Acronis

Ransomware

A Revenue Bonanza for Service Providers

Content

How to Win New Revenues and Customer Loyalty by Fighting the Terrifying Rise in Ransomware

Introduction

Ransomware – malware that gets on your customers' computers, encrypts their data, and extorts a hefty ransom for the decryption keys – is a surging new threat, and what you don't know about it can hurt you in three ways. One, as a user, you can become a ransomware victim yourself, facing a choice between paying an online criminal's extortion demands or losing your data forever. Two, as a service provider, you can miss a golden opportunity to win new customers and expand your footprint with your existing customers. Three, you can lose customers and sales to competitors that recognize how serious a problem ransomware is for their customers and position themselves to fight it.

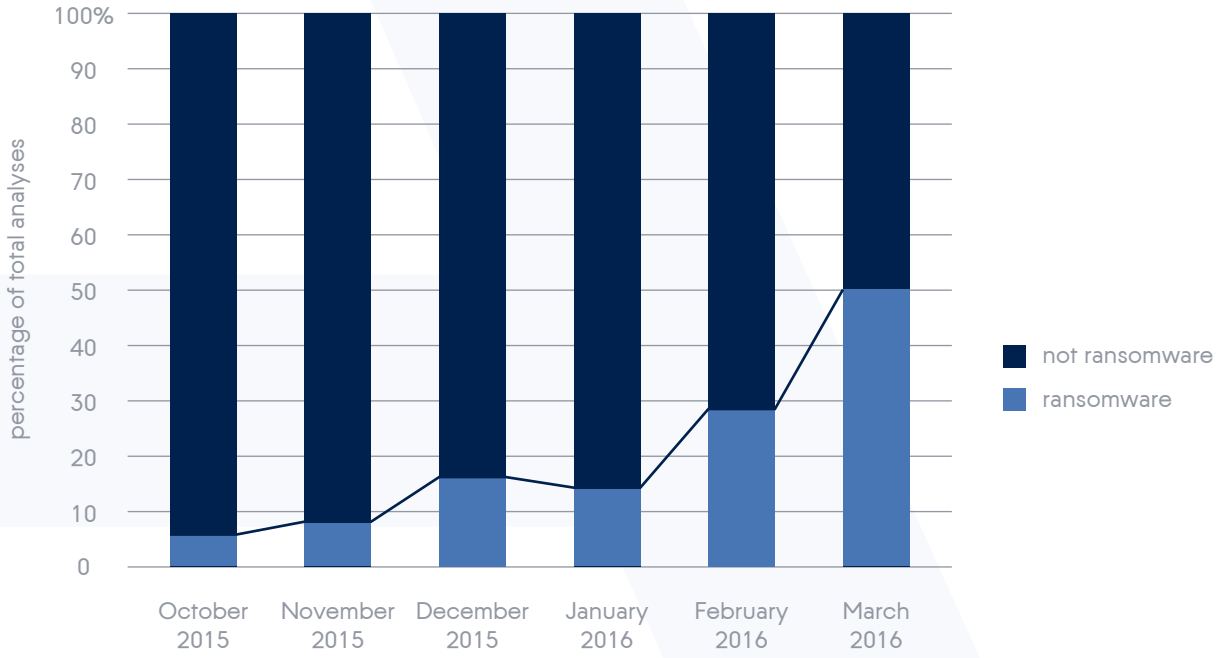


Figure 1: Growth of Encryption Ransomware Against All Other Malware Q2 2016.
Source: PhishMe Q1_2016 Malware Review.

Ransomware represents a new front in the ongoing arms race between cybercriminals and security vendors. Online crooks are constantly looking for new techniques to "kidnap the endpoint," while security vendors try to anticipate the next attack and implement effective countermeasures. In this tug of war, the bad guys are shifting the balance of power in several ways. One, ransomware is growing very quickly relative to other types of malware (see Figure 1): in the first quarter of 2016, it accounted for approximately 15 percent of all malware, but grew to 50 percent by March. Two, new distribution methods have increased the number of ransomware attacks. Three, criminals are using new technologies to quickly and easily craft new variants of ransomware, making it harder for security vendors to keep their defenses up to date. This combination of factors makes it a near-mathematical certainty that any given company, institution or organization will eventually become a ransomware victim.

Introduction

As with any new malware threat, end users are deploying commercial defense-in-depth solutions to detect and remove ransomware before it can take hold of their PCs and servers. However, with the increasing sophistication of ransomware code and a new software-as-a-service development and deployment model, cybercriminals are widening their lead over the defenders. In this new threat environment, hybrid backup represents the only foolproof mechanism for defending against ransomware. When a breach is inevitable and purely a matter of time, the only way you can protect your users is to use backup to restore their systems to their operating state prior to the breach.

