Christian Taillon ☕

ARIZONA CYBER THREAT RESPONSE ALLIANCE
ACTRA

From Threat Intel Feed Fatigue to Threat-Informed Defense Decisions

How Communities Design the Wheel Once

CYBER SOUTHWEST

10th Annual Cyber Southwest

NDIA Southwest

TUCSON CHAPTER AFCEA

AZ CYBER initiative

SSE

Christian Taillon

Grand Canyon Education

IT Security Engineer

Arizona Cyber Threat Response Alliance

Threat Intelligence Director

Dark Roast Cyber

Principal Consultant

Engineering (build)

Architecture (design)

Consulting (advisory)

The Isolated Defender:

Trying to stay left of boom

Every Bad Day's Critical Decision:

- Alert on DC—Domain Admin privileges
- DCSync stopped in progress
- VirusTotal and Enrichment provides no context on indicators
- Files executed—unclear what's malware and what's not
- Malware Sandbox: "40/100 suspicious"

Boss asking: Report? Call IR? Is this reportable (CMMC/DFARS)?

Every Good Day's Simple Question:

Where do I apply time and attention (today|this week|this month)?

Bottom line: Defenders are often alone with partial information making high stakes decisions that have rippling impact.

Adversaries Evolved from this…

Nearly a **Hundred** Named Adversaries

Hundreds of **Tools**

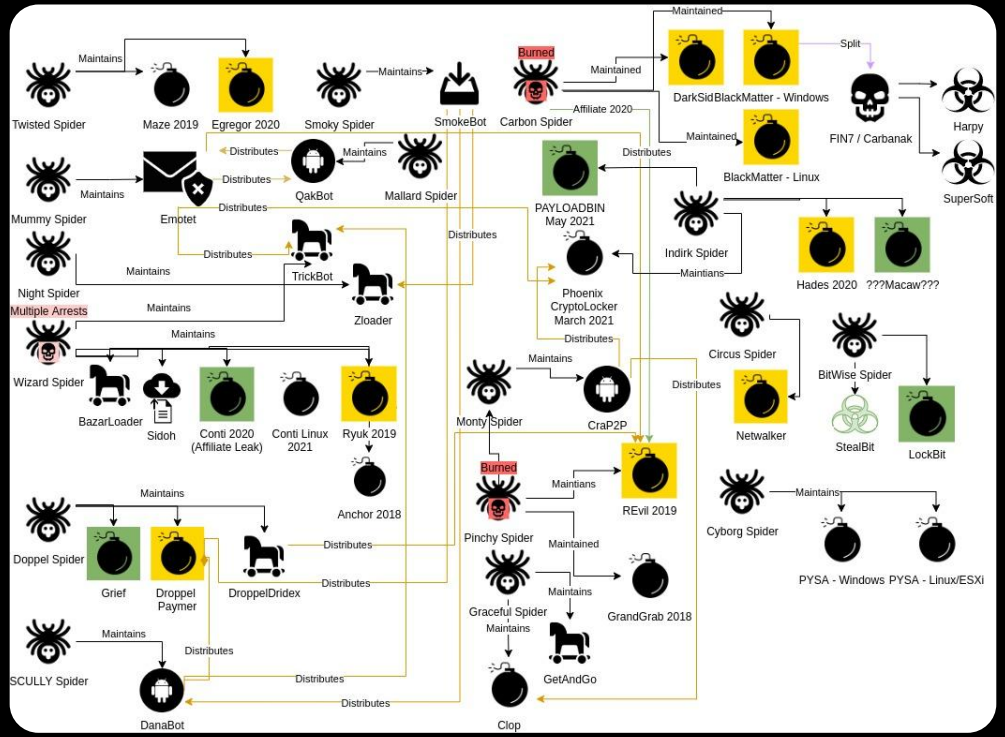
Long Lived **MO**

Long Lived **Collaboration**

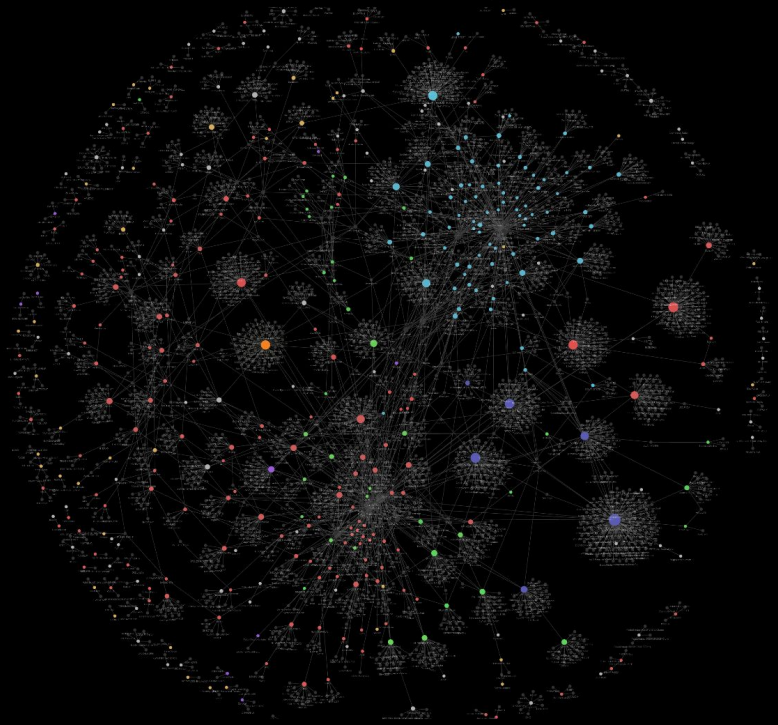
Low **OpSec**

Developing **Service Models**

Public **Dark Web Forms**



.... to this



Thousands of **Named Adversaries and Intrusion Sets**

Thousands of **Tools**

Adaptive (**exploit kit, pocs, services**)

Large Service and **Tool Marketplace**

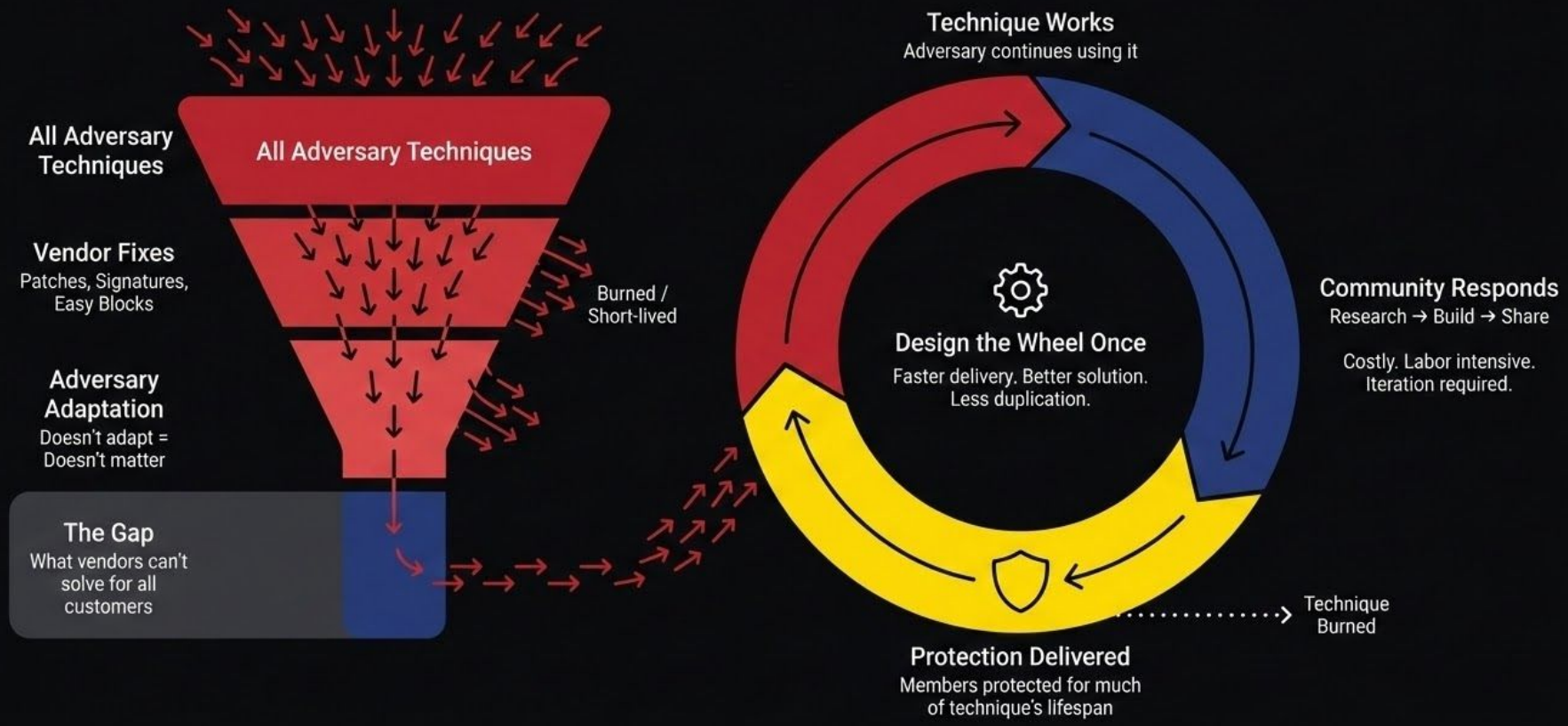
Higher **OpSec**

Mature **Services** Models

More **Private Chats and Forms**

XaaS exploits the division of labor.

