INDUSTRIAL CONTROL
SYSTEM THREATS

DRAGOS

"Industrial Control System Threats", Dragos, Inc., Hanover, MD, 1 March 2018

TABLE OF CONTENTS

DRAGOS

A YEAR IN THREATS

2017

2017 represents a defining year in ICS security: two major and unique ICS-disruptive attackers were revealed; five distinct activity groups targeting ICS networks were identified; and several large-scale IT infection events with ICS implications occurred. While this represents a significant increase in 'known' ICS activity, Dragos assesses we are only scratching the surface of ICS-focused threats. 2017 may therefore represent a break-through moment, as opposed to a high-water mark – with more activity to be expected in 2018 and beyond.

While our visibility and efforts at hunting are increasing, we recognize that the adversaries continue to grow in number and sophistication. By identifying and focusing on adversary techniques – especially those which will be required in any intrusion event – ICS defenders can achieve an advantageous position with respect to identifying and monitoring future attacks. This report seeks to inform ICS defenders and asset owners on not just known attacks, but to provide an overview for how an adversary must and will operate in this environment moving forward. By adopting a threat-centric defensive approach, defenders can mitigate not just the adversaries currently known, but future malicious actors as well.

Joe Slowik
Adversary Hunter | Dragos, Inc.

INDUSTRIAL CONTROL SYSTEM THREATS

2017 ICS THREAT REVIEW

2017 was a watershed year in industrial control systems (ICS) security largely due to the discovery of new capabilities and a significant increase in ICS threat activity groups. Cybersecurity risks to the safe and reliable operation of industrial control systems have never been greater. While numerous, incidental infections occur in industrial networks on a regular basis, ICS-specific or ICS-tailored malware is rarer.

Prior to 2017 only three families of ICS-specific malware were known: STUXNET, BLACKENERGY 2, and HAVEX. In 2017 the world learned of two new ICS-specific malware samples: TRISIS and CRASHOVERRIDE. Both of these samples led to industry firsts. CRASHOVERRIDE was the first malware to ever specifically target and disrupt electric grid operations and led to operational outages in Kiev, Ukraine in 2016 (although it was not definitively discovered until 2017). TRISIS is the first malware to ever specifically target and disrupt safety instrumented systems (SIS), and is the first malware to ever specifically target, or accept as a potential consequence, the loss of human life. The impact of these events cannot be understated.

The number of adversaries targeting control systems and their investment in ICS-specific capabilities is only growing. There are now five current, active groups targeting ICS systems – far more than our current biases with respect to the skill, dedication, and resources required for ICS operations would have us believe possible. These events and continued activity will only drive a hidden arms race for other state and non-state actors to mature equivalent weapons to affect industrial infrastructure and ensure parity against possible adversaries.

We regrettably expect ICS operational losses and likely safety events to continue into 2018 and the foreseeable future.

2017 ICS THREATS

A SUMMARY

2017 featured multiple, concerning developments within the ICS security space. On a general level, wormable ransomware such as WannaCry and NotPetya provided notice to ICS owners and operators that industrial networks are far more connected to the IT environment than many realized. While significant and – for some organizations – costly, 2017 also featured some targeted events led by activity groups focused exclusively on the ICS environment.

Previously, defenders perceived ICS threat actors as rare with significant technical limitations or hurdles to overcome. But 2017 demonstrated – either because ICS is an increasingly enticing target, or because researchers and defenders are merely 'looking harder' – that these groups are more common than previously thought. Toward that end, Dragos identified five active, ICS-focused groups that displayed various levels of activity throughout 2017. While only one has demonstrated an apparent capability to impact ICS networks through ICS-specific malware directly, all have engaged in at least reconnaissance and intelligence gathering surrounding the ICS environment.

Overall, the scope and extent of malicious activity either directly targeting or gathering information on ICS networks increased significantly throughout 2017.

As a result of these events, Dragos has been able to analyze and develop strategies for defending and mitigating various types of attack against ICS assets.

NEW ICS-FOCUSED MALWARE

2017 witnessed a dramatic expansion in ICS security activity and awareness. During the year, Dragos identified and analyzed CRASHOVERRIDE, responsible for the Ukraine power outage event that occurred in December of 2016, and then discovered and analyzed TRISIS, the first ICS malware designed to target industrial safety systems in October. Considering that defenders knew of only three ICS-focused malware samples before 2017 – STUXNET (pre-2010), BLACKENERGY2 (2012), and HAVEX (2013), the emergence and discovery of two more this year indicates that adversaries are focusing more effort and resources on ICS targeting, and those capabilities are expanding.

