On Australia's Doorstep:

Tracking – and Stopping - High Profile Targeted Attacks, Threat Actors & TTPs

Eoin Healy

WHO AM I?

Eoin Healy

Senior Threat Researcher, Threat Intelligence
From Cork, Ireland to Australia

/in/eo-healy
@_eohealy

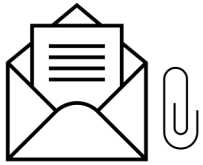
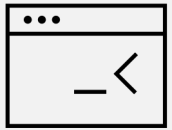
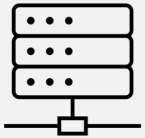
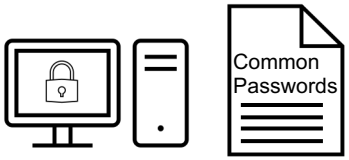
Agenda

What are we going to cover?

- Initial Access Trends
- Cybercrime Insights
- Targeted Attacks
- Mitigations

Initial Access Trends

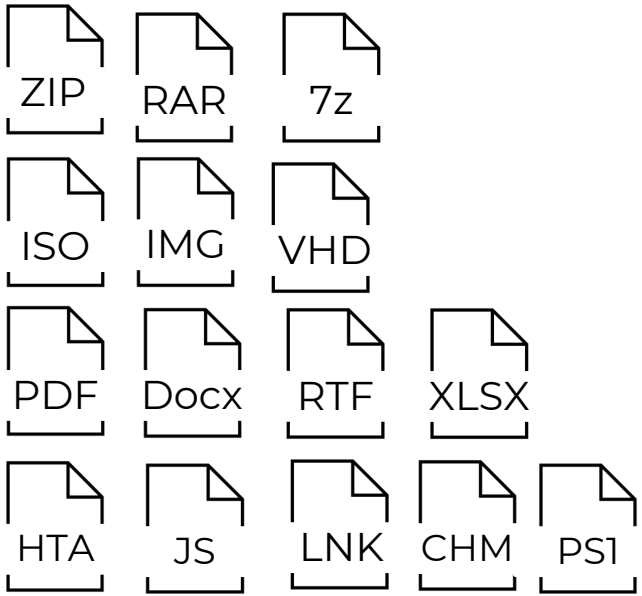
Initial Access

Phishing T1566	 Email Attachment	 Malicious Link	 Malvertising
Vulnerabilities T1190	 Applications	 Services	 Devices
Brute Force T1110	 Password Guessing	 Password Spraying	 Breach Dumps Credential Stuffing

Phishing

File Formats Utilized

- Compressed archives
- Disk image files
- Documents
- Other



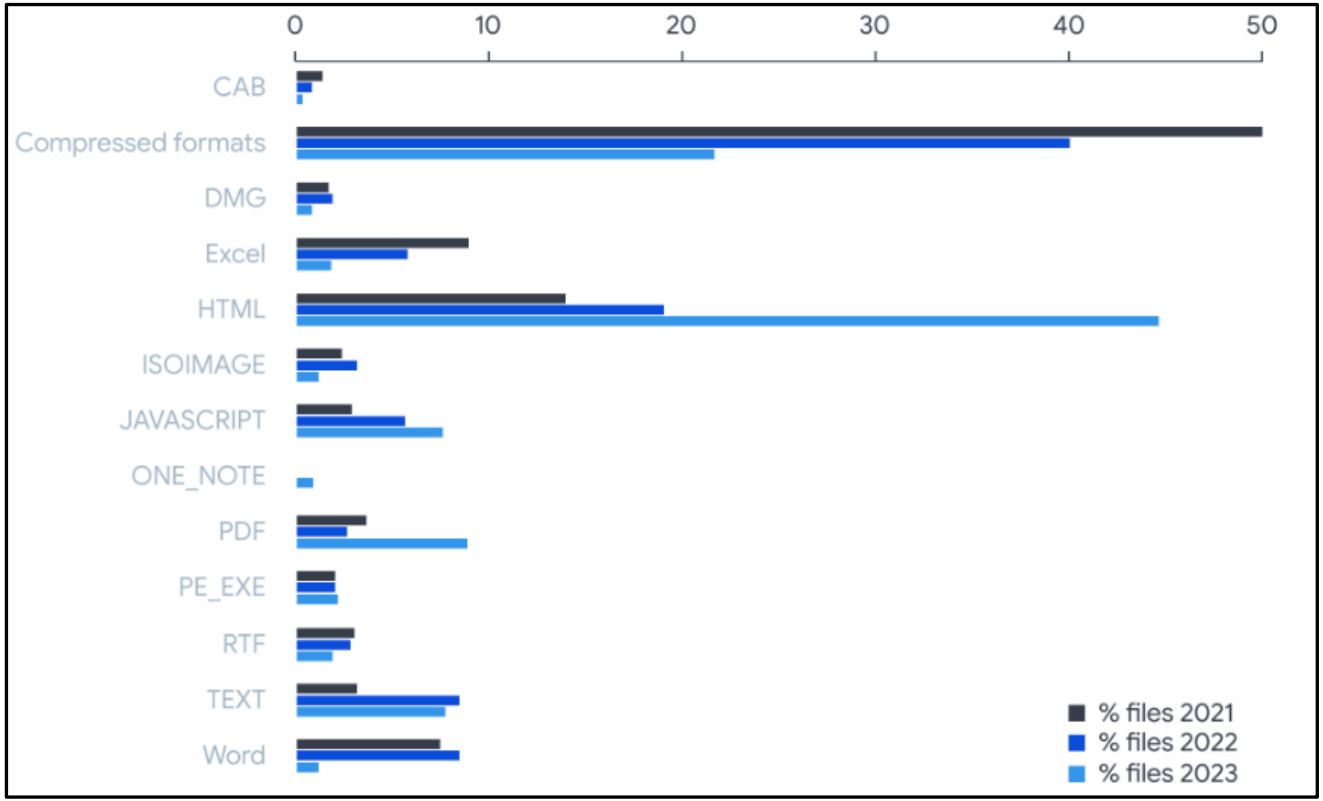
Phishing – File Formats

Why?

Mostly defense evasion

- VBA blocked by default
- Early stages are usually lightweight and try to look as legitimate as possible
- Subvert Trust Controls: Mark-of-the-Web Bypass (MOTW) T1553.005

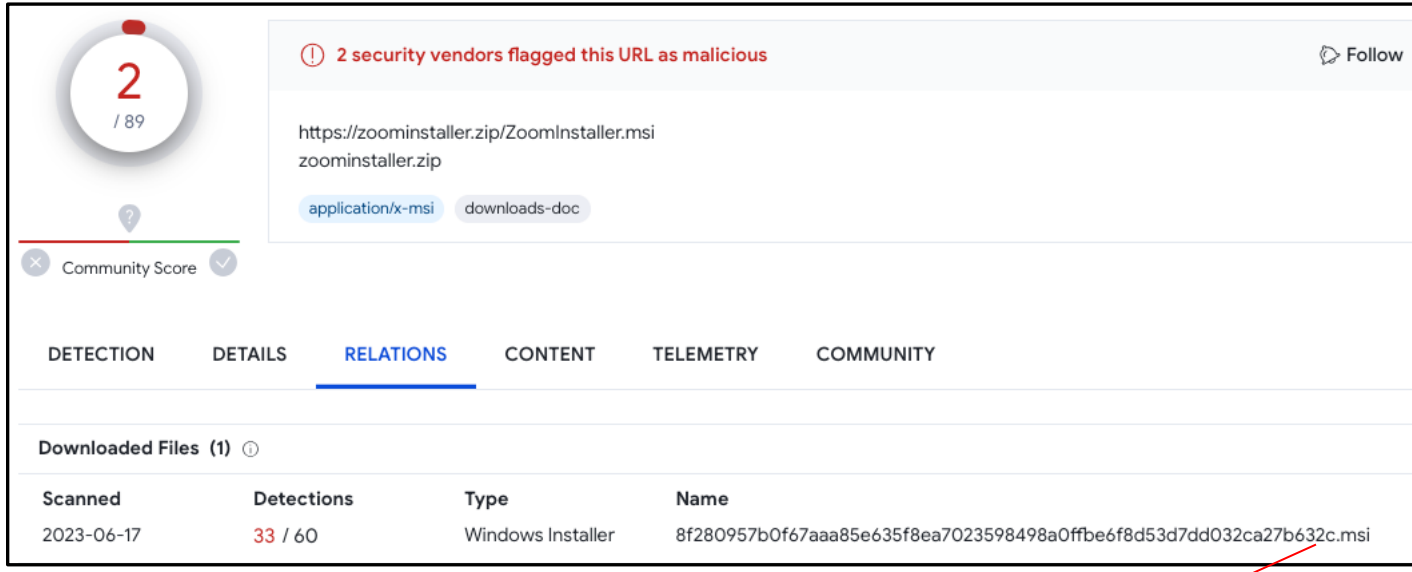
Phishing - Delivery trends

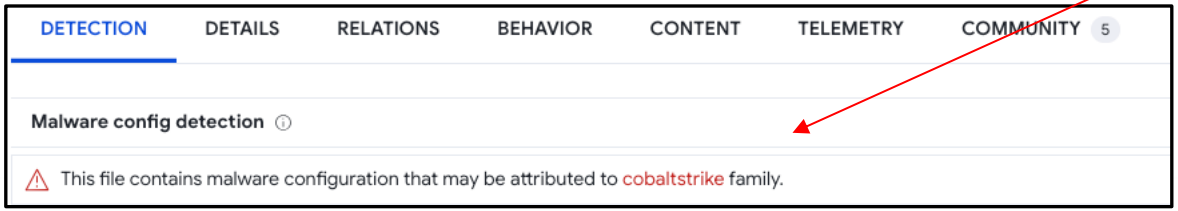


Ref: https://blog.virustotal.com/2023/07/virustotal-malware-trends-report.html

Phishing – Obvious Prediction…

- Google released TLDs for .zip and .mov
- .zip TLDs will be used by attackers for deception
- .zip TLD -> MSI -> Cobalt strike





Vulnerabilities CVEs

Numbers are only so good..

