DRAGOS

ASSESSING RANSOMWARE AND EXTORTION ACTIVITIES IMPACTING INDUSTRIAL ORGANIZATIONS

RANSOMWARE IN ICS ENVIRONMENTS

AUTHORS

SELENA LARSON, DRAGOS
CAMILLE SINGLETON, IBM SECURITY X-FORCE

December 2020

DRAGOS, INC.
Intel@Dragos.com
@DragosInc

Table of Contents

EXECUTIVE SUMMARY

RANSOMWARE REMAINS AN ONGOING THREAT TO INDUSTRIAL AND CRITICAL INFRASTRUCTURE ENTITIES GLOBALLY

Although many ransomware strains impacting industrial control systems (ICS) and related entities are IT-focused, such ransomware can have disruptive impacts on operations. Ransomware can directly impact the operational technology (OT) environment if it is able to bridge the gap between enterprise and operations due to improper security hygiene. Ransomware can also have indirect access on operations by impacting resources such as logistics, fleet management, sales operations and fulfillment, or loss of view to enterprise resource management tools. Additionally, in 2019 and through 2020, ransomware strains began incorporating ICS-focused mechanisms, such as containing code that can stop industrial processes, which can have potentially disruptive effects. Attackers are becoming increasingly hostile in terms of attack behavior, including stealing data before deploying ransomware and threatening companies with its release if ransomware is not paid.

Dragos monitors cyber events impacting ICS entities. IBM Security X-Force provides incident response and intelligence services to organizations across a range of verticals, including those with ICS and OT networks as part of their infrastructure. Dragos and X-Force have observed a real appreciable rise in the number of both nonpublic and public ransomware events affecting ICS environments and operations. Through joint collaboration, intelligence analysts mapped publicly known and internal client incidents of ransomware attacks on industrial entities from 2018 through October 2020. The goal of this research is to identify trends, impacts, and consequences of ransomware on ICS.

Dragos and IBM assessed 194 confirmed ransomware attacks against ICS and supporting entities. Researchers found ransomware against ICS entities and supporting organizations increased 75% in this time-frame, with activity peaking in May 2020. Of the attacks in which the scope of impact is known, 56% of ransomware attacks affected operations functionality at victim organizations, including in some cases weeks-long downtime. Manufacturing was the most targeted industry, followed by utility companies.

The information shared in this report is based on publicly available information as well as data from incidents identified and responded to by X-Force and Dragos' Services team. It is worth noting that entities who experience disruptive ransomware events frequently do not report them unless compelled by regulators. Thus, publicly reported details of ransomware attacks on ICS and related entities neglect to provide a full picture of the threat landscape.

KEY FINDINGS

- Ransomware attacks on industrial entities increased more than 500% from 2018 to 2020.
- Manufacturing entities comprise over one-third of confirmed ransomware attacks on industrial organizations, followed by utilities, which make up 10%.
- Newer ransomware strains have the ability to stop industrial processes.
- Ransomware operators are increasingly incorporating data theft and extortion operations into their attack techniques, potentially posing even greater impact from ransomware than disrupted operations through leaked intellectual property and other critical data.
- Data stolen and leaked on publicly available websites could provide ICS-targeting attackers with victim data that could inform or guide future ICS-disruptive attacks.
- Asset owners and operators should engage in effective defense-in-depth security strategies. Ensure an understanding of network interdependencies and conduct crown jewel analysis to identify potential weaknesses that could disrupt business continuity and production.

Ransomware Against ICS: Definition, History, Implications

Malicious software that encrypts files and disrupts computer operations for monetary extortion, known as ransomware, has existed for decades. It is a large and increasing threat to ICS operations as ransomware attackers recognize the value of targeting organizations that have little tolerance for downtime—including many manufacturing and energy companies—and capitalize on that low tolerance in an effort to more consistently extract ransom payments from victims.

The WannaCry and NotPetya worms in 2017 crystallized the threat that ransomware and disruptive IT malware posed to enterprise – and in many cases industrial – operations. These state-sponsored cyberattacks disrupted global operations—from automotive production lines to shipping and logistics to semiconductor manufacturing. With automated functionality leveraging vulnerabilities in Windows computers, these worms spread quickly and haphazardly across the globe.

