IcedID Malware: Traversing Through its Various Incarnations

research.loginsoft.com/threat-research/icedid-malware-traversing-through-its-various-incarnations/

May 2, 2023

May 02, 2023
By **System-41 Team**

Executive Summary

- IcedID, the notorious malware, is actively involved in several delivery campaigns, demonstrating versatility and adaptability.
- The latest IcedID variants indicate the malware's continuous evolution, and the need for robust cybersecurity measures.
- Surging use of IcedID in order to deploy ransomware makes it a significant threat to organizations worldwide.
- IcedID stays true to its roots, employing consistent Tactics, Techniques, and Procedures (TTPs) across various campaigns over the year.
- Tidal Cyber's visibility and features provide a better landscape for identifying and understanding TTPs.
- Osquery rules by Loginsoft published on Tidal Cyber's platform will bolster your organization's security posture.

Evolution & Variants

Continuously active since its initial appearance, IcedID has no periods of dormancy. Using various delivery mechanisms, and evolutionary strategies, IceID serves as an exemplary model for other malware. Widely observed in countries like the United States, United Kingdom and Canada, where the Threat Actors (TAs) not only targeted financial Institutions but also ecommerce, payment, and telecommunication industries. In recent years, these threat actors repurposed IcedID's functionality, transforming it from a banking Trojan to a ransomware detonator. As a result, many TAs added IcedID to their arsenal, while most TAs still prefer the standard variant of the malware. The standard IcedID variant propagates through emails with diverse attachments like html files, zip files, iso images and more.

In **March of 2023**, Proofpoint reported the discovery of two new variations of IcedID. Detected in November 2022 as part of the Emotet malware campaign, the first novel variant lacked certain features, making it lightweight and difficult to detect. The second new variant, observed in **February 2023**, bore a strong resemblance to the standard edition, and mainly propagated through phishing emails with OneNote attachments.