- 2023 has overtaken 2022 for the number of 0-days detected and disclosed in-the-wild with 51 for the year so far
- 12 zero days in September alone

Name	Description
CVE-2023-24880	Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2022-47986	IBM Aspera Faspex 4.4.2 Patch Level 1 and earlier could allow a remote attacker to execute arbitrary code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system. The obsolete API call was removed in Faspex 4.4.2 PL2. IBM X-Force ID: 243512.
CVE-2022-47966	Multiple Zoho ManageEngine on-premise products, such as ServiceDesk Plus through 14003, allow remote code execution due to use of Apache Santuario xmlsec (aka XML Security for Java) 1.4.1, because the xmlsec XSLT features, by design in that version, make the application responsible for certain security protections, and the ManageEngine applications did not provide those protections. This affects Access Manager Plus before 4308, Active Directory 360 before 4310, ADAudit Plus before 7081, ADManager Plus before 7162, ADSelfService Plus before 6211, Analytics Plus before 5150, Application Control Plus before 10.1.2220.18, Asset Explorer before 6983, Browser Security Plus before 11.1.2238.6, Device Control Plus before 10.1.2220.18, Endpoint Central before 10.1.2228.11, Endpoint Central MSP before 10.1.2228.11, Endpoint DLP before 10.1.2137.6, Key Manager Plus before 6401, OS Deployer before 1.1.2243.1, PAM 360 before 5713, Password Manager Pro before 12124, Patch Manager Plus before 10.1.2220.18, Remote Access Plus before 10.1.2228.11, Remote Monitoring and Management (RMM) before 10.1.41. ServiceDesk Plus before 14004, ServiceDesk Plus MSP before 13001, SupportCenter Plus before 11026, and Vulnerability Manager Plus before 10.1.2220.18. Exploitation is only possible if SAML SSO has ever been configured for a product (for some products, exploitation requires that SAML SSO is currently active).
CVE-2022-40684	An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

Name	Description
CVE-2021-27878	An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection. The attacker could use one of these commands to execute an arbitrary command on the system using system privileges.
CVE-2021-27877	An issue was discovered in Veritas Backup Exec before 21.2. It supports multiple authentication schemes: SHA authentication is one of these. This authentication scheme is no longer used in current versions of the product, but hadn't yet been disabled. An attacker could remotely exploit this scheme to gain unauthorized access to an Agent and execute privileged commands.
CVE-2021-27876	An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection. By using crafted input parameters in one of these commands, an attacker can access an arbitrary file on the system using System privileges.
CVE-2021-21974	OpenSLP as used in ESXi (7.0 before ESXi70U1c-17325551, 6.7 before ESXi670-202102401-SG, 6.5 before ESXi650-202102101-SG) has a heap-overflow vulnerability. A malicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.

Google TAG -https://docs.google.com/spreadsheets/d/1IkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit#gid=1746868651

Vulnerabilities CVEs

Good Resources

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- ACSC's Brief Collateral sessions

Name	Description
CVE-2023-33308	A stack-based overflow vulnerability [CWE-124] in FortiOS version 7.0.0 through 7.0.10 and 7.2.0 through 7.2.3 and FortiProxy version 7.0.0 through 7.0.9 and 7.2.0 through 7.2.2 allows a remote unauthenticated attacker to execute arbitrary code or command via crafted packets reaching proxy policies or firewall policies with proxy mode alongside deep or full packet inspection.
CVE-2023-27997	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.
CVE-2023-27532	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts.
CVE-2023-0669	Fortra (formerly, HelpSystems) GoAnywhere MFT suffers from a pre-authentication command injection vulnerability in the License Response Servlet due to deserializing an arbitrary attacker-controlled object. This issue was patched in version 7.1.2.

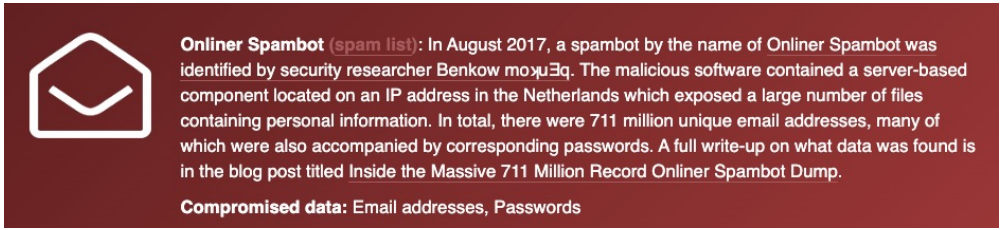
Name	Description
CVE-2023-34362	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.
CVE-2023-28252	Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2023-27351	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to exploit this vulnerability. The specific flaw exists within the SecurityRequestFilter class. The issue results from improper implementation of the authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19226.
CVE-2023-27350	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to exploit this vulnerability. The specific flaw exists within the SetupCompleted class. The issue results from improper access control. An attacker can leverage this vulnerability to bypass authentication and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-18987.

Credential Stuffing

* DISCLAIMER – 2017 Data Breach – All Data is in HaveIBeenPwned

OSINT of Malware Repository

- 10 minutes hunting
- 354 @gov.au addresses and passwords discovered
- 51 different official government departments
- Defence, Police, Prime Ministers office, Infrastructure, Transport, Aviation, State Governments, Law etc etc..



Cybercrime Insights - Stealers and Loaders

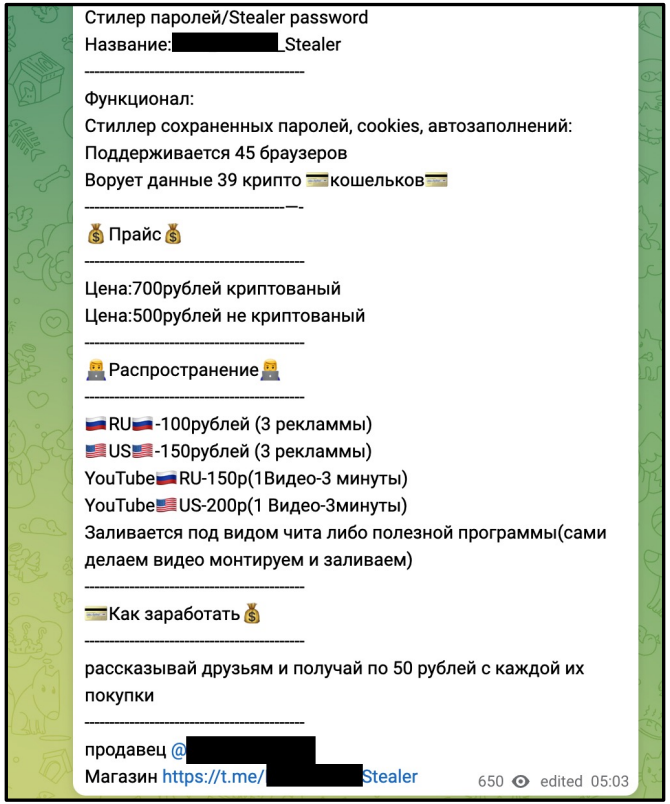
Stealers and Loaders

Low Barrier to Entry

Malware as a Service (MaaS) operations has lowered the technical barrier to entry into cybercrime

Stealer:

- Supports 45 browsers
- 39 crypto wallets.
- 700 rubles (12AUD) for a crypted version

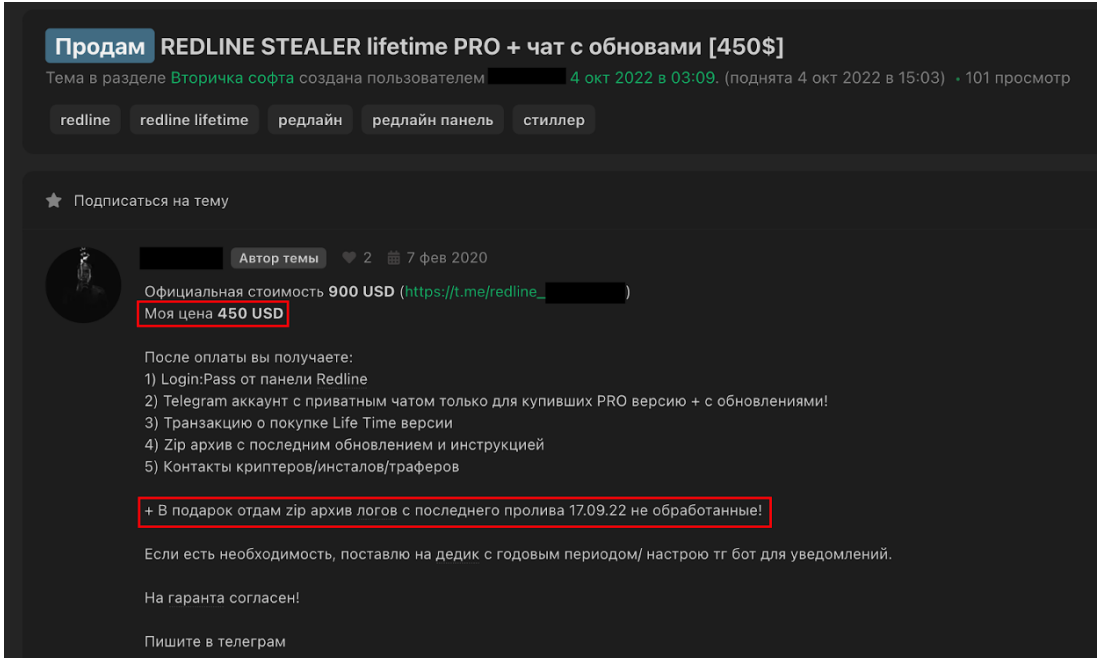


Stealers and Loaders

Low Barrier to Entry

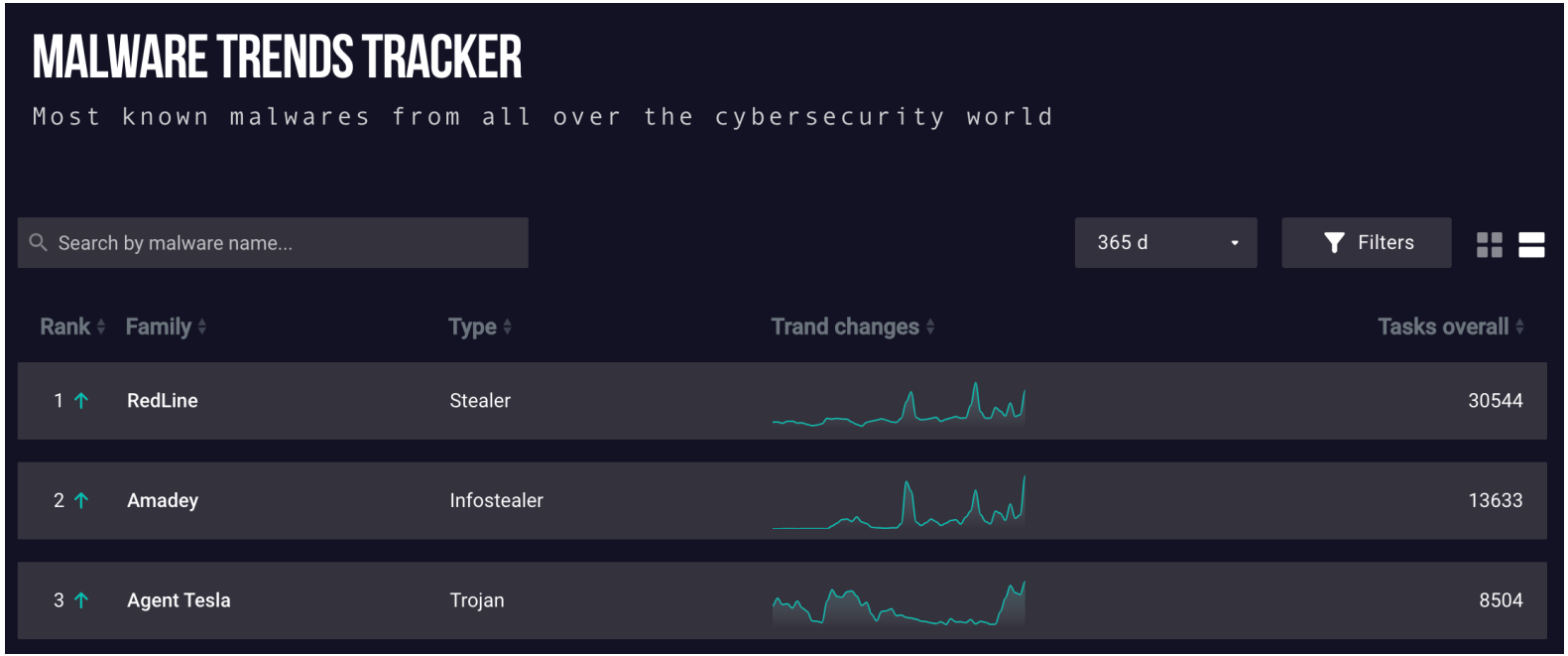
Redline
- Easily Accessible
- Cheap Cost
- Gift of zipped unprocessed “logs”

