Client Alert: The Ransomware Epidemic

Aon's Cyber Solutions and Stroz Friedberg Incident Response

Ransomware is, by multiple measures, the top cyber threat facing businesses today[1]. Unlike data breach, ransomware is a risk without discretion. Any company that either requires access to critical data, or faces loss or hardship in the event of business interruption is a potential ransomware victim.

The Attack Evolution

In a ransomware attack, threat actors gain unauthorized access to company networks and files using malicious software or malware. After gaining access, these cybercriminals encrypt files making them inaccessible, and demand a ransom payment in cryptocurrency in exchange for the digital key code(s) to decrypt the files. Ransomware attacks have become more advanced in their approach, including pre-emptive measures intended to coerce ransom payment such as targeting and destroying data backups to prevent restoration, and stealing data prior to encryption with the threat of public release. This leaves many victims with the difficult choice of either permanent loss of data and extended business disruption or paying a ransom to regain access and restore operations.

For many ransomware victims, paying the ransom may seem like the only viable option. The possible consequences of business disruption and loss or public exposure of sensitive data are severe, and can include loss of revenue, breached contracts, missed deadlines, failure to meet customer or client expectations, damage to goodwill, or even, in the most extreme examples – such as with healthcare providers – possible loss of life.

The most recent statistics on ransomware are staggering. The total number of global ransomware reports increased by 715.8% from 2019 to 2020[2]. Ransom payments have risen as well, making a 60% leap in payment value since last year[3]. Some of the most sophisticated ransomware attack groups and malware variants are now averaging over $780,000 per payment[4]. At these rates and amounts, it is no surprise that the predicted damages from ransomware are expected to be $20 billion in 2021[5].

The Payment Conundrum

Amid this cyber crisis, law enforcement has remained mostly neutral on the issue of ransom payments. Generally, law enforcement provides cautionary guidance around the risks associated with paying a ransom, warning that either the supplied decryption files may not work, or that the payment of a ransom may attract further exploitation. But, there is also consensus across law enforcement that those experiencing ransomware events are victims[6 7]. Not surprisingly, to date there is scant record of prosecutions, much less convictions, of ransomware victims who have chosen to pay a ransom to recover critical files or restore the operation of critical systems.

Until recently, the difficult decisions facing victimized entities (or those companies participating in incident response activities) was not whether it was a legal risk to pay a ransom. Rather, the primary focus in the ransomware conundrum was whether it made business sense to pay the ransom and, if so, how to both engage with the threat actor to negotiate and navigate the often-unfamiliar cryptocurrency landscape to facilitate payment. Post-payment, the most difficult issue typically facing a victimized entity was the often time-consuming and technically taxing decryption process.

Find out how our cyber security solutions can help you.

Visit **aon.com/cyber-solutions**

or call +1 212.981.6540

Empower Results®

If law enforcement was involved or notified by a victimized entity at any point throughout this process, it was generally in the hope of receiving guidance (based on experience with similar previous attacks) or justice (if law enforcement could identify the ransomware threat actors). While law enforcement remained eager to work with victimized companies, the increase in ransomware attacks forced the selective prioritization of which cases to handle. Those cases that law enforcement could take on were appropriately focused on their mandate of criminal investigation and prosecution. This mandate, combined with the deluge of ransomware matters, ensures that victimized entities that notify and work with law enforcement still handle most aspects of the incident response investigation themselves, including root-cause analysis of the incident, the scope of the intrusion, and restoration of the business.

The "Evil Corp" Effect

The ransomware payment landscape began to change when a sophisticated, Russian-based threat actor group called "Evil Corp" (via some of its known individual members), as well as several other cyber criminals, first appeared on the Treasury Department's Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list. Like other sophisticated threat actors, Evil Corp moved into the easy monetization of ransomware. What separated Evil Corp from many other criminal enterprises, however, was their self-developed, sophisticated malware. Evil Corp's malware was generally thought by the threat intelligence community to be singularly used by Evil Corp, and unshared with other criminal enterprises. Specifically, the effective "WastedLocker" malware variant used in many devastating ransomware attacks is believed by many within the threat intelligence community as belonging solely to Evil Corp.

OFAC SDN diligence had previously focused on whether easily changeable cryptocurrency wallets used to receive ransom payments could be tied to specific threat actor groups that might appear on the OFAC SDN list. Generally, they could not, so very few ransomware payments were impacted by OFAC diligence. But, where WastedLocker malware was part of the ransomware attack, OFAC SDN diligence might conclude the ransom recipient was a blocked person or entity without separately determining that the cryptocurrency wallet used by the attacker to receive the ransom payment was associated with Evil Corp or any other known SDN.

