**IcedlD malware**

**What is IcedlD malware?**

IcedID is a sort of malware known as a banking trojan that lets attackers use it to steal the victims' banking credentials. BokBot, also known as IcedID, primarily targets companies and steals payment information. It can also operate as a loader to spread other viruses or download extra modules.

After IcedID's first victims were attacked in the autumn of 2017, researchers first discovered the malware. Further study revealed that IcedID is a modular malware with highly sophisticated features. Also, it was first noted that IcedID does not appear to contain any code that was appropriated or stolen from other trojans, which is unusual for more sophisticated malware samples like the one we are dealing with right now.

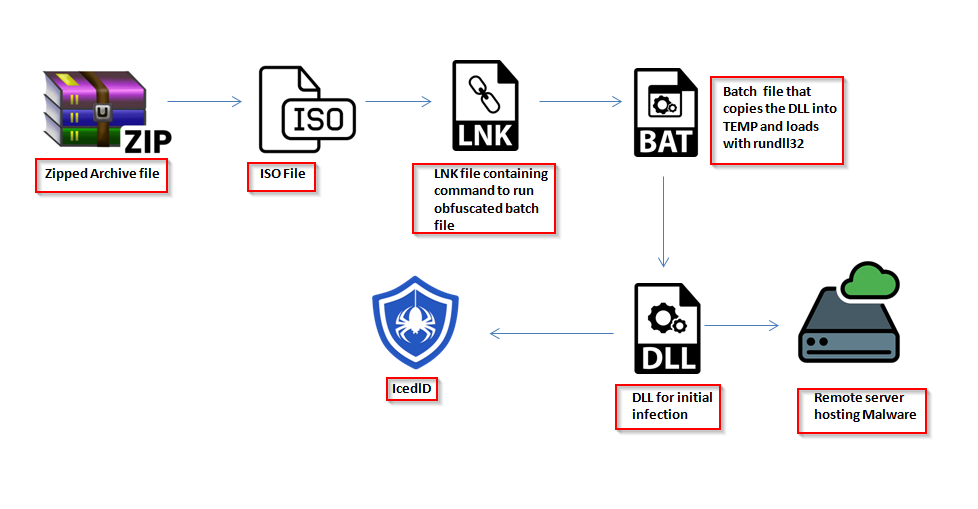
**Threat Summary**

|  |  |
| --- | --- |
| Name | IcedlD |
| Threat type | Malware |
| Static analysis | IcedID infections typically begin with the victim opening a password-protected zip file that contains an ISO file. |
| Target | IT , banking or medical sector |
| Malware type | banking Trojan |
| Delivery method | Archive Zip files |
| Impact | Data exfiltration , C2 deployment |

**Initial Access**

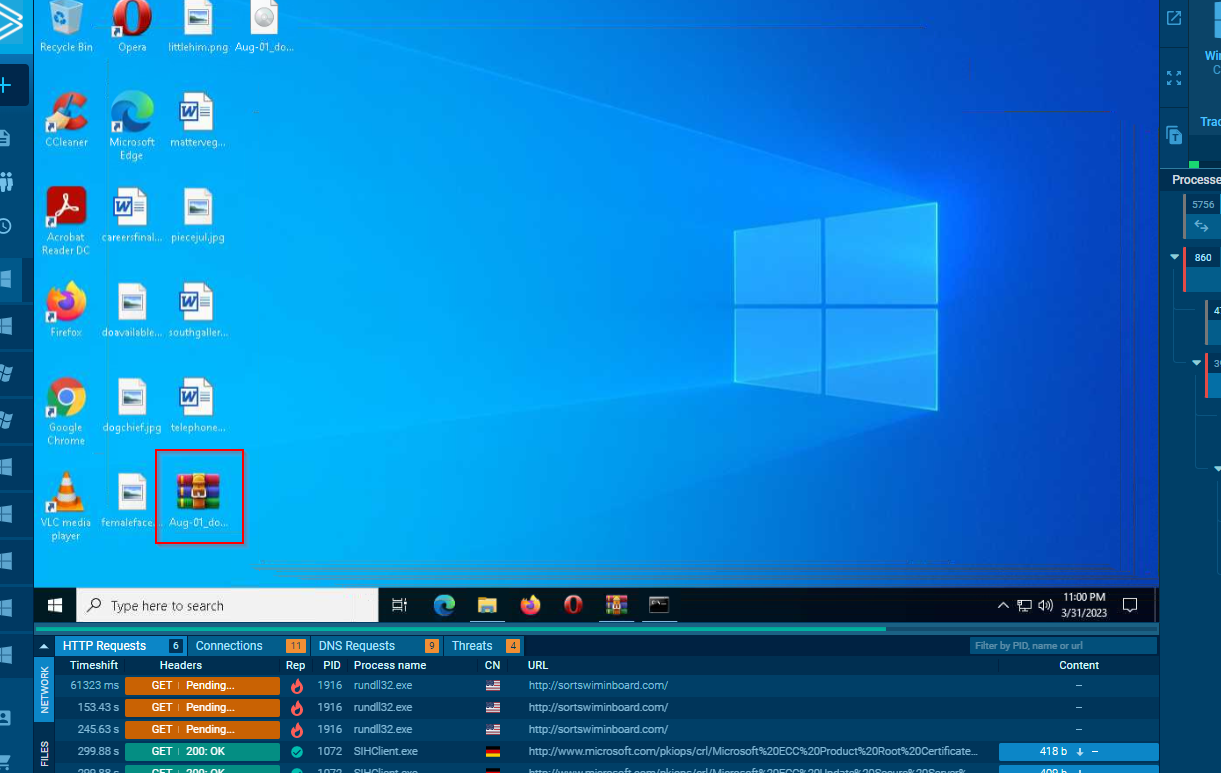
* IcedID uses a typical delivery method for banking trojans — attackers distribute it in malicious Microsoft Office documents that prompt the users to enable macros and, once it is done, activate the download of the executable to the victim's machine.
* IcedID authors use spear-phishing techniques, meaning that they learn details about their victims and use them to increase the effectiveness of their emails.

