A Concrete Data Backup Playbook to Combat Ransomware & Malware

What MSPs Need to Know to Use Backups as a Viable Defense

Table of Contents

Introduction

Malware is malicious software. It is designed to cause harm in some fashion to software, computers, networks, data, or simply the interests of the organization such as data theft. Malware includes trojan horses, rootkits, key loggers, ransomware, worms, adware, spyware, scareware, and more. Ransomware has surged to the top of the malware threat food chain for good reasons. It works most of the time and it's very profitable for the cybercriminals.

Most common malware

| Trojan Horses | Rootkits | Key Loggers | Ransomware | Worms | Adware | Spyware | Scareware |
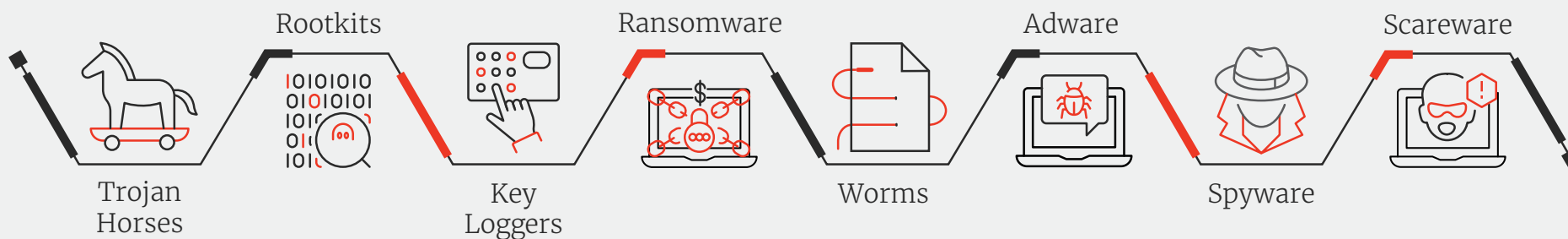
Ransomware is an insidious form of malware. It is designed to extort a ransom from the victims by threatening to publish and/or perpetually block access to their data unless they pay a ransom. Typically, the currency of choice for threat-actors is Bitcoin (BTC) or using more obscure Altcoin cryptocurrencies. The extortion is generally tied to a specific timeframe. If the ransom is paid within that timeframe the cybercriminals will generally provide the encryption key to unencrypt the data allowing access. More often than not the key will not unencrypt all the data, and additional ransom is required to unlock the rest of the data. These threat actors are opportunistic and paying them doesn't guarantee your data, in some cases, the cybercriminals fail to provide a working key even after the ransom is paid. That's the exception, not the rule. It is a business after all. If they do not provide a working encryption key, their reputation will force victims to never pay the ransom.

Several things can occur when the victim does not pay the ransom in the defined timeline. The ransom could increase. Some or all of the data can be effectively destroyed. Some or all of the data can be exposed online, especially sensitive data. All of these possibilities are designed to pressure the victim to pay the ransom. A properly executed ransomware extortion attack makes unencrypting the data without the encryption key a fruitless effort.

Breaching the Gates

In an age of layered defenses (firewalls, deep packet inspection, anti-virus software, black lists, white lists, etc.), how does ransomware and malware in general penetrate an organization? The answer is human engineering. The cyber criminals leverage human failings with highly customized targeted phishing. They determine the personnel likely to have the permissions to the most sensitive data. Then they send specific phishing emails that appear to come from their direct managers, CIO, CTO, CFO, CMO, or even the CEO. It will contain an attachment or link that demands urgent attention. **The email is designed to raise the target's anxiety but not raise suspicions, so they click on the infection.** Or the phishing email will look identical to a common application generated email with an attached report the target sees frequently. In all cases, when the target clicks on the attachment, link, or report, nothing seems to happen. Most won't think anything of it and continue with their normal busy day. Unfortunately, no amount of training will always overcome human emotional reactions. It will help, but it's not foolproof by any means. And once they click on what they should not, that's when the infection begins. Not the attack, the infection.

Example Email

Example 4

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify...

Verify Now

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

The infection will not show any symptoms immediately, similar to a human viral infection. It immediately uses a rootkit to hide from operating system and any anti-viral scans. It then steals the user's permissions to spread as far and wide as it can. For every additional system it infects, it does the same thing until it can spread no further. At that point it can do a variety of things including detonate. Detonation is the process of encrypting all of the data on the machines it has infected. It's the last thing it does. Before it detonates it may do one or more of the following: look for and delete any backups or snapshots it can find; look for and delete any object store buckets it can find; and/or look for and delete any tape library metadata it can find. And/or it may copy out sensitive data sending it to the cybercriminals to use as additional leverage to force ransom payment or become another asset they can sell on the dark web. And/or it will do nothing for months and wait. This guide will go deeper into these issues.