“logs” = stolen information from a previous victim



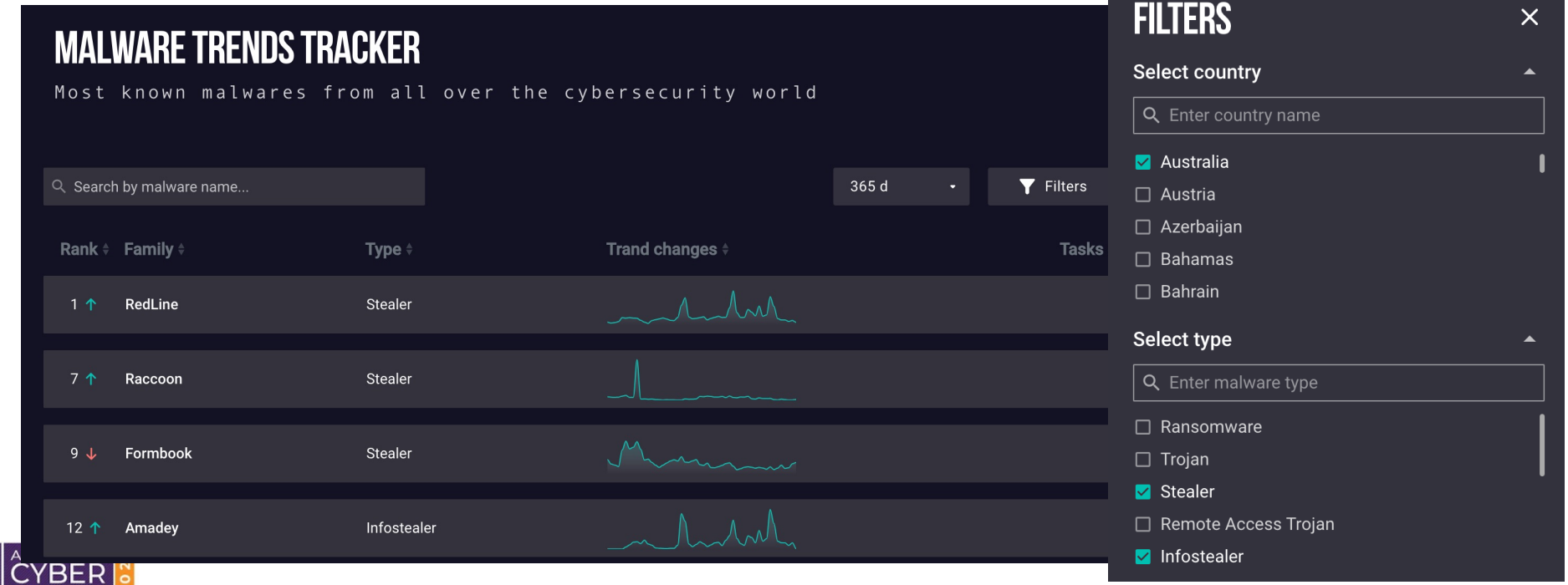
Stealers and Loaders

Any.run Sandbox Trends Global Trends – August



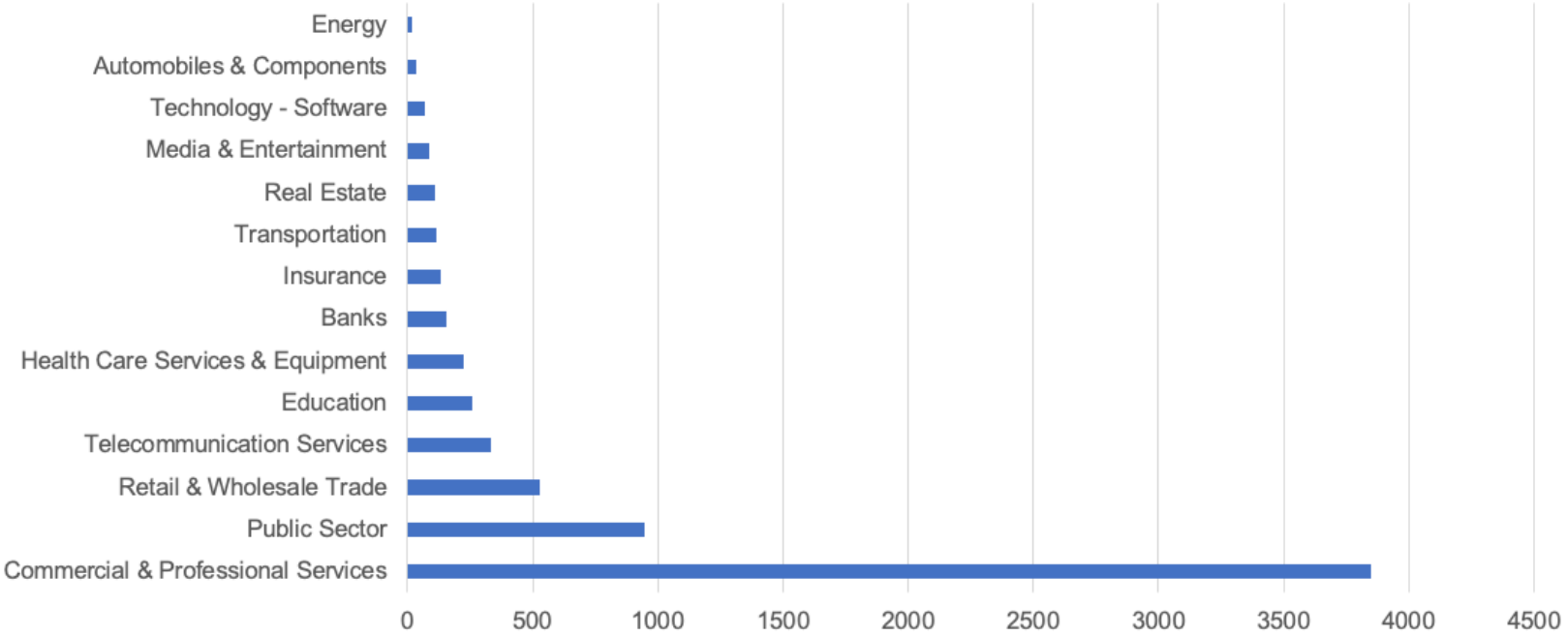
Stealers and Loaders

Any.run Sandbox Trends Australia



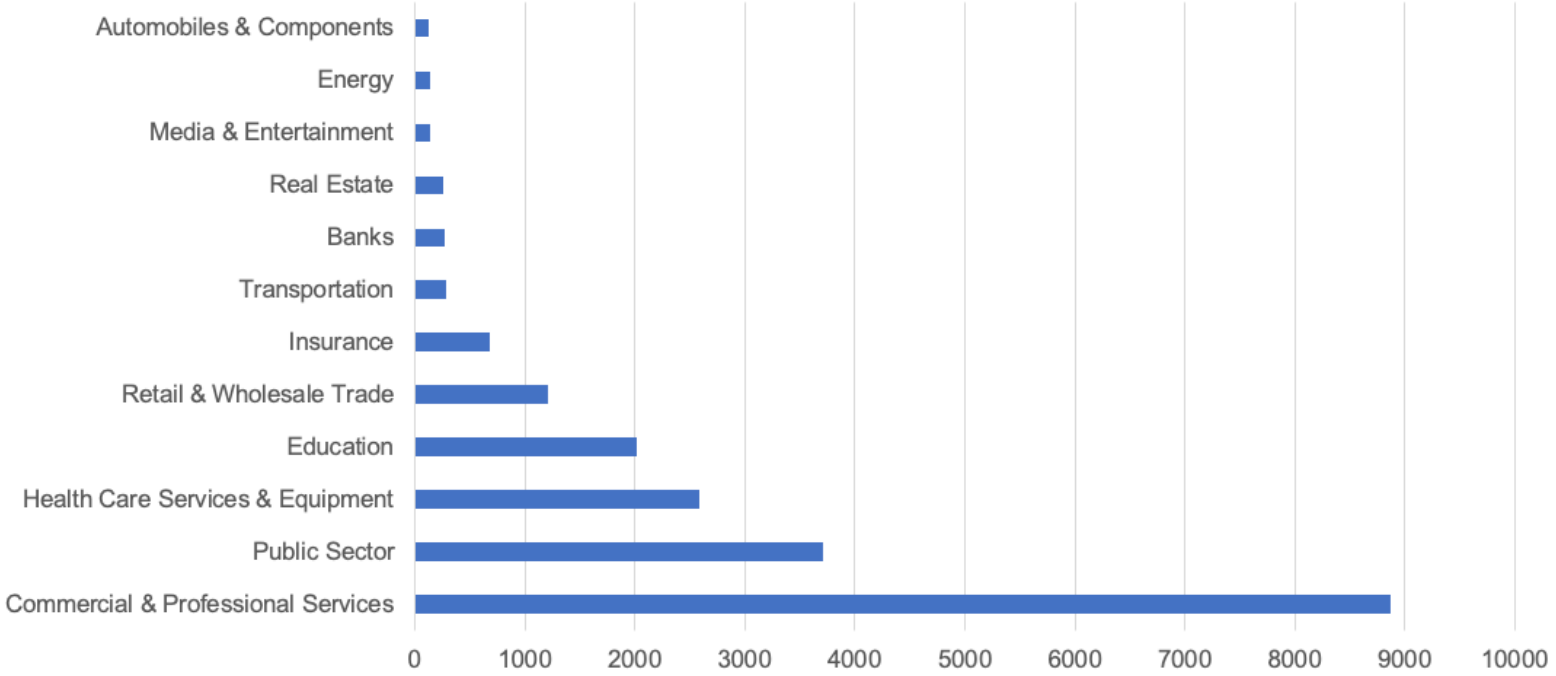
APAC Statistics – Stealers

Industry



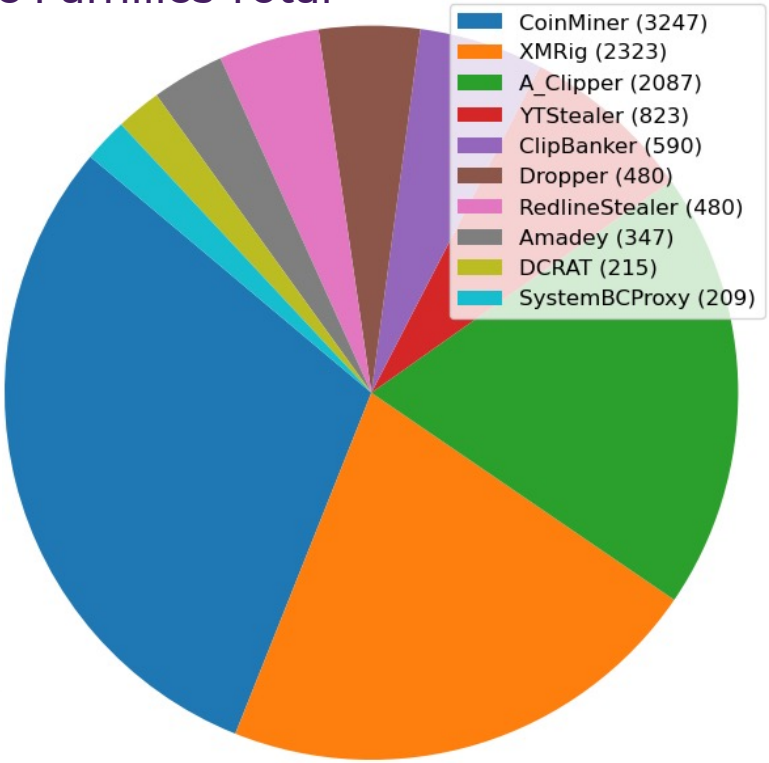
APAC Statistics - Loaders

Industry



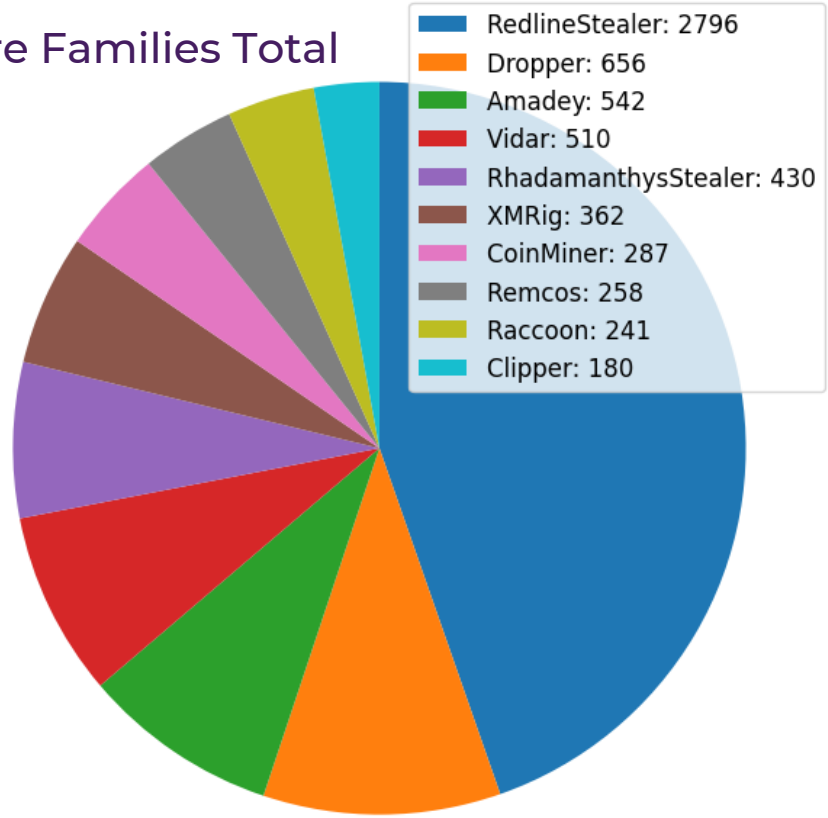
Long term Redline Trends

Top 10 Spread Malware Families Total



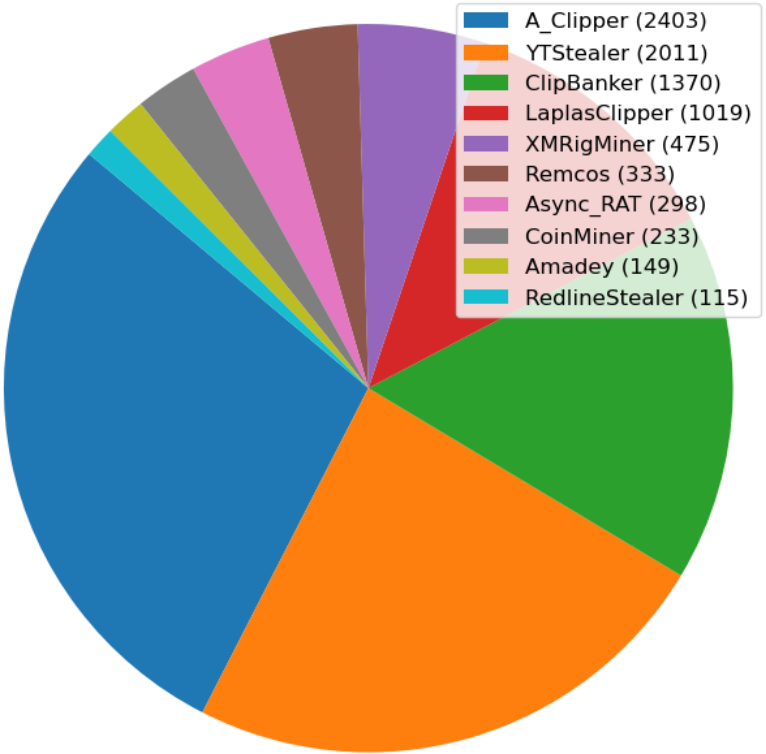
Long term Amadey Trends

Top 10 Spread Malware Families Total



Long term Racoon Trends

Top 10 Spread Malware Families Total

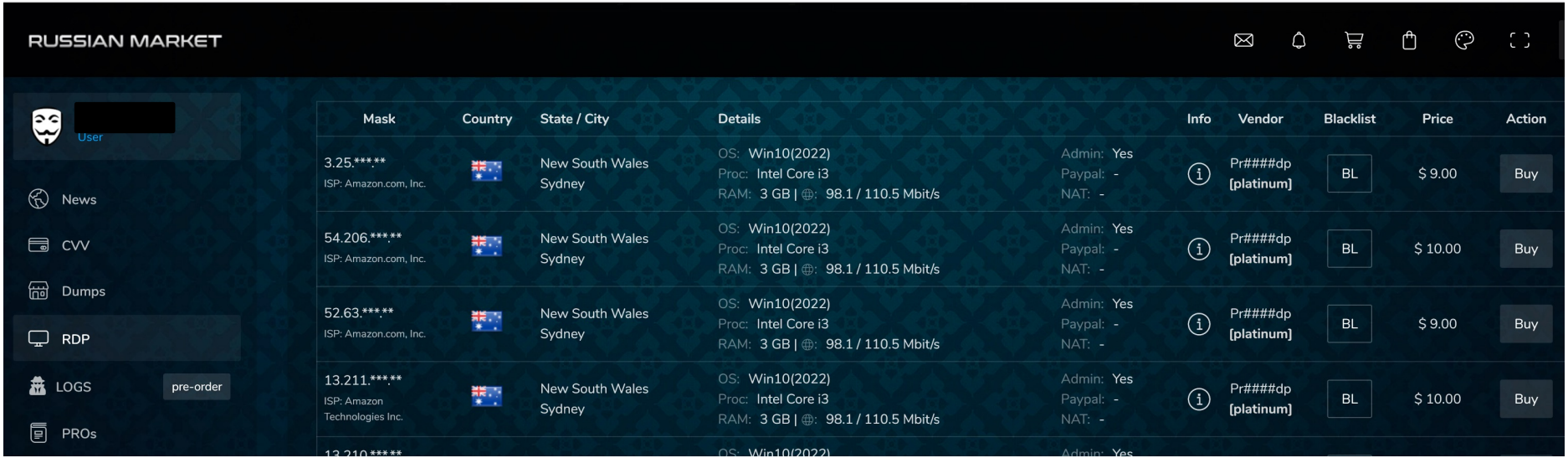


Cybercrime Insights – Access Markets/IABs

Access Markets/IABs

Russian Market

RDP Access - Filtered by Australia $9 USD



Access Markets/IABs

Russian Market

”Logs” - Filtered by Australia $10 USD

Sortable↓

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Redline	New South Wales ISP: Aussie Broadband	roblox.com | web.roblox.com | discord.com | chat.chatogo.com | twitch.tv | roblox.com | my.account.sony.com | roblox.com | connect.ubisoft.com | twitch.tv | Show more...	-	-	archive.zip DomainDetects.txt ImportantAutofills.txt InstalledBrowsers.txt InstalledSoftware.txt Passwords.txt ProcessList.txt Screenshot.jpg UserInformation.txt Autofills Cookies Steam	2023.09.11 *0.36Mb*	sm####ez **[platinum]**	$ 10.00	Buy

Access Markets/IABs

Russian Market

”Logs” - Filtered by Australia & .gov.au in Links. $10 USD

Sortable↓

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Redline	New South Wales ISP: SingTel Optus Pty Ltd	portal.cju.ac.kr | ecalleehj.us5.quickconnect.to | iris.go.kr | ecalleehj.tw2.quickconnect.to | nid.naver.com | portal.cju.ac.kr | hive.cju.ac.kr | pki.cju.ac.kr | hancom.com | login.live.com | Show more...	-	-	archive.zip DomainDetects.txt ImportantAutofills.txt InstalledBrowsers.txt InstalledSoftware.txt Passwords.txt ProcessList.txt UserInformation.txt Autofills Cookies	2023.09.07 *0.40Mb*	sm####ez **[platinum]**	$ 10.00	Buy
Redline	Queensland ISP: SingTel Optus Pty Ltd	accounts.google.com | fed.education.qld.gov.au | auth.services.adobe.com | flightsim.to | login.live.com | virtualairlineschedules.net | discord.com | login.live.com | library.avsim.net | maxteamdesign.com | Show more...	-	-	archive.zip	2023.08.28 *0.89Mb*	sm####ez **[platinum]**	$ 10.00	Buy
