Harvard Law School Forum on Corporate Governance
SUPPORTED BY pwc

What Companies Need to Know About Modern Ransomware Attacks and How to Respond

Posted by Antonia M. Apps, Adam Fee, and Matthew Laroche, Milbank LLP, on Wednesday, July 14, 2021

Editor's note: Antonia M. Apps and Adam Fee are partners and Matthew Laroche is special counsel at Milbank LLP. This post is based on their Milbank memorandum.

Ransomware is an escalating and evolving cybersecurity threat facing organizations around the world. In 2020, ransomware attacks increased seven-fold by year end, with over 17,000 devices detecting ransomware each day.[1] As an added challenge, ransomware is more sophisticated than ever before with modern variants designed to inflict immense damage and perpetrators demanding higher payouts. In the past few months alone, ransomware has caused catastrophic disruptions to the business activities of, among others, Colonial Pipeline, food processing giant JBS USA Holdings Inc., and Ireland's national health care system.[2] Successful attacks cost businesses millions of dollars, including disruption to business, personnel cost, device cost, network cost, lost opportunity, reputational harm, and a potential payment of a ransom.[3] Cybercriminals are demanding and making more and more money, with the average ransomware payout per event growing from approximately $115,000 in 2018 to more than $300,000 in 2020; and the highest ransom paid more than doubling from $5 million between 2015 and 2019 to $11 million in 2021.[4] Governments, law enforcement, and regulatory bodies have taken notice, with companies facing pressure to effectively prepare for and respond to ransomware attacks.[5]

Given the current threat environment, it is critical that companies seeking to manage their cybersecurity risks have some understanding of how ransomware has evolved to become one of the most damaging cybersecurity threats today. Companies are facing increased legal, regulatory, and political scrutiny in the wake of these attacks, which in turn requires companies to have appropriate management structures and controls in place, with board oversight, in order to anticipate and address the significant harms that can be caused from a ransomware attack. Below we examine the key features of modern ransomware that companies should be

[1] *See* Fortinet, Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs (Feb. 2021), *available at* https://www.fortinet.com/content/dam/maindam/public/02_marketing/08_Report/Global-TLR-2021-2H.pdf.

[2] Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall St. J. (May 19, 2021); Catherine Stupp, *Irish Healthcare System Struggles With Tech Disruptions After May Ransomware Attack*, Wall St. J. (June 18, 2021).

[3] *See* Dep't of Health & Human Serv., Ransomware Trends 2021 at 11 (June 3, 2021), *available at* https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf.

[4] Palo Alto Networks, Ransomware Threat Report at 4 (2021); *see also* Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, Wall St. J. (June 9, 2021).

[5] *See, e.g.*, Press Release, U.S. Senator Jackie Rosen, Rosen Leads Bipartisan Group of Senators to Reintroduce Bipartisan Electric Grid Security Legislation (June 24, 2021); Press Release, Fed. Bureau of Investigation, FBI Statement on Recent Ransomware Attacks (June 4, 2021); Press Release, Dep't of Homeland Security, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021).

considering, including how ransomware actors are now targeting specific companies, threatening to post their victims' most sensitive data online, and collaborating with other cybercriminals to increase the sophistication of attacks. After exploring modern ransomware, we then recommend guidelines for companies responding in the immediate aftermath of an attack so that companies are best positioned to contain the incident, resume normal business operations, and appropriately assess legal and regulatory risks.

