Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT | Mandiant

By Mandiant

Published: 2020-02-24 · Archived: 2026-04-05 15:44:12 UTC

Written by: Daniel Kapellmann Zafra, Keith Lunden, Nathan Brubaker, Jeremy Kennelly

---

Since at least 2017, there has been a significant increase in public disclosures of ransomware incidents impacting industrial production and critical infrastructure organizations. Well-known ransomware families like WannaCry, LockerGoga, MegaCortex, Ryuk, Maze, and now SNAKEHOSE (a.k.a. Snake / Ekans), have cost victims across a variety of industry verticals many millions of dollars in ransom and collateral costs. These incidents have also resulted in significant disruptions and delays to the physical processes that enable organizations to produce and deliver goods and services.

While lots of information has been shared about the victims and immediate impacts of industrial sector ransomware distribution operations, the public discourse continues to miss the big picture. As financial crime actors have evolved their tactics from opportunistic to post-compromise ransomware deployment, we have observed an increase in adversaries' internal reconnaissance that enables them to target systems that are vital to support the chain of production. As a result, ransomware infections—either affecting critical assets in corporate networks or reaching computers in OT networks—often result in the same outcome: insufficient or late supply of end products or services.

Truly understanding the unique nuances of industrial sector ransomware distribution operations requires a combination of skillsets and visibility across both IT and OT systems. Using examples derived from our consulting engagements and threat research, we will explain how the shift to post-compromise ransomware operations is fueling adversaries' ability to disrupt industrial operations.

Industrial Sector Ransomware Distribution Poses Increasing Risk as Actors Move to Post-Compromise Deployment

The traditional approach to ransomware attacks predominantly relies on a "shotgun" methodology that consists of indiscriminate campaigns spreading malware to encrypt files and data from a variety of victims. Actors following this model will extort victims for an average of $500 to $1,000 USD and hope to receive payments from as many individuals as possible. While early ransomware campaigns adopting this approach were often considered out of scope for OT security, recent campaigns targeting entire industrial and critical infrastructure organizations have moved toward adopting a more operationally complex post-compromise approach.

In post-compromise ransomware incidents, a threat actor may still often rely on broadly distributed malware to obtain their initial access to a victim environment, but once on a network they will focus on gaining privileged access so they can explore the target networks and identify critical systems before deploying the ransomware. This approach also makes it possible for the attacker to disable security processes that would normally be enough to detect known ransomware indicators or behaviors. Actors cast wider nets that may impact critical systems, which expand the scale and effectiveness of their end-stage operations by inflicting maximum pain on the victim. As a result, they are better positioned to negotiate and can often demand much higher ransoms—which are commonly commensurate with the victims' perceived ability to pay and the value of the ransomed assets themselves. For more information, including technical detail, on similar activity, see our recent blog posts on FIN6 and TEMP.MixMaster.