The gap is where your effort—and your community—matters.



We Optimized for the Wrong Thing

TTPs: Infinite complexity; spans millions of behavioral scenarios.

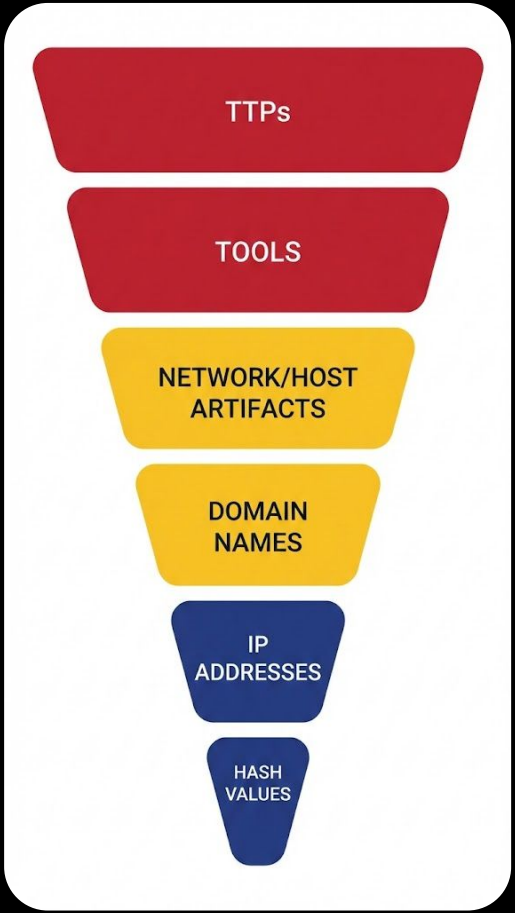
Tools: Dual-use dilemma; legitimate utilities cannot simply be blocked.

Artifacts: Fragmented; logic depends on vendor-specific syntax.

Domain Names: Ambiguous; requires investigation into hosting and intent.

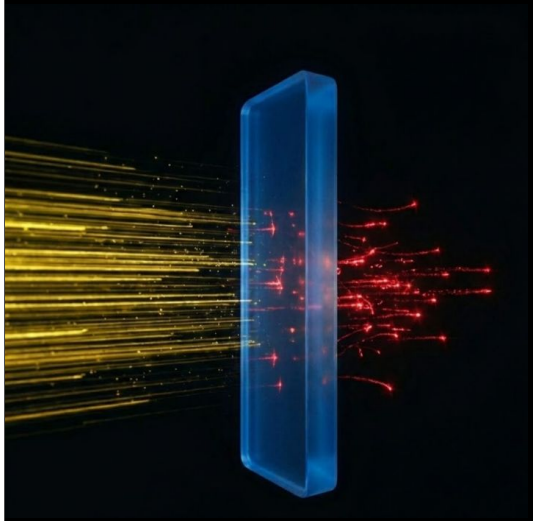
IP Addresses: High maintenance; risky to block without context.

Hash Values: Trivial automation; agents handle 10,000+ instantly.



David J. Bianco in **2013**

Technique Mitigation

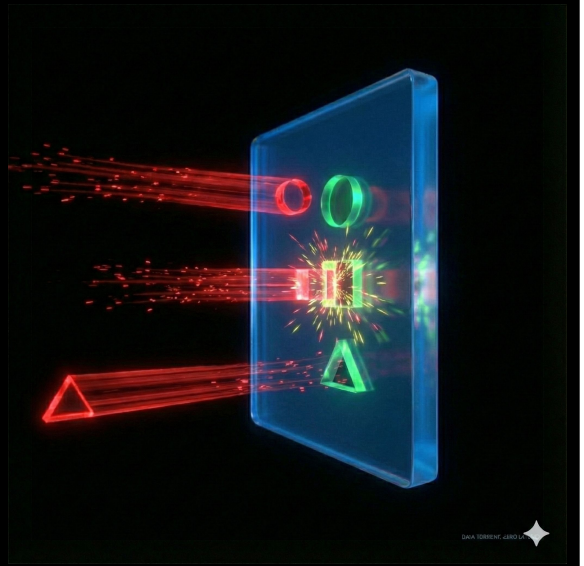


Don't Stop the Feed: Indicator sharing works. It stops the noisy attacks.

The Reality: It's ephemeral. The adversary changes the (IP|CVE|Domain|Command); the threat lives on.

The Missing Piece: Vendors can't block admin tools & blocking infrastructure can't block intent.

