DataLocker
Simply Secure

EBOOK

WINNING THE RANSOMWARE WAR

Ransomware Protection, Response, and Recovery Using Managed Secure USB Drives

TABLE OF CONTENTS

SECTION 1
THE RANSOMWARE WAR

A ransomware cyberwar is raging. Not a shot has been fired, nor a bomb guided to its target, but don't let the digital silence fool you. Hostile, even state-sponsored actors actively hunt for vulnerable victims, using every potential attack vector to deploy ransomware payloads. Attackers use phishing, password cracking, supply chain attacks, and malware-wrapped ransomware. Even less skilled attackers can lean on ransomware-as-a-service suppliers to access the technology they require. The result? A quiet-yet-massive cyberwar leading to huge costs for businesses and consumers alike.

SINCE 2016, 4000 RANSOMWARE ATTACKS HAVE OCCURRED DAILY IN THE UNITED STATES

Since 2016, 4000 ransomware attacks have occurred daily in the United States. In an instant, a victim might find their machine unusable and data inaccessible until they pay a ransom with an untraceable cryptocurrency. In many cases, attackers will download a victim's data and release it publicly unless the ransom is paid. Often, attackers will release or sell this sensitive data even if the ransom is paid.

And it gets worse. Though attacks may seem relegated to computer systems, they can have long-lasting effects on the physical world and even disrupt crucial supply lines. For instance, consider the Colonial Pipeline attack, which caused large regional gas shortages in the United States. Or consider the devastating attack on Maersk shipping that brought ports around the world to a grinding halt.

But in the silence, there's an even worse issue that's becoming painfully clear. Cloaked by anonymous