eaee76df0fa27ae5ddd2988222b8afefd73ff80f5a5a14108cb499b85a23
- f30f283832f7a371c2c23cb2b5801e71bd33856c026480ab9165e584300fa3b3
- 57ea3ae558efce33cf28a5cefa26e93a07186e5cdf799d5d066edaf581f66706
- 2e294fbc75cefcbece50a3e57730212fd7672a4cce487db0bdfd241032a5bcb7
- 3a11e16512b0f4c1380c5f94ff65312c421955c5693ea73260e2274eb34470c8

2nd stage download domains

- 2pillsofhunderts[.]pw
- 3chickens[.]pw
- 3glanzepages[.]top
- bividilli[.]xyz
- carpetkisa[.]xyz
- connuwedro[.]xyz
- feminization[.]xyz
- filacolonel[.]xyz
- fredoferodo[.]top
- frenchfries8[.]top
- ghefgekil[.]club
- gigakolors[.]club
- goodcolonell[.]xyz
- groggypirogy[.]top
- hinkaly[.]club
- karantino[.]xyz
- kassadesada[.]top
- knockaddress[.]xyz
- knockdomain[.]xyz
- lokolojazz[.]club
- pyramide33[.]pw
- siffersniffer[.]best
- silkycow[.]pw
- stuffed8tomatoes[.]club
- testermeisterz[.]top
- tryfreder[.]xyz
- vodkahater[.]xyz
- yahzdaje2[.]website
- zajjizev[.]club
-

3rd stage loader hashes

- c35dd2a034376c5f0f22f0e708dc773af8ee5baf83e2a4749f6f9d374338cd8e
- 014b422e6c1bc23db2b5898dd0c49ac61fbac174c1e0d916f68b41cfb535cdb5
- 015243f1e4fa8c0eabf86ae752056e2876e50b3b67e95fa486451904d311580d
- 021cae01a3e9e734ca0b96c30d7d358b7b41c84565c95b448771de56ae85621e
- 063ed7054f8f7d72cb34f9a37725b5974fdafc743c338b07bc7b0b2ab6a212e1
- 06d21126d11e3fd07c66c7f9c096f80fa8046b5e1bf4370187401890fdf4fd5c
- 07671c10dd548d8a535939c0282d6710b07c8e2e8e7efa466de09202d02cd550
- 08bb93772c22c2842e968f5ad3753062530c4fcee87110afe46d95889c484dfb
- 0b0b92a625911a7065cf0e48d470acac71290c6832363a715b1f46aff01fe4c8
- 0c69c38b7d436280492807d77a308f2eec5007afc0683aa206358db91c116def
- 15041d3408372977905bda10cbccd9a86135eb441152968299e3c05ebcbae93c
- 16ae5983ca6e3f7bf893e0ba9ef44f2f46270a717abed860fdd56a7ad5cc8f77
- 16efa114618cdf5426f514c79597d29fe0ced79f32c5b56985cf2820854d7a36
- 18726b5405dc2f8159f3496939c5df3ca742ff271a2dd294b033433203f35eb3
- 1faa5ce90b3496c6938f3fe3a25f89939a297254a183fb75a8d58abfcc9fddfd
- 1fd7fea39524f3e5edcd0d41e9b2f9c9fa639ec22e80bacd173b7744b4a05601
- 2660abba68d81b50c997b787a98484e1eeea47269cdbe1f5ae87e6ac086b5237
- 26e0468acd186e744e895f116d14e20179d74f61fa819b5984442cac51f07b00
- 284aaafa51b1131e6656b270af6c3a032cf454ead1d5f0a5926ebe22772cf0d9
- 2aab4bb300e505e278a20a2aa804c9ba5920c2513b425440b1c818d53a0dd672