Response-Driven: Sharing the *human* analysis that closes the gap.



Automate the Ephemeral, Collaborate on the Gap

Technical Logic to Enforced Policy

Policy Enforcement

Content: blocking unapproved services globally.

Example: Restricting MegaSync or personal cloud storage at the firewall.

Configuration Standards

Content: Reducing attack surface via access control.

Example: Limiting GitHub downloads to Developer roles only.

Behavioral Detection

Content: Alerting on "known good" tools used badly.

Example: Logic to detect RMM tools executing dropped .dll files.

Workforce Awareness

Content: Targeted communication to high-risk teams.

Example: Specific alerts to HR regarding malicious foreign remote IT worker applicants.

Share the remedy, not just the symptom.

Where the rubber hits the road.

The "Ghost" Payload: DarkGate & AutoIT

The Incident

The Anomaly Dynamic Sandbox "Suspicious" (40/100). VirusTotal: 0/60 Clean. ML Detection: None.

The Confusion Code looked like junk variables. No C2 signatures.

The Spark Community Member: *"Wait... is that AutoIT?" We've seen that to.*

The Verdict: DarkGate Abusing a 1999 tool to defeat 2025 AI.

AutoIT Scripting

Legitimate scripting language for automating Windows GUI. Used by Help Desks globally and IT Admins.

The AutoIT Blind Spot

Easy to Obfuscate: Trivial to hide malicious logic in "noise".

Compiled binaries of malware written in AutoIT compiled were rare.

Script + Valid Interpreter

EDRs inspect .js, .ps1 & .py, etc.

They often ignore .au3 scripts.

AutoIT for Defense Evasion (T1027)

Agent Tesla

A deeply entrenched RAT and InfoStealer, often used in Business Email Compromise (BEC) campaigns targeting corporate finance sectors.

AutoIT for Evasion via Hollowing.

RedLine Stealer

The most popular "Stealer-as-a-Service" for grabbing passwords, cookies, and crypto wallets. It is frequently distributed as "cracked software" or game cheats.

AutoIT for Evasion via Packing/Crypting.

FormBook / XLoader

A resilient infostealer and veteran of malspam campaigns. Its AutoIT scripts are notorious for being filled with functional "junk code" designed to frustrate analysts.

AutoIT for Evasion via Anti-Analysis.

Lumma Stealer

A rising modern threat aggressively targeting crypto and corporate credentials. It uses social engineering tactics like fake "Google Chrome Update" errors & ClickFix.

AutoIT for Evasion via legitimate signed binaries.

BypassIT Public

Unwatch 3 | Fork 14 | Starred 43

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

CroodSolutions Update README.md e714132 · 3 months ago 109 Commits

1 - Covert Malware Delivery and Ingress Tool ...	Create readme.md	last year
2 - Discovery	Update DiscoverPortScanner.au3	last year
3 - Defense Evasion	Create NTDLL_Modification.au3	10 months ago
4 - Privlege Escalation	Delete 4 - Privlege Escalation/ReadMe.md	last year
5 - Peristence	Add files via upload	last year
6 - Credential Access	removed unnecessary files.	last year
7 - Lateral Movement	Script to Download and install Putty	last year
8 - Command and Control	Delete 8 - Command and Control/Placeholder.txt	last year
9 - Impact	removed unnecessary files.	last year
Detection	moved content within repo	9 months ago
.gitignore	updated gitignore	last year
.gitmodules	moved content within repo	9 months ago
LICENSE	Initial commit	last year
README.md	Update README.md	3 months ago

README | GPL-3.0 license

BypassIT

About

BypassIT is a framework for covert malware delivery and post-exploitation using AutoIT for red / blue team self assessment.

autohotkey | ahk | autoit | blueteam | redteam | purpleteam | lotl | defcon32 | selfassessment | cactuscon | bypassit

Readme
GPL-3.0 license
Activity
43 stars
3 watching
14 forks
Report repository

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Contributors 8

BEACONATOR
EVADE. EDUCATE. ITERATE.

Crowdsource the research, analysis, required to formulate a long term response.

- Ideas
- Observations
- Challenges
- Tools

THREAT INTELLIGENCE SUPPORT UNIT
ARIZONA CYBER THREAT RESPONSE ALLIANCE

BypassIT Public

Unwatch 3 | Fork 14 | Starred 43

main | 1 Branch | 0 Tags | Go to file | Add file | Code

CroodSolutions Update README.md e714132 · 3 months ago 109 Commits

1 - Covert Malware Delivery and Ingress Tool ...	Create readme.md	last year
2 - Discovery	Update DiscoverPortScanner.au3	last year
3 - Defense Evasion	Create NTDLL_Modification.au3	10 months ago
4 - Privlege Escalation	Delete 4 - Privlege Escalation/ReadMe.md	last year
Detection	moved content within repo	9 months ago
.gitignore	updated gitignore	last year
.gitmodules	moved content within repo	9 months ago
LICENSE	Initial commit	last year
README.md	Update README.md	3 months ago

```
; Generate a strong random password (16 characters)
Local $password = ""
Local $chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()_+-=[]{}|;:,.<>?"
For $i = 1 To 16
    $password &= StringMid($chars, Random(1, StringLen($chars), 1), 1)
Next
```

