CYBER THREAT BRIEFING

SELENA LARSON, DRAGOS INC.

YEAR IN REVIEW

THREAT BRIEF

Dragos' Year in Review provides insights and lessons learned from our team's first-hand experience hunting, combatting, and responding to ICS adversaries throughout the year

ICS VULNERABILITIES

Provides an analysis of ICS-specific vulnerabilities and discusses impacts, risks, and mitigation options for defenders

ICS THREATS

Provides insights on the state of ICS cybersecurity, the latest trends and observations of ICS-specific adversaries, and proactive defensive recommendations

LESSONS LEARNED FROM IR

Provides a synopsis of trends observed within the industry and lessons learned from Dragos' proactive and responsive service engagements

ICS VULNERABILITIES

KEY FINDINGS

- Dragos assessed 212 vulnerability advisories consisting of 438 vulnerabilities

- Of the 438 vulnerabilities, 24% affected industrial-specific protocols or file formats

ICS VULNERABILITIES

VULNERABILITY VISIBILITY

- 9% of advisories covered products that would be deemed high-likelihood initial targets in the ICS space.
- 40% of advisories covered engineering workstation and operator station software.
- 37% of advisories covered field equipment: industrial controllers, sensors, and the network equipment responsible for connecting controllers and sensors to the broader control systems network.

ICS VULNERABILITIES

VULNERABILITY PATCHING

- 26% of advisories had no patch available when the initial advisory came out, presenting a challenge for users trying to take action on the published vulnerability.
- 30% of advisories published incorrect data preventing operators from accurately prioritizing patch management.

ICS THREAT LANDSCAPE

KEY FINDINGS

- Dragos continues to identify ICS activity groups targeting ICS entities globally, increasing the total count to 11 public activity groups.
- Adversaries are increasingly targeting remote connectivity.
- Third-party and supply chain threats are increasing.
- Ransomware and commodity malware remain threats to industrial operations.
- Common tactics such as phishing, password spraying, and watering holes remain popular and effective as initial access vectors into industrial organizations

ICS THREAT LANDSCAPE

NEW ACTIVITY TREND

Threat proliferation contributed to increased risk as entities expanded targeting and capabilities.

Similar to physical weapons proliferation, **threats are spreading in the cyber realm.**

This is caused by **increasing government investment in offensive cyber capabilities** with ability to disrupt critical infrastructure.

Adversaries are **more easily obtaining resources and skills necessary** for a disruptive physical cyber event.

ICS THREAT LANDSCAPE

THREAT PROLIFERATION

X_t XENOTIME
since 2014

MODE OF OPERATION
Focused on physical destruction and long-term persistence

CAPABILITIES
TRISIS, custom credential harvesting, off the shelf tools

VICTIMOLOGY
Oil & Gas, Electric, Middle East, US, Europe, APAC

LINKS
None

M_a MAGNALLIUM
since 2016

MODE OF OPERATION
IT network limited, information gathering against industrial orgs

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Oil & Gas, Electric, Saudi Arabia, North America

LINKS
APT33, PARISITE

CONCLUSION

- Throughout 2019, Dragos observed an **increase of threats targeting industrial organizations.**
- Vulnerability reporting errors can **prevent proper patch management** and addressing acceptable risk.
- Understanding today's evolving cyber threat landscape—through a deep understanding of how adversaries behave and the potential operational, safety, and financial impacts they can cause—**is vital for the ICS community to raise the bar in cybersecurity.**