Hacking Farm to Table: Uncovering Threats to Agriculture

crowdstrike.com/blog/how-threat-hunting-uncovered-attacks-in-the-agriculture-industry

Falcon OverWatch and CrowdStrike Intelligence Teams

November 18, 2020

Life on the farm isn't what it used to be. With overall cyberattacks on the rise, even agriculture has found itself in the crosshairs of cyber threat actors. In fact, during the last ten months alone, the CrowdStrike® Falcon OverWatch™ team has observed a tenfold increase in interactive, or hands-on-keyboard, intrusions impacting the agriculture industry.

This blog is the latest installment in a series exploring the types of malicious hands-on-keyboard activity discovered in specific industries by OverWatch threat hunters, who work with organizations of all sizes – across all industries and in all timezones – to alert them to these threats. With still over a month to go in 2020, the OverWatch team is on track to record double the number of targeted and interactive eCrime intrusions uncovered in 2019.

Previous blogs have focused on some of this year's most frequently targeted industries such as healthcare and manufacturing. In contrast, this blog takes a deep dive into the agriculture sector, a less commonly impacted industry that has nonetheless experienced a dramatic acceleration of intrusion activity in 2020.

For insights into how other industry verticals are faring this year, check out the 2020 OverWatch Threat Hunting Report.

Why Agriculture and Why Now?

The digital transformation of the agriculture sector is expanding it from the physical world into the cyber realm. While the adoption of internet of things (IoT) and smart technologies opens the door to innovation and new efficiencies, it also exposes the sector to new cyber threats. eCrime operations are perpetually looking for new victims, especially among those larger businesses perceived to have a high capacity to pay. At the other end of the spectrum, smaller agricultural companies may be seen as soft targets, particularly those in the early stages of digitizing their businesses with less mature security infrastructure and processes. In addition, state economic interests are contributing to a heightened interest in the sector, increasing the likelihood of targeted intrusion activity. To a lesser extent, opportunistic hacktivism also presents a risk. It is crucial that defenders in the agriculture sector are aware of the complex global threat landscape that exists for this industry, and are familiar with real-world examples of how adversary activity could play out in their environment.

eCrime Threat

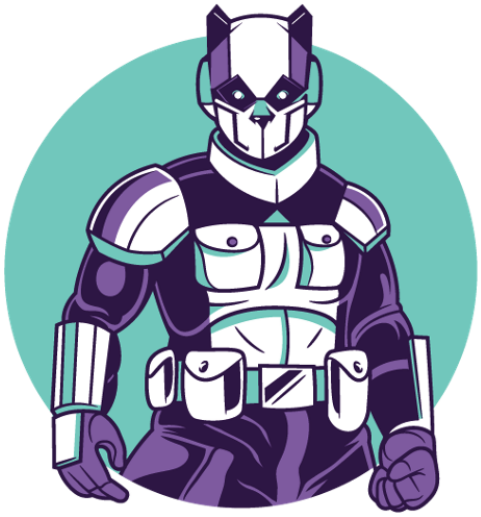
CrowdStrike Intelligence has assessed with a high degree of confidence that eCrime activity is currently the most likely cyberthreat to the agriculture industry. This is supported by OverWatch findings — nearly 80% of interactive intrusions in the agriculture industry in 2020 were perpetrated by suspected eCrime adversaries (of those intrusions where attribution was possible).

Large agriculture sector businesses may be viewed as a valuable target by eCrime adversaries. In "big game hunting" (BGH) ransomware campaigns, adversaries will adjust their ransom demands based on a company's size and perceived capacity to pay, often resulting in ransoms in the millions of dollars. Organizations should also be aware that the use of data extortion is increasing among BGH adversaries. Adversaries use this strategy to increase the likelihood that even those companies with effective data-backup systems can be pressured to pay ransoms to protect sensitive data from being leaked.

The proliferation of these data encryption and extortion activities has prompted a wide variety of government policy interventions aimed at both crime prevention and consumer protection. The onus is on organizations to not only ensure adequate security

protections are in place, but to also be aware of any regional regulatory obligations that relate to protection of data and dealings with criminal entities.

Targeted Threat



The agricultural industry is at risk of economically motivated targeted intrusions seeking intellectual property or other sensitive business information. More extreme weather patterns, water scarcity and diminishing availability of productive

land haveencouraged innovation in agricultural processes, tools and crop varieties. This intellectual property is a valuable target for countries seeking to grow their agricultural outputs and boost their competitive advantage relative to regional neighbors. In particular, CrowdStrike Intelligence has highlighted Democratic People's Republic of Korea (DPRK)-nexus and China-nexus adversaries as the leading threats. This is again consistent with OverWatch threat hunting data, which has uncovered both DPRK- and China-nexus actors involved in intrusions against the agriculture sector in 2020. The following table summarizes likely motivations and adversary groups involved in these espionage activities.