This uniquely effective approach to ransomware mitigation presents a golden opportunity for service providers (including managed service providers, cloud service providers, and VARs preparing to enter the cloud services business) to offer their customers anti-ransomware services based on a combination of on-premise backup and cloud-based backup services, also known as **hybrid backup.**

The purpose of this eBook is to educate the reader about ransomware attacks:

- How attacks happen
- What forms ransomware takes
- What security vendors offer to stop and remediate attacks
- Why security software can't always stop ransomware attacks
- How hybrid backup guarantees timely mitigation and the recovery of data
- The opportunity and benefits that hybrid backup offers service providers

Next / Ransomware: How It Works

Ransomware: How It Works

Ransomware is a type of malicious software that infiltrates servers, PCs, laptops, tablets and smartphones via a variety of mechanisms. It often takes advantage of unwary users, zero-day vulnerabilities, and holes in unpatched applications. In the most prevalent form of attack, ransomware encrypts a user's files and presents a screen or a recording with a ransom demand that the user must pay in order to get the decryption key. Thanks to the strength of the encryption used, brute-force attempts to deduce the key are hopeless. Fears of paying for the decryption key but not receiving it are generally unfounded: criminals deliver the key to ransom payers in over 99 percent of cases, apparently understanding that reneging on their end of the deal would be bad for their very lucrative business.

The ransom demand is payable in the online crypto-currency, Bitcoin. The use of Bitcoin makes it difficult for law enforcement to track down the gangs who are writing and deploying the malware. Individuals typically pay ransoms of a few hundred dollars, while organizations can pay many thousands of dollars.

The growing list of infiltration methods includes getting users to:

- Open an email attachment that includes a malicious Word macro or self-executing Java applet
- Click on a counterfeit online ad or email link that brings the user to a compromised or counterfeit website that performs a drive-by download of malware
- Plug in an infected USB thumb drive
- Download legitimate software or pirated content that contains ransomware

Ransomware: How It Works

Phishing is a very common infiltration method that relies on the unwariness of end users. Phishing emails are designed to look like they come from trusted sources, e.g., a familiar bank, retailer or vendor. Figure 2 is an example. Believing the email to be trustworthy, the user clicks on a link or opens an attachment, opening the door to the ransomware infection.

Some ransomware variants are bundled with suites of malware with other goals, like the Angler exploit kit, which combines Cryptowall 4.0 ransomware with Pony, malware that steals passwords and Bitcoin wallets.