Key Features of Modern Ransomware

Ransomware attacks traditionally operated by gaining entry to a system, usually through phishing emails, and then automatically locking or encrypting data by scanning for files with certain extensions. In the past, most ransomware actors used a "spray and pray" or "shotgun" approach in which ransomware was indiscriminately distributed in search of a vulnerable organization. While these opportunistic attacks had several notable successes, by 2018, organizations had largely adapted to the threat by implementing cybersecurity measures and disaster recovery and business continuity plans in response to attacks. As a result, traditional ransomware became less successful and was, for a time, largely overshadowed by other cyberthreats.[6]

In the past 18 months, however, ransomware has roared back to the forefront of the cyberthreat landscape. Modern ransomware attacks are more sophisticated and damaging in several key ways. First, modern ransomware actors frequently use a targeted approach, known as "big-game hunting" or "human-operated attacks," in which the ransomware is tailored for specific victims. Before an attack is even initiated, ransomware actors engage in deep victim profiling.[7] Ransomware actors have become more proficient at doing so for several reasons, including the availability of databases and other tools that help identify victims based on their location, industry, size, and revenue; and anonymous communication platforms that allow for secure interactions and increased collaboration of cybercriminal groups. After identifying a victim and gaining access to their network, ransomware actors spend a substantial amount of time (typically weeks or months) taking over sections of the network before executing the ransomware. By spending more time in the targeted system, cybercriminals are able to move laterally to gain access to more parts of the network, identify the most sensitive data stored by the victim, and infiltrate critical backups making it harder for victims to recover from an attack. With greater access to sensitive data, ransomware actors also have more insight into their victim's financial health, which drives more tailored ransom demands.[8]

Second, in conjunction with the broad access to sensitive data provided by targeted attacks, ransomware actors now employ "double extortion" in which the ransomware not only encrypts the victim's data, but also exfiltrates it from the victim's network. This gives cybercriminals another

[6] Magno Logan, Erika Mendoza, et al., The State of Ransomware: 2020's Catch-22 (Feb. 3, 2021), *available at* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22.

[7] Mayra Fuentes, Feike Hacquebord, et al., Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them at 9 (2021), *available at* https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf.

[8] *Id.* Some ransomware actors include a third layer of extortion by adding denial-of-service ("DDoS") attacks against victim websites, which can overwhelm a network with traffic, causing further disruption of operations. Others have even added a fourth layer of extortion by directly contacting a victim's customers in an effort to increase pressure on the victim to pay. *See* Janus Agcaoili, Miguel Ang, et al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti* (June 15, 2021), *available at* https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

avenue for extortion: if a victim does not pay the ransom, the attacker can publish or threaten to publish the victim's data online, sell the data on the dark web, or use the stolen data to exploit vulnerabilities in related systems. Victims face significant pressure to pay ransoms under those circumstances, which has led to a substantial increase in the amount of both ransom demands and payouts.[9]

Third, modern ransomware attacks are often conducted by multiple groups collaborating on different aspects of the infiltration. One example is the so-called ransomware-as-a-service ("RaaS") subscription model, in which ransomware developers look for affiliates to carry out attacks and in exchange receive a share of the proceeds.[10] In those scenarios, one group owns the ransomware and another group or groups control the compromised infrastructure, which allows cybercriminals to use experts at each stage of the attack. With broader access to a victim network, cybercriminals also have become more effective at monetizing different portions of the compromised assets. For example, ransomware actors might choose to deploy ransomware to one portion of a victim network while selling access to another, thereby creating multiple revenue streams for the same attack.[11] This dynamic also makes it more difficult for victim organizations to assess the duration and scope of the breach and identify all of the perpetrators.

Finally, modern ransomware actors now typically use cryptocurrency as their preferred method of ransom payment. In the past, cybercriminals were forced to use other financial instruments to receive payments—such as mobile phone payment platforms or electronic wallets—that were localized to a particular geographic region and/or regulated by governments. Cryptocurrency, by contrast, bypasses regulations and is capable of transferring money around the globe, allowing cybercriminals to initiate high volume, cross border money transfers anonymously with little risk.

