EKANS Ransomware Misconceptions and Misunderstandings

dragos.com/blog/industry-news/ekans-ransomware-misconceptions-and-misunderstandings/

June 18, 2020

Blog Post

By Joe Slowik

06.18.20

Since its initial public disclosure by Vitali Kremez, MalwareHuntTeam, and others on 06 January 2020, [1] a relatively new ransomware variant referred to as EKANS by Dragos has continued to operate against multiple, high-profile organizations. [2] Beginning in 2020, the following organizations have experienced at least attempted intrusions, if not outright disruption, traced to this ransomware variant:

- Fresenius Group [3]
- Honda [4]
- Enel Group [5]

This group of identified activity likely represents a subset of behavior, as other events are either disputed or nonpublic at this time. [6] Irrespective of specific victimology, EKANS incorporates certain specific functionality – previously deployed via stand-alone scripts or supporting tools [7] – directly into a ransomware executable.

As EKANS continues to develop and present itself in high-profile events, several misconceptions and misunderstandings have developed about the malware, its authors, and what it means for Industrial Control System (ICS) networks.

> **1. Why EKANS, and how does EKANS relate to Snake, or Turla activity?**

When first reported in early January, the malware since referred to as EKANS by Dragos was labeled both EKANS and SNAKE by its original discoverers. On further analysis, Dragos referred to this malware as “EKANS” for several reasons:

1. The string “EKANS” is actually present in both the malware and in the malware’s operations on victim machines (by creating and checking a mutex value to prevent reinfection of the same victim).
2. While “EKANS” is “SNAKE” spelled backwards, the word “SNAKE” did not appear in any observable aspect of the malware.
3. “SNAKE” has a long-standing relationship with an existing threat actor, referred to variously as Turla, SNAKE, or VENOMOUS BEAR. [8] More significantly, this entity is associated with Russian state espionage activity and not ransomware deployment.

While no consistent mechanism or convention exists for naming malware, Dragos adheres to the practice of naming malware based on observables or details within obtained samples. The existence of a long-running, state-sponsored threat referred to as “SNAKE” is reason for caution in referring to a new ransomware variant by the same name, if only to avoid confusion. Various outlets and individuals have already mistakenly made the connection between EKANS ransomware and the Turla actor based on the “SNAKE” reference – confusion best avoided given the possible repercussions of creating an unfounded link between these entities.

Given the potential consequences of linking a state-sponsored or -directed entity to multiple disruptive ransomware events, Dragos finds the use of the “SNAKE” label not just inaccurate (as it is not present in the malware), but dangerous as well. Ultimately, EKANS ransomware has no known, provable connection to the threat actor variously referred to as SNAKE, Turla, VENOMOUS BEAR, or other names. While the original discoverers – Vitali Kremez and MalwareHunterTeam – reserve the right to name this activity, given the use of both “SNAKE” and “EKANS” in public postings and the baggage associated with the former, Dragos emphasizes the desirability of using the latter to avoid confusion with state-sponsored cyberespionage activity.

2. How does EKANS impact ICS assets?

Since discovery, several reports have emerged about EKANS’ notional abilities relative to industrial assets. [9] While EKANS features several functional characteristics keyed to industrial environments – specifically process kill functionality related to ICS data historians, licensing servers, and similar items – such functionality is relatively simple, largely untargeted (given lack of variation in the list of process names targeted between victims), and rather blunt in design.

EKANS essentially internalizes an extensive process kill list associated with MegaCortex ransomware activity in mid- to late-2019, and potentially associated with LockerGoga events even earlier. Given obfuscation mechanisms deployed, use in EKANS likely

achieves a higher degree of defense evasion and functionality masking than these earlier examples. The only functionality associated with these items is forcibly killing a named process. This is much different than the subtle process manipulation and integrity destruction seen (or attempted by) events such as Stuxnet, CRASHOVERRIDE, or TRISIS. [10]

Dragos assesses with high-confidence that the process kill functionality built into EKANS is designed primarily to remove file locks from sensitive items – such as license keys or data stores –to extend the impact of a ransomware event by encrypting these vital files. While deeply concerning, this is significantly different from modifications to an industrial process to produce a potential physical disruption. Based on identified functionality, the most concerning aspect of EKANS is that its blunt, indiscriminate process termination functionality leads to unintended side effects in production environments.

