Tracking and combatting an evolving danger: Ransomware extortion

accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

Cyber Defense

December 15, 2020

Share

Ransomware gangs have intensified their impact by attempting, and often succeeding, in stealing data to coerce payments. The onset of the COVID-19 pandemic offered a catalyst for this tactic with its accompanying weakened organizational security and increased levels of fear and anxiety among workers—key conditions for successful extortion attempts. As a result we are seeing more companies being targeted with various new extortion techniques and ransomware gangs are accumulating large profits.

How have ransomware extortion tactics evolved?

In the second half of 2020, Accenture Cyber Threat Intelligence has observed ransomware groups attempting to ratchet up pressure on victims to pay ransoms by increasing service disruptions, and reputational damage. At the same time, some groups are also attempting

to build trust with their victims, by setting out a framework of “principles” they adhere to, or providing a set of “guarantees”, to increase the chances ransoms will be paid.

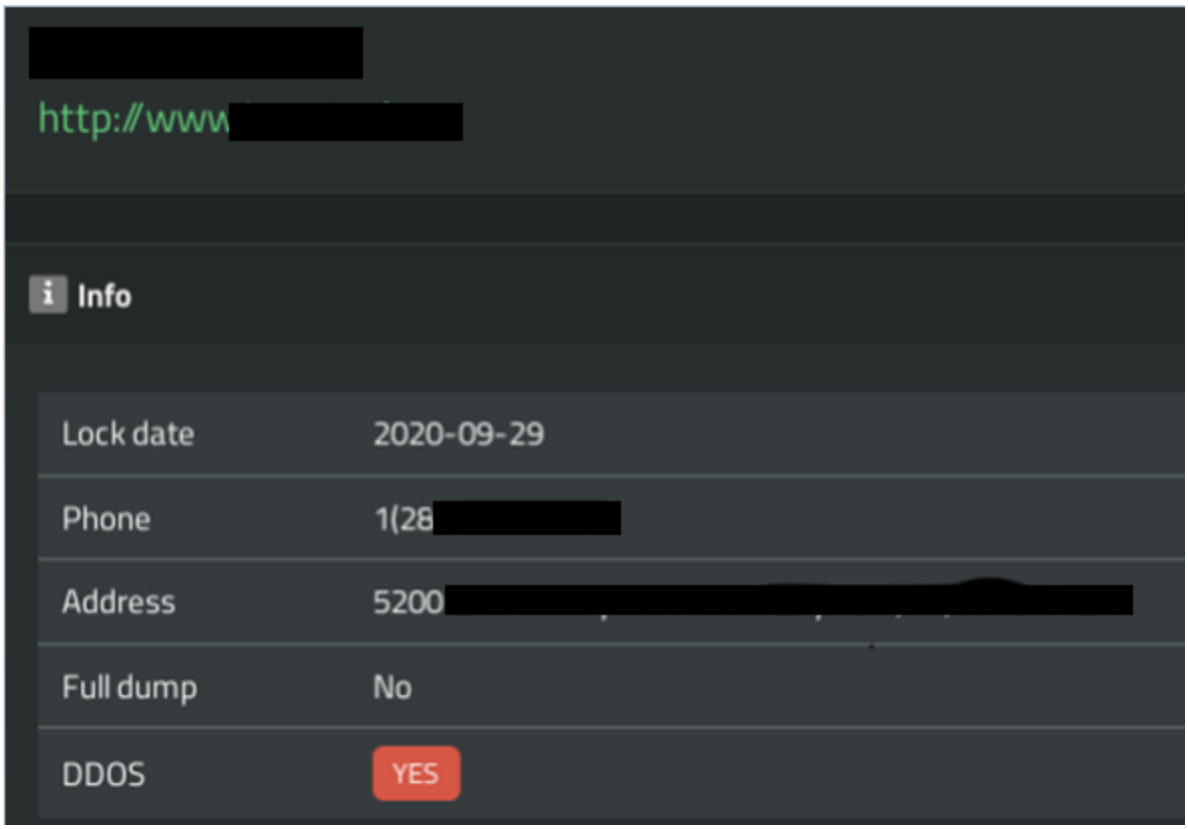
Trend 1: Expanded service disruption

The principal impact of a ransomware attack has always been service disruption. When its network or a portion is ‘held hostage,’ an organisation faces pressure to acquiesce to ransom demands in the hope of restoring operations. The good news is that many organisations are now more effective at defending against and recovering from the ransomware itself. Unfortunately, threat actors are also upping their game.