README | GPL-3.0 license

BypassIT

About

BypassIT is a framework for covert malware delivery and post-exploitation using AutoIT for red / blue team self assessment.

autohotkey | ahk | autoit | blueteam | redteam | purpleteam | lotl | defcon32 | selfassessment | cactuscon | bypassit

Readme

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Contributors 8

BEACONATOR
EVADE. EDUCATE. ITERATE.

Crowdsource the research, analysis, required to formulate a long term response.

- Ideas
- Observations
- Challenges
- Tools

THREAT INTELLIGENCE SUPPORT UNIT
ARIZONA CYBER THREAT RESPONSE ALLIANCE

BypassIT Public

Unwatch 3 | Fork 14 | Starred 43

main | 1 Branch | 0 Tags | Go to file | Add file | Code | About

CroodSolutions Updat

1 - Covert Malware D
2 - Discovery
3 - Defense Evasion
4 - Privlege Escalatio
5 - Peristence
6 - Credential Access
7 - Lateral Movemen
8 -
9 -
Detection
.gitignore
.gitmodules
LICENSE
README.md

framework for covert
y and post-exploitation
ed / blue team self

autoit | blueteam | lotl | defcon32 | bypassit

```
Function to recursively encrypt files in a directory
Func EncryptFiles($directory)
    Local $search = FileFindFirstFile($directory & "\\*")
    If $search = -1 Then
        LogMessage("No files found in: " & $directory)
        Return 0
    EndIf

    Local $file, $filePath, $encryptedCount = 0

    $filePath = $directory & "\\" & $file

    ; If it's a directory, recursively encrypt its contents
    If StringInStr(FileGetAttrib($filePath), "D") Then
        $encryptedCount += EncryptFiles($filePath)
        ContinueLoop
    EndIf
```

README | GPL-3.0

BypassIT

TLDR; AutoIT that should have been caught wasn't

BEACONATOR
EVADE. EDUCATE. ITERATE.

Crowdsource the research, analysis, required to formulate a long term

s
ervations
- Challenges
- Tools

THREAT INTELLIGENCE SUPPORT UNIT
ARIZONA CYBER THREAT RESPONSE ALLIANCE

Community crowdsourced & shared **solutions**.

No rocket science or new products. One org packages up what they did for others to do also.

Started as an email chain, a few chats, and resulted in a github.

🚀 Why AutoIt Detection Matters

The Threat Landscape

AutoIt has become a **favorite tool** among threat actors, particularly in campaigns like:

- **Darkgate Malware** (Dec 2023) - Used AutoIt for initial access and execution
- **Ransomware Operations** - Leveraged for encryption and lateral movement
- **APT Campaigns** - Utilized for persistence and data exfiltration

Detection Challenges

- ⚠️ **Legitimate Usage** - AutoIt is widely used in IT automation
- 🎭 **Evasion Techniques** - Renamed executables, obfuscated scripts
- 🔍 **File Extension Independence** - Scripts can run without `.au3` extensions
- 🛡️ **Encoded Content** - Encrypted or encoded script payloads

---

📁 Detection Rules

🔧 Core Detection Rules

Rule File	Detection Focus	Severity	Status
`Basic AutoIT Exec.yaml`	Renamed AutoIt executables	🔴 High	Experimental
`AutoIt Scripting Activity Detection...`	Comprehensive command-line patterns	🟡 Low	Experimental
`AutoIt Strings Detection.yaml`	File content string analysis	🟡 Low	Experimental
`Detect AU3 EA06 String.yaml`	AU3!EA06 signature detection	🟡 Low	Experimental
`Renamed AutoIT Exec.yaml`	Executable name evasion	🔴 High	Experimental

🎯 Key Detection Capabilities

How Hackers Hide Malicious AutoIT Scripts:

