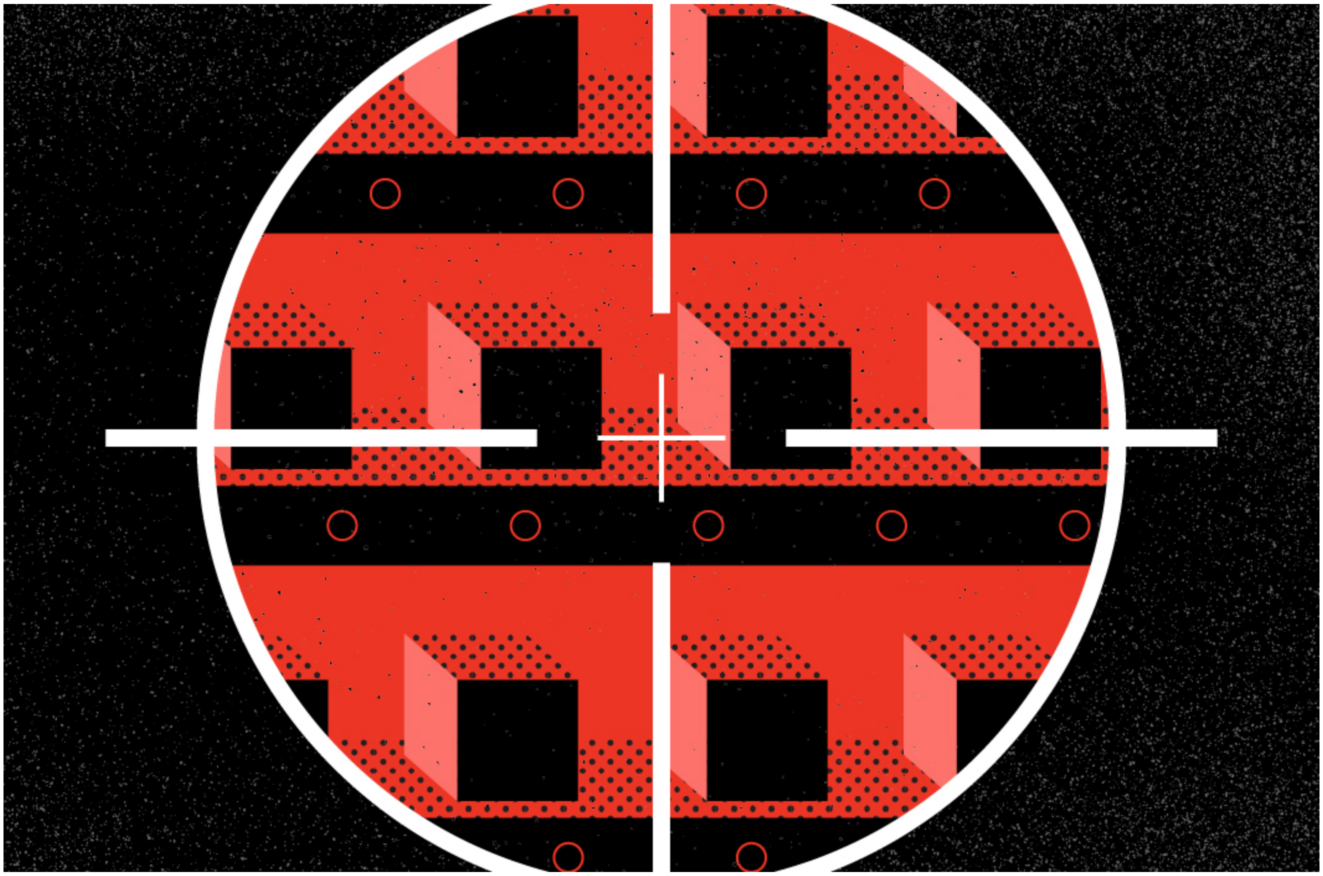
The Manufacturing Threat Landscape in 2020

crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/

Falcon OverWatch Team

July 14, 2020



Since January 2020, the CrowdStrike® Falcon OverWatch™ managed threat hunting team has observed an escalation in hands-on-keyboard activity. The COVID-19 pandemic has fundamentally shifted the way businesses are working, and adversaries are taking full advantage of businesses that fail to adapt their security postures in response.

In just the first six months of 2020, OverWatch has tracked more intrusions than were seen throughout all of 2019. The top industries impacted have been manufacturing, technology, finance, telecommunications and healthcare. This blog is part of a series from the Falcon OverWatch team, and each will be a deep dive into the types of targeted intrusions being observed in these industries.