Click here to view the infographic "**Truly Frightening Ransomware Statistics—And It's Getting Worse, not Better**".

Developing a Solid Ransomware & Malware Backup Playbook

Key questions asked by security teams and IT shops are "how do I defend myself against ransomware and where do I start?" An important first step is to establish a process around ransomware response – that is, a Ransomware & Malware Playbook. For MSPs that don't have a playbook, a starting point would be to implement solutions that provide a reliable backup of customer computing devices, and ensure they are working to regularly patch critical, exploitable vulnerabilities. More security-minded MSPs should strongly consider the data integrity and protection of these backups if it's not already in place. Even though these recommendations sound straightforward to MSPs, but maintaining oversight into all these aspects of a ransomware playbook is not that simple. In order for MSPs to maintain control over their security posture related to ransomware and malware and be able to quickly adapt to new threats, it is important to have a Backup Platform that supports your Prevention Playbook.

STEP ONE: DEVELOP A PREVENTION PLAYBOOK (aka A PROCESS)

More Than Just Good Hygiene – A Holistic Approach to Cyber Security

Traditional ransomware prevention strategies have focused on practicing common sense security hygiene and if compromised, focusing on removing infected devices from a network to control the ransomware. But the evolution of ransomware requires a holistic approach to security that provides better visibility of potential ransomware activity across an environment. Backup might be the failsafe or insurance plan you put to action once things go pear-shaped, but Backup in itself is just as vulnerable to being attached if the MSP does not have a good overall threat prevention process in place to ensure good cyber hygiene.

Even though this is a Backup Playbook, one simply cannot ignore having a good threat prevention process in place. Here are the FBI's best-practice guidelines for dealing with these cyber threats:

FBI GUIDELINES FOR DEALING WITH CYBER THREATS

Prevention Efforts

1

Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.

2

Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
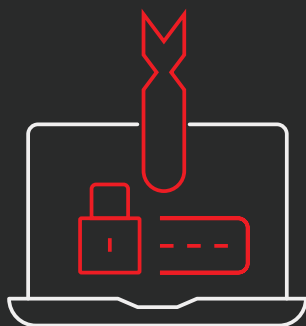
3

Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.

4

Manage the use of privileged accounts—no users should be assigned administrative access unless needed, and only use administrator accounts when necessary.

FBI GUIDELINES FOR DEALING WITH CYBER THREATS

Prevention Efforts

5

Configure access controls, including file, directory and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.

6

Disable macro scripts from office files transmitted over e-mail.

7

Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

Business Continuity Efforts

1

Implement 3-2-2 backup strategy. The 3-2-2 is an update on the 3-2-1 strategy, which advocates a second offsite copy in a different geographical location, and typically it's the cloud.

2

Back up data regularly and verify the integrity of those backups regularly.

3

Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

STEP TWO: MINIMIZE THREAT EXPOSURE TO BACKUPS)

In a perfect world we would be able to build 100% secure systems, free from the threat of viruses or data breach. Unfortunately, even when cyber security best practices are followed, the risk of a system becoming infected remains. While no one can guarantee complete protection, MSPs can take steps to mitigate their risk and make the aftermath of an attack much easier to recover from while minimizing the damages. Antivirus software can go a long way in helping to prevent, and alert you when viruses get too close for comfort. But if a virus does strike, having a backup plan in place, pun intended, is still your best bet to ensure that your important data will remain safe and secure in a crisis event. But now ask yourself what if the backups are infected…what then?

What About Backups?

They're supposed to be the last line of defense against ransomware. That's what the authorities preach and backup vendors push. Don't pay the ransom. Just recover from a "good" backup. That should not be too much of an inconvenience especially now with instant recoveries. At least, that's the conventional wisdom. What happens when the conventional wisdom is wrong?
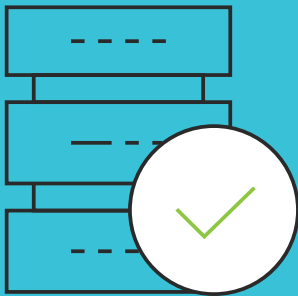
The cybercrooks realized good backups have been able to defeat ransomware, which threatens their revenue streams. That's why they have poured research and development into defeating backups. Most of the modern ransomware variants attack backups and/or utilize them as attack vectors. They turn the cure into a source of infection.

