FORTRESS
Information Security

Threat Intelligence Report

Kaseya REvil Supply-Chain Ransomware Attack (Update A)

July 7, 2021

Date: July 7, 2021
https://www.fortressinfosec.com

Fortress Information Security, LLC
Phone: 855.FORTRESS
189 S. Orange Ave., Orlando, FL 32801

Table of Contents

Executive Summary Update

The July 2nd, 2021, ransomware attack on managed service provider (MSP) Kaseya is still ongoing as of July 7th. Kaseya has broadcasted their efforts at deploying an update for their Virtual System Administrator (VSA) that patches the flaw used by the attackers, allowing the company to bring their Software as a Service (SaaS) back online. The on-premises VSA reportedly has changes coming today in order to prepare customers for a patch. Kaseya is still working on implementing changes for the SaaS deployment and plans on restoring that service no later than evening of July 8th. The attacker, REvil, has asked $70MM for a universal decryption key. There are rumors that REvil has reduced the asking price and may go even lower. However, it is unlikely at this point that Kaseya will pay the ransom, which may cause REvil to shift focus onto the individual clients affected by the attack.

The US Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger released a statement on July 4th stating that the FBI and CISA would be assisting Kaseya and investigating the incident.

Fortress Information Security (FIS) will continue to monitor this threat and will update this report as new information is observed.

Incident Analysis[1]

On July 2nd, 2021, a sophisticated, mass-scale ransomware campaign was discovered targeting customers of Kaseya's managed services software and delivering REvil ransomware. This attack was initial thought to be a software supply chain attack enabled by a malicious update to Kaseya's VSA, but was soon found to be conducted leveraging a zero-day exploit against internet-facing Kaseya VSA servers.

Immediately after the attack, Kaseya started working on resolving the issue and restoring services to their customers. The company took preventive measures by shutting down the SaaS servers in order to protect their on-premises customers and strongly recommending keeping hosted VSA servers offline until further notice. Based on the technical analysis carried out by security researchers at Huntress, adversaries appear to have exploited an SQLi vulnerability within Kaseya's VSA servers. Adversaries applied an authentication bypass to gain access to the compromised VSA servers, upload the original payload, and run commands using the SQL injection flaw.

The attack resulted in more than a million individual devices being encrypted, according to an update on the official REvil blog. Simultaneously, security experts were able to identify infections at over 30 MSPs and over 1,000 businesses in the US, Australia, Europe, and Latin America. According to the REvil statement, the attackers plan to release a single decryption key for all victims if Kaseya pays a $70,000,000 ransom in Bitcoin. A security researcher reached out to REvil about the universal decryption tool over the weekend and received a response lowering the ransom price to $50 million, suggesting the actual price is negotiable.

---

[1] https://www.sentinelone.com/blog/revils-grand-coup-abusing-kaseya-managed-services-software-for-massive-profits/

