How ransomware works — Your malware encryption 101

Imagine your data inaccessible. Now, imagine it inaccessible and encrypted, with a ransom note attached. Today, cyber criminals are encrypting businesses' servers and workloads, and then demanding money for the encryption key. It's called ransomware—and it's on a meteoric rise.

Like other virus attacks, ransomware is a malicious attack—though this type of intrusion effectively kidnaps your data.

The infected data and systems are just the start, of course. Untold time and money, not to mention hard-won reputation, can be lost as a result of the downtime and data loss—all with devastating consequences for your business.

It's important to keep in mind, here, that these ransomware perpetrators are not to be characterized as pesky kids with computer smarts. These are ruthless, highly organized, professional criminals, inventing new methods of invasion every single day.

Of course, forewarned is forearmed, so let's get started—here's how ransomware works.

How ransomware spreads

Ransomware relies on deception to infect your systems. And you have to understand how, exactly, it gets in.

The most common method is email.

Cyber criminals will ingeniously devise seemingly innocent means of tricking end users. That's why it's critical that you never download an email attachment from someone you don't know. Just because it's labeled "photo.gif," doesn't mean that's what it actually is.

Sure, it may sound obvious, but simple techniques like these infiltrate businesses every day.

Number two is the internet.

Again, end user education is critical, here. Each employee must be vigilant about not being duped into clicking on questionable links, infected popup ads, or visiting ransomware-infected websites.

Creative cyber criminals may also go analogue.

There are reports of nondescript USB sticks being dropped in parking lots just outside businesses, as if they had just fallen harmlessly out of someone's pocket. Then, an employee stumbles across it, picks it up, and says, "Hey, a 16 gig USB stick! I can use this!" They take it inside with the intent of using it to store music, and plug it into their workstation.

Now, the criminals have just gained a window into the network.

Never underestimate the ingenuity of the criminal mind.

Ransomware kidnaps your files and asks you to pay for it

The scope of ransomware is more vast than you might imagine. Billions upon billions of dollars are lost every year. And, all told, about 60% of its victims choose to pay the ransom.

Without exception, cyber criminals demand payment in untraceable Bitcoin, the same currency associated with illicit drug and arms deals. (That should tell you something.)

And, cyber criminals are getting more sophisticated by the moment. It's so prevalent, in fact, that ransomware is even being offered as a service on the dark web.

Remember: Criminals don't do "customer service"

If you pay the ransom, there's simply no guarantee that you'll get your data back.

Some attackers will take their money and run—others will determine that if you paid once, you might be willing to pay again and demand a second payment. For those that do get their data back, it may come back incomplete or corrupted.

Even if you get your data back entirely, count on the fact that there's now a target on your back. You've just demonstrated that you're vulnerable—and that you're willing to pay.

While mid-market and enterprise businesses realize they're under threat, small and mid-sized businesses often think they're too small to attract notice—but that's not the case. Ransomware attackers realize that smaller businesses often have smaller, less sophisticated IT departments, so they're easier to target and extort.

And, unfortunately, by the time you learn that it's happening, it's already too late.

A real-world ransomware recovery

Ransomware attacks always come at a price—but some do have happy endings.

Phished by an email, one ransomware attacker tampered with a medical clinic's admin account and installed a cryptowall variant. To complicate things further, applications and the exposed local backup copy were deleted—as was the clinic's backup and recovery solution.

Here's the good news: they had been backing up to an offsite server, so they were able to fully restore their data and applications. That's right, they didn't lose a scrap of data.

The lesson here is: if you have redundant backups, then you can tell the "kidnappers" to stuff it—they can keep one.

How to prevent ransomware

It pays to note that 90% of ransomware breaches are cured by end user education.

Of course, it's also imperative that you maintain a fortified perimeter and robust cyber security, as well. Always update your software and backup data as a daily matter of policy.

That said, you simply can't prevent every attack. You need to have a sound, tested ransomware recovery plan, too.

A business that mirrors its operations at all times can cut off the infected portion of its network and recover from a clean backup—whether it lives onsite, offsite, or offline.

A forensics approach then follows: What caused the breach? How can it be excised from the future? What is likely to happen next? Would additional IT staffers or managed services prevent future attacks?

Now, you know the basics of how ransomware works.

In the coming series of posts, we'll present specific methods to protect your critical business data and applications against ransomware, including deep dives on end user education, endpoint security, and backup and recovery.

So, please—stay tuned.

For more information on Arcserve, **please visit** arcserve.com