wiley

ALERT

Ransomware Payment Lessons Amid DOJ Recovery Success

September 27, 2022

This article was originally published in Law360.

With mounting government and private sector concern about ransomware attacks, the FBI and U.S. Department of Justice continue to publicly acknowledge more frequent success in recovering ransom payments made to hacking groups.

These successes provide lessons for private organizations that may be considering what they will do if faced with a ransomware attack and asking whether they should work with law enforcement.

In a recent publicly reported successful recovery,[1] an FBI and DOJ investigation led to the seizure of $500,000 in funds that had been paid by various victims to a North Korean hacking group. There, hackers used a ransomware strain, dubbed Maui, to encrypt data and servers of, among others, a medical center in Kansas.

According to the DOJ press release on this effort, after being unable to access its encrypted computers and equipment for over a week, the Kansas hospital paid approximately $100,000 in bitcoin to the threat actors.

The government's seizure of $500,000, which included the $100,000 paid by the hospital, is the latest in a string of acknowledged successes, with the FBI last year clawing back $2.3 million in bitcoin paid to the DarkSide ransomware group, as well as another $6.1 million paid by software vendor Kaseya to a ransomware group using Sodinokibi/REvil code.

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Privacy, Cyber & Data Governance

As discussed below, law enforcement's successes are a result of novel investigative techniques, interagency coordination and international cooperation to track down the crypto wallets into which ransom payments have been paid.

It is also a testament to significant cooperation by victim companies, which the DOJ lauded in its release.

Ultimately, this success gives companies additional data to help them consider how best to partner with law enforcement in a breach, and in weighing whether to pay a ransom demand.

Ransomware Attacks Are Prevalent, and Government Continues to Warn of Effects While Taking Aggressive Action

Ransomware attacks continue to increase in prevalence and are affecting companies in nearly every sector of the economy. In addition to their increasing frequency, the sophistication of attacks is creating heightened risks, with artificial intelligence, for example, allowing more efficient and targeted attacks.

Ransomware as a service is making it easier to conduct illegal operations, and the financial incentives remain skewed toward attackers. The resulting increase in attacks is unsurprising, particularly because the monetary payments are large and, until recently, threat actors rarely suffered repercussions.

Government agencies have been sounding the alarm about ransomware risks and readiness, offering tools to prepare, such as the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency's cybersecurity evaluation tool,[2] and guidance for managing an attack, such as the Ransomware Response Checklist from a joint CISA and Multi-State Information Sharing and Analysis Center Ransomware Guide.

The government also renders assistance in the midst of an attack. Our experience confirms that field agents and analysts at FBI, CISA and other agencies will endeavor to be helpful and seek information to assist the government in their ongoing investigations.

Sometimes those investigations will include attempts to interrupt bad actors' work or recover ransom payments.

Historically, law enforcement had limited success in recovering bitcoin ransom payments paid to hackers. This is due in large part to the anonymous nature of crypto wallets, which are known for being difficult to link to any particular person.

In order for law enforcement to successfully recover payments using crypto, several pieces have to fall in place. For example, the FBI and DOJ need cooperation from the victim company, legal process that helps trace the funds whereabouts, and interagency or international cooperation with the seizure of funds.

Each step can be a substantial hurdle, with many companies reluctant to notify law enforcement — although this may be shifting, with the government strongly encouraging public-private sharing and coordination.[3]

As discussed below, there are many reasons why a company may not notify law enforcement, including wanting to avoid the burden of yet another stakeholder among many mandatory and prudential reporting obligations.

As incident reporting obligations proliferate, companies may be reluctant to work with federal law enforcement outside of the mandatory channels, or they may find that the involvement of the FBI is helpful in managing follow-up inquiries from other agencies, customers and the public.

Recent Law Enforcement Efforts Are Bearing Fruit

Law enforcement is having more success in recovering crypto payments made to hacking groups. As noted at the outset, law enforcement's most recent publicly noted success came in recovering $500,000 from a North Korean hacking group.

This success is due in large part to a more aggressive effort by law enforcement to disrupt cyber threats, deploy novel techniques, and coordinate their actions with domestic as well as international partners.

