Denise Boehm sample
Host-Telecom article posted at https://www.host-telecom.com/blog/beat-ransomware-attacks-punch/

Beat ransomware attacks to the punch

03.10.2017

Ransomware, a type of cyberattack tool that encrypts data on computers and networks and demands money to release or not publish them, has been on quite a rampage this summer, first with the global outbreak of WannaCry/WanaCrypt0r followed quickly by the spread of updated Petya malware. Infecting hundreds of thousands of machines around the world and halting operations in small businesses as well as large corporations such as FedEx and LG Electronics, SMBs prove to be a particularly vulnerable target for ransomware.

At first glance, the issue would seem to be the ransomware cost, but that is a secondary concern. By far the more serious problem is the downtime and subsequent revenue loss while you deal with the attack, whether or not you choose to pay the ransom. Lacking the resources of larger corporations, SMBs can feel the hit much more intensely.

Here we'll discuss how to minimize your risk of data lockdown from ransomware and how you can use Backup to the Cloud and Disaster Recovery solutions from Host-

Telecom to keep your data and your data infrastructure up and running. But first let's talk more about the ransomware variants du jour, WannaCry and Petya.

The dreaded takeover "screen"

Malware, including ransomware, has been around about as long as computers have, but ransomware seems to be enjoying a special surge of popularity at the moment. According to Malware Lab's Cybercrime Tactics and Techniques Q2 2017 report, ransomware comprised no less than 50% of total malware attacks in January to a high of more than 70% in June. Appearing on May 12, WannaCry, which is just one of many ransomware families, began its worldwide spread, affecting about 300,000 systems. Figure 1 shows the takeover screen.

Figure 1. WannaCry GUI (credit: Malware Bytes, Cybercrime tactics and techniques Q2 2017)

Petya followed WannaCry on June 27, its lockdown potential greatly exacerbated with updated worm capabilities that enable the spread of ransomware from a single unpatched machine across the network, taking the whole thing down.

Payment demands

Ransomware demands vary, with WannaCry and Petya not being terribly exorbitant, but the sheer number of computers affected reaches pandemic proportions so quickly that the crime tends to pay off. Targeting smaller companies without sophisticated data backup solutions who may then respond more quickly is lucrative, although there's no guarantee your files will necessarily be released. In addition, some ransomware variants are beginning to demand payment in Bitcoin as seen in the WannaCry screen in Figure 1, making it much harder to trace payments and therefore emboldening attackers.

Backups - Shoulda, Coulda, Woulda

As is often typical of malware, a patch that would have subverted WannaCry attacks was developed before cyber criminals unleashed it. Unfortunately and also typically, the fix was extremely sparsely deployed, resulting in widespread shutdowns with a huge economic impact. Malware is nothing new, but unfortunately few organizations are setting records with timely updates.

Yeah, you'll be down awhile, and yeah, it'll cost a lot

How bad could ransomware really be? Well, the sick feeling that the takeover screen evokes is completely secondary to the ongoing trauma of lost revenue as you resolve the issue. Figures estimate those costs at $325M a few years ago and increasing at a blazing rate. By May of this year, Cybersecurity Ventures editor-in-chief Steve Morgan reported that global damages from ransomware had multiplied 15 times in two years. He predicted 2017 losses at $5B, with attacks on healthcare organizations quadrupling by 2020.

With the threat increasing in both frequency and cost, at a minimum your organization should follow rudimentary policies to reduce infection, which we now discuss.

Basic protection

To avoid ransomware, establishing a strict patch update schedule and enforcing it is absolutely critical. As noted, security measures are often available months before data takeover attempts, as was the case with WannaCry and Petya. For example, a patch for WannaCry was available before it started spreading in May, but LG was infected by WannaCry in August.

Keeping staff aware and vigilant about opening suspicious email and attachments is also a must. Even technically savvy people can let their guard down when faced with a huge workload, a full inbox, and Internet pop-up screens. However, neither patching nor employee vigilance is enough.

The inevitable problem with basic protection

While basic network hygiene can mitigate the risks of ransomware, the human factor ensures fallibility. In fact, despite the importance of employee vigilance about suspicious email and similar phishing ploys, Fortinet security states:

> "THIS IS CRITICAL: Do NOT count on your employees to keep you safe. While it is still important to up-level your user awareness training so employees are taught to not download files, click on email attachments, or follow unsolicited web links in emails, human beings are the most vulnerable link in your security chain, and you need to plan around them."

The advice not to count on your employees inevitably extends to strict patch updates where enforcement depends on a human for timely application. Despite the imperfection of these protection measures, you should still do what you can to reduce your risks and start evaluating a higher level of protection.

We'll address data security and infrastructure solutions now, including how to get a meaningful risk assessment for your business that helps you to plan and budget for what you may encounter in ransomware and other malware exploits.

Calculate real world risk

Two highly useful methods to evaluate the resiliency of your business in case of a hit by ransomware or some other type of disaster are Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is an estimate of how long your organization can survive with systems down while RPO is a measure of how well your company operates when faced with data loss.