Historically, cybercrime operators largely targeted victims with ransomware indiscriminately and actors aimed to get money from individual victims who would pay to get their sensitive data – such as financial or personal information – unlocked. In 2018, criminal operators began shifting to what is known as "big game hunting." Human operators specifically targeted a smaller pool of corporate and government victims with ransomware in an effort to receive a higher payoff. The assumption was organizations and corporations would be willing to pay larger ransoms to prevent extensive downtime and loss of productivity or revenue. An October 2019 Federal Bureau of Investigation alert described the issue thus: Since early

2018, the incidents of "broad, [indiscriminate] ransomware campaigns [have] sharply declined, but the losses from ransomware attacks have increased significantly."[1]

Ransomware can be particularly disruptive to industrial operations that rely on computerized systems for things like production, automation, quality assurance, monitoring, and safety. Compromising the availability or visibility of such industrial processes causes significant downtime and can cost companies hundreds of millions of dollars. Commodity ransomware is generally designed to target Windows machines due to the proliferation of such devices throughout enterprises. And often the technology within operations networks – such as human machine interfaces (HMIs) or engineering workstations – run on Windows software and can be disrupted if attackers are able to access it.

Concerningly, some ransomware types such as EKANS have begun to adopt the ability to disrupt industrial equipment.[2] Written within the code are mechanisms that can force stop processes on certain HMIs, data historian, and licensing servers, and the list of targeted devices grows as new strains are found.

Dragos and IBM identified ransomware attacks impacting industrial and related entities from 2018 through October 2020.

1 FBI warns of major ransomware attacks as criminals go "big-game hunting" – Ars Technica (https://arstechnica.com/information-technology/2019/10/fbi-warns-of-major-ransomware-attacks-as-criminals-go-big-game-hunting/)
2 EKANS Ransomware and ICS Operations – Dragos (https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/)

RANSOMWARE IMPACTING INDUSTRIAL AND RELATED ENTITIES

Analysts have observed a real, appreciative rise in ransomware targeting industrial organizations, and many of the incidents have resulted in disruption to industrial operations.

Between January 2018 and October 2020, the number of tracked ransomware incidents impacting industrial companies increased over 500%. In addition, analysis of the frequency of ransomware attacks on industrial organizations per month indicates that attacks have been trending slightly upward over time—with an all-time high in May 2020.