TRADITIONAL IT MALWARE CRIPPLING OPERATIONAL NETWORKS

Early 2017 saw the release of the EternalBlue vulnerability (MS17-010) and the subsequent WannaCry ransomware worm. The infection of operational networks with this ransomware and operational disruption illustrated the symbiotic relationship between the two networks. While engineers and operations staff have long held the separation between "business" and "operational" environments as the ICS model, the border is increasingly permeable and therefore operational ICS networks are facing traditional business threats.

Closely following the WannaCry ransomware adversaries launched NotPetya. What was unique is that this was a wiper masquerading as ransomware appearing to initially target Ukraine business and financial sectors. In addition to weaponizing the EternalBlue exploit, NotPetya leveraged credential capture and replay to provide multiple means of propagation, resulting in rapid spreading to organizations well-removed from Ukrainian business sectors. Perhaps the most sobering example is Maersk, which is estimated to have lost up to $300 million USD while also having to rebuild and replace most of its IT and operations network.[1]

To combat malware infection events such as the above examples, Dragos pursues 'commodity', non- ICS-focused malware through the MIMICS project: Malware In Modern ICS Environments. By aggressively hunting for standard IT threats that can pose a specific danger to ICS environments, Dragos works to provide early warning and defensive guidance on potentially overlooked threats.

ADVERSARIES STAYING BUSY: ICS-FOCUSED ACTIVITY

Dragos currently tracks five activity groups targeting ICS environments: either with an ICS-specific capability, such as CRASHOVERRIDE or with an intention to gather information and intelligence on ICS-related networks and organizations. These groups have remained relatively constant regarding overall activity throughout the year, and Dragos is confident that additional unknown events have occurred.

[1] https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815

RECOMMENDATIONS

An ICS intelligence-driven approach to threat intelligence is not universal. Indicators of compromise are not intelligence and will not save any organization. Organizations must understand and consume ICS-specific threat intelligence to monitor for adversary behaviors and tradecraft instead of simply detecting changes, anomalies, or after-the-fact indicators of compromise.[2]

DETECTION-IN-DEPTH

Just as defense-in-depth is a necessary component of modern cybersecurity, so must detection-in-depth monitoring of behaviors across all industrial control levels but also. Enhanced monitoring must especially Include any permeable "barriers" such as the IT-OT network gap. ICS networks are increasingly connected not only to the IT network but also directly to vendor networks and external communication sources leaving monitoring of the IT environments alone entirely inefficient.

ASSUME BREACH

Disruptive ICS-specific malware is real, traditional IT threats now regularly cross the "IT-OT" divide, and ICS knowledgeable activity groups are targeting industrial infrastructure directly instead of just the IT networks of industrial companies. Gone are the days of protection via a segmented network – detection is the first component of an assume- breach model – you can only respond to what you can see.

ICS-SPECIFIC INVESTIGATIONS

In the event of a breach or disruption there must be ICS-specific investigation capabilities and ICS-specific incident response plans. This is the only effective way of identifying root cause analysis and reducing mean time to recovery in the operations environments when facing industrial specific threats.

RESILIENCE AGAINST CYBER ATTACK

Resiliency analysis and engineering surrounding industrial processes must include cyber-attacks. For example, safety systems must be designed and operated with the understanding that they may now be purposefully attacked and undermined.

2 To understand ICS threat intelligence read the Dragos whitepaper "Industrial Control Threat Intelligence" https://dragos.com/media/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

2017

ICS THREATS

IN DETAIL

CRASHOVERRIDE

Although taking place in late December 2016, the ICS security community did not fully understand the extent and significance of the 2016 Ukrainian power outage until later in 2017. After identifying samples, Dragos determined that specifically-tailored malware caused the 2016 event by manipulating the breakers at the target substation in Ukraine.

At the time, this represented only the second instance where malware was utilized to directly impact an ICS device or process with little human intervention – the other example being the Stuxnet worm. In this case, the adversary developed a modular attack framework that combined a reasonably protocol-compliant manipulation program to create an ICS impact (opening breakers to generate a power outage), with malicious wiper functionality to impede and delay system recovery.

Further investigation identified a distinct activity group behind the CRASHOVERRIDE event, as both a developer and attacker: ELECTRUM. As detailed below, ELECTRUM is assessed to be a highly sophisticated, well-resourced activity group that remains active.