1 Four Key Ways to Get Started Combating Backup Threats
Prevent Unauthorized Backup-set Deletions

Ransomware evolved to neuter backups as a threat to the ransom. It does this by locating the backups, snapshots, or replications and deletes them. It utilizes the admin privileges or published API to delete all of the backups just before it detonates. There are perfectly good reasons for a backup data set, snapshot, or replication to be deleted. Reasons such as age, end of retention period, or compliance time out. This is why data protection software vendors have provided features and APIs to enable that deletion. Ransomware takes advantage of that to delete all the backups, snapshots, or replications to eliminate any possibility of recovery once it detonates.

Many data protection vendors pushed the old backup 3-2-1 methodology to get around ransomware deletions. This methodology is 3 copies of the backup data, on 2 different media, with 1 offsite being tape. The problem with this work-around is that it makes recoveries long, arduous, and error prone because it always comes down to tape. Any backup storage media not air-gapped, meaning not connected to a network, is subject to ransomware deletions. That includes cloud managed service providers. The only media that falls into this category is the tape removed from the automated tape library.

Tape recoveries are painfully slow and error prone. Recovery time objectives (RTO) are going to be far longer than anticipated or acceptable. This is why modern backups have moved away from tape. Most tape backups are rarely the most recent copy of the data because it exceeds backup windows. That means the recovery point objectives (RPO) are much bigger with more data loss.

These attacks have forced many data protection vendors to enhance their software to prevent unauthorized deletions. They do this primarily by making the backup data sets, snapshots, or replications immutable for the retention period. Some make them immutable or WORM forever[1]. Immutability prevents the ransomware from deleting, modifying, or encrypting the data during the immutable retention period. At least that's what most vendors and users believe. Ransomware continues to evolve. There are approximately 4,800 new

---

1 Forever is not recommended because of long-term cost and liability.

variants every day[2]. Some of the variants now go after the storage where the backup datasets, snapshots, or replications are stored. They are designed to steal the storage admin privileges and delete the buckets, volumes, or filesystems where the backup data resides. Doesn't matter if the data is immutable if the underlying storage has been compromised.

Some data protection vendors have gone further to defeat these insidious ransomware backup attacks. They have implemented 2-factor authentication (2FA) on multiple devices so that deletions require a confirmation on a separate device such as a smart phone. Others have enabled backup renaming so the ransomware can't find them. If it can't find them, it can't delete them, nor does it know what storage volumes, file systems, or buckets to delete. And a few have developed a hidden folder so that when the backups are deleted, they're moved to that hidden folder. The backups appear to be deleted, but they're not for a set period of time pre-determined by the admin. This deceives the ransomware into thinking it has eliminated the backups when it has not.

---

2 Source: blog.barkly.com

A. Only the Asigra software does all of the above. It makes backup datasets immutable for the retention period; has 2FA, allows backup renaming, and has a hidden folder for deleted backups with admin adjustable retention periods.

2 Four Key Ways to Get Started Combating Backup Threats
Stop Attack-Loops

While the data protection vendors established methodologies to neutralize ransomware from deleting backups, the cybercrooks focused their efforts on launching new attack vectors. The most perilous being the stealthy Attack-Loop. Attack-Loop ransomware behaves like most ransomware. It infects, hides itself via rootkit, steals permissions, and spreads as far as it can. It's at that point where Attack-Loop diverges. Instead of detonating encrypting all the data, it goes quiescent for a set period of time typically measured in months. The backup software, snapshots, and replications continue to go about their jobs backing up the data. However, unbeknownst to the data protection software, they're also backing up the Attack-Loop ransomware.

At the designated day and time coded into the Attack-Loop ransomware, it detonates simultaneously in all of the infested systems. The data protection administrator goes into action and recovers those systems with the latest backups. As soon as those systems are recovered, the ransomware embedded in the backups, detonates all over again. The admin then recovers from an older backup. After the recovery is completed, the embedded Attack-Loop ransomware detonates again, and again, and again.

How far back must the admin go to recover from a supposedly "good" backup? Do they have to go back one month, two months, four months, six months? How much data can the organization afford to lose? The RPOs become unacceptable. The victimized organization has to pay the ransom to get access to their data.

