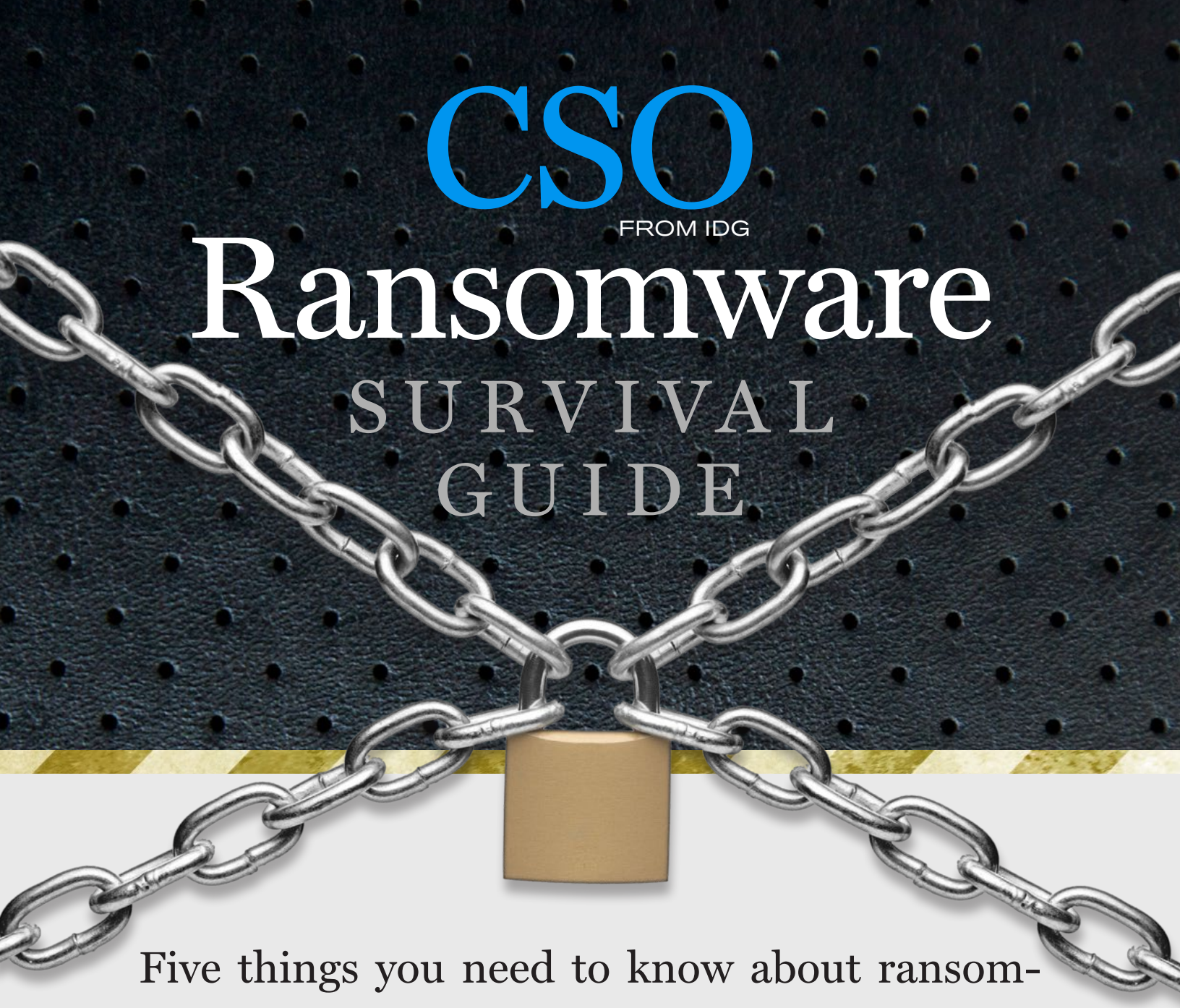


CSO
FROM IDG

Ransomware SURVIVAL GUIDE

Five things you need to know about ransomware | *Why ransomware should haunt you all the time* | **You've been hit with ransomware. Now what?** | Q&A: Responding to ransomware the right way | *A Blue Team's reference guide to dealing with ransomware* | **6 things your users need to know**

sponsored by

KnowBe4
Human error. Conquered.

Ransomware reckoning

Hardly a week goes by without ransomware making news. New variants defeat decryption tools; new decryption tools defeat those variants.

Fingers are pointed: At users, at overburdened, underfunded security staff, at companies that pay (or don't pay) the ransom.

As Lucian Constantin puts it in the lead story in this collection, "there's no end in sight."