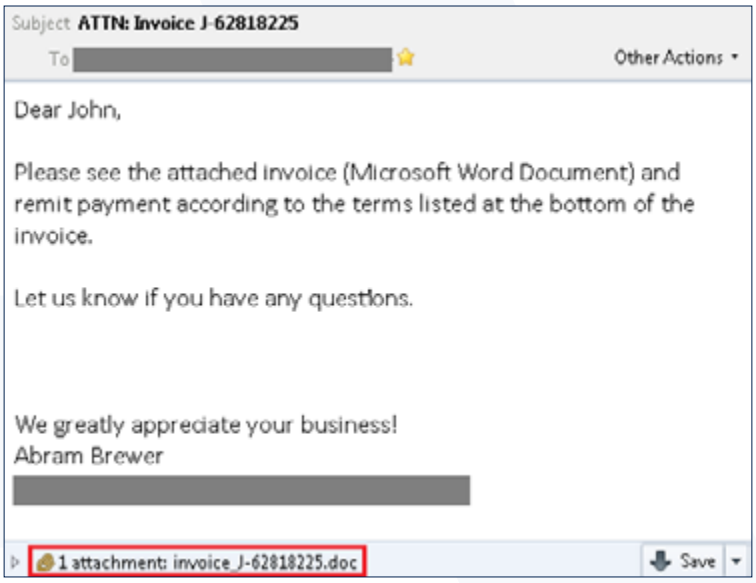


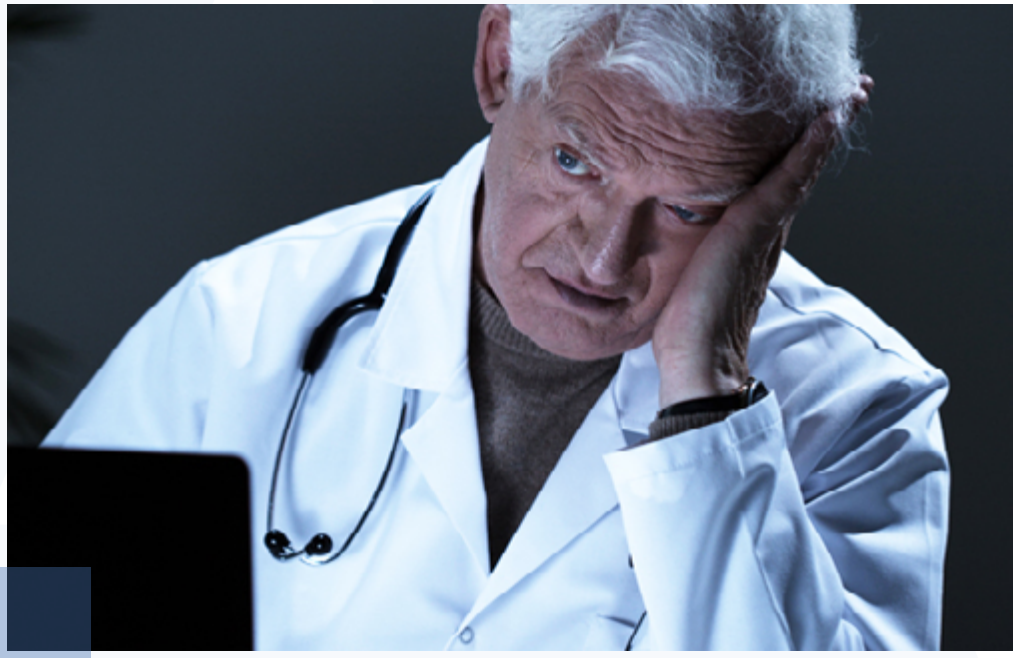
Figure 2: Sample Ransomware Email
Source: blog.avast.com/a-closer-look-at-the-locky-ransomware

Ransomware is the market correction for traditional malware. It is the highest evolutionary stage we have seen thus far, combining malicious intent, broad distribution capabilities, and a native revenue model.

Dennis Fisher, June 2016, "Ransomware is Dope".

Next / Recent Ransomware Attacks

Examples of Ransomware Attacks



In March 2016, MedStar, which operates 10 hospitals and 200 outpatient facilities in the Baltimore, Washington area, was the victim of a ransomware attack. In the ransom note, the gang demanded three Bitcoins, roughly US$ 1,250 for the decryption keys to each infected computer. With 15 systems infiltrated, that amounted to 45 Bitcoins for a total ransom of US$ 18,750.

MedStar was not the only hospital hacked; four medical facilities in California and Kentucky were also hit. One of them, Hollywood Presbyterian Medical Center of Los Angeles, paid cybercriminals US$ 17,000 in Bitcoin to unlock their systems.

In addition to hospitals, "universities, school districts and police departments have been the victims of ransomware attacks with alarming regularity."[1] In March 2016, websites, including the New York Times, the BBC, AOL, and the NFL, were victims of ransomware malvertising.

[1] www.campussafetymagazine.com/article/heres_how_7_institutions_dealt_with_recent_ransomware_attacks

Next / How Ransomware Has Become the Biggest Security Threat Today

How Ransomware Has Become the Biggest Security Threat Today

Ransomware is hardly a new threat. The very first ransomware ever documented was the AIDS Trojan in December 1989. It was spread via diskette and worked by hiding directories and encrypting the names of all files on the computer's hard drive to render the PC unusable. Today, experts have identified more than 120 separate families of ransomware, while other researchers have determined that there has been a 35-fold increase in the number of web domains that ransomware gangs use to host key distribution and payment systems. According to a PhishME report, 93 percent of all phishing emails contain encryption ransomware.