Victim	Date	Victim	Date	Victim	Date	Victim	Date	Victim	Date	Victim	Date	Victim	Date
Grubman Shire Meiselas & Sac	2020-05-13	NEDA USA	2020-08-20	taylorfarms.com	2020-09-09	Darby Group	2020-11-18	Southern Arkansas University	2021-02-17	RHA Health Service	2021-04-14	Citroen Wells	2021-05-28
Actuaries and Associates	2020-08-20	ODLO International AG	2020-08-20	MEINHARDT	2020-09-14	EMAG company	2020-11-21	RS Hughes Co Inc	2021-02-18	Universal Group Inc.	2021-04-17	GRAYSONS SOLICITORS	2021-05-28
Adif (adif.es)	2020-08-20	Patten & Prentice patten.co.uk	2020-08-20	Russell,Kraft&Gruber	2020-09-24	Kenneth Copeland	2020-11-24	www.argomind.biz	2021-02-18	boulos.com	2021-04-18	Royal Resorts	2021-05-29
Agromart Group	2020-08-20	Plasmaterials Inc	2020-08-20	Synsam Group AB	2020-09-24	argentina.gob.ar	2020-11-26	www.thinkcaspian.com	2021-02-18	Carpenter Co.	2021-04-18	Aspire	2021-06-03
Alaska General Seafoods & Lea	2020-08-20	Plaza Collection LTD	2020-08-20	Global Cloud Xchange	2020-09-25	ctag.com	2020-11-26	MJS Packaging Inc	2021-02-22	EMC, Electric Motor and Contra	2021-04-18	ESD Dienstleistungs Gruppe	2021-06-03
Allison-Smith Company LLC	2020-08-20	quest-worldwide.com	2020-08-20	High Mark Real Estate	2020-09-25	fm-advogados.com.br	2020-11-28	Standley Systems	2021-02-22	Fonds Finanz	2021-04-18	Law Offices of Michael B. Brehn	2021-06-03
Armour & Associates	2020-08-20	Scalepeople	2020-08-20	MORRIS PETROLEUM Inc.	2020-09-25	https://local881ufcw.org/	2020-12-02	Wallin Hester, PLC	2021-02-23	Oré Peinture	2021-04-18	Sjk	2021-06-03
ASCENT Network	2020-08-20	Schramm Inc.	2020-08-20	Vard Group AS	2020-09-25	HEKEMIAN	2020-12-05	Ottawa, Kansas Cooperative As	2021-02-26	PB Swiss Tools	2021-04-18	SOL	2021-06-03
athrone.com	2020-08-20	Sherwood Food & Harvest Distri	2020-08-20	MARTIN	2020-10-06	High Point Engineering	2020-12-05	Union Bank of Nigeria	2021-02-26	Prerni Beauty Industries	2021-04-18	Tendriade	2021-06-03
australian company ARAFMI	2020-08-20	Silvaris	2020-08-20	ScentAir	2020-10-07	RMD Kwikform	2020-12-05	Blazona Concrete Construction	2021-03-02	Thomas Concrete Group	2021-04-18	Willson	2021-06-03
Brooks International	2020-08-20	Snaptron Inc	2020-08-20	Deltrol	2020-10-08	FDR & CP SERVICES	2020-12-09	Brownstein Rask LLP	2021-03-02	ReppertFactor, LLC.	2021-04-18	Arnoff Moving & Storage	2021-06-08
Brown Automotive Group Ltd	2020-08-20	SoftwareOne.com	2020-08-20	HERITAGE RECOURCE MANA	2020-10-09	Cardinal Logistics	2020-12-10	Reno & Zahm LLP	2021-03-02	Call Assist Ltd	2021-04-19	Macpherson Kelley Lawyers	2021-06-10
BROWN-FORMAN CORPORAT	2020-08-20	SPEC Inc	2020-08-20	JCI Industries	2020-10-09	Bentek	2020-12-14	PALIG.com	2021-03-06	Quanta Computer INC.	2021-04-20	********	2021-06-11
BURHANIGLASS.AE	2020-08-20	Strategic Sites	2020-08-20	ESII	2020-10-10	Dr. Macho + Partner	2020-12-14	Architectural Products of Virgini	2021-03-08	Harold Marcus Ltd.	2021-04-25	Feedback Technology Corp.	2021-06-12
CAT RICAMBI SRL Italy car sal	2020-08-20	Symbotic LLC	2020-08-20	UM1	2020-10-10	Trevor Sorbie	2020-12-15	TRIGANO, EUROPE'S NUMBE	2021-03-08	govnet of fiji	2021-04-26	WestCongress Insurance Servic	2021-06-14
CENTROID	2020-08-20	hrerarma.com	2020-08-20	DSBLS.COM	2020-10-13	HUBER+SUHNER	2020-12-18	Banco Inmobiliario Mexicano	2021-03-09	Habia Cable	2021-04-26	Whittlesey & Hadley	2021-06-14
chempack.com.au	2020-08-20	TO Engineers	2020-08-20	JMW.COM	2020-10-13	axiomstone.co.uk	2020-12-19	CIBA Insurance (The story abou	2021-03-09	mipharm.it	2021-04-26	BridgePoint Financial Services	2021-06-15
CINCINNATI CAPITAL CORPOR	2020-08-20	Universal Logistics Holdings	2020-08-20	Paradies Lagardere	2020-10-13	Ficosa	2020-12-21	cockram	2021-03-17	SOUTHERN ASPHALT	2021-04-26	PM Law Solicitors	2021-06-15
CivicSmart (ex Duncan Technol	2020-08-20	Vierra Magen Marcus LLP	2020-08-20	USPOLYCO	2020-10-13	Ghilotti Bros. Inc	2020-12-22	Acer Inc.	2021-03-18	Kajima corp	2021-04-27	lstaff.com	2021-06-15
COTTONWOOD FINANCIAL IN	2020-08-20	VIVA RESORTS	2020-08-20	ANSA McAL	2020-10-14	Communauto	2020-12-24	Corbally, Gartland and Rappleye	2021-03-18	Treehouse hotels	2021-04-27	atworksprofessional	2021-06-19
Duncan Co (www.duncanco.com	2020-08-20	VP Supply Corp	2020-08-20	Chesters International	2020-10-15	TheHospitalGroup	2020-12-24	McCabe & Romsman	2021-03-18	JHK Legal	2021-04-30	Moore Stephens Cape Town	2021-06-20
ehalc.com	2020-08-20	Wartman Law Firm	2020-08-20	www.braskem.com.br	2020-10-16	Ribstein & Hogan law firm	2021-01-03	www.crj.org The Crime and Just	2021-03-18	https://galoninsurance.ca/	2021-05-01	HAAI GmbH	2021-06-21
eurecat.com	2020-08-20	www.aaaambulance.net	2020-08-20	SHIONOGI & CO., LTD	2020-10-21	GRAND POWER, S.R.O.	2021-01-11	Milsoft Utility Solutions Inc	2021-03-23	Amfine Chemical Corporation	2021-05-02	Dicky Smith & Co Inc	2021-06-21
FGXI	2020-08-20	www.atlascars.com	2020-08-20	Beacon Health Solutions, LLC	2020-10-22	Preferred Home Care	2021-01-27	Summit Credit Union	2021-03-23	ASARCO LLC	2021-05-03	Canad Inns.	2021-06-21
Fraser Wheeler & Courtney LLP	2020-08-20	www.cablex-group.com	2020-08-20	Arapahoe Libraries	2020-10-24	Kahan, Kerensky & Capossela	2021-01-29	merrittwoodwork.com	2021-03-24	KEYENCE DEUTSCHLAND Gm	2021-05-03	French Connection	2021-06-22
Geidi.com	2020-08-20	www.intercardinc.com	2020-08-20	www.matson.com	2020-10-24	http://weilandlogistics.com	2021-02-01	Xchange Telecom - Brooklyn, N	2021-03-25	Lydall Inc.	2021-05-03	The Smith & Wollensky Restau	2021-06-24
Genesis Products Inc.	2020-08-20	www.lionco.com	2020-08-20	Hartz Mountain Industries	2020-10-30	E. & J. Gallo Winery	2021-02-02	MBA Group LTD	2021-03-30	Peter Müller GARTENGESTALT	2021-05-05	Trasporti Internazionali Transme	2021-06-24
GOODMANMINTZ	2020-08-20	in&k technology inc	2020-08-23	GPIGAMING.COM	2020-10-31	UCAR.FR	2021-02-02	Benetech, Inc.	2021-04-01	Thackray Williams LLP Solicitor	2021-05-06	Malcolm C Foy & Co Limited	2021-06-25
Groupe Cactus	2020-08-20	DYNEA.NET	2020-08-24	New Jersey Dental Hygienists' A	2020-11-05	Civinity Solutions	2021-02-03	Maestri Murrell Commercial Rea	2021-04-03	Apex America	2021-05-13	Grupo Fleury	2021-06-25
HAKUYOHIN	2020-08-20	Nature's Bakery, LLC	2020-08-24	Richardson	2020-11-05	Reese , Pyle , Drake & Meyer ,	2021-02-04	NorthWest , Insuranse Services	2021-04-04	GDS Gesellschaft für Datenverar	2021-05-13	Primo Water	2021-06-26
Hustech Installations AG husted	2020-08-20	Amicorp Group	2020-08-26	nexiamelbourne.com.au	2020-11-06	General Insulation	2021-02-08	Tristate Midstream	2021-04-04	Allen, Dyer, Doppelt, & Gilchrist	2021-05-14	Transform SR Brands, LLC	2021-06-29
HYMAN GROUP COMPANIES	2020-08-20	Elsa LLC	2020-08-26	TheLeeco	2020-11-06	Jacobs Vanaman Agency Insura	2021-02-08	Tata Steel GROUP	2021-04-05	Betenbough Homes	2021-05-15	University Medical Center of Sou	2021-06-29
insport.com.au	2020-08-20	Long & Foster	2020-08-27	ASGCO Complete Conveyor So	2020-11-08	SOUTHERN CONCRETE & CO	2021-02-08	NEO DERM GROUP LTD	2021-04-06	CEC Vibration Products	2021-05-15	Asfaltproductienijmegen	2021-06-30
jnbs	2020-08-20	Valley Health Systems	2020-08-27	JBS United www.jbsunited.com	2020-11-08	Resort Lifestyle Communities	2021-02-10	Varner & Brandt LLP	2021-04-06	ENPOL LLC	2021-05-18	CYMZ	2021-06-30
Kenneth Cole Productions	2020-08-20	4datanet.com	2020-09-09	WORLD LOGISTICS USA INC	2020-11-08	Dairy Farm	2021-02-15	Harris Federation	2021-04-08	laffaldano, Shaw & Young LLP	2021-05-19	Vic Pharma Industry and Trade	2021-06-30
M J Payne Ltd	2020-08-20	Agrosuper	2020-09-09	ILG.COM.AU	2020-11-14	SHELLY & SANDS, INC	2021-02-15	Honeywell International Inc.	2021-04-09	Agile Property Holdings	2021-05-24	Masmovil ibercom SA	2021-06-30
malabs.com	2020-08-20	DXP Enterprises, Inc.	2020-09-09	Tree Top	2020-11-14	J & B Distributing Co.	2021-02-16	Heartland Automotive, LLC	2021-04-10	angstrom automotive group	2021-05-24	neroindustry.com	2021-07-01
MAN België	2020-08-20	greatnorthemcorp.com	2020-09-09	CMC Consulting	2020-11-16	Malcolm Drilling Company, Inc.	2021-02-16	Fultz Maddox Dickens	2021-04-11	Möbelstadt Sommerlad	2021-05-26	Stevens & Lee	2021-07-03
National Western Life	2020-08-20	Sampoerna Agro	2020-09-09	Siplec.com	2020-11-16	D.M. BARONE SPA	2021-02-17	Pierre Fabre Group	2021-04-12	Gosiger	2021-05-27	kuk.de / KREBS + KIEFER	2021-07-03

