Making Recovery Part of your Ransomware Preparedness Strategy

A ConversationalGeek® Executive Brief

Ransomware: Today's Threat Reality

Ransomware has become the threat-du-jour for most enterprise organizations, as they struggle to keep up with the rapidly changing threat landscape and barrage of attacks from money-hungry cybercriminals and hackers. IT teams, cyber and info-sec departments, CISOs and CIOs are left feeling like they're stuck in a giant revolving door that rotates between states of secure and insecure in their environments. Ransomware is the latest in a line of threats to come rolling down their internet connection causing that door to spin so fast everything becomes a sickening blur.

It's hardly surprising ransomware has become so ubiquitous and successful because of it's frankly impressive ability to evolve. It sneaks past existing defenses like secure email gateways and desktop anti-virus with ease, then tricks users into running its viral payload themselves for that added killer punch. All of this, on top of our end-users facing other threats such as phishing, vishing, whaling (or business email compromise), plain old spam, malware and internet-villainy. Just when we thought we'd escaped the latest in that long list of threats, along comes ransomware to test out defenses and preparedness to the max.

The Cost Potential in Ransomware

Today, ransomware is a business – yes, *business*. Driven mostly through ransomware-as-a-service platforms run by organized crime gangs, ransomware is the fastest growing threat today. And it's no surprise, given a single ransomware attack campaign can net the criminals millions of dollars, in return for very little risk, expenditure or chances of being caught.

The following stats will give you some idea of the cost of ransomware:

Revenue (annually):	**$1 Billion+**
Infections:	**4000+ daily**
Avg. Ransom:	**3-5 Bitcoins**
(in USD):	**$3500-6000**
Avg. Impact:	**6 workstations**
	2 servers
Avg. Downtime:	**12 hours**
Avg. Remediation:	**12 hours**

Sources: FBI, KnowBe4 Survey

If this sounds like you or your organization, then you're not alone. Ransomware attacks organizations of every size, geography, and industry vertical, although some industries are hit harder, given an assumption that their data is move valuable to the operational ability of the business. The frustration of those affected by these problems is palpable, and most are now looking at a broader cross section of technologies to protect themselves and importantly to recover *post-attack*, rather than rely on pure-play security solutions alone.

Methods of Entry

Ransomware needs a means of entry, some method of delivery, and an ability to execute. Like most malware, ransomware finds its way into an organization through either email or maliciously coded websites. The code used at this point is merely a trojan – some kind of code that is accepted by the OS as a valid *type* of code that an email might contain, or website might need to run.

Once the trojan is launched, it needs a way to download and deliver the ransomware. At this point, trojans rely on macros (like those found in Word and Excel), javascript, and even vulnerabilities found in Java, Flash, web browsers, and browser plugins.

Like security software vendors who strive to improve their product with each passing release, cyber criminals work tirelessly to improve their "product" as well. Using sophisticated and what can only be considered "long-tail" methods – where multiple steps are taken to both avoid detection *and* ensure execution of the ransomware – ransomware authors are proving themselves to be a formidable adversary.

And with social engineering and unsuspecting employees on their side, there doesn't appear to be any end in sight for ransomware in the near future.

Preparing for Ransomware

Assuming it's a *when* and not an *if* ransomware will strike, it's critical to have your IT organization prepare in every way possible, to either thwart an attack, or to minimize its impact within the organization. There are a few common recommended steps:

1. Patch everything, patch often

According to the 2016 Verizon Data Breach Investigations Report, the average time to develop an exploit to a published vulnerability is only 30 days. And with attacks today leveraging vulnerabilities that have been out, literally, since 1998 (*1998!*), it's evident that the *everything* part of the recommended steps is not being taken seriously.

2. Use a multi-layered defense strategy
Many organizations put their trust in antivirus solutions, which rely on signatures and behaviors to identify maliciously-intentional code. But given malware authors not only are familiar with how AV works, but intentionally *study* how specific AV vendors detect malware, and write code that avoids detection *by using current AV software to test against.*

What's needed is a combination of antivirus, email protection, endpoint protection (e.g. application white/black listing), least privilege, user training, and phishing testing.

Part of the layered approach includes some ability to identify the presence of malware/ransomware *and* notify IT so that the instance can be isolated and eradicated.

3. Planning the road to recovery
Your ransomware preparedness and protection strategies can't simply contain steps that are designed to stop ransomware from entering the organization; to be truly prepared, your plan must include measures that allow you to put any manipulated data and systems back into a productive, pre-ransomware state.

You might think it cheaper to simply pay the ransom, however, because we're talking about data being truly modified, you don't want the success of your recovery resting on trusting criminals that your data will be decrypted perfectly, with data integrity perfectly maintained. Relying on data recovery from your own tested backups provides 100% confidence in your recoverability. Also, there's still the issue of removing the ransomware and trojans on your systems. According to a recent Citrix survey, 36% of organizations are not confident they can completely eradicate malware from systems.

So what's needed for recovery?

- **Recover server data** – Many variants of ransomware connect from the infected user device out to any servers it can reach via existing or cached SMB connections, thereby allow it to encrypt files on multiple servers. To be certain data is back in a production state, recovering any manipulated data is necessary. Because you can't know the extent of an attack until it occurs, ensuring all critical files – both user and system – are included as part of your backup and recovery strategy.
- **A plan for user devices** – whether laptops or desktop workstations, these devices need to be completely reimaged to ensure any malware remnant is removed. Devices used by critical users may need image-level backups of their own to get those users back up and working quickly. Other users may simply be recovered using a redeployed standard workstation image.