Combatting this devious attack vector requires the backup software scanning the data during the backup process via multiple malware detection engines. To be highly effective these anti–malware engines should not be dependent on black or white listings. But rather designed to root out zero–day ransomware and malware even when they're a new variant. Upon detection the infected files are quarantined and NOT backed up. The admin can then determine which systems are compromised with these infected files and remove them before they detonate. If the ransomware and/or malware manages to escape detection in the

backup stream or if the backup was backed up before it was scanned, the cyber software should scan the data upon recovery and catch the ransomware and/or malware then. Once again, the infected files are quarantined and not recovered. The admin can do with them what they want. Some will recover them in a sandbox to see what they do. Most will just delete them.

> **A.** The key to the Asigra cyber software is to be able to do the scanning in real-time, without meaningfully slowing the backups or recoveries. Virus scanning is notoriously slow and cumbersome. Doing those scans without impacting backup windows or RTOs is non-trivial. Asigra is the first to accomplish it.

3 Four Key Ways to Get Started Combating Backup Threats
Implement Proactive rather than Reactive-Ransomware Functions

Many data protection vendors tout their anti-ransomware capabilities. These capabilities are generally reactive not proactive. The software utilizes heuristic or behavioral algorithms to detect significant change rates during a backup. When it detects change rates well outside the historical norm, it correlates that to a ransomware detonation. It will then alert the data protection admin that this is taking place. Some will automatically start a recovery on the systems exhibiting that abnormal change rate.

This is analogous to closing the barn door after the horse has departed. It does not detect infections, only detonations. It does not prevent the ransomware detonation, only reacts to it. If it does not prevent unauthorized backup deletions, it is completely pointless. And it does not in any way shape or form prevent, mitigate, or resolve Attack-Loops.

A. Asigra detects ransomware AND malware infections before they detonate. Asigra quarantine identifies the ransomware and malware within a backup dataset enabling the admin to identify the infected systems. Other data protection software and systems do none of this.

4   Four Key Ways to Get Started Combating Backup Threats
Continue to Evolve Your Playbook

Ransomware and Malware in general continue to evolve, the cybercriminals are constantly looking for new vulnerabilities and avenues of attack. The latest is targeting the managed service provider (MSP) via remote monitoring and management (RMM) tools. RMM is an incredibly useful tool for the MSP. It provides MSPs an enormous productivity multiplier by empowering admins to monitor and manage many more systems than they normally could. One major RMM advantage is its ability to push patches, microcode, and updates to lots of systems concurrently. It saves MSPs immense amounts of time, personnel, and cost. It's much more difficult for MSPs to be profitable without RMMs.

The cybercrooks have figured out that by stealing the RMM admin privileges they can use the RMM as a massive multiplier attack vector. It allows them to attack hundreds to thousands of MSP customers simultaneously simply by leveraging the RMM. This is not hypothetical. It's happened to several MSPs. What makes it worse is when that RMM is integrated with the backup as a service (BaaS) software especially when that software does not prevent unauthorized backup deletions.

This is why it's absolutely critical to make sure the BaaS and DRaaS software requires separate logins, passwords, and authentication from the RMM. MSPs hit like this are not dealing with ransoms in the hundreds or thousands of US dollars. They are dealing with millions of US dollars ransoms. Cyber insurance will not cover all of this or even most of it.

Ransomware and malware keep evolving, just like biological viruses. And they can be just as deadly to IT organizations.Ransomware and malware have become the number one threat to IT organizations.

Closing Thoughts

Cybercrime is a lucrative business raking in billions of US Dollars[3] each and every year with a lot of the profits being poured into R&D. Cybercrime is organized and state sponsored. For example, North Korea cybercrime captures significant amounts of foreign currency for the notorious hermit nation[4].

There is never going to be perfect security. Security best practice is for IT organizations make it as hard as they can for the cybercriminals incenting them to find easier targets. This is why security pros emphasize layered defense in depth.

It is that last layer of defense that needs the most attention today. That layer being the data protection. Asigra is committed to making that defense layer as difficult as possible to compromise.

---

3 Ransomware Statistics and Comparitech
4 How Cybercrime Funds North Korea's Nuclear Programme

About Asigra

Asigra's trusted technology is proudly developed in and supported from North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global partner network of Managed IT service providers. As the industry's most comprehensive data protection platform for servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, and eliminates silos of backup data by providing a single consolidated repository with 100% recovery assurance and anti-ransomware defense. Asigra's software has won numerous awards in the Best Enterprise Backup and Recovery Software and Storage Innovation categories for its unmatched defense of backup data against the rapidly growing threat of ransomware infiltrating backup repositories.