Malware Progression

ICEDID CAMPAIGN – 2021

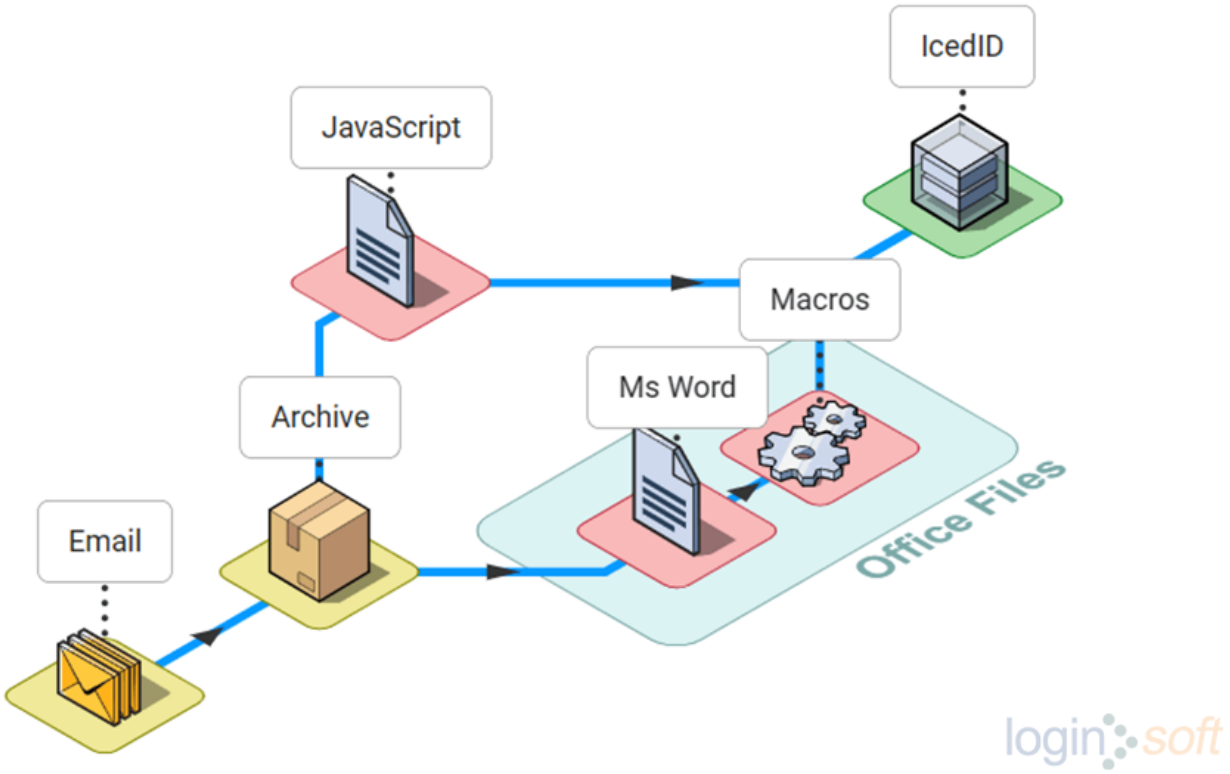

Figure: IcedID 2021 Distribution Chain

Our observations reveal that **TA551** employed several tactics to distribute malicious payloads via email, including office files with malicious macros. Another variant of this campaign used an archived JavaScript file that downloads the IcedID DLL, and masquerades with .jpg or .png extension to evade detection. The execution of the IcedID DLL, accomplished by executing Rundll32 LOLBin with an uncommon DllRegisterServer parameter, establishes communication with the attacker's command and control (C2) server.