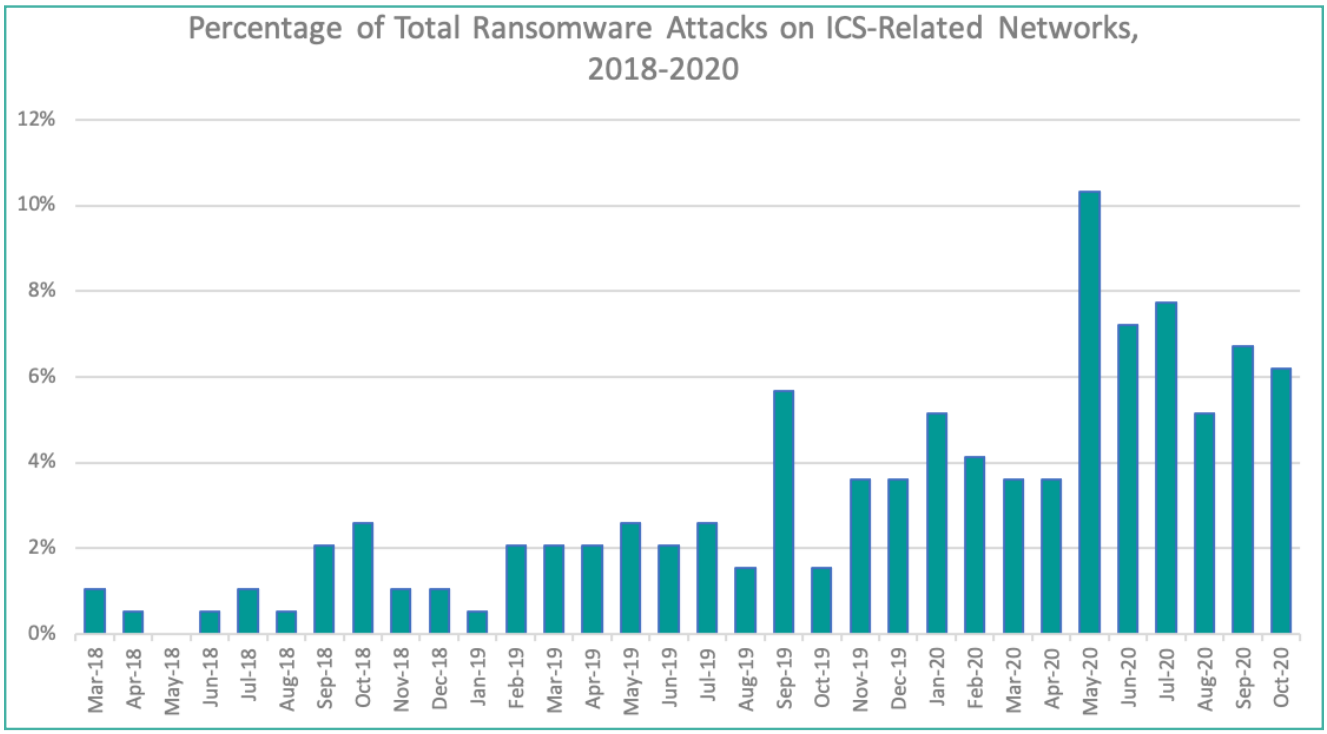

Figure 1: Percent of total ransomware attacks on organizations with or supporting ICS networks, 2018 - 2020

The increase in ransomware events in 2020 appears to coincide with the spread of the coronavirus pandemic globally. Ransomware adversaries leveraged coronavirus-themed phishing lures for initial access operations, preying on users' concern for health and safety.[3] In some cases, ransomware adversaries are targeting cold storage facilities and biomedical, and pharmaceutical manufacturers researching and developing virus vaccines and distribution methods, which could disrupt the development and distribution of the vital drugs.[4]

3 COVID-19 Exploited by Malicious Cyber Actors – CISA (https://us-cert.cisa.gov/ncas/alerts/aa20-099a)
4 German Task Force for COVID-19 Medical Equipment Targeted in Ongoing Phishing Campaign – IBM Security Intelligence (https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/); Cold storage giant Americold hit by cyberattack, services impacted – Bleeping Computer (https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-hit-by-cyberattack-services-impacted/); Dr Reddy's: Covid vaccine-maker suffers cyber-attack – BBC (https://www.bbc.com/news/technology-54642870)

Analyst Note: Dragos and X-Force did not include healthcare facilities and hospitals in this research as they are not in scope of our definition of industrial operations. However, analysts must acknowledge the major disruptions to healthcare and hospitals due to ransomware, and the significant harm caused by these events.[5] The amount and scope of attacks on healthcare entities is concerning and Dragos assesses with high confidence these attacks will continue, especially while the industry remains under stress from the pandemic.

Most ransomware attacks occurred in North America, followed by Europe and Asia. In fact, North America saw nearly half (45%) of ransomware attacks on ICS-connected networks since 2018, followed by Europe at 31% and Asia at 18% of total attacks we have tracked.

The largest increase in targeting was observed in the manufacturing sector, with the number of incidents in that sector tripling from 2018 to 2020. Manufacturing was also the hardest hit, experiencing 36% of all ransomware attacks on ICS-related networks from 2018-2020. Utility companies came in second, at 10% of attacks—a percentage that has increased dramatically since 2018.

Of incidents in which the scope of impact is known, 56% of ransomware attacks affected operations functionality at victim organizations. Sodinokibi, Ryuk and Maze were the most commonly observed ransomware strains compromising industrial organizations from 2018-2020. Specifically, Sodinokibi accounted for 17% of the ransomware attacks against industrial organizations where the ransomware strain was known, while Ryuk made up 14% and Maze 13%. Doppelpaymer and WannaCry tied for fourth, at 7% of ransomware attacks against industrial organizations.