Redline	Western Australia ISP: SingTel Optus Pty Ltd	facebook.com | apod.com.au | spotlightstores.com | accounts.google.com | dreams10.defence.gov.au | portal.homestart.net.au | australiandirect.com.au | online.transport.wa.gov.au | facebook.com | apod.com.au | Show	-	-	archive.zip	2023.08.30 *0.07Mb*	sm####ez **[platinum]**	$ 10.00	Buy

Example “Logs”

Australian Example

```
*******************************************************
*  Telegram: https://t.me/redline_market_bot  *
*******************************************************

Build ID: [redacted]
IP: [redacted]
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
UserName: [redacted]
Country: AU
Zip Code: [redacted]
Location: [redacted] Western Australia
[redacted]
Current Language: English (United States)
ScreenSize: {Width=1920, Height=1080}
TimeZone: (UTC-08:00) Pacific Time (US & Canada)
Operation System: Windows 10 Home x64
UAC: AllowAll
Process Elevation: False
Log date: 1/4/2023 5:00:54 PM

Available KeyboardLayouts:
English (United States)

Hardwares:
Name: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz, 4 Cores
Name: Intel(R) HD Graphics 530, 1073741824 bytes
Name: Total of RAM, 16078.96 MB or 16860008448 bytes

Anti-Viruses:
Reason Cybersecurity
Windows Defender
```

```
*******************************************************
*  Telegram: https://t.me/redline_market_bot  *
*******************************************************

Build ID: [redacted]
IP: [redacted]
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
UserName: [redacted]
Country: AU
Zip Code: [redacted]
Location: Melbourne, Victoria
[redacted]
Current Language: English (Australia)
ScreenSize: {Width=1536, Height=864}
TimeZone: (UTC+10:00) Canberra, Melbourne, Sydn
Operation System: Windows 10 Home x64
UAC: AllowAll
Process Elevation: False
Log date: 1/6/2023 6:51:55 AM

Available KeyboardLayouts:
English (Australia)
English (United States)

Hardwares:
Name: Intel(R) Core(TM) i5-10500H CPU @ 2.50GHz
Name: Intel(R) UHD Graphics, 1073741824 bytes
Name: NVIDIA GeForce GTX 1650 with Max-Q Design
Name: Total of RAM, 16205.8 MB or 16993009664 b
```

