COMMUNITY VALUE FIRST

Cybersecurity Update

23 Aug 2023

TACOMA PUBLIC UTILITIES

Agenda

- Threat Actor Deep Dive
- Cyber Threat Intelligence
- Active Threat Hunting
- Save the Date!
- Questions

Chinese 'Volt Typhoon' hack underlines shift in Beijing's targets, skills

"The PRC's goal is developing capabilities to disrupt critical infrastructure in the event of a future conflict," NSA Cybersecurity Director Rob Joyce told Breaking Defense in a statement.

By SYDNEY J. FREEDBERG JR. on June 07, 2023 at 9:42 AM

China's Volt Typhoon APT Burrows Deeper Into US Critical Infrastructure

US officials are concerned that the Beijing-directed cyberattacks could be a precursor to military disruption and broader destructive attacks on citizens and businesses.

Nate Nelson
Contributing Writer, Dark Reading

July 31, 2023

Cyber Threat Intelligence Sources

TPU's Cybersecurity and NSOC teams consume threat feeds from a variety of industry-leading sources. Several are general-purpose, covering a broad array of threats while others are targeted toward threats to critical infrastructure. These sources, combined with open-source intelligence, paint an accurate picture of the threat landscape facing TPU.

TALOS

A DIVISION OF NERC E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Cyber Threat Sources In Use

Daily Operations

- IOC's and malware definitions are used by security tools to detect malicious activity on TPU's systems.
- This is fully-automated and is our first point of detection.

Vulnerability Management

- Intelligence sources drive discovery of vulnerabilities, their severity and the likelihood of exploitation.
- This helps us develop & prioritize remediation actions as early as possible.

Incident Response

- Intel plays a crucial role in containment and eradication of threats.
- IOC's and TTP's are used to hunt for malicious activity.

Active Threat Hunting

Attention: The public facing network of U.S. Electric Companies have been identified as the target of a People's Republic of China (PRC) cyber reconnaissance and enumeration campaign. The following indicators of compromise (IOCs) for this campaign are listed below include possible malicious internet addresses...

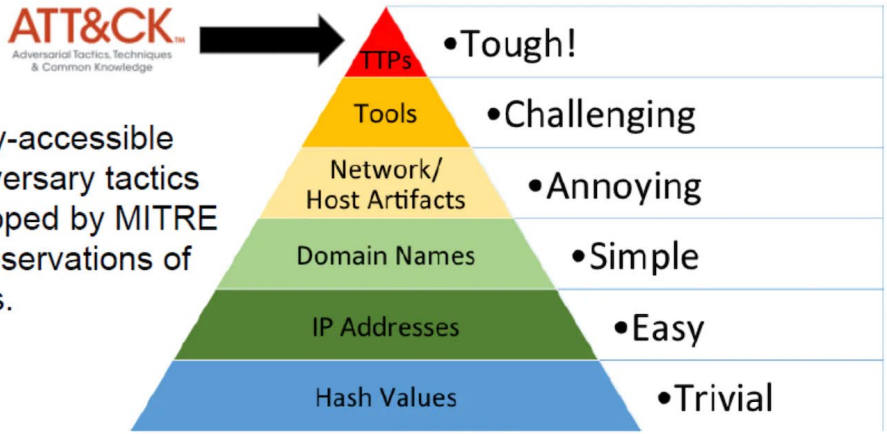
Active Threat Hunting

MITRE ATT&CK

Overview on Attacker Techniques and Attack Phases

attack.mitre.org

ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques, developed by MITRE based on real-world observations of adversaries' operations.



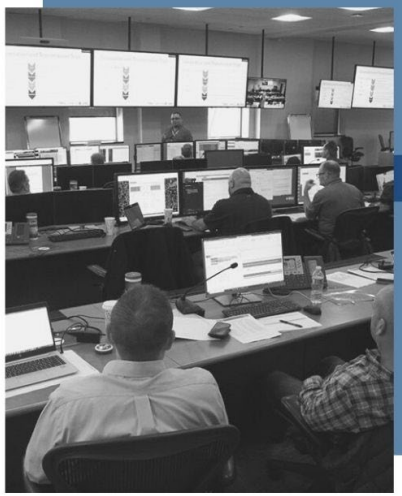
Source: David Bianco

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTPs = Tactics, Techniques, and Procedures

Save the Date!

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



GRIDEX VII

NOVEMBER 14-15, 2023

The GridEx VII Planning Team registration for Lead Planners and Planners will open soon. Information will be available via the E-ISAC Portal.

FOLLOW TO KEEP UP TO DATE

LPPC
LARGE PUBLIC POWER COUNCIL

Sept 25-27

TACOMA PUBLIC UTILITIES


Thank you
TACOMA PUBLIC UTILITIES