DRAGOS
SAFEGUARDING CIVILIZATION

YEAR IN REVIEW

2018

ICS ACTIVITY GROUPS AND THE THREAT LANDSCAPE

The Dragos Intelligence team discusses threat activity groups targeting ICS in 2018 and provides details of their activity, methodologies, victimologies, and future concerns.

CONTENTS

EXECUTIVE SUMMARY

Throughout 2018,

the amount of activity targeting industrial control systems (ICS) increased substantially. Dragos identified three new activity groups adding to the five we discovered in 2017. This is consistent with previous Dragos assessments – as our capabilities in threat hunting and identification of ICS-focused threats expand, we achieve greater visibility into the threat landscape and can create a more holistic picture of the threats, behaviors, and tradecraft affecting ICS environments.

ICS security risk grew in 2018 even absent any destructive attacks. This year, four major elements contributed significantly to greater risk:

1) More numerous intrusions into ICS networks enabling research and reconnaissance of ICS operations and technology
2) Commodity malware and wormable ransomware causing ICS infections
3) Infrastructure-targeting activity groups adopting Living off the Land tactics and behaviors that bypass traditional security protection mechanisms
4) The compromise of several industrial control equipment manufacturers enabling potential supply-chain threats and vendor-enabled access to ICS networks

Adversaries using traditional malware and techniques to make the jump from IT to operations continued to be a major issue across ICS, including continued WannaCry infections impacting ICS environments. Olympic Destroyer,[1] though not specifically targeted to ICS, provided an example of how operational systems may be impacted through future wormable malware that avoids the use of exploits.

In 2018, Dragos identified three more activity groups targeting ICS: ALLANITE, XENOTIME, and RASPITE, the latter of which is linked to newly-identified behavior targeting US electric utilities. ALLANITE targeting also includes electric utilities in the US, in addition to UK entities. XENOTIME, the activity group associated with TRISIS, expanded its operations beyond the Middle East and the Triconex safety instrumented system including compromising several ICS manufacturers. Dragos also identified new behaviors and victimology from adversaries first discovered in 2017.

Dragos identified no new malware with life-threatening or ICS-specific destructive capabilities. However, numerous intrusions into ICS networks stole the type of information that would be valuable to future ICS-disruptive capabilities such as HMI screenshots and process historian information. We anticipate increased risk of operational losses due to incidental malware infections in ICS environments; the results of mishaps during initial intrusion and reconnaissance operations within the OT realm; and new disruptive attacks based on the results of increasing research and reconnaissance activity. Malicious activity is increasing, and it will have large impacts – but there are people hard at work securing infrastructure to defend against the growing threat landscape.

This year Dragos championed private sector collectives like the Cyber Threat Alliance[2] and government cooperation to promote critical infrastructure cybersecurity.[3] Recognizing that smaller entities provide an environment for adversaries to train and prepare undetected, as well as localized attacks, Dragos also began work on Neighborhood Keeper,[4] a research and development effort done in concert with the Department of Energy, Idaho National Labs, the Electric ISAC, Ameren, First Energy, and Southern Company, to bring affordable threat detection technology and shared insight to a broader set of infrastructure providers.

Further, Dragos provided a variety of public resources including monthly webinars[5] and ICS security training for practitioners looking to expand their knowledge of ICS and threats facing these industries.

[1] https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
[2] https://www.cyberthreatalliance.org/press-releases/cyber-threat-alliance-continues-strong-growth-new-members-alienvault-dragos-lastline-nec/
[3] https://www.energy.senate.gov/public/index.cfm/2018/3/full-committee-hearing-to-examine-cyber-security-in-our-nations-critical-energy-infrastructure-030118
[4] https://dragos.com/neighborhood-keeper.html
[5] https://www.dragos.com/webinars.html

THREATS IN DETAIL

Dragos witnessed a concerning number of ICS threats targeting vendors, integrators, original equipment manufacturers (OEMs), and other third-party OT players. Of all threats, the following are the most concerning to Dragos.

