IcedID Banking Trojan returns with new TTPS – Detection & Response

socinvestigation.com/icedid-banking-trojan-returns-with-new-ttps-detection-response/

June 24, 2022

IOC

By

BalaGanesh
-

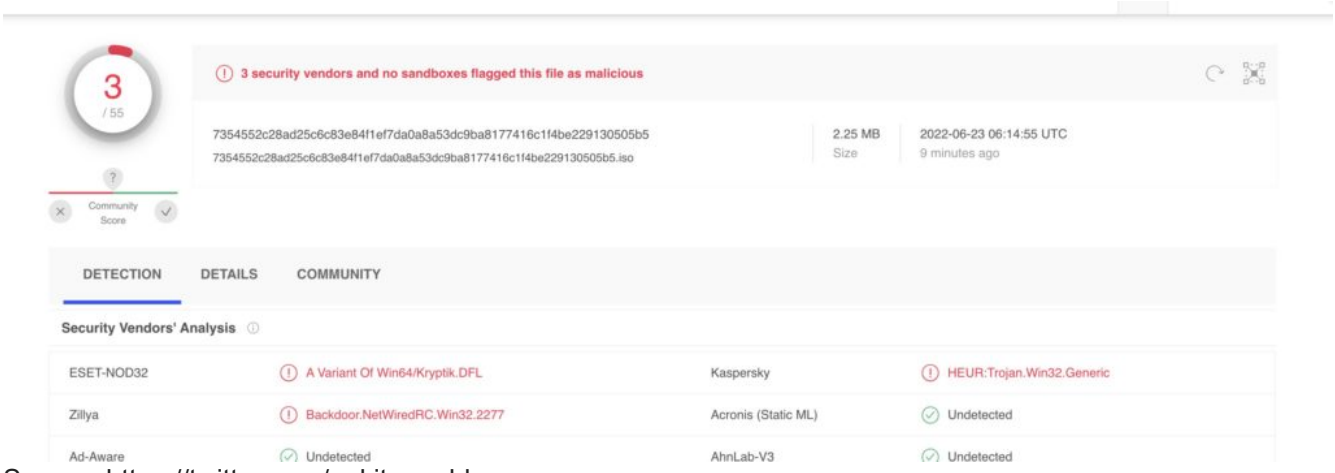
June 24, 2022
0

Malware researchers have noticed that the ever-evolving banking trojan IcedID is back again with a phishing campaign. In this campaign, malware abuses **Google cloud** and **Google firebase** to deliver phishing links.

Security researcher **ankit_anubhav** has observed the malware sample. Phishing email with an email body containing “Please find document links” and the researcher says Pressing the “download” button loads another google link (firebase) to download the actual zip, which contains an iso to launch payload.

> Please find documents link:
>
> https://storage.googleapis.com/rj66f513.appspot.com/o/Bx9PomC.htm
>
> Please let me know if you received the document.
>
> Kind regards,

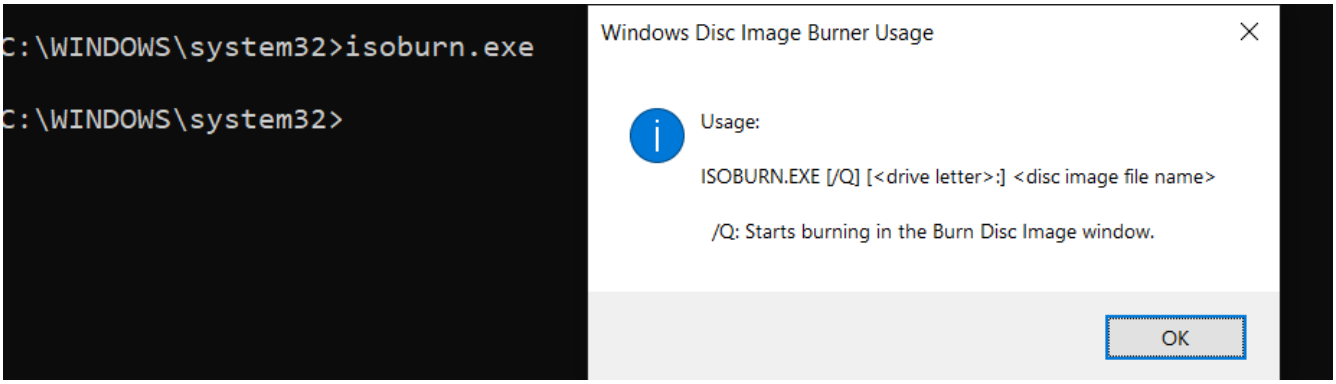
Source: https://twitter.com/ankit_anubhav



Source: https://twitter.com/ankit_anubhav

The use of ISO files allows the threat actor to bypass the **Mark-of-the-Web** controls, resulting in the execution of the malware without warning to the user.