ICEDID CAMPAIGN – 2022

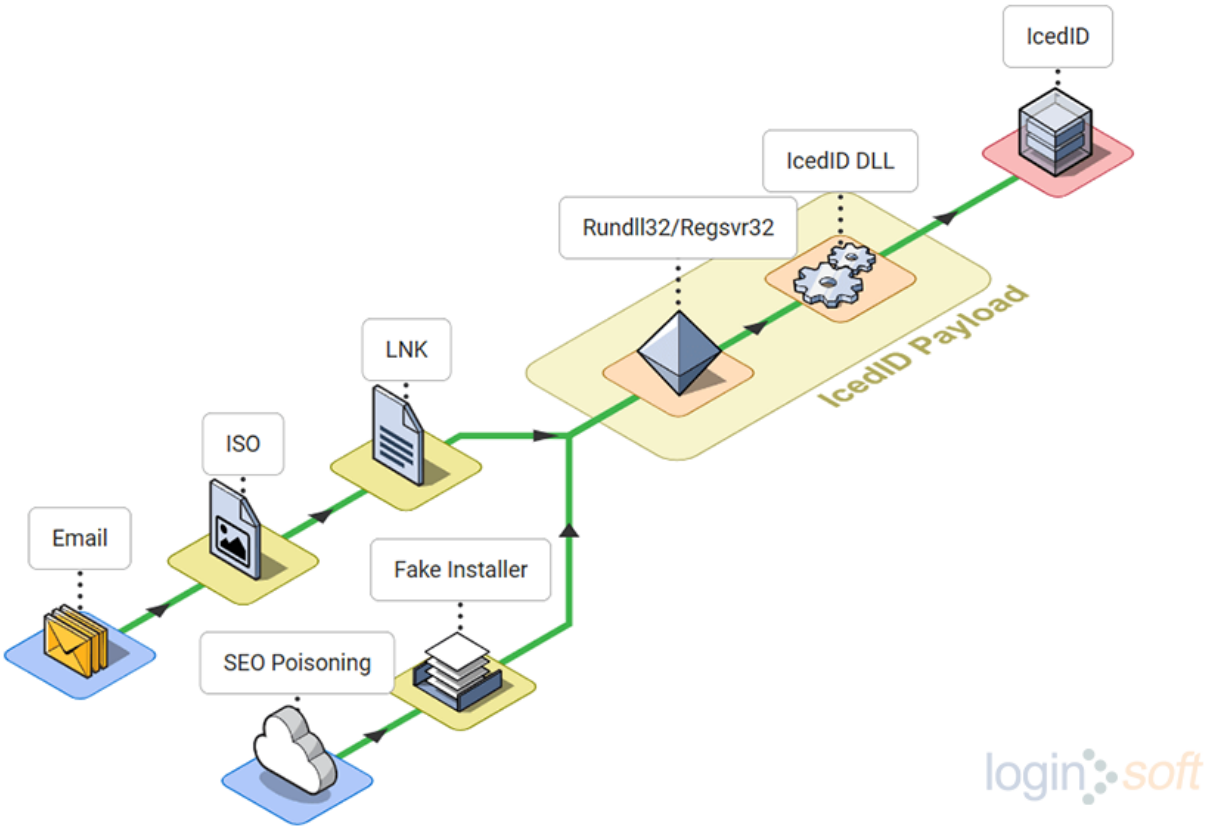

Figure: IcedID 2022 Distribution Chain

TAs began disseminating malware through ISO files sent via email. Once clicked, the shortcut file executes the IcedID payload using regsvr32 or rundll32 LOLBin, bypassing MoTW flag. Upon execution of the IcedID DLL, the malware performed discovery tasks through Windows utilities like systeminfo, ipconfig, net, and nltest. A Cobalt Strike beacon was then deployed, and hands-on-keyboard activities were observed executing AdFind to perform enumeration. IcedID obtained credentials by accessing LSASS memory, using the credentials to establish RDP connections within the network. Subsequently, the TAs initiated a ransomware attack after gaining access to the compromised network.

Additionally, in the same year, the TAs spread IcedID malware via Google Ads by creating fake software installer pages. Some variations of IcedID were also found to use Dark VNC as a backdoor.