Figure 1 Example List of Infected Companies

On Monday, July 5th, Kaseya announced they were developing a patch for on-premises installations in order to assist customers in getting back to service. Kaseya also published a Compromise Detection Tool for customers to check if their on-premises installation had been compromised. Since the initial attack, other threat actors have been scanning for Kaseya on-premises servers exposed to the internet using publicly available platforms such as Shodan. This time window between the vulnerability disclosure and the release of a patch allows threat actor groups besides REvil to potentially obtain access to exposed Kaseya VSA servers. This attack highlights the necessity for a modern endpoint detection and response (EDR) solution which defends against improper use of built-in operating system executables, such as detecting *certutil.exe* writing executables or usage of signed software such as *MsMpEng.exe* running from unexpected locations and executing unexpected software.

MITRE ATT&CK

The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. Below is a list of various phases and attack types used by REvil.

Common Tactics, Techniques, and Procedures (TTPs) used by REvil.

Below are TTPs used in the Kaseya attack.

Initial Access

- Supply Chain Compromise [T1195]
- Exploit Public-Facing Application [T1190]

Execution

- Native API [T1106]

Persistence

- DLL Side-Loading - T1073
- Create or Modify System Process: Windows Service [T1543.003]

Defense Evasion

- Modify Registry T1112

- Masquerading T1036
- Masquerading: Rename System Utilities T1036.003
- Indirect Command Execution T1202

Discovery

- Query Registry [T1012]
- System Information Discovery [T1082]
- Peripheral Device Discovery [T1120]

Impact

- Data Encrypted for Impact [T1486]
- Defacement [T1491]

Technical Details[2]

Logic flaws in one of the VSA components *dl.asp* may have led to an authentication bypass vulnerability. The attackers then used *KUpload.dll* to drop multiple files including *agent.crt*, a fake certificate that contains the malware dropper. Another dropped artifact, *Screenshot.jpg*, appears to be a JavaScript file and has only been partially recovered at this time. Specific details regarding the exact nature of the exploit used are still being discovered as the analysis is ongoing. The suspected exploit chain ends with a SQL injection in *userFilterTableRpt.asp* in order to queue up a series of VSA procedures that would execute the malware and purge the logs. This activity was seen originating from a hijacked AWS EC2 instance **18(.)223.199.234**. Additional activity was observed originating from 161(.)35.239.148 (DigitalOcean), 162(.)253.124.16 (Sapioterra), and 35(.)226.94.113 (Google Cloud).