What's a smart company to do?

This guide will help you understand and minimize the risk, offer best practices for preventing attacks, and give you strategies for responding after criminals have encrypted your machines.

CONTENTS

Five things you need to know about ransomware

Ransomware has become a real scourge for consumers, businesses and even government institutions. Unfortunately, there's no end in sight, so here's what you should know.

BY LUCIAN CONSTANTIN

Over the past few years, millions of PCs from around the world have been locked or had their files encrypted by malicious programs designed to extort money from users. Collectively known as ransomware, these malicious applications have become a real scourge for consumers, businesses and even government institutions. Unfortunately, there's no end in sight, so here's what you should know.

1. It's not just your PC that's at risk

Most ransomware programs target computers running Windows, as it's the most popular operating system. However, ransomware applications for Android have also been around for a while, and recently, several variants that infect Linux servers have been discovered.

Security researchers have also shown that ransomware programs can be easily created for Mac OS X and even for smart TVs, so these and others devices are likely to be targeted in the future, especially as the competition for victims increases among ransomware creators.

2. Law enforcement actions are few and far between

There have been some successful collaborations between law enforcement and private security companies to disrupt ransomware campaigns in the past. The most prominent case was Operation Tovar, which took over the Gameover ZeuS botnet in 2014 and recovered the encryption keys for CryptoLocker, a notorious ransomware program distributed by the botnet.

In most cases, however, law enforcement agencies are powerless in the face of ransomware, especially the variants that hide their command-and-control servers on the Tor anonymity network. This is reflected in the multiple cases of government agencies, police departments and hospitals that were affected by ransomware and decided to pay criminals to recover their files. An FBI official admitted at an event in October 2015 that in many cases the agency advises victims to pay the ransom if they don't have backups and there are no other alternatives.

3. Back up, back up, back up

Many users back up their sensitive data, but do it to an external hard drive that's always connected to their computer or to a network share. That's a mistake, because when a ransomware program infects a computer, it enumerates all accessible drives and network shares, so it will encrypt the files hosted in those locations too.

The best practice is to use what some people call the 3-2-1 rule: at least three copies of the data, stored in two different formats, with at least one of the copies stored off-site or offline.

4. You might get lucky, but don't count on it

Sometimes ransomware creators make mistakes in implementing their encryption algorithms, resulting in vulnerabilities that allow the recovery of the files without paying the ransom. There have been several cases where security companies were able to create free decryption tools for particular versions of ransomware programs. These are temporary solutions though, as most ransomware developers will quickly fix their errors and push out new versions.

There are other situations where security researchers take control of command-and-control servers used by the ransomware authors and make the decryption keys available to users for free. Unfortunately these cases are even rarer than vulnerabilities in the ransomware programs themselves.

Most security vendors discourage paying the ransom, because there's no guarantee that the attackers will provide the decryption key and because it ultimately encourages them.

If you decide to hold your ground, keep a copy of the affected files as you never know what might happen in the future. However, if those files are critical to your business and their recovery is time sensitive, there's little you can do other than pay up and hope that the criminals keep their word.

5. Prevention is best

Ransomware programs get distributed in a variety of ways, most commonly through malicious email attachments, Word documents with macro code and Web-based exploits launched from compromised websites or malicious advertisements. Many are also installed by other malware programs.

As such, following the most common security best practices is critical. Always keep the software on your computer up to date, especially the OS, browser and browser plug-ins like Flash Player, Adobe Reader, Java and Silverlight. Never enable the execution of macros in documents, unless you have verified their senders and have confirmed with them that the documents should contain such code. Carefully scrutinize emails, especially those that contain attachments, regardless of who appears to have sent them. Finally, perform your day-to day activities from a limited user account, not from an administrative one, and run an up-to-date antivirus program.

Why ransomware should haunt you all the time

The problem is much more complex than whether or not to just pay the ransom.

BY TIM GREENE

When the ransomware demands come in it's really too late to come up with a good response plan, so do that as soon as you can, an Interop audience was told.

"You need to decide beforehand whether you will pay and under what circumstances," John Pironti, president of IP Architects, says. "It's a cost benefit decision in the end."

But in the heat of the moment what should be a rational business decision becomes an emotional issue that challenges the morals and pride of decision makers. "They don't want to be the ones that paid," Pironti says, speaking from experience consulting with ransomware victims. It just feels wrong to cave in to the demands of criminals who have encrypted your machines and won't turn over the keys until you pay.