Democratic People's Republic of Korea (DPRK, or North Korea)	China

Self-sufficiency is a core tenet of the DPRK's underlying political philosophy, and agricultural independence is seen as a key enabling factor for the country's growth. Despite the DPRK's long-held ambitions to achieve agricultural self-sufficiency, efforts to modernize and expand the sector have faced repeated setbacks. These include a lack of arable land, widespread natural disasters and limited access to many crucial agricultural inputs due to DPRK's government-controlled economy. In this context, CrowdStrike Intelligence assesses that proprietary information related to agricultural production would likely be a significant asset to the DPRK's agricultural programs. Two DPRK-nexus targeted intrusion adversary groups associated with agricultural sector targeting — LABYRINTH CHOLLIMA and SILENT CHOLLIMA — are assessed to conduct espionage operations in support of the DPRK's Reconnaissance General Bureau (RGB) Bureau 121, which could support the country's agricultural development goals.

China is the world's largest agricultural producing nation, despite a limited amount of arable land relative to the country's size. The sector accounts for approximately 10% of China's total gross domestic product (GDP) and employs more than a quarter of the country's workforce. For these reasons, the agricultural sector is inexorably tied to Chinese economic growth.
China-nexus adversary groups engage in aggressive economic espionage campaigns to forcibly transfer proprietary technology and intellectual property from advanced industrial nations, with the goal of spurring economic development.

Many of these campaigns have targeted the 10 industrial areas highlighted in Beijing's "Made in China 2025 Plan," which includes agricultural machinery.

The China-nexus adversary WICKED PANDA is known to target the agricultural sector for likely economic espionage goals.

Hacktivist Threat

Finally, agriculture is a sector that attracts attention from a diverse range of interest groups, among them animal rights and environmental protection activists. While the threat level is perceived to be low, organizations in this industry should remain alert to the possibility of opportunistic hacktivist activity.

Follow the Hunt

The intrusion story below explores an incident involving a CrowdStrike Falcon® platform customer in the agriculture sector that did not have Falcon deployed to all workloads in its network. One of the unmonitored hosts, not covered by Falcon, became the weak point in the business's cyber defenses. This single host became a beachhead from which an eCrime adversary was able to achieve lateral movement and commence credential harvesting activities. CrowdStrike strongly recommends customers deploy full sensor coverage across their environment to ensure that there are no weak points in their defense. This case study shows how quickly an eCrime adversary can navigate a victim's environment once they have managed to gain access. It also details how OverWatch threat hunters acted equally rapidly to find the intrusion and enable this agricultural business to eradicate the adversary from their environment, despite only having limited visibility within the network environment.

Threat Hunting Enables Timely Pest Control Against SPIDER Adversary

Recently, Falcon OverWatch discovered a suspected interactive SPIDER (aka eCrime) intrusion against a large agriculture company. In the early morning, outside of the customer's normal operating hours, OverWatch hunters uncovered suspicious discovery commands being executed on a Windows host under a process that was unique in the customer's environment. OverWatch regularly uses telemetry from across the global Falcon install base to rapidly identify activity that is anomalous and worthy of further investigation. In this instance, the unique binary was:

```
FILE: C:\Windows\IntelliAdminRPC\RemoteExecute.exe
```

```
HASH: aa63dfec54e9bdf529fdad1fe47eee45391a99b007878abf56a490b023e6b245
```

This binary is associated with commercially available remote administration software. However, the hunters recognized it as only present on this one host within this customer's network environment, along with suspicious commands spawned from it, so they continued hunting further.

Within the first three minutes of establishing a presence on the host, the adversary executed several basic initial reconnaissance commands using the `RemoteExecute.exe` process:

```
ver
```

```
systeminfo
```

```
net group \"Domain Admins\" /domain
```

```
netstat -ano -p tcp
```

OverWatch threat hunters immediately notified the victim of the suspicious activity before commencing a more detailed investigation into the source of the intrusion.

Retracing the Adversary's Steps

OverWatch found that the `RemoteExecute.exe` binary was written to the victim host by another host within the network's VPN range. That other host did not have the Falcon sensor installed, which meant that OverWatch did not have visibility to identify the intrusion at initial access. This allowed the adversary to establish an internal beachhead from which they executed their commands remotely.