Name	Size	Type
Autofills		File folder
Cookies		File folder
CreditCards		File folder
Steam		File folder
DomainDetects	1 KB	Text Document
ImportantAutofills	1 KB	Text Document
InstalledBrowsers	1 KB	Text Document
InstalledSoftware	3 KB	Text Document
Passwords	2 KB	Text Document
ProcessList	31 KB	Text Document
Screenshot	130 KB	JPG File
UserInformation	2 KB	Text Document

Example “Logs”

Australian Example

```
*************************************************
*                                               *
*  Telegram: https://t.me/redline_market_bot    *
*************************************************

Build ID: [redacted]
IP: [redacted]
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
UserName: [redacted]
Country: AU
Zip Code: [redacted]
Location: [redacted] Queensland
[redacted]
Current Language: English (Australia)
ScreenSize: {Width=1920, Height=1080}
TimeZone: (UTC+10:00) Brisbane
Operation System: Windows 10 Home x64
UAC: AllowAll
Process Elevation: False
Log date: 12/29/2022 7:46:22 PM

Available KeyboardLayouts:
English (United States)
English (Australia)

Hardwares:
Name: AMD Ryzen 5 5500                  , 6 Cores
Name: NVIDIA GeForce RTX 3060, 4293918720 bytes
Name: Total of RAM, 16175.49 MB or 16961228800 bytes

Anti-Viruses:
Windows Defender
```

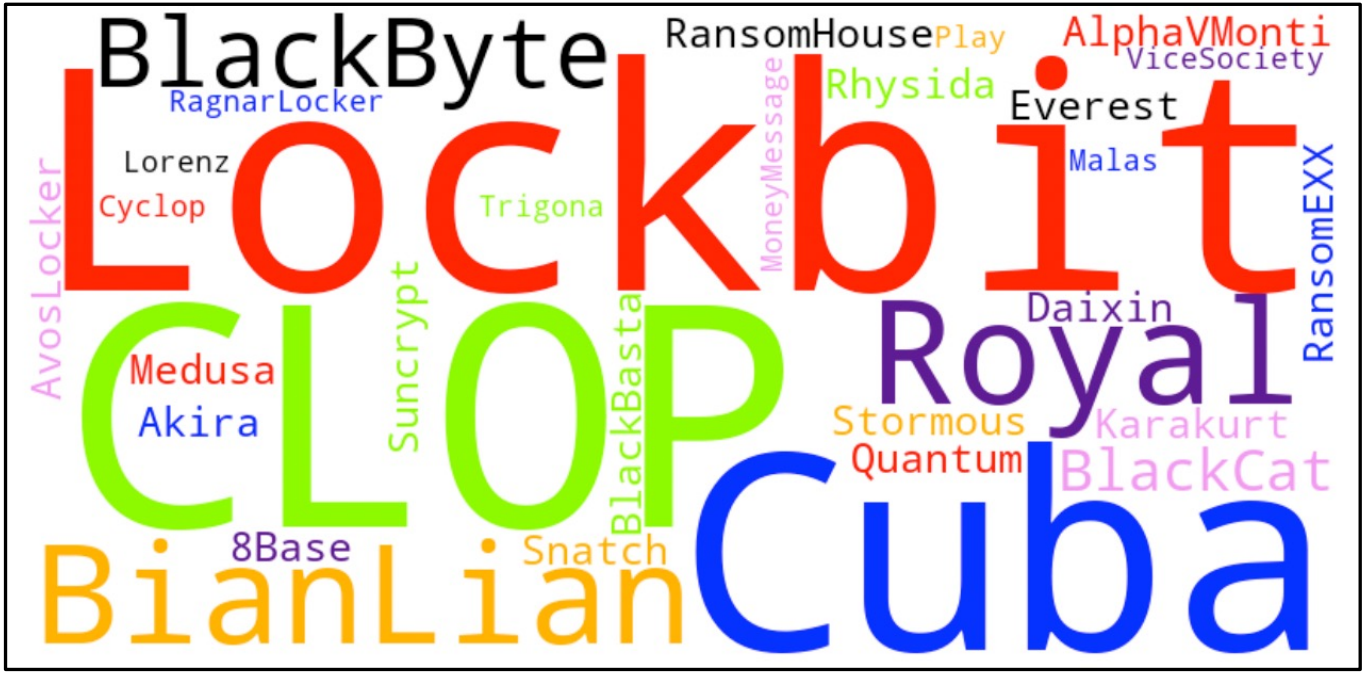
```
*************************************************
*                                               *
*  Telegram: https://t.me/redline_market_bot    *
*************************************************

Build ID: [redacted]
IP: [redacted]
FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
UserName: [redacted]
Country: AU
Zip Code: [redacted]
Location: Brisbane, Queensland
[redacted]
Current Language: English (Australia)
ScreenSize: {Width=1505, Height=846}
TimeZone: (UTC+10:00) Brisbane
Operation System: Windows 10 Home x64
UAC: AllowAll
Process Elevation: False
Log date: 1/6/2023 11:11:49 PM

Available KeyboardLayouts:
English (Australia)
English (United States)
Russian (Russia)
English (United Kingdom)

Hardwares:
Name: Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz, 4 Cores
Name: NVIDIA GeForce GTX 1070, 4293918720 bytes
Name: Total of RAM, 32727.64 MB or 34317418496 bytes

Anti-Viruses:
Windows Defender
```

Name	Size	Type
Autofills		File folder
Cookies		File folder
CreditCards		File folder
Discord		File folder
FileGrabber		File folder
Steam		File folder
DomainDetects	1 KB	Text Document
ImportantAutofills	1 KB	Text Document
InstalledBrowsers	1 KB	Text Document
InstalledSoftware	5 KB	Text Document
Passwords	4 KB	Text Document
ProcessList	124 KB	Text Document
Screenshot	76 KB	JPG File
UserInformation	2 KB	Text Document

Cybercrime Insights - Ransomware

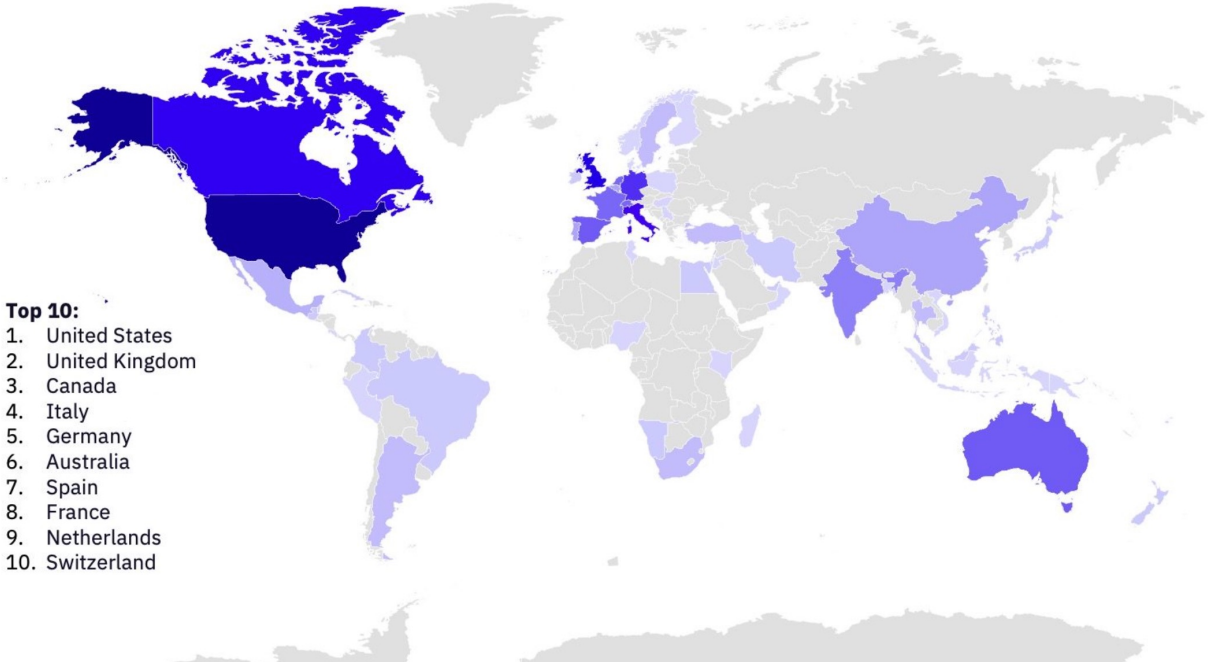
Ransomware/RaaS

Dynamic, Opportunistic & Profit-driven



Ransomware/RaaS

Ransomware Victims by Country



Ref: https://www.guidepointsecurity.com/blog/grit-ransomware-report-july-2023/

Ransomware/RaaS

Ransomware Activity Q3

DarkFeed @ido_cohen2 · Sep 11
Last Week #Ransomware Statistics 🎯

➡️TOP TARGETED COUNTRIES
🇺🇸 USA:50
🇬🇧 UK:5
🇦🇺 **Australia**:5

➡️TOP TARGETED SECTORS
Retail:13
Healthcare:10
Financial:5

➡️TOP ACTIVE TEAMS
Cactus:20
Lockbit:16
Ransomed:14

DarkFeed @ido_cohen2 · Sep 5
🌐 Top Targeted Countries August🎯

🇺🇸 USA: 183
🇩🇪 Germany: 24 💥
🇬🇧 UK: 17
🇫🇷 France: 15 💥
🇮🇹 Italy: 13
🇨🇦 Canada: 11
🇦🇺 **Australia**: 8
🇮🇳 India: 7
🇦🇪 UAE: 5
🇯🇵 Japan: 5
🇳🇱 Netherlands: 5
🇲🇽 Mexico: 5
🇪🇸 Spain: 5

DarkFeed @ido_cohen2 · Sep 4
Last Week #Ransomware Statistics 🎯

➡️TOP TARGETED COUNTRIES
🇺🇸 USA:62
🇫🇷 France:14
🇦🇺 **Australia**:6

➡️TOP TARGETED SECTORS
Legal:12
Education:11
Healthcare:10

➡️TOP ACTIVE TEAMS
Lockbit:68
BlackCat:12
Akira:8

ThreatMon Ransomware Monitoring ✔
@TMRansomMonitor

🚨This Week #Ransomware Activities🚨

Total Activities: 213 ‼️

Top Actives Groups
- #ClopLeaks 80
- #LockBit 73
- #BlackCat 13
- #Akira 11
- #RaGroup 7