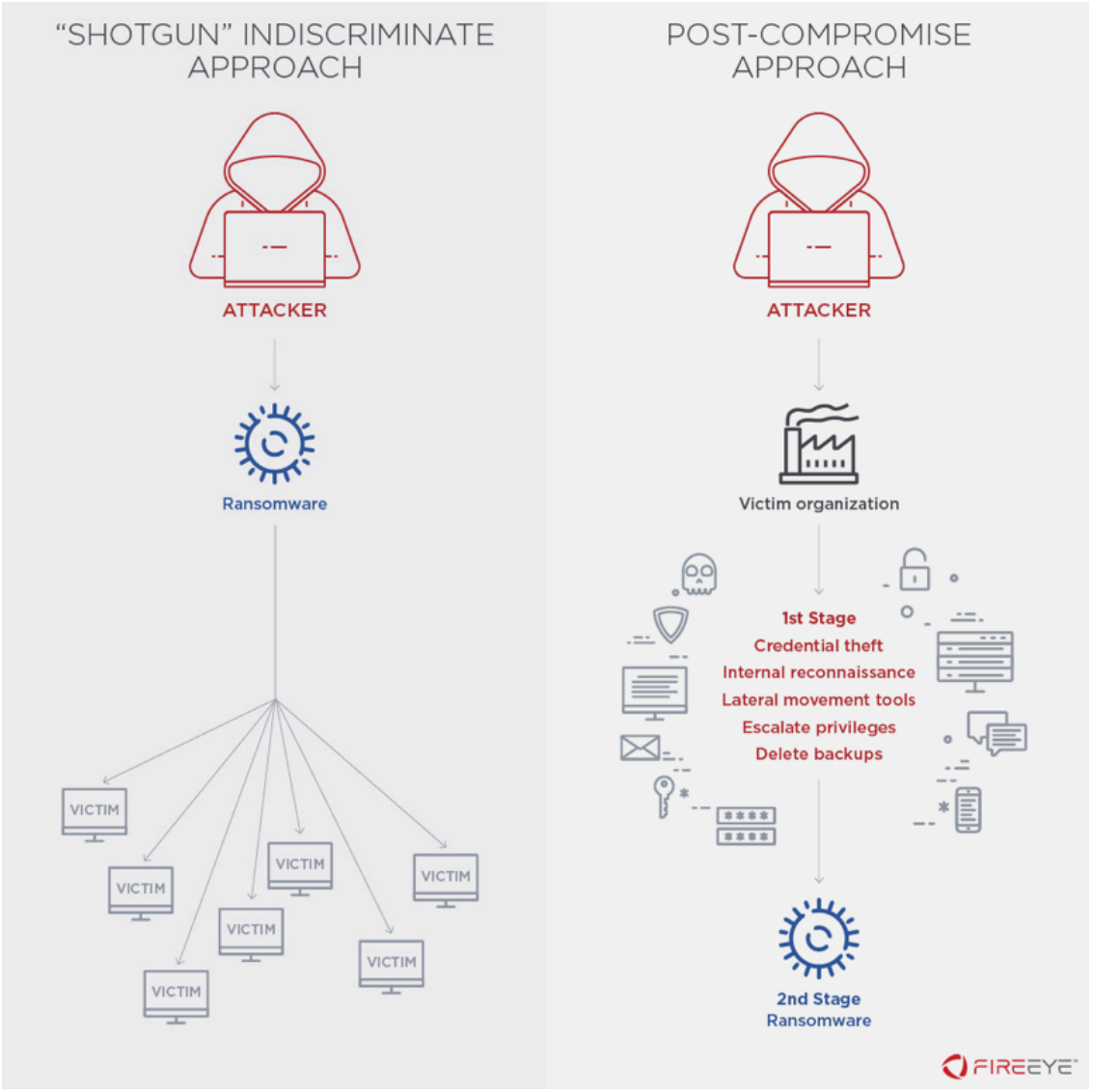


Figure 1: Comparison of indiscriminate vs. post-compromise ransomware approaches

Historical incidents involving the opportunistic deployment of ransomware have often been limited to impacting individual computers, which occasionally included OT intermediary systems that were either internet-accessible, poorly segmented, or exposed to infected portable media. In 2017, we also observed campaigns such as NotPetya and BadRabbit, where wiper malware with worm-like capabilities were released to disrupt organizations while