Tactic: DDOS attacks

A concerning new tactic is the addition of distributed denial of service (DDOS) attacks to ransomware and data theft attempts. On their ‘name and shame’ website, the ransomware group **SunCrypt** specifies whether it launched a DDOS attack against a victim, as shown in the image below.

<<< Start >>>



<<< End >>>

SunCrypt often deploys a DDOS attack when ransom payment negotiations stall. For organizations already suffering a service disruption due to the ransomware, a DDOS attack may exacerbate the disruption and complicate mitigation. This is particularly troublesome

for organisations in industries where any extended downtime can be very damaging, such as healthcare, logistics, and financial services.

The Accenture Cyber Threat Intelligence (ACTI) team expects other ransomware gangs will adopt this tactic in the near future.

How to protect against DDOS attacks

ACTI suggests organizations:

- Establish strong working relationships with their internet service providers while also preparing a coordinated approach to DDOS attacks.
- Deploy appropriate technology to recognize the signs of a DDOS attack early.
- Prepare and test Incident Response playbooks and DDOS mitigation plans.

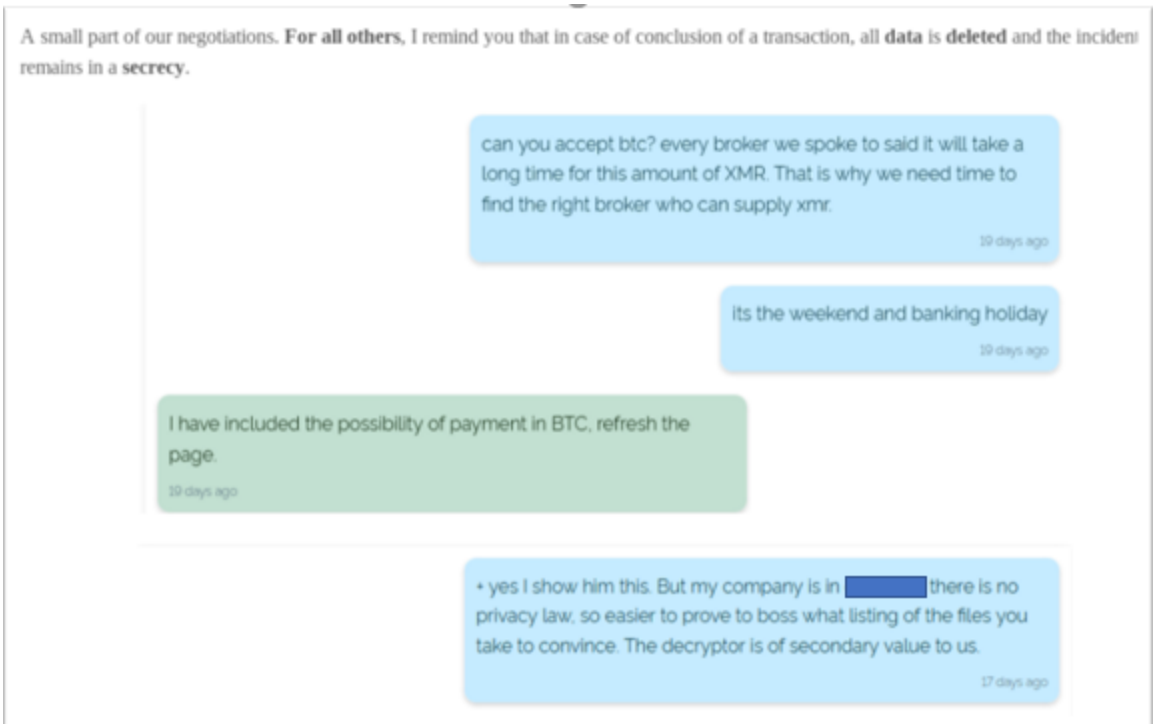
Trend 2: Increased reputation damage

Ransomware gangs are becoming increasingly effective at exposing successful attacks to the public to elicit payment. To pressure victims to pay, particularly those that succeed in minimizing the service disruption, groups usually first threaten to damage the reputation of the victim and, if that does not succeed, start releasing sensitive information. Publicly exposing information may lead a victim's customer base to believe the victim is lying about the compromise, has poor network security, or could still be compromised—all of which can lead to long-term reputational damage for the victim.