Top Targeted Countries
🇺🇸 #UnitedStates 108
🇫🇷 #France 17
🇬🇧 #UK 10
🇨🇦 #Canada 8
🇦🇺 #Australia 7

Ransomware Optimizations

E.g. Cuba Ransomware

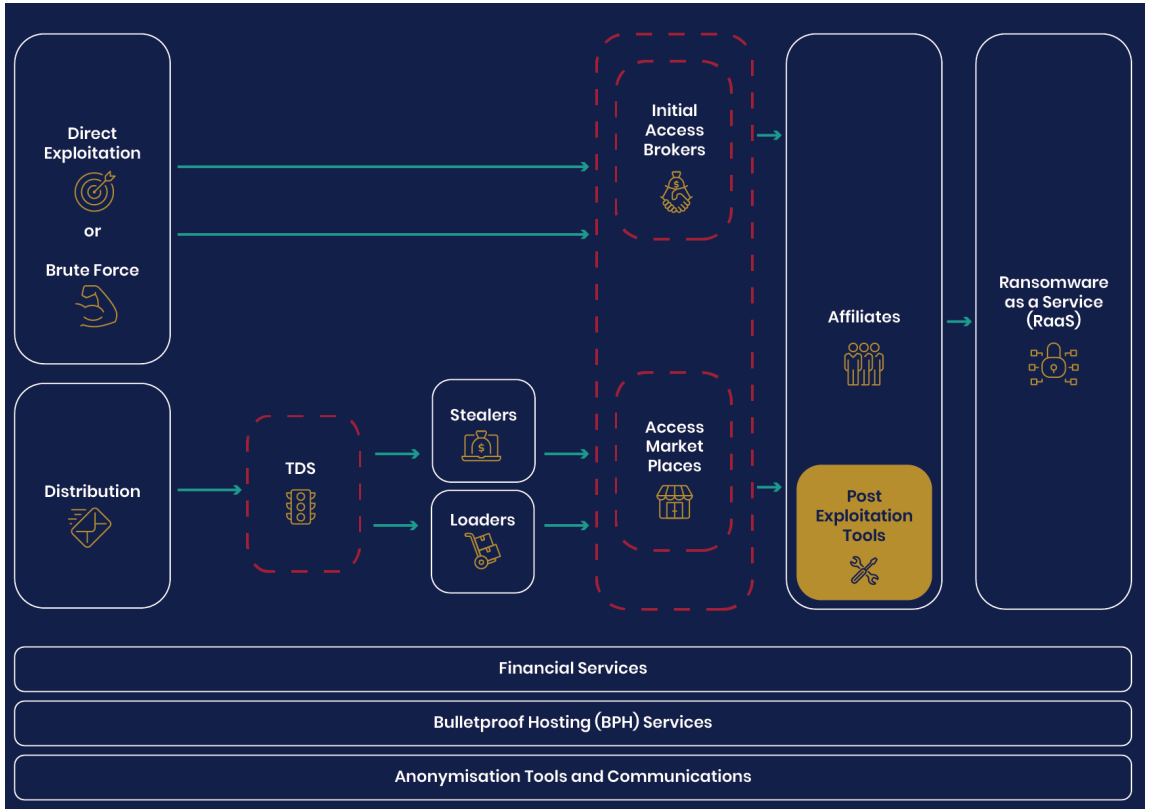
- Subtle incremental changes to their playbook/TTPs
  - Initial Access – Unknown – Valid Credentials/Credential Stuffing potentially
  - PowerShell Loaders --> DLL Loaders (MFCLibrary)
  - String Encoding - CRC-64 hashing, Base64 encoding
  - Callback Shellcode Injection
    - Using different API calls with application-defined callback functions
    - CreateTimerQueueTimer(Bughatch)

Ransomware Optimizations

E.g. Cuba Ransomware

- Subtle incremental changes to their playbook/TTPs
  - Utilising different vulnerable drivers (BYOVD)
  - Leverages known exploits to fit their needs
    - E.g. Need: Credential access for lateral movement of network
    - CVE-2023-27532 – Vulnerability in Veeam Backup & Replication

Cybercrime Ecosystem



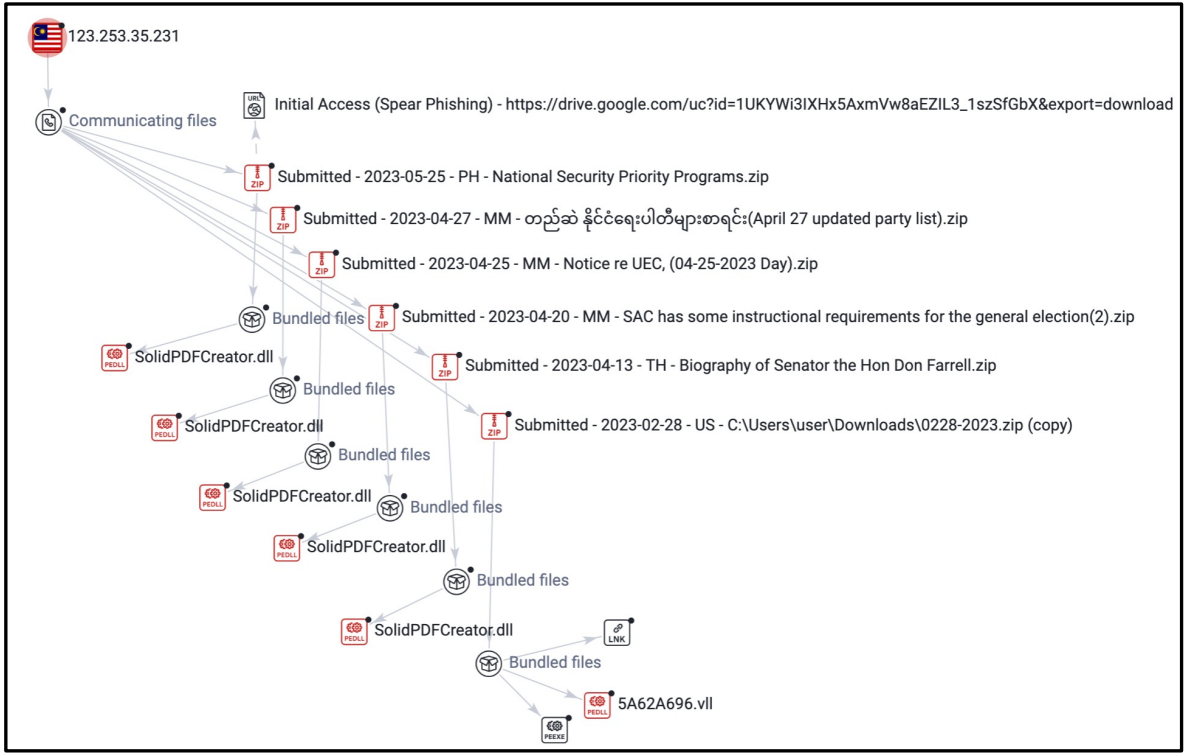
Ref: https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_9

Targeted Attacks

Mustang Panda

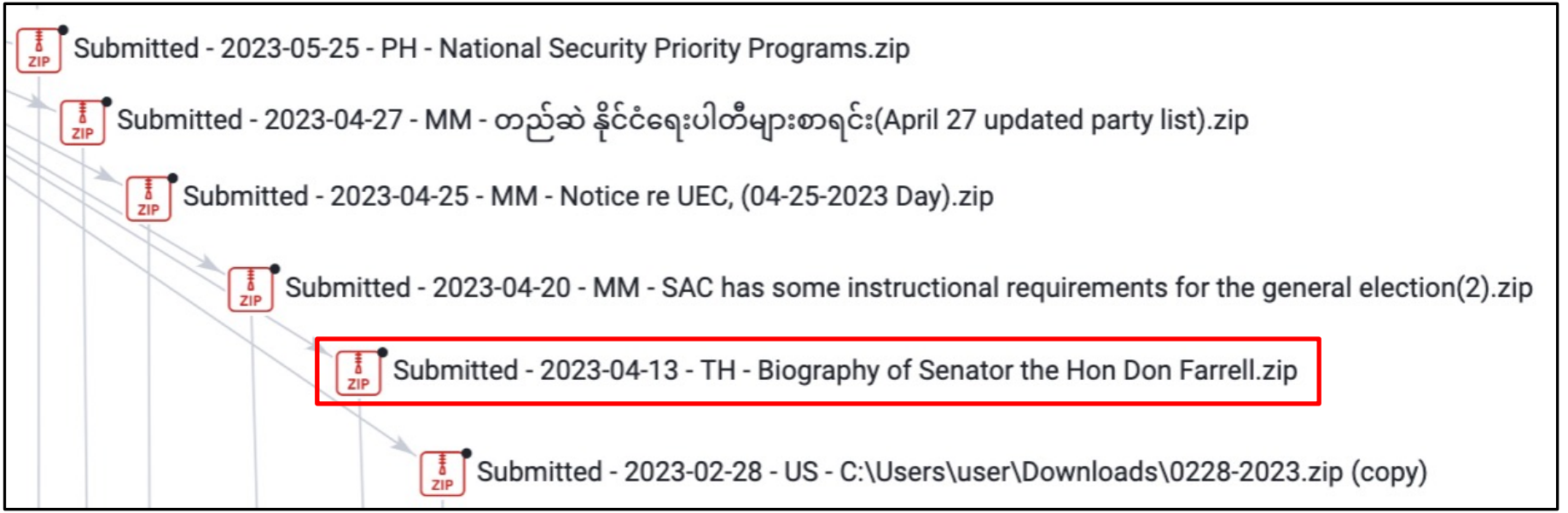
APAC Campaign Feb - June

- Government/Military themed lures
- Seen previously targeting Myanmar(Burma)
- Fluctuating between EU and APAC
- Legitimate application utilized for DLL hijacking/sideloading



Mustang Panda

APAC Campaign



Mustang Panda

Delivery

- Spear phishing
- Compressed Archive – Zip file
  - Zip file -> Legitimate App, DLL loader (embedded payload)
  - Zip file -> Legitimate App, DLL loader, encrypted .dat file
  - Zip file -> Legitimate App, DLL loader, encrypted .dat file, .lnk file
- DLL side-loading, hijacking

Mustang Panda

Callback Shellcode Injection - <API Name>(Callback, dwFlags)

Likely used to evade detection – Good examples can be found here:

- https://github.com/ChaitanyaHaritash/Callback_Shellcode_Injection/tree/main

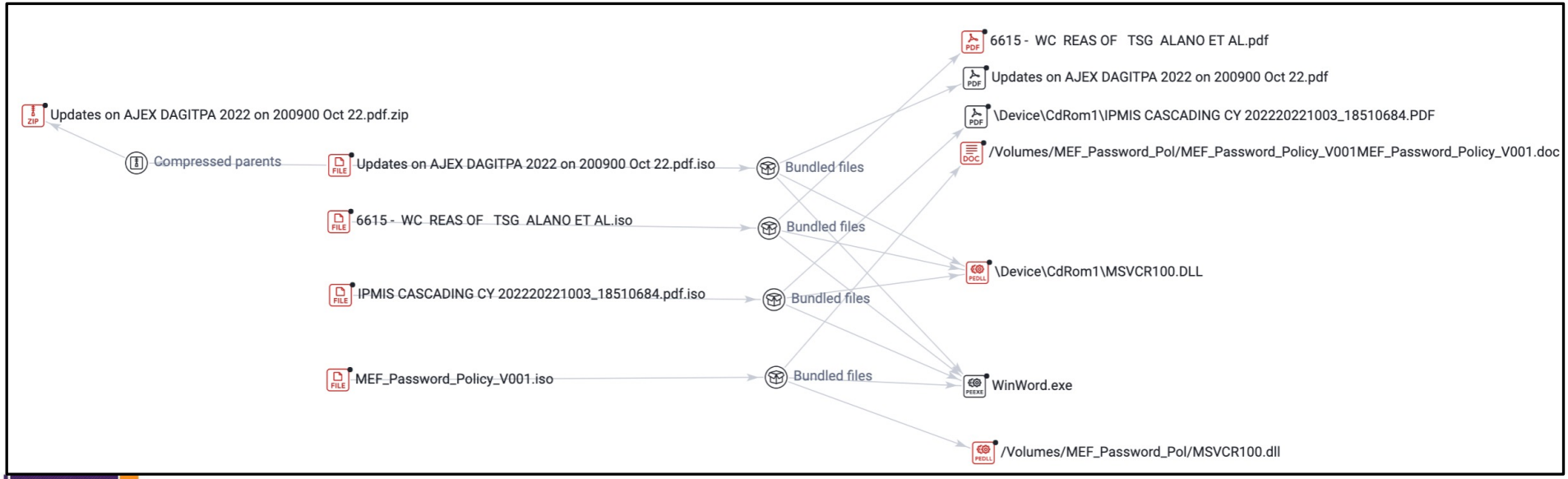
February 2022 – May 2023

2022-03-13	Log.dll	Direct Call to Decrypted Shellcode
2022-08-04	AcroDistDLL.dll	EnumThreadWindows(Shellcode)
2022-08-17	AcroDistDLL.dll	EnumThreadWindows(Shellcode)
2022-10-05	AcroDistDLL.dll	EnumSystemCodePagesW(Shellcode)
2022-10-25	ClassicExplorer32.dll	EnumSystemCodePagesW(Shellcode)
2022-11-21	LMIGuardianDLL.dll	EnumSystemCodePagesW(Shellcode)
2022-11-21	LMIGuardianDLL.dll	EnumSystemCodePagesW(Shellcode)
2022-11-23	LMIGuardianDLL.dll	EnumSystemCodePagesW(Shellcode)
2022-12-05	LMIGuardianDLL.dll	EnumSystemCodePagesW(Shellcode)
2022-12-27	LMIGuardianDLL.dll	Direct Call to Decrypted Shellcode
2022-12-29	LMIGuardianDLL.dll	Direct Call to Decrypted Shellcode
2023-01-03	LMIGuardianDLL.dll	Direct Call to Decrypted Shellcode
2023-04-11	SolidPDFCreator.dll	CryptEnumOIDInfo(Shellcode)
2023-04-20	SolidPDFCreator.dll	Direct Call to Decrypted Shellcode
2023-04-25	SolidPDFCreator.dll	Direct Call to Decrypted Shellcode
2023-04-27	SolidPDFCreator.dll	Direct Call to Decrypted Shellcode
2023-05-24	SolidPDFCreator.dll	Direct Call to Decrypted Shellcode

Dark Pink/Saaiwc Group

Delivery

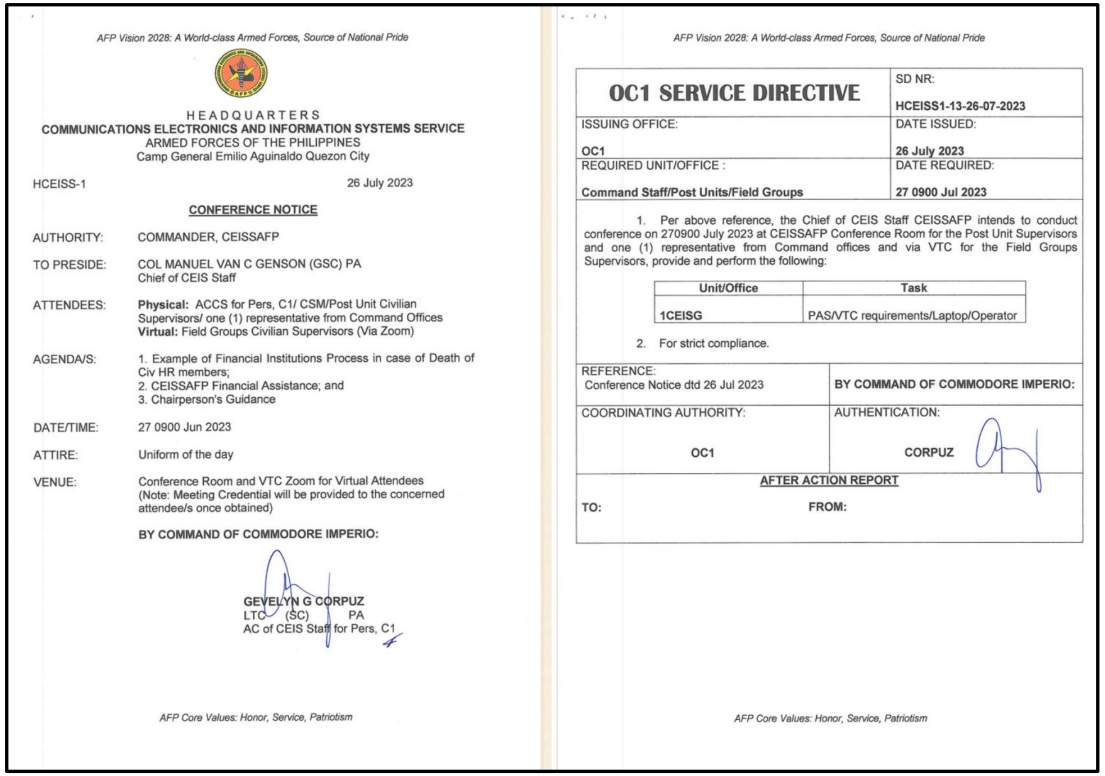
- Military & Government themed lures
- Targets Cambodia, Indonesia, Malaysia, the Philippines, and Vietnam



Dark Pink/Saaiwc Group

Delivery

- Spear phishing
- Compressed Archive – Zip files
- ISO file usage
- DLL Side-loading/hijacking



AFP Vision 2028: A World-class Armed Forces, Source of National Pride

HEADQUARTERS
COMMUNICATIONS ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo Quezon City

HCEISS-1 — 26 July 2023

CONFERENCE NOTICE

AUTHORITY: COMMANDER, CEISSAFP

TO PRESIDE: COL MANUEL VAN C GENSON (GSC) PA
Chief of CEIS Staff

ATTENDEES: **Physical:** ACCS for Pers, C1/ CSM/Post Unit Civilian Supervisors/ one (1) representative from Command Offices
Virtual: Field Groups Civilian Supervisors (Via Zoom)

AGENDA/S: 1. Example of Financial Institutions Process in case of Death of Civ HR members;
2. CEISSAFP Financial Assistance; and
3. Chairperson's Guidance

DATE/TIME: 27 0900 Jun 2023

ATTIRE: Uniform of the day

VENUE: Conference Room and VTC Zoom for Virtual Attendees
(Note: Meeting Credential will be provided to the concerned attendee/s once obtained)

BY COMMAND OF COMMODORE IMPERIO:

GEVELYN G CORPUZ
LTC (SC) PA
AC of CEIS Staff for Pers, C1

AFP Core Values: Honor, Service, Patriotism

AFP Vision 2028: A World-class Armed Forces, Source of National Pride

OC1 SERVICE DIRECTIVE | SD NR: **HCEISS1-13-26-07-2023**

ISSUING OFFICE: **OC1** | DATE ISSUED: **26 July 2023**

REQUIRED UNIT/OFFICE : **Command Staff/Post Units/Field Groups** | DATE REQUIRED: **27 0900 Jul 2023**

1. Per above reference, the Chief of CEIS Staff CEISSAFP intends to conduct conference on 270900 July 2023 at CEISSAFP Conference Room for the Post Unit Supervisors and one (1) representative from Command offices and via VTC for the Field Groups Supervisors, provide and perform the following:

Unit/Office	Task
1CEISG	PAS/VTC requirements/Laptop/Operator

2. For strict compliance.

REFERENCE: Conference Notice dtd 26 Jul 2023 | **BY COMMAND OF COMMODORE IMPERIO:**

COORDINATING AUTHORITY: **OC1** | AUTHENTICATION: **CORPUZ**

AFTER ACTION REPORT

TO: FROM:

AFP Core Values: Honor, Service, Patriotism

Dark Pink/Saaiwc Group

Delivery

← **Post**

Ginkgo
@ginkgo_g

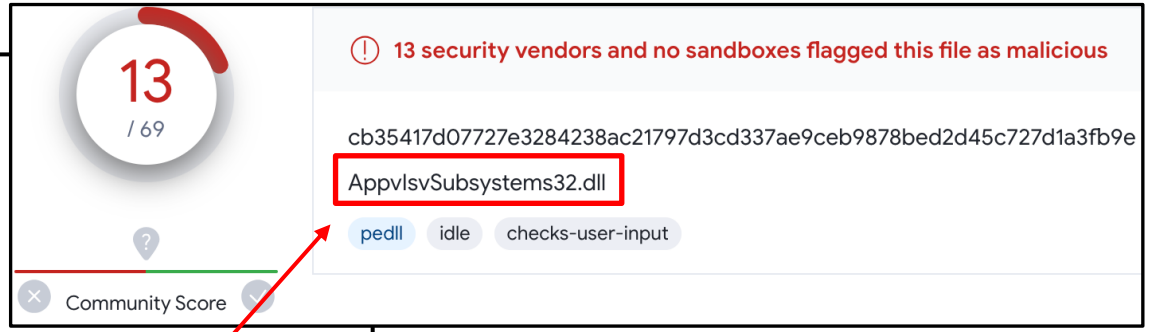
#Saaiwc #DarkPink #APT

ISO File: 53472EC4AF7C51CDAC5DFFCD7125101C

ZIP->ISO->PDF/EXE/DLL

DLL: 765F2EEB86C1307F442A267E80AF5B32

Using DLL sideloading as usual, and target the Armed Forces of The Philippines



APT29

Delivery

- Spear phishing
- PDF with embedded JavaScript
- DLL Hijacking requires a legitimate application and DLLs – that won't draw much attention

Hashes	ae79aa17e6f3cc8e816e32335738b61b343e78c20abb8ae044adfeac5d97bf70
File name,	**mso.dll**
File Path,	C:\Windows\Tasks
Weapon Type	Downloader
Hashes	4da57027ffe7e32c891334d6834923bc17e4174c53ace4ff69de6410c24d84cb
File name,	**AppVIsvSubsystems64.dll**
File Path,	C:\Windows\Tasks
Weapon Type	DUD File – Included as a dependency for MsoEV.exe
Hashes	06cea3a5ef9641bea4704e9f6d2ed13286f9e5ec7ab43f8067f15b5a41053d33
File name,	**MsoEV.exe**
File Path,	C:\Windows\Tasks
Weapon Type	Legitimate Application – Sideloads the malicious Mso.dll

```
<<
/Type /Action / S / JavaScript / JS(this.exportDataObject({cName: 'Invitation_Farewell_DE_EMB.html', nLaunch: 2,});)
>>
```