Once zip files are executed, Malware creates a new shell `"C:\Windows\system32\cmd.exe"` and executes the command `cmd /c "C:\Users\Admin\AppData\Local\Temp\document 2.iso"`. Windows default disc burner "isoburn.exe" is utilized "C:\Windows\System32\isoburn.exe" "C:\Users\Admin\AppData\Local\Temp\document 2.iso" to execute these ISO files.



The infected machine downloads a new file in the directory `"C:\Users\Admin\Downloads\PowerISO8.exe"` and some DLLs are installed using Regsvr32 utility.

- C:\Windows\SysWOW64\regsvr32.exe

```
regsvr32.exe /s /u "C:\Program Files (x86)\PowerISO\PWRISOSH.DLL"
```

- C:\Program Files (x86)\PowerISO\setup64.exe

```
"C:\Program Files (x86)\PowerISO\setup64.exe" cp C:\Users\Admin\AppData\Local\Temp\
nszB61B.tmp "C:\Windows\system32\Drivers\scdemu.sys"
```

But the attacker has already executed the ISO with windows default disk burner, this PowerIS08.exe download activity looks something suspicious like threat actors want a backup of alternate ISO software to execute malicious files.

Infected machines connect with C2 bredofenction[.]com and use a man-in-the-browser attack to steal financial information, including login credentials for online banking sessions.

Indicator of compromise:

File:
https://www.virustotal.com/gui/file/7354552c28ad25c6c83e84f1ef7da0a8a53dc9ba8177416c1f4be229130505b5

Stage 1 html https://storage.googleapis[.]com/rj66f513.appspot.com/o/Bx9PomC.htm#

Stag 2 link https[:]//firebasestorage.googleapis[.]com/v0/b/causal-tracker-354112.appspot.com/o/q4DLC3Kw3k%2Fdocument.zip?alt=media&token=70ade0dd-fc8b-4044-bf3b-f9912d9c9bfe

C2s

bredofenction[.]com

aniogarphianeo[.]com

carbrownleger[.]com

Intel source: **ankit_anubhav** / **Mikhail Kasimov**

Detection & Response:

Qradar:

```
SELECT UTF8(payload) from events where LOGSOURCETYPENAME(devicetype)='Microsoft Windows Security
Event Log' and (("Process CommandLine" ilike '%cmd /c%' and "Process CommandLine" ilike
'%\AppData\Local\%' and "Process CommandLine" ilike '%.iso%' and "Process CommandLine" ilike
'%C:\Users\%' and (("Image" ilike '%\cmd.exe') or "Image" ilike '%\isoburn.exe')) or ("Image" ilike
'%\regsvr32.exe' and "Process CommandLine" ilike '%/s%' and "Process CommandLine" ilike '%C:\Program
Files%' and "Process CommandLine" ilike '%PowerISO%') or "Image" ilike '%PowerISO8.exe')
```

Splunk:

```
((CommandLine="*cmd /c*" AND CommandLine="*\\AppData\\Local\\*" AND CommandLine="*.iso*" AND
CommandLine="*C:\\Users\\*" AND ((Image="*\\cmd.exe") OR Image="*\\isoburn.exe")) OR
(Image="*\\regsvr32.exe" AND CommandLine="*/s*" AND CommandLine="*C:\\Program Files*" AND
CommandLine="*PowerISO*") OR Image="*PowerISO8.exe") AND source="WinEventLog:*"
```

ElasticQuery:

```
((process.command_line:*cmd\ \/c* AND process.command_line:*\\AppData\\Local\\* AND
process.command_line:*.iso* AND process.command_line:*C\:\\Users\\* AND
(process.executable:*\\cmd.exe OR process.executable:*\\isoburn.exe)) OR
(process.executable:*\\regsvr32.exe AND process.command_line:*\/s* AND
process.command_line:*C\:\\Program\ Files* AND process.command_line:*PowerISO*) OR
process.executable:*PowerISO8.exe)
```