ICEDID CAMPAIGN – 2023

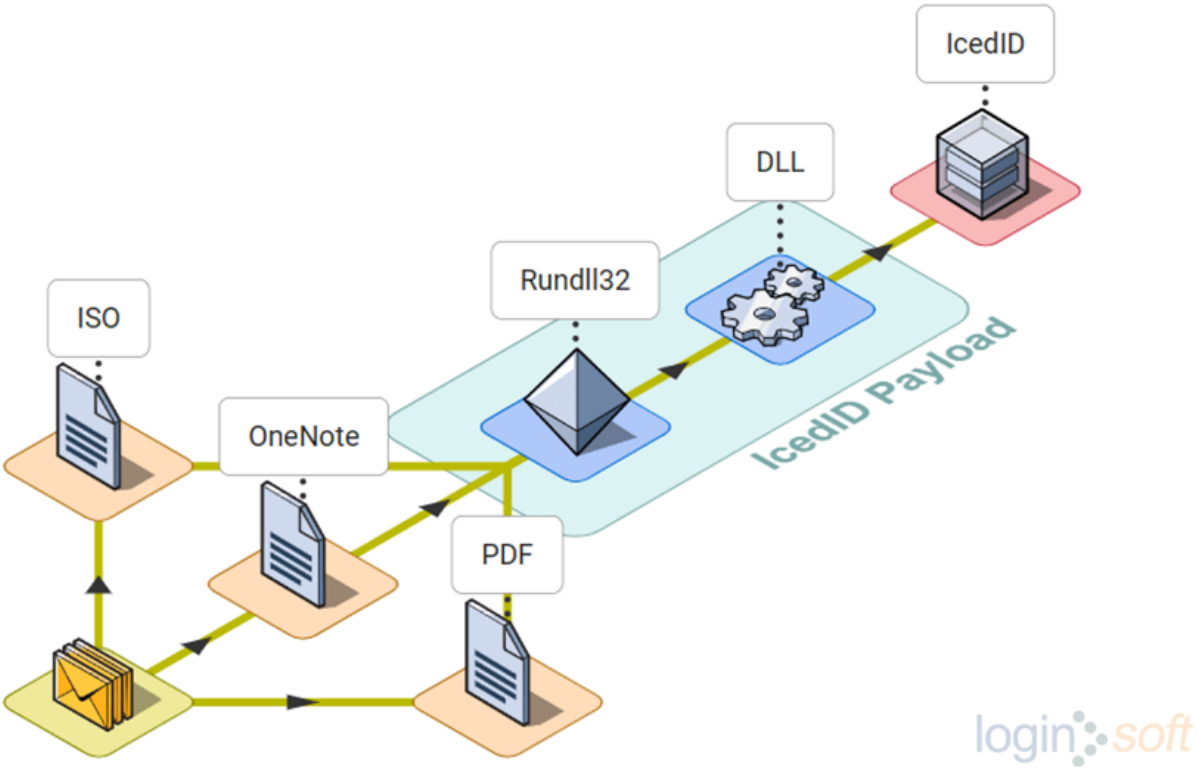

Figure: IcedID 2023 Distribution Chain

In 2023, TAs launched various IcedID malware distribution campaigns , but quickly consolidated due to their common delivery method, phishing emails. Initially, emails contained ISO files as attachments, later the TAs switched to OneNote, and PDFs, to spread the malware.

The IcedID infection started when the user clicked on the malicious file, which then executed the IcedID DLL. In some cases, it created a scheduled task to run the malware. Once the patient-zero machine was infected, the malware began enumerating to escalate privileges and move laterally across the network. After gaining access to all the machines, including the AD server, the threat actors detonated the ransomware.

Known cases where IcedID executed quantum ransomware, surprised many. Despite the change in behaviour of the malware, from a banking trojan to a ransomware deployer using many tactics, techniques and procedures (TTPs) were common.

Visibility Through Tidal

For better visibility of all three campaigns, we used Tidal Cyber's Community Edition to map the TTPs. Tidal Cyber is a defense platform utilizing threat intelligence to help cybersecurity teams promptly, and effortlessly, identify and address potential security incidents. The

platform incorporates osquery from Loginsoft, detecting security threats and allowing users to research, and create, threat profiles. This results in Tidal Cyber enabling defenders to take informed defensive measures by prioritizing relevant threats.

The image below displays a matrix that covers the TTPs of the IcedID malware campaign from the past three years.