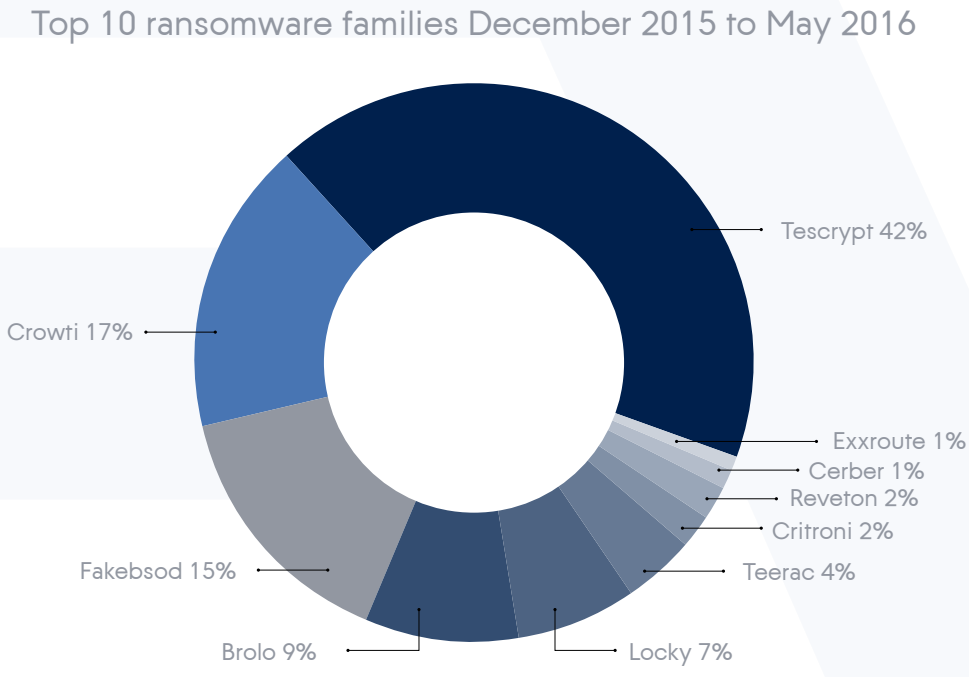


Figure 3:
Source: www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

How Ransomware Has Become the Biggest Security Threat Today

Figure 3 shows the top 10 ransomware families from December 2015 to May 2016. The popularity of ransomware types changes frequently. For example, instances of Tescrypt grew significantly between December 2015 and May 2016; in the same period, Reveton dropped to 2 percent from 7 percent.

In 2015, Ransomware as a Service (RaaS) arrived on the malware scene – "...a variant of ransomware designed to be so user-friendly that it could be deployed by anyone with little cyber know-how."[2] Tox was one of the first RaaS kits available. It allows an individual to register for free and build crypto malware in three steps. The ransomware goes undetected by most anti-virus (AV) software and provides a dashboard to monitor the number of infected PCs and profit in real-time. Tox is only one of many RaaS instances.

While cybercriminals initially focused their attacks on the consumer market, they are increasingly targeting small and medium-sized businesses (SMBs) and larger enterprises. According to a study commissioned by Intermedia and executed by Researchscape International, a market research consultancy, nearly 60 percent of businesses hit by ransomware had more than 100 employees, and 25 percent were enterprises with more than 1,000 employees. The worm capabilities of many ransomware variants let them propagate to other local machines. This means that if only one user in an organization is successfully breached, the result can be a fast-spreading outbreak that can shut down many other servers, workstations, and business-critical applications.

The staggering acceleration in the rate of ransomware attacks is alarming. Walter Chamblee, director of Information Technology at Signaturefd.com, explains, "Ransomware attacks are on the rise and are growing in complexity. Without the right protection measures in place, ransomware can be majorly disruptive to a business. In these cases, it's the user downtime and the hassle for IT that's far costlier, even if you pay the ransom."[3]

---

[2] www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12

[3] betanews.com/2016/03/22/downtime-vs-ransomware-cost/

Next / The Cost of Ransomware Attacks

The Cost of Ransomware Attacks

According to the FBI, cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers.

At that rate, ransomware is on pace to be a $1 billion a year crime this year. The FBI told CNN that the number "is quite high" because a few people "reported large losses."

More expensive than the ransom is the downtime individuals and businesses experience. According to the same study commissioned by Intermedia and Researchscape International, 72 percent of infected business users could not access their data for at least two days following a ransomware outbreak and 32 percent lost access for five days or more.

To do some rough projections of potential costs, a report issued by Emerson Network Power and The Ponemon Institute estimates the average total cost per minute of a data center outage is $8,851. If a ransomware attack brought a data center down for two days, the cost of downtime could run as high as $850,000 for an eight-hour-a-day business.

Next / Endpoint-Based Ransomware Countermeasures

Endpoint-Based Ransomware Countermeasures

Traditional IT security vendors recognize the opportunity in fighting ransomware and are bringing a diverse arsenal of technologies that are often bundled as endpoint security suites for defense-in-depth. Figure 4 outlines the capabilities of a typical bundle and assigns a weight to the importance of each element. A higher score means that the AV software is better than those with lower scores.

