WAIT....ARE YOU REALLY HUNTING THREATS?

NATHALIE CORNEJO
BLUETEAMCON 2024

ABOUT ME

- 7+ years of experience in the cybersecurity field
- SOC analyst, Incident Response, currently leading a Threat-Hunting team
- GSEC, GCIH, GNFA, AWS CCP
- STEM volunteer, CR coffee lover

The information shared below does not represent my employer's views on this matter.

AGENDA

- What is Threat Hunting?
- Fundamental elements
- Hunting deliverables
- Artificial Intelligence in Hunting

Detect threats that our security tools miss, through proactive searches executed by humans

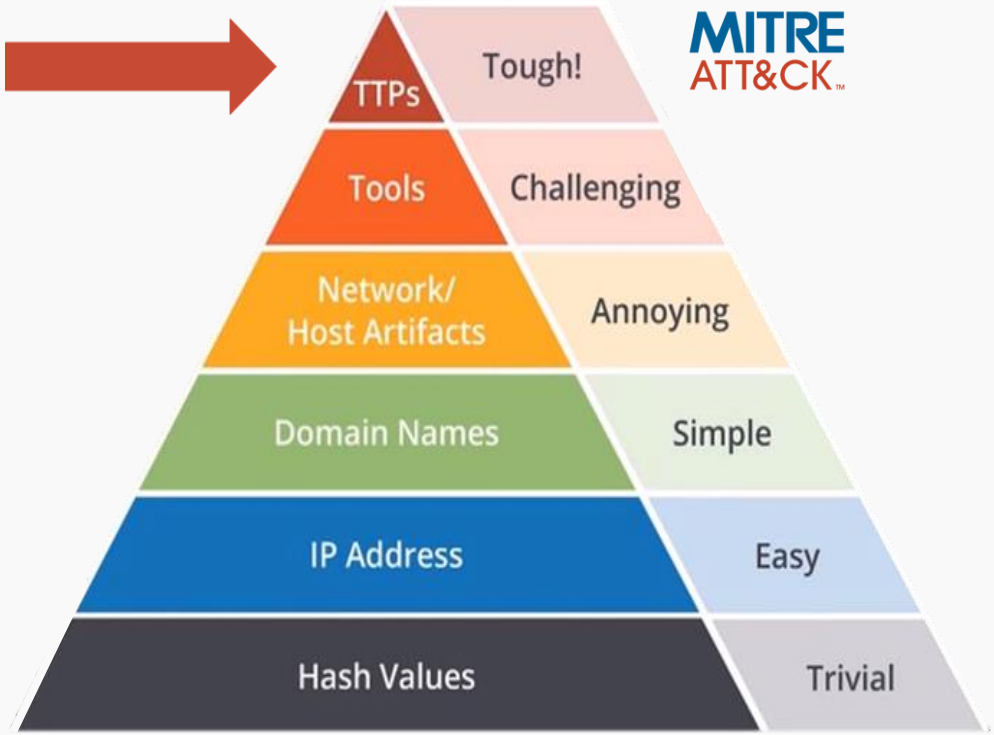
DEFINING THREAT HUNTING

Detect threats that our security tools miss, through proactive searches **executed by humans**

