DARKReading

Edge Articles

5/26/2020
04:00 PM

Nicole Ferraro
Edge Articles

0 COMMENTS
COMMENT NOW

Tweet

How to Pay a Ransom: A Step-By-Step Guide for Something You'd *Never* Do

Even prior to the COVID-19 pandemic, ransomware attacks were on the rise and becoming more expensive. Now your, um, friend's organization has fallen victim and is going to pay. Here's how they should handle it.

(Image: logo3in1 via Adobe Stock)

It's Tuesday morning. You arrive at your desk (in the living room) and, oh no ... bad news.

Not only is your cat asleep on your keyboard again, but when you try logging onto your network, a message on the screen confirms the worst: Your organization has been hit with ransomware. Making matters even worse, your backups are running, shall we say, just a *tad* behind.

Cue internal screaming. (Your spouse is on a Zoom call a few feet away, so you have to be quiet.)

Seriously, though. As an infosec professional, what do you do now?

Ransomware attacks have been on the rise. This was true even before the COVID-19 pandemic forced workers to go home, sending a myriad of new vulnerable connections online. According to data supplied to The New York Times by security firm Emsisoft, 205,280 organizations submitted files that were hacked in a ransomware attack in 2019 — a 41% increase year-over-year.

They're also getting more expensive: Q1 data reported by cybersecurity firm Coveware shows average ransom payments increasing 33% from last quarter, to $111,605.

While you may not envision a scenario where your company would give in to paying ransom, it's happening more often as organizations weigh the risks and benefits and find they have no choice.

So say this is your reality. Dark Reading spoke to several cybersecurity experts to map out the step-by-step process of paying ransom and what you must know to complete the process.

Step 1: Assess the Situation
Once you've been hacked with ransomware, you need to take fast action.

The first thing you want to know, says Jeff Horne, CSO of cybersecurity company Ordr, is whether the ransomware is propagating through your network – and then stop it from doing so by using detection and response (XDR) or incident response tools.

After you've done all you can to isolate and get your machines off the infected network, the next step is to find out what you're dealing with, Horne says. For that, just conduct a simple search for the specific ransomware on Google to see what kind it is and "subsequently, is there a decryptor available so I don't have to pay that ransom at all?" he says.

It's possible to find the key yourself, Horne says, as there are sometimes instances of programmatic errors in ransomware code whereby the key gets exposed before the files are locked. Other times the same key gets used across attacks. That means one victim who pays the ransom enables everyone else to decrypt.

But let's say you can't easily find a decryption key on Google, and you don't have internal backup processes in place that allow you to recover everything on your own. What do you do now?

This is when your organization needs to make critical decisions about whether paying the ransom is worth it.

"I've had an evolving position on complying with extortion demands," says Charles Carmakal, SVP and strategic services CTO at cybersecurity firm Mandiant. "[There are] a lot of different variables you'll want to look at in order to pay."

Variables include everything from whether your network being compromised could have a material impact on human life (for example, city services, hospitals, etc.) to whether your organization can afford to lose the infected data.

Step 2: Enlist Outside Help
Assuming you have ruled out your preferred options of finding decryption keys loose on the Internet, recovering your networks through sophisticated backup solutions, or just considering the data lost, it's time to start communicating with your attacker.

If your company has internal security expertise and a full supply of cryptocurrency at hand, then this may be a task you can handle without outside help.

If that's not the case, Mandiant's Carmakal recommends enlisting third-party providers that specialize in resolving ransomware attacks. These organizations possess insights into the credibility of threat actors and the chances they will cooperate if paid, he says. Furthermore, they have bitcoins in reserve, making it a faster process to pay the ransom than if you sought to purchase cryptocurrencies on your own.

Step 3: Test the Decryption Codes

But recovering from a ransomware attack is not as simple as surrendering bitcoins and getting your network back. The back-and-forth process between you/your third-party firm and the threat actor involves a series of communications via email where there's usually a testing process that goes on to decrypt a sample of your network to prove they really have the keys.