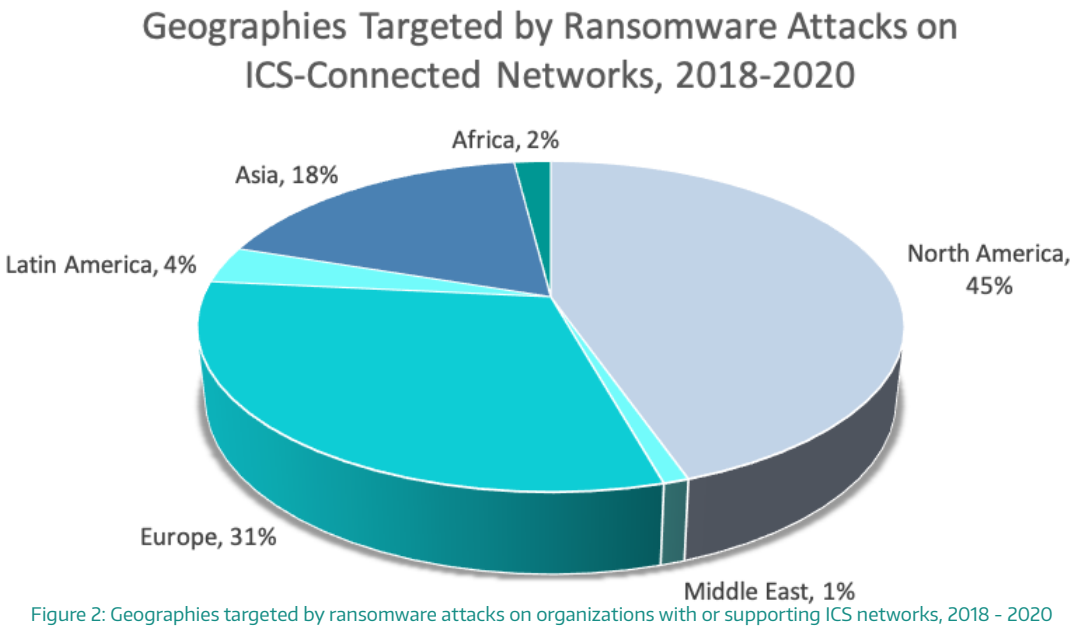

Figure 2: Geographies targeted by ransomware attacks on organizations with or supporting ICS networks, 2018 - 2020

5 Cyberattacks targeting health care must stop – Microsoft (https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/)

Ransomware Types Against Industrial Networks, 2018-2020

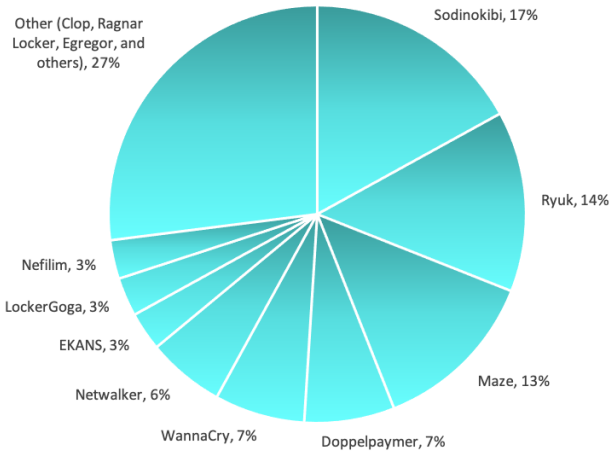

Figure 3: Geographies targeted by ransomware attacks on organizations with or supporting ICS networks, 2018 - 2020

RANSOMWARE DATA

Dragos and X-Force identified 194 confirmed ransomware attacks impacting industrial entities. The dataset includes managed service providers and telecommunications companies as these industries greatly support industrial processes. Their functionality – including mobile and satellite infrastructure and data management and processing – can be deeply integrated into OT environments.