Protection Type	Rating	Rating Reasoning
Signature-Based Detection	3	Effective against known malware
Heuristic Detection	3	Helpful against morphing and new malware
Rootkit Detection	1	Great when it works, but can miss new rootkit variants
Real-Time Monitoring	2	Effective in applying signature-based and heuristic detection in real time; slows down computer processes slightly

Figure 4: Anti-Virus Protection Types and Ratings.

Traditional endpoint security measures such as AV scanners and host intrusion prevention systems (HIPS), which monitor the behavior of code on endpoints, do provide a level of defense against ransomware. However, a number of factors contribute to the reality that these defenses cannot keep up with the accelerating volume and sophistication of ransomware attacks:

- The barriers to enter and participate in the ransomware underworld are now much lower. Ransomware kits are widely available, enabling amateur hackers with relatively low technical skills to snap together unique variants of ransomware at very low cost.

- Hiding ransomware from signature-based security scanners is much easier. Polymorphic ransomware (e.g., ransomware that constantly changes) creates a unique binary for each machine it infects, making it difficult for antivirus signature databases to keep up. Even without polymorphic code, inexpensive morphing services are now available online that wrap each instance of ransomware in an obfuscating envelope, hiding identifiable malware signatures and malicious code elements from signature and heuristics scanners.

Endpoint-Based Ransomware Countermeasures

- Ransomware is getting better at defeating behavior-detection security measures like HIPS. For instance, some ransomware instances will go dormant for a period after successfully infiltrating a machine, falling off the radar of endpoint security software and then self-activating later.
- With the arrival of RaaS, some cybercriminals now serve purely as distributors whose task is to infect user systems with the malware and pay a percentage of their ransoms back to the RaaS provider. This model, which mimics the two-tier distribution model of legitimate cloud service providers, has greatly increased the scale and reach of new ransomware attacks.
- The control infrastructure of ransomware attackers and RaaS providers is getting smarter. For example, RaaS providers shift the web locations of their command and control servers multiple times a day, making it difficult for security researchers and law enforcement to identify and locate them. Shifting these server locations also defeats security countermeasures that use URL whitelists and blacklists.
- The range of ransomware attack vectors is growing. Today, ransomware variants infiltrate endpoints via spam and phishing email attachments and embedded links, compromised or malicious websites that deliver malware via drive-by downloads, counterfeit online ads that direct users to malicious sites, exploits of operating system and application vulnerabilities, and infected USB thumb drives. The RaaS model is innovative and has increased the scale of infiltration methods; it has created a tier of criminals whose earnings depend on the number of machines they manage to get infected.

In short, fighting ransomware attacks at the endpoint requires a multifaceted, defense-in-depth strategy that includes security awareness training (e.g., reminding users to stop opening email attachments from strangers), web and spam filtering, diligent operating system and application patching, application whitelisting, and privileged-user management.

Next / Your Customers and Prospects Will Be Attacked

Your Customers and Prospects Will Be Attacked

Given the geometric expansion of ransomware distribution via RaaS, the increasing sophistication of ransomware techniques to defeat endpoint security, and the security-challenged behaviors of end users, your customers will eventually be victims of a ransomware attack. The good news is that there is one foolproof method for recovering from a ransomware breach: hybrid backup that combines cloud backup services and on-premise backup.

Assume that an attack will eventually succeed, and prepare for it with timely, consistent backups.

Next / When Endpoint Defenses Fail, Hybrid Backup Succeeds

When Endpoint Defenses Fail, Hybrid Backup Succeeds

In the wake of a ransomware attack, a scrupulous backup regimen makes it possible to virtually travel back in time to the point before the infiltration occurred. Routine backups enable the restoration of any ransomware-infected system to a clean state prior to the breach.

Defense-in-depth demands not only a local backup, but another backup in an offsite location such as the cloud. Offsite or cloud backup is necessary because some ransomware variants are capable of searching for and encrypting any local backups they can find. The option to perform bare-metal backups – the type that entirely restores the operating system, all applications, and all user data – further ensures that an infected system can be restored to a clean state.

This is why it is important that companies deploy the most important weapon to protect their data from ransomware attacks – hybrid cloud backup.

Next / Use Case: Ransomware Attack

Use Case: Ransomware Attack

The following use case demonstrates how one business effectively recovered from a ransomware attack with the help of a service provider offering a hybrid of cloud backup services and on-premise backup.

The Environment

The company has 150 employees located in one central office, using a mixture of Windows®-based laptops and desktops as well as Macs® connected to a central data center via wired and wireless LANs. Most of the employees do not store critical company data in the company's central repositories, but instead store it on their machines. For this reason, the company includes all personal computing devices in the scope of the company's backup policy.

