Whitepaper

HOW DRAGOS ACTIVITY GROUPS OBTAIN INITIAL ACCESS INTO INDUSTRIAL ENVIRONMENTS

Conor McLaren
Senior Threat Intelligence Analyst
Threat Intelligence | Dragos, Inc.

info@dragos.com
@DragosInc

As the threat landscape continues to evolve with a perpetual influx of new network anomalies and Indicators of Compromise (IOC), prudent defenders must focus on more actionable elements of attack characteristics, such as Tactics, Techniques and Procedures (TTPs). One such example of this is the Initial Access Tactic.

An adversary uses Initial Access techniques to gain an initial foothold within a victim environment.[1] This is perhaps one of the most crucial tactics that adversaries use as part of an intrusion, as most attacks (excluding those such as denial of service) are not successful without first obtaining this access into the target environment. As such, defenders consider it a critical dependency of all other tactics.

While some adversaries see initial access as the means to perform further actions on objectives, a number of Dragos Activity Groups focus on developing and obtaining initial access against industrial organizations. A prime example of this is PARISITE's exploitation of known VPN vulnerabilities in order to obtain initial access and enable further operations for the MAGNALLIUM Activity Group.[2] Given this characteristic, eliminating (or reducing) initial access vectors can prove to be a successful method of thwarting many intrusion attempts, particularly when there is consistency in the underlying adversarial techniques.

This white paper steps through the most common initial access techniques Dragos observes being utilized by activity groups in order to equip defenders with some of the vital elements of threat behavior knowledge and thus address the associated risks.

Industrial Control Systems/Operational Technology (ICS/OT) organizations should be well-versed in Initial Access Techniques for the following reasons:

- Initial access is the pre-requisite to further stages of an attack and therefore focusing on this tactic can aid in the prioritization of efforts for defenders.
- The rapidly changing nature of network anomalies and IOCs mandates the focus on threat behaviors, such as the more slowly changing TTPs.
- While direct access to an ICS/OT environment is considered the code red of initial access scenarios, gaining access to a corporate/IT network can act as a precursor to an ICS/OT pivot.
- Numerous Dragos-tracked Activity Groups have been known to explicitly target/develop initial access to industrial organization environments.

MITRE ATT&CK FOR ICS FRAMEWORK: THE INITIAL ACCESS TACTIC

MITRE ATT&CK for ICS is a community-sourced framework for identifying malicious threat behaviors, specifically the tactics and techniques of the adversaries in industrial control systems (ICS).[3] Dragos significantly contributed to this community-supported knowledgebase with findings from our customers and insights from our services and intelligence efforts. Dragos maps its technology and services to MITRE ATT&CK for ICS and is the first ICS vendor to fully integrate MITRE ATT&CK for ICS into its platform.

MITRE ATT&CK for ICS outlines twelve individual techniques within the Initial Access tactic, spanning from spearfishing to the exploitation of public-facing applications. While many of these techniques are shared by the MITRE ATT&CK enterprise framework, 40 percent of the listed techniques are exclusive to the ICS framework.

Every technique within this tactic ultimately endeavors to achieve one primary objective: gain access to the target environment. However, the actual entry vectors differ greatly between each of the techniques. Additionally, while each technique can exist in isolation, some may also be utilized together to achieve initial access into the target environments.

MITRE ATT&CK FOR ICS Initial Access [TA0001]

- **Drive-By Compromise [T0817]**
- **Exploit Public-Facing Infrastructure [T0819]**
- **Exploitation Of Remote Services [T0866]**
- **External Remote Services [T0822]**
- **Internet Accessible Device [T0883]**
- **Remote Services [T0886]**
- **Replication Through Removable Media [T0847]**
- **Rogue Master [T0848]**
- **Spearfishing Attachment [T0865]**
- **Supply Chain Compromise [T0862]**
- **Transient Cyber Asset [T0864]**
- **Wireless Compromise [T0860]**

Figure 1: The MITRE ATT&CK for Industrial Control Systems Initial Access Techniques

OBSERVED INITIAL ACCESS TECHNIQUES BY KNOWN ACTIVITY GROUPS

The following are initial access techniques that Dragos has observed known Activity Groups using to gain access into industrial organizations.