Increases in Intrusion Numbers and Sophistication

In the manufacturing industry in particular, it is notable that an escalation in activity has occurred both in terms of the quantity and sophistication of these intrusions. The number of targeted intrusions against the manufacturing industry in just the first half of 2020 was more than triple what was observed by OverWatch throughout 2019.

Another feature of the manufacturing threat landscape is that it is one of only a handful of industries that OverWatch routinely sees targeted by both state-sponsored and eCrime adversaries.The often-critical nature of manufacturing operations and the valuable data that many manufacturing businesses hold make them an enticing target for adversary groups seeking to extract value and further their strategic objectives. CrowdStrike Intelligence has identified 10 distinct adversary groups — encompassing both state-sponsored and eCrime actors — known to intentionally target the manufacturing industry. And there are many other opportunistic adversaries that could also reasonably be expected to target the industry should the chance arise.

Big Game Hunting on the Rise

Among the intrusions uncovered this year, Overwatch has recently observed a state-sponsored actor employing novel techniques to deploy tooling within a victim environment. It is also clear that eCrime actors are continuing to adapt and evolve big game hunting (BGH) activities. Notably, the first half of 2020 has seen more BGH adversary groups adopt data exfiltration techniques and threaten data leaks to reinforce ransom demands. Further, new BGH campaigns have emerged employing ransomware capable of killing industrial control system processes (among a range of other processes).

Examples of current adversary activity targeting the manufacturing industry are explored below. Now more than ever, there is a clear impetus for defenders in the manufacturing industry to be prepared to respond to a diverse range of adversary tactics, techniques and procedures (TTPs). OverWatch expects to see this escalation of activity targeting the manufacturing industry persist throughout the remainder of 2020.

Suspected State-Sponsored Adversary Deploys Malicious Tooling via an Enterprise Application

OverWatch's discovery of an intrusion using ShadowPad malware against a manufacturing company in the North America region reveals that adversaries likely working on behalf of the Chinese state are actively exploiting newly discovered vulnerabilities to target the manufacturing industry. Interestingly, this case study demonstrates the adversary's capability to quickly operationalize newly identified vulnerabilities, giving them the potential to pursue their mission objectives at scale.

In the intrusion, uncovered earlier this year, a suspected state-sponsored adversary gained access to the victim's network by exploiting a public-facing application on the initial host. OverWatch discovered this activity shortly after it began due to a rapid succession of unusual host activities.

The combination of process-hollowing, registry changes and an interactive command shell being executed quickly captured the attention of threat hunters. Instead of attempting to move from one host to the next manually, the adversary deployed tooling using an enterprise application capable of updating its client software. Using the compromised server, they copied a malicious dynamic-link library (DLL) file named `dbghelp.dll` into place for distribution to client systems. The DLL was then executed on the client systems by the enterprise application leveraging DLL search-order hijacking.

Once the initial DLL was executed — triggered by either a user login or a host restart — it deployed two files to the operating system temporary directory `C:\Windows\temp`. The first was an embedded copy of `consent.exe`, a valid Windows executable, which was written to disk using a similar name to the affected enterprise application, and the second was a malicious ShadowPad DLL. The ShadowPad DLL masquerades as a legitimate Windows file by using the name `secur32.dll`.

```
C:\Windows\temp\[REDACTED]Update.exe
```

```
C:\Windows\temp\secur32.dll
```

The initial DLL then executed `[REDACTED]Update.exe`, which then loaded `secure32.dll` through search-order hijacking. `[REDACTED]Update.exe` made another copy of `consent.exe` and `secur32.dll` to a different directory on the host. Once these files are in place, they are executed, and the second malicious DLL is again loaded using search-order hijacking.

```
C:\ProgramData\Gateway\Algs.exe
```

```
C:\ProgramData\Gateway\secur32.dll
```

`Algs.exe` then uses process injection to hide its malicious code under `svchost.exe` and `dwm.exe`. The first attempt to execute by injecting the malicious code into `svchost.exe` was blocked by the CrowdStrike Falcon® sensor. The attacker then attempted execution under `dwm.exe`. At this point, `dwm.exe` began to communicate with adversary infrastructure masquerading as the vendor of the enterprise application. `Algs.exe` was also installed using the Windows Registry to execute when a user logs in.

```
KEY:  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
NAME: LayerGatewayService
```

```
VAL:  C:\ProgramData\Gateway\Algs.exe
```

The adversary used the backdoors on several client hosts to create a new service to establish persistence and prepare the system for credential harvesting attacks. They first queried the `Algs.exe` process to ensure it was running, then made a renamed copy of `AppLaunch.exe` and a third malicious DLL to another directory on the host.

```
C:\ProgramData\Bluetooth\BluetoothSvc.exe
```

```
C:\ProgramData\Bluetooth\mscoree.dll
```

A service was then installed on the host using a seemingly benign name. The third DLL was loaded by `BluetoothSvc.exe` and also began communicating with adversary infrastructure.