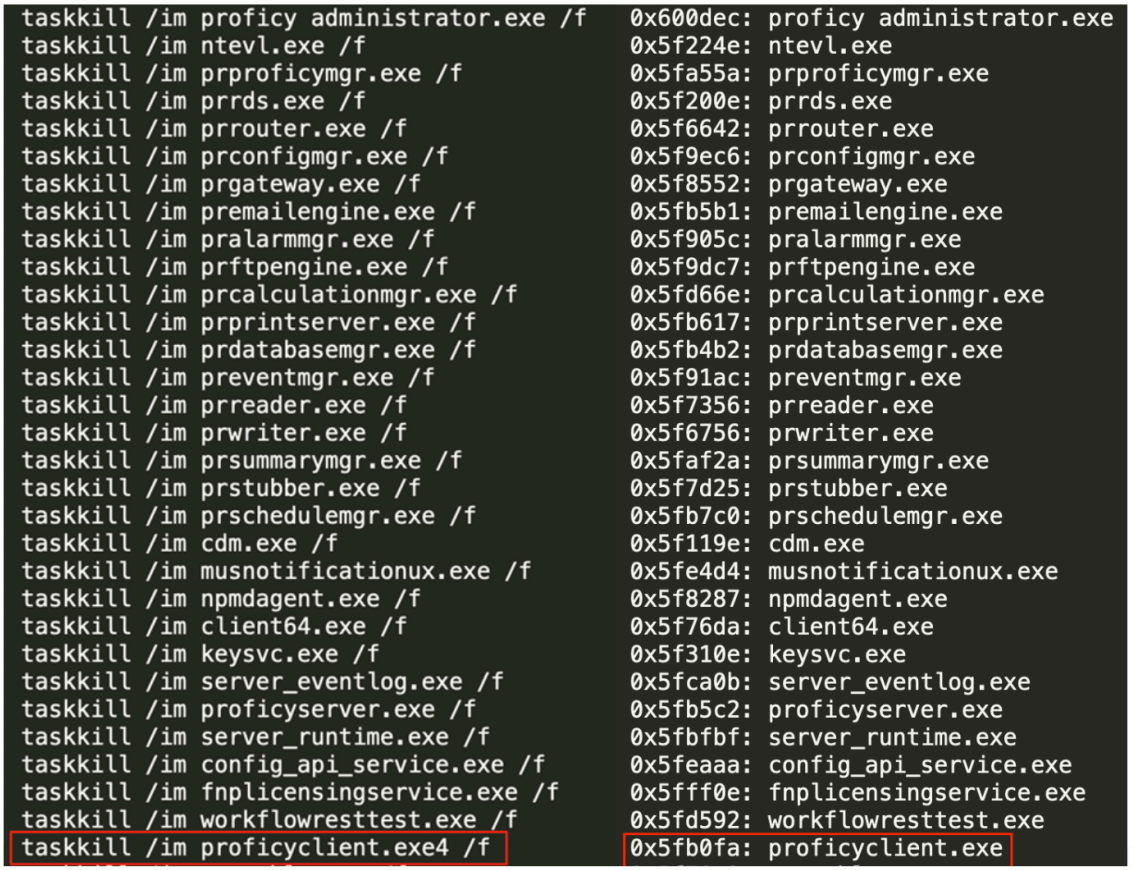
masquerading as ransomware. While these types of campaigns pose a threat to industrial production, the adoption of post-compromise deployment presents three major twists in the plot.

- As threat actors tailor their attacks to target specific industries or organizations, companies with high-availability requirements (e.g., public utilities, hospitals, and industrial manufacturing) and perceived abilities to pay ransoms (e.g., higher revenue companies) become prime targets. This represents an expansion of financial crime actors' targeting of industries that process directly marketable information (e.g., credit card numbers or customer data) to include the monetization of production environments.
- As threat actors perform internal reconnaissance and move laterally across target networks before deploying ransomware, they are now better positioned to cast wide nets that impact the target's most critical assets and negotiate from a privileged position.
- Most importantly, many of the tactics, techniques, and procedures (TTPs) often used by financial actors in the past, resemble those employed by high-skilled actors across the initial and middle stages of the attack lifecycle of past OT security incidents. Therefore, financial crime actors are likely capable of pivoting to and deploying ransomware in OT intermediary systems to further disrupt operations.

Organized Financial Crime Actors Have Demonstrated an Ability to Disrupt OT Assets

An actor's capability to obtain financial benefits from post-compromise ransomware deployment depends on many factors, one of which is the ability to disrupt systems that are the most relevant to the core mission of the victim organizations. As a result, we can expect mature actors to gradually broaden their selection from only IT and business processes, to also OT assets monitoring and controlling physical processes. This is apparent in ransomware families such as SNAKEHOSE, which was designed to execute its payload only after stopping a series of processes that included some industrial software from vendors such as General Electric and Honeywell. At first glance, the SNAKEHOSE kill list appeared to be specifically tailored to OT environments due to the relatively small number of processes (yet high number of OT-related processes) identified with automated tools for initial triage. However, after manually extracting the list from the function that was terminating the processes, we determined that the kill list utilized by SNAKEHOSE actually targets over 1,000 processes.

In fact, we have observed very similar process kill lists deployed alongside samples from other ransomware families, including LockerGoga, MegaCortex, and Maze. Not surprisingly, all of these code families have been associated with high-profile incidents impacting industrial organizations for the past two years. The earliest kill list containing OT processes we identified was a batch script deployed alongside LockerGoga in January 2019. The list is very similar to those used later in MegaCortex incidents, albeit with notable exceptions, such as an apparent typo on an OT-related process that is not present in our SNAKEHOSE or MegaCortex samples: "proficyclient.exe4". The absence of this typo in the SNAKEHOSE and MegaCortex samples could indicate that one of these malware authors identified and corrected the error when initially copying the OT-processes from the LockerGoga list, or that the LockerGoga author failed to properly incorporate the processes from some theoretical common source of origin, such as a dark web post.



```
taskkill /im proficy administrator.exe /f
taskkill /im ntevl.exe /f
taskkill /im prproficymgr.exe /f
taskkill /im prrds.exe /f
taskkill /im prrouter.exe /f
taskkill /im prconfigmgr.exe /f
taskkill /im prgateway.exe /f
taskkill /im premailengine.exe /f
taskkill /im pralarmmgr.exe /f
taskkill /im prftpengine.exe /f
taskkill /im prcalculationmgr.exe /f
taskkill /im prprintserver.exe /f
taskkill /im prdatabasemgr.exe /f
taskkill /im preventmgr.exe /f
taskkill /im prreader.exe /f
taskkill /im prwriter.exe /f
taskkill /im prsummarymgr.exe /f
taskkill /im prstubber.exe /f
taskkill /im prschedulemgr.exe /f
taskkill /im cdm.exe /f
taskkill /im musnotificationux.exe /f
taskkill /im npmdagent.exe /f
taskkill /im client64.exe /f
taskkill /im keysvc.exe /f
taskkill /im server_eventlog.exe /f
taskkill /im proficyserver.exe /f
taskkill /im server_runtime.exe /f
taskkill /im config_api_service.exe /f
taskkill /im fnplicensingservice.exe /f
taskkill /im workflowresttest.exe /f
taskkill /im proficyclient.exe4 /f
```

```
0x600dec: proficy administrator.exe
0x5f224e: ntevl.exe
0x5fa55a: prproficymgr.exe
0x5f200e: prrds.exe
0x5f6642: prrouter.exe
0x5f9ec6: prconfigmgr.exe
0x5f8552: prgateway.exe
0x5fb5b1: premailengine.exe
0x5f905c: pralarmmgr.exe
0x5f9dc7: prftpengine.exe
0x5fd66e: prcalculationmgr.exe
0x5fb617: prprintserver.exe
0x5fb4b2: prdatabasemgr.exe
0x5f91ac: preventmgr.exe
0x5f7356: prreader.exe
0x5f6756: prwriter.exe
0x5faf2a: prsummarymgr.exe
0x5f7d25: prstubber.exe
0x5fb7c0: prschedulemgr.exe
0x5f119e: cdm.exe
0x5fe4d4: musnotificationux.exe
0x5f8287: npmdagent.exe
0x5f76da: client64.exe
0x5f310e: keysvc.exe
0x5fca0b: server_eventlog.exe
0x5fb5c2: proficyserver.exe
0x5fbfbf: server_runtime.exe
0x5feaaa: config_api_service.exe
0x5fff0e: fnplicensingservice.exe
0x5fd592: workflowresttest.exe
0x5fb0fa: proficyclient.exe
```

Figure 2: ‘proficyclient.exe’ spelling in kill lists deployed with LockerGoga (left) and SNAKEHOSE (right)

Regardless of which ransomware family first employed the OT-related processes in a kill list or where the malware authors acquired the list, the seeming ubiquity of this list across malware families suggests that the list itself is more noteworthy than any individual malware family that has implemented it. While the OT processes identified in these lists may simply represent the coincidental output of automated process collection from target environments and not a targeted effort to impact OT, the existence of this list provides financial crime actors opportunities to disrupt OT systems. Furthermore, we expect that as financially motivated threat actors continue to impact industrial sector organizations, become more familiar with OT, and identify dependencies across IT and OT systems, they will develop capabilities—and potentially intent—to disrupt other systems and environments running industrial software products and technology.

Ransomware Deployments in Both IT and OT Systems Have Impacted Industrial Production

As a result of adversaries’ post-compromise strategy and increased awareness of industrial sector targets, ransomware incidents have effectively impacted industrial production regardless of whether the malware was deployed in IT or OT. Ransomware incidents encrypting data from servers and computers in corporate networks have resulted in direct or indirect disruptions to physical production processes overseen by OT networks. This has caused insufficient or late supply of end products or services, representing long-term financial losses in the form of missed business opportunities, costs for incident response, regulatory fines, reputational damage, and sometimes even paid ransoms. In certain sectors, such as utilities and public services, high availability is also critical to societal well-being.

