Getting the Story Right, and Why It Matters

Published: 2020-01-28 · Archived: 2026-04-05 18:08:38 UTC

The realm of computer security incidents and events draws increasing amounts of attention, not only from specialists and key decision-makers within the field but also “lay” (or non-technical) audiences. As a result of such increasing desire to know about and understand events in this field, researchers as well as journalists publishing public material must take care to ensure accuracy in communication while at the same time balancing this with accessibility. Getting lost in technical jargon or very precise conditional phrasing may be most accurate, but will likely lose a “general” audience resulting in a failure to communicate a story. However, moving too far in the other direction may mean the nature of an event is obscured or distorted. Finally, the desire to either “be first” or ensure maximal engagement provides a temptation to “sex up” wording and inflate claims (such as my personal favorite, equating “phishing” or “scanning” with a “cyber attack”). Overall there are many pressures, competing interests, and at times limited sourcing to develop public communication that meets the criteria of technical accuracy, general accessibility, and measured language – yet if the overall community of “communicators” in information security doesn’t try, we are all the worse for it.

This morning, I read an article about a “new” strain of ransomware which includes industrial control system (ICS) specific capabilities. Yet from the start, the article errs as the ransomware is not new – it was previously reported in several other outlets and social media.

Cybersecurity

‘Snake’ Ransomware Linked to Iran, Targets Industrial Controls

By Gwen Ackerman
January 28, 2020, 7:17 AM MST

- Israeli company says Bahrain Petroleum may be potential victim
- Code goes after specific programs, many tied to GE: Otorio

LIVE ON BLOOMBERG
Watch Live TV
Listen to Live Radio

LISTEN TO ARTICLE
▶ 3:11

In this article

GE
GENERAL ELECTRIC
11.70 USD
▲ +0.26 +2.23%

CL1
WTI Crude
53.81 USD/bbl.
▲ +0.67 +1.26%

An Israeli cybersecurity firm has identified a new type of ransomware that it believes was created by Iran and has the ability to lock up or even delete industrial control systems.

Tel Aviv-based Otorio, a cybersecurity firm which specializes in industrial control systems (ICS), said that the ransomware called “Snake,” like others of its kind, encrypts programs and documents on infected machines. But it also removes all file copies from infected stations, preventing the victims from recovering encrypted files.

Snake searches for hundreds of specific programs -- including many industrial processes that belong to General Electric Co. -- in order to terminate them and allow it to encrypt the files, Otorio said.

It is worth noting that public reporting did not capture the ICS-specific angle at the time of discovery outside of easily-lost Twitter conversation. However, this omission of prior, publicly-available work 20 days before the new article is interesting – and reveals an issue that will come up throughout this analysis. Namely, the reporter in question appears completely dependent upon the single source cited in the article, the firm Otorio.

In any event, identifying and publicly reporting on the ICS-specific aspects of this ransomware variant (which I'll refer to as EKANS given "Snake" conjures up images of Turla for much of my audience) is nonetheless important. Previously, the only publicly-known connections between ransomware and industrial environments are IT-centric infections spreading into control system environments, or potentially misguided proof-of-concepts designed for either academic or marketing purposes. So – there is an important story here, yet further reading indicates continued issues of accuracy and identifying implications.

First, and addressing the delicate issue of balancing technical accuracy with general accessibility, there is the question of precise impact. The following is reported in the article, largely relying on single-source statements from the security firm mentioned earlier:

> Snake searches for hundreds of specific programs -- including many industrial processes that belong to General Electric Co. -- in order to terminate them and allow it to encrypt the files, Otorio said.
>
> "Deleting or locking targeted ICS processes would prohibit manufacturing teams from accessing vital production-related processes including analytics, configuration and control," Otorio said in a statement. "This is the equivalent of both blindfolding a driver and then taking away the steering wheel."

The above is roughly correct, but not quite. Again, publicly-available work from a few weeks prior exists providing a list of the specific processes targeted. From this list (or contacting an independent analyst to verify findings), interesting observations appear. First, it is true that specific programs are searched for – but only 64 instead of hundreds. Second, while GE is prevalent, the specific types of processes targeted (including beyond GE) are interesting and have implications beyond the alleged loss of operational control. When looked at in detail, the list of processes and descriptions shows a particular focus:

GE Processes	Focus on Client and Server processes related to the GE Proficy data historianProficy licensing server targetingAdditional targeting of GE-owned Fanuc (CNC and related robots platforms for manufacturing) licensing system
ThingWorx Industrial Connectivity Suite	Remote data collection and centralized display for industrial processesFocus on visibility and monitoring, not control

FLEXNET Licensing Service	License management and activation serviceFocus on ICS/IoT markets
Honeywell HMIWeb	Web-based HMI softwareUsed for management and control of systems
Sentinel HASP Licensing Manager	Software protection and licensing serviceIncludes security modules like hardware tokens
VMWare Processes	VMWare activation servicesVMWare guest processes/services
Various Remote Data Collection or Monitoring Services	BlueStripe Data CollectorTivoliRabbitMQ ServerMicrosoft SQL Server and SCCM services

Overall, the focus on ICS-related technologies is clear, but the specific focus reveals potential attacker intentions. The processes identified largely relate to licensing and data transfer services for centralized monitoring (whether in ICS-specific applications like data historians or more general applications like Microsoft SQL or IBM Tivoli). The only real exception is the Honeywell HMIWeb process, which would kill the process allowing for a human to interact via the HMI with the underlying process.

Thus what emerges is not so much a disruption of the process or elimination of process control (outside of the Honeywell HMIWeb item). Instead, the attacker appears to focus on the elimination of process (and plant) view. Even licensing server attacks can induce a “mission kill” on operational view and remote management via a pseudo “denial of service” attack by eliminating the licensing check from completing within the environment. Overall, these actions inhibit operations and makes them more expensive, but should not (deliberately) induce physical plant disruption. Manual operations would be the obvious and predictable response to such an event, and while expensive and inconvenient they are nonetheless planned for and possible within industrial environments. Essentially, the ICS-specific process elimination appears designed to increase the pain inflicted through a ransomware event in certain types of industrial environments.

But just what sort of environment, and what sort of actor? The next section attempts to answer these questions, but in a way that leaves much to be desired:

> Otorio researchers began investigating the appearance of a new ransomware in mid-December and soon realized it was one of the first designed to target the industrial sector. As they dug further, the researchers found that Bahrain Petroleum Co. -- known as Bapco for short - was potentially vulnerable to this new cyber threat.
>
> Not only does Bapco use GE equipment, its name was found in the malware's code, Otorio said.
>
> "There are findings and fingerprints inside the malware that when taken into account with the circumstances surrounding this campaign make it highly unreasonable that Snake was carried out by a different actor other than Iran," the Otorio report said.
>
> Boosting the researchers' confidence that the Snake originated in Iran was an alleged separate attack on Bapco carried out in parallel with the finding of Snake.
>
> "It is highly unlikely that a Gulf-area company will be attacked by two different potent actors, each targeting a different part of the organization at the same time," the researchers said in an email.

The connection to the Bahrain Petroleum Company (Bapco) is based almost entirely on the email address included in the ransom note delivered following EKANS execution:

```
----------------------------------------------
| What happened to your files?
----------------------------------------------
We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more -
all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry!
You can still get those files back and be up and running again in no time.

----------------------------------------------
| How to contact us to get your files back?
----------------------------------------------
The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network.
Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with
better cyber security in mind. If you are interested in purchasing the decryption tool contact us at bapcocrypt@ctemplar.com

----------------------------------------------------
| How can you be certain we have the decryption tool?
----------------------------------------------------
In your mail to us attach up to 3 files (up to 3MB, no databases or spreadsheets).
We will send them back to you decrypted.
```

The email address, bapcocryp[AT]ctemplar[.]com, would, under this interpretation, denote the campaign's victim. This is not an outlandish conclusion to draw, but one that can only be made at low levels of confidence using proper estimative language. To support this initial conclusion, the security company providing all information for the report points to an event previously reported on at Bapco, but associated with the Dustman wiper.

This connection leads to a host of follow-on questions concerning assumptions and potentially faulty logic – all of which lie with the sources of the article, but which would ideally be explored by the reporting journalist. Among other items, the connectivity between Dustman and Bapco could be called into question now, rather than looking at these as mutually reinforcing claims linked to a single actor or entity. For one, the Dustman report was provided by the Saudi National Cybersecuirty Authority, which would imply the victims were in Saudi Arabia and not Bahrain. Second, the timing indicates separation in events, from mid-December (EKANS) to late-December (Dustman). All of this could be explored or questioned, but instead the connectivity is simply left in place making a highly circumstantial claim (that EKANS is the work of Iran and conducted against a Gulf state-owned oil company) seem far stronger than what little evidence supports it.