Tactic: Retaliating against companies that deny or withhold information about a breach

This past October, **REvil** (a.k.a. Sodinokibi) ransomware operators noticed that one of its targets had notified its clients that it was unable to verify claims of data theft. In retaliation, REvil published screenshots of negotiations with the company to refute that statement:

<<< Start >>>



<<< End >>>

Nefilim ransomware operators use their blog “Corporate Leaks” to release victims' data in increments. In September, the media reported on a victim of a yet-unattributed cyber attack, which included a quote from a security professional associated with the victim. The quote suggested there was no evidence of access or theft of data. In response, in an October blog post, Nefilim pasted the quote and uploaded several files purportedly belonging to the victim, along with the statement:

"It seems that the security advisors do not know how to do their job or they were asked by [COMPANY NAME REDACTED] to lie for them. [COMPANY NAME REDACTED] knew that the breach has happened and received proof of the breach.

This confirms ransomware gangs follow news coverage on their victims and will discredit them by publishing and responding to victim statements.

In September, a **SunCrypt** ransomware victim issued a brief statement on its company's website (since removed) titled “[COMPANY NAME REDACTED] repels cyber attack.” The statement said the “incident is under further investigation, but at present there are no indications that information has been stolen.” SunCrypt operators copied the statement to their victim blog and uploaded screenshots and a file of data allegedly stolen from the victim.

Tactic: Use of mainstream platforms to increase pressure

An actor associated with **REvil** carried out an-in depth interview with a Russian security researcher in October. Uploaded to YouTube, the video showed the actor alluding to an attack on a major game developer, to pressure it into paying.

In November, **Ragnar Locker** ransomware operators used a hacked Facebook account to release an advertisement that stated one of their victims had falsely claimed no data had been stolen. They then issued a deadline for the victim to pay. Although the advertisement was not seen by a wide audience before it was blocked by Facebook, the media picked up on it and spread the message further.

Tactic: Press releases

Maze was the frontrunner of the 'press release' strategy to call out uncompliant targets. They have since retired, but their apparent successor – **Egregor** – gives out a "Hole of the Month Award" to reveal the organization with the biggest "gap in security practices." In October, two companies received the award, which included details on how the companies left sensitive information unprotected – passwords, source code, unencrypted chats, and contracts. They concluded the press release with a statement indicating the group maintains access to the targeted company's network: "*P.S. Everyone who is going to use the products of that companies soon, try to think about the possible backdoors from Egregor Team*."

Darkside and **SunCrypt** ransomware also have a dedicated Press Release section on their website.

Mitigation

To protect against reputational damage, ACTI suggests organizations:

- Implement a clear media strategy to convey information about a cyber security incident.
- Exercise caution when releasing statements denying the extent of any attack until the full details are known as attackers will expose any miscommunications or falsehoods.

<<< Start >>>

<<< End >>>

Trend 3: Increased attack costs

Data theft and exposure is now firmly front and center in the arsenal of most ransomware gangs' extortion tactics, which can increase the cost of the attack. Attackers are extorting higher ransoms and eliciting prompt victim payment by taking advantage of data breach regulations such as the European Union's General Data Protection Regulation (GDPR) or US state legislation requiring those suffering a data breach to notify relevant stakeholders. Data breach victims can face stiff fines for violating such rules. Added to this is the personal cost to the individuals exposed in the breach: Threat actors often seek out insurance policies, credit card data, passports, personal emails and more, to expose them on their website.

Tactic: Exposing increasingly personal and sensitive information

In October, the **REvil** blog posted a page that contained the last will and testament of the company owner of one of its victims, and threatened to publish passport information on the owner's family. In addition they posted the company's entire insurance policy which included a "Cyber Extortion Loss" coverage limit of $5 million. This imitates a LockBit ransomware affiliate that emailed a victim's stolen cyber insurance policy to security researchers for reporting purposes and to extort the victim.