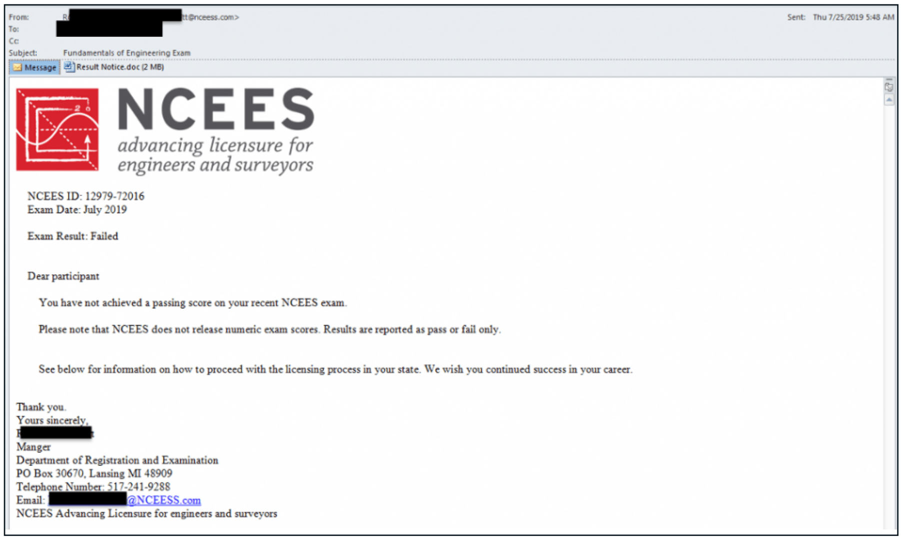
Spearphishing Attachment [T0865]

The Spearphishing attachment technique forms the most frequently observed Initial Access technique amongst the Dragos-tracked Activity Groups – with at least 10 out of the 15 AGs utilizing this technique.[4] These ten groups are shown by their tokens below.

- AL ALLANITE
- Ch CHRYSENE
- Co COVELLITE
- Dy DYMALLOY
- Hx HEXANE
- Ka KAMACITE
- Ma MAGNALLIUM
- St STIBNITE
- Ta TALONITE
- Wa WASSONITE

Spearphishing differs from conventional phishing in the way that adversaries specifically target a victim, with the associated email often containing tailored information to instill a false sense of legitimacy. While other forms of spearphishing (such as those facilitating credential access) may also eventually lead to initial access, for example via enabling access to remote services, the MITRE ATT&CK for ICS spearphishing attachment technique explicitly refers to an adversary sending malware via email.[5]

A prime example of this technique in use is TALONITE's utilization of engineering-themed spearphishing emails to deliver malicious documents and executables, such as the FlowCloud malware, which has been deployed against the United States Electric sector.[6]



From: R[redacted]tt@nceess.com>
To: [redacted]
Cc:
Subject: Fundamentals of Engineering Exam
Sent: Thu 7/25/2019 5:48 AM

NCEES ID: 12979-72016
Exam Date: July 2019

Exam Result: Failed

Dear participant

You have not achieved a passing score on your recent NCEES exam.

Please note that NCEES does not release numeric exam scores. Results are reported as pass or fail only.

See below for information on how to proceed with the licensing process in your state. We wish you continued success in your career.

Thank you.
Yours sincerely,
[redacted]
Manger
Department of Registration and Examination
PO Box 30670, Lansing MI 48909
Telephone Number: 517-241-9288
Email: [redacted]@NCEESS.com
NCEES Advancing Licensure for engineers and surveyors

Figure 2: TALONITE's engineering-themed phishing email

Despite the widespread knowledge of this technique, adversaries continue to utilise spearphishing attachments, largely owing to the continued success of the technique and the relative ease in execution. Thankfully, security measures such as end-user security awareness training paired with a multi-layered approach to security can be highly effective in minimising the risk of further follow-on activity.