Modern ransomware actors have deployed some or all of the above methods, achieving several recent high profile successes. Notable examples include:

DarkSide: Darkside is one of the most notorious modern ransomware variants and it has wreaked havoc across the globe, infiltrating organizations from various industries in more than 15 countries. Originally introduced in 2020 by a cyberhacker group known as Carbon Spider, Darkside operates as a RaaS and uses a variety of methods to gain initial access to its target system, including through phishing, Remote Desktop Protocol ("RDP") exploitation, and other exploits.[12] Once Darkside infects the victim network, it moves to the domain controller (a server that verifies user credentials on a computer network), where it steals credentials and moves laterally to identify other valuable assets to steal. Before launching the ransomware payload, Darkside exfiltrates critical files, using TOR-based leak sites to host stolen data.[13]

The most notorious Darkside deployment was the May 2021 attack against Colonial Pipeline, a company responsible for nearly half the fuel supply for the U.S. East Coast.[14] Darkside used

[9] *See* Palo Alto Report, *supra* note 4, at 4.

[10] *See* Fuentes et al., *supra* note 7, at 6.

[11] Bob McArdle, The Life Cycle of a Compromised (Cloud) Server, Trend Micro (Sept. 1, 2020), *available at* https://blog.trendmicro.com/the-lifecycle-of-a-compromised-cloud-server.

[12] *See, e.g.*, Cybersecurity Infrastructure & Sec. Agency ("CISA"), Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (May 30, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa21-131a. TOR is a free software that enables anonymous communications over the Internet.

[13] *Id.*

[14] *Id.*

double extortion by locking Colonial Pipeline's computer systems and stealing over 100 gigabytes of corporate data.[15] This attack caused a significant disruption in fuel distribution in the United States, and Colonial Pipeline paid a $4.4 million ransom in bitcoin to regain access to its systems. The Federal Bureau of Investigation subsequently recovered a portion of the ransom by monitoring a publicly visible bitcoin ledger as hackers transferred the bitcoin ransom to other digital ledgers, which are akin to personal digital wallets. When a significant portion of the ransom, about 64 bitcoins, was transferred to a digital address for which the FBI had obtained a "private key" (*i.e.*, the password to access the address), the FBI obtained a search warrant and seized the bitcoin.[16] Other recent Darkside victims span across multiple sectors, including financial services, legal, manufacturing, professional services, retail, and technology.[17]

Nefilim: Nefilim was first identified in March 2020 and has been among the most successful variants in breaching victim networks. Nefilim typically gains initial access to a victim network by exploiting weak credentials on exposed RDP or other related services. Once inside a target network, Nefilim actors download additional administrative tools to facilitate lateral movement in the network. Nefilim then exfiltrates the data, publishes it on TOR-protected websites, and launches the ransomware payload to encrypt the victim's network. In the past year, Nefilim has published approximately two terabytes of stolen data online.[18]

Nefilim has distinguished itself from other ransomware families by targeting companies with annual revenues in the billions of dollars. Nefilim's highest-profile attack was against the Australian shipping organization, Toll Group, in May 2020. Toll Group reportedly refused to pay Nefilim's ransom demands and, as a result, Nefilim leaked sensitive Toll Group data and publicized how Toll Group could be infiltrated in the future.[19] Nefilim also has been identified as the perpetrator in a number of other attacks, including against victims in the United States, South American, Europe, and Asia.

REvil: REvil (also known as Sodinokibi) emerged in 2019 and began targeting various industries in the United States, Australia, Canada, Finland, and Hong Kong. REvil's recent variants generally gain access to victim networks through malicious spam emails, RDP vulnerabilities, and compromised websites. Like Darkside and Nefilim, after gaining access to the victim network, REvil uses double extortion, has a dedicated leak site for publishing sensitive data, and has reportedly attempted to auction stolen data online.[20]

REvil has been identified as the perpetrator of several high-profile ransomware attacks, including (i) the June 2021 attack on Grupo Fluery, a Brazilian medical diagnostic company that performs approximately 75 million clinical exams every year; (ii) the June 2021 attack on food processing firm JBS, which shut down plants that process roughly one-fifth of the United States' meat supply; and (iii) the May 2020 attack on the law firm Grubman Shire Meiselas & Sacks, which allegedly

[15] Jordan Robertson & William Turton, *Colonial Hackers Stole Data Thursday Ahead of Shutdown*, Bloomberg (May 8, 2021), *available at* https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown.