In the same month, for a **REvil** victim in the office equipment industry, the actors searched the stolen data for the word "bank" and published a screenshot of its findings. The group was likely looking for bank account numbers or other lucrative financial information.

<<< Start >>>

<<< End >>>

Mitigation

To protect against theft and exposure of data, ACTI suggests organizations:

- Incorporate strict handling policies for personal identifiable information (PII) and ensure minimal personal sensitive data is stored on corporate networks.
- Take steps to secure networks against data theft: keeping software up to date, carrying out regular risk assessments, encrypting and backing up data and training staff on best practices.

Trend 4: Facilitating ransom payment to resolve a breach

In stark contrast to the above trends, some gangs are attempting to set themselves apart as trustworthy, charitable and easy to do business with, in order to encourage ransom payment cooperation. These gangs will streamline the payment and decryption process and publicly state their ‘ethical’ business model, which supposedly translates to less chance of media coverage, less downtime and no data exposure.

Tactic: The ‘nice guy’ approach

Ragnar Locker ransomware operators provide clear instructions on how to pay and use their decryptor, and provide the 'Ragnar_Locker Team Guarantee':

<<< Start >>>

After the deal would be successfully closed and payment is received, Ragnar_Locker Team Guarantee:

- Delete all the downloaded information from our servers.
- Delete all temporary posts\sites\pages and etc. related to this case
- Delete all backdoors, if ones still exists
- Never attack again using existed vulnerabilities or if new one appears, but to notify if we find any new vulnerability in future
- Not to attack with DDOS or any other type of attacks
- Not to share the details of conversation and\or personal data, with any third-parties
- Provide a list of recommendations to improve security measures
- Provide Decryption software along with manual and support if needed

<<< End >>>

The guarantee touches upon malicious extortion techniques employed by other gangs: posting conversations (REvil), leaving backdoors (Egregor) and launching DDoS attacks (SunCrypt). They also claim to identify and address other vulnerabilities to reduce their victim's chance of suffering a future ransomware attack.

The **Darkside** ransomware operators donated funds to two legitimate non-profit charities in October to demonstrate 'altruistic' behavior. Additionally, on their website, they include 'assurances' that they have pre-determined the ransom amount a victim can afford to pay and that they promise not to attack hospitals, schools, non-profits or governments:

<<< Start >>>

Based on our principles, we will not attack the following targets:

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

<<< End >>>

Mitigation

ACTI acknowledges that the ransom payment debate is complicated. Victims must weigh the pros and cons of ransom payment with the pressure to quickly resolve the network disruption. Despite attempting to appear principled, threat actors are not always true to their word. Ransomware gangs have said they will not attack hospitals, but have then attacked a hospital. They have promised to delete stolen data that subsequently appeared on dark web forums.

ACTI suggests following the guidance contained within Accenture Security's 30 November blog Securing your business and the world from ransomware. This highlights the need to follow advice contained within the US government advisory related to ransom payments. ACTI also stresses the importance of having a clear post-breach strategy in place to lessen the impact of these extortion techniques if an attack occurs. This includes comprehensive incident response playbooks, business continuity and disaster recovery plans, and implementing a clear media strategy.
Our ACTI team provides actionable and relevant threat intelligence to support decision makers. The intelligence analysis and assessments in this report are grounded in verified facts; more information on this activity is available to subscription customers on ACTI IntelGraph. IntelGraph is a proprietary next generation security intelligence platform that allows users to search, visualize, and contextualize the relationships between malicious actors, their tools and the vulnerabilities they exploit.

Paul Mansfield is a senior analyst in Accenture CTI Reconnaissance Team, which produces actionable intelligence and tracking threat actors operating in both open and closed communities.

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture help organizations protect their valuable assets, end-to-end. With services that include strategy and risk management, cyber defence, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

Paul Mansfield

Cyber Threat Intelligence Analyst

Paul is a lead analyst on Accenture’s iDefense Reconnaissance Team, producing actionable intelligence and tracking threat actors.

Follow me: