KING & SPALDING

Client Alert

Data, Privacy and Security

MAY 12, 2021

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Chris Burris
+1 404 572 4708
cburris@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Robert Hudock
+1 202 626 5521
rhudock@kslaw.com

Nicholas Schmidt
+1 202 626 5573
nschmidt@kslaw.com

Jillian Simons
+1 404 572 2721
jsimons@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Avenue
Washington, D.C. 20006
Tel: +1 202 737 0500

Ransomware on the Rise in Critical Infrastructure Sector

Recent ransomware attacks against U.S. critical infrastructure, which includes the energy sector's production of oil and natural gas, and other sources of electricity and power, have shed a spotlight on the importance of staying updated on sector-specific techniques, tactics and procedures ("TTPs"), and preventative and remediation actions.

This Client Alert will: (1) provide a brief background on the nature and risks of ransomware on critical infrastructure; (2) discuss the current ransomware threat landscape; (3) note legal considerations companies should take into account when determining how to respond to ransomware attacks; (4) discuss recent calls for cybersecurity oversight; (5) provide an overview of recent public ransomware incidents; and (6) set forth potential steps companies can take to mitigate the risks of ransomware.

RANSOMWARE IMPACT ON CRITICAL INFRASTRUCTURE

Ransomware is defined by the U.S. National Institute of Standards and Technology ("NIST") as a "type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid." Often, the ransom is requested for payment through cryptocurrency or blockchain methods that provide for anonymity on behalf of the recipient of the payment.

Ransomware attacks directed against critical infrastructure systems are relatively rare, but the impact could be significant. If a threat actor gained access to the control network, a skilled threat actor could then upload exploits and/or entirely new firmware, which could allow the hacker to cause physical damage to components of the infrastructure at will. In other words, the threat actor could potentially take complete control of an entire system or device.

Another strategy used by ransomware threat actors is to threaten to "brick"—destroy beyond repair—the software and hardware that control the infrastructure in addition to corrupting the data stored on the system using malicious encryption. This is similar to the Ukrainian power grid attack in 2015 where the threat actors corrupted the firmware of devices controlling various power substations.[1] In such an instance where control components are “bricked,” a victim must physically change each bricked component by replacing it.

The Federal Bureau of Investigation (“FBI”) has identified several key threat actor collectives emerging from the recent attacks, including a malware variant attributed to Darkside.[2] The Darkside developers, Carbon Spider, operate as a Ransomware-as-a-Corporation (“RaaC”)[3] provider, thought to be located in Eastern Europe.[4] The FBI also notes that Darkside actors are encouraged by the malware developers to use Monero cryptocurrency in the demands because it uses privacy-enhancing technologies to provide users with greater anonymity compared to more traditional cryptocurrencies.[5] The Darkside TTPs, and those of similarly sophisticated collectives such as Viking Spider, Graceful Spider and Pioneer Kitten, have been identified as early as December of 2019 with at least 16 new collectives and their malware emerging in 2020.[6]

Darkside-related ransomware variants have been in the threatscape since at least September of 2020. This variant is typical of those used by many ransomware collectives today, but also shows some innovations, namely the use of custom-designed executables for each target. The Darkside group follows the RaaC paradigm, and thus strives to appear professional, offering press releases and corporate language in its communications and executables. Like many modern ransomware collectives, in addition to seeking to deny a company access to its own data, Darkside often attempts to exfiltrate personally identifiable information and other data on finances, business partners, and operations, and posts it on its dark web “leak site” if its ransomware demands are not met. The Darkside group is noted for performing extensive due diligence on its targets and generally only attacking high-revenue companies; avoiding other “critical” targets such as hospitals or governments. Darkside’s strategy of generally targeting valuable companies is part of a clear trend of “big game hunting” that took off in 2020.