File Extension Spoofing

Steganography

Archive Embedding

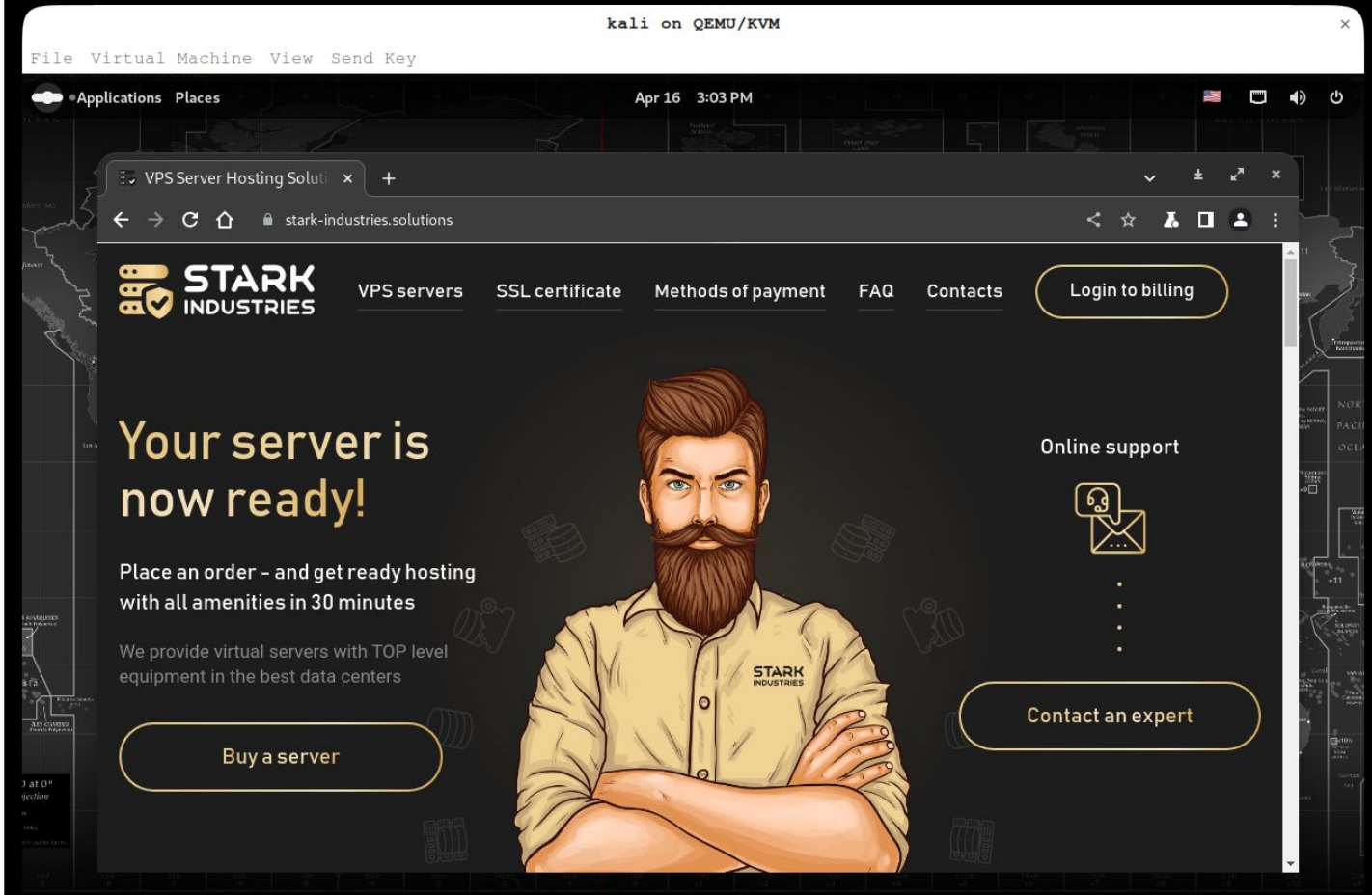
Polyglot Files

Custom File Formats

Base64 Encoding

Comment Injection

Executable Packers



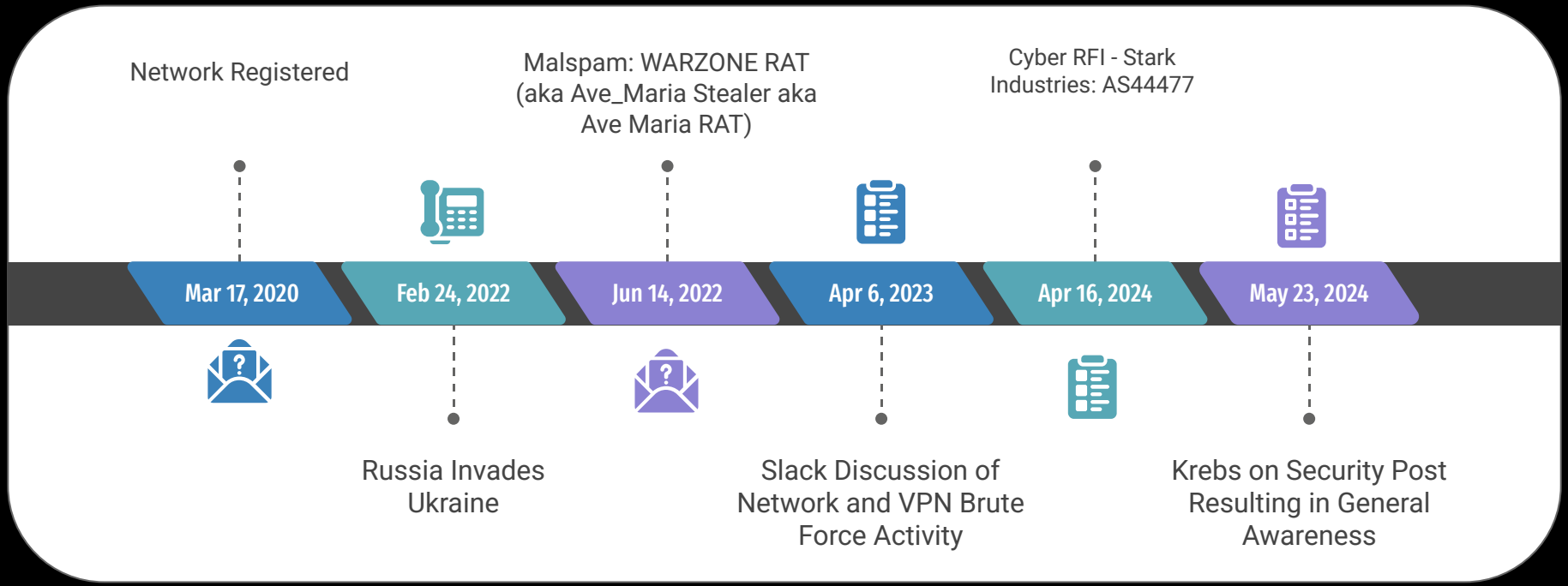
Stark Industries AS44477: Politically Motivated DDoS (Hacktivism)

Primary Actor: Pro-Russian group *NoName057(16)*.

Mechanism: Hosts the DDOSIA crowdsourced toolkit, enabling volunteers to attack NATO, Ukrainian, and European targets.

The "Gap": feeds flag individual attacking IPs but miss the forest through the trees.