- DISRUPTIVE IT MALWARE
- MID-POINT NETWORK ACCESS
- SUPPLY CHAIN/ THIRD-PARTY COMPROMISE
- SIGNIFICANT TTPs

Disruptive IT Malware

IT malware impacting operations is not new or unique,[6] and Dragos expects these types of infections will continue to be prevalent for years to come due to ease of use, effectiveness within enterprise environments, and the widely-available nature of commodity malware.

WannaCry and wormable ransomware leveraging vulnerabilities detailed in Microsoft bulletin MS17-010 continues to be a major threat to ICS. The MS17-010 vulnerabilities were first weaponized in May 2017, and despite patches being available since spring of that year, many enterprises – especially those within the OT space – have not or cannot update machines due to poor patch management, refusal to accept downtime, or system end-of-life considerations.

This remains a continuing threat. In August, an operational error during software installation at Taiwan Semiconductor Manufacturing Company caused a WannaCry infection and affected over 10,000 machines, leading to a financial impact of at least $250 million.[7]

Olympic Destroyer — the malware known for causing a network disruption during the PyeongChang 2018 Winter Olympic Games — represented another IT-focused malware with the potential to bridge the IT-ICS gap. Although not an immediate threat to ICS networks, Olympic Destroyer provides an example for exploit-less propagation within a victim network paired with a disruptive effect that could cause significant disruption in ICS environments.

[6] https://dragos.com/blog/mimics/

[7] https://www.theregister.co.uk/2018/08/06/tsmc_malware/

Mid-point Network Access

In May, researchers identified VPNFilter router malware targeting small office/home office (SOHO) network devices and some commercial equipment that harvested information, stole credentials, and could cause a denial of service. While this malware does not appear to be targeted towards ICS, a Ukrainian chemical plant reportedly identified VPNFilter[8] on its network. The malware alone does not have destructive capabilities, however information gathered could further lead to a damaging attack. SOHO equipment is sometimes connected to ICS environments in an out-of-band manner without approval from IT departments, thus a VPNFilter infection could cause major issues.

[8] https://dragos.com/blog/20180716UkraineChemicalPlantEvent.html

Supply Chain/Third-party Compromise

Third-party access to OT networks is a common and necessary component of modern operations. However, the OT network access granted to vendors and others can also expose an asset operator to significant risk as compromises can move from vendors' networks to the asset operator's network. Third-party or supply chain[9] compromise leverages explicit trust between parties and bypasses a large part of the security stack, potentially including perimeter defenses, such as firewalls or proxy servers, to access a target. Once an adversary accesses the victim network, it is possible to pivot throughout the network, steal credentials or other sensitive data, and further embed themselves within IT or operations.

Most concerning to Dragos are several compromises of ICS vendors and manufacturers in 2018 by activity associated with XENOTIME, providing potential supply chain threat opportunities and vendor-enabled access to asset owner and operator ICS networks. We suspect that there are other unknown manufacturer/vendor compromises and that this trend will continue because the value of such access is high. Other significant activity of interest involves the compromise of legitimate websites enabling exploitation and access of networks when engineers and operators access these sites or download legitimate-looking software (e.g., ICS watering holes).

In April, a business tool used by a number of energy firms for communication purposes experienced a cyber incident,[10] exclusively affecting business communications across oil and gas and electric utility sectors. It forced a number of energy companies to shut down communication connections and hampered data processing. Further underscoring potential for third-party infections, the Department of Justice in December indicted[11] alleged members of the APT 10 hacking group in part for accessing companies' Managed Service Providers (MSPs) to gain access into primary victim networks to steal sensitive information. Additionally, in August Schneider Electric alerted customers that some USB media shipped with two Conext products may have been infected with unidentified malware during manufacturing by a supplier.[12] No customers publicly reported incidents of infection in this case.

[9] https://dragos.com/blog/20180522SupplyChainThreats.html

[10] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay

[11] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[12] https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SESN-2018-236-01+Conext+USB+Malware.pdf&p_Doc_Ref=SESN-2018-236-01

Significant TTPs

ICS-directed threat behavior continues to transition away from unique malware and vulnerabilities for most operations, which is concerning because many OT security practices rely on anti-virus and vulnerability-based protection schemes to reduce risk. Thus, their fundamental behavior becomes a key detection element for defense.