Treasury and Justice Departments' Advisories

Recently, the United States federal government released two significant documents focused on cryptocurrency and the facilitation of ransomware payments. These were likely issued in response to the increasing pressure on law enforcement and the business community by the magnitude of the ransomware epidemic, mounting questions around potential payments to blocked persons or entities, and the need for guidance on pre-payment diligence and collaboration with law enforcement and regulators.

On October 1, 2020, the Department of the Treasury issued an advisory notice related to facilitating ransomware payments. It reminded the public of several important, pre-existing provisions relevant to incident response with respect to a ransomware event.

On October 9, 2020, the Department of Justice issued its Cryptocurrency Enforcement Framework outlining, in part:

- how cryptocurrency technology is currently used and illustrating how malicious actors have misused that technology;
- laws and regulations that exist at the federal level as it relates to cryptocurrency transactions; and
- public safety challenges related to cryptocurrency.

Key takeaways from both advisories include:

- Law enforcement will continue to treat entities affected by ransomware as victims. These advisories signal no intent to the contrary.
- Cryptocurrency has both legitimate and illegitimate uses. Impermissible transfer of funds to entities on the OFAC SDN list – along with money laundering and tax evasion – is specifically identified as an illegitimate use of cryptocurrency.
- Cryptocurrency transactions, whether as part

of a ransom payment or otherwise, may be regulated, including under Financial Crimes Enforcement Network (FinCEN) regulations. However, regulations may vary based on several factors, including the size of the transaction and the source and recipient of payment.

- While considered best practice, neither referenced advisory creates a new requirement that entities must notify law enforcement if victimized by ransomware or in connection with payment of a ransom as part of a ransomware event. This appears to remain within a victim organization's discretion, unless other already existing regulations are implicated. However, in exercising this discretion, companies should consider the benefits of working with law enforcement (and notifying them of payment), including taking advantage of law enforcement experience with threat actor(s) across many incidents and industries.
- OFAC SDN and blocked-jurisdiction diligence must be a critical part of any organization's process prior to making a ransomware payment.
- Should it be determined that a ransom payment will likely be made to an entity on the OFAC SDN list, the Treasury Department's guidance is clear: proceed having been warned. At this point, it would be imprudent to even consider making a ransom payment without first engaging with legal counsel, law enforcement, and relevant government agencies.
- The Treasury Department's advisories appear to tacitly acknowledge that an entity may unknowingly make a ransom payment to an OFAC SDN. If it is later determined that such payment occurred, mitigating factors would likely include the involvement and notification of law enforcement, as well as the existence and quality of the OFAC SDN diligence performed prior to the ransom payment.
- Left unanswered is the most difficult scenario where a ransomware victim performs diligence and determines that the attacker involved is, or is likely, on the OFAC SDN list. In that instance, the victim entity is left with the impossible choice of either making a payment that may be considered unlawful, or unrecoverable systems that could lead to material business injury or demise. In these situations, a victimized entity's best course would be to: (i) engage and work with legal counsel and (ii) notify and work with appropriate law enforcement and regulators. In doing so, there is the possibility the victim entity could mitigate or possibly avoid severe prosecution if it ultimately pays a ransom under duress to an OFAC SDN.

Risk Mitigation Strategies

Ransomware attackers often operate with the same discipline and approach of a traditional business, except in a criminal venture with criminal intent. Threat actors typically choose the path of least resistance to achieve their business goals, attacking vulnerable companies taking advantage of common exploits, or a lack of cyber defense and preparedness. To help mitigate the risk of falling victim to ransomware and in an effort to better prepare for a ransomware incident, consider these eight tips:

1 **Be proactive** – Being victimized by ransomware is a jarring experience. It tests an organization's emotional responses to crisis, escalation procedures, technical prowess, business continuity preparedness, and communication skills, especially because the organization must sometimes interact directly with the attackers. Ensure that the Incident Response (IR) Plan/Playbooks, and/or Business Continuity Plan/Disaster Recovery Plan has been recently assessed, reviewed, and updated. But, most important, these plans and playbooks must be tested through simulated practice across realistic scenarios to help improve resilience.