"Some will stay on the phone with you while you test the decryption key. Once you've verified it works, they hang up," said Christopher Kuhl, CISO and CTO at Dayton Children's Hospital, speaking of his experience in roles prior to joining the hospital, where he has not seen any ransomware attacks. "What's crazy is that a lot of ransomware operators, the larger ones, have their own call center. People there are incredibly nice and friendly. They recognize what they're doing is wrong."

However, smaller ransomware operators, or those that just want to get their bitcoins and get away, will send the decryption key and close their email accounts, he adds.

Side Note: Don't Try to Negotiate

While it may be tempting (particularly if the call center people are kind), both Kuhl and Horne agree that it's neither worth it nor in your best interest to negotiate on the ransom sum.

"The prices that either I've seen or other people have seen have been non-negotiable. So we've never tried," Kuhl says.

"You're dealing with an anonymous party," Horne adds. "You have literally no leverage. If I were a ransomware operator and you came to me and said, 'Instead of paying me $1,000, you're going to pay $500,' well, now you owe me $20,000."

Step 4: Decrypting the Network

Once the sample has been successfully tested, the ransom amount paid, some tears shed, and the decryption key received, the rest is hardly smooth sailing.

"Decrypting is not a trivial process. It could take days, weeks, over a month," Carmakal says. "Some organizations choose to pay the threat actor and decrypt in parallel on different systems as they're recovering systems through backups."

Those that pay "are paying to accelerate the recovery process," he adds.

Plus, paying the ransom doesn't necessarily mean you'll actually get the decryption key or that it will work. Threat actors have been known to collect their bitcoins and provide fake decryption keys or keys to unlock only part of the network if more than one type of ransomware was used.

And in instances where older ransomware is being used that operators have since abandoned, paying means you are "throwing money into a bucket no one's monitoring anymore," Horne says. "At the end of the day, those operators are not operating the backend anymore, not exchanging keys, so there's less than a 50% chance of ever getting your data back."

How to Avoid This Mess at All Costs

Paying a ransom is, overall, a losing game, with organizations often having no choice but to shell out cash for access to networks they may never be able to really recover.

A better option is to be proactive, which means effectively convincing leadership that they'd rather invest in security now than pay later.

Kuhl says he's had success convincing business leaders of this at Dayton Children's Hospital.

"We've convinced them that [ransomware] is an enterprise risk, that it impacts patient safety, financial vitality, and that we need the proper tools and training to decrease the amount of time from prevention to detection," he says.

Ordr's Horne adds that the only way out of this is to ensure a proper backup is in place that would diminish the harm a ransomware attack could do to your organization.

"A robust backup, like an offline N+1 backup strategy, is absolutely critical for organizations," he says. "Organizations that have been hit by ransomware that had robust backup strategies don't care if they're hit by ransomware. Backup with redundancy, and offline backup specifically, is the way you defeat this ultimately."

Related Content:

- The Entertainment Biz Is Changing, but the Cybersecurity Script Is One We've Read Before
- This Is Not Your Father's Ransomware
- Ransomware, Data Breach Follow Phishing Attack at Magellan Health
- Maze Ransomware Operators Step Up Their Game
- How Cybersecurity Incident Response Programs Work (and Why Some Don't)
- Latest Security News & Commentary about COVID-19

Learn from industry experts in a setting that is conducive to interaction and conversation about how to prepare for that "really bad day" in cybersecurity. Click for** more information and to register**.

Nicole Ferraro is a freelance writer, editor and storyteller based in New York City. She has worked across b2b and consumer tech media for over a decade, formerly as editor-in-chief of Internet Evolution and UBM's Future Cities; and as editorial director at The Webby Awards. ... View Full Bio

Recommended Reading:

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts

SASE: The Right Framework for Today's Distributed Enterprises

Managing a Hybrid Cloud Infrastructure

MORE WEBCASTS

White Papers

Threat Reconnaissance Lessons from the Private Sector for Federal & State Agencies

2021 Application Security Statistics Report Vol.2

MORE WHITE PAPERS

Reports

Building an Effective Cybersecurity Incident Response Team

2021 Top Enterprise IT Trends - Network Computing

MORE REPORTS

Copyright © 2021 UBM Electronics, A UBM company, All rights reserved. Privacy Policy | Terms of Service