- 2b7ccec0aa1d9f09fb7d17034acf00b0e96dd47ecabe767b419a474a0854e42c
- 2ba7ecdb95e16f4af77d2cb09e301306c2115350da49e36afa26a365fceb110c
- 2bfa9f878dce2de087715d7986e369197aecd166a635c80a2f2c39a9b8e327fd
- 2e1d4c5755845068909b229939511d6a9a0b7b5df6801f44a3a3a274d6048804
- 32efada9f1ba73c5ded10c2338fe261e0e4c997f48696464978af942c9f2599f
- 3391f3da58a8b440b0c58084a280cf9cac28395ecf87c8307d5efb9d66b6164f
- 359ea0e4217bea81d92e6e274681ab7df24caaaaa0e6ad412e2f9045113c6ea1
- 386becd1260847d03958dbc82b5f6565e2855ed5439eef34b57678410877174e
- 396a445f43fc63122543cbb16fe2919e19aa2371f7165c3817acac7885701afd
- 3a09fb755bb94cfbd598d16c3a8dd430be51a1eed9dc5791a8f07bab6e2bc284
- 4267ef18ddeb15cf6920e2bc89f5c9247b6f554112a124ee2211281ce98ec04f
- 43275d3fdf60216df9c0151b11db2896a1dd56b9e7267ed6db78f4ef21cb8b46
- 44271a7612f1b32ed5fb0bac211992ea5e5c243710b9b4e8ad83f08af6a6cf4f
- 46a19f4b4dcfcb51b0db1718ad6d64bf0eb28170c61421e87e7edc07facd329c
- 48293a9ec8e7d12370cb1c1266653053ad5861761c74c437b2350aa909490327
- 4aec02ec7bc4ff2fbde2e36eb40411bcd69ee2dd9abeaccdd306a3aca8f5ad1a
- 4e7161be03f206c1b086bb15b47470ec1c9381302eb34d0e76915496aec77193
- 50cee93429653fd24d534c31c52a94e71b4fdc1e5409f8ac4ae2a81210ea12e2
- 5542f9cc78b5aa2901c2187f1dcee8e214aca20465c81c4da51035477d19287c
- 55acf5558ef68bd26148074c6f916311ea760edc6cbd136973ea638c98606a93
- 57100de2a289e45824f5cbaf8074e3f6e543eb2aa9a18584b1a007c7b4ddaa48
- 5c91d58ad4b5f1536c2548ac3080f02155df555025c634659cb15dfc5ec2143f
- 5de3eb250030550512c0ce92923ff30bc16529a45a5f24c624e9d7c7a4e0c1e4
- 5e38dcb3632d7ac183bded4662c139db2f54c104ae1efda75b62b0bd0b9882f1
- 61ca03447437e224ac301c56a72684a3c08310a3b850aff69952d124b488bc4e
- 696ef2c7fb064b293173bae309c1cabe3d2dd2d1a1becab040acb05c82022c2e
- 69fced2e42d5fcb3b0ade5ebc81359c1f8c2e51935db74f40c94fb5c646130d9
- 6c02225c8a5ae583e738417866bc2f66636834ff025749da7f36ea639cbcacb6