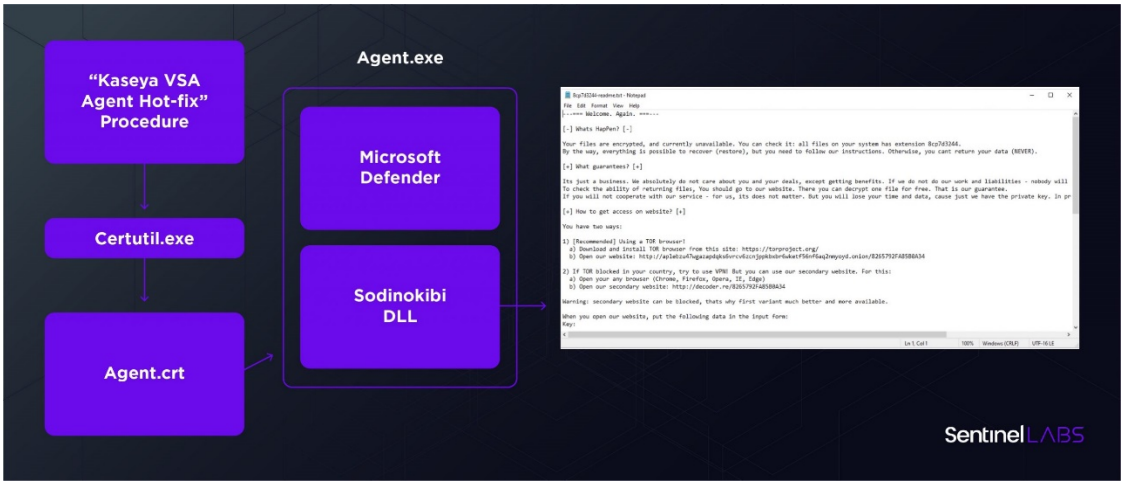

Figure 2 REvil Kaseya Malware Infection Chain

The malicious procedure was labeled 'Kaseya VSA Agent Hot-fix'. This procedure is a series of commands that checks for internet access and uses PowerShell to disable a sequence of native Operating System security measures including real-time monitoring, intrusion prevention, network protection, and sample auto-submission. The procedure then invokes the native certutil.exe application commonly used to validate certificates and uses it to decode the contents of 'agent.crt' into an executable, agent.exe.

[2] https://cryptobook.nakov.com/symmetric-key-ciphers/popular-symmetric-algorithms

REvil is using the Salsa20 symmetric stream algorithm for encryption with an elliptic curve asymmetric algorithm. Salsa20, also known as ChaCha, is a family of modern, fast, symmetric stream ciphers and takes an input as 128 bit or 256-bit symmetric secret key, a randomly generated 64 bit nonce, and a stream of data of unlimited length and produces an encrypted stream of data with the same length as the input stream. Salsa20 encryption has also been seen in the EternalPetya attacks and most recently the Colonial Pipeline ransomware attack.

Indication of Compromise

The following files are known to be involved in the Kaseya breach. If you notice a device contains these files, you have likely been compromised and should seek immediate remediation.

Samples

- agent.crt encoded dropper
  2093c195b6c1fd6ab9e1110c13096c5fe130b75a84a27748007ae52d9e951643
- agent.exe dropper
  d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

Payloads

- e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
- 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

Signatures

- aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7
- df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e
- f6908ef76b666157a13534db47652a845d8f7d985fdf944f7e43a3afd3f3d8c2
- d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f
- d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20
- dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f
- cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6
- 81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471

Adversary's Actions and Tactics[3]

The REvil (also known as Sodinokibi) ransomware was first identified on April 17, 2019. It is used by the financially motivated GOLD SOUTHFIELD threat group, which distributes ransomware via exploit kits, scan-and-exploit techniques, RDP servers, and backdoored software installers. REvil is likely associated with the GandCrab ransomware due to similar code and the emergence of REvil as GandCrab activity declined. Researchers attribute GandCrab to the GOLD GARDEN threat group. REvil is maintained actively and is under constant development, just as GandCrab was. The most recent REvil ransomware at the time of this report is version 2.1.

The main actor associated with advertising and promoting REvil ransomware is called Unknown aka UNKN. The RaaS is operated as an affiliate service, where affiliates spread the malware by acquiring

[3] https://intel471.com/blog/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/

victims and the REvil operators maintain the malware and payment infrastructure. Affiliates receive 60% to 70% of the ransom payment.

REvil is highly configurable and allows operators to customize the way it behaves on the infected host. Some of its features include:

- Exploits a kernel privilege escalation vulnerability to gain SYSTEM privileges using CVE-2018-8453.
- Whitelists files, folders, and extensions from encryption.
- Kills specific processes and services prior to encryption.
- Encrypts files on local and network storage.
- Customizes the name and body of the ransom note, and the contents of the background image.
- Exfiltrates encrypted information on the infected host to remote controllers.
- Uses Hypertext Transfer Protocol Secure (HTTPS) for communication with its controllers.

REvil - Victim Interactions[4]

The lowered ransom price from $70MM to $50MM indicates that REvil is not getting the payoff result they want from Kaseya and are forced to deal with individual clients, which number in the thousands. In one instance, an unknown company affected by the ransomware reached out to REvil to negotiate a ransom price and was met with confusing messages, showing a breakdown of the REvil ransom team. The original asking price was $45,000, then increased to $550,000, then reduced to $225,000. The company also dealt with multiple REvil representatives, also leading to confusion about chat history and repeating information. Three bitcoin addresses were sent and as of July 6th they were still inactive. These details indicate a lack of organization on REvil's part and indicate the group may be unprepared to monetize attacks affecting more than a few organizations. At this time no other interactions between REvil and the affected organizations are known.

Other Recent Engagements

REvil has recently involved in an attack against a US clean power company, Invenergy. REvil claimed to have downloaded terabytes of sensitive data along with personal details on Invenergy chief executive Michael Polsky from his personal computer. Invenergy operations have not been impacted and no data was encrypted during the attack. Invenergy has also stated that they have not paid or intend to pay any ransom from REvil.

