WHITEPAPER

Redmond MAGAZINE

PREVENTING AND MITIGATING RANSOMWARE INFECTIONS

KnowBe4
Human error. Conquered.

www.knowbe4.com

Editor's note: *Two hikers in the woods looked behind them and saw a bear loping towards them. The first hiker, sat down, pulled off his hiking boots and put on running shoes. "You think you can outrun the bear?" the second hiker asked. The first hiker, already on his feet and taking off, called back: "I don't have to outrun the bear. I just have to outrun you."*

Faced with increasing threats from highly organized crime syndicates purveying ransomware, IT professionals cannot be sure that any antivirus solution will save their mission critical data. With cyber criminals using sophisticated social engineering to target naïve end users with emails that appear to be legitimate business communications. A human resources representative clicking on what appears to be a resume can set off a ransomware attack that cripples your business, says Stu Sjouwerman, founder and CEO of KnowBe4, Inc. Once the bad guys have locked up your data, you may have no other choice than to pay the ransom for a decryption key.

The ransomware landscape is not a pretty picture and Sjouwerman expects it to get darker in 2017. He suggests that the first line of defense may not be antivirus software on endpoints but ransomware awareness by the end users. If IT can make their end users less susceptible to the increasingly cunning social engineering email schemes, they may be able to harden their business from attack and send the cybercriminals off in search of softer targets.

In a one-hour discussion with Mike Crowley, principal consultant at Baseline Technologies, Sjouwerman, an expert in security solutions, who is working on the frontlines in the cyber wars, covered four main topics that IT professionals need to be aware of if they want to make their organization a hard target:

1. The Business of Ransomware
2. Patient Zero: Social Engineering
3. Nuts and Bolts: What can IT Do?
4. Thought Leadership: Unmet Needs in the Market?

THE FIRST COMMERCIAL INDUSTRY STRENGTH **RANSOMWARE PLATFORM WAS CRYPTOLOCKER.**

THE BUSINESS OF RANSOMWARE

The first commercial industry strength ransomware platform was CryptoLocker, spread via email that targeted Microsoft Windows machines in September 2013. It is believed to have made its creator as much as $23 million in four months.

"That woke everyone up to the underground economy of cybercrime," Sjouwerman explains. "And from that point forward it's been an arms race. Several cyber mafias are furiously competing for market share with different families of Ransomware and that's how it started. Ransomware itself is more than twenty years old, but 2013 is when it hit the big time."

"YOU'RE TALKING **VERY WELL ESTABLISHED, DEEPLY ENTRENCHED CRIMINAL ORGANIZATIONS** WHERE YOU SEE PEOPLE MAKING LITERALLY **A BILLION DOLLARS A YEAR**."

While there still may be the proverbial hacker working out of a basement apartment, or a few cyber crooks plying the ransomware trade and taking in several thousand dollars a month, the big threat is coming from organized crime syndicates running ransomware as a business.

"You're talking very well established, deeply entrenched criminal organizations where you see people making literally a billion dollars a year," Sjouwerman says.

This is organized crime that while it may be based in Eastern Europe, is organized like a Silicon Valley software company.

"They have six or seven different disciplines," Sjouwerman explains. "First, people who hack into websites, then other teams that put exploit kits on there, and third teams that create databases, and a fourth team that are social engineering experts, a fifth team that does the actual phishing. And then there is the customer support that does negotiations and helps people decrypt their files. You're really talking billion dollar businesses, with hundreds of employees."

PATIENT ZERO: SOCIAL ENGINEERING

Like any other software company, the ransomware organizations thrive on innovation both in software and in tactics. The new wrinkle in cybercrime is the use of social engineering to produce the click bait that entices an end user to unknowingly launch a ransomware attack at the place where they work. Emails are deceptively designed to appear as if coming from the CFO, or a co-worker, or a friend or relative. It may look a little odd. Maybe the company name or logo isn't quite right. But the social engineering experts at Ransomware Limited may have identified patient zero, an employee who tends to click on email attachments and links without paying much attention. Web surfing on the job can also lead an end user into a trap. Perhaps an attractive looking pop up appears that draws the user into

clicking on a link that launches ransomware. Once the impulsive or naïve end user clicks on the bait, the attack is on and things go bad quickly.

"Encryption happens in a flash," Sjouwerman warns. "Within ten seconds the network is no longer able to function."

The ransomware quickly moves through the company network encrypting files and locking up databases. Next comes the demand from the criminal customer service department for payment of ransom, which usually needs to be in the form of Bitcoin because it is generally anonymous, easy to launder and hard for law enforcement to trace.

THE RANSOMWARE **QUICKLY MOVES** THROUGH THE COMPANY NETWORK **ENCRYPTING FILES AND LOCKING UP DATABASES**.

If you want to avoid having a patient zero in your company, tell end users to NOT:

- Open suspicious files from strangers
- Open odd emails from people you know
- Open attachments you did not ask for
- Give out personal or business information
- Share your username or password

NUTS AND BOLTS: WHAT CAN IT DO?

Contrary to the message from advocates of antivirus software, Sjouwerman does not put much faith in technology as a silver bullet for stopping ransomware attacks. His recommendation, based on hard earned experience with clients who have suffered ransomware attacks, is to harden yourself as a target by doing the basics:

- Backups, backups, backups
- Religiously patch your OS and apps
- Get a secure email gateway that does URL filtering
- Train end users to avoid ransomware traps

Sjouwerman recommends using software that simulates a companywide phishing attack, what he terms "a baseline test" to gauge users' susceptibility and raise awareness.