> **3. Is EKANS a state-sponsored or -directed activity against critical infrastructure?**

In addition to the disambiguation with Turla provided above, other reports have surfaced allegedly linking EKANS activity to state-sponsored activity.[11] While the potential victimology in such reports may be accurate, ties to state-sponsored activity rely on indefensible logical leaps that simply are not proven after further analysis. [12]

Although Dragos cannot completely or definitively disprove that EKANS is part of a state-sponsored or -directed effort, the preponderance of evidence would indicate otherwise. Among other items, connection to past ransomware activity, such as MegaCortex, combined with subsequent victims in unrelated industries and regions suggests that EKANS as a potential disruptive tool tied to Iranian (or other) strategic interests, is at best, a very weak argument.

All available evidence at present indicates EKANS is a likely criminal activity designed for monetization, and not a state-sponsored, disruptive campaign masquerading as ransomware.

> **4. Given the above, is Dragos suggesting that EKANS is therefore not that significant?**

The above statement does not reflect Dragos' position in the slightest. In evaluating items like EKANS, we must ensure balance between over-hyping threats out of proportion and minimizing activity so that it is not taken seriously. While EKANS is no Stuxnet or similar threat, EKANS does not resemble some sort of "play malware" that just so happens to feature ICS-specific references.

EKANS represents one aspect of a continued evolution by multiple ransomware entities toward targeting industrial and critical infrastructure entities. Although relatively straightforward in behavior and functionality, EKANS remains a notable and significant

threat to ICS operations. Even if its functionality is relatively “basic” in being limited to process termination, such activity performed at the wrong time or against the wrong system could lead to potentially disastrous process interruption. Although not designed to physically disrupt or destroy, malware such as EKANS brings the possibility of ICS-specific impacts from traditionally state-directed activity to likely criminally-motivated actions.

Given the above, asset owners and operators should treat EKANS as a serious threat, and as a likely sign of continued evolution in ransomware operations. Malicious entities continue to refine their operations to target entities ranging from manufacturers through critical infrastructure providers, such as power and water utility companies. Such shifts are likely due to assumptions on the need to pay a ransom to ensure continuous operation by vital entities. Irrespective of motivation, ICS asset owners and operators are at increasing risk of ever more refined malware operations targeting their organizations. Discounting the threat posed by items such as EKANS due to a perceived lack of sophistication is not merely misguided but may potentially lead to operational disaster.

ICS asset owners and operators find themselves in an increasingly contested environment, with both state sponsored and criminally motivated entities interested in this operational space. To combat such efforts, organizations must invest in increasing visibility – across network, host, and process areas – and the ability to respond and remediate potential disruptions. Only by identifying potential threats at the earliest possible instance and having the capacity to recover and restore operations to a recent known-good state can industrial operators forge resilience in the face of an ever-more hostile threat landscape.

[1] Vitali Kremez (https://twitter.com/VK_Intel/status/1214333066245812224?s=20); SNAKE Ranswomare is the Next Threat Targeting Business Networks – BleepingComputer (https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/)

[2] EKANS Ransomware and ICS Operations – Dragos (https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/); Dragos WorldView customers should consult TR-2020-02 EKANS Ransomware and ICS Operations

[3] European Health Care Giant Fresenius Group Grappling with Computer Virus – CyberScoop (https://www.cyberscoop.com/fresenius-health-care-cyberattack-coronavirus/); Dragos WorldView customers should consult AA-2020-16 Ransomware Activity Impacting European Medical and Pharmaceutical Manufacturing

[4] Is There a “Snake” Under Honda’s Hood? – CISO Magazine (https://www.cisomag.com/honda-snake-ransomware-attack/#:~:text=Operations%20of%20the%20Japanese%20automobile,late%20hours%20of%20Sunday%20night.); Snake Ransomware Delivers Double-Strike on Honda, Energy Co.

– ThreatPost (https://threatpost.com/snake-ransomware-honda-energy/156462/); Dragos WorldView customers should consult AA-2020-21 EKANS Activity at Multinational Manufacturing and Energy Companies

[5] SNAKE Ransomware Affected Enel Group's Internal Network – TripWire (https://www.tripwire.com/state-of-security/security-data-protection/snake-ransomware-affected-enel-groups-internal-network/); Snake Ransomware Delivers Double-Strike on Honda, Energy Co. – ThreatPost (https://threatpost.com/snake-ransomware-honda-energy/156462/); Dragos WorldView customers should consult AA-2020-21 EKANS Activity at Multinational Manufacturing and Energy Companies

[6] Getting the Story Right, and Why It Matters – Joe Slowik (https://pylos.co/2020/01/28/getting-the-story-right-and-why-it-matters/)