RANSOMWARE THREAT LANDSCAPE

In 2020 and 2021 there has been a surge in sophisticated ransomware campaigns that are “human-operated,” where an operator controls the attack instead of delegating it to a bot or other automated tasks, which is a TTP of Darkside actors. Once inside, the threat actors move around the network, identify any valuable data, and assess the security controls used, which often ends with them disabling endpoint protection tools and deleting backups prior to making a ransom demand. Like many other ransomware variants, Darkside follows the rising trend of “double extortion” by: (i) deleting or corrupting backups, exfiltrating targeted data, and making the demand for payment; and, (ii) encrypting targeted data, thereby locking the company out until payment. If effective, this technique can render the strategy of backing up data as a precaution against a ransomware attack moot. At the start of 2020, few ransomware groups both encrypted and exfiltrated data, but by the end of the year, at least 17 groups have used this tactic.

This level of sophistication is often associated with “big game hunting,” which are ransomware campaigns aimed at high-value targets. Such attacks dominated the ecosystem of threat actors in 2020, priming the market for the increase of “network access brokers”—threat actors that gain backend access to an organization and who then sell this access to a third party. Often, threat actors leverage the research and targeting already performed by the broker, which allows for a faster malware deployment lifecycle, which in turn increases the likelihood of potential monetization. Carbon Spider, the group purportedly behind Darkside—and the third-highest reported threat actor in 2020 according to CrowdStrike—began this trend in April 2020.[7] By November 2020, they had established procedures for other threat actors in their collective to provide them with a portion of each campaign’s profit. This RaaS business model allows less-savvy threat actors to leverage target research and sophisticated malware in exchange for paying a commission of any ransom received.

According to a recent report by British security company Sophos,[8] 51% of surveyed companies were impacted by a ransomware attack in the last year, and of those, 73% resulted in successful data encryption, which may represent more mature tactics and an increase in targeting larger corporations using more individually-tailored methods that are similar to Darkside.

According to cyber insurance firm Coalition, ransomware attacks are the most commonly reported cyber insurance claim. In the first half of 2020, Coalition observed a 260% increase in the frequency of ransomware attacks among its policyholders, with the average ransom demand increasing 47% to an average of $338,669.[9] The average ransom paid in 2020 was $170,404.[10] In 2021 to-date, the average cost of handling a ransomware incident totaled $1,850,000, which is more than double the average cost in 2020 at $761,106.[11] The 'Energy, Oil and Gas, and Utilities' industry has the highest propensity to pay, at 43%, which is higher than the 2021 year-to-date rate of 32% and the 2020 rate of 26%.[12] The 'Energy, Oil and Gas, and Utilities' industry typically has significant legacy infrastructure that cannot easily be updated, so victims may feel compelled to pay the ransom to enable the continuation of services.

Troublingly, paying the ransom rarely results in full restoration of the impacted data. The average company only restores 65% of its data following a ransom payment.[13] According to a report from ransomware negotiation firm Coveware, in Q4 2020, exfiltration as part of a ransomware attack has increased markedly to 70% of all attacks (up 43% from Q3 2020).[14]

LEGAL IMPLICATIONS OF RANSOMWARE PAYMENT

In addition to the technical woes, legal implications can complicate the payment decision. On the threshold question of whether to pay, the FBI "advocate[s]" against it, in part because payment does not guarantee an organization will regain access to its data. The FBI nonetheless acknowledges "that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers."[15]

Organizations also must be mindful of the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") October 2020 advisory on potential sanctions risks associated with ransomware payments. Key takeaways from this advisory are:[16]

- OFAC has designated "numerous" malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions.
- Under the authority of the International Emergency Economic Powers Act ("IEEPA") and Trading with the Enemy Act, U.S. persons generally are prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List, other blocked persons, and those covered by comprehensive country or region embargoes.
- Any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is prohibited.
- U.S. persons, wherever located, are generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations.
- OFAC can impose civil penalties for sanctions violations based on strict liability.

- OFAC encourages financial institutions and other companies – including those that engage with victims of ransomware attacks – to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.
- OFAC will consider a company's "self-initiated, timely, and complete" report of a ransomware attack to law enforcement to be a "significant mitigating factor" in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.
- OFAC also will consider a company's "full and timely cooperation" with law enforcement both during and after a ransomware attack to be a "significant mitigating factor" when evaluating a possible enforcement outcome.

