2022-09-23 (FRIDAY) - ICEDID (BOKBOT) INFECTION WITH COBALT STRIKE

NOTES:

- Zip files are password-protected. If you don't know the password, see the "about" page of this website.

ASSOCIATED FILES:

- **2022-09-23-IOCs-for-IcedID-and-Cobalt-Strike.txt.zip** 2.0 kB (2,046 bytes)
- **2022-09-23-IcedID-infection-with-Cobalt-Strike.pcap.zip** 4.0 MB (3,990,992 bytes)
- **2022-09-23-IcedID-malware-and-artifacts.zip** 2.3 MB (2,315,310 bytes)

```
2022-09-23 (FRIDAY) - ICEDID (BOKBOT) INFECTION WITH COBALT STRIKE

INFECTION CHAIN:

email --> zip --> ISO --> files for IcedID --> HTTP traffic for gzip binary --> IcedID C2 traffic --> Cobalt Strike

NOTES:

- The zip attachment was retrieved through VirusTotal, and I do not have a copy of the email it came from.

ZIP ATTACHMENT AND EXTRACTED ISO IMAGE:

- SHA256 hash: 13822a4691c0ad279068a67fe20c2f51f01a039c87da694134edc1e68183db02
- File size: 268,464 bytes
- File name: document_09-22_invoice_7328_unpaid.zip
- File description: password-protected zip archive
- Password: 0922

- SHA256 hash: e2963ba47d2e07a98eafbd2ef56ffc6ae0e0c483e5e8e1fb1f24f8516abd246a
- File size: 753,664 bytes
- File name: document_09-22_invoice_7328_unpaid.iso
- File description: ISO image extracted from the above zip archive

CONTENTS OF ISO IMAGE USED FOR THE INFECTION:

- SHA256 hash: b786df690a4b21d95767cad695948330c60bb22fd521175c8a07a6f793b35a1e
- File size: 1,229 bytes
- File name: document.lnk
- File description: Windows shortcut that runs script file

- SHA256 hash: b42b11426614f7c16faa7088b53ffa73fd1a6af51f5253970920393629d8088a
- File size: 211 bytes
- File name: scabs\formingGuying.js
- File description: script file run by the above Windows shortcut

- SHA256 hash: 9764eb9519b6790dbc58e8d8e75acf83a2b46a711a983c8cf1599ed9a0010db0
- File size: 61 bytes
- File name: scabs\gloatingChambermaids.cmd
- File description: batch command file run by the above script

- SHA256 hash: 771449df7202c64ee3c03224829ab93851f52818ec028632a2ef75b35425c5fe
- File size: 325,120 bytes
- File name: scabs\rarest.db
- File description: 64-bit DLL installer for IcedID
- Run method: rundll32.exe [filename],#1

FILES FROM THE INFECTION:

- SHA256 hash: 0fd654199d8030eba8d8d55618c096155974e3897c176c5434c75eb1d55d1754
- File size: 678,971 bytes
- File description: gzip binary from trallfasterinf.com used to create license.dat and persistent IcedID DLL

- SHA256 hash: 55be890947d021fcc8c29af3c7aaf70d8132f222e944719c43a6e819e84a8f8b
- File size: 363,338 bytes
- File location: C:\Users\[username]\AppData\Roaming\SingDinner\license.dat
- File description: data binary used to run persistent DLL for IcedID

- SHA256 hash: 37ef80062837ca9a6fe9cafa74e6df25efda161112da393b470a9056534c03c4
- File size: 314,880 bytes
- File location: C:\Users\[username]\AppData\Local\[username]\{1CAD7EB1-C42E-9422-A23B-CC72B20910C3}\axoxyidk.dll
- File description: 64-bit persistent DLL for IcedID
- Run method: rundll32.exe [filename],#1 --id="[path to license.dat]"

TRAFFIC FROM THE INFECTION:
```

```
INSTALLER RETRIEVES GZIP BINARY:

- 137.184.114.20 port 80 - trallfasterinf.com - GET / HTTP/1.1

ICEDID C2 TRAFFIC:

- 64.227.116.208 port 443 - algerat.cyou - HTTPS traffic
- 5.252.177.10 port 443 - considerf.info - HTTPS traffic

SELF-SIGNED CERTIFICATE ISSUER DATA FROM BOTH SERVERS FOR ICEDID C2 HTTPS TRAFFIC:

- id-at-commonName=localhost
- id-at-countryName=AU
- id-at-stateOrProvinceName=Some-State
- id-at-organizationName=Internet Widgits Pty Ltd

COBALT STRIKE TRAFFIC:

- 78.128.112.139 port 443 - HTTPS traffic

SELF-SIGNED CERTIFICATE ISSUER DATA FROM SERVER FOR COBALT STRIKE HTTPS TRAFFIC:

- id-at-countryName=
- id-at-stateOrProvinceName=
- id-at-localityName=
- id-at-organizationName=
- id-at-organizationUnitName=
- id-at-commonName=

AD ENUMERATION TOOL FOUND ON INFECTED WINDOWS HOST:

- SHA256 hash: fc4da07183de876a2b8ed1b35ec1e2657400da9d99a313452162399c519dbfc6
- File size: 754,176 bytes
- File location: C:\Users\[username]\AppData\Local\Temp\adget.exe
- File description: 64-bit EXE command line tool to gather information about AD environment
```

Click here to return to the main page.