The company bought a cloud backup subscription from a service provider. It uses this service to protect all of its systems in its data center, including all PCs and Macs. The company initially backs up all of its systems to local network-attached storage (NAS) devices and then copies the backups to the service provider's cloud. This mirrors the industry-standard best practice known as the 3-2-1 rule of backups, maintaining all data in three locations: one in a live production system; a second copy in a local, on-premise NAS, and a third in the cloud.

The company creates and manages its backups both locally and in its service provider's backup cloud. Laptops are backed up during the working day since many laptops are configured to go to sleep during evening hours. Desktop backups start after office hours.

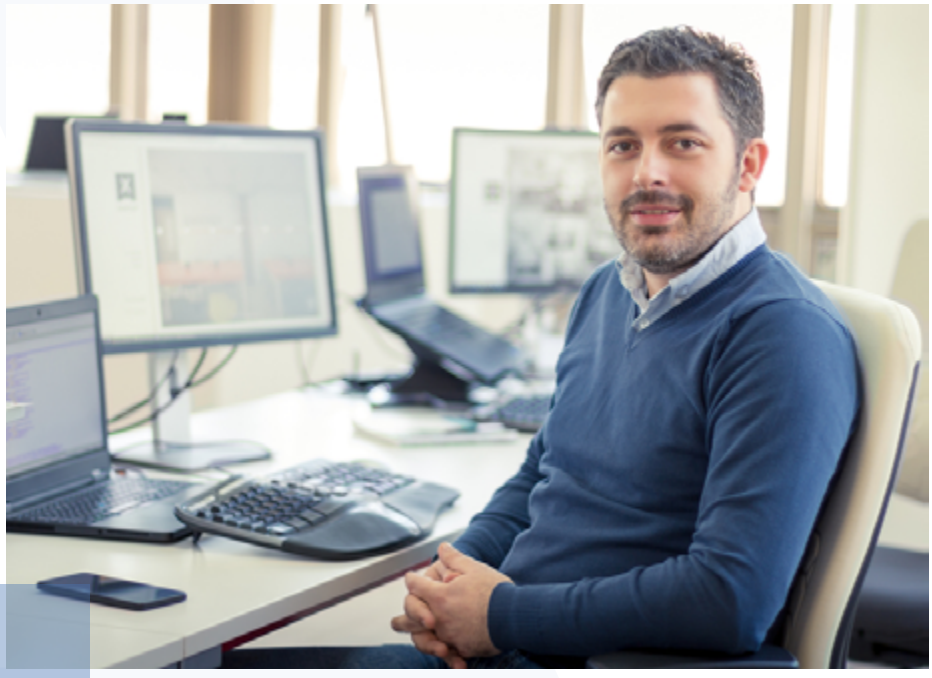
Use Case: Ransomware Attack

The Ransomware Attack and Recovery

The ransomware strike affects numerous PCs and Macs across the company, and the company IT team invokes the recovery plan. Here is the timeline.

Date	Time	Action/Event	Details
Day 1	10:30am	A ransomware attack successfully breaches one PC and starts spreading throughout the facility.	The company IT team is yet unaware of the strike.
	10:42am	First report reaches the IT team and the Help Desk responds.	IT disconnects the infected PC from the network.
	10:51am	Users report seven more ransomware strikes.	The IT team realizes the scale of infection, shuts down the company network, and starts a company-wide check.
	12:07pm	Company-wide check is complete.	IT identifies that 23 machines (a combination of PCs and Macs) are affected.
	12:18pm	IT restarts the network.	IT shuts down all affected machines and keeps them disconnected from the LAN.
	12:27pm	IT contacts the service provider support team.	The customer requests the service provider to send a Large Scale Recovery hard disk drive (HDD) that contains the backed up data (stored in the service provider cloud) for the 23 PCs/ Macs.
	3:45pm	The service provider sends the HDD by courier to the company.	The service provider copies 23 backups to the external HDD and sends it to the company via an overnight courier.
Day 2	8:33am	The HDD arrives at the company.	
	8:51am	IT copies the HDD to central storage.	The IT team copies the backups to higher-performance central storage to facilitate the parallel recovery.
	9:05am	The first backup is copied to storage; the first machine's recovery can start.	The IT team boots the affected PC from a bootable media backup copy while still disconnected from the network.
	9:07am	First boot is complete.	A backup agent is installed on the PC. The IT team connects the network and launches the recovery process.
	9:53am	First recovery is complete.	The machine is restored to its pre-infection state and rebooted.
	10:02am	The first machine is restored.	Copying of backups to central storage continues.
	12:37pm	All backups are copied to central storage.	15 machines (a combination of PCs and Macs) are now recovered.
	2:29pm	The final affected machine is restored.	All 23 machines are recovered. No ransomware is detected.