RTO may stop you dead in your tracks as it can bring down your entire IT infrastructure, but RPO can vary if you have a solid data backup that the ransomware has not encrypted. A good way to differentiate RPO is to think of it as the shortest time you can continue to operate with your latest data backup. Depending on what you use the data for, the backup may suffice for a few days or more before business suffers. However, if your business requires the latest updates, RPO could be zero. To calculate it, determine the time between data backups, the data lost in between, and when the lost data lost becomes critical to business operations.

Risk assessment based on RTO and RPO gives you a much more accurate idea of the appropriate tools, preparation, and associated budget requirements for ensuring ongoing business operations when facing unanticipated shutdowns due to ransomware and other malicious system breaches. Now let's take a look at some of those tools and their costs as well as cost-benefits.

Host-Telecom vs Ransomware

Host-Telecom together with partner Hystax offers Backup to the Cloud and Disaster Recovery, both of which ensure that your latest data are immediately available in case of ransomware lockdown. If a cyberattack causes total system failure, Disaster Recovery can restore your entire operating environment in addition to your data within minutes.

Fast, highly reliable backup recovery at lower costs

Both Backup to the Cloud and Disaster Recovery are based on OpenStack cloud, which we use because of its speed and technical advantages. In addition, you achieve significant savings when operating in an OpenStack environment, which unlike commercial platforms, does not charge software licensing fees.

And while you may harbor concerns about the security of cloud, you should really think again. Although heightened security risk is often cited as a factor in the latency of SMB cloud adoption, research does not support this concern. Analysis shows that the risk of malware infection from using cloud applications is low, with no correlation between usage and threat levels.

With understanding of the cost savings of a dependable environment, let's get into the technical details about our solutions, beginning with Backup to the Cloud.

Backup to the Cloud

To enable Backup to the Cloud, Host-Telecom installs a small, pre-configured virtual machine on your side that transmits your data to our OpenStack cloud in the Host-Telecom data center, where Backup to the Cloud compresses, duplicates, and encrypts your data, creating a complete shot of your data. You can immediately access the continually refreshed data version if your data is compromised.

WannaCry accesses a specific port to attack your computer and network. If you have it open for any reason, the ransomware has easy access. We close this port in the Host-Telecom data center, keeping your workloads secure.

In addition, with Backup to the Cloud you avoid the time and expense of creating your own backup system or spending ever-growing sums for Backup as a Service as your storage needs increase. Check out our prices and particulars.

Disaster Recovery

Disaster Recovery replicates your data as well as your entire IT infrastructure in the OpenStack cloud deployed in the Host-Telecom data center. Accommodating VMware, vSphere, Hyper-V, OpenStack, Virtuozzo, and bare metal workloads, you can access your data and/or deploy your operations in the OpenStack cloud environment immediately in case of system failure. Minimizing RTO and RPO, Disaster Recovery includes plans testing and powerful failback to production at very competitive and affordable prices.

Ransomware personalized

You need affordable solutions and you need them to operate at the highest level. At Host-Telecom we genuinely care about your well being and have exacting standards for the solutions we provide you, testing and using them in our own workspace to make continuing improvements. The following statement by Jean-Philippe Taggart, Senior Security Researcher at Malwarebytes Labs in their Q2 2017 report, echoes our sentiments as he describes his experience facing the biggest disaster failure he's seen:

> *(I witnessed)… a small business owner having to pay for a ransomware decryption key. This particular individual had no disaster recovery plan and would have had to put the key under the door and close the business as critical data was encrypted. Never in my life was buying bitcoins and acquiring the decryption key a more depressing event. This is the worst-case scenario and the worst possible outcome.*
>
> *Not only did such an event demonstrates (sic) the viability of a ransomware attacks (sic) to criminals, it is something I never want to have to do again. Needless to say, this particular victim now has multiple backup solutions, as well as a strictly enforced work-only machine policy. I was profoundly uneasy in providing assistance with this ransomware infection, as I am a strong advocate in never paying, but in this case they saw no other solution. Despite successfully recovering most of the data, it felt like a defeat."*

Like Taggart, Host-Telecom wants you to operate with state-of-the-art security tools at prices you can afford. No one should have to face ransomware or system failure without excellent protection. Contact us today to learn how we can work together to ensure the security of your company's data and infrastructure.

Sources

- Cybersecurity Ransomware Damage Report, 2017 Edition

- Ransomware: an executive guide to one of the biggest menaces on the web
- Is the Network part of your backup strategy?
- Fortinet Threat Report, Q2 2017
- The Cost of Ransomware Attacks Estimated to Reach $5 Billion in 2017
- Will Linux protect you from ransomware attacks?
- Ten steps for protecting yourself from ransomware
- Downtime from ransomware more lethal to small businesses than the ransom
- Three smart cloud services that can keep your business more secure
- WannaCry: Why this ransomware just won't die
- WannaCry ransomware attack at LG Electronics takes systems offline
- Your failure to apply critical cybersecurity updates is putting your company at risk from the next WannaCry or Petya
- 4 ways to avoid the next Petya or WannaCry attack
- Ransomware grows up, goes after data centers
- CyberSecurity 101: The Fundamentals of today's threat landscape
- Cybercrime tactics and Techniques, Q2 2017
- Gallery: 10 major organizations affected by the WannaCry ransomware attack
- Petya ransomware attack: What it is, and why this is happening again

BY

Denise Boehm