Ultimately those who make the decision must act in the best interest of the company. That means deciding when not paying the cost of the ransom is worth the consequences: lost productivity, missed customer engagements and the cost of replacing devices that are irreversibly encrypted. "At what point does it cost more to respond to the incident than to pay the ransom?" he says. Businesses need a response playbook.

One company Pironti dealt with was being threatened with a crippling DDoS attack if they didn't pay $9,000. Rather than do so they spent more than $200,000 on DDoS protection gear and consultants to ward off the attack. And then the attack never came.

When it comes time to pay, try to negotiate down the demand. Earlier this year extortionists demanded $3.6 million from Hollywood Presbyterian Medical Center to unlock ransomware. They wound up paying $17,000.

In some cases the negotiations don't even go through a human being, he says. Automated responses sometimes accept lower amounts, and the keys are delivered also automatically once payments — typically in Bitcoin — are made.

Beyond deciding to pay or not to pay, businesses should do threat and vulnerability analyses to identify how adversaries could get in, what they could infect and what the business impact would be.

Planning is also important because the timeframe for making a decision can be narrow depending on the time limit set by the extortionist.

Once paid, getting the network back to normal is no simple matter. Businesses need to do forensics to see how the attack unfolded so measures can be taken to block the same type of attack in the future. That's because attackers sell lists of businesses that have paid ransom and what methods the attackers used against them so those who buy the lists can use the same attack tool again and again. "They only work as hard as they have to," Pironti says. So it may create a long-term problem to pay.

Businesses also need to find out where the attackers went within the network to discover where they might have buried malware for use at a later time, he says. Often the ransomware

attack is used as a distraction so network security pros don't notice other types of attacks.

One of the best protections against ransomware attacks is effective backup, but it's not foolproof. For example, if it is inserted in machines and lies dormant the ransomware itself can be backed up, so machines restored with the backup will still be infected. That's why forensics are important to determine when and where the malware was placed. And it's important to reimage machines, not just restore data.

"You have to ask did your backups backup everything? Do so recently enough? Do they have integrity?" he says.

If there is a bright side, ransomware extortionists generally do what they say they will do. If the victim pays up, they'll send the keys to unlock the encryption.

The problem isn't likely to go away anytime soon. Over time, these attacks are getting more sophisticated and difficult to prevent. When security researchers reverse engineer a strain of ransomware to find out how to disarm it, the criminals quickly abandon it and come up with something else.

The FBI suspects that in the first quarter of 2016 $209 million was collected by ransomware crooks. Pironti says the figure is likely much higher, and so the problem will continue.

"The only way we know to break the cycle is to refuse to pay," he says, but that option may come at a high cost. "Are you willing to become the sacrificial lamb?"

You've been hit with ransomware. Now what?

When their data has been stolen, and is being held hostage, companies are increasingly caving in to cybercriminal demands for payment. Short of paying up, the best defense is a good offense.

BY JONATHAN HASSELL

Imagine waking up to an urgent 5 a.m. call: Something has taken over your corporate network and encrypted all of your data, and supposedly the only way to get it all back is to pay a significant sum to an anonymous third party using Bitcoin. While that scene might sound like something out of Hollywood, it is actually very real — and it's exactly what several variants of ransomware are doing to organizations around the globe.

Two recent appearances of ransomware in the news demonstrate that it is a problem that is growing in both volume and significance, as larger and larger organizations, some critical to public and social services, are impacted by an outbreak:

- The BBC reports that the Chino Valley Medical Center and Desert Valley hospital, in the state of California, were infected with ransomware. A spokesman for the owner of the medical center, Prime Healthcare Services, confirmed that there were some "significant disruptions of [the medical center's] hospital systems."
- In a recent high-profile case, the Hollywood Presbyterian Medical Center declared an internal emergency after suffering on outbreak of ransomware. Ultimately, this hospital decided to ante up the required Bitcoin ransom payment, handing over $17,000 in order to get access to its computers. The original ransom demand was for $3.7 million in Bitcoins, so if nothing else, that is some decent negotiating on the part of the hospital.
- A Kentucky medical center, Methodist Hospital, was recently infected by a ransomware attack. This time, the strain of the ransomware was confirmed: Locky, a newer variant of Cryptolocker, infiltrated the defenses of the medical center's network and spread to the entire internal network as well as several other systems, according to the CNBC report. At the time of this writing, the ransom demand was for $1,600 for this particular hospital, and it was unclear if the hospital intended on paying the ransom. Another report in Ars Technica quotes the hospital's attorney: "I think it's our position that we're not going to pay it unless we absolutely have to."

This stuff is insidious. Ransomware typically comes in as an email attachment, purporting to be an invoice or a shipment tracking document or something else seemingly innocuous. Once open, ransomware typically silently begins encrypting all of the files it can, without any user interaction or notification. It is only once its dastardly deed is done that it prompts the user with information about how much the ransom is, how to pay it and more.

It used to be that the first versions of Cryptolocker were not smart enough to go after data on network drives and only inflicted unwanted

encryption on files stored locally to a machine. This could still be paralyzing in some instances, but for medium to large businesses who stored the majority of their data on network shared drives and SANs or NASes, this provided a level of relief.

That is sadly not the case anymore, because as the virus has grown more successful and more profitable to the writers, most of the ransomware variants can now traverse network drives and UNC paths, encrypting anything that they can actually touch and access with the level of permissions granted to the user account under which the malware is executing. The results, as you can tell from recent news reports about ransomware, can wreak havoc.

Strategies for dealing with ransomware

There are two basic solutions to the ransomware problem, one simple and one that will probably tear your team apart during the implementation. (Technically, there are three, but I don't count actually paying the ransom as a solution because there are no blanket immunities offered in paying the ransom and surely the price will continue to increase as attacks and infestations become more successful.)

Regular and consistent backups along with tested and verified restores. The only way not to feel held hostage because of a ransomware attack is to have the next best viable alternative — to not pay it, because you have full and recent backups of all of your data that have also been tested through consistent, regular restore procedures to make sure that the backups actually worked.

Then, along with vigilant monitoring (many technologists report success with using file monitoring screening to detect large numbers of files being changed in sequence, especially if those files have not been touched otherwise in a while) and ensuring you have appropriate file and folder permissions set, you can simply detect an outbreak quickly and then restore any encrypted data from your backups.

Application whitelisting. Essentially the only way to definitively protect against a ransomware attack and invasion — or any other malware infestation for that matter — from even taking hold is to implement application whitelisting. Whitelisting involves computing checksums and other "digital fingerprints" for applications that you deem permitted to run on your systems, and then basically cutting everything else out and disallowing the code from executing at all.

Sounds great, right? No exploits can run if they are not already whitelisted, so not only does this approach protect you from current threats, but it also acts as a prophylactic for future malware as well — even though you would still do well to have edge and endpoint security, having a known good list of applications and then black-holing everything else would be a significant step up in security.

But therein lies the rub: If you took the superset of all of the regularly used applications you have by all of your users as well as their varying versions and patch levels, you might very well have thousands of programs — and to use the built-in software whitelisting functions within Windows, you would need to create a signature for all of them. Every single one of them. There are various automated solutions available, but they all have a cost for the licensing as well as the administration time.

Finally, with whitelisting, there's the user acceptance factor: your users won't be able to download anything, including browser plugins, which you have not already allowed in advance. This includes even the most minor programs like PuTTY for secure shell tunneling over the internet using SSH, popular with your IT staff, or something like Notepad+, a great text editor many knowledge workers like to download to enhance quick notetaking. (Both of those programs are single executable files with no installation required and are portable between systems, meaning that they often find their way

onto thumb drives or USB storage devices and are shared freely among coworkers.)

Are you and your IT team up for the massive effort not only to establish the initial set of whitelisted definitions but also to continually maintain them, even as new patches change digital signatures, new employees request new programs, and additional services come online? It would truly be a massive undertaking, but I call it the nuclear option simply because it is the most straightforward (not easiest; but most plainly simple) way of all but eliminating the threat of ransomware on your systems.

Q&A: Responding to ransomware the right way

Rob Gresham, Sr. Consultant with the Foundstone Services DFIR team, a part of Intel Security, explains the evolution of ransomware and shares insights into smarter ways to prepare and respond

BY MICHAEL SANTARCANGELO

You get the call you've been dreading. No, not a breach. The other call. That despite best efforts and good intentions, ransomware has locked up critical servers. And now the attackers are demanding you pay them in bitcoin if you want the information back.

What do you do?

Sure. It sounds simple. We don't negotiate. We don't pay.

Is that the right answer? Are we giving people good advice?

Turns out the answer is a bit nuanced. Getting us up to speed is Rob Gresham, Sr. Consultant with the Foundstone Services DFIR team, a part of Intel Security. Rob also serves in the National Guard. He brings vendor agnostic experience in dealing with advanced adversaries techniques, tactics and procedures. Which is why he leads the Threat Intelligence program for Foundstone Services team.

When I brought the concept of ransomware up, Rob quickly brought me up to speed. Now it's my turn to share our conversation with you.

You mentioned that ransomware is evolving. It's more of a business now. How so?