The best-known example of ransomware impacting industrial production due to an IT network infection is Norsk Hydro's incident from March 2019, where disruptions to Business Process Management Systems (BPMS) forced multiple sites to shut down automation operations. Among other collateral damage, the ransomware interrupted communication between IT systems that are commonly used to manage resources across the production chain. Interruptions to these flows of information containing for example product inventories, forced employees to identify manual alternatives to handle more than 6,500 stock-keeping units and 4,000 shelves. FireEye Mandiant has responded to at least one similar case where TrickBot was used to deploy Ryuk ransomware at an oil rig manufacturer. While the infection happened only on corporate networks, the biggest business impact was caused by disruptions of Oracle ERP software driving the company temporarily offline and negatively affecting production.

Ransomware may result in similar outcomes when it reaches IT-based assets in OT networks, for example human-machine interfaces (HMIs), supervisory control and data acquisition (SCADA) software, and engineering workstations. Most of this equipment relies on commodity software and standard operating systems that are vulnerable to a variety of IT threats. Mandiant Intelligence is aware of at least one incident in which an industrial facility suffered a plant shutdown due to a large-scale ransomware attack, based on sensitive sources. The facility's network was improperly segmented, which allowed the malware to propagate from the corporate network into the OT network, where it encrypted servers, HMIs, workstations, and backups. The facility had to reach out to multiple vendors to retrieve backups, many of which were decades old, which delayed complete restoration of production.

As recently as February 2020, the Cybersecurity Infrastructure and Security Agency (CISA) released Alert AA20-049A describing how a post-compromise ransomware incident had affected control and communication assets on the OT network of a natural gas compression facility. Impacts to HMIs, data historians, and polling servers resulted in loss of availability and loss of view for human operators. This prompted an intentional shut down of operations that lasted two days.

Mitigating the Effects of Ransomware Requires Defenses Across IT and OT

Threat actors deploying ransomware have made rapid advances both in terms of effectiveness and as a criminal business model, imposing high operational costs on victims. We encourage all organizations to evaluate their safety and industrial risks related to ransomware attacks. Note that these recommendations will also help to build resilience in the face of other threats to business operations (e.g., cryptomining malware infections). While every case will differ, we highlight the following recommendations.

For custom services and actionable intelligence in both IT and OT, contact FireEye Mandiant Consulting, Managed Defense, and Threat Intelligence.

- Conduct tabletop and/or controlled red team exercises to assess the current security posture and ability of your organization to respond to the ransomware threat. Simulate attack scenarios (mainly in non-production environments) to understand how the incident response team can (or cannot) detect, analyze, and recover from such an attack. Revisit recovery requirements based on the exercise results. In general, repeatedly practicing various threat scenarios will improve awareness and ability to respond to real incidents.

- Review operations, business processes, and workflows to identify assets that are critical to maintaining continuous industrial operations. Whenever possible, introduce redundancy for critical assets with low tolerance to downtime. The right amount and type of redundancy is unique for each organization and can be determined through risk assessments and cost-benefit analyses. Note that such analyses cannot be conducted without involving business process owners and collaborating across IT and OT.
- Logically segregate primary and redundant assets either by a network-based or host-based firewall with subsequent asset hardening (e.g., disabling services typically used by ransomware for its propagation, like SMB, RDP, and WMI). In addition to creating policies to disable unnecessary peer-to-peer and remote connections, we recommend routine auditing of all systems that potentially host these services and protocols. Note that such architecture is generally more resilient to security incidents.
- When establishing a rigorous back-up program, special attention should be paid to ensuring the security (integrity) of backups. Critical backups must be kept offline or, at minimum, on a segregated network.
- Optimize recovery plans in terms of recovery time objective. Introduce required alternative workflows (including manual) for the duration of recovery. This is especially critical for organizations with limited or no redundancy of critical assets. When recovering from backups, harden recovered assets and the entire organization's infrastructure to prevent recurring ransomware infection and propagation.
- Establish clear ownership and management of OT perimeter protection devices to ensure emergency, enterprise-wide changes are possible. Effective network segmentation must be maintained during containment and active intrusions.
- Hunt for adversary intrusion activity in intermediary systems, which we define as the networked workstations and servers using standard operating systems and protocols. While the systems are further away from direct control of physical processes, there is a much higher likelihood of attacker presence.
- Note, that every organization is different, with unique internal architectures and processes, stakeholder needs, and customer expectations. Therefore, all recommendations should be carefully considered in the context of the individual infrastructures. For instance, proper network segmentation is highly advisable for mitigating the spread of ransomware. However, organizations with limited budgets may instead decide to leverage redundant asset diversification, host-based firewalls, and hardening as an alternative to segregating with hardware firewalls.

Posted in

- Threat Intelligence
- Security & Identity