During earlier phases of operation threats increasingly use a methodology known as Living off the Land, leveraging native system commands, applications, and software to gain access to the system and move throughout the network undetected. Most ICS-impacting incidents still begin in an enterprise IT network although with the interconnection of industrial environments to vendors, integrators, and others, it is important to note that the enterprise IT network the compromise begins in may not belong to the organization that owns and operates the ICS. Living off the Land can allow an adversary to execute behaviors ranging from conducting research to executing an attack on a target while evading many signature- and blacklist-based detection methods. Living off the Land techniques encompass abuse of native functionality and features in the ICS, such as operations of HMIs, and should not simply be considered the same Living off the Land techniques common in enterprise IT security.

Five out of eight of the activity groups Dragos tracks use some Living off the Land techniques to accomplish early-phase operations. While detecting commodity malware and Living off the Land techniques seems straightforward, it often fails by traditional IT security approaches because of the complex nature and mission requirements of operations environments. As anti-virus products, detection software, and other threat detection methods become more robust and capable of detecting various malicious activity, adversaries must modify their methods to evade capture by blending in with the environment and not leaving behind identifiable artifacts.

Dragos has also identified a growing trend of adversaries using open source or commercially-available penetration testing tools in real-world campaigns. Mimikatz is the most popular and effective tool that lets adversaries capture Windows credentials from system memory. Multiple activity groups, including ELECTRUM, ALLANITE, and DYMALLOY, use Mimikatz, and major wormable malware including NotPetya and Olympic Destroyer with built-in Mimikatz-like functionality for credential capture to propagate through infected networks. This tool can be leveraged for a pivot point within the network and used for traversing the IT and ICS boundary. Other tools include penetration testing frameworks Metasploit and PowerShell Empire, both of which contain versions of Mimikatz.

Later operational phases against ICS networks see the usage of ICS-specific knowledge, technology, processes, and capabilities. Threats continue to require months-to-many years of dedicated ICS research and reconnaissance to achieve any specific intent – hence our concern of the growing number of ICS intrusions which are the precursor to any disruptive action. Later operational phases leverage ICS-specific technologies and protocols to interact with and ultimately disrupt an industrial process. This means that a comprehensive ICS cybersecurity strategy must incorporate ICS-specific defenses and IT cybersecurity mechanisms.

Other tools include penetration testing frameworks Metasploit and PowerShell Empire, both of which contain versions of Mimikatz.

ACTIVITY GROUPS

Dragos categorizes behavior by activity group,[13] creating analytics that provide comprehensive data around actions, capabilities, and intentions. We currently publicly label eight ICS-focused activity groups and track more unlabeled activity of interest. The following summaries include newly-identified activity groups as well as recent activity that Dragos links with high confidence to tracked activity groups.

XENOTIME

ALLANITE

ELECTRUM

RASPITE

CHRYSENE

DYMALLOY

COVELLITE

MAGNALLIUM

[13] http://www.diamondmodel.org

CAPABILITIES
TRISIS, custom credential harvesting

VICTIMOLOGY
Oil & Gas, Middle East

XENOTIME

XENOTIME is the group behind TRISIS, the destructive, ICS-tailored malware targeting Triconex safety instrumented systems (SIS) in the Middle East. In 2018 Dragos identified new XENOTIME activity targeting entities in the US, and devices beyond Triconex. While TRISIS would be difficult to replicate to other SIS's, the malware provided a roadmap for other adversaries to target these types of devices. In addition to customizing the malware specifically for the target environment, the group uses stolen credentials to move between networks, legitimate but compromised servers for communication, and some Living off the Land techniques.

Dragos identified TRISIS targeting an oil and gas facility in Saudi Arabia in the fall of 2017. It represented an escalation of ICS attacks due to its targeting of safety systems that could lead to potential loss of life and physical damage.

XENOTIME has operated since at least 2014 and it is not currently linked to any other known groups. Dragos assesses this is one of the most adept and notable ICS-targeting activity groups.

CAPABILITIES
Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSExec

VICTIMOLOGY
Electric utilities, US & UK

ALLANITE

In 2018, Dragos identified victims and attack methodology that sufficiently differentiated ALLANITE from other activity groups. This group targets business and ICS networks in the US and UK electric utility sectors and maintains access to understand the operational environment and for potential disruptive events.