Defenders lack any knowledge of CRASHOVERRIDE itself or similar capabilities used after the December 2016 event. While CRASHOVERRIDE, as deployed in the Ukraine attack, is not capable of impacting environments dissimilar to the equipment and protocol setup at the target utility, the framework and method of operations deployed provide an example for other adversaries to follow. Examples of new 'tradecraft' to emerge from CRASHOVERRIDE include: leveraging ICS protocols to create a malicious impact; creating modular malware frameworks designed to work with multiple protocols; and incorporating automatically- deployed wiper functionality chained to an ICS impact.

Thus, even if CRASHOVERRIDE itself cannot be used again outside of very narrow circumstances, the tactics, techniques, and procedures (TTPs) employed by it can be adapted to new environments. By identifying these TTPs and building defenses around them, organizations can prepare themselves for the next CRASHOVERRIDE-like attack, rather than focusing exclusively on the specific events from December 2016 leaving the enterprise open and undefended against even minor variations in the attack.

TRISIS

TRISIS is the third-recorded ICS attack executed via malware, the previous two being Stuxnet and CRASHOVERRIDE (see above). TRISIS is a specifically-targeted program designed to upload new ladder logic to Schneider Electric Triconex safety systems. The malware utilizes a specially-crafted search and upload routine to enable overwriting ladder logic within memory based on a deep understanding of the Triconex product.

Unique compared to past ICS events, TRISIS targeted safety instrumented systems (SIS), those devices used to ensure system remain in and fail to a 'safe' state within the physical environment. By targeting SIS, an adversary can achieve multiple, potentially dangerous impacts, ranging from extensive physical system downtime to false safety alarms, physical damage, and destruction. Additionally, by targeting a SIS the adversary must either intend or willfully accept the loss of human life from the operation.

Although extremely concerning both as an attack and as an extension of ICS operations to cover SIS devices, TRISIS represents a highly-targeted threat. Specifically, TRISIS is designed to target a specific variant of Triconex systems. Additionally, an adversary would need to achieve extensive access to and penetration of a target ICS network to be in a position to deliver a TRISIS-like attack.

While TRISIS is profoundly concerning and represents a significant new risk for defenders to manage, TRISIS-like attacks require substantial investments in both capability development and network access before adversary success.

While ICS defenders and asset owners should note the above regarding TRISIS' immediate impact, in the longer-term TRISIS is likely to have a concerning effect on the ICS security space. Specifically, while TRISIS itself is not portable to any environment outside of the specific product targeted in the attack, the TRISIS tradecraft has created a 'blueprint' for adversaries to follow concerning SIS attacks. This is not bound to any specific vendor and vendors such as ABB maturely and rightfully stated that similar styled attacks could equally impact their products. Furthermore, the very extension of ICS network attack to SIS devices sets a worrying precedent as these critical systems now become an item for adversary targeting.

DISRUPTIVE IT MALWARE

IT malware infecting and causing issues in operational networks is not a new phenomenon. Tracking the metrics related to these infections has always been difficult due to collection issues from these environments. This led to very low metrics, such as the ICS- CERT's consistent ~200 incidents each year, to very high metrics including some vendors claiming upwards of 500,000 infections a year. For this reason, Dragos created the Malware in Modern ICS (MIMICS) project in late 2016 and running through early 2017.[3] The research performed a census-styled metrics count of infections in ICS networks and identified around 3,000 unique industrial infections during the research period. This led to the estimate of around 6,000 unique infections in industrial environments every year including various types of viruses, trojans, and worms. While any of these infections could cause issues in operational environments none represented the type of disruption that would come from the latest generation of ransomware worms.

WannaCry appeared in May 2017 following the weaponization of the MS17-010 vulnerability in the Microsoft Server Message Block (SMB) protocol (EterenalBlue[4]), released as part of the 'Shadow Brokers' continual leak of alleged National Security Agency hacking tools. WannaCry itself was a form of ransomware designed to self-propagate via the MS17-010 vulnerability, resulting in not only a quick spread globally but also the systematic infection of networks due to the malware's 'wormable' nature.

3 To understand ICS threat intelligence read the Dragos whitepaper "Industrial Control Threat Intelligence" https://dragos.com/media/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

4 https://docs.microsoft.com/en-us/security- updates/securitybulletins/2017/ms17-010

While ransomware is typically not a concern for ICS defenders, WannaCry challenged the traditional view due to its self-propagating method exploiting a common ICS communication mechanism (SMB).

Various data transfer functions, such as moving data from the ICS network (e.g., historians) to the business network for business intelligence purposes, rely upon SMB for functionality. Combined with poor patch management and enabling older, vulnerable forms of SMB instead of the newer SMB version 3 variant, hosts within the ICS network were not only reachable through pre-existing connections to the IT network but vulnerable as well.