**Attack analysis**

****

**The above mention diagram, describe the deployment mechanisms observed during this case:**

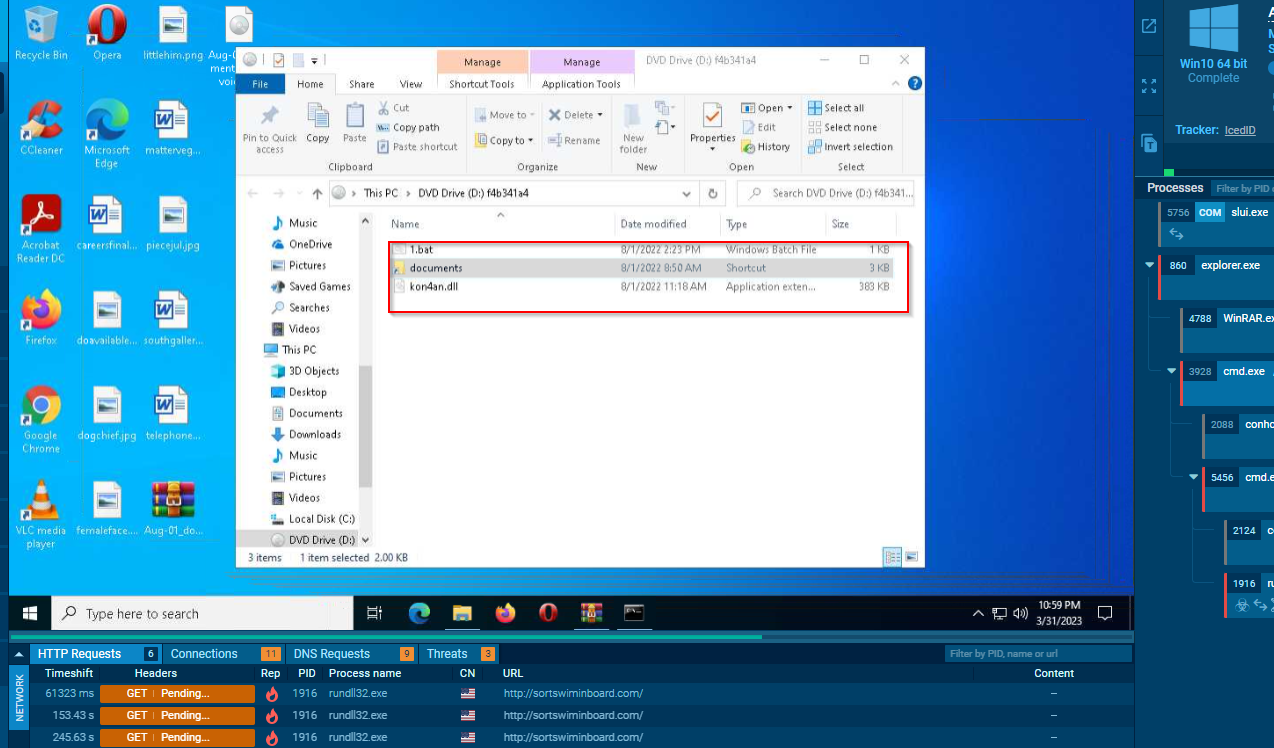
* Victim opens an archive.
* Victim clicks the ISO file, which creates a virtual disk.
* Victim navigates to the virtual disk and clicks the only file visible, which actually is an LNK file.
* LNK file runs a batch file which drops a DLL into a temporary folder and runs it with rundll32.exe.
* Rundll32.exe loads the DLL, which creates network connections to IcedID-related domains, downloading the IcedID payload.
* IcedID payload is loaded into the process.