There are no easy answers to the difficult question of whether to pay threat actors. Companies must balance the potential near-term benefit of decrypting data, which is not always guaranteed, against the risk of legal and reputational exposure for making a payment to a prohibited person or entity—not to mention the risk of increased targeting by threat actors once a payment has been made. Waiting until right-of-boom to assess these issues only will complicate the situation. As OFAC's advisory makes clear, companies should have a plan in place before an attack ever occurs.

RECENT CALLS FOR CYBERSECURITY OVERSIGHT

In April 2021, a broad coalition of experts from industry, government, law enforcement, civil society, cybersecurity insurers, and international organizations formed the Ransomware Task Force ("RTF") and set forth a proposal for a "systemic, global approach" to mitigating the growing ransomware threat. The RTF chairs, including executives from Microsoft, Rapid7, Palo Alto Networks, and the Institute for Security and Technology, published five priorities that they felt were "foundational and urgent":[17]

1. Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.
2. The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House. In the U.S., this must include the establishment of: (i) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; (ii) an internal U.S. Government Joint Ransomware Task Force; and (iii) a collaborative, private industry-led informal Ransomware Threat Focus Hub.
3. Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities, mandate that organizations report ransom payments, and require organizations to consider alternatives before making payments.
4. An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to drive adoption.
5. The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter trading "desks" to comply with existing laws, including Know Your Customer, Anti-Money Laundering, and Combatting Financing of Terrorism laws.

Per news reports, the cybersecurity industry is increasing pressure on the Biden administration to pass an executive order or other guidance for federal agencies and contractors, which the private sector can use as a general guideline. Pressure is also increasing on the Biden administration to use diplomatic pressure to persuade ransomware host countries to deny such threat actors safe havens. Compliance and legal departments should be alert for new guidelines emerging from the administration in the coming months, particularly following this attack.

LATEST PUBLIC INCIDENTS

Recent ransomware attacks include:

- In May 2021, the city of Tulsa reported that it recently had to shut down several internal systems due to a ransomware attack. The outage is expected to last into early next week and residents may experience delays in network services run by the city.
- Earlier this month, a student seeking to pirate a data visualization tool caused a Ryuk-variant ransomware attack at an undisclosed biomedical research institute in Europe, which was doing research work on COVID-19. The institute lost approximately a week of research data due to the incident.
- A major San Diego hospital system suffered a ransomware attack on May 1, 2021. The attack shut down numerous IT resources (including email and the patient records portal), disrupting the hospital's ability to provide healthcare, access medical records, and communicate with patients. The attack temporarily forced doctors, nurses, and other staff to return to using physical charts, and ambulances were routed to other hospital systems as a precautionary measure through May 5, 2021.
- A successful DoppelPaymer-variant ransomware attack against the Illinois Attorney General in early April resulted in stolen internal documents containing Illinois resident information (including Social Security numbers) being posted to the dark web.
- Apple supplier Quanta Computer, Inc. was impacted by a ransomware attack by the REvil ransomware gang in March, which Quanta states did not disrupt business operations. On April 20, 2021, the same day that Apple publicized several new products, REvil announced on their website that they had stolen blueprints of those new products from Quanta during the attack and posted some images appearing to depict plans for a new Apple laptop. During the attack, REvil demanded a $50 million ransom from Quanta.

MITIGATING THE RISKS FROM RANSOMWARE ATTACKS: INCIDENT RESPONSE, COMPLIANCE AND RISKS ASSESSMENTS

The first and most important step is to develop an Incident Response Plan (or "IRP"). An IRP documents the steps of responding to a cyber incident, from first activation of the plan (which should be available to all employees) through final disposal of the incident. The IRP should include: (i) criteria for escalating the incident to higher levels of the business, including the board of directors, based upon incident severity; (ii) procedures for filing a cyber insurance claim; (iii) procedures for activating legal counsel and retaining cyber forensics specialists; (iv) criteria and procedures for contacting the relevant governmental regulators and any other governmental authorities; (v) an activation list and procedures for calling in IT support to restore operations as soon as possible; and (vi) a specific ransomware addendum or playbook. This plan should be regularly tested, including at the board level, through tabletop exercises. Tabletops can help refine the plan and ensure that corporate stakeholders are familiar with their role and important decision points.

