Ransomware

What it is and how to fight it

whitehat VIRTUAL TECHNOLOGIES

whitehat VIRTUAL TECHNOLOGIES

whitehat VIRTUAL TECHNOLOGIES

What is ransomware?

Ransomware is a dirty, dirty word.

It's the latest cyber crime to sweep the globe and it cost business and industry more than $325M in 2015, according to a report by the Cyber Threat Alliance. Bored with simply stealing credit card numbers, inventive criminals have turned to infecting computing environments with malware — delivered via any of hundreds of types of computer files — that locks up a computer or a network of computers until the victim pays a price — often very high — to regain access to files on the computer. If the kidnappers' demands are not met, the victim will not receive the magic "key" to unlock the data and the files will remain encrypted and useless, or possibly deleted.

A huge cost

The ransom isn't the only cost of this type of attack, according to a recent survey commissioned by cloud-services company Intermedia. One of the key takeaways of the survey found that the **biggest cost to businesses is downtime**, not the ransom payment. Looking at average salaries, and employee counts, based on data from the U.S. government, one can arrive at an average daily downtime cost of nearly $4,000 for a company with 20 employees.

"If you've got a large number of users and downtime runs into multiple days, then the cost of that downtime adds up pretty quickly," according to Intermedia.

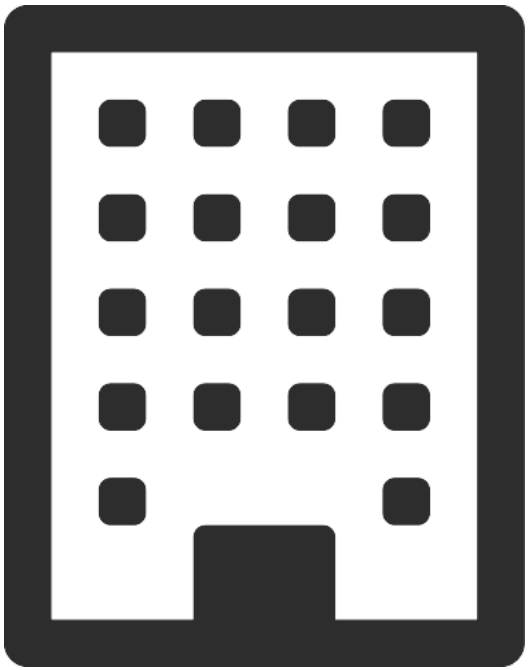
The analysis, which surveyed 300 IT professionals, found that 72% of employees were locked out of their files for at least two days (**a $5,622 productivity loss),** and 32% were locked out for at least five days (a $6,267 loss). 59% of respondents expected the number of attacks to increase this year.

Who is affected?

The breadth of victims of this crime is astonishing.

Hospitals and banks, you've probably heard of. But did you know that schools and police departments — public entities with as limited resources as anyone — have also been hit? All types of small businesses, including law firms (see our mini case study at the end of this book) have been victimized. Private individuals, too, are targets — really, anyone taken in by a legitimate-appearing email who clicks on a fateful link.

The survey also found that ransomware is increasingly targeting bigger businesses (60% had more than 100 employees) and is spreading within corporate networks. These larger businesses take huge productivity hits: **$18,592 per day in payroll losses on average.** Down for five days? Almost a hundred grand. Now we're getting into some real numbers and we have not factored in lost revenue, potential data loss, damage to company reputation or the cost of the cleanup effort, if in fact everything can be recovered.



Defending against ransomware attacks

You can take a number of steps to protect your business and avoid the widespread lack of business continuity planning that contributes to the dangers posted by ransomware

Educate your users

Many of these attacks come in the form of an e-mail. Train your users to be wary of spammish e-mails and to delete suspicious missives after alerting you to the domain that sent the offensive e-mail. Caution them against willy-nilly clicking on links on shady-looking websites. Word documents and Excel spreadsheets, too, can contain macros that are "perfect" delivery mechanisms for malware. **Advise your users not to open documents they aren't expecting.** It's better they call the sender to confirm the legitimacy of the file rather than open up an infected e-mail attachment.

If a user becomes suspicious that something is amiss, they should be advised to **immediately unplug their computer's ethernet cable** from the wall. Their second step should be to contact IT right away.

Make sure your users are aware of your software installation policy. Assuming they're supposed to leave app installation to the IT team, make sure this policy is enforced. If you don't have an IT staff, it may behoove you to bring in an expert for some training, at the very least.

Strong defense is crucial

Access management

A subset of user management is access management. Narrow your exposure by locking down file access only to those with absolute need. Consider carefully which users have admin rights to your network and to all components of your network. **This isn't to presume malicious intent**, of course, on the part of any of your staff; it's just another layer of protection from accidental infection. Ransomware cannot encrypt what it cannot see, and damage will be limited to what the end user has access to.

Educate your IT staff

The #1 reason IT organizations use to explain a weak overall security posture is that they are too busy putting out fires and dealing with day-to-day issues to give security the full attention it needs.