[16] Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021).

[17] Shining a Light on Darkside Ransomware Operations, Fireeye (May 11, 2021), *available at* https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html.

[18] *See* Fuentes et al., *supra* note 7.

[19] Ry Crozier, *Toll Group May Have Lost Over 200GB of Data In Ransomware Attack*, IT News (May 20, 2020).

[20] Phil Muncaster, *REvil Ransomware Group Auctions Stolen Data*, Info Security Group (June 3, 2020), *available at* https://www.infosecurity-magazine.com/news/revil-ransomware-group-auctions.

resulted in the theft of almost one terabyte of sensitive client data.[21] JBS eventually paid REvil $11 million in cryptocurrency to shield JBS from further business disruption, which is the largest publicly reported ransomware payout to date.[22]

Responding to a Modern Ransomware Attack

In light of the recent success of modern ransomware attacks, we fully expect that ransomware will continue to plague industries around the world in the coming years. When an attack occurs, the victim organization must act decisively to contain the incident, and the first 48 hours following the attack are the most critical. During that time, organizations must act expeditiously to assess the attack, isolate affected systems, identify whether data is recoverable through backup files or other methods, and evaluate legal and regulatory risks, of which there are many. An organization that effectively addresses each of those issues will be in the strongest possible position to resume normal operations and determine whether or not to pay the ransom. Considering the sophistication of modern ransomware attacks, we recommend that organizations prioritize the following steps immediately after a breach.

Mobilize Breach Response Team: Organizations should form a team to coordinate the breach response. Ideally, this team had already been identified and prepared long before the breach occurred, and includes senior management, forensics, information security, information technology, and legal components. In light of the complexity of modern ransomware attacks, organizations should consider using independent forensic investigators with ransomware expertise. Organizations also should strongly consider retaining outside counsel to guide them through the incident response under attorney-client privilege, including the legal and regulatory issues discussed below. Moreover, if the organization decides to use independent forensic investigators, those individuals should be retained by outside counsel to maintain legal privilege for their work, including any reports or assessments concerning the breach and how it occurred.

Assess the Damage: Organizations must move as quickly as possible to assess the scope of the attack. This includes identifying the affected computer system or systems, the origin of the attack, the ransomware variant or other malware used to infiltrate the system, and any current external connections to the system. This step is more complicated when responding to a modern ransomware attack because, as described above, the attack may involve multiple cybercriminals who have spent weeks or months moving through the victim's network. Victim organizations should not assume that the identification of malware on one section of their system constitutes the full scope of the breach. Rather, the response team should determine whether that malware has been used as part of a larger targeted ransomware attack. If it was, then the victim organization likely will have other areas of the network to investigate before confirming that it has neutralized the incident.

Preserve Log Files: Log files are critical to assessing the ransomware attack, and organizations should take immediate steps to preserve them. This includes increasing the default size of log files on servers and disabling automated maintenance tasks such as temporary file removal and

[21] Lawrence Abrams, *Healthcare Giant Grupo Fleury Hit By REvil Ransomware Attack*, BleepingComputer (June 23, 2021), available at https://www.bleepingcomputer.com/news/security/healthcare-giant-grupo-fleury-hit-by-revil-ransomware-attack/; Press Release, Fed. Bureau of Investigation, FBI Statement on JBS Cyberattack (June 2, 2021).

[22] *See* Bunge, *supra* note 4.

log rotation to prevent logs from being overwritten. If an affected system does not have logging enabled, the organization should enable logging immediately, which might also yield helpful information in the aftermath of the breach.