With their backdoor services in place, the adversary added a Windows Registry key to enable in-memory credential caching.

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```

At this point the adversary's session with the host ended, presumably to wait for credentials to be stored in memory for later collection.

Alerting the Victim

Within an hour of initial execution, OverWatch had notified the victim of the known compromised hosts. Overwatch quickly widened its search and was able to alert the victim to several other hosts compromised by the adversary in the same time period. Because the adversary leveraged legitimate operating system executables and authorized enterprise applications, they decreased their chances of discovery by traditional security monitoring.

Further, the three malicious files used in this intrusion were named to masquerade legitimate DLL names or at least appear benign without further analysis. OverWatch was able to discover the adversary thanks to advanced hunting capability, informed by in-depth knowledge of the tactics and techniques used by attackers. This enabled the victim organization to quickly and comprehensively contain the affected hosts and remediate the intrusion.

Subsequent analysis by CrowdStrike Intelligence indicated that the DLL files were either droppers or payloads for the ShadowPad malware. Infrastructure from command-and-control (C2) domains used by the ShadowPad malware overlapped with Bisonal malware activity in a campaign that is currently attributed to KARMA PANDA with low confidence.

Adversary Capabilities and Motivations

This adversary exhibited several interesting techniques that provide clues to their capabilities and motivations:

- First, the compromise of a vulnerability in an enterprise application to automate the deployment and execution of their toolset, combined with the deliberate methods used to execute their payloads, paints a picture of a meticulously planned intrusion. This is further supported by the absence of superfluous arguments or typographical errors in the actor's interactive commands.

- Second, the adversary’s deliberate and patient approach to credential harvesting stands in stark contrast to noisier smash-and-grab attacks that go after low-hanging fruit. The Windows Registry changes to `WDigest` node prepared the system to store the credentials unencrypted in system memory to be harvested over time. This adversary behavior is indicative of more complex motivations, perhaps the intention to return in subsequent attacks to steal intellectual property or disrupt the victim’s operations.

eCrime Adversaries Continue to Evolve Their Tactics

It is not just state-sponsored adversaries that manufacturing defenders need to be alert to. The growth of BGH activities in recent years has been well documented by CrowdStrike. These targeted, criminally motivated, enterprise-wide ransomware attacks have proliferated, and adversaries are constantly evolving their TTPs to extract maximum value from their victims. For eCrime adversaries, the manufacturing industry is an attractive BGH target, with a perceived high ability and incentive to pay.

EKANS (aka Snake) ransomware has emerged as a unique new threat to the manufacturing industry due to its reported ability to kill a wide range of processes, including those related to SCADA systems, industrial control systems, virtual machines, remote management tools and network management software, to enable encryption of files related to those systems. CrowdStrike Intelligence first reported on EKANS in January 2020. While the adversaries operating EKANS appear to be targeting organizations opportunistically, the manufacturing industry — alongside the automotive, engineering, financial and healthcare industries — is known to have been hit by this new threat.

Data extortion has proven to be another trend that the manufacturing industry needs to watch. CrowdStrike’s 2020 Global Threat Report revealed that toward the end of 2019, data extortion began to gain traction as an alternative method of monetizing BGH attacks. Adversaries have started using the threat of leaking or selling sensitive data instead of — or in combination with — ransomware to increase their chances of extracting payment.

Interestingly, Crowdstrike Intelligence found that manufacturing was the industry most targeted by data leaks in the first quarter of 2020. In late February, DOPPEL SPIDER appeared to become the latest adversary group to join this trend with the launch of the Dopple leaks (sic) website. The website, claiming to be linked to DOPPEL SPIDER, lists information stolen from past victims who failed to pay ransoms.

DOPPEL SPIDER Found in Hands-on-Keyboard Reconnaissance in a Manufacturing Environment

OverWatch threat hunters recently discovered DOPPEL SPIDER in a manufacturing environment. The intrusion, which stemmed from a successful phishing attack, followed the expected pattern of a hands-on-keyboard attack with a range of discovery techniques used to conduct reconnaissance in the environment. The intrusion was initially observed when a malicious DLL was side-loaded by legitimate executables and the victim was notified.