A disruption to such integrations due to a ransomware attack can potentially impact the operations environment. Additionally, the data includes ransomware attacks on government entities only if they impacted utility operations. The dataset only includes organizations which experienced confirmed ransomware attacks. It does not include organizations listed on ransomware leak sites if attempted or successful ransomware deployment and file encryption could not be confirmed.

COMMON ATTACK PATHS

Despite the large number of ransomware types, ransomware strains share many commonalities in initial access, credential theft, lateral movement, and encryption techniques. According to data collected by Dragos and X-Force, the most common initial access vectors are phishing, remote services compromise such as Remote Desktop Protocol (RDP), and exploiting software vulnerabilities like virtual private network (VPN) concentrators and enterprise network equipment.

An April 2020 Microsoft assessment of common human-operated ransomware families found groups using common tools or built-in services for credential theft and lateral movement including Mimikatz, Cobalt Strike, PSExec, and the abuse of Windows service accounts and management tools.[6]

Many human-operated ransomware strains including LockerGoga, Maze, and EKANS encrypt systems in the same effective manner: Windows Active Directory compromise. Active Directory is used for a variety of authentication, security, and administrative services within Windows environments, and a compromise can enable an attacker to quickly encrypt computers across the entire organization's domain.

The good news for organizations is that it is possible to defend against many types of ransomware by practicing proper security hygiene as described in the Recommendations section of this report.

The surge in attacks and attention paid on ransomware has prompted companies to be more proactive in their defense against the threat.

6 Ransomware groups continue to target healthcare, critical services; here's how to reduce risk – Microsoft (https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/)

CASE STUDY

One of the most common types of ransomware attacks against ICS-connected infrastructure is Sodinokibi (also known as REvil)—a malware strain that accounted for more than one in six ransomware attacks against industrial networks from 2018-2020, according to X-Force and Dragos data tracking. Sodinokibi first appeared in April 2019, and nearly 20% of the ransomware actor's claimed victims are in the manufacturing sector—currently the top attacked vector by these threat actors. Transportation, construction, and utilities companies have also been targeted by Sodinokibi ransomware.

Sodinokibi operates as a Ransomware-as-a-Service (RaaS) cartel, where the malware developers contract with other malicious actors who infiltrate and deliver the ransomware to victims—with the malware developers taking a cut of the proceeds after a ransom payment is made. Thus, the tactics, techniques and procedures associated with Sodinokibi ransomware attacks vary significantly, with each contracting threat group using its own set of tactics to compromise a victim.X-Force and Dragos have both remediated Sodinokibi ransomware attacks, and have observed several sets of techniques associated with these actors. In some cases, attackers gain entrance to a network through vulnerabilities in a Citrix server and then deploy CobaltStrike malware and move laterally before deploying the Sodinokibi ransomware. In other instances, attackers have employed phishing techniques with malicious attachments and then downloaded a Carbanak backdoor to pave the way for a ransomware deployment. In one Sodinokibi attack on an ICS organization, attackers initially gained access through a vulnerable Remote Desktop Protocol connection and were able to move laterally into a portion of the network governing operational technology. Once there, the attackers were able to encrypt several sensitive systems in the OT environment—underscoring the threat of ransomware to OT networks.

RANSOMWARE AND EXTORTION

Such activities – like maintaining offline backups, developing incident response plans, and practicing proper security hygiene – can enable quick remediation and response in the event of a ransomware attack. However, this reduces the opportunity for ransomware operators to make money, and many are now incorporating data extortion into their attack behaviors.

With this method, attackers will steal data from a target company before encrypting affected machines and then threaten to publish the data online either on attacker-run websites or hacking forums if a ransom demand is not paid. Multiple ransomware strains leverage the hack and leak technique including Maze, DoppelPaymer, Sodinokobi, Netwalker, and Cl0p.