Impact on Critical Infrastructure Sectors

North America, Europe, South America, and parts of Asia were hit the hardest by the Kaseya attack. In Sweden, the grocer retail chain Coop was forced to close 800 stores due to issues with their billing systems. Other impacted businesses include gas stations, railways, pharmacies, and the public

[4] https://www.suspectfile.com/kaseya-data-breach-70m-per-il-decrittatore-universale-intanto-revil-tratta-privatamente-con-alcune-vittime/

broadcaster SVT. In Germany and the Netherlands three large IT companies were forced to shut down as well, impacting thousands of their clients.

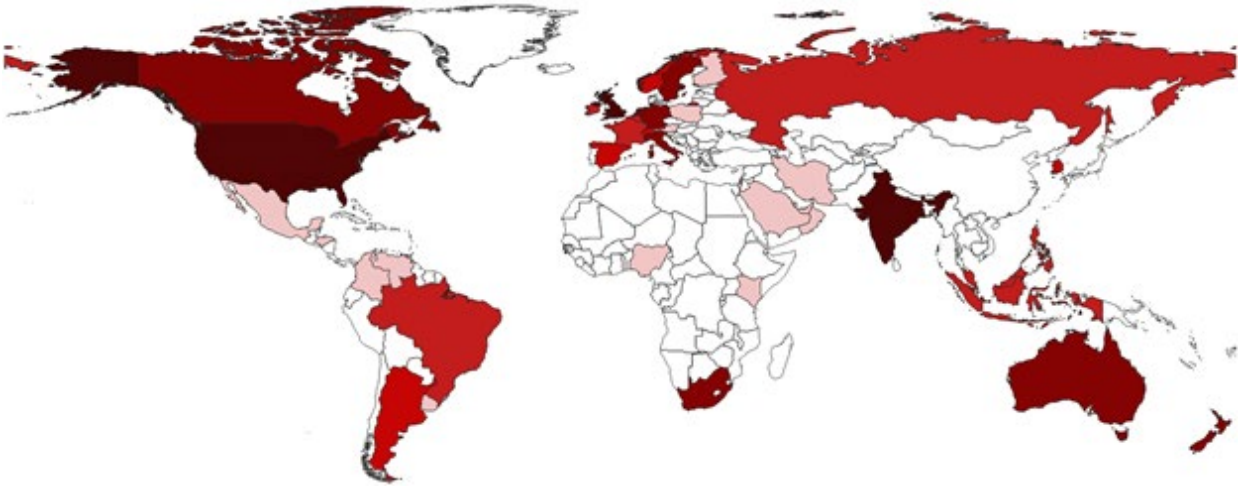

Figure 3 Kaseya users by country, darker fill signifies higher number of users

A scan for the Kaseya favicon hash revealed approximately 1700 results within the USA, including results associated with at least two utility companies based in Kansas and Iowa. Both companies' Kaseya-linked web assets are currently offline. This could be an indicator of attack, or more likely, indicates that they were taken down to prevent vulnerability exploitation.

This list is incomplete and Fortress is still investigating possible links between the Kaseya attack and US critical infrastructure entities.

Security Recommendations and Mitigation Strategies

MITRE D3FEND

The MITRE D3FEND framework is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques.

Harden

- Platform Hardening
  - Disk Encryption [D3-DENCR]
  - Software Update [D3-SU]

Detect

- Operating System Monitoring
  - Endpoint Health Beacon [D3-EHB]
  - System File Analysis [D3-SFA]

Fortress Information Security Recommendations

Fortress Information Security (FIS) recommends companies take defensive measures to minimize the risk of exploitation of vulnerabilities. Specifically, companies should:

Implement Controls to Prevent and Detect Malware Deployment:

- Ensure that antivirus/endpoint protection software is deployed on all endpoints. Antivirus signatures should be kept updated to ensure it is protecting against the latest threats.
- Monitor outbound network traffic for any suspicious activity – this could serve as an indicator of malware attempting to communicate with a Command and Control (C2) server.
- Ensure your security tools are monitoring for known indicators of compromise.
- Malware is frequently delivered by phishing emails, so ensure that users are trained not to open attachments or click on links from suspicious sources.

Protect your Network from External Attackers:

- Ensure all network and system resources are properly protected by firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).
- Configure firewalls to block known malicious IP addresses.
- If remote access to corporate resources is needed, be sure employees use a Virtual Private Network (VPN).
- Ensure that your company maintains an up-to-date inventory of all externally facing assets. Maintaining an accurate asset inventory is critical in ensuring defensive measures are properly deployed across the entire perimeter.

Develop a Data Loss Prevention Program:

- Ensure system monitoring is in place to be able to track who is accessing specific files. This will help pinpoint exactly when files were extracted and who was involved.
- Scan all outgoing emails to detect any potential confidential data leaving the company's network.
- Consider limiting access to cloud storage websites that can be accessed from outside of the corporate network. If there is not a legitimate business need to use these types of websites, they may present undue risk of data exfiltration.
- Limit users' ability to store data on external storage devices, unless there is a business need to do so.

Have a Vendor Risk Management Program:

- Security breaches at vendors that have access to your company's data or systems can pose just as much of a threat as a data breach at your company. Ensure you have a program in place to manage these risks and respond to vendor breaches when they occur.
- Ensure that network traffic and email communications between your company and its vendors is monitored for any anomalies that could indicate malicious activity.
- Evaluate all vendors' security controls regularly to ensure they align with your company's risk posture.

FIS reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Appendix A: Kaseya REvil Supply-Chain Ransomware Attack

Executive Summary

On July 2nd, 2021, Kaseya, a Managed Service Provider company, announced they were experiencing a potential attack against their Virtual System Administrator (VSA) and some on-premises clients had been affected. Kaseya has approximately 40,000 clients using one or all of their VSAs, either on-premises or Software-as-a-Service (SaaS). The attack culminated with supply chain ransomware demands from the known ransomware-as-a-service (RaaS) group REvil. Technical details on how the attack was executed have not been fully released however we do know that the initial intrusion vector was a zero-day vulnerability found in the Kaseya VSA. Kaseya has taken their on-premises and SaaS servers offline until a patch has been released.