APT29

Delivery

1. HTML Smuggling
2. Zip Archive
3. HTA
4. Drop 4 binaries
5. DLL Side-loading/hijacking

```
<!DOCTYPE html>
<html>
<head>
<title>Invitation_Farewell_DE_EMB</title>
</head>
<body>
<script>


var d = [80,75,3,4,20,3,0,[Redacted] 0,0,0,0,1,0,1,0,112,0,0,0,9,71,1,0,0,0];

var e = new Uint8Array(d);
var f = new Blob([e], {type: "application/zip"});

var fileName = 'Invitation_Farewell_DE_EMB.zip';

if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(f,fileName);
} else {
    var a = document.createElement('a');
    document.body.appendChild(a);
    a.style = 'display: none';

    var url = window.URL.createObjectURL(f);
    a.href = url;
```

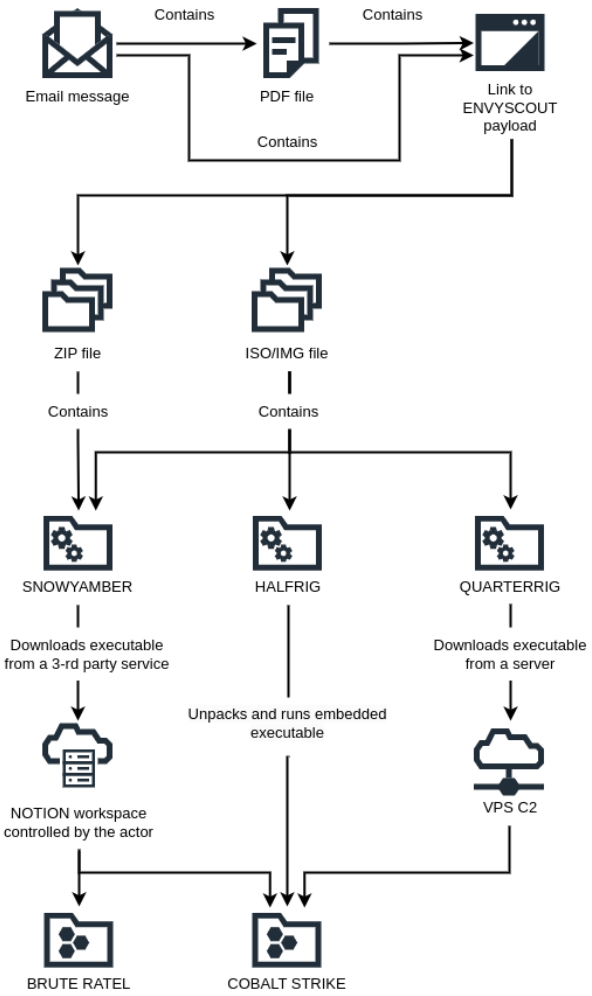
Obfuscated Files or Information: HTML Smuggling	APT29 has embedded an ISO file within an HTML attachment that contained JavaScript code to initiate malware execution.[36]

APT29

Delivery

Why ISOs?

- When opened ISOs are automatically mounted in the file system
- Once mounted the contents are displayed in Windows Explorer.
- Some ISO files don’t carry mark-of-the-web



Ref: https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services

Unknown Actor Targeting South Korea

Delivery

Target – South Korea

- Royal Road RTF document

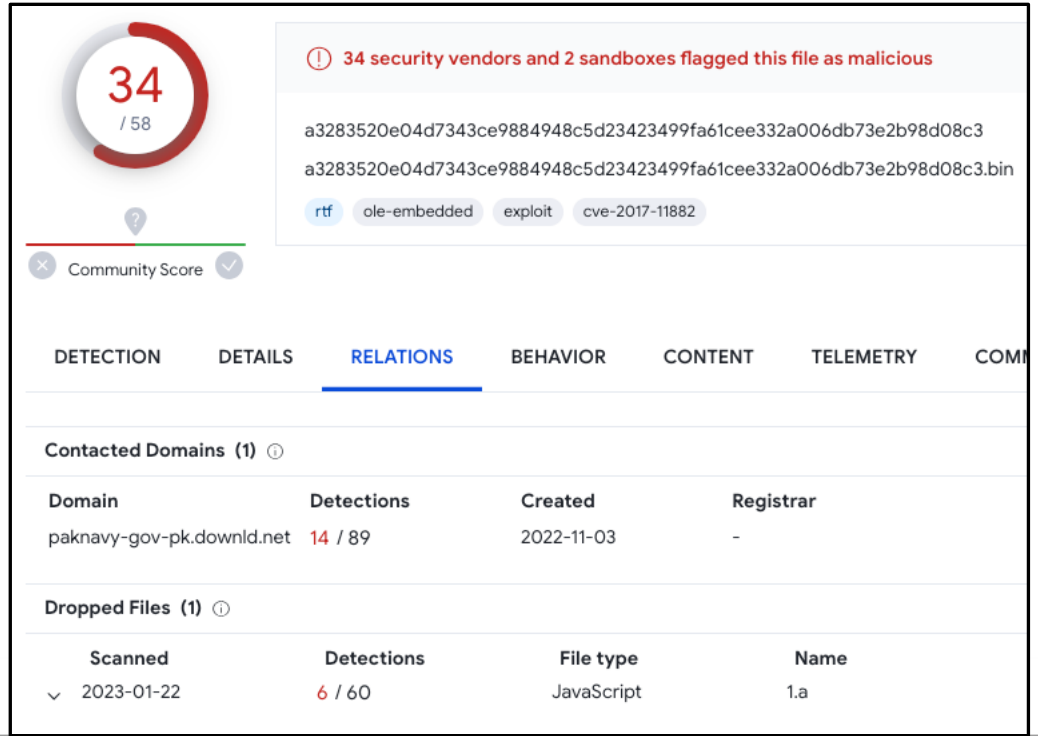
- Checks for analysis tools
- Checks if *%COMPUTERNAME%* contains “GOV”
- If it’s operating on a GOV computer -> Download a PS1 file
- powershell -executIonpolIcy byPAss -w hidden -noexit -file

- Check for AV
- Download a tool used for espionage

Sidewinder

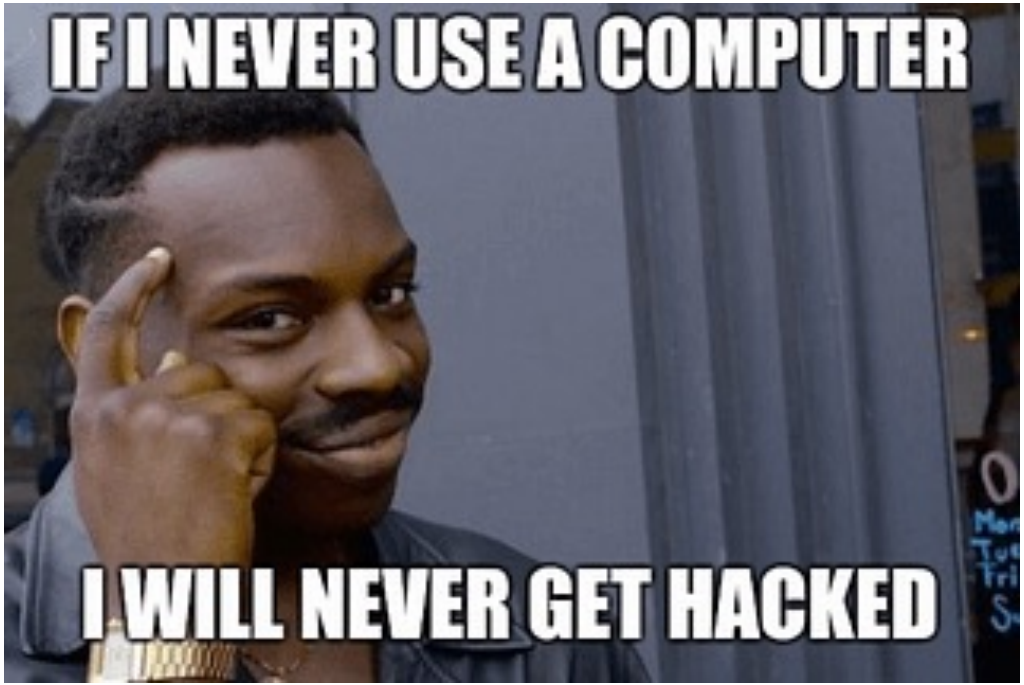
Targeted Attack Against Pakistan Government Officials

- Government/Military themed lures
- Seen previously targeting Pakistan, Afghanistan, China, and Nepal.
- RTF -> Java Script -> DLL
- Sidewinder also utilizes DLL hijacking/sideloading



Mitigations

Mitigations



Mitigations

Initial Access

- Email gateway solution to help prevent phishing and spam emails as an infection vector
- Attachment filtering
- Web Filtering and URL Scanning
- EDR rules for file creation events *zip, rar, 7z, iso, img, vhd, pdf, docx, rtf, xlsx, hta, js, lnk, vbs, chm etc.*.
  - Chain logic to not completely block normal user behavior.
  - E.g {PDF | Docx | Xlsx} -> creating a {.zip | .iso | .lnk | .img etc..} file

Mitigations

Vulnerabilities

- Patch Management

**ACSC Brief Collateral Advice*

- High priority targets should be considered higher priority for patching
  - DC's
  - Auth Sources (ADFS, Certificate Services, SSO servers etc)
  - Jump Boxes
  - Supporting Infra (ESX/Hyper V)
  - Exchange
  - Internet Facing systems

Mitigations

Brute Force

- Multi-Factor Authentication (MFA)
- Credential Hygiene
- Account Lockouts
- Strong Password Policies
- Rate Limiting
- Deep Web Intelligence Services/HaveIBeenPwned Service

Mitigations

Ransomware

* Profit driven/easy profits - security hardening might disrupt them enough to move on

- Segmentation of networks
- Comprehensive backup solution.
- Security awareness training
- Good cyber-hygiene practices

Good Reference: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Mitigations

Other

- Blocking the ability to mount disk images on the file system.
- API telemetry for callback shellcode injection - depends on your threat model (resource intensive)
- Detection rules for DLL side-loading/hijacking scenarios (Difficult - FP prone)
  - Zip -> File Creation {.exe and .dll} in {Temp | AppData | ProgramData | Downloads}
  - Process Start and Module Load
  - Great Resource from BinaryDefense

Resources

Additional Links

- Nao-sec Roayl Road Tracking spreadsheet
- Cert.PLs APT 29 Report
- Dark Pink targeting Philippines,
- Callback shellcode injection examples
- Sidewinder targeting Pakistan
- CERT.NZ - https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/
- Binary Defense - DLL Hijacking/Sideloading/Proxying detection
- https://twitter.com/ginkgo_g
- LAB 52 write up on Mustang Panda targeting Australia
- NCSC Ransomware Ecosystem
- DarkFeed Twitter
- Virus Total Trends Report
- Any.Run Malware tracker
- RedCanary Initial Acces Tradecraft & zip TLD

Credits

- Masaki Kasuya, Principal Threat Researcher, Japan
- Dean Given, Senior Threat Researcher, Ireland
- Jacob Faires, Senior Threat Researcher, US

AISA

THANK YOU