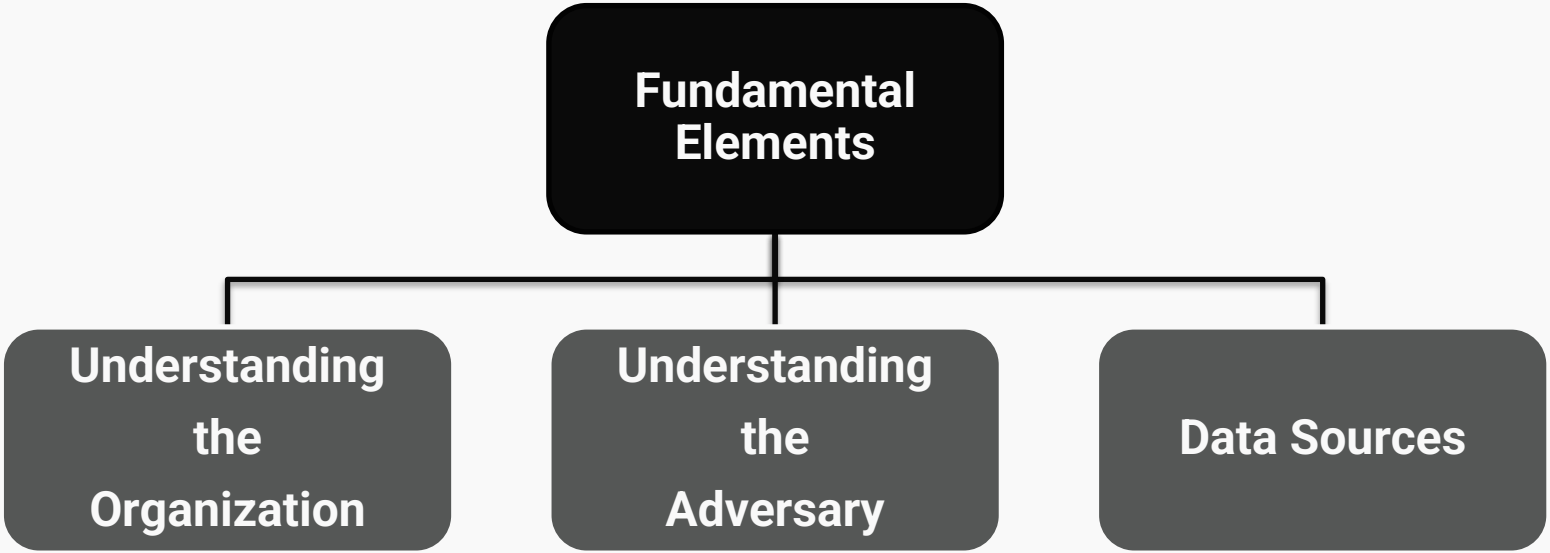
Detect threats that our security tools miss, through proactive searches executed by humans