ALLANITE uses phishing and compromised websites, called watering holes, for credential theft. Dragos assesses the group's operations are limited to information gathering and have not yet demonstrated disruptive capabilities. ALLANITE avoids custom malware, instead utilizing Living off the Land techniques.

ALLANITE activity includes the Palmetto Fusion[14] event described by the US Department of Homeland Security (DHS). In October 2017, a DHS advisory[15] documented ALLANITE technical operations combined with activity with a group Symantec calls Dragonfly 2.0 (the latter has links to the activity group Dragos tracks as DYMALLOY).

[14] https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?noredirect=on&utm_term=.89566d6d9d26

[15] https://www.us-cert.gov/ncas/alerts/TA17-293A

CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan, Europe

RASPITE

In August 2018, Dragos identified a new group targeting access operations in the US electric utility sector, with additional victims in Saudi Arabia, Japan, and potentially Europe. The group appears active since at least mid-2017.

RASPITE compromises websites its targets are likely to visit in an attempt to gain initial access to victim networks. Similar to ALLANITE and DYMALLOY, RASPITE will embed a link to a resource to prompt an SMB connection and steal Windows credentials. The group then deploys install scripts for a malicious service to beacon back to RASPITE-controlled infrastructure, allowing the adversary to remotely access the victim machine. The group shares similarities with a group known as Leafminer by Symantec.

Despite demonstrating the steps necessary for initial intrusion into an IT network and potentially preparing a path for an ICS event at a later time, there is no indication the group currently has a destructive capability that could, for instance, cause energy sector disruptions.

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

DYMALLOY

In fall 2018, Dragos identified multiple new malware infections matching DYMALLOY's behavior. These observations may indicate a potential resurgence of DYMALLOY activity, or a different entity leveraging similar toolsets. This discovery is concerning; the malware Dragos recently identified as part of new activity is only associated with known intrusions into ICS networks.

The DYMALLOY activity group, associated with "Dragonfly 2.0," uses methods such as spearphishing and watering hole attacks for initial access, and commodity backdoors Goodor, DorShel, and Karagany for post-exploitation activity. The group first emerged in late 2015, and was able to successfully compromise multiple ICS targets in Turkey, Europe, and North America, including obtaining access to human machine interface (HMI) devices and stealing screenshots.

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia

MAGNALLIUM

In 2018, MAGNALLIUM's victimology expanded to additional targets, including entities in Europe and North America. MAGNALLIUM used phishing emails purporting to be job advertisements relating to oil and gas companies to gain access to victims' machines. The group used publicly-available phishing kits to construct the emails' contents, and leveraged variants of the StoneDrill wiper and TURNEDUP malware family in infection events before transitioning to PowerShell based post-exploitation tools in 2018.

Although the expansion is concerning, MAGNALLIUM's capabilities appear to still lack an ICS-specific capability, and remain focused on initial IT compromise and information gathering.

Dragos identified MAGNALLIUM in 2017 and determined that the group targeted IT operations at petrochemical and aerospace manufacturers since at least 2013. The group initially targeted Saudi Arabian energy firms and an aircraft holding company, but new intelligence suggests the group is expanding their targeting.

ELECTRUM

In summer 2018, Dragos identified multiple samples of a malicious tool previously associated with ELECTRUM's 2016 CRASHOVERRIDE event in Ukraine. Although some samples of this tool had been previously identified "in the wild," this tool is only associated with ELECTRUM activity. Dragos also identified new intelligence providing additional information into ELECTRUM infiltration techniques and the capabilities of the CRASHOVERRIDE malware.

The group does not rely on zero-day vulnerabilities, instead leveraging common exploitation behaviors and tools, including Mimikatz. Our intelligence indicates that the group remains active and is no longer focusing exclusively on Ukraine.