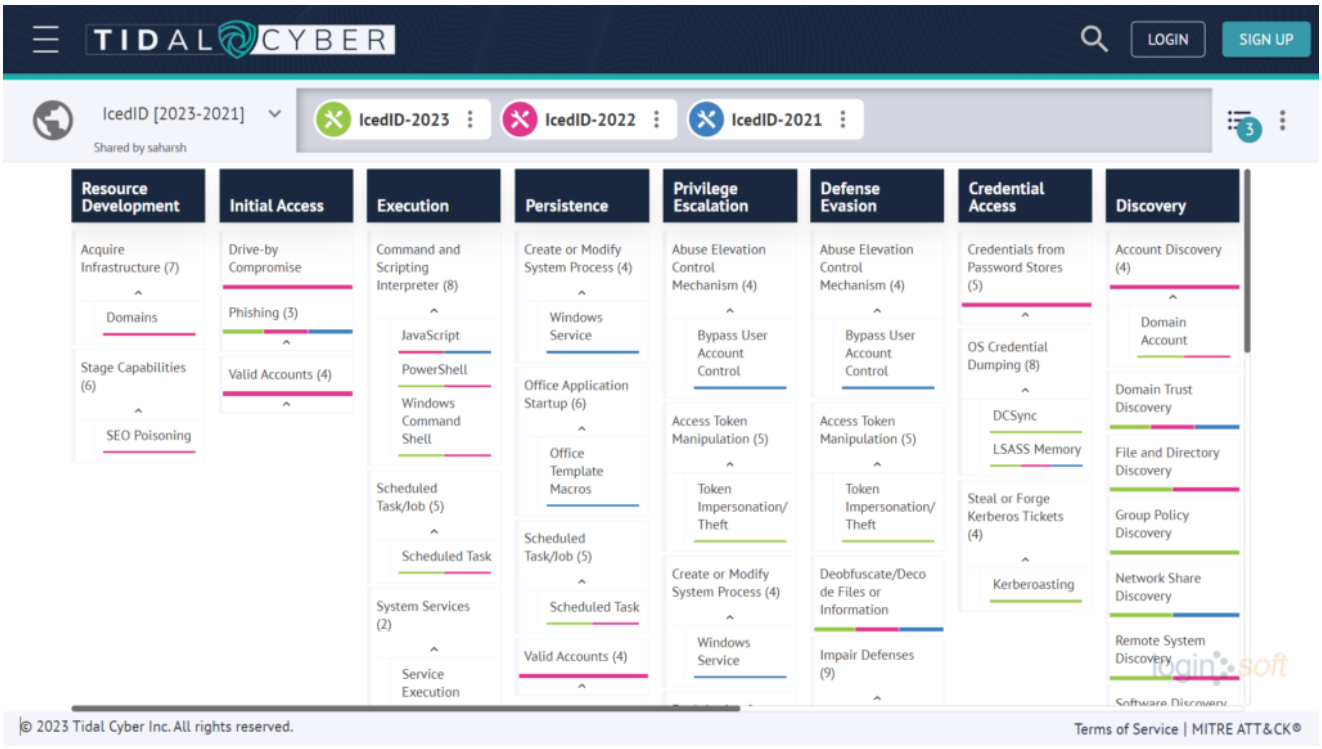

Figure: Tidal Cyber's Navigation Layer

Loginsoft uploaded osquery rules on the Tidal platform, which can be used to detect malicious activities based on TTPs. Access these rules here.

Osquery Rules To Detect IcedID Activity

Below are specific osquery rules to help defend against the malicious behaviours exhibited by IcedID malware.

Detects suspicious hidden files from the mounted drive

```
SELECT
    atime,
    btime,
    ctime,
    device,
    directory,
    path,
    filename,
    file_id,
    attributes
FROM file
JOIN (SELECT device_id FROM logical_drives where file_system = 'UDF') AS drives
ON directory LIKE device_id || '\%'
AND
(
    path LIKE '%.dll'
    OR path LIKE '%.bat'
    OR path LIKE '%.cmd'
    OR path LIKE '%.dat'
)
AND attributes LIKE '%H%';
```

Detects the use of windows binary Regsvr32 making a network connection

```
SELECT
  ps.name AS process_name,
  ps.pid AS process_id,
  ps.cmdline AS process_cmdline,
  pos.local_address AS local_address,
  pos.local_port AS local_port,
  pos.remote_address AS remote_address,
  pos.remote_port AS remote_port
FROM processes ps, process_open_sockets pos
WHERE ps.pid = pos.pid
AND LOWER(ps.name) = 'regsvr32.exe';
```

Detects named pipes used by CobaltStrike

```
SELECT
  p.name as process_name,
  p.pid as process_pid,
  p.path as process_path,
  p.cmdline as process_cmdline,
  pipes.name as pipe_name,
  pipes.instances as pipe_instances,
  pipes.flags as pipe_flags
FROM processes p , pipes
WHERE p.pid = pipes.pid
AND
(
  LOWER(pipe_name) LIKE 'msagent_%'
  OR LOWER(pipe_name) LIKE 'interprocess_%'
  OR LOWER(pipe_name) LIKE 'sarpc_%'
  OR LOWER(pipe_name) LIKE 'samr_%'
  OR LOWER(pipe_name) LIKE 'netlogon_%'
  OR LOWER(pipe_name) LIKE 'wkssvc_%'
  OR LOWER(pipe_name) LIKE 'srvsvc_%'
  OR LOWER(pipe_name) LIKE 'mojo_%'
  OR LOWER(pipe_name) LIKE 'postex%'
  OR LOWER(pipe_name) LIKE 'status_%'
  OR LOWER(pipe_name) LIKE 'msse-%'
);
```

Threat Bites

Threat Actor

Targeted Country

Targeted Industry

First Seen

Last Seen

LOLBAS

Backdoor

Telemetry

Samples

:

:

:

:

:

:

:

:

:

TA578, TA551, TA577, TA544, TA581, TA542

US, UK, Canada, Italy

Financial Institution, Ecommerce, Payment, Telecommunication

2017

2023

Rundll32, Regsvr32, Wmic

Dark VNC, Anubis VNC, Keyhole VNC

Sysmon, Security, Windefend, PowerShell

https://bazaar.abuse.ch/browse/tag/IcedID/

References