[7] New Version of MegaCortex Targets Business Disruption – Accenture (https://www.accenture.com/us-en/blogs/blogs-megacortex-business-disruption); Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT – FireEye (https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html)

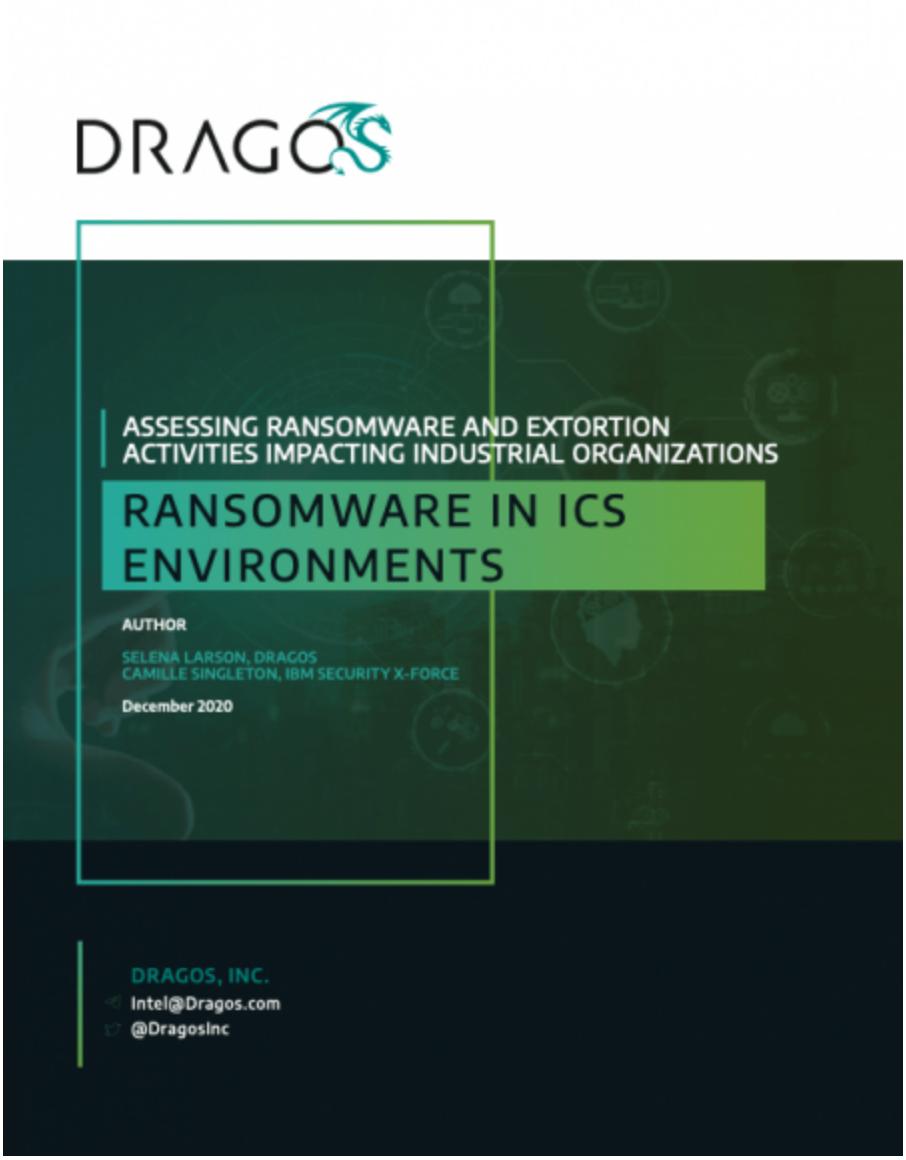
[8] Turla – MITRE (https://attack.mitre.org/groups/G0010/); Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR – CrowdStrike (https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/)

[9] Honda Hackers May Have Used Tools Favored by Countries – The New York Times (https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html)

[10] Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments – Joe Slowik, Dragos (https://www.dragos.com/wp-content/uploads/relocated/p/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf)

[11] Ransomware Linked to Iran, Targets Industrial Controls – Bloomberg (https://www.bloomberg.com/news/articles/2020-01-28/-snake-ransomware-linked-to-iran-targets-industrial-controls)

[12] Getting the Story Right, and Why It Matters – Joe Slowik (https://pylos.co/2020/01/28/getting-the-story-right-and-why-it-matters/)



Read the whitepaper

Understand the ransomware and extortion activities impacting production environments and steps you can take to protect your critical assets.

Learn more