Supply Chain Compromise [T0862]

At least 6 out of the 15 Dragos Activity Groups have leveraged the Supply Chain Compromise technique to facilitate initial access.

AL ALLANITE

Ch CHRYSENE

Dy DYMALLOY

Hx HEXANE

Ra RASPITE

Xt XENOTIME

The Supply Chain Compromise technique is defined within the MITRE ATT&CK for ICS Initial Access tactic as “the manipulation of products, such as devices or software, or their delivery mechanisms before receipt by the end consumer.[7]” While the targeting of the supply chain forms the distinctive initial component of the attack, the objective is to compromise the target environment/end-consumer in mind.

While software updates and routine patching are frequently abused, these are not the only potential entry vector in a supply chain intrusion. Original Equipment Manufacturers (OEM), vendors, and third-party contractors could provide an ingress into ICS/OT environments via compromised or poorly secured direct network connections and remote access connections.

The last 12-18 months has been saturated with numerous examples of supply chain compromises, such as the SolarWinds incident amongst many others.[8] Nevertheless, one of the most notable examples in an ICS/OT context is XENOTIME’s compromise of ICS vendors and manufacturers, which provided potential supply chain threat opportunities and vendor-enabled access to target ICS networks.[9]

A key defensive recommendation in relation to supply-chain compromises is to ensure that third-party connections and OT interactions are monitored and logged, while adopting a “trust, but verify” approach. Adding to this, it is important (where possible) to isolate or create demilitarized zones (DMZs) for such access to ensure that third parties cannot gain complete access to the entire OT network. Additionally, Dragos recommends that defenders explore the implementation of features such as jump hosts, bastion hosts, and secure remote authentication schema wherever possible. Finally, as a proactive measure, it is also recommended that organizations conduct third party security reviews when evaluating potential vendors.

Exploitation of Remote Services and/or Public-Facing Applications [T0866 & T0819]

The exploitation of public-facing applications and/or remote services techniques have been utilized by at least five Dragos activity groups as part of initial access operations.

- ELECTRUM
- KAMACITE
- PARISITE
- VANADINITE
- XENOTIME

The exploitation of public-facing applications and/or remote services techniques refer to the exploitation of a vulnerability or weakness in the underlying software, which yields access to the associated victim host. [10,11] While MITRE ATT&CK for ICS classifies these two exploitation types as different techniques, for the purpose of this whitepaper they have been listed together given their similarities in mitigative measures. It is important to note that exploitation of public-facing applications may also be paired with other initial access techniques. For example, a vulnerability in a strategically significant website could be exploited to facilitate the hosting of malicious code, which could later be used as part of drive-by compromises.

One such example of the Exploitation of Remote Services Technique [T0866] is PARISITE's targeting of ICS/OT organizations using known Virtual Private Network (VPN) vulnerabilities. PARISITE successfully leveraged exploits against vulnerabilities affecting Fortinet, PulseSecure and Palo Alto Networks appliances in order to successfully develop initial access to the victim environments.[12]

An additional contemporary (and now almost exhaustively publicized) example of this technique is the widespread exploitation of the Log4j vulnerability in order to achieve remote code execution and thus initial access to a plethora of victims, many of whom were industrial organizations.[13] In cases such as these, the existence of public exploits can lower the barrier of entry to utilizing this technique for initial access, which can increase the prevalence of intrusion activity tied to a particular vulnerability.

Given that both the exploitation of public-facing applications and/or remote services techniques often involve the existence of known vulnerabilities, adopting a regular patching routine is paramount to reduce the incidence of this vector. However, in some scenarios, patching alone may not suffice, thus placing a greater reliance on the additional controls and mitigations such as multi-layered security paired with proactive threat hunting and the application of threat intelligence products.

