New ICS Threat Activity Group: STIBNITE

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

March 24, 2021

Blog Post

By Dragos, Inc.

03.24.21

Dragos first disclosed four new threat activity groups targeting ICS/OT last month in the ICS Cybersecurity 2020 Year in Review report. In this blog post, we will provide more information on one of the new groups: **STIBNITE**. 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

STIBNITE Activity Group Overview

The STIBNITE Activity Group targeted wind generation and government entities in Azerbaijan. STIBNITE launched multiple intrusion operations against targets from late 2019 through 2020. STIBNITE leverages spearphishing to drop a custom malware known as PoetRAT. Dragos assesses with moderate confidence that the adversary performed focused intrusion and information gathering operations aligned with Stage 1 of the Industrial Control System (ICS) Cyber Kill Chain.

STIBNITE activity focuses on a region, the Caucasus, not typically observed in ICS targeting. As stated in past Dragos reporting and public comments, critical infrastructure intrusions and ICS events can correlate to areas of latent or existing conflict. As a result, known disruptive operations largely focus on existing conflict zones, such as Ukraine or the Gulf region.

STIBNITE gains initial access via credential theft websites spoofing Azeri government organizations, and spearphishing campaigns using variants of malicious Microsoft Office documents.

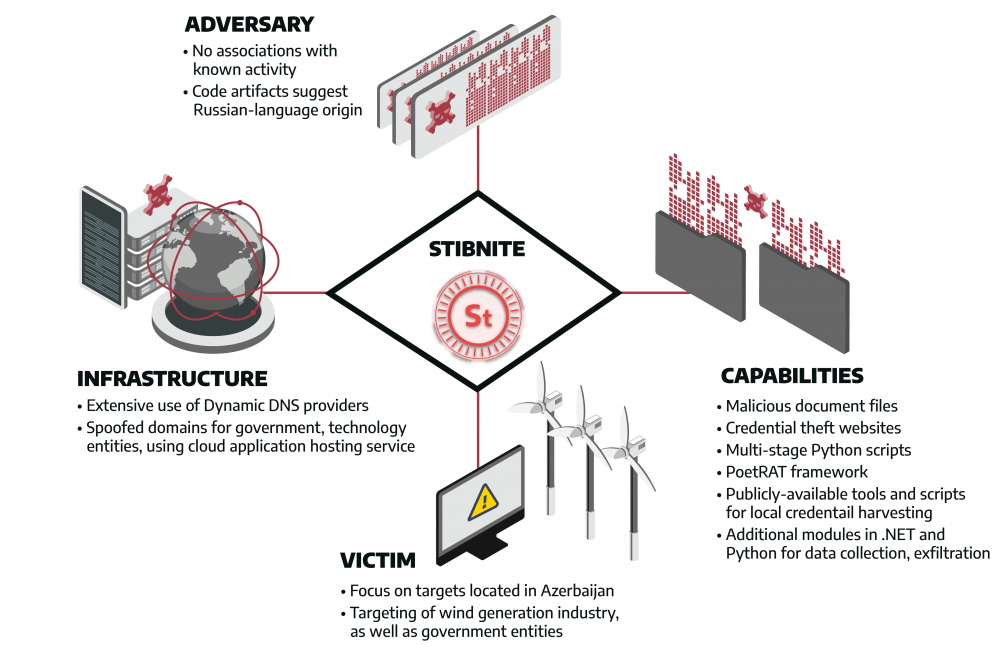

Figure 1: Diamond Model representation of STIBNITE

The group leverages customized malware, called PoetRAT, for information gathering activities and post exploitation activity including listing files, taking screenshots, transferring files, and command execution. STIBNITE is known to use Dynamic Domain Name System (DDNS) and common ports for C2 traffic. Dragos also discovered that STIBNITE reused infrastructure between its 2020 campaigns.

STIBNITE uses an executable package of a Python-based implementation of Mimikatz (PypyKatz) and the open-source LaZagne credential collection project for credential harvesting. The group also uses other open-source resources for web browser credential theft and data encoding and decoding routines using the Affine substitution cipher. Credential harvesting tools could allow adversaries to propagate throughout the network. As reported in the ICS Cybersecurity Year in Review, Dragos discovered that in 2020, 88 percent of Dragos services engagements involved significant issues with network segmentation.

At this time, the extent of the group's ICS interest is limited to targeting wind generation in Azerbaijan. STIBNITE's tools and targeting focus would enable transition from Stage 1 operations to a Stage 2 intrusion given developed access and stolen information, such as user credentials. Dragos tracks many threats earlier in the ICS Cyber Kill Chain because Activity Groups may cross over into the OT environment. It can take years for a Stage 1 group to transition into OT access depending on its objectives and timeline.

Detecting and Mitigating STIBNITE Activity

Although STIBNITE activity is currently focused on IT networks, information gathered – such as logon credentials and network information – can be used to facilitate follow-on ICS network compromise. OT operators should look for PoetRAT activity in IT and OT environments through execution of Python and Lua.

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 STIBNITE behaviors are available in the Dragos Platform.

ICS Considerations for the Future

The identified activity in Azerbaijan, while limited in scope at this time, emphasizes the proliferation of ICS targeting in combination with more traditional tensions. Azerbaijan remains at war with Armenia over the Nagorno-Karabakh region and continues to emerge as an alternative oil and gas provider to Europe. As interest in ICS-related cyber effects continues to increase, ICS-related intrusions such as those associated with STIBNITE will only continue and grow.

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