- 6c878a7145e9f783f28b665207d9d180d04d0fe8e42bb2ff594faf5692f25ebd
- 72d4df9bca3cdf2074ffa84580c01fa425d528be54f331c59eb27a12a3736093
- 7a41e722fb6fd0067378cba5e4ddcb9c122205f41eee22204ce83af63a89b4fe
- 7babfaa95153f3f4c06630ff30d225760ae4a50e75764b9e049d8d70bfd88107
- 7f45cf09a572799af51ea935b95b185c05e13f749c9f1e2a2d41f8001c76487e
- 7fb71830442acb35dd86e559d632d7a14c21b60639203c61d371831b78dde6e3
- 81869e50ce5599cab247458445cc36b5a3108398f1ed520d29a4e7395a81afe0
- 82f48defd2de04d87de86ce8e584c6cb1bad8581d99e65ae99b58ef96f623089
- 87322aed33bf01ca618ad94e1d6a042bae91c978fabfb3e7fcccfa75a64c5d6a
- 882a9e7001dd1618c593f68e11f77c8e86239f610283e88981eecab93b5158a7
- 8831ac358046286facb6ca2643927aa837907937d1895ee3b73472c58bf3ef2c
- 8a4b045d11a898ced073e564e601b9624ace121be688ec20f31d56bc1edfc377
- 8a60949ae63dd0d80a49485a7a2ce1a29505ed76eee018ef12d28ac70bece07d
- 8d1b83eff1b3c604365fd29de1bb43204852de842c0bb148975fe7a7485310e4
- 8d97b91ce882f9405b7a7de5b1f08fdef0a0db4303977140546ebff72af1bc7f
- 9118ba30cefcc565be8a9ba85ee66da7670f18b08ec3cb205be80e78bf64f5fa
- 927a8d1445750400db3850d0b2dc3522b0f373098385373efa3d7762120f3689
- 949d06fb921d1e32be7232933d0578c086112c5b782640cd5b9a6b6570f27bf7
- 961588c90fe84a65e9aff3b98a95cd46d581add783ce639065665a01a16530f5
- 961ced78105cf07255f79dd7ad0ecaa2360b6ac08264acfb22d927e3d7f441c4
- 96c825103005a025660b5d32002a636d2242801949d0b970a77625be268a8cd5
- 97a32b419c28bfa62220fc8a7c715a899bf84484e34a75ee97c766d7d43b2b4a
- 9c19493c7ecb8067a0a52e089b819f53adf6a1f6b0535b42f1e5325a789125d9
- 9caa061ca9619b215e657357f368e9fa7d64e402c13d55b76578c5acddd25aab
- 9ff86c3e52aea34f885d1f298ee9e448368d941bf122f61278b6d50addb36744
- a234c29baff478276e9ae616046d98ca1ed57311616691a7e048e0af6d9c1c44
- a24fe24beb66aef2978017939f29a7eb3cbd1ca3d210a9834cae112ba86d075b
- a299a3d1d838adc37ea985039650b7b32428d3787a0b7e31feeafcb831eb984d

