# IcedID Banking Trojan returns with new TTPS – Detection & Response - Security Investigation

By BalaGanesh

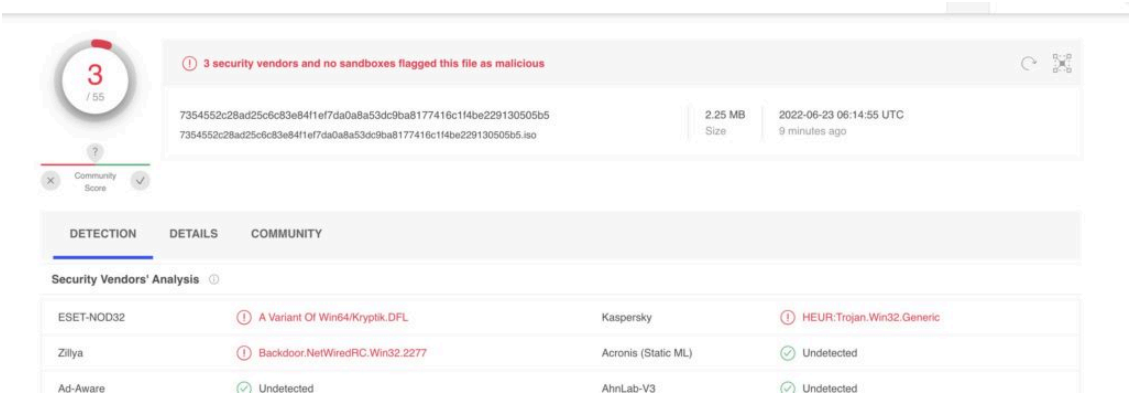
Published: 2022-06-24 · Archived: 2026-04-05 16:13:53 UTC


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,

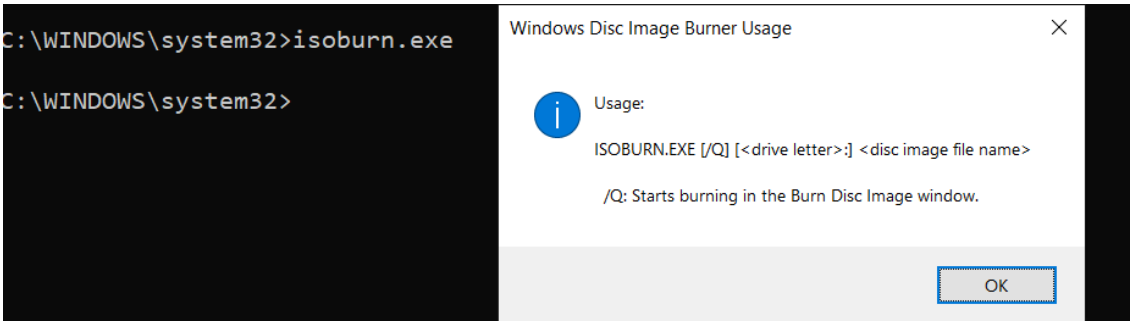
Source: https://twitter.com/ankit_anubhav



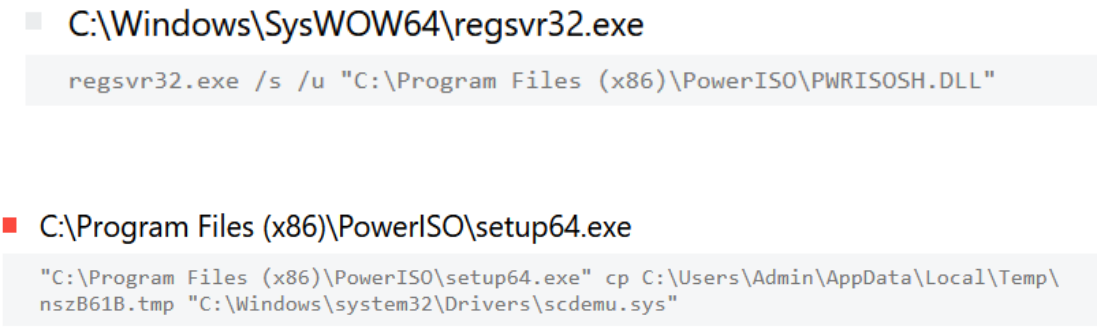

Source: https://twitter.com/ankit_anubhav

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.




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
Splunk:


 ((CommandLine="*cmd /c*" AND CommandLine="*\\AppData\\Local\\*" AND CommandLine="*.iso*" AND CommandLine="*C:\
ElasticQuery:


 ((process.command_line:*cmd\ \/c* AND process.command_line:*\\AppData\\Local\\* AND process.command_line:*.iso
Crowstike:


 ((((ImageFileName="*\\cmd.exe") AND (CommandLine="*cmd /c*" OR CommandHistory="*cmd /c*") AND (CommandLine="*\
FireEye:
```

```
 (metaclass:`windows` ((args:`cmd /c` args:`\AppData\Local\\` args:`.iso` args:`C:\Users\\` (process:`*\cmd.exe`
```

GrayLog:

```
 ((CommandLine.keyword:*cmd\ \/c* AND CommandLine.keyword:*\\AppData\\Local\\* AND CommandLine.keyword:*.iso* AN
```

Logpoint:

```
 ((CommandLine="*cmd /c*" CommandLine="*\\AppData\\Local\\*" CommandLine="*.iso*" CommandLine="*C:\\Users\\*" (
```

Microsoft Defender:

```
 DeviceProcessEvents | where ((ProcessCommandLine contains "cmd /c" and ProcessCommandLine contains @"\AppData\L
```

Microsoft Sentinel:

```
 SecurityEvent |  where EventID == 4688 | where ((CommandLine contains 'cmd /c' and CommandLine contains @'\AppL
```

Google Chronicle:

```
 ((target.process.command_line = /.*cmd \/c.*/ and target.process.command_line = /.*\\AppData\\Local.*/ and targ
```

RSA Netwitness:

```
 (((CommandLine contains 'cmd /c') && (CommandLine contains 'AppData\Local\\') && (CommandLine contains '.iso')
```

Sumologic:

```
 (_sourceCategory=*windows* AND (((CommandLine="*cmd /c*" AND CommandLine="*\AppData\Local\\*" AND CommandLine="
```

CarbonBlack:

```
 ((process_cmdline:*cmd\ \/c* AND process_cmdline:*\\AppData\\Local\\* AND process_cmdline:*.iso* AND process_cr
```

Aws Opensearch:

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

Arcsight:

```
(((((((deviceProcessName CONTAINS "*\\cmd.exe" OR destinationProcessName CONTAINS "*\\cmd.exe" OR sourceProcess
```

---

Source: https://www.socinvestigation.com/icedid-banking-trojan-returns-with-new-ttps-detection-response/