As of July 3rd, eight Managed Service Provider (MSP) clients have been infected with at least three victims within the USA. The specific MSP clients have not been publicly named yet. Kaseya posts updates every few hours on their website about the ongoing attack and what they are doing to combat the ransomware. Kaseya is working continuously to bring updates to its customers and the public every 3 to 4 hours.

Fortress Information Security (FIS) will continue to monitor this threat and will update this report as new information is observed.

Incident Analysis[5][6]

On July 2nd, 2021, a ransomware attack targeted at least 200 U.S company networks. REvil, a RaaS group appears to be behind this attack. REvil targeted a software supplier called Kaseya using its network management package as a conduit to spread the ransomware through cloud-service providers. Similar to the SolarWinds incident in 2020, this attack is considered to be a highly sophisticated supply chain attack using ransomware.

Both the Federal Bureau of Investigation (FBI) and Federal Cybersecurity and Infrastructure Security Agency (CISA) is working closely together to collect more information about this attacks impact. CISA urges companies affected by Kaseya follow their guidelines and shutdown VSA servers immediately.

What is a Supply Chain Attack?

A supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates a company through an outside provider with access to its systems and/or data. These attacks attempt to inflict damage to a company by exploiting vulnerabilities in its supply chain network. Supply chain attacks have dramatically changed the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data.

---

5 https://apnews.com/article/business-technology-3011c6037bda9ac11b1249a4beb13b06

6 https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b

The supply chain network is a frequent target for malicious threat actors, as a weak link in the supply chain can grant the attackers access to the target organization in custody of the data sought after. A company's supply network usually consists of third-party entities like manufacturers, suppliers, handlers, shippers, and purchasers all involved in the process of making products available to the end consumers. Because the target company may have a security system that is difficult to penetrate for even sophisticated attackers, supply chain attacks are carried out on suppliers that are deemed to have the weakest security measures.

Another way a supply chain can be leveraged to attack a target company is through malicious software, popularly known as malware. By embedding malware or counterfeit components that modify the manufacturer's software source code, cyber attackers can infiltrate the target company and steal its proprietary information.

MITRE ATT&CK

The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. Below is a list of various common phases and attack types used by REvil.

Initial Access, Lateral Movement, Command and Control, Execution, Exfiltration, Persistence, Collection, Privilege Escalation, Discovery, Defense Evasion

- Valid Accounts [T1078]
- Phishing [T1566]
- Exploit Public-Facing Application [T1190]
- External Remote Services [T1133]
- Remote Desktop Protocol [T1021.001]
- Web Protocols [T1071.001]
- Multi-hop Proxy [T1090.003]
- PowerShell [T1059.001] Automated Exfiltration [T1020]
- Scheduled Task [T1053.005]
- Archive Collected Data [T1560]
- Automated Collection [T1119]
- Bypass User Account Control [T1548.002]
- Account Discovery [T1087] Modify Registry [T1112]

Discovery

- File and Directory Discovery [T1083]
- Process Discovery [T1057]

Impact

- Service Stop [T1489]
- Inhibit System Recovery [T1490]
- Data Encrypted for Impact [T1486]

Technical Details[7][8]

Kaseya has reported that the initial entry for the supply chain ransomware attack occurred using a zero-day vulnerability in Kaseya VSA, this allowed attackers to launch remotely executed commands on the VSA appliance. Technical details on how the exploit of the vulnerability works will not be provided until the patch has become available.

What is known is that the delivery of the ransomware was done via an automated fake software update using Kaseya VSA. The attack immediately stops administrator access to the VSA, and then adds a task called *Kaseya VSA Agent Hot-fix*. This fake update is then deployed across the network including on MSP client customers' systems as it a fake management agent update. This management agent update is actually the REvil ransomware. Organizations that are not Kaseya's customers are still encrypted. The deployment also attempted to tamper with products for other vendors such as Sophos while the ransomware deliberately targets backup systems to hinder restoration attempts.