"With that baseline you see, oh, 23 percent of my users clicked on this link," he explains. "Well, that's actually a crisis you can use to your advantage. That's a catalyst. You then announce company-wide: Hey, we did a test and twenty-three percent clicked. We really have to do something about this."

That kicks off a 12-month online training program. In Sjouwerman's experience, the once-a-year practice of herding employees into the break room, keeping them awake with coffee and donuts while exposing them to "death by PowerPoint" is not

effective for more than five days. On-going, on-demand online training works better.

"Then you send them frequent simulated phishing attacks to keep them on their toes with security top of mind and it really works," he says.

get the key. They need to contact their command and control server."

IT also needs to have policies and procedures in place in case despite taking every precaution, including having an up-to-the-minute "weapons grade backup," the company is hit with a ransomware attack.

FURTHER SECURITY NEEDS TO BE IN PLACE FOR END USERS WHO HANDLE **SENSITIVE INFORMATION** SUCH AS **FINANCIALS, CLIENT DATA,** AND **HUMAN RESOURCES FILES**.

While IT can publish the results of the test companywide showing the percentage of end users who clicked on the link or attachment during the simulated phishing attack, and can also provide percentages by department, Sjouwerman discourages singling out individual employees. That may cause bad feelings and be counterproductive to the goal of getting end users battle ready for ransomware attacks.

Further security needs to be in place for end users who handle sensitive information such as financials, client data, and human resources files. Sjouwerman recommends enforcing dual or multi-factor authentication. Make sure your policies and procedures are up to date, particularly for financial transactions.

"Check your firewall configuration and make sure that no criminal traffic is allowed out," Sjouwerman says, "because that's how these ransomware infections

"If you have a ransomware infection you just wipe those machines and reimage them from bare metal," Sjouwerman says. "There's a funny expression, nuke from orbit, because you want to make sure that no root kit was left behind."

THOUGHT LEADERSHIP: UNMET NEEDS IN THE MARKET?

If all else fails and you are hit with a ransomware attack and your data is encrypted and you can't recover it any other way, you may have to make a business decision to pay the ransom.

"Obviously, this is a matter of ultimately your business decision," Sjouwerman says. "Am I going to pay the bad guys to get my files back? Well, if it's a thousand bucks to get your files back or three weeks of work lost, most businessmen will say: Okay, I'll pay the ransom and see how it goes."

Based on his experience, sometimes the business executive has to make a pragmatic decision rather than taking the moral high road.

"It is ultimately just math," Sjouwerman says. "How much down time are we going to have when we restore a petabyte of files? Is that three days-worth of down time? How much is that going to cost for 68 people sitting on their hands or pay a thousand bucks or fifteen hundred bucks in Bitcoin and be back up and running tomorrow morning. Those are relatively easy decisions. This is why ransomware is a billion dollar business model.

RANSOMS MAY VARY AND SOMETIMES NOT IN A GOOD WAY, BUT **THEY ARE ALSO NEGOTIABLE.**

"The moment you find yourself with a sufficient amount of files encrypted, it's a math function and no one is going to say, Oh, well, I'll just eat three weeks of lost files because on principle I am not paying criminals. You're in business to make money. We've seen dozens of people do this and we know there are tens of thousands of people who have done this, because of the money that was made."

In his experience, even police departments that were hit with ransomware attacks have paid the ransom when their existing backup strategy didn't work. There is risk involved in paying the ransom. It's possible you were hit by some small time hacker who got Ransomware as a Service (it does exist) but doesn't actually have the decryption key or for whatever reason doesn't provide it after he's collected your Bitcoin payment. However, if you've been hit by a large ransomware gang, their customer service department may be able to reassure you.

"More modern strains have a demo where they decrypt one or two files, for free," Sjouwerman says. "Can you believe it?"

Since the ransom will probably have to be paid in Bitcoin, part of being prepared may include setting up a Bitcoin wallet. Based on his experience helping clients pay the ransom, the founder of KnowBe4 says it can take up to four days to get a Bitcoin wallet. He notes that some companies set up a wallet with a nominal amount of money in it, so they have it in their back pocket if they want to quickly pay the crooks off and get their files back.

Ransoms may vary and sometimes not in a good way, but they are also negotiable. Sjouwerman relates the story of a small medical center, KnowBe4 helped with negotiations.

KNOWBE4 HAS DEVELOPED **A RANSOMWARE SIMULATOR, RANSIM,** THAT IS A **FREE DOWNLOADABLE TOOL**.

"They had two hundred and fifty machines," he recalls. "All were encrypted in one fell swoop."

At first, the medical center was told they needed to pay 26 Bitcoins to get their files back. So they paid it and the bad guys came back and said, "Oh, that was a mistake, it was one hundred and twenty-six Bitcoin."

"Now you're talking real money," Sjouwerman says. "Ultimately, they negotiated it down to about sixty-five Bitcoin, but that's the kind of money you might ultimately wind up with. So, having a wallet in place might not be a bad idea."

FIND OUT WHERE YOU ARE WITH RANSIM

KnowBe4 has developed a Ransomware Simulator, RanSim, that is a free downloadable tool from https://www.knowbe4.com/ransomware-simulator RanSim gives you a quick look at the effectiveness of your existing network protection by simulating 10 ransomware infection scenarios that will show you if a workstation is vulnerable to infection. Here's how RanSim works:

- 100% harmless simulation of a real ransomware infection
- Does not use any of your own files
- Just download the install and run it
- Results in a few minutes

"People test their antivirus and see if their antivirus is blocking ten different scenarios of ransomware infections and the results are not good," Sjouwerman said. "I'm expressing myself mildly. I would recommend going to the KnowB4 website and downloading the free RanSim and then see what you need to do."