We've said this before: we have no doubt your IT staff is very smart and we know they work really hard. But just like a mechanic who could fix any problem under the hood of a pre-computerized car, but might struggle with the incredibly sophisticated electronics typical of modern vehicles, IT staff who aren't fully up to speed with the intricacies of how to mitigate your exposure or combat ransomware **may leave you vulnerable.**

Some administrators are experts at managing the overall environment, but may not have firm command of the individual systems at play. Many large companies have purchased a variety of tools of one sort or another but fail to train IT staff how to get the most out of them or, in many cases, even how to use them. Others may know 1-2 tools really well, but not everything. Smaller organizations, particularly, likely have a jack-of-all-trades IT person who may not have the required security expertise.

You must have confident administrators who are **skilled in security matters** and who have thorough knowledge of your entire environment. If your current team falls short, help them get up to speed, or pursue a third-party solution of IT security professionals who can be dedicated to monitoring and managing your security posture at a fraction of the price of hiring a full time staff.

Top 3 reasons for weak security

1 The #1 reason IT organizations use to explain a weak overall security posture is that they are too busy putting out fires and dealing with day-to-day issues to give security the full attention it needs.

2 A lack of understanding of the layers of security it takes to create a truly secure environment (Hint: There is more to IT security than just IT — employees are often the biggest single risk factor). Security vendors can add to the chaos by offering spot solutions that solve one problem but ignore every other aspect of security. Without a complete understanding of how to build appropriate layers of security or working with a firm or product set that addresses security from a holistic point of view, gaps can and often do emerge.

3 The third most-common reason we hear from organizations trying to exlain weak security is simply the extrapolation of the "It will never happen to us" mentality which manifests itself in often a sense of denial and no true assessment of the actual security risks faced by the firm. Often we hear "We have Antivirus and firewalls in place, we are protected".

Make backups. A lot of backups

Having access to a recent and easily restorable backup of your data will save your bacon in the event of a ransomware attack.

But if you don't have the right back-up procedures in place, you may lose several days or longer of work. Failure to confirm the quality of your backups until you need them could lead you to the same discovery made by one now-famous firm, where the backups were all made after all of the data was encrypted.

In addition to pulling the backups, you'll want to be sure to **perform monthly or quarterly tests** to ensure your backup and restoration routines perform as expected. (The maximum time between tests should be what you are comfortable losing in a worst case scenario.)

Even with daily backups, if your workflow is transactional, you will likely suffer the loss of a considerable amount of data from a ransomware attack. Minute-by-minute transactions can't be backed up without risking also backing up malware.

Your backup frequency needs to be designed specifically for your company's workflow and risk tolerance, not to mention the impact that backing up production data has on daily operations.

Use tools that protect your data

Anti-malware software

Install software that helps defeat malware. And be aware that it's not sufficient to install the app and then walk away. You must be **very vigilant** in keeping the anti-malware signatures updated. You must make sure every computer has the anti-malware software installed, is reporting in and is getting the updates.

Dual-pronged intrusion-prevention system

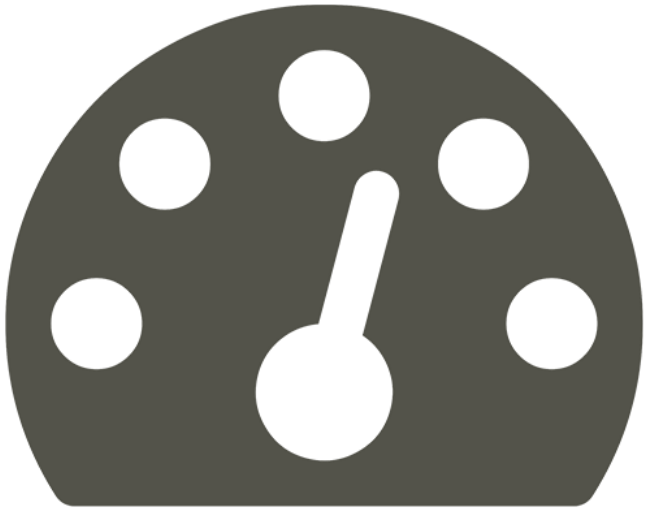
Intrusion detection and prevention systems are appliances that monitor for malicious activity. They can be host-based or network-based. Signature-based systems check for aberrant or malicious actions that take place, whereas behavioral-based systems "learn" your environment's usual behavior and then report on something that is out of line with the usual behavior. These systems **identify malicious activity**, log information about the activity and report it. These tools are your 24/7 eyes and ears.

Community support

Join one of the free or subscription-based communities that regularly share intel about cyberthreats in action around the globe. These **"early-warning" resources** can help you be prepared for threats before they hit you. Sophisticated companion tools, such as ones developed by Whitehat, can even automatically add defensive mechanisms to your environment based on info gathered from these communities.

Get a SIEM

Our discussion thus far has given a lot of attention to reporting. Every computer and server logs every activity it does — this adds up to thousands of lines of data from each device on the network, every day. The best way to monitor these logs, reports and alerts is through a security information and event management tool (SIEM; pronounced “sim”). This is a **centralized manager** that keeps track of all network information and events coming in from your various protection tools. It’s kind of like a dashboard for everything that’s going on in your network, and it immediately alerts you to activity that is outside the norm. Your SIEM must be constantly monitored by your staff or by a third-party IT provider, such as Whitehat.



Citrix: An added layer of protection

Among the more strategic defenses against ransomware is to simply implement Citrix XenApp/ XenDesktop. A hosted virtual machine desktop image created from a read-only image is immune to virus attacks, right?

Immune? No. However, the virus will be destroyed when the system is rebooted as it has no place to live, adding another level of protection. With virtual desktops or shared hosted desktops, your risk is reduced to the window from when the virus was introduced into the environment and when the reboot takes place. So, simply slap some anti-virus software on those images and call it a day, right?

Hold up there, cowboy. Short answer, yes, that line of thinking makes sense, but that is not the end to the thinking here. While Citrix can provide an added layer of security and an easy way to mitigate damage to the servers, not taking into consideration user bandwidth requirements or the impact on the user's profile among other elements can have a seriously negative impact on the end user experience. While it's not rocket science by any means, you'll nevertheless want to make sure you understand these elements and how to properly set up exclusions to optimize the experience and maintain that added layer of security.

By its very nature, a **Citrix environment can offer substantial protection** against cyber attacks because often the network's most vulnerable spot, the user endpoint, is no longer important as it is acting as a "dummy" terminal, with no smarts of its own, when connected to a Citrix XenApp or XenDesktop environment. The actual work takes place back on servers sitting in the datacenter.

While Citrix is a terrific step in the right direction in terms of security, we would be remiss if we didn't point out that Citrix does not protect file servers; other security measures must be implented to keep them safe.

Case studies

Over the last year, three of our clients—one in healthcare, one in financial services and one law firm—were hit by ransomware attacks that circumvented the anti-virus/malware packages that were in place.

In each case, the end user opened the door by accessing a questionable website or being lured in by a well-crafted email. One end user unplugged their computer from the network in time to isolate the virus in that single computer for remediation. One notified IT immediately, one kept quiet and shut off their monitor to avoid seeing the red box on the screen with the 90 minute timer demanding payment.

Now you know why educating end users was the first thing we discussed. The attackers, for their part, each **demanded some amount of money** in the form of pre-paid, Visa-purchased Bitcoins.

However, each customer was prepared with a diligent backup routine and a good plan to restore operations.

While the recovery efforts ranged from a half an hour of time for a single end user to four hours for 30+ users, the bad guys got nothing for their efforts. The backup strategy for each customer was unique based on that firm's risk tolerance profile, but the results were the same, operations were restored...with a few lessons along the way which we will share on the next page.

Lessons from real life

Lesson 1

Educated employees are your first and best line of defense. Train them well — regular reminders don't hurt, either. Turning off your monitor is not a successful ransomware mitigation technique, but unplugging the Ethernet cable before the ransomware can spread can certainly help. We discovered there was a gap of time between when the virus was activated and when it began looking for other places to go on the network that can give an on-the-ball employee time to save the day.

Lesson 2

Anti-virus/anti-malware packages are another necessary layer of security but are certainly not foolproof. They are simply another layer of protection. We have since introduced more proactive measures as added layers of protection. While the virus definitions were up to date, sophisticated hackers are developing ever-more-clever methods of entry that can slip by if we're not extra careful.

Lesson 3

Ultimately, the last line of defense, backups, need to be rock solid and tested regularly. While we would have liked to have caught these particular bits of ransomware earlier, at least they were caught and the recovery managed.

Note 1: Pay special attention to how and where your backups are stored and how long it is going to take you to do a restore if everything goes sideways. While having a backup is great, it is not particularly valuable if it is going to take you 4 days to pull that data back across the wire and restore your systems.

Note 2: In two of these cases, a small amount of data was lost, or more accurately, had to be re-created. This was not a problem for us because this was a known issue that both clients considered an acceptable risk and were prepared for. Our lesson here was to make sure we spend at least as much time designing for how we bring systems back as we do backing them up in the first place.

How Whitehat can help

We get it. Small business or large, you have to balance IT needs, security included, against every other need your business faces.

Our customers tell us that they want to stay focused on their business and core expertise. And with some exceptions, they want an equivalent expert in the security space that keeps their interests in mind, manage and mitigate IT security risks for them, 24/7 without hiring dedicated security staff.

Small business or large multi-national, we have a straightforward process to identify your security gaps as measured against the standards of every major security standards organization, providing a clear outline of your strengths and weaknesses across the 15 major security segments that make up a full information security program.

The results are delivered in simple English so you understand your overall risks and threats, with enough information to make an informed business decision on a logical path forward to protect your organization.

We are proactive. We've built proprietary tools that help us defend your business from attack.

We are here to help.

Headquarters
Capital View Center
1301 S. Capital of Texas Hwy
Suite A-136
Austin, TX 78746

Mailing Address
10601 RR 2222
Suite R-129
Austin, TX 78730

sales@whitehatvirtual.com

Phone: 888-406-8719
Fax: 866-627-3088

whitehat
VIRTUAL TECHNOLOGIES