The result of the above circumstances was WannaCry spreading into and impacting ICS environments, including automotive manufacturers and shipping companies. The impact to operations from system loss due to encryption certainly varies, but in ICS environments the damage potential is significant regarding lost production and capability.

Furthermore, WannaCry was not the only ransomware type to implement worm-like functionality, with additional malware NotPetya and BadRabbit emerging over the course of 2017. Of these, NotPetya was especially concerning for several reasons: first, it included multiple means of propagation through credential capture and re-use aside from relying solely on the MS17- 010 vulnerability; second, the malware was effectively a 'wiper' as encrypted filesystems could not be recovered. Although initially targeting Ukrainian enterprises, NotPetya soon spread to many organizations resulting in significant system impacts and, in several documented cases, production losses in ICS environments.

Although not targeted at ICS environments, the impact of WannaCry and related malware demonstrates the capability for IT-focused malware to migrate into ICS environments. While patching may not be a viable solution for ICS defenders in cases such as MS17-010, strengthening and hardening defenses at porous boundaries could help.

ACTIVITY GROUPS

Dragos tracks and organizes related threat activity as 'activity groups': essentially, combinations of behavior or techniques, infrastructure, and victimology.[5] This process avoids the potentially messy and hard-to- prove traditional attribution route – aligning activity to specific actors or nation-states – while also providing concrete benefits to defenders by organizing observed attackers into collections of identified actions.

Within the scope of ICS network defense, Dragos currently tracks five activity groups that have either demonstrated the capability to attack ICS networks directly or have displayed an interest in reconnaissance and gaining initial access into ICS-specific entities.

5 The concept of activity groups comes from The Diamond Model of Intrusion Analysis: http://www.diamondmodel.org/

ELECTRUM

ELECTRUM is responsible for the 2016 Ukrainian power outage event, created through CRASHOVERRIDE. In addition to this signature, high-profile event, Dragos has linked ELECTRUM with another group, the SANDWORM Advanced Persistent Threat (APT) (iSight), responsible for the 2015 Ukrainian outage. ELECTRUM previously served as the 'development group' facilitating some SANDWORM activity – including possibly the 2015 Ukrainian power outage – but moved into a development and operational role in the CRASHOVERRIDE event.

While ELECTRUM does not have any other high-profile events to its name as of this writing, Dragos has continued to track on- going, low-level activity associated with the group. Most notably, 2017 did not witness another Ukrainian power grid event, unlike the previous two years. Based on available information, ELECTRUM remains active, but evidence indicates the group may have 'moved on' from its previous focus exclusively on Ukraine.

While past ELECTRUM activity has focused exclusively on Ukraine, information from low- level ongoing events and the group's link to SANDWORM Dragos assesses that ELECTRUM could be 're-tasked' to other areas depending on the focus of their sponsor.

Given ELECTRUM's past activity and ability to successfully operate within the ICS environment, Dragos considers them to be one of the most significant and capable threat actors within the ICS space.

COVELLITE

COVELLITE First emerged in September 2017, when Dragos identified a small, but highly targeted, phishing campaign against a US electric grid company. The phishing document and subsequent malware – embedded within a malicious Microsoft Word document – both featured numerous techniques to evade analysis and detection. Although the attack identified is particular to the one targeted entity, Dragos soon uncovered attacks with varying degrees of similarity spanning Europe, North America, and East Asia.

Common to all of these observed COVELLITE-related instances was the use of similar malware functionality, including the use of HTTPS for command and control (C2), and the use of compromised infrastructure as C2 nodes.

As Dragos continued tracking this group, we identified similarities in both infrastructure and malware with the LAZARUS GROUP APT[6] (Novetta), also referred to as ZINC (Microsoft), and HIDDEN COBRA (DHS). This activity group has variously been associated with destructive attacks against Sony Pictures[7] and to bitcoin theft incidents in 2017.[8] While Dragos does not comment on or perform traditional nation-state attribution, the combination of technical ability plus the willingness to launch destructive attacks displayed by the linked group LAZARUS make COVELLITE an actor of significant interest.

Dragos has yet to identify another grid- specific targeting event since September 2017 although similar malware and related activity continue. Finally, noted capabilities thus far would only suffice for initial network access and reconnaissance of a target network – COVELLITE has not used or shown evidence of an ICS-specific capability.