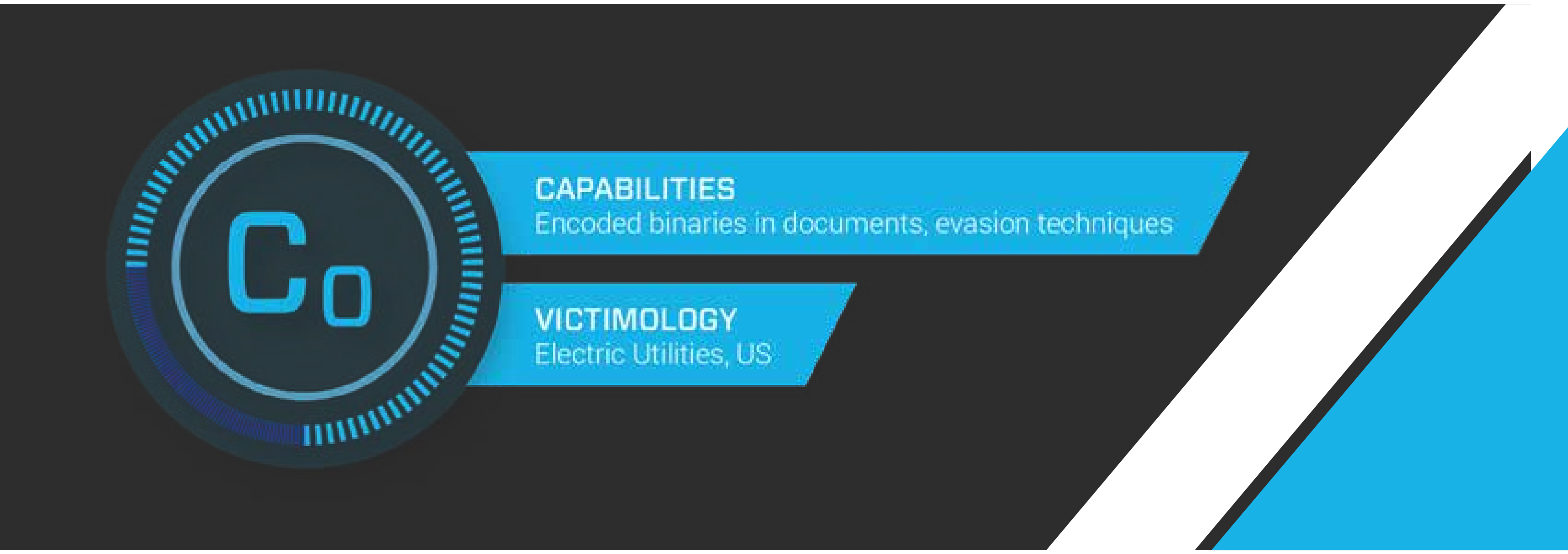
CAPABILITIES
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR

VICTIMOLOGY
Oil & Gas, Manufacturing, Europe, MENA, N. America

CHRYSENE

Dragos uncovered multiple samples of CHRYSENE-related malware and other activity this year, indicating the group remains active and is evolving in more than one area, including revising and updating its malicious software toolkit. CHRYSENE aims to evade existing anti-virus and other detection mechanisms.

CHRYSENE developed from an espionage campaign which first appeared on the public's radar after the destructive SHAMOON cyberattack in 2012 impacting Saudi Aramco. The activity group targets petrochemical, oil, gas, and electric generation sectors and has shifted targeting outside the Gulf Region.



COVELLITE

COVELLITE compromised networks associated with electric energy, primarily in Europe, East Asia, and North America. The group lacks an ICS-specific capability at this time. Dragos identified COVELLITE activity targeting US electric utilities in 2017.

While technical activity linked to COVELLITE behaviors exist in the wild, there has been no evidence or indications this group remains active from an ICS-targeting perspective, nor has Dragos identified new activity against electric infrastructure specifically.

RECOMMENDATIONS

Organizations can lower their risk profiles and proactively protect against common attack techniques by performing security best practices. Implement proper security hygiene and the principle of least privilege based on a deep knowledge of the environment. For instance: question whether tools like PSExec are necessary for every user; use access control lists and restrict administration rights across all devices; prohibit OT devices, including engineering workstations, from connecting to the internet or email services wherever possible; and ensure employees are trained to identify and report phishing and malicious activity. Additionally, increase visibility into host and ICS processes as a means to identify suspicious behavior within otherwise legitimate processes, such as PowerShell execution resulting in network connectivity.