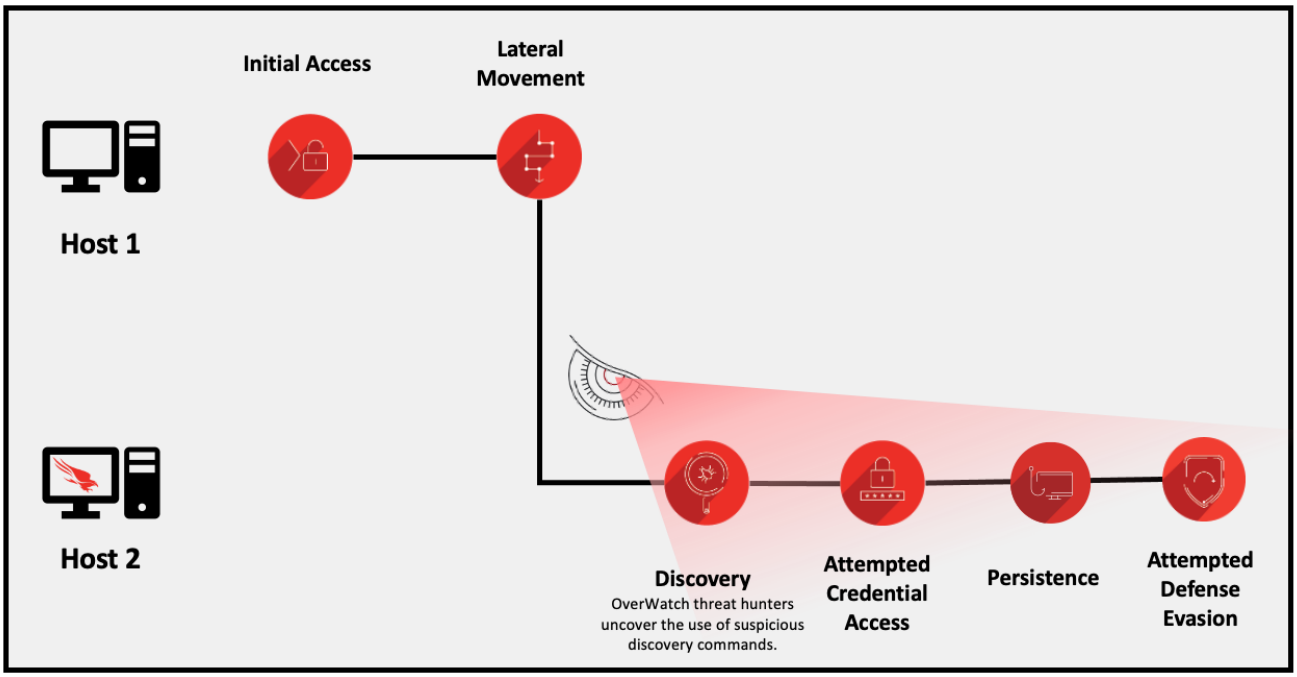


Figure 1. Intrusion sequence showing the adversary's movement between hosts (click image to enlarge)

Five minutes after gaining access to the host OverWatch could see, the adversary modified the registry to implement a widely known procedure that enables credentials to be stored in clear text within memory, facilitating credential theft:

```
reg  add hklm\system\currentcontrolset\control\securityproviders\wdigest /v UseLogonCredential /t REG_DWORD /d 1 /F
```

Roughly 15 minutes later, after running additional basic host and network discovery commands, the adversary ran the following command:

```
"c:\windows\system32\cmd.exe"  /c rundll32 C:\windows\system32\comsvcs.dll, MiniDump 576 c:\windows\temp\TMPdx12.dmp full
```

This is an example of a known technique for creating a minidump of the LSASS process to extract credentials without using Mimikatz. In this particular method, the adversary abused the Windows native `comsvcs.dll` dynamic link library (DLL), executing the binary via `rundll32.exe` to perform the credential dumping. This binary is generally associated with legitimate Windows COM+ Services. Thanks to the Falcon sensor's defenses, the credential dumping attempt did not succeed.

Next, the adversary executed the script `%SYSTEMROOT%\IntelliAdminRPC\inst.bat`, which resulted in a series of commands consistent with those within a publicly shared registry file. In doing so, the adversary implemented a form of Component Object Model (COM) hijacking in an attempt to create persistence and execute their tooling without detection. The adversary next attempted to finalize persistence by registering a scheduled task masquerading as "GoogleUpdates" in order to spawn their backdoor every 30 minutes:

```
"c:\windows\system32\cmd.exe" /c cmd /c schtasks /create /F /SC minute /MO 30 /TN "\UpdateTasks\GoogleUpdates" /TR "rundll32 /sta {[CLSID for Hijacked COM Object]}"
```

It is unclear if the adversary's `inst.bat` script functioned as intended, as they proceeded to run it multiple times over the course of the next hour. This activity took place concurrently with further account, host and network discovery.