Several procedures and compliance measures can help to limit the impact of a ransomware attack, especially the risk of exfiltration of data. One of the best is creating and enforcing a strict retention schedule across the business, which will limit the available data for a ransomware gang to exfiltrate. Another is to maintain a regular, daily backup schedule and store backups in a location entirely unconnected to the corporate network. Regular and protected backups will limit data loss and virtually eliminate the need to pay a ransom. The insertion of data privacy/cybersecurity addenda into vendor contracts can help to limit the impact to a company from an attack at one of its vendors by mandating early notice of a ransomware incident. Organizations also should acquire and maintain an appropriately sized cyber insurance policy to limit potential costs stemming from a ransomware incident. In addition, establishing a network protection strategy based on the principle of defense-in-depth and implementing a “Zero Trust Access Control” architecture will enhance the overall data protection and security posture.

While ransomware presents a significant threat to companies and organizations across industries, a variety of resources are available to assist in risk mitigation efforts. For example, the NIST Special Publication 800-82 (revision 2), entitled, *Guide to Industrial Control (ICS) Security* (May 2015), is an excellent resource for conducting a risk assessment of ICS based systems. *Appendix C* of that publication details known incidents, threat actor capabilities, and ICS vulnerabilities one should evaluate as a component of the risk assessment process. This publication also provides tailored guidance as to suggested security controls based on NIST’s control framework.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our Privacy Notice.

ABU DHABI
ATLANTA
AUSTIN
BRUSSELS
CHARLOTTE
CHICAGO
DUBAI
FRANKFURT
GENEVA
HOUSTON
LONDON
LOS ANGELES
MOSCOW
NEW YORK
NORTHERN VIRGINIA
PARIS
RIYADH
SAN FRANCISCO
SILICON VALLEY
SINGAPORE
TOKYO
WASHINGTON, D.C.

[1] *See* WIRED, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, available at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (visited May 10, 2021).
[2] *See* FBI, *FBI Statement on Compromise of Colonial Pipeline Networks*, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks (May 10, 2021).
[3] RaaC threat actors seek to provide a professional or corporate image compared to Ransomware as a Service (“RaaS”) providers who sell ransomware development kits to third parties.
[4] *See* De Blasi, Stefano, *Darkside: The new ransomware group behind highly targeted attacks,* Digital Shadows, available at https://www.digitalshadows.com/blog-and-research/Darkside-the-new-ransomware-group-behind-highly-targeted-attacks/ (visited May 10, 2021).
[5] See FBI, *Flash Report MU-000146-MW: Indicators of Compromise Associated with Darkside Ransomware* (May 10, 2021).
[6] *See* CrowdStrike, *2021 Global Threat Report*, available at https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf at 20 (April 2021).
[7] *See* CrowdStrike *supra* at 27.
[8] It should be noted that other recent sources report numbers which are significantly higher in both hits and impact. Sophos’s report (dated April of 2020) should be taken as a conservative representation of the threat landscape.
See Sophos Group PLC, *The State of Ransomware 2021*, available at https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf (April 2020).

[9] *See* Coalition, *H1 2020 Cyber Insurance Claims Report*, available at https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf (September 2020).
[10] *See* Sophos Group PLC, *supra* at 12.
[11] *Id. At 3*.
[12] *Id.* at 9-10.
[13] *Id*. at 11.
[14] *See* Coveware, *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*, available at https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 (September 2020).
[15] *See* FBI, *IC3 PSA: High-Impact Ransomware Attacks Threaten U.S. Business and Organizations*, available at https://www.ic3.gov/media/2019/191002.aspx (Oct. 2, 2019).
[16] *See* U.S. Department of Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (Oct. 1, 2020).
[17] *See* Institute for Security + Technology, *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, available at https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf (April 2021).