6 https://www.novetta.com/tag/the-lazarus-group/
7 http://www.novetta.com/2016/02/operation-blockbuster-unraveling-the-long-thread-of-the-sony-attack/
8 https://www.recordedfuture.com/north- korea-cryptocurrency-campaign/

DYMALLOY

Dragos began tracking the activity group we refer to as DYMALLOY in response to Symantec's 'Dragonfly 2.0' report. Importantly, Dragos found a significant reason to doubt an association to the legacy Dragonfly ICS actor with the newly-identified activity.

Dragonfly was originally active from 2011 to 2014 and utilized a combination of phishing, strategic website compromise, and creating malicious variants of legitimate software to infiltrate ICS targets. Once access was gained, Dragonfly's HAVEX[9] malware leveraged OPC communications to perform survey and reconnaissance activities within the affected networks.

Although no known destructive attacks emerged from these events, Dragonfly proved itself to be a capable, knowledgeable entity able to penetrate and operate within ICS networks.

DYMALLOY is only superficially similar to Dragonfly, in that the group utilized phishing and strategic website compromises for initial access. However, even at this stage, DYMALLOY employed credential harvesting techniques by triggering a remote authentication attempt to attacker-controlled infrastructure, significantly different from the exploits deployed by Dragonfly. All subsequent activity shows dramatic changes in TTPs between the groups, such as differences between the content and targeting of the phishing messages, and the outbound SMB connections.

[9] The Impact of Dragonfly Malware on Industrial Control Systems – SANS Institute Whitepaper

Although DYMALLOY does not appear to be linked with Dragonfly, or at least not directly, the group remains a threat to ICS owners.

Starting in late 2015 and proceeding through early 2017, DYMALLOY was able to successfully compromise multiple ICS targets in Turkey, Europe, and North America. Dragos has also learned that, while the group does not appear to have a capability equivalent to Dragonfly's HAVEX malware, the group was able to penetrate the ICS network of several organizations, gain access to HMI devices, and exfiltrate screenshots. While less technically sophisticated than HAVEX, such activity shows clear ICS intent and knowledge of what information could be valuable to an attacker – either to steal information on process functionality in the target environment or to gather information for subsequent operations.

Since Symantec's public reporting, followed by additional US-CERT notifications several weeks later, Dragos has not identified any additional DYMALLOY activity. While analysts found some traces of DYMALLOY-related malware in mid-2017, no artifacts or evidence suggesting DYMALLOY operations appear since early 2017. Given the publicity, Dragos assesses with medium confidence that DYMALLOY has reduced operations or significantly modified them in response to security researcher and media attention.

CHRYSENE

CHRYSENE is an evolution of on-going activity which initially focused on targets in the Persian or Arabian Gulf. CHRYSENE emerged as an off-shoot to espionage operations – as well as potential preparation actions before destructive attacks such as SHAMOON[10] – that focused mostly on the Gulf area generally, and Saudi Arabia specifically. CHRYSENE differs from past activity in that it utilizes a unique variation of a malware framework employed by other groups such as Greenbug (Symantec) and OilRig (Palo Alto Networks), with a very particular C2 technique reliant upon IPv6 DNS and the use of 64-bit malware.

Where CHRYSENE mostly differentiates itself is in targeting: all observed CHRYSENE activity focuses on Western Europe, North America, Iraq, and Israel. CHRYSENE targets oil and gas and electric generation industries primarily within these regions. This activity first emerged in mid-2017 and had continued at a steady state since.

While CHRYSENE's malware features notable enhancements over related threat groups using similar tools, Dragos has not yet observed an ICS-specific capability employed by this activity group. Instead, all activity thus far appears to focus on IT penetration and espionage, with all targets being ICS-related organizations. Although CHRYSENE conducts no known ICS disruption, the continued activity and expansion in targeting make this group a concern that Dragos continues to track.

[10] http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

MAGNALLIUM

DRAGOS began tracking MAGNALLIUM in response to public reporting by another security company on a group identified as 'APT33' (FireEye). The press initially treated MAGNALLIUM as a significant threat to ICS and critical infrastructure. A subsequent investigation by Dragos indicated that all of this group's activity focused on Saudi Arabia, specifically government-run or -owned enterprises in petrochemicals and the aerospace industry.

While the group targets organizations which contain ICS, the lack of an ICS-specific capability combined with the group's very narrow targeting profile make this less of a concern.

We continue to monitor MAGNALLIUM to determine if targeting changes, or if this group's actions splinter resulting in new, 'out of area' operations, as observed with CHRYSENE.

DRAGOS

DRAGOS, INC.

www.dragos.com
1745 DORSEY ROAD
HANOVER, MD 21076 USA
EMAIL: INFO@DRAGOS.COM