The above is further muddied by the closing quotes such as it is "highly unreasonable that [EKANS] was carried out by a different actor other than Iran" and "it is highly unlikely that a Gulf-area company will be attacked by two different potent actors…at the same time". These two quotes are, quite simply, bonkers and don't stand up to even minimal exploration or investigation. For one, we have numerous examples of networks breached by multiple adversaries at the same time – even different groups aligned to the same state sponsor, such as the Democratic National Committee intrusion where APT28 and APT29 lived concurrently and independently during the course of the breach.

But even aside from this example, EKANS itself shows no signs of overlap or relation to any known Iranian state-sponsored activity. First, the authors claim that the ransomware is positioned as a disruptive wiper (similar in intention to NotPetya), and thus it is meant for recovery to be either not possible or not intended. While the idea is not far-fetched (and I will be presenting on just this at TROOPERS in March 2020), no evidence exists within EKANS' execution or code indicating such is the case. Instead, the malware appears as another piece of ransomware, programmed using the Go language and using the relevant libraries for functionality. This stands apart from known Iran-nexus IT disruption activity, which has previously leveraged Distrack wiper variants and the EldoS RawDisk driver to produce direct disruption. Technical observables do not mesh with known Iran-nexus activity. Furthermore, Iran-related entities have not previously demonstrated much desire or need to mask activity for disruption by hiding behind a fig leaf of criminal activity. Aside from blatant attacks such as ZeroCleare and Shamoon3 within the past year or so, Iranian-linked entities were happy to launch missiles and drones at Saudi Arabia in 2019 to produce a disruption in oil and gas facilities. Thus the need for ransomware-as-wiper seems highly unlikely, and outside of all past experience.

Overall, Otorio appears to use some strange transitive property of attribution, relying on the following sequence of reasoning:

1. EKANS is specifically targeted at Bapco.
2. Bapco was targeted by Iranian entities via Dustman roughly concurrently with EKANS.
3. Assume that it is highly unlikely for different entities to be engaged in the same environment with disruptive purposes simultaneously.
4. Therefore, Dustman and EKANS are linked.
5. Since Dustman is assessed to be Iranian in origin, then EKANS must be as well.

The logical progression here leaves much to be desired, and should have been examined in greater depth instead of simply reporting as unquestioned truth.

Finally, there is an issue with EKANS' very uniqueness. An analysis of the ICS-related processes targeted in the malware shows that they are also included in a MEGACORTEX ransomware sample (SHA256: 873aa376573288fcf56711b5689f9d2cf457b76bbc93d4e40ef9d7a27b7be466) identified "in the wild" in August 2019, possibly in the United States. The list of processes in this case encompasses thousands of items, almost all related to security products, with the only ICS-related items being the exact same list as in EKANS. Furthermore, this sample was publicly reported by Accenture after discovery, including a list of processes identified. So EKANS itself seems novel only for adding layers of obfuscation to the process list, but any targeting specificity in terms of ICS functionality would appear to map back to the MEGACORTEX event earlier in the year. Unless Bapco was targeted by this MEGACORTEX sample, the direct link to Bapco based on specific ICS technologies therefore seems weak or nonexistent. Overall, these observed samples align with well-documented, criminal activities designed to harvest money from victim environments, and not state-sponsored disruption operations masquerading as ransomware.

The article in question taken without criticism would appear to indicate a new type of state-sponsored disruption campaign in the Middle East, tied to Iranian aggression in the Gulf. Yet under moderate scrutiny many (if not all) of these claims fall apart. Unfortunately, the article does an insufficient job in attempting to validate or otherwise enrich any of the claims provided by the reporting security company, thus producing an inflammatory article where such concern is unwarranted.

The above is not meant to shame the journalist in question* (or even the reporting company, although I do think the lion's share of any blame for the errors and misconceptions reside with them). However, given the attention items such as this can draw in an increasingly tense environment – both in cybersecurity more generally and potential Iranian actions specifically – an inability to vet or explore the claims made produces substandard reporting. If (or more likely when) some entity picks this up and uses it as evidence of increasing Iranian aggression, not only has the report misled audiences on the activity in question, but may even help influence defensive and policy choices in ways which are simply not supported by evidence.

To conclude, we must all strive to do our best when reporting items of significance, such as alleged Iranian cyber disruptive activity in the Gulf. The above criticism is not meant to insult or otherwise "blast" any of the parties in question, but it is definitely intended to provide a thorough example for all parties on how we can (and should) strive to do better in this field.

*Note: I looked for a means to contact the journalist privately on this matter, but was unable to identify any means to do so other than a public Twitter stream, which seemed a poor way to communicate some of the detailed and nuanced points above.