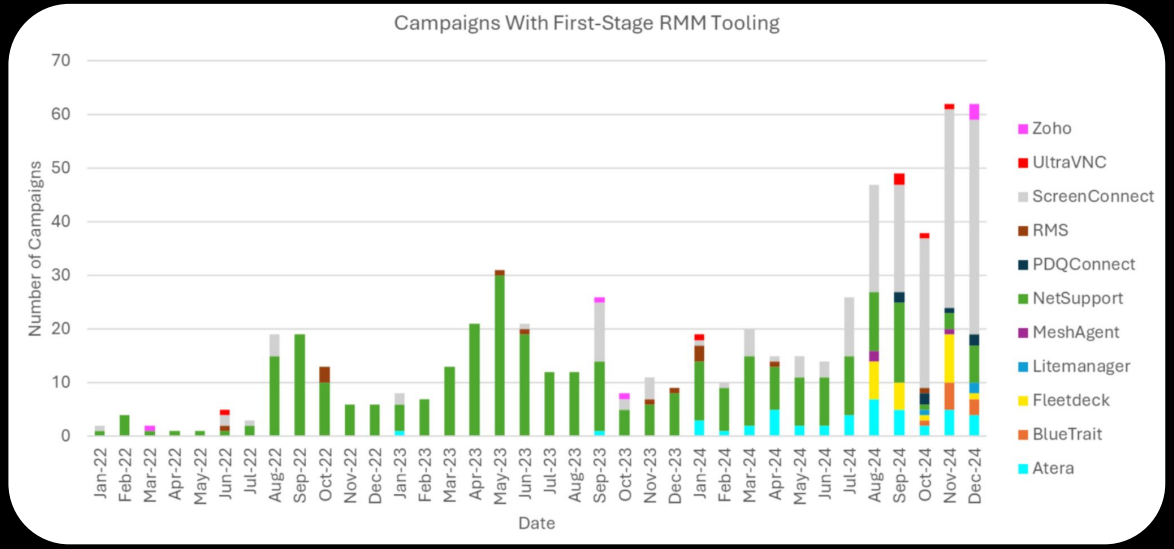
ASN44477 Stark Industries Solutions



The RMM Dilemma (Strategic)

Community Member A: They gave us a bad day, and they didn't use C2, they just used ScreenConnect.

The Mandate: "We only use AnyDesk. Lest block everything else".



The High Cost of distinguishing "Admin" *from* "Adversary"

March 07, 2025 Ole Villadsen, Selena Larson, and The Proofpoint Threat Research Team

The RMM Dilemma (Strategic)

Operational / Engineering Team Burden:

The Problem: "To block 'everything else,' you must define 'everything else'."