Gresham: With over $445 billion in losses to consumers, Cybercrime is a big business. Like all business though, initial rollouts of ransomware didn't live up to expectations, so criminals are innovating. Would you continue to pay for a product if it never delivered on those expectations?

If the criminals want the extortion to work, they have to deliver the goods. Otherwise, caveat emptor right? Additional issues apply to takedowns, where the authorities took down the sites, but the customers didn't get the keys or products to get their data back. Some companies have helped in this area when taking part of the takedowns and created decryption tools to help consumers.

Innovation in cybercrime is must. As we learn the techniques, we protect our customers. For example, first versions of cryptolocker didn't take into account Windows Volume Shadow Copy services. So customers could just right click their data and rollback. Criminals innovated to turn off the service prior to encrypting. Now it is a standard process. If the ransomware is of a static build, then we find creative ways to block it consistently. Criminals innovate and use malware techniques to create polymorphic ransomware. Very much like supply and demand, criminals are creating SaaS solutions and selling them in the dark corners of the Internet.

We always told people not to pay. We cautioned them it was akin to negotiating with terrorists. Has this advice changed? Should companies pay?

Gresham: It is still extortion/blackmail and I

personally tell customers not to pay. However, the authorities have said differently. It boils down to motivations. If we keep paying, the market keeps innovating ways to keep us paying. However, if nobody paid, criminals would have to find something else to make money. For me, the advice hasn't changed. What has changed is the acceptance of risk and cost to recover. We are choosing the easy way and for some it may be the only way if they didn't have a good business continuity plan (BCP) and tested it. This way you know what your real losses are and you choose the moral right over easy wrong.

But it doesn't always work that cleanly. Some customers get attacked and vital company information is compromised. They don't have a solid BCP in place. With no way to recover the information, I can't honestly tell them *not* to pay.

In most cases, it is a business risk transaction on a ROI cost equation. Compare the cost of the ransom to recover data versus the loss of time (which might include new business), actual business loss, reputational damage, and the like. The hope is that payment results in data restored with no loss. Not so much because of the shady criminal element, but because the programs are designed by people, and sometimes the decryption process doesn't always work as well as we'd like.

There is an upside: payment changes the legal dynamic. It starts a money trail, which helps authorities prosecute, eventually. There are a lot of skilled investigators who know how to follow the money either virtually or physically.

Do the companies who pay get their data back? How does that work?

Gresham: I like to explain to leadership teams like this: when you leave on vacation, I come to your house and change all the locks and board up all the windows. I leave a note on the front door with ransom instructions on how to get back into your house. If you pay, I drop the keys off. If a week goes by and you don't pay, I burn your house down.

You may have to break a few things to get back in and stop the fire. Some customers pay, there are others that don't. They understand the cost when it comes to their business user's data and most are quick to share the pain thru the data loss. At least that's how it used to be.

More criminals use tactics that convince consumers to pay and pay now. Getting ransomware to critical business data by using their externally compromised resources to deploy and spread ransomware to critical internal systems. This innovating change in tactics is frightening. Before, it was a phishing attack, local to phished customer and could compromise shared data, but server infections were rare.

Either scenario creates additional issues. Take what happens, a malware dropper is implanted on the system or external exploit is used deliver the encryptor payload and export the encryption keys. Both require you to clean up the systems after the files are recovered.

Otherwise, what stops them from doing it again?

After paying the ransom, they have more work to do? What does that involve?

Gresham: Customer have to determine the initial infection point and time of infection. They still should call incident response processes into play and ensure they don't get blackmailed again. Traditionally, extortionists keep coming back until the money is gone.

You need to ensure the integrity of your business environment. That means determining systemic cause and root cause OR it will happen again. Frequently, we have arrived at a customer site for them to tell us it has happened multiple times. Why doesn't our software fix the issue!?!? Then we have to explain why you don't get mugged every time you go to the store. Crime is opportunity and location and both have to be in the criminal's advantage. How does that happen on the Internet? Unrated websites, dark web connections, vulnerabilities, and phishing opportunity (awareness).

What can security leaders do to better prepare against ransomware?

Gresham: Customers need to have a business continuity plan. This includes tested backups, alternate processes to get work done. Those organizations in high risk natural disaster areas usually do. Yet, we find they don't regularly test their backups. Customers need to keep their patches and antivirus signatures up to date, which reduces their attack surfaces. It may not help if you are one of the first in a new variant, but it ensures you aren't the last and learn from others' mistakes. Avoid being the first through monitoring, hygiene, and awareness.

Monitoring doesn't require fancy tools. Take notice when 'protected' processes are being 'attacked' by another process. This usually signals some type of malware. Ransomware wants to shut off the antivirus services, so it hits those files quickly, usually within the first hour.

Monitoring for these types of events makes a difference. Catch the event within the hour, remove it from the network, and shut it down. Done right, it stops the ransomware and future loss of data. Most everyone watches server uptime and availability. How hard is it to have a malware event timeline? Adjust what you look for to get ahead.

Hygiene and awareness are harder to implement. Just as you learned or gained experience to avoid certain areas at night with no friends or lights. You walk fast, no eye contact and get to a populous as quick as possible. To improve hygiene and awareness, communicate more. Share the stories. Engage them in conversation. Let people know what you're doing to protect yourself and your organization. Show them simple things they can do, too. And make sure they know your door is open for them to come to you with concerns.

The incident response process makes the difference in organizations. Those who choose to monitor and *ACT* are the ones that don't have to pay criminals. All others have to choose between the cost and risk of paying or losing their information.

A Blue Team's reference guide to dealing with ransomware

Ransomware is a known threat in IT/InfoSec, but sometimes it's good to be reminded of the defenses that can be marshaled against it.

BY STEVE RAGAN

Ransomware has been around since 2013, but it was the success of CryptoLocker that spawned a booming market for criminals.

The effect of ransomware has been felt by organizations both large and small; each of them well aware of the risks associated with this type of malware. Some even had what they assumed, were solid defenses against this type of attack — but their assumptions were wrong.

Most ransomware victims have a shared connection — they lacked some essential security basics, and that's what this article will address.

Daniel Tharp, a government IT manager in New Mexico, published a blog post on ransomware that's worth further examination.

In it, he addresses the topic of ransomware as something that's here to stay and hammers home some essential practices that administrators can use to help defend their networks and users from the threat.

"The trouble with ransomware right now is that it behaves like a standard application. It doesn't require local administrator privileges, it doesn't care if UAC is on, and most of them make use of the standard Windows API for encryption, which you can't disable without really messing up a workstation. So if we can't control the behaviors, we have to make do for controlling the vectors," Tharp told me in an interview.

For example, there's a great Office ADMX template for disabling macros. The template kills the non-executable variants of ransomware that are starting to gain in popularity among criminals. One of the reasons such variants exist is because they load directly into RAM and bypass most restriction policies.

Tharp's post lists a number of other protective steps; we've reproduced a few of them below.

- **Avoid mapping your drives and hide your network shares.** WNetOpenEnum() will not enumerate hidden shares. This is as simple as appending a $ to your share name.
- **Work from the principle of least permission.** Very few organizations need a share whereby the Everyone group has Full Control. Delegate write access only where it's needed, don't allow them to change ownership of files unless it's a must.
- **Be vigilant and aggressive in blocking file extensions via email.** If you're not blocking .js, .wsf, or scanning the contents of .zip files, you're not done. Consider screening ZIP files outright. Consider if you can abolish .doc and .rtf in favor of .docx which cannot contain macros.
- **Install the old CryptoLocker Software Restriction Policies** which will block some rootkit-based malware from working effectively. You can create a similar rule for %LocalAppData%*.exe and %LocalAppData%**.exe as well. It was pointed out in the Reddit comments, that if it's at all feasible, run on a whitelist approach instead of a blacklist. It's more time-intensive but much safer.

- **Backups.** Having good, working, versionable, cold-store, tested backups makes this whole thing a minor irritation rather than a catastrophe. Even Windows Server Backup on a Wal-Mart External USB drive is better than nothing. Crashplan does unlimited versioned backups with unlimited retention at a flat rate, and there's a Linux agent as well. Hell, Dropbox does versioned backups. Get something.

"I didn't make mention of it at all in the article, but some firewalls have the ability to block connections to known botnet servers," Tharp explained.

"If that's not available, you can use DNS sinkholing to block connections to known bad domains. SANS released a tool to that end for Windows Server DNS and documentation for it here. This isn't enough on its own but answering this issue needs a multi-layered approach."

He offered another tip for organizations that manage their shares with File Server Resource Manager. Those that do can set file screens.

"You might want to add a screen like *decrypt*, one for *.locky, and look at the common names given for the decryption help instructions (e.g., help_your_files.txt for CryptoWall). FSRM can take action if a screened file is attempted to be written, which includes firing arbitrary commands. You could kill your LanManServer service, for example," Tharp said.

It's possible that after seeing Tharp's list, some administrators will consider the information old news — and if so — they're not wrong.

But consider this, if these protections are dated — why is ransomware still so effective? The gut reaction is to blame the user, and that's not wrong either. However, sometimes the user is always going to be a problem — the trick is to expect an end user will eventually make a mistake and look for ways to limit exposure regardless of what they're doing.

Tharp says he was taken to task by fellow administrators because some of the things he suggested were outdated, particularly the blacklist-based Software Restriction Policy.

"In my defense, that was one point out of seven, but people have really pushed me to point out that a whitelist-based solution is better than a blacklist-based one. I don't disagree at all, but if you're an MSP with 150 clients that's a lot of R&D time to be billed," he said.

"If you're managing one infrastructure you should certainly spend the time to work on an application whitelist. AppLocker is available in Enterprise versions of Windows and has some huge timesaving features, like the ability to allow certain signed publishers across the board. If you don't have AppLocker, working with Software Restriction Policies on a whitelist basis will also do what you need but with a bit more work."

The point is that while some of these methods might seem old, they're still needed. They're the basics that most organizations are missing.

Rather than using a layered approach, organizations rely on a mix of endpoint signature-based protections and awareness training. Teaching users is good, but it isn't a foolproof method of defense.

"My last thought is that if the end-user is put in a position where they're my last line of defense to not open that attachment, to not click that ad, then I have failed them. Not to say that training is useless; we conduct security awareness training and are rolling out phishing testing, but the responsibility ultimately falls on my team to prevent them from ever being put in that position in the first place," Tharp said.

"It's a team effort, but don't mistake it for being a 50/50 split of duties, it's something closer to 97/3. So, do everything you can to close the vectors of infection, and have those well-trained users represent your plan F, G, or H in mitigating this threat. Plans A through E are all on you."

Ransomware infections are being reported consistently in the media these days. Antivirus can't stop these types of infections, because the

vendors have a hard time keeping up with the latest variants. Adding fuel to the fire, because the latest generation of ransomware payloads are smaller scale and more focused, IDS/IPS protections do little to prohibit their spread as well.

So the key is to use a layered approach like the one Tharp outlined. However, it's the existence of (current) tested backups, paired with a solid BC/DR plan that's going to make a world of difference in most cases.

As part of the interview, I asked Tharp to share some ransomware-based war stories, as they almost always make for a good lesson. He delivered as expected:

"I did see it put a company out of business, we were called for the first time after the damage was done. Their antivirus didn't catch the ransomware until it had finished encryption, and when it sprang into action, it not only deleted the virus but also the registry keys the virus created that contained the data on how to decrypt when payment was received.

You know the story, [the company] never tested their backups [and discovered that] backups hadn't run in five years. We had the AV vendor on the phone seeing if there was any way to un-quarantine the registry keys, no solution could be found.

On the other hand, an organization where users knew that their workstations were treated like disposable goods and put everything on the server, was hit. The file server did backups twice daily just with standard Windows Server Backup going to a $50 external hard drive.

That was all it took to have them operational again in hours. It doesn't have to be a gigantic expense to work from a reactive-only standpoint. Add on a cloud-backup solution that supports versioning and you at least don't have to worry about how you're going to figure out who you were supposed to bill for that order."

6 things your users need to know

The best defense is a well-trained user.

BY CSOONLINE STAFF

It's hard to understate the importance of awareness training when it comes to ransomware — or any attack that relies on social engineering. After all, your users are on the front line in this battle.

Yes, you need to have a solid backup and recovery plan in place in case the worst happens, but when it comes to stopping ransomware, prevention should take priority. If you don't let ransomware in the door, it can't hurt you.

So how do you approach awareness training when anyone and everyone is a target? The good news: Your users don't need to become experts in every new malware variant. That's your job. Instead, teach them the following essentials and how to spot common ransomware tricks.

1. Know your enemy

Ransomware is cheap and effective, which explains why it has become the attack of choice for criminals looking to make easy money.

"Other types of cyberattacks typically take more work to monetize," writes Maria Korolov. "Stolen credit card numbers have to be sold and used before the cards are canceled, for example. Identity theft takes even more of a time commitment."

"With ransomware, however, victims tend to pay quickly. Instead of hunting through company networks for valuable data, exfiltrating it, processing it, and monetizing it, ransomware criminals can just sit back and watch the money flow in."

What users need to understand is that the attacker's motive is money. The harder you make their job, the more likely they are to move on to another potential victim.

2. Don't fall for phishing

A report released in March found that 93 percent of all phishing emails contained encryption ransomware. "That was up from 56 percent in December, and less than 10 percent every other month of last year," writes Korolov.

