New ICS Threat Activity Group: TALONITE

dragos.com/blog/industry-news/new-ics-threat-activity-group-talonite/

April 26, 2021

Blog Post

By Dragos, Inc.

04.26.21

Dragos first disclosed four new threat activity groups targeting ICS/OT in the ICS Cybersecurity 2020 Year in Review report. In this blog post, we will provide more information on one of the new groups: **TALONITE**. The fundamental assessment of threats tracked by Dragos is that they *are explicitly attempting to gain access to ICS networks and operations or are successful in achieving access*, not simply trying to gain access to an industrial organization. To learn more about ICS threat activity groups and how they're created, we invite you to read our blog post "Uncovering ICS Threat Activity Groups."

> **Activity Group:** *a set of intrusion events related with varying degrees of confidence by similarities in their features or processes used to answer analytic questions and develop broad mitigation strategies that achieve effects beyond the immediate threat.*

Dragos ICS Cybersecurity 2020 Year In Review

TALONITE Activity Group Overview

Dragos began tracking the TALONITE activity group in July 2019 with operations focusing on initial access compromises in the United States (U.S.) electric sector. The group uses phishing techniques with either malicious documents or executables. TALONITE uses two custom malware families that both feature multiple components known as LookBack and FlowCloud.

TALONITE focuses on subverting and taking advantage of trust with phishing lures focusing on engineering-specific themes and concepts, malware that abuses ***otherwise*** legitimate binaries or modifies such binaries to include additional functionality , and a combination of owned and compromised network infrastructure. This activity is difficult to track and contain given the group's propensity to blend techniques and tactics in order to ensure a successful intrusion. There is behavioral and tooling overlap between TALONITE and activity known by some as APT10. Alleged members of APT10 were indicted in 2018.

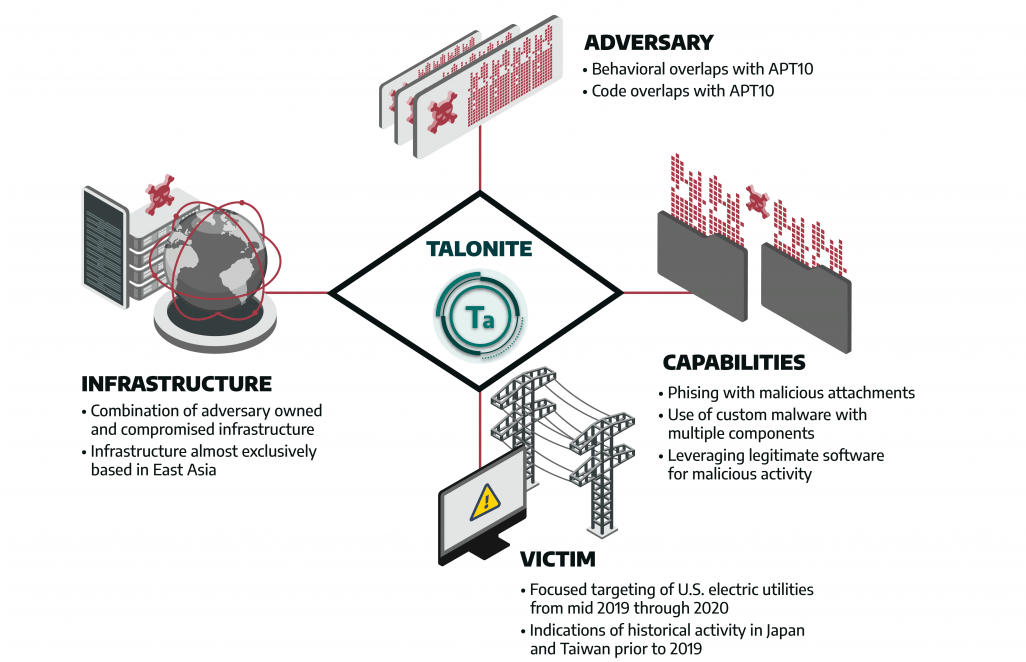

Figure 1: Diamond Model representation of TALONITE

Detecting and Mitigating TALONITE Activity

TALONITE gains initial enterprise network access via spearphishing activity that leverages malicious documents and executables. The lures (Figure 2) focus on engineering-specific themes and concepts, and distributed malware known as FlowCloud and LookBack.