Use Case: Ransomware Attack



Conclusion

With the help of its cloud backup service provider, the IT team achieved all of the business objectives set forth in the PC recovery plan and restored productivity to all users in 28 hours – well below the two days it takes 72 percent of users to access their data if they pay the ransom.

For a more in-depth review of this incident, refer to the Acronis use case, "Recovering Your Company's PCs Affected by Ransomware."

Next / The Opportunity for Service Providers to Fight Ransomware

The Opportunity for Service Providers to Fight Ransomware

Ransomware represents a unique new threat to your customers. Its rapid growth, accessibility to low-skilled criminals, highly leveraged distribution model, and wide-ranging ability to defeat a variety of endpoint security measures is unprecedented in the history of malware. The uncertainty and fear that accompanies this pervasive new threat has the potential to paralyze your customers and adversely affect their everyday operations. With stories about new breaches and their high costs appearing weekly in the business and technology press, providers do not need to spend a lot of time and money educating customers and prospects on the nature and urgency of the problem.

These factors present an attractive business opportunity to service providers that can offer hybrid backup as a foolproof defense against ransomware. It gives them an opportunity to talk to their customers about an urgent business problem, sell them the most effective mitigation solution on the market, and wrap additional services around it – including security awareness training, endpoint security software, and design and deployment services. It also positions the service provider as a trusted ally: a partner who helps their customers focus on their daily business and not worry about an eventual ransomware breach. Indeed, as a solution to an IT security threat, hybrid backup uniquely instills confidence, not fear.

With the increasing urgency and awareness of the ransomware threat, now is the time to educate your customers that hybrid backup is the only foolproof ransomware mitigation solution on the market.

Next / Conclusion

Conclusion

Ransomware is a huge and growing problem to which your customers are desperately seeking a solution. Traditional IT security vendors are bringing a welter of techniques to the anti-ransomware struggle, but it is a battle that will always leave them one step behind. The result: your customers will inevitably suffer ransomware breaches at some point.

The only foolproof ransomware defense is a rigorous backup regimen, one that assumes the inevitability of a successful ransomware attack and so focuses on recovery by restoring systems to their pre-infiltrated state. And since many ransomware variants can encrypt local backup servers, this strategy demands both cloud-based as well as on-premise backup.

Acronis offers a uniquely flexible, powerful platform that enables service providers to deliver on-premise and cloud-based backup services to their customers and realize a fast path to profitability.

About Acronis

Acronis sets the standard for hybrid cloud data protection through its backup, disaster recovery, and secure file sync and share solutions. Powered by the Acronis AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and affordable data protection of all files, applications and operating systems across any environment – virtual, physical, cloud and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 500,000 businesses in over 145 countries. With more than 100 patents, Acronis products have been named best product of the year, and cover a range of features, including migration, cloning and replication. Today, Acronis solutions are available worldwide through a global network of service providers, distributors and cloud resellers. For additional information, please visit www.acronis.com

Follow Acronis on Twitter: twitter.com/acronis

Next / What Makes Acronis Backup Cloud Unique

What Makes Acronis Backup Cloud Unique

Acronis Backup Cloud is a proven platform that enables service providers to deliver hybrid cloud backup to their customers as a defense against ransomware. To that end, it:

- Leverages the power of the Acronis AnyData Engine to protect any device (physical server, virtual machine, workstation, laptop, tablet, smartphone) in any location (on premise, in remote offices, in the cloud) and recover to any platform
- Simplifies and accelerates the sale of backup-as-a-service (BaaS) by combining the power of the Acronis AnyData Engine with a secure and scalable cloud architecture that integrates with popular cloud management tools
- Enables service providers to offer a true multi-tier solution that gives them control over the packaging and delivery of their backup service
- Provides a multi-tenant solution that reduces overhead by consolidating customer views and administration into a single easy-to-use, unified management console – available anywhere, at any time
- Provides flexible storage options for customer backups, including local, on-premises, service-provider hosted, Acronis-hosted, and third-party hosted, including Microsoft Azure, Amazon S3, and IBM Softlayer
- Supports the 3-2-1 rule of data protection by backing up your customers' data locally and to the cloud
- Allows service providers to offer a unique blend of customer self-service and white-glove management
- Offers service providers an easy-to-use, touch friendly console to manage all of their customers' data protection activities