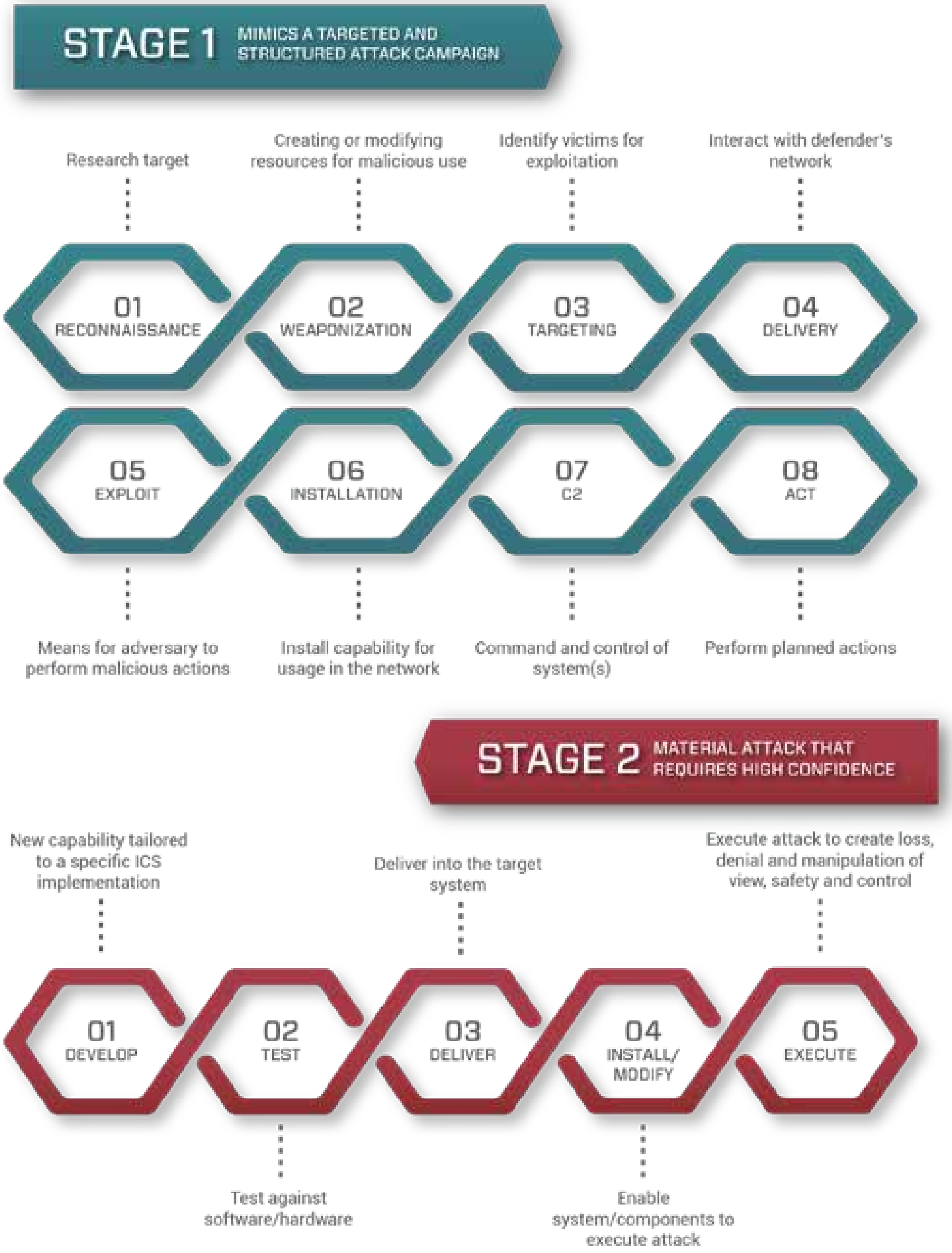
DEFENDING THE ENTIRE KILL CHAIN

LEVERAGE THREAT BEHAVIOR ANALYTICS

UNDERSTAND AND ANTICIPATE THREATS

DEFENDING THE ENTIRE KILL CHAIN

Defending against a dynamic threat landscape requires adopting a "Whole of Kill Chain"[16] approach, keying in on adversary behaviors from the initial intrusions through second-stage impacts. Defenders can use a mix of modern threat detection strategies including indicator- or behavior-based methods, or approaches relying on modeling and configuration.[17] Diversifying threat detection strategies can help asset owners and operators identify threats earlier, and achieve greater visibility into potential threats.