During that time period, the adversary also attempted to save the SAM and SYSTEM registry hives for attempted credential access and created a new user account with a password set to not expire. Next, they executed the following commands to employ further variations of attempted credential dumping, but Falcon blocked these efforts as well:

```
powershell  -ep bypass "Import-Module c:\windows\system32\catroot\mini.ps1;Get-Process lsass | Out-Minidump"
```
(Likely the PowerSploit Minidump script)

```
procdump64.exe  -accepteula -ma lsass.exe dmp.se.dmp
```

Threat hunting ensured the timely discovery and disruption of this eCrime intrusion. OverWatch tracked the adversary from the initial attempt to access a Falcon-protected endpoint until the customer used the Falcon platform to isolate the victim host, containing the intrusion and avoiding a potential breach. After the immediate threat was addressed, OverWatch reviewed all related malicious activity in detail. Hunters used this information to hone their preparation for this adversary by identifying features of these malicious actions that will inform future threat hunting efforts. Feeding key observations like this into future hunting leads is an essential part of the iterative threat hunting process, as described in a blog outlining the OverWatch SEARCH hunting methodology.

This incident also serves as an important reminder of the very real threat that eCrime poses to the agriculture sector. This is particularly true in the context of the sudden and unprecedented spike in intrusion activity that OverWatch has recorded in this sector in recent months. Businesses that have until now considered themselves an unlikely target for interactive threats should take notice of the shifting cyber landscape. Now is the time to look at measures to mature security posture preemptively.

While this attack could have been opportunistic rather than specifically focusing on an agriculture target, it is at least indicative of the threats agriculture organizations face. For another case study of how OverWatch threat hunting uncovered and stopped an interactive intrusion against a global agriculture company, be sure to check out the 2020 OverWatch Threat Hunting Report. The story *Hunting Thwarts LABYRINTH CHOLLIMA Attack Launched Over Social Media* walks through an intrusion perpetrated by a state-sponsored adversary.

Security Recommendations

Threat Hunting

The eCrime intrusion chronicled in this blog demonstrates the critical importance of threat hunting supported by comprehensive visibility across the environment at all hours of the day. In this case, the lack of OverWatch visibility into the initially compromised host enabled the adversary to establish a beachhead on this unmonitored part of the network. Yet despite having gained access to the network through the customer's VPN pool, proactive threat hunting was there to catch them as soon as they tried to perform actions on endpoints covered by Falcon. Further, despite this intrusion taking place in the early morning, the Overwatch team's continuous hunting meant that the breach was rapidly discovered and reported, so the victim could disrupt the adversary and stop the breach before further impact.

- We strongly recommend that defenders implement proactive threat hunting as part of their defense-in-depth strategy, to support the timely discovery and disruption of adversary tradecraft designed to evade detection by systems built on technology alone.
- Organizations should also deploy capabilities that provide their threat hunters with full visibility across the entire network's workloads to avoid blind spots that can become a safe haven for adversaries.
- Finally, it is crucial that organizations employ *continuous* threat hunting. The longer an adversary has access to your network, the greater the risk of serious impact to your operations. OverWatch's 24/7/365 hunting ensures that adversaries have nowhere to hide, even when your staff is off the clock.

Security Hygiene

It is crucial to plug gaps in your defenses. OverWatch routinely sees adversaries finding and exploiting the weakest point of entry. All too often, that point of weakness is an organization's VPN or another remote access setup, but it can also be an unpatched vulnerability or simply the part of a victim's environment without Falcon sensor coverage.

> Defenders should regularly monitor VPN and other remote access account behavior to identify anomalous behavior, particularly given the increase in remote work many organizations have implemented due to COVID-19.

Know Your Adversary

The best defenses are always built on the latest and most comprehensive cyber threat intelligence. OverWatch threat hunters and Crowdstrike Intelligence work hand-in-hand to continually feed the threat intelligence lifecycle, allowing you to stay one step ahead of the adversary.

> Defenders in all settings should develop a deep understanding of the threat landscape for their organization. Staying up-to-date with key adversaries, their motivations, and their tactics, techniques and procedures (TTPs) will support data-backed, proactive security decisions.

Additional Resources

- *Download the 2020 OverWatch Threat Hunting Report.*
- *Register for the webcast to hear CrowdStrike threat hunting experts discuss report findings.*
- *Visit the CrowdStrike Falcon OverWatch webpage.*
- *Download the CrowdStrike 2020 Global Threat Report.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*