The use of this technique is one of the initial hunting leads that brought it to the threat hunter's attention. Later, the adversary returned and was discovered when a burst of unusual commands occurred within a short period of time.

The adversary used legitimate executables, regularly used by administrators, to gather information about the victim's Active Directory environment. The adversary created and executed batch scripts on the host, which then ran the reconnaissance commands and captured the output into text files. They then used 7zip to compress the files in preparation for exfiltration.

Reconnaissance:

```
nltest  /dclist:
```

```
adfind.exe  -subnets -f (objectCategory=subnet)
```

```
nltest  /domain_trusts
```

```
net  group "Domain Computers" /DOMAIN
```

Data Staging:

```
7.exe  a -mx3 ad.victim.7z ad_*.*
```

```
FILE: victim\ad_computers.txt
```

```
FILE: victim\ad_subnets.txt
```

```
FILE: victim\ad_users.txt
```

While the data gathered on this occasion using these commands would not contain data such as intellectual property, it is information that would be extremely useful to an attacker in furthering the intrusion. Effective threat hunting is about assessing behaviors in their specific context to identify potentially malicious activity. OverWatch recommends that defenders watch for unexpected series of commands.

Though this activity could certainly be something that an administrator would perform during the course of their duties, OverWatch threat hunters are always watching out for and digging into bursts of activity or an uncharacteristic series of commands similar to this. Without continuous hunting, these types of commands may never be discovered because security software would not see them as malicious. Because this activity was identified, the victim organization was able to take action and prevent further activity or the exfiltration of data.

Security Recommendations

These intrusions highlight the lengths to which adversaries will go to achieve their mission objectives. Both state-sponsored and eCrime adversaries have demonstrated their ability to evolve their TTPs to exploit new vulnerabilities or increase the pressure on their victims. OverWatch expects to see the manufacturing industry remain a high-frequency target through the remainder of 2020. Accordingly, defenders need to be alert to the sophisticated and diverse threats taking aim at the industry.

Threat Hunting

These case studies highlight the heightened threat environment currently facing the manufacturing industry. In both examples, adversaries used living-off-the-land (LOTL) techniques to avoid detection. Human-driven continuous threat hunting is the most effective way of identifying and derailing intrusions that leverage LOTL techniques long before adversaries can establish a foothold in the environment.

Recommendations

- **Know your environment. Being able to identify malicious activity in your environment comes down to understanding what behavior falls outside of your "normal." Be on the lookout for unusual sequences of commands, or commands being executed from unexpected hosts.**
- **Know your enemy.** Familiarize yourself with the TTPs of the adversaries that target your industry. Prioritize your hunt by focusing on those behaviors known to be prevalent in manufacturing.

Vulnerability Management

Today's adversaries move fast to operationalize exploits for newly disclosed vulnerabilities, and they have shown their capacity to roll out their attacks at scale. Defenders need to be prepared to move faster than the enemy to implement short-term workarounds or apply security patches.

Recommendations

- **Know your weaknesses.** Effectively prioritizing vulnerability management in your environment is about understanding the relative risk of any individual vulnerability, while also drawing on up-to-the-minute threat intelligence to understand what threats are most active in your region or industry.
- **Shine a spotlight on your environment. It is critical that your security team has comprehensive visibility of your environment to avoid any blind spots that could become an access point for an adversary. CrowdStrike® Falcon Spotlight™ offers security teams a real-time assessment of vulnerability exposure across their environment, enabling teams to quickly pinpoint and patch vulnerable hosts.**

Social Engineering Schemes

Due to the widespread use of COVID-19-themed phishing lures and scams and an increasing number of remote workers, employees in all industries should remain vigilant and take advantage of the resources available to enhance their security postures in the context of this new threat landscape.

Recommendation

> **Enlist your users in the fight.** While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques.

Additional Resources

- *Read the CrowdStrike Services Cyber Front Lines Report: Observations From the Front Lines of Incident Response and Proactive Services in 2019 and Insights That Matter for 2020*
- *Watch an on-demand webcast that takes a deep dive into the findings, key trends and themes from the report: CrowdStrike Cyber Front Lines Report CrowdCast.*
- *Read an eBook about securing your remote workforce during the global pandemic.*
- *Learn more about the powerful CrowdStrike Falcon platform by visiting the webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*