Ransomware actors may collaborate with other cybercriminal entities either via enlisting hackers via Ransomware-as-a-Service (RaaS) operations like Sodinokibi[7] and Netwalker[8], are collaborating on leaking victim data by creating "extortion cartels," such as the Maze gang with other operators.[9]

Sometimes the ransomware attackers may not achieve encryption but will still hold data for ransom. For instance, in August 2020, Sodinokibi ransomware attackers targeted a U.S.-based spirits and wine company. The firm identified and stopped the attack before systems were encrypted, but attackers still stole sensitive information and leaked some of the data on the Sodinokibi leak site.[10]

Ransomware attackers adopting the hack and leak method is concerning for a variety of reasons, including:

- Victims are unable to confirm whether data is destroyed.
- Data stolen or leaked by attackers could contain sensitive information on the target company and customers that could aid in future attack planning.
- Different regulatory and legal issues arise from data breaches than ransomware.
- Data leaks provide additional incentive for victims to pay a ransom—yet, when paid, ransoms validate cybercriminals' business model and encourages additional attack activity from ransomware cartels.
- Once information is stolen, victims generally have no control over, or visibility into, what attackers do with it.
- Releasing sensitive intellectual property – for instance manufacturing details – could enable counterfeit products being produced. People can copy the manufacturing process more specifically creating better counterfeits.

7 REvil Ransomware-as-a-Service – An analysis of a ransomware affiliate operation – Intel 471 (https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/)
8 Take a "NetWalk" on the Wild Side – McAfee (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/)
9 Ransomware News Roundup: Maze Gang Forms Extortion Cartel – IBM Security Intelligence (https://securityintelligence.com/news/ransomware-news-maze-gang-forms-extortion-cartel/)
10 U.S. spirits and wine giant hit by cyberattack, 1TB of data stolen – Bleeping Computer (https://www.bleepingcomputer.com/news/security/us-spirits-and-wine-giant-hit-by-cyberattack-1tb-of-data-stolen/)

STOLEN DATA PERSISTS LONGER THAN RANSOMWARE'S EFFECTS

Traditionally, ransomware attackers will provide decryption keys to victims once a ransom is paid, which confirms the criminal upholds their end of the transaction. The issue can be addressed within the confines of the impacted network, with the victim maintaining visibility into malicious activities. Data theft and extortion activities introduce additional uncertainty into the calculus, particularly since an organization loses complete control over sensitive data once it is released publicly. In addition, the time-frame for potential damage is not finite as with ransomware, but can extend to months or even years. There is no way for a victim organization to know with certainty what a data theft has done with the victim's sensitive data, or what the attacker may do with it in the future.

ATTACK PLANNING

Multiple ransomware and data leak incidents identified by Dragos and X-Force have included attackers leaking data relating to a victim's customers, including in the manufacturing, utility, defense, and aerospace industries. Although ransomware attackers may only be interested in leveraging such data for financial purposes – i.e. encouraging the company to pay the ransom – attackers interested in specifically targeting ICS could use the leaked data to aid in attack development. Additionally, even if data is not shared publicly, adversaries could potentially buy data from ransomware attackers. Sodinokibi, for instance, created an auction site for interested parties to buy stolen data with no limits on what will be done with it. [11]

An attacker focused on infiltrating or potentially disrupting ICS could use stolen victim and customer data to identify potential opportunities for third-party or supply chain compromise. Customers or employees could be likely targets for phishing activity, or sensitive financial data that could aid in espionage operations. An attacker could also use data like schematics, network diagrams, or other internal documentation to identify targets for operational gain and assess the level of obscurity a target has from internal and external resources.

For example, Dragos reviewed select files from a compromised oil and gas services company published on the Maze ransomware leak website and identified multiple items of interest in the publicly available data leak. This included lists of companies that used the firm's services, employee information, natural gas flow data, information related to a Canadian government energy regulator, and geospatial data which could be related to companies' sites of current upstream and midstream operations.

It is possible to see the value of such data when mapped to frameworks such as IBM's Cyberattack Preparation Framework and MITRE's PRE-ATT&CK tactics. Data leaks can facilitate external reconnaissance—a key component of the "Prepare Attack" phase that aligns with MITRE's PRE-ATT&CK tactics[12] of Target Selection [TA0014]; Technical, People, and Organizational Information Gathering [TA0015, TA0016, TA0017]; or Organizational Weakness Identification [TA0020].