- a3d5871579dd194d86e5af84e306c38d27703bbe9b7e7d4209b68cafd21464e6
- a55a668b4180ea3cd58472dc0fb9b45dd92c09cf049644cbc25f5b50a9d05001
- a6fa541a097faa1f61b7085eb52b46bd893944f93a8bd20205118b1b7b802fd4
- a9129fc61d0ea9a2756c64febfc486895e37312e5ff8eabd16b7ff201bb90e7c
- ad58f15ff69ee59a32ae410acd564cd4b53a5cfaea6ede136046cee12f1c0b59
- adc05158b29dcb3f96532e526bdb296cb5e424a96e6f7b83b6c0b82b811d2740
- ade52f993013635afe7eaf0d91cc0521b97f3de1ca541882bde3ee94c872982f
- ade6356fb4f693664d5dcb54c3e1ca6a9013ef653b473bdd7a2e1407bddc6193
- b6c2ebd3be005f672514cbc3ab320b9dd887f17b6bc14bd5bd34adc5a951ef17
- b78d867fa64b9c7f8ad19b6fc4ec934b3c1c13e6fe080c84d4685629f18a0de6
- b7de965c5e2cfef42def39f124d37d1302ea93b91aa394d2cf41cfa7df2607e6
- b8768315d048093fc216c8921dcc392628d977ea97efcf352e5a89035635ffdd
- b90881ea27e45a5beec5abdcfa7f83709b8ca02b9a533a7d1325df059522d21c
- bdb743a2f2cd6ef45f9d0c97ec8feb590831d108bc7d434b5f65e87ab4be9746
- bf4da5aa980f12573157473f694210276a72d4f26cb7bfce38b84be5e33fd195
- c35dd2a034376c5f0f22f0e708dc773af8ee5baf83e2a4749f6f9d374338cd8e
- c57c797dc857427dd9d34524f32897cd001dd0d5526b7ae382158989a57541a4
- c7ef139a5291a1e2b70551f4fc8290a4bc963ba4bf36101aa787eab21fa2aa83
- ca59caa3199f6ec24cead3e4b705f8a22c5b78f3b62f84791c03784e3b55993a
- cba5edb9a6a3c25b635a050492d6f9e6cd69f916ec57f4787e5b2e3a8356182c
- cddb94b07baa8502aa7ec15815606d89630fc6d62790a42fb9b0aabe76700de1
- cebb538862dcfa960e48d09a7d44dc0b096cff66bd61606f54949433ce94ff7f
- ced9b6411f4c3db104f9b25b9c638f5874097219152c1800fd7988f03da15b29
- cf79819a5ab92e53568736463be90254504a60a07543f6d1d14148808940519e
- d5e2868d0eaab6056d49a9f2a35842e0d2390e84beed0e352ed3cb19f3dc380e
- d8619ab7066af14878548719f8737ec110df19badbdd3d6394a941127c268d19
- d9ea9d94359fa3e8edda3e1e659925f25e7003a8254b52229800220b67b651bb
- df0b5d6ca7ba81e22d98e1f4dafe4d222ce496c31299e4189d8d773d9b70d6ec
- df30ccce6ec03c03e2e1ca041200267cd3b708946cc2f18577dfee7ea351272c
- e0d78b3a64c0d256d4be7c2b959fb8ce49950bd2abb975aa35b6421d1be6e9e9
- e1a2490b48fe59d053f5d486af00f72b2973d71ea87496c8158cd60e72f9b386
- e48d5ea33faf98eb5264896ad8fdc72cb53998282c871edd189a615096c3ec56
- e624144b6c38455eb528fa2fdb1631b822608bde5eacbec097a18ef3e54c40b7
- e6c21816d712973a1e6b615164ed475dc58694afb88c69ec61c81bba7daa1297
- e7bcd48b2948a278876343900aa3ee30cab266e6fa26c3031eee5dd846983ce2
- ea6cecdaef1dde96281060a27ba65beb4079c04313697f60073be1196af7ecc6
- ebac2e585e43af2737f6bdf291b93e88dfddb64efc97ed5c514afd2848814515
- ec1f379b1032fc9f8acb9785d83978e3197dda7a3ab42ff697529c8cb7dfa579
- ec56f0a98216810fe2706d04c9c7350e3e125b3e3207ccde0442f91fb8804921
- ee1bc25f45c431fce214dc0f0838fa8969142296a20c3887282750521ee41518
- ee29459f34c2d80b939ee41268e4c7f09eb639b2f4b97346ef10722d999323ec
- eeb4caedbe98e144bf7e30165f9c4e16525b964927af3dda94616abe18d0c476
- ef25d0b852fc83e6843c0ad7e081cbcc4541a4a0713f81a8261375f451585f6b
- f02094836adc271479734dfd5326a74f79a7545b679df03e03e339cd5db0c116
- f3ba5d0b27ff406dcd1c624aee919f394d231b878f040ec23e36c7f0cf81df99
- f77ff256c9e359a4d6fb7dc28aebaef987c919c54b001494e1624df09b73fb26
- f78bfa34d031119443d2e4fac2c291cd2e16fe932cec448cd88b8f8592aa76d5
- f7b5c622fd5f295615df5af2ad883f5946ad2f72002c4c3be1a9ad0df7c2b2e5
- fb82d8338af07adaa5d46c372e5597015ccfb0f6e48dd9dbfceb282d5e8781b7
- fd56107c80cef6e7b7493d01175d6801ba28c0393c4f36f440bc97c8cf5f0e3d