2 **Educate employees on cyber security and phishing awareness** – Phishing is still a leading cause of unauthorized access to a corporate network, including as the entry point for ransomware attacks. Training users to not only spot a phishing email, but to also report the email to their internal cyber security team is a critical step in detecting the early stages of a ransomware attack. Companies must create a culture where all employees feel responsible for enterprise security, and are encouraged to participate in proactive detection of, and defense against, threats, risks, and attacks. Phishing awareness is a critical cornerstone to such a cyber secure culture.

3 **Employ multi-factor or "two-step" authentication** – Multi-factor authentication (e.g., a password – something employees know, plus an authentication key – something employees have) across all forms of login and access to email, remote desktops, external-facing or cloud-based systems and networks (e.g., payroll, time-tracing, client engagement) should be a requirement for all users. In many—but not all—instances, the presence of multi-factor authentication may even prevent the exploitation of stolen login credentials because the attacker does not also possess the necessary second piece of the login process, the authentication key. It is important to ensure proper multi-factor configuration. Multi-factor access controls can be even more effective if coupled with the use of virtual private network (VPN) interaction.

4 **Keep systems patched and up-to-date** – The rudimentary cyber hygiene activity of system updates and patching often falls by the wayside, especially as operations and security teams are stretched, systems and endpoints age and move towards legacy status, and new systems, hardware, and applications are introduced as businesses grow, mature, merge and divest. There are—and will continue to be—major unpatched vulnerabilities that allow attackers to compromise corporate networks. Attackers can often identify a vulnerable system with a simple scan of the Internet using free tools. They engage in this exercise broadly and indiscriminately, looking for exploitable systems on which to unleash ransomware and other cyber attacks.

5 **Install and properly configure endpoint detection and response tools** – Tools that focus on endpoint detection and response can help decrease the risk of a ransomware attack and are useful as part of incident investigation and response. However, many entities that invest in these tools fail to properly configure them to be of assistance in the event of a cyber event and investigation. Properly configured security tools give a much greater chance of detecting, alerting on, and blocking threat actor behavior.

6 **Design your networks, systems, and backups to reduce the impact of ransomware** – Ensure your privileged accounts are strictly controlled. Segment your network to reduce the spread of adversaries or malware. Have strong logging and alerting in place for better detection and evidence in the event of incident response. Having a technical security strategy that is informed by architects that know the latest attacks and adversary trends is important, as is the use of continuous threat intelligence monitoring in open source and on the dark web.

7 **Consider risk transfer options** – Because a ransomware attack can threaten an entity's reputation and goodwill, the complete risk of ransomware can never be fully mitigated or transferred. However, in practicing ransomware preparedness, organizations should consider obtaining appropriate cyber insurance coverage. In doing so, organizations should review how coverage addresses indemnification for financial loss, business interruption, fees and expenses associated with the ransom and incident response, as well as considerations for service providers, such as the ability to work with incident response providers of choice.

8 **Pre-arrange your third-party response team** – An effective ransomware response will often include all or some third-party expertise across the disciplines of forensic incident response, legal counsel, crisis communications and ransom negotiation and payment. Seeking out, vetting and engaging with these professionals during a ransomware incident places additional burden on an already strained enterprise, and is ineffective and inefficient when every second counts and every decision is critical. As time is of the essence, it is critical to pre-vet and pre-engage a team of professionals to monitor and be ready to respond to a ransomware attack when it happens.

Contacts:

Chad Pinson
President of DFIR, Engagement Management, and Investigations
Stroz Friedberg
+1.214.377.4553
chad.pinson@strozfriedberg.com

Jonathan Rajewski
Vice President, Digital Forensics and Incident Response
Stroz Friedberg
+1.802.238.8530
jonathan.rajewski@strozfriedberg.com

Stephanie Snyder
SVP, Commercial Strategy Leader
Aon's Cyber Solutions
+1.312.381.5078
stephanie.snyder@aon.com

Sources

1. **Ransomware Is the No. 1 Cyber Threat This Year. Here's What You Can Do.**
2. **Bitdefender's Mid-Year Threat Landscape Report 2020**, page 14
3. **Coveware Ransomware Marketplace Report**, August 3, 2020
4. **Coveware**, January 23, 2020
5. Cyber Security Ventures, **https://www.thesslstore.com/blog/ransomware-statistics/**
6. **FBI Ransomware Prevention and Response for CISOs**
7. **Obama PPD-30**

About Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

This client alert is not legal advice. Neither Aon's Cyber Solutions, nor Stroz Friedberg Incident Response engages in the practice of law. Should you need legal advice or legal services related to ransomware or a ransomware incident, we encourage you to engage with your in-house counsel or outside legal counsel.

AON
Empower Results®