It also depended on the voluntary cooperation of a victim. As the DOJ's release noted,

> [b]ecause the Kansas medical center notified the FBI and cooperated with law enforcement, the FBI was able to identify the never-before-seen North Korean ransomware and trace the cryptocurrency to China-based money launderers.

In order to facilitate these recoveries, law enforcement has to take several steps that involve coordinating with both private and governmental partners. In a typical case, we see the following challenges.

First, law enforcement has to locate both the crypto wallet containing the assets, as well as the corresponding private key. Generally, threat actors provide companies with a specific crypto wallet address for the company to deposit the ransom payment. If law enforcement is provided this address, using legal process they can then try to locate the crypto exchange that actually hosts the wallet.

Once law enforcement has found which exchange hosts the crypto wallet and obtained the private key, law enforcement can apply for a Federal Rule of Criminal Procedure 41 seizure warrant and seize the bitcoin paid as ransom in the wallet.

Notably, this tends to apply only to so-called hot wallets, which are those that are connected to the internet 24/7, whose private keys are stored on a cloud and which are in the possession of the exchange hosting the wallet.

This is in contrast to cold wallets, which are specially designed offline devices — typically a USB drive or an external hard drive — that are not hosted by an exchange and need to be connected to a PC to carry out transactions.

In other words, subpoenaing an exchange for information on a cold wallet would be a fruitless effort, leaving law enforcement with few options for tracking down the owners of cold wallets.

Crypto exchanges oftentimes comply with anti-money laundering policies and know your customer rules. This can help law enforcement. These laws impose certain user information collection requirements on financial institutions, which many cyber exchanges comply with.

Such information can be used to criminally charge responsible individuals. This has led to some notable domestic and international criminal prosecutions, with the person responsible for the breach of Kaseya recently extradited from Poland.[4]

Companies Have a Lot to Consider Before Seeking Ransom Recovery

Many companies do not presently face mandatory incident reporting requirements, though Congress has directed DHS to create mandatory reporting about ransomware payments by critical infrastructure companies in the Cyber Incident Reporting for Critical Infrastructure Act. Until those rules are developed, working with law enforcement remains largely voluntary.

Voluntary notification can be a tough decision, but is often the prudent course in a ransomware event. But even where a victim company decides to notify law enforcement of an attack and to seek assistance on attribution or forensics, a company still may not want law enforcement to attempt to recover the ransom payment.

One consideration is whether the company's data was exfiltrated by the threat actor. When a hacking group successfully exfiltrates some or all of a company's data, the company may pay a ransom payment in order for a threat actor to purportedly delete their data.

However, aside from the threat actor's representation that it deleted the company's exfiltrated data, a victim company oftentimes does not have any absolute guarantee that a threat actor did, in fact, delete its data.

This lack of guarantee is an important factor for companies to consider when deciding whether to authorize law enforcement to attempt a recovery of the ransom payment.

In other words, if law enforcement successfully recovers the ransom payment, the threat actor could very well not have deleted the company's data and could still publish the stolen data. And, even if the threat actor actually did delete the stolen data, the company risks the threat actor attempting to retarget the company.

There are instances, however, where law enforcement attempting to recover a ransom payment makes sense for a company. For example, cyberattacks where a company's data was not exfiltrated may present a reasonable instance for a company to authorize law enforcement to attempt to recover a ransom payment — with the major caveat that a company should be confident the threat actor no longer has access to its systems.

Ultimately, these are only a few of the many factors that companies must consider when weighing whether trying to recover a ransom payment makes sense in their situation.[5]

Conclusion

Law enforcement continues to gain traction in the fight against cyber criminals. This includes increased success in recovering ransom payments. This success gives companies an additional factor to consider when deciding whether and how to engage with law enforcement after experiencing a breach, whether to pay a ransom demand, and whether to try to recover the payment.

[1] https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors.

[2] https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr.

[3] Perspectives From the Public and Private Sectors on Information Sharing During COVID-19, Vincent Pitaro, Cybersecurity Law Report (June 24, 2020), https://www.cslawreport.com/7022886/perspectives-from-the-public-and-private-sectors-on-information-sharing-during-covid19.thtml.

[4] https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas.

[5] One particularly important consideration is whether a company's insurance policy includes coverage for ransom payments.