Drive-By Compromise [T0817]

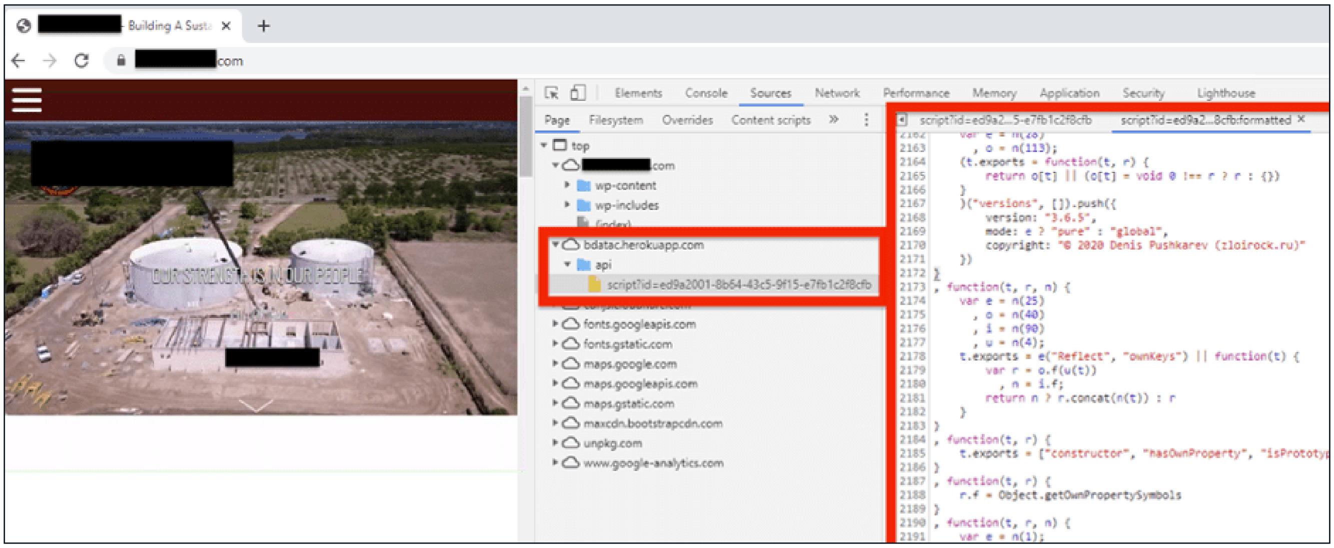
The Drive-By Compromise technique has been leveraged by at least four out of the 15 Dragos Activity Groups to obtain initial access.

- ALLANITE
- DYMALLOY
- RASPITE
- STIBNITE

This technique refers to initial access being achieved when a victim is exploited upon visiting a compromised website.[14] In instances where specific targeting is involved, for example, compromising a known website that is frequently visited by the intended victim, it is referred to as a watering hole attack or a strategic web compromise. Drive-by compromises (much like many other techniques) can also be the primary technique or conversely a single component of a collection of techniques. For example, an adversary could use a compromised website to host credential stealing code and/or facilitate the delivery of malware, both of which could subsequently provide initial access.

One such example of this technique within an ICS/OT context is DYMALLOY's hosting of malware on compromised industrial-related websites to facilitate credential theft and subsequent initial access, before leveraging a range of commodity malware such as Goodor, DorShel, and Karagany, in addition to the overt credential dumping tool Mimikatz.[15]

However, not all drive-by compromises facilitate initial access. This technique can also be leveraged as part of a wide variety of campaigns – a prime example being the watering hole on a Florida water utility contractor website, which Dragos discovered and associated with a malicious data gathering campaign.[16]



```
    var e = n(26)
      , o = n(113);
    (t.exports = function(t, r) {
        return o[t] || (o[t] = void 0 !== r ? r : {})
    }
    )("versions", []).push({
        version: "3.6.5",
        mode: e ? "pure" : "global",
        copyright: "© 2020 Denis Pushkarev (zloirock.ru)"
    })
}
, function(t, r, n) {
    var e = n(25)
      , o = n(40)
      , i = n(90)
      , u = n(4);
    t.exports = e("Reflect", "ownKeys") || function(t) {
        var r = o.f(u(t))
          , n = i.f;
        return n ? r.concat(n(t)) : r
    }
}
, function(t, r) {
    t.exports = ["constructor", "hasOwnProperty", "isPrototyp
}
, function(t, r) {
    r.f = Object.getOwnPropertySymbols
}
, function(t, r, n) {
    var e = n(1);
```

