Defending Your Grid from Cyber Threats

Jason Miller, BitLyft Security
Mike Johnson, LogRhythm
“All men can see these tactics whereby I conquer, but what none can see is the strategy out of which victory is evolved.”

- Sun Zsu, Art of War
The Highly Dangerous 'Triton' Hackers Have Probed the US Grid

The same hackers behind a potentially lethal 2017 oil refinery cyberattack are now sniffing at US electrical utility targets.
91% of Attacks Are Delivered Via the Front Door …

- Email Attack Types -
  - Phishing
  - Spear-phishing
  - Business Executive Compromise

- Payloads and Motives
  - Ransomware – Financial Gain or Nation Interests
  - Malware - Nation State Interests
Even Engineers Are Falling Prey...

US Utilities Hit with Phishing Attack

An email phishing attack, thought to be from a nation-state actor, claims that engineers have failed licensing exams.

A new phishing attack is hitting US utilities with threats that their engineers could be in danger of losing their professional licenses. But in reality, the only danger comes from panicked employees clicking on the embedded Word document and infecting their computers with a remote access Trojan (RAT) and command-and-control proxy.

The RAT and proxy appear to originate with a nation-state actor rather than a financially motivated criminal organization. Researchers at Proofpoint found that the LookBack malware and many of the macros used in the campaign look very similar to tools used in a 2018 campaign against Japanese...
Finding and Defending Against the Needle in a Haystack

- Enhance Detection thru SIEM Adoption
- Gold Standard: 24/7 real-time monitoring over all assets
  - Economizing on coverage only creates zones of vulnerability that hackers will find and exploit
- Behavior-based detection will alert in real-time, days before legacy signature-based blacklists
- Traffic pattern analysis, dynamic risk-scoring, auto-response detected threats
Monitoring and Defending In-Network SCADA Servers
Create a DEW Line...

✔ Benchmark against a Security Operations Maturity Model and adopt a proactive plan to systematically address points of vulnerability

✔ Adopt/expand SIEM coverage – SIEM/SOCasS models make NextGen accessible

✔ Upgrade email defenses to scrub both header and body elements and periodically refresh staff training

✔ Verify the quality, accuracy, and timeliness of all 3rd-party contractor work

✔ Stay apprised of reported cyber activity through e-ISAC and MS-ISAC

✔ Collaborate with MMEA members to collapse the collective window of vulnerability by pooling real-time SIEM/threat intel to create a cyber ‘DEW Line’
NERC CIP v5:
Compliance Reporting as a Defense

Mike Johnson
Business Partner Manager
Mid-Atlantic and Ohio Valley

LogRhythm
The Security Intelligence Company
Questions??

Jason Miller
Jason.miller@bitlyft.com
727.543.5514

Mike Johnson
Mike.johnson@logrhythm.com
937.572.7149