The Scope: 284 documented tools (Source: *LOLRMM.io*).

The Obstacles:

- **Signature:** Valid, Trusted, Signed.
- **Network:** Custom protocols over common ports.
- **Shadow IT:** "Allowed" = "In Use."

Contextually Permission

- ❑ Remote Workforce
- ❑ Server Data Decent
- ❑ Office Spaces
- ❑ Cloud Environments

LOLRMM

README.MD Added CrowdStrike resources 8 months ago

README GPL-3.0 license

AutoRMM

---What is AutoRMM?---

AutoRMM is a testing and red teaming framework we are building out, for covertly delivering and installing Remote Management and Screen Sharing tools, to begin to accurately simulate observed adversary activity in this area. This is called AutoRMM not because it does anything automatically, but because we intend to start off using AutoIT and AutoHotKey, due to the evasiveness already noted in our other projects. That said, we will not limit testing to exclusively these languages, in particular for the initial delivery and installation of RMM tools.

---How is this different from BypassIT and AutoPwnKey---

BypassIT and AutoPwnKey are h ed to improve awareness around how a wide range of tactics th s to detect, become evasive when performed natively using Aut these other projects, for AutoRMM, our goal is not to work using a given language, but instead to find out what s can be enhanced or replaced by RMM tools - and also, ex these scenarios. It is possible, even likely, features created h into these other frameworks, or that we may leverage functionality we , when building AutoRMM. That said, this framework has a different goal an , which will likely cause it to evolve in different directions.

---Why are we creating this? ---

We have noticed that adversaries are using a variety of delivery mechanisms to launch Remote Management / Screen Sharing tools, as an alternative or supplement to traditional

README GPL-3.0 license

LOLRMM Detection Resources

The Community Maturity Model

Moving from "Passive Awareness" to "Collective Action"

Made Aware

"I read the headline."

VALUE: LOW

Informed

"I read the technical report."

VALUE: LOW-MED

Testing

"I ran the emulation and understand my risk"

VALUE: MEDIUM

Learned Response

I adopted detection & dashboards or tools and verified with emulation."

VALUE: HIGH

Collective Maturity

"We standardized. Everyone imports Taking someone's response is a simple decision and easy to act on."

VALUE: MAXIMUM

Most communities stop at Stage 2. The **ROI** happens at later.
By sharing the community can progress collectively.

THE BARRIERS TO SHARING

Perceived Risks vs. Operational Reality

1. The Legal Shield

The Fear "Policy and risk forbid us from talking."

The Reality We need Detection insight, not Victim Info. TLP provides the framework and NDA's can be signed in formal communities.

2. The Reputation Trap

The Fear "Admitting we saw something implies we are weak."

The Reality Everyone is a target. Silence only protects the adversary. SOCs add value if they are responding to threats that warrant time and attention.

3. The Perfection Paradox

The Fear "We need a dedicated STIX/TAXII server to start."

The Reality Start with a screenshot in a secure chat. Don't over-engineer. Communication and community are the only dependencies.

4. The Wrong Metric

The Fear "We need to share millions of indicators to be useful."

The Reality One high-fidelity response strategy is worth 10,000 IPs. Some of these observations stop millions of attack attempts with simple responses.

The adversaries found a way to collaborate with strong OpSec, defenders need to as well. We are highly dependent on each other (supply chain).

Maximizing Community ROI

Stop Spending Human Hours on Disposable Indicators

EFFORT TO ANALYZE / SHARE

START OF KILL CHAIN

IGNORE

Custom effort for ephemeral intel.

"The threat will move before you finish writing the report."

HIGH VALUE INTEL

THE SWEET SPOT

Behavioral Logic, De-obfuscation Methods, RMM Policies.

"This is where the community lives. High cost to solve alone, massive value to share."

DISPOSABLE INDICATORS

AUTOMATE IT

IP Addresses, Hash Values, Domains, Payloads.

"Let the feeds handle this. Do not type these into a chat."

HARDENING

QUICK WINS

Simple Config Changes (e.g., "Block ASN, Block .au3 File Writes").

"High impact, low cost. Share these immediately."

THREAT LIFESPAN (SHORT LONG)

If the adversaries are using a technique for years that we can address, it's worth the days it takes to do so.

The Monday Morning...

The Question That Defines Your Week

The Challenge

We cannot hire enough analysts to solve every problem alone. Your supply chain cannot afford to solve the same problem twice.

The Action

Find your community Find the people who are doing the work, not just reading the news. We share a common enemy and don't have the luxury of time.

"What gave you a bad day this week and what did you have to do about it?"

(And how can I stop them from doing it to my neighbor?)

THANK YOU

ctaillon@actraaz.org | https://ctaillon.io