Figure 3: Florida water utility contractor website compromised with a unique browser enumeration and fingerprinting script

One of the challenges associated with drive-by compromises, and especially those that are targeted in nature, is often that legitimate and frequently browsed (by the victims) websites are compromised. This deems content-based filtering to be somewhat ineffective and instead places an increased emphasis on pairing end-user training with actions such as hypothesis-driven threat hunting, for example to identify suspicious data transfer volumes to known websites above the defined baseline. Finally, threat detection solutions such as those offered by the Dragos platform are also critical in preventing follow-on activity.

CONCLUSION

Initial access is one of the most important adversarial tactics and may form the critical dependency on which further tactics rely, or conversely it may be the end goal in itself. Irrespective of the adversary's intent, preventing successful initial access is paramount in preventing successful intrusions against your organization.

Monitoring for threat behaviour paired with comprehensive asset visibility is critical in preventing follow-on activity that stems from the initial access techniques listed in this blog. The Dragos Platform is an industrial control systems (ICS) cybersecurity technology that delivers unmatched visibility of your ICS/OT network assets and communications, rapidly pinpoints threats through intelligence-driven analytics, and provides best-practice playbooks to investigate and respond to threats before they cause significant impacts to your operations, processes, or people.

Defenders should also take advantage of the more slowly-changing nature of TTPs (relative to IOCs) and utilize actionable threat intelligence to priortise their efforts. Dragos threat intelligence leverages the Dragos Platform, our threat operations center, and other sources to provide comprehensive insight into threats affecting industrial control security and safety worldwide. Dragos focuses on threat behaviors and appropriate detection and response, which as highlighted in this blog, is essential in defending against the modern-day adversary.

Looking forward, Dragos assesses with high confidence that adversaries will continue to target ICS/OT organizations using initial access techniques such as spearfishing attachments, supply chain compromises, drive-by compromises, and via the exploitation of remote services and/or public-facing applications.

While this whitepaper provided a high-level overview of the initial access techniques deployed by Dragos Activity Groups, Dragos does not publicly describe ICS/OT activity group technical details except in extraordinary circumstances in order to limit tradecraft proliferation. However, full details on a range of initial access techniques and campaigns are available to network defenders through Dragos WorldView Threat Intelligence, a subscription offering that provides the latest threat intelligence to you on a daily and weekly basis.

REFERENCES

1 Initial Access – MITRE ATT&CK®

2 PARISITE – Dragos

3 ATT&CK® for Industrial Control Systems – MITRE

4 2021 ICS CYBERSECURITY YEAR IN REVIEW – Dragos

5 Spearphishing Attachment – MITRE

6 New ICS Threat Activity Group: TALONITE – Dragos

7 Technique/T0862/ – MITRE

8 Attacks on the Supply Chain and Critical Infrastructure – Dragos

9 XENOTIME – Dragos

10 Exploit Public-Facing Application – MITRE

11 Exploitation of Remote Services – MITRE

12 PARISITE – Dragos

13 Implications of Log4j Vulnerability for Operational Technology (OT) Networks – Dragos

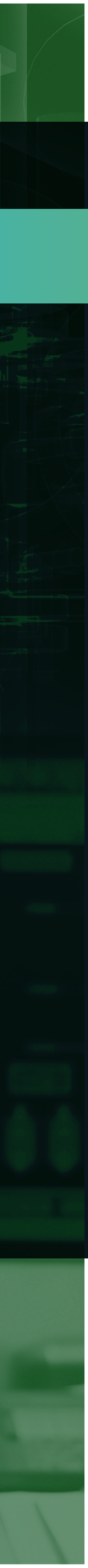
14 Drive-by Compromise – MITRE

15 DYMALLOY – Dragos

16 When Intrusions Don't Align: A New Water Watering Hole and Oldsmar – Dragos

TAGS:

Frontline Perspective, MITRE ATT&CK, Initial Access, Conor McLaren



ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT

www.dragos.com.

THANK YOU