CnC domains

- 30miles[.]xyz

- antivarevare[.]club
- antivarevare[.]pw
- bavadivaclub[.]club
- beradocolon[.]top
- bluekit[.]pw
- bonwes[.]bid
- bredretre[.]uno
- carztesla[.]xyz
- chumocarz[.]club
- citytrallbus[.]xyz
- colocarantino[.]xyz
- cosacasa[.]top
- costacolonel[.]club
- costamustero[.]pw
- coucarachiz[.]top
- cozyappt[.]club
- crossbones[.]email
- cryptocrio[.]pw
- cryptocrio[.]top
- cucumberz99[.]club
- dayafterthe[.]xyz
- dezisenkor[.]club
- docccutime[.]xyz
- emergencytoolz[.]pw
- extraordinarycurc[.]club
- fekilopol[.]xyz
- fidelliware[.]pw
- filacolonel[.]site
- filteroggy[.]pw
- fishmak[.]pw
- flighfinder[.]xyz
- flightslots[.]online
- forwardnogi[.]pw
- fullplainefares[.]club
- gerenada[.]club
- glassyradua[.]xyz
- goodservers[.]top
- herekeder[.]best
- instarobotics[.]club
- loacorecoder[.]club
- menosmeno[.]best
- millogorillo[.]top
- nadalia[.]top
- northdestrickt[.]top
- oggytarakan[.]club
- oggythecoucca[.]xyz
- polymorphis[.]top
- pravizzillo[.]club
- pravizzillo[.]email
- presserdresser[.]best
- pythonfinder[.]top
- safebanktest[.]top
- seguridadcolonel[.]club
- sharedocar[.]xyz
- smallhole[.]club
- svaerossi[.]pw

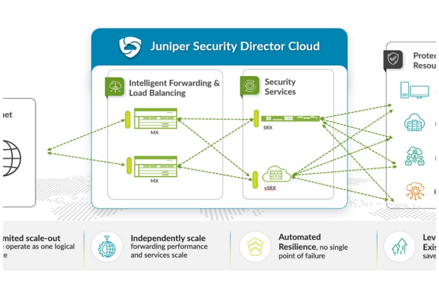
- tourdayly[.]top
- trythisone2[.]best
- uxozhuki[.]pw
- vereseptem[.]pw
- withoutemblems[.]top

References

- https://www.group-ib.com/blog/icedid
- https://securityintelligence.com/posts/breaking-the-ice-a-deep-dive-into-the-icedid-banking-trojans-new-major-version-release/
- https://isc.sans.edu/forums/diary/Microsoft+Word+document+with+malicious+macro+pushes+IcedID+Bokbot/26146/
- https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-one

Share

Related posts



Juniper Security Director Cloud
Intelligent Forwarding & Load Balancing
Security Services
MX
SRX
vSRX
Protec
Resou
imited scale-out
operate as one logical
Independently scale forwarding performance and services scale
Automated Resilience, no single point of failure

Juniper Networks Evolves Modern Data Ce... Architectur

October 18, 2023

Shishir

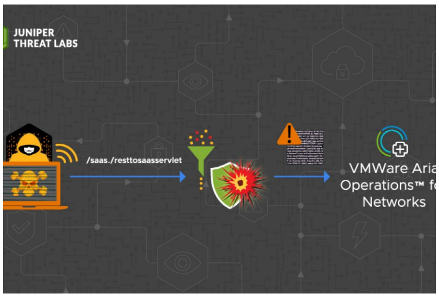
by Singh

Juniper Networks Achieves AWS Security Competency
aws
PARTNER
Security Software Competency

Juniper Networks Achieves AWS Security Competency

September 26, 2023

by Candie Mitchell



CVE-2023-20887: VMware Aria Operatio... Code Executio

September 20, 2023

by Ashish Joshi

Search

Search Blogs

Subscribe to blogs

Categories

All

Ask Juniper

Corporate Social Responsibility

Driven by Experience

- Engineering Simplicity
- Enterprise Cloud and Transformation
- Industry Solutions and Trends
- Security
- Security Incident Response
- Service Provider Transformation
- Threat Research

Global Blogs

- Dutch – Blog
- French – Blog technique
- German – Blogbeiträge
- Italian- Blog
- Japanese - ⍰⍰⍰⍰⍰⍰⍰⍰⍰)
- Korean - ⍰⍰ ⍰⍰⍰
- Portuguese - Blog de tecnologia
- Russian - Технический блог
- Simplified Chinese - ⍰⍰⍰⍰
- Spanish – Blog de tecnología
- UK – Tech Blog