11 Sodinokibi ransomware gang auctions off stolen data – Malwarebytes (https://blog.malwarebytes.com/ransomware/2020/06/sodinokibi-ransomware-gang-auctions-off-stolen-data/)
12 RE-ATT&CK Tactics – MITRE ATT&CK (https://attack.mitre.org/tactics/pre/)

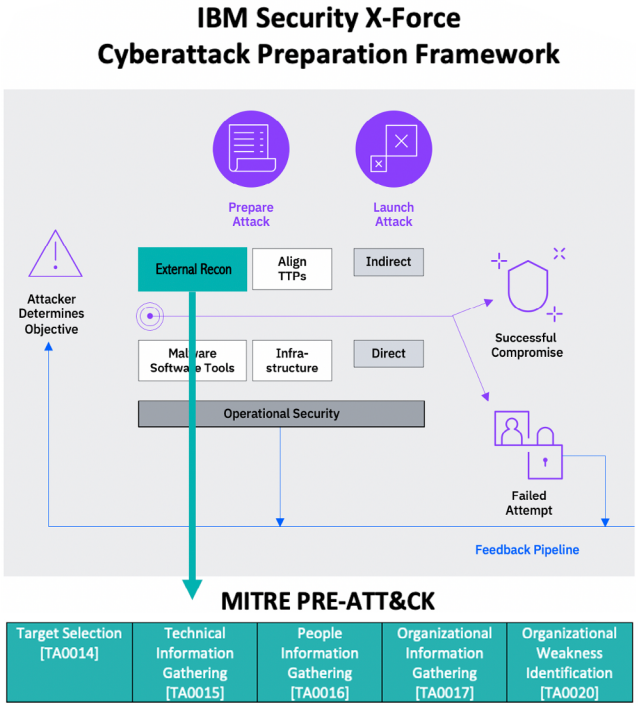

Figure 4: Cyberattack preparation framework as mapped to MITRE PRE-ATT&CK

REGULATORY AND LEGAL ISSUES

Government agencies globally encourage companies to report ransomware and other cyberattacks to authorities, but informing customers, users, or the general public is not required, except in some circumstances. For instance, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) regulations require electric organizations supporting the Bulk Electric System (BES) to report downtime and remediation efforts if it involves the critical infrastructure network.[13] Public companies will also report ransomware incidents that have material business impacts in financial filings with federal agencies but otherwise attacks frequently go unreported.

Data breach laws vary globally, and not every country has them. But such laws generally require companies to publicly report incidents when people's sensitive data is lost or stolen, including personally identifiable information like email addresses, passwords, and human resources records.[14] In Europe, for instance, the General Data Protection Regulation (GDPR) rules govern data breach notification laws, and in North America and Australia, privacy statues vary between federal legislation and state or territorial rules.

Ultimately, a company impacted by a cyber data breach faces more legal hurdles and will face more scrutiny than one impacted by a ransomware attack alone—potentially causing more financial and reputational damages.

RANSOMWARE AND STATE SPONSORED OPERATIONS

Multiple government agencies attributed the disruptive global WannaCry attack in 2017 to state actors known as the Lazarus Group.[15] Shortly after, the NotPetya worm encrypted (and ultimately wiped) systems around the globe, and multiple government entities associated this event with a state-sponsored group.

Recently, ransomware events have demonstrated the hallmarks of state-sponsored activity, including a series of attacks on industrial entities in Taiwan in May 2020. Known as ColdLock ransomware, the attacks targeted Taiwanese companies in the natural gas, petrochemical, and

13 CIP-008-6 — Cyber Security — Incident Reporting and Response Planning – NERC (https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf)
14 Data Protection Laws of the World – DLA Piper (https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US)
15 WannaCry ransomware attack 'linked to North Korea' – The Guardian (https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group)

semiconductor industries. Following the attacks, Taiwanese authorities said that Winnti was responsible for the event.[16]

Dragos has explored the possibility that the 2019 LockerGoga ransomware incident that disrupted operations at the aluminum manufacturer Norsk Hydro may have been linked to state-directed activity.[17] However, definitively linking or identifying ransomware attacks as potential cover for state-sponsored activity is difficult, due to the commonality of the threat and similarities in behavior across ransomware adversaries. It is likely that operators working on behalf of government-backed actors will use ransomware in the future as part of their operations to obscure goals related to espionage, disruption, or destruction of systems.

