IcedID, Software S0483 | MITRE ATT&CK®

Archived: 2026-04-05 16:33:06 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

IcedID can query LDAP and can use built-in `net` commands to identify additional users on the network to infect. [1][3]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

IcedID has used HTTPS in communications with C2. [2][3][4]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

IcedID has established persistence by creating a Registry run key. [1]

Enterprise T1185 Browser Session Hijacking

IcedID has used web injection attacks to redirect victims to spoofed sites designed to harvest banking and other credentials. IcedID can use a self signed TLS certificate in connection with the spoofed site and simultaneously maintains a live connection with the legitimate site to display the correct URL and certificates in the browser. [1][2]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

IcedID has used obfuscated VBA string expressions. [2]

Enterprise T1482 Domain Trust Discovery

IcedID used Nltest during initial discovery. [4][3]

Enterprise T1189 Drive-by Compromise

IcedID has cloned legitimate websites/applications to distribute the malware. [5]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

IcedID has used SSL and TLS in communications with C2. [1][2]

Enterprise T1048 .002 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

IcedID has exfiltrated collected data via HTTPS. [4]

Enterprise T1105 Ingress Tool Transfer

IcedID has the ability to download additional modules and a configuration file from C2. [1][2][3][6]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

IcedID has modified legitimate .dll files to include malicious code.[5]

Enterprise T1106 Native API

IcedID has called `ZwWriteVirtualMemory`, `ZwProtectVirtualMemory`, `ZwQueueApcThread`, and `NtResumeThread` to inject itself into a remote process.[2]

Enterprise T1135 Network Share Discovery

IcedID has used the `net view /all` command to show available shares.[3]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

IcedID has packed and encrypted its loader module.[2]

.003 Obfuscated Files or Information: Steganography

IcedID has embedded binaries within RC4 encrypted .png files.[2]

.009 Obfuscated Files or Information: Embedded Payloads

IcedID has embedded malicious functionality in a legitimate DLL file.[5]

.013 Obfuscated Files or Information: Encrypted/Encoded File

IcedID has utilzed encrypted binaries and base64 encoded strings.[2]

Enterprise T1069 Permission Groups Discovery

IcedID has the ability to identify Workgroup membership.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

IcedID has been delivered via phishing e-mails with malicious attachments.[2][4]

Enterprise T1055 .004 Process Injection: Asynchronous Procedure Call

IcedID has used `ZwQueueApcThread` to inject itself into remote processes.[1]

.012 Process Injection: Process Hollowing

IcedID can inject a Cobalt Strike beacon into cmd.exe via process hallowing.[3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

IcedID has created a scheduled task to establish persistence.[2][3][4]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

IcedID can identify AV products on an infected host using the following command: `WMIC.exe WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get * /Format:List`.[4][3]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

IcedID can inject itself into a suspended msiexec.exe process to send beacons to C2 while appearing as a normal msi application. [2] IcedID has also used msiexec.exe to deploy the IcedID loader.[5]

.011 System Binary Proxy Execution: Rundll32

IcedID has used rundll32.exe to execute the IcedID loader.[5][3]

Enterprise T1082 System Information Discovery

IcedID has the ability to identify the computer name and OS version on a compromised host.[1][3]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

IcedID used the following command to check the country/language of the active console: `cmd.exe /c chcp >&2`.[3]

Enterprise T1016 System Network Configuration Discovery

IcedID used the `ipconfig /all` command and a batch script to gather network information.[3]

Enterprise T1204 .002 User Execution: Malicious File

IcedID has been executed through Word and Excel files with malicious embedded macros and through ISO and LNK files that execute the malicious DLL.[2][3][4]

Enterprise T1497 Virtualization/Sandbox Evasion

IcedID has manipulated Keitaro Traffic Direction System to filter researcher and sandbox traffic.[5]

Enterprise T1047 Windows Management Instrumentation

IcedID has used WMI to execute binaries.[2][4]
