ATOMICS ON A FRIDAY
SS

Agenda

- Who are we?
  - Intros
- Purple Madness
  - Approach
- Theme: Gootloader
- Schedule
- Coming up on *Atomics On A Friday*

Who Are We?

Michael Haag

Sr. Threat Connoisseur

@M_Haggis

Paul Michaud

Principal Hunter of Threats

@Burning_PM

ATOMICS ON A FRIDAY

Who Are We?

Harrison Van Riper

Sr. Threat Connoisseur

@pseudohvr

Anton Ovrutsky

Threat Research, Team Lead

@Antonlovesdnb

Nasreddine Bencherchali

Threat Researcher

@nas_bench

ATOMICS ON A FRIDAY

Intros

- Who are you?
- What do you do?
- What's your favorite group/malware/tool?
- What’s your favorite Atomic/Technique?
- Vim vs Nano
- OST - good / bad?

March Madness

- What are we even doing here?
  - Make a threat report actionable and approachable
  - New threat report is released:
    - What do we do?
    - How do we action it?
    - What do we prioritize?
    - Common pitfalls?
- Provide perspectives from individuals with backgrounds in:
  - Cyber Threat Intelligence
  - Purple Team
  - Threat Research and Detection Engineering

Approach

Cyber Threat Intelligence

- Understanding TTPs
- Mapping/Listing TTPs for testing
- Things to look for
- Pitfalls to avoid

Purple Teaming

- Leverage TTPs from CTI
- Develop a plan
- Rip tests/Atomics
- What now?

Detecting Engineering

- Review the data from our tests
- Determine coverage
- Build detection
- Validate detection

Gootloader

Gootloader

cobaltstrike gootloader lazagne psexec

SEO Poisoning – A Gootloader Story

May 9, 2022

In early February 2022, we witnessed an intrusion employing Gootloader (aka GootKit) as the initial access vector.

The intrusion lasted two days and comprised discovery, persistence, lateral movement, collection, defense evasion, credential access and command and control ac

threat actors used RDP, WMI, Mimikatz, Lazagne, WMIExec, and SharpHound. The threat actors then used this access to re

the multi-staged payload distribution by Sophos in March 2021. The threat actors utilize SEO (search engine optimization) po

hosting malware to the top of certain search requests such as "what is the difference between a grand agreement and a con

ent?"

ses and clicks on one of the top results, they are left with a forum looking web page where the user is instructed to download

click to open). You can learn more about Gootloader by reading these references. 1 2 3 4

most recent malicious infrastructure. They

. Thank you!

BLOG

Welcome to Goot Camp: Tracking the Evolution of GOOTLOADER Operations

GOVAND SINJARI, A

JAN 26, 2023 | 16 MIN

Gootloader Malware Leads to Cobalt Strike and Hand-on-Keyboard Activity

5 MINUTES READ

SHARE:

ATOMICS ON A FRIDAY

Schedule

Friday, March 10

- Harrison Van Riper
- Cyber Threat Intelligence

Friday, March 17

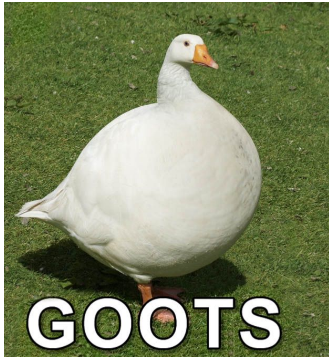
- Anton Ovrutsky
- Purple Teaming

Friday, March 24

- Nasreddine Bencherchali
- Detection Engineering

Thank you

- https://github.com/redcanaryco/invoke-atomicredteam
- http://atomicredteam.io
- https://www.mandiant.com/resources/blog/tracking-evolution-gootloader-operations
- https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
- https://github.com/Atomics-on-A-Friday



ATOMICS ON A FRIDAY