STAGE 1
MIMICS A TARGETED AND STRUCTURED ATTACK CAMPAIGN
Research target
Creating or modifying resources for malicious use
Identify victims for exploitation
Interact with defender's network
01 RECONNAISSANCE
02 WEAPONIZATION
03 TARGETING
04 DELIVERY
05 EXPLOIT
06 INSTALLATION
07 C2
08 ACT
Means for adversary to perform malicious actions
Install capability for usage in the network
Command and control of system(s)
Perform planned actions
STAGE 2
MATERIAL ATTACK THAT REQUIRES HIGH CONFIDENCE
New capability tailored to a specific ICS implementation
Deliver into the target system
Execute attack to create loss, denial and manipulation of view, safety and control
01 DEVELOP
02 TEST
03 DELIVER
04 INSTALL/ MODIFY
05 EXECUTE
Test against software/hardware
Enable system/components to execute attack

[16] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
[17] https://dragos.com/blog/FourTypesOfThreatDetection.html

LEVERAGE THREAT BEHAVIOR ANALYTICS

As adversaries increasingly adopt Living off the Land and ICS-specific techniques, leveraging Threat Behavior Analytics (TBA) – or identifying patterns in behavior and malicious activity alongside static operations – can help improve identification of malicious activity within the environment. Dragos develops TBAs[18] to help define activity groups, providing analytic identifiers that allow defenders to detect malicious behavior holistically, regardless of whether the individual indicators of compromise (IOCs) relating to the analytic change in different attacks.

UNDERSTAND AND ANTICIPATE THREATS

ICS threat intelligence can give asset owners and operators actionable information to anticipate and defend against threats by providing visibility into the current landscape, trends, and targeting. Threat intelligence combines information from various sources and expert assessments to form conclusions that decision-makers can use to implement vertical-specific controls that result in effective security postures.

[18] https://dragos.com/blog/20180226ThreatAnalyticsAndActivityGroups.html

COMBATING FUD

FEAR

UNCERTAINTY

DOUBT

COMBATING FEAR, UNCERTAINTY, AND DOUBT

Dragos frequently receives feedback that ICS security practitioners take weeks or months to address FUD, or fear, uncertainty, and doubt, caused by misreported or misunderstood incidents. Addressing FUD keeps them from actually defending networks, thereby making ICS security worse by a significant margin.

For instance, in July, the media reported[19] the Department of Homeland Security (DHS) publicly disclosed Russian hacking activity targeting US electric utilities. But the article contained previously-reported information: activity linked to the DYMALLOY and ALLANITE activity groups. This reporting and the exaggerated statements reported within continued coverage generated concern because it was not clear that the activity and had been known for some time.

As the scope and number of reported threats or cyberattacks against ICS entities expands, it's important to ensure a realistic understanding of what malicious activity organizations in the electric, oil and gas, manufacturing, aerospace, and a variety of other industries face. Industrial infrastructure is defensible, and destructive attacks are difficult to execute and scale. Further, while numerous, incidental malicious activity commonly occurs in industrial networks (like commodity malware or phishing attacks), ICS-specific or ICS-tailored malware remains rare.

[19] https://dragos.com/blog/20180806ElectricGridThreats.html

CONCLUSION

This year Dragos expects to identify more activity targeting ICS, due to greater visibility into OT networks and adversary behavior driven by ICS threat intelligence. Adversaries will continue to bridge IT and OT networks leveraging traditional malware and Living off the Land techniques, while largely avoiding the use of zero-days.

We anticipate growing our list of publicly-tracked adversaries and providing our customers the most in-depth and intelligence-driven ICS threat analysis. Dragos will continue our efforts to bring ICS cybersecurity resources to all levels and encourage collaboration across all sectors to ensure a greater understanding of the threats these industries face and how to combat them.