16 Bureau names ransomware culprits – Taipei Times (https://www.taipeitimes.com/News/taiwan/achives/2020/05/17/2003736564)
17 Spyware, Stealer, Locker, Wiper: LockerGoga Revisited – Joe Slowik, Dragos (https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/)

FUTURE PREDICTIONS

Ransomware will continue to be a major threat to industrial operations in the future. Despite efforts to improve security hygiene across multiple business sectors, poor security practices including improper segmentation between enterprise and operations networks will enable the infection and propagation of ransomware across business and ICS systems. Additionally, attacker behavior is adapting to corporate ransomware security efforts and expanding behaviors to include data theft and extortion.

Ransomware operators will likely continue to incorporate data theft and extortion techniques into their ransomware campaigns—potentially at increasing rates going forward, particularly if current threat actors using this technique find the business model to be successful. Dragos and X-Force also anticipate that ransomware attacks in the future will be used as a cover for state-sponsored operations.

Dragos and X-Force assess with high confidence that the threat of ransomware attacks to ICS and OT-connected networks is likely to increase, as future attacks build on the new efforts of ransomware such as EKANS, capable of disrupting industrial processes. This trend is also driven by the growing adoption of "big game hunting" efforts as well as data breach components forcing companies to publicly report incidents of compromise.

RECOMMENDATIONS

- Conduct architecture reviews to identify all assets, connections, and communications between IT and OT networks. Identify Demilitarized Zones (DMZs) to restrict traffic between enclaves. Critically examine and limit connections between corporate and ICS networks to only known, required traffic.
- Engage in effective defense-in-depth security strategies. Especially for ransom-ware attacks, having effective preventative, detective, and corrective controls in place is critical for reducing risk. Even if malware can evade anti-virus detection, endpoint detection systems and other controls can stop the threat before it spreads.
- Enforce Multifactor Authentication (MFA) wherever possible. Focus critically on connections to integrators, maintenance, vendor personnel, and crown jewels such as safety equipment. Ensure that critical network services, such as Active Directory (AD) and the servers hosting it, are well-defended and that administrative access to hosting devices is restricted to the greatest degree possible.
- Ensure remote access services such as virtual private network (VPN) and Remote Desktop Protocol (RDP) connections use industry standard secure credentials and cross to a separate OT domain.
- Ensure employees are trained to detect phishing attempts and report to security personnel when observed.
- Ensure backups of enterprise and operations network systems are maintained on a daily basis and test backups during disaster recovery simulations. For greatest security, store backups offline, but if this is not cost effective, ensure that any main network access to backups has only read—not write—access to prevent attackers from encrypting or

destroying backup files. Testing backup reconstitution plans is critical.

- Create an ICS-specific ransomware incident response plan and test this plan under pressure using a tabletop or cyber range exercise. These attacks move quickly, so developing your security team's muscle memory is critical and can make all the difference in preventing millions of dollars' worth of damage. Additionally, these experiences can help address the psychological impact of a breach event.
- Establish an alternate location from which critical business functions can run temporarily should a destructive malware or ransomware attack occur. Organizations that have been able to restore even some business operations following a destructive or ransomware attack have fared better than their counterparts. This capability allows your business to run even as attack remediation is ongoing.
- Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defense in depth strategies at the network level, leading to a more robust investigation ability by defenders and analysts.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE, PLEASE VISIT WWW.DRAGOS.COM.

TO LEARN MORE ABOUT IBM X-FORCE'S THREAT INTELLIGENCE AND INCIDENT RESPONSE SERVICES, PLEASE VISIT IBM.COM/SECURITY/SERVICES/THREAT-INTELLIGENCE

OR

IBM.COM/SECURITY/SERVICES/INCIDENT-RESPONSE-SERVICES.

THANK YOU