



# 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



# Who Are We?



Harrison Van Riper


**Sr. Threat Connoisseur**

 @pseudohvr



Anton Ovrutsky


**Threat Research, Team Lead**

 @Antonlovesdnb



Nasreddine Bencherchali

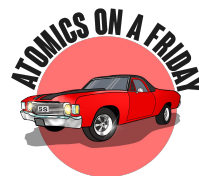
**Threat Researcher**

 @nas\_bench



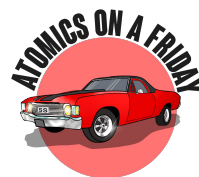
# Intros

- 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

```
// -----  
{  
  "id" : ObjectId("59cd0b81ff174b855170d58d"),  
  "localDate" : ISODate("2017-09-28T14:47:27.000+0000"),  
  "deviceName" : "SafeNet Token JC 0",  
  "eventName" : "insert_device",  
  "lastWindowName" : "Electronic Service Information System (GBGB61TS - DP2IT63) - Internet Explorer",  
  "lastProcessPath" : "C:\\Program Files\\Internet Explorer\\iexplore.exe",  
  "creationDate" : ISODate("2017-09-28T14:47:29.338+0000"),  
  "botguid" : "k1a456_4993b7a310b227023edf",  
  "__v" : 0  
}  
  
// -----  
{  
  "id" : ObjectId("59cd0c8aff174b855170d8d4"),  
  "localDate" : ISODate("2017-09-28T14:51:21.000+0000"),  
  "deviceName" : "Liteon HP Smart Card Reader 0",  
  "eventName" : "insert_device",  
  "lastWindowName" : "EMIS Web Site - 3009",  
  "lastProcessPath" : "C:\\Program Files\\Internet Explorer\\iexplore.exe",  
  "creationDate" : ISODate("2017-09-28T14:51:21.000+0000"),  
  "botguid" : "SCCEDA150289W_474caaaf4e30c9f6e8f9",  
  "__v" : 0  
}  
  
// -----  
{  
  "id" : ObjectId("59cd0ca60a84206151eaf64b"),  
  "localDate" : ISODate("2017-09-28T14:50:17.000+0000"),  
  "deviceName" : "OMNIRKEY AG Smart Card Reader USB 0",  
  "eventName" : "insert_device",  
  "lastWindowName" : "Home Page - Mediscan Diagnostic Services PRS - Google Chrome",  
  "lastProcessPath" : "C:\\Program Files (x86)\\Google\\Chrome\\Application\\chrome.exe",  
  "creationDate" : ISODate("2017-09-28T14:52:22.319+0000"),  
  "botguid" : "SCN66_4dbfa386e2c965218867",  
  "__v" : 0  
}
```

**GOOT  
LOADER**



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 access. The 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) poisoning by hosting malware to the top of certain search requests such as "what is the difference between a grand agreement and a contract?"

When a user enters a search query and clicks on one of the top results, they are left with a forum looking web page where the user is instructed to download and click to open). You can learn more about Gootloader by reading these references. [1](#) [2](#) [3](#) [4](#)

most recent malicious infrastructure. They  
Thank you!

# Gootloader

BLOG

## Welcome to Goot Camp: Tracking the Evolution of GOOTLOADER Operations

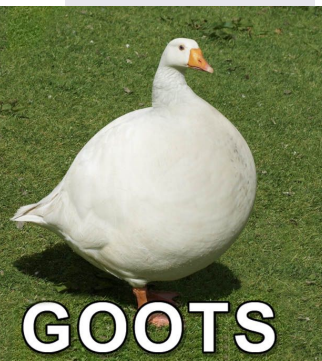
GOVAND SINJARI, A

JAN 26, 2023 | 16 MIN

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

5 MINUTES READ

SHARE:



# 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/Atoms-on-A-Friday>