DEFINING THREAT HUNTING

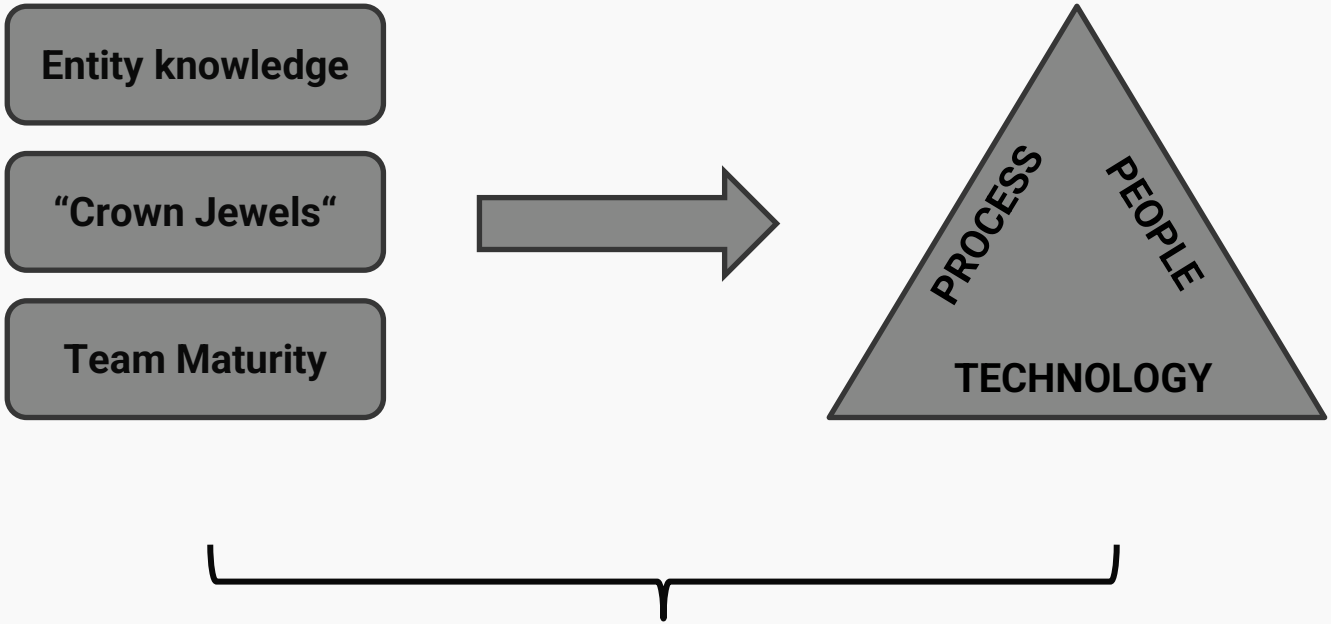
PYRAMID OF PAIN



https://www.sans.org/tools/the-pyramid-of-pain/
https://gblogs.cisco.com/ca/2020/08/26/the-canadian-bacon-cisco-security-and-the-pyramid-of-pain/


Fundamental Elements
Understanding the Organization
Understanding the Adversary
Data Sources

UNDERSTANDING THE ORGANIZATION



UNDERSTANDING THE ADVERSARY

- Targeted organizations:
  - Finance, Manufacturing, Healthcare, etc.
- TTPs associated with the adversary
  - Hunting methodologies focusing on specific threats and tools
  - Understanding the threat
- In collaboration with the CTI team (Cyber Threat Intelligence team)
  - https://thedfirreport.com/

gootloader

SEO Poisoning to Domain Control: The Gootloader Saga Continues

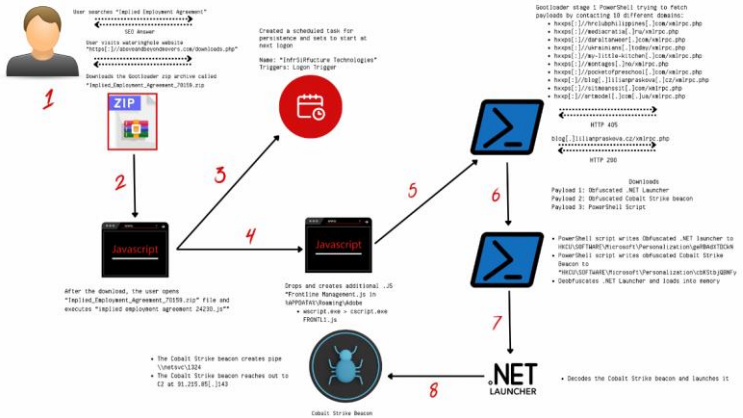
February 26, 2024

Key Takeaways

- In February 2023, we detected an intrusion that was initiated by a user downloading and executing a file from a SEO-poisoned search result, leading to a Gootloader infection.
- Around nine hours after the initial infection, the Gootloader malware facilitated the de
directly into the host's registry, and then executed it in memory.
- The threat actor deployed SystemBC to tunnel RDP access into the network, which a
backup servers, and other key servers.

Execution

Gootloader employs several executions across the whole infection chain.