Next / References

References

Avast. (2016). A closer look at the Locky ransomware. Retrieved July 28, 2016 from blog.avast.com/a-closer-look-at-the-locky-ransomware

Berenson, M., (2016). When ransomware strikes your business, are you prepared? Our new report findings may surprise you. Retrieved July 28, 2016 from www.intermedia.net/blog/2016/03/17/is-your-business-prepared-for-ransomware/

eBay. (2016). Different Types of Antivirus and Security Software. Retrieved July 28, 2016 from www.ebay.com/gds/Different-Types-of-Antivirus-and-Security-Software-/10000000177629318/g.html

Emerson Network Power. (2016 press release). Emerson Network Power Study Says Unplanned Data Center Outages Cost Companies Nearly $9,000 Per Minute. Retrieved July 28, 2016 from www.emersonnetworkpower.com/en-US/About/NewsRoom/NewsReleases/Pages/Emerson-Network-Power-Study-Says-Unplanned-Data-Center-Outages-Cost-Companies-Nearly-9000-Per-Minute-.aspx

FadilpaAiA, S., (2016). Downtime costs more than ransomware. Retrieved July 28, 2016 from betanews.com/2016/03/22/downtime-vs-ransomware-cost/

Fisher, D., (2016). Ransomware is Dope. Retrieved July 28, 2016 from www.onthewire.io/ransomware-is-dope/

Fitzpatrick, D., Griffin, D., (2016.) Cyber-extortion losses skyrocket, says FBI. Retrieved July 28, 2016 from money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

Fox-Brewster, T., (2016). As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin. Retrieved July 28, 2016 from www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#14adb56775b0

Hern, A. (2016). Major sites including New York Times and BBC hit by 'ransomware' malvertising. Retrieved July 28, 2016 from www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising

Korolov, M., (2016). 93% of phishing emails are now ransomware. Retrieved July 28, 2016 from www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html

Lee, T., (2013). 12 questions about Bitcoin you were too embarrassed to ask. Retrieved July 28, 2016 from www.washingtonpost.com/news/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/

Microsoft Malware Protection Center. How does malware infect your PC? Retrieved July 28, 2016 from www.microsoft.com/en-us/security/portal/mmpc/help/infection.aspx

Microsoft Malware Protection Center. Ransomware. Retrieved July 28, 2016 from www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

Murdock, J., (2016). Hospitals crippled by cybercriminals: Ruthless MedStar hack demands A12,900 to unlock computers. Retrieved July 28, 2016 from www.ibtimes.co.uk/hospitals-crippled-by-cybercriminals-ruthless-medstar-hack-demands-12900-unlock-computers-1552429

Patterson, D., (2016). Ransomware-as-a-service is exploding: Be ready to pay. Retrieved July 28, 2016 from www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/

Pauli, D., (2015). Cryptowall 4.0: Update makes world's worst ransomware worse still. Retrieved July 28, 2016 from www.theregister.co.uk/2015/11/09/cryptowall_40/

PhishMe (2016). Q1 2016 Malware Review. Retrieved July 28, 2016 from phishme.com/phishme-q1-2016-malware-review/

Pollack, D., (2016). Data racketeering: When ransomware holds your business hostage. Retrieved July 28, 2016 from iapp.org/news/a/data-racketeering-when-ransomware-holds-your-business-hostage/

Tech Guardian. (2016). Ransomware Jigsaw Deletes Files If You Don't Pay. Retrieved July 28, 2016 from techguardian.co/ransomware-deletes-files-dont-pay/

TechTarget. Defense in Depth. Retrieved July 28, 2016 from searchsecurity.techtarget.com/definition/defense-in-depth

Turkel, D., (2015). There are now programs that anyone can use to extort money from you. Retrieved July 28, 2016 from www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12

Ward, M., (2016). 'Alarming' rise in ransomware tracked. Retrieved July 28, 2016 from www.bbc.com/news/technology-36459022

Winn, Z., (2016). Here's How 7 Institutions Dealt with Recent Ransomware Attacks. Retrieved July 28, 2016 from www.campussafetymagazine.com/article/heres_how_7_institutions_dealt_with_recent_ransomware_attacks

Zaharia, A., (2016). The Ultimate Guide to Angler Exploit Kit for Non-Technical People [Updated]. Retrieved July 28, 2016 from heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-technical-people/

Zorz, Z., (2015). A deadly campaign delivers Pony info-stealer followed by Cryptowall ransomware. Retrieved July 28, 2016 from www.helpnetsecurity.com/2015/12/04/a-deadly-campaign-delivers-pony-info-stealer-followed-by-cryptowall-ransomware/