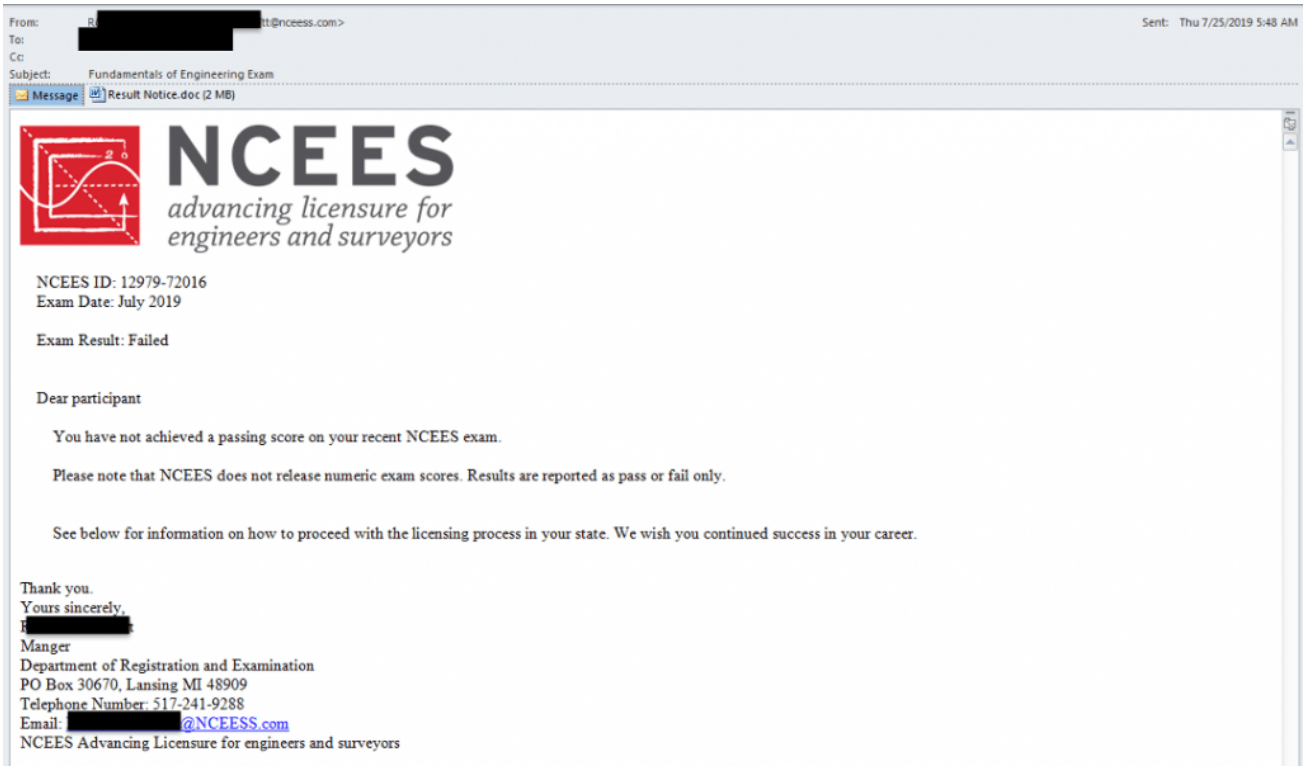

Figure 2: TALONITE phishing engineering-themed email

The malware incorporates multiple components including legitimate items such as certutil.exe from Microsoft that the malware abuses, or malware components items masquerading as legitimate utilities such as the malicious proxy tool GUP.exe , named after a legitimate Notepad++ executable.

The infrastructure appears to be shared or reused through the overlapping LookBack and FlowCloud campaigns. Dragos previously identified infrastructure associated with LookBack and concurrently used in FlowCloud activity. Most items indicate an adversary registering, hosting, and maintaining infrastructure on controlled servers. TALONITE registers domains masquerading as legitimate engineering or regulatory bodies and uses mostly adversary-owned and -controlled domains and servers, occasionally using legitimate but compromised infrastructure.

Dragos did not observe any lateral movement for TALONITE. Based on the capabilities of LookBack and FlowCloud, both of which facilitate various means of credential capture, Dragos assesses with high confidence that TALONITE lateral movement incorporates credential reuse. Both malware types are Remote Access Trojans (RAT) that contain capabilities to establish persistence within the environment. LookBack malware contains persistence mechanisms that add two Windows registry keys to execute legitimate but maliciously modified files when the infected user next logs in.

To obtain persistence, FlowCloud performs minor operations on the system then launches a renamed copy of the legitimate HTML Help Workshop (hhw.exe) utility from Microsoft. Extensive database and related processes are used to capture host data that is stored in those database files in a subdirectory of the legitimate but renamed utility.

The Dragos Platform incorporates multiple detections and analytics designed specifically to detect credential reuse and malicious logon activity. Such tactics are deployed by multiple activity groups tracked by Dragos, making coverage of such abuse vital for ICS network protection. In the ICS Cybersecurity 2020 Year in Review, Dragos found that 90 percent of its services customers lacked fundamental visibility into ICS environments. This means most ICS asset owners and operators will be blind to threats and lack critical cybersecurity data. Learn more about the value of asset visibility in building a comprehensive OT cybersecurity program by downloading our OT asset visibility white paper.

Detections for all TALONITE behaviors are available in the Dragos Platform.

ICS Considerations for the Future

There is no evidence indicating TALONITE has executed a disruptive ICS attack or penetrated control system networks in a victim environment. Targeting behavior from July 2019 through the present strongly indicates that TALONITE is exclusively focused on the electric sector, especially within the United States. TALONITE at minimum represents an initial access and information gathering capability leveraged against multiple entities within

the U.S. electric sector over an extended period of time. TALONITE focuses on U.S. electric utilities, with some evidence of capabilities targeting unknown entities in Japan and Taiwan prior to 2019.

Dragos cannot definitively link TALONITE to any known intrusion set or state interest, despite behaviors and tooling that suggest an overlap with APT10 (also referred to as menuPass and STONE PANDA). TALONITE's targeting focus on critical engineering, and power generation and distribution know-how within electric utilities is consistent with a well-resourced adversary with strong long-term interests in industrial control and grid operations.

TALONITE targets U.S. electric utilities for initial access and information gathering. Although TALONITE is not associated with any known and deliberate ICS disruptive event, TALONITE's identified behaviors and capabilities do not rule out future ICS-targeting operations. While TALONITE's relationship to People's Republic of China (PRC) strategic interests is unknown, sufficient information identifies this group as an emerging and serious threat to security in the electric sector.

To learn more about Dragos and our industrial cybersecurity products and services, visit: dragos.com/why-dragos.