Crowstike:

```
((((ImageFileName="*\\cmd.exe") AND (CommandLine="*cmd /c*" OR CommandHistory="*cmd /c*") AND
(CommandLine="*\\AppData\\Local\\*" OR CommandHistory="*\\AppData\\Local\\*") AND
(CommandLine="*.iso*" OR CommandHistory="*.iso*") AND (CommandLine="*C:\\Users\\*" OR
CommandHistory="*C:\\Users\\*")) OR (ImageFileName="*\\isoburn.exe" AND (CommandLine="*cmd /c*" OR
CommandHistory="*cmd /c*") AND (CommandLine="*\\AppData\\Local\\*" OR
CommandHistory="*\\AppData\\Local\\*") AND (CommandLine="*.iso*" OR CommandHistory="*.iso*") AND
(CommandLine="*C:\\Users\\*" OR CommandHistory="*C:\\Users\\*"))) OR
(ImageFileName="*\\regsvr32.exe" AND (CommandLine="*/s*" OR CommandHistory="*/s*") AND
(CommandLine="*C:\\Program Files*" OR CommandHistory="*C:\\Program Files*") AND
(CommandLine="*PowerISO*" OR CommandHistory="*PowerISO*")) OR ImageFileName="*PowerISO8.exe")
```

FireEye:

```
(metaclass:`windows` ((args:`cmd /c` args:`\AppData\Local\\` args:`.iso` args:`C:\Users\\`
(process:`*\cmd.exe` OR process:`*\isoburn.exe`)) OR (process:`*\regsvr32.exe` args:`/s`
args:`C:\Program Files` args:`PowerISO`) OR process:`*PowerISO8.exe`))
```

GrayLog:

```
((CommandLine.keyword:*cmd\ \/c* AND CommandLine.keyword:*\\AppData\\Local\\* AND
CommandLine.keyword:*.iso* AND CommandLine.keyword:*C\:\\Users\\* AND (Image.keyword:*\\cmd.exe OR
Image.keyword:*\\isoburn.exe)) OR (Image.keyword:*\\regsvr32.exe AND CommandLine.keyword:*\/s* AND
CommandLine.keyword:*C\:\\Program\ Files* AND CommandLine.keyword:*PowerISO*) OR
Image.keyword:*PowerISO8.exe)
```

Logpoint:

```
((CommandLine="*cmd /c*" CommandLine="*\\AppData\\Local\\*" CommandLine="*.iso*"
CommandLine="*C:\\Users\\*" (Image IN "*\\cmd.exe" OR Image="*\\isoburn.exe")) OR
(Image="*\\regsvr32.exe" CommandLine="*/s*" CommandLine="*C:\\Program Files*"
CommandLine="*PowerISO*") OR Image="*PowerISO8.exe")
```

Microsoft Defender:

```
DeviceProcessEvents | where ((ProcessCommandLine contains "cmd /c" and ProcessCommandLine contains @"\AppData\Local\" and ProcessCommandLine contains ".iso" and ProcessCommandLine contains @"C:\Users\" and ((FolderPath endswith @"\cmd.exe") or FolderPath endswith @"\isoburn.exe")) or (FolderPath endswith @"\regsvr32.exe" and ProcessCommandLine contains "/s" and ProcessCommandLine contains @"C:\Program Files" and ProcessCommandLine contains "PowerISO") or FolderPath endswith "PowerISO8.exe")
```

Microsoft Sentinel:

```
SecurityEvent |  where EventID == 4688 | where ((CommandLine contains 'cmd /c' and CommandLine contains @'\AppData\Local\' and CommandLine contains '.iso' and CommandLine contains @'C:\Users\' and ((NewProcessName endswith @'\cmd.exe') or NewProcessName endswith @'\isoburn.exe')) or (NewProcessName endswith @'\regsvr32.exe' and CommandLine contains '/s' and CommandLine contains @'C:\Program Files' and CommandLine contains 'PowerISO') or NewProcessName endswith 'PowerISO8.exe')
```

Google Chronicle:

```
((target.process.command_line = /.*cmd \/c.*/ and target.process.command_line = /.*\\AppData\\Local.*/ and target.process.command_line = /.*\.iso.*/ and target.process.command_line = /.*C:\\Users.*/ and (target.process.file.full_path = /.*\\cmd\.exe/ or target.process.file.full_path = /.*\\isoburn\.exe/)) or (target.process.file.full_path = /.*\\regsvr32\.exe/ and target.process.command_line = /.*\/s.*/ and target.process.command_line = /.*C:\\Program Files.*/ and target.process.command_line = /.*PowerISO.*/) or target.process.file.full_path = /.*PowerISO8\.exe/)
```