***(Archive Zip file highlighted in Red box)***

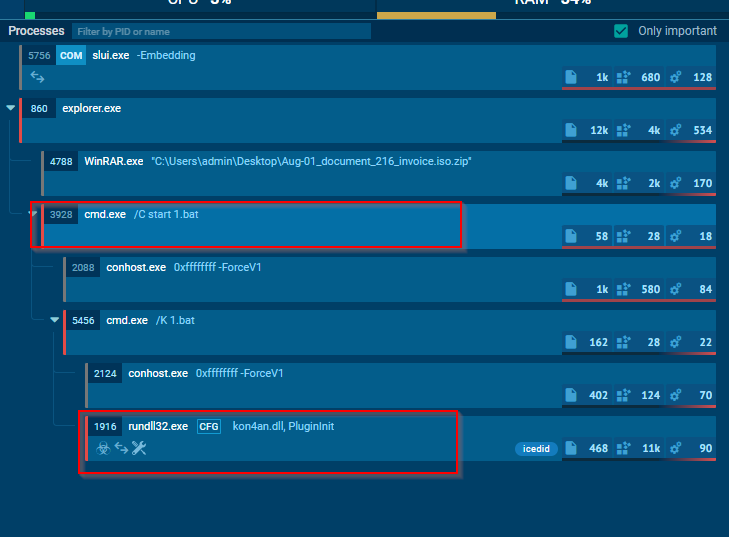
Similar IcedID infections typically begin with the victim opening a password-protected zip file that contains an ISO file.

When double-clicked, ISO files automatically mount themselves as a read-only directory. This directory contains LNK (shortcut) file.

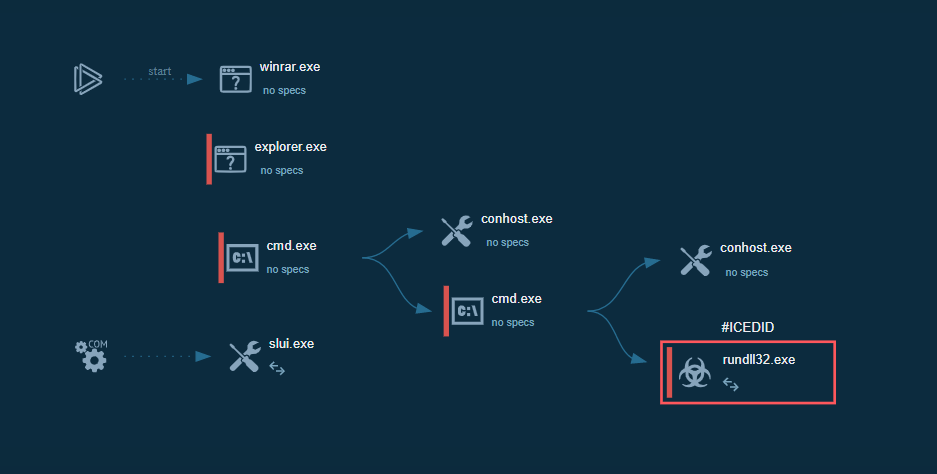


When the shortcut file is clicked, it executes the batch file in the hidden directory, through the system component cmd.exe.

This batch file spawned the rundll32.exe process to execute DLL



**Process Tree**

****

**Indicator Of Compromised (IOCs)**

**HASHES**

|  |
| --- |
||

**IP ADDRESS**

|  |
| --- |
| 207.154.202.192  138.197.195.62  209.97.134.125  104.248.153.44  159.89.43.72  159.223.109.133  134.209.170.133  94.140.114.143  134.209.107.62  137.184.94.136  94.140.114.184  164.92.104.194  103.208.86.7  5.181.80.214  204.11.56.48  23.202.231.167  80.78.24.30  23.202.231.167  79.110.52.253  192.168.100.5 |

**DOMIANS**

|  |
| --- |
| 0.pool.ntp.org  doxbin.com  zerit.top  fuyt.org  tzgl.org  kotob.top  brandyjaggers.com  tbpws.top  astdg.top  securebiz.org  frederikkempe.com  majul.com  isns.net  str-master.pw  ticket.ipv10.eu  3jkpvk2m8y.dattolocal.net  pluto.iziis.ukim.edu.mk  ritstraveapt.buzz  webmails.literhost.com  gronlundsplat.xyz |

**RECOMMENDATION**

* Phishing email protection : If possible, block or quarantine password-protected zip files in your email gateway.
* Warn your users against similar threats : Use caution when handling files that are out of the ordinary and from the internet (ex - ISO and LNK files).
* Disable disk image file auto-mounting : To avoid this infection technique to succeed, please consider disabling auto-mounting of disk image files (mainly, .iso, .img, .vhd, and .vhdx) globally through GPOs
* This can be achieved by modifying the Registry values related to the Windows Explorer file associations in order to disable the automatic Explorer "Mount and Burn" dialog for these file extensions.
* Block compromised users: Block users whose machines were involved in the attack, in order to stop or at least slow down attacker propagation over the network.
* Identify and block malicious network connections: Identify network flows toward malicious IPs or domains identified in the reports and block connections to stop the attacker from controlling the compromised machines.