<u>Isolate and Image Affected Systems</u>: Once affected systems have been identified, they must be isolated. This process includes not only removing those systems from the network itself, but also securing physical areas potentially related to the breach. Once those systems are isolated, they should also be forensically imaged, which will assist in investigating the origins and causes of the breach. Moreover, if the organization pays the ransomware actor for a decryption key, it is possible that the key might have bugs that can damage the data during the decryption process. If that occurs, the forensic image can be used to try to repeat the decryption without damaging the original data.

<u>Secure Backups Files</u>: Securing backup files as quickly as possible plays a crucial role in quickly resuming business operations. Ideally, at least some backup files are stored on an air gapped network to which the attack did not and could not reach. To the extent the backup files are connected to the infected network, organizations should disconnect backup storage from the network and/or lock down access to backup systems until the infection is resolved. Here, again, organizations must move cautiously because modern ransomware attacks have specifically targeted backup files to purposefully prevent a speedy recovery. Furthermore, because modern ransomware attacks have longer timeframes, organizations should be prepared to identify and retrieve backup files that significantly pre-date when the intrusion was discovered.

<u>Assess Legal and Regulatory Issues</u>: Organizations face a variety of legal and regulatory considerations at the state, federal, and, potentially, international level following a ransomware attack, and many of those issues must be addressed immediately. Depending on the organization and type of compromised data, the ransomware attack might trigger a complex patchwork of legal notification requirements, some of which have short notification turnarounds. For example, states have enacted legislation requiring notification of security breaches involving personal information, some within 24 hours of discovering the theft. Additionally, the SEC has issued guidance concerning disclosures following a cybersecurity breach. And the United Kingdom's General Data Protection Regulation imposes a duty on organizations to report certain personal data breaches within 72 hours, where feasible. U.S. Senators also recently proposed the Cyber Incident Notification Act of 2021 that would require certain companies to report significant "cybersecurity intrusions" to the Department of Homeland Security within 24 hours of discovery.[23]

Organizations also must prepare for government investigations and litigation. Regulated industries such as healthcare, finance, and critical infrastructure regularly face scrutiny after cyber attacks from regulatory authorities and state attorneys general. Where consumer data is involved, private rights of action under state consumer protection laws may lead to class action litigation. Beyond that, organizations must also determine whether or not to pay the ransom, which raises a host of other practical and legal issues. The FBI generally advises companies not to pay ransoms. The Treasury Department's Office of Foreign Assets Control ("OFAC") has stated that some ransomware payments may also constitute violations of economic sanctions laws. Beyond OFAC, paying the ransom may implicate anti-money laundering laws and the Patriot Act.

[23] *See* S. 645, 117th Cong. (2021), *available at* https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/warnerrubiodraftbill.pdf

Moreover, some members of Congress have expressed support for a potential federal law prohibiting ransomware payments, and lawmakers in four states have proposed legislation banning ransomware payments using taxpayer dollars.[24] In New York, lawmakers also have proposed legislation that would ban ransomware payments by any entity conducting business in New York or healthcare facility regulated by the New York Department of Health.[25] As noted, early involvement of legal counsel is important for assessing all of these issues while preserving privilege.

* * *

Given the proliferation of sophisticated ransomware actors seeking ever increasing bounties for sensitive company data, companies should both anticipate and be prepared to respond to the inevitable attack. By taking the steps outlined herein, companies will put themselves in the best position to contain the breach once it happens, prevent additional data loss, begin the recovery process, limit legal and regulatory exposure, and determine whether to pay the ransom.

[24] *See, e.g.*, Doug Olenick, Should Paying Ransoms to Attackers Be Banned, Data Breach (May 24, 2021); Cynthia Brumfield, *Four States Propose Laws to Ban Ransomware Payments*, CSO (June 28, 2021), *available at* https://www.csoonline.com/article/3622888/four-states-propose-laws-to-ban-ransomware-payments.html.

[25] N.Y. S. 6806, 2021-2022 Legislative Sess. (May 18, 2021), *available at* https://www.nysenate.gov/legislation/bills/2021/s6806.