RSA Netwitness:

```
(((CommandLine contains 'cmd /c') && (CommandLine contains 'AppData\Local\\') && (CommandLine contains '.iso') && (CommandLine contains 'C:\Users\\') && ((Image contains '\cmd\.exe') || (Image contains 'isoburn.exe'))) || ((Image contains 'regsvr32.exe') && (CommandLine contains '/s') && (CommandLine contains 'C:\Program Files') && (CommandLine contains 'PowerISO')) || (Image contains 'PowerISO8.exe'))
```

Sumologic:

```
(_sourceCategory=*windows* AND (((CommandLine="*cmd /c*" AND CommandLine="*\AppData\Local\\*" AND CommandLine="*.iso*" AND CommandLine="*C:\Users\\*" AND (((Image = "*\cmd.exe") OR Image="*\isoburn.exe"))) OR (Image="*\regsvr32.exe" AND CommandLine="*/s*" AND CommandLine="*C:\Program Files*" AND CommandLine="*PowerISO*") OR Image="*PowerISO8.exe")))
```

CarbonBlack:

```
((process_cmdline:*cmd\ \/c* AND process_cmdline:*\\AppData\\Local\\* AND process_cmdline:*.iso* AND process_cmdline:*C\:\\Users\\* AND (process_name:*\\cmd.exe OR process_name:*\\isoburn.exe)) OR (process_name:*\\regsvr32.exe AND process_cmdline:*\/s* AND process_cmdline:*C\:\\Program\ Files* AND process_cmdline:*PowerISO*) OR process_name:*PowerISO8.exe)
```

Aws Opensearch:

```
((process.command_line:*cmd\ \/c* AND process.command_line:*\\AppData\\Local\\* AND process.command_line:*.iso* AND process.command_line:*C\:\\Users\\* AND
```

```
(process.executable:*\\cmd.exe OR process.executable:*\\isoburn.exe)) OR
(process.executable:*\\regsvr32.exe AND process.command_line:*\/s* AND
process.command_line:*C\:\\Program\ Files* AND process.command_line:*PowerISO*) OR
process.executable:*PowerISO8.exe)
```

Arcsight:

```
(((((((deviceProcessName CONTAINS "*\\cmd.exe" OR destinationProcessName CONTAINS "*\\cmd.exe" OR
sourceProcessName CONTAINS "*\\cmd.exe")) AND (((deviceCustomString1 CONTAINS "*cmd /c*" OR
destinationServiceName CONTAINS "*cmd /c*")) AND ((deviceCustomString1 CONTAINS
"*\\AppData\\Local\\\\*" OR destinationServiceName CONTAINS "*\\AppData\\Local\\\\*")) AND
((deviceCustomString1 CONTAINS "*.iso*" OR destinationServiceName CONTAINS "*.iso*")) AND
((deviceCustomString1 CONTAINS "*C:\\Users\\\\*" OR destinationServiceName CONTAINS
"*C:\\Users\\\\*")))) OR (((deviceProcessName ENDSWITH "*\\isoburn.exe" OR destinationProcessName
ENDSWITH "*\\isoburn.exe" OR sourceProcessName ENDSWITH "*\\isoburn.exe")) AND
(((deviceCustomString1 CONTAINS "*cmd /c*" OR destinationServiceName CONTAINS "*cmd /c*")) AND
((deviceCustomString1 CONTAINS "*\\AppData\\Local\\\\*" OR destinationServiceName CONTAINS
"*\\AppData\\Local\\\\*")) AND ((deviceCustomString1 CONTAINS "*.iso*" OR destinationServiceName
CONTAINS "*.iso*")) AND ((deviceCustomString1 CONTAINS "*C:\\Users\\\\*" OR destinationServiceName
CONTAINS "*C:\\Users\\\\*")))))) OR (((deviceProcessName ENDSWITH "*\\regsvr32.exe" OR
destinationProcessName ENDSWITH "*\\regsvr32.exe" OR sourceProcessName ENDSWITH "*\\regsvr32.exe"))
AND (((deviceCustomString1 CONTAINS "*/s*" OR destinationServiceName CONTAINS "*/s*")) AND
((deviceCustomString1 CONTAINS "*C:\\Program Files*" OR destinationServiceName CONTAINS
"*C:\\Program Files*")) AND ((deviceCustomString1 CONTAINS "*PowerISO*" OR destinationServiceName
CONTAINS "*PowerISO*")))) OR deviceProcessName ENDSWITH "*PowerISO8.exe" OR destinationProcessName
ENDSWITH "*PowerISO8.exe" OR sourceProcessName ENDSWITH "*PowerISO8.exe"))
```

LEAVE A REPLY

Please enter your comment!

Please enter your name here

You have entered an incorrect email address!

Please enter your email address here