Also of note is that "soft targeted" phishing email in particular is increasingly used by criminals. "This type of email targets people in a particular job category, but may include some customization, such as the name of the recipient in the salutation," writes Korolov. These emails aren't as highly specialized as spearphishing attacks but the combination of added personalization and broader distribution gives them a higher success rate than a run-of-the-mill spam blast.

Fortunately, there's plenty of very good advice out there about how to spot a phishing email. And plenty of real world examples to incorporate into your training program.

3. Look askance at attachments

Ransomware is often delivered via malicious attachments. Here are some types of suspicious files to avoid:

- "The use of JavaScript-based attachments to distribute Locky began earlier this year," writes Lucian Constantine. "However, it is very uncommon for people to send legitimate applications written in JavaScript via email, so users should avoid opening this kind of files."
- A popular type of phishing email is the resume email. If you're not in Human Resources and

someone sends you an unsolicited resume as an attachment, don't open it.

- Microsoft has added a feature in Office 2016 in response to the increased use of attacks involving malicious macros.

4. Find the fakers

Fake ransomware can be as bad as the real stuff if the story ends with you paying the bad guys. Here are a few ways to know the difference:

Real: You can identify the ransomware. "If the ransom demand includes the name of the ransomware, then there's no mystery, and you're in trouble," writes Infoworld's Fahmida Rashid. "But there are plenty of ransom plays that don't bother with names. For example, CryptoLocker simply warned that your files have been encrypted and never flaunted its name. Instead, you'll have to look for other clues: Is there a support email address? Search the Internet for the bitcoin payment address or the actual ransom message and see what comes up on forums or from security researchers."

Fake: You can close out a locked screen. "If it's possible to close out of the screen using key commands, such as Alt-F4 on Windows and Command-W on Mac OS X, then the ransom demand is fake. Or try force-restarting the device and see if the message goes away," says Rashid.

Fake: You can open the files. "Ransomware tends to change the filename as part of the encryption process. Locky adds a .lock file extension to all documents, while CryptXXX uses the .crypt file extension. Look through the files and see which files have been modified. See if you can still open them or if you can change the file extensions back and open the files. Sometimes, the file extensions have been changed without actually encrypting the files."

5. Practice the plan

"Providing people with the actions to take if they perceive themselves to be under attack gives them control," write Ira Winkler and Araceli Treu Gomes. "The threat, actualization and prescribed actions should be specific and should include how to prevent the attack and to whom to report the potential incident."

But don't stop there. Teach them what happens after they report potential incidents. As a security pro, you know that when "when someone reports the attack in progress, the security team can then take actions to prevent the attack from being successful against less aware individuals," write Winkler and Gomes. But your users need to know that as well. Give them the wider view.

6. Education will be ongoing

Because ransomware is proving so lucrative for attackers, you can expect it to be around for a long time. You can also expect that attacks will become increasingly sophisticated. What this means for users is more than one-and-done security training.

Underscoring the importance of continued training in security hygiene, a Vanson Bourne survey from 2015 found that "IT employees were actually more likely than average to open attachments from unknown senders, download apps from outside the official app stores, click on links in social media sites — even though they were also more likely to know that this was risky behavior," writes Maria Korolov.

Take your ransomware education back to basics: Train, test, repeat.

KnowBe4 Ransomware IDG CSO Guide Assets

MANUAL

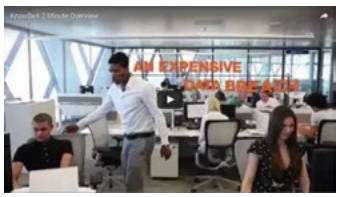
Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.
https://info.knowbe4.com/ransomware-hostage-rescue-manual-idg

WHITEPAPER

How to Transform Employee Worst Practices Into IT Security Best Practices

The bad guys are just one gullible user click away from staging an all-out invasion. Get clear direction on how to go about improving your organization's security posture against social engineering attacks.
https://info.knowbe4.com/whitepaper-employee-worst-best-practices-enterprise-security-idg



VIDEO

Are You Protected Against the Weakest Link in Network Security?

Watch this 2-minute video and learn how you can keep your users on their toes with security top of mind.
https://www.knowbe4.com/knowbe4-2-minute-video

FREE TOOL

Phishing Security Test

91% of successful data breaches started with a spear phishing attack. Find out what percentage of your employees are Phish-prone™ with your free phishing security test.
https://info.knowbe4.com/phishing-security-test-eb-idg

FREE TOOL

Domain Spoof Test

Would you like to know if hackers can spoof your domain? KnowBe4 can help you find out if this is the case with our Domain Spoof Test. It's quick, easy and often a shocking discovery.
https://info.knowbe4.com/domain-spoof-test-eb-idg