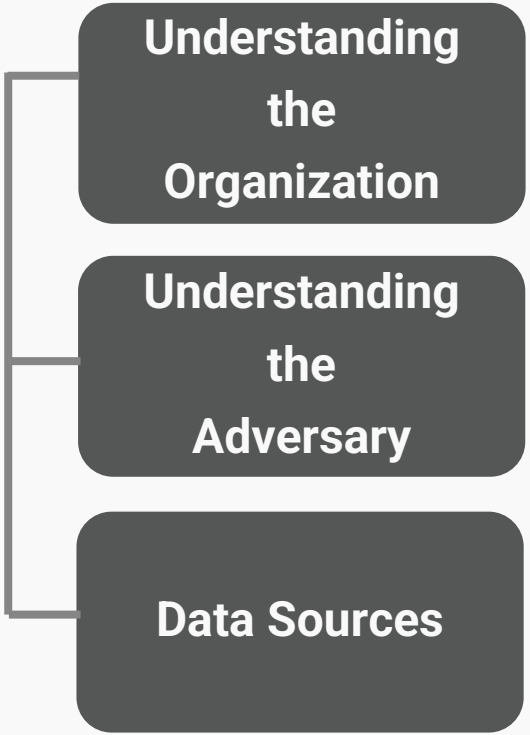
DATA SOURCES

- How much visibility do we have of the company?
- What is the data retention time?
- How long does it take to access data?
- Data Manipulation & Storage platforms :
  - Splunk, Sentinel, SOF-ELK, Elastic Stack

DATA SOURCES

Network	Devices	Internal Intelligence	External Intelligence
• Proxy • DNS • VPN • IPS/Firewall • NetFlow	• OS logs- Win/Nix* • Sysmon • Email logs • Registry	• User Roles • Assets Inventory • Installed Apps • Past Incidents	• Trustable Sources • Vendors, Community groups • Intelligence related to Threat Actors

https://chrissanders.org/training/



https://www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html

HUNTING DELIVERABLES

https://www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html

“HUNT ONCE”

01

Development of detections based on threat understanding

02

Improve visibility in the environment through new alerts and existing ones

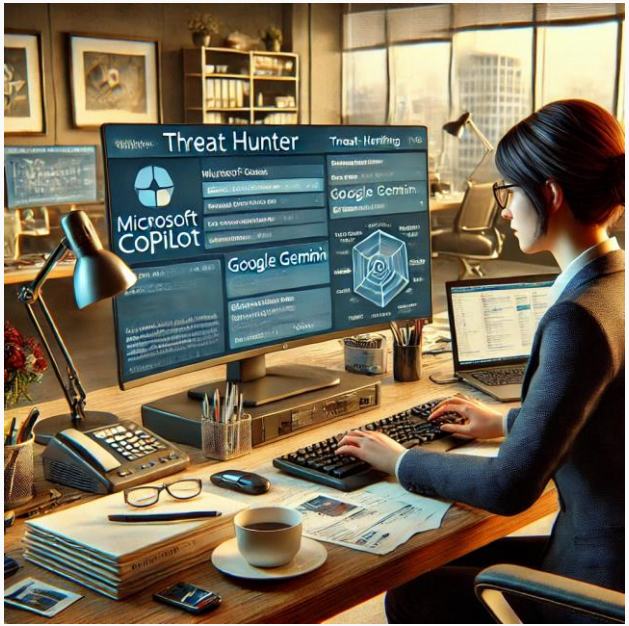
03

Mapping new and existing data sources

HTTPS://WWW.SANS.ORG/MEDIA/ANALYST-PROGRAM/BUILDING-MATURING-THREAT-HUNTING-PROGRAM-39025.PDF

ARTIFICIAL INTELLIGENCE IN HUNTING

- Data Analysis and Interpretation
- Threat Intelligence
- Collaborative problem solving
- Documentation
- Training and Education
- Custom Querying and Scripting
- And so much more….



Note: Review company policies for AI usage and double-check results (LLM Hallucinations)

USEFUL RESOURCES

- **MITRE ATT&CK FRAMEWORK**
  - https://attack.mitre.org/
- **Open Threat Hunting Framework – IBM**
  - https://github.com/TactiKoolSec/OTHF
- **Intelligence-Driven Threat Hunting Methodology** - Joe Slowik
- **Practical Threat Hunting Training –** Chris Sanders

Q & A

THANK YOU! ¡MUCHAS GRACIAS!

WWW.LINKEDIN.COM/IN/NATHALIECORNEJO/