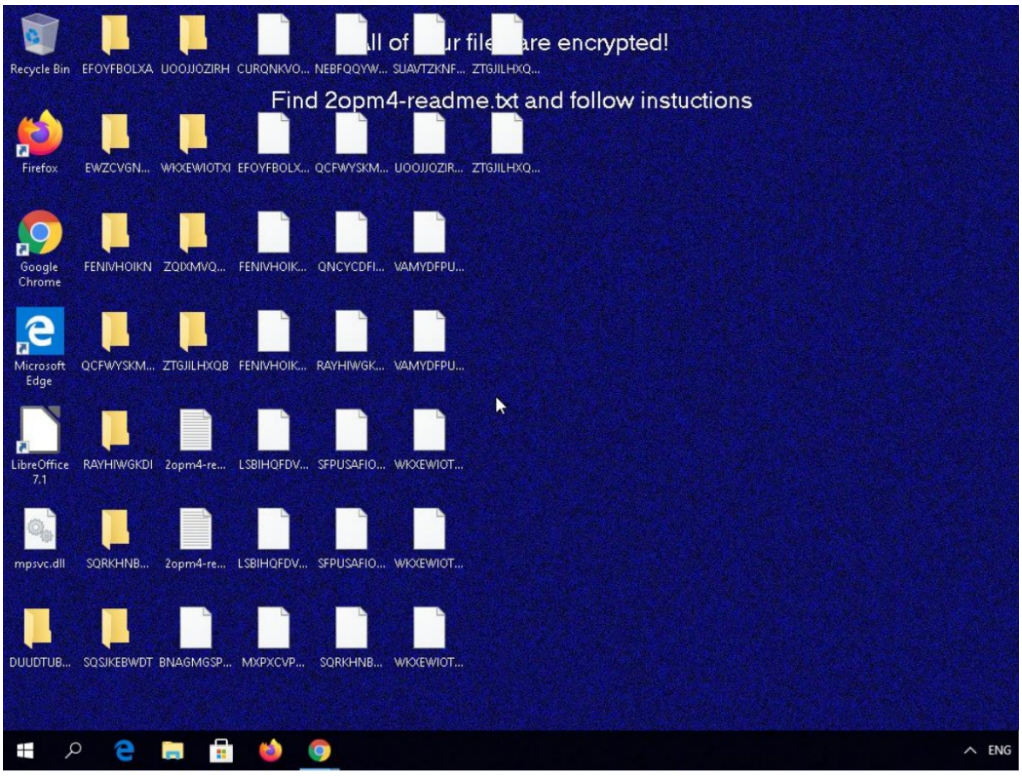

Figure 3 Display of REvil ransomware infected systems

As of July 3rd, 2021, three executable files, one certification, and one dll have been validated as indication of compromise. The ransomware encryptor is dropped to c:\knowrking\agent.exe, the VSA procedure is renamed to Kaseya VSA Agent Hot-fix, the agent.exe runs, then the legitimate Windows

[7] https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-3rd-2021

[8] https://www.zdnet.com/article/kaseya-urges-customers-to-immediately-shut-down-vsa-servers-after-ransomware-attack/

Defender executable MsMpEng.exe and encryptor payload mpsvc.dll are dropped into the hardcoded path c:\Windows to DLL sideload.

```
/* WARNING: Globals starting with '_' overlap smaller symbols at the same address */

undefined4 __fastcall
WinMain(undefined param_1,undefined param_2,undefined param_3,undefined param_4,LPWSTR param_5)

{
  HRSRC pHVar1;
  HGLOBAL pvVar2;
  LPWSTR lpApplicationName;

  pHVar1 = FindResourceW((HMODULE)0x0,(LPCWSTR)0x65,L"SOFTIS");
  if (pHVar1 != (HRSRC)0x0) {
    pvVar2 = LoadResource((HMODULE)0x0,pHVar1);
    if (pvVar2 != (HGLOBAL)0x0) {
      DAT_004143a0 = LockResource(pvVar2);
      pHVar1 = FindResourceW((HMODULE)0x0,(LPCWSTR)0x66,L"MODLIS");
      if (pHVar1 != (HRSRC)0x0) {
        pvVar2 = LoadResource((HMODULE)0x0,pHVar1);
        if (pvVar2 != (HGLOBAL)0x0) {
          _DAT_004143a4 = LockResource(pvVar2);
          FUN_00401000((int)_DAT_004143a4,0xc5588,L"mpsvc.dll");
          lpApplicationName = FUN_00401000((int)DAT_004143a0,0x56d0,L"MsMpEng.exe");
          _DAT_004143a8 = 0x44;
          CreateProcessW(lpApplicationName,param_5,(LPSECURITY_ATTRIBUTES)0x0,
                         (LPSECURITY_ATTRIBUTES)0x0,0,0x230,(LPVOID)0x0,(LPCWSTR)0x0,
                         (LPSTARTUPINFOW)&DAT_004143a8,(LPPROCESS_INFORMATION)&DAT_004143ec);
        }
      }
    }
  }
  return 0;
}
```

Figure 2 MsMpEng.exe and mpsvc.dll embedded in agent.exe

Indication of Compromise[9]

The following IP addresses, ports, and files are known to be involved in REvil's supply chain ransomware attack. If you notice a device is communicating to these addresses or contains these files, you have likely been compromised and should seek immediate remediation.

Known Files:

- C:\windows\cert.exe
  - 36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752
- C:\windows\msmpeng.exe
  - 33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a
- C:\kworking\agent.crt
- C:\Windows\mpsvc.dll
  - 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
- C:\kworking\agent.exe

[9] https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers

- d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

Registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlackLivesMatter
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Kaseya\Agent\<unique id>

Ransomware Extension:

- <unique id>-readme.txt

```
---=== Welcome. Again. ===---

[-] Whats HapPen? [-]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has
extension [REDACTED].
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise,
you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do
not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for
free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and
data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: [REDACTED]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: [REDACTED]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:


[REDACTED]



--------------------------------------------------------------------------------

!!! DANGER !!!
DON'T try to change files by yourself, DON'T use any third party software for restoring your data or
antivirus solutions - its may entail damage of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make
everything for restoring, but please should not interfere.
!!! !!! !!!
```

Figure 2 REvil readme.txt

Domains:

- ncuccr[.]org
- 1team[.]es
- 4net[.]guru
- 35-40konkatsu[.]net
- 123vrachi[.]ru
- 4youbeautysalon[.]com
- 12starhd[.]online
- 101gowrie[.]com
- 8449nohate[.]org
- 1kbk[.]com[.]ua
- 365questions[.]org
- 321play[.]com[.]hk
- candyhouseusa[.]com
- andersongilmour[.]co[.]uk
- facettenreich27[.]de
- blgr[.]be
- fannmedias[.]com
- southeasternacademyofprosthodontics[.]org
- filmstreamingvfcomplet[.]be
- smartypractice[.]com
- tanzschule-kieber[.]de
- iqbalscientific[.]com
- pasvenska[.]se
- cursosgratuitosnainternet[.]com
- bierensgebakkramen[.]nl
- c2e-poitiers[.]com
- gonzalezfornes[.]es
- tonelektro[.]nl
- milestoneshows[.]com
- blossombeyond50[.]com
- thomasvicino[.]com
- kaotikkustomz[.]com
- mindpackstudios[.]com
- faroairporttransfers[.]net
- daklesa[.]de
- bxdf[.]info
- simoneblum[.]de
- gmto[.]fr
- cerebralforce[.]net
- myhostcloud[.]com
- fotoscondron[.]com
- sw1m[.]ru
- homng[.]net

Adversary's Actions and Tactics

REvil[10][11][12]

REvil (also known as Sodinokibi/Sodin) has been active since 2019. The REvil RaaS group shares similarities to the GandCrab RaaS which was linked to the Gold Southfield Group, suggesting the attackers responsible for the malware have been active for even longer. REvil is also possibly a parent organization for the now deactivated DarkSide group who was responsible for the USA Colonial Pipeline attack in May. REvil's ransomware code, ransom note structure, and country-of-origin code check system are all very similar to DarkSide's code used during their Colonial attack. REvil is believed to be based in Russia, as the threat actor group does not target organizations within Russia or other former Soviet territories.

[10] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/

[11] https://twitter.com/markloman/status/1411053456983564300

[12] https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html

Figure 3 DarkSide readme.txt. Note similar section titles "What happened?", "What guarantees?", "How to get access on website", and "DANGER" message to the REvil readme.txt

REvil first made headlines in 2019 after a successful ransomware attack on Travelex, who reportedly paid a 2.3-million-dollar ransom. Since then, REvil has become notorious for targeting large organizations, and demanding massive ransom payments. In 2021 alone, REvil has targeted the following organizations:

- **April 2021 – Quanta Computer and Apple** – REvil compromised Quanta Computer, a primary supplier for Apple, and attempted to extort a 50-million-dollar ransom in exchange for not releasing information related to upcoming Apple products. After Quanta was unwilling to comply, REvil then shifted their focus and demanded that Apple pay the ransom.

- **May 2021 – JBS Foods** – REvil successfully compromised JBS Foods and temporarily shut down the company's operations in both the United States and Australia. JBS eventually paid the demanded ransom of 11 million dollars, reportedly in an effort to protect their customers and employees. After this attack, a member of REvil said in an interview that their original was not JBS but was instead an unnamed Brazilian organization.

- **June 11 – Invenergy –** REvil claimed to have downloaded 4 terabytes of sensitive data, including projects, contracts, and non-disclosure agreements. They also claimed to have hacked Invenergy's CEO Michael Polsky's personal computer and threatened to release the data unless ransom was paid. Invenergy stated they will not pay the ransom and to date it is unknown if this data was released.

- **July 2 – Kaseya –** Currently ongoing ransomware attack

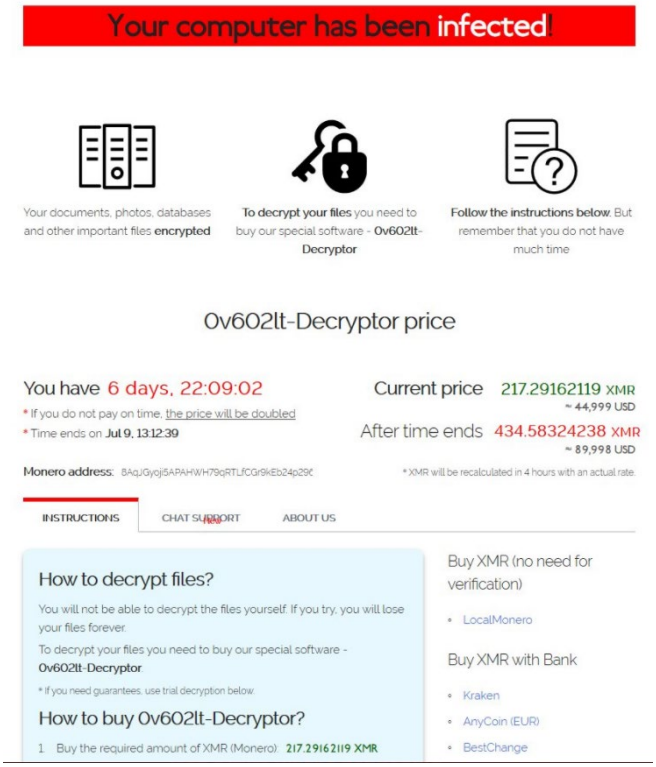

Figure 4 REvil ransom note screenshot from encrypted end-point user, ransom request of $44,999

Impact on Critical Infrastructure Sectors

Ransomware can cripple critical systems, violating one of the utilities sectors' most import characteristics: service reliability. Modern ransomware attacks represent a serious security challenge for infrastructure operators because even a short amount of downtime or latency can significantly impact the delivery of essential services. In addition, cyber-attacks against critical infrastructure systems (CIS), do not only pose a risk to customer data or corporate reputation at risk but can also impact the safety of citizens. Ransomware attacks directed against CIS systems are relatively uncommon according to public reports, but the impact can be significant.

A ransomware operators' main motivation is financial; they attempt to disrupt/destroy software and hardware systems and/or threaten companies with the disclosure of sensitive information for monetary gain. If a successful attack were launched on an electric grid, a water supply system, or natural gas pipeline, we could see sensitive data stolen and used for extortion or entire regions left without essential resources. While ransomware attacks have traditionally focused on companies' information technology (IT) networks, we are now seeing more instances of malware spreading to the operational technology (OT) technologies that control key mechanical equipment. The successful attacks on Electrobras and Copel Utility saw the temporary shutdown of operations and services. The attack also allowed Sensitive data to be stolen and dumped online, including network access logins and engineering plans. The ransomware group Darkside, was found to be responsible for the Copel utility attack and stole more than 1,000 gigabytes of Copel data, including sensitive information allowing for access to key infrastructure, personally identifiable information (PII) or top management and customers, and detailed engineering plans of the companies' network. The Eletrobras attack hit the administrative network of its Electronuclear subsidiary, which runs two nuclear power plants. This incident demonstrates how electricity operators are at significant risk from a potential adversary with

malicious intent. These attacks forced A sustained failure of the electricity grid could also have potentially devastating consequences for the other industries that are dependent on it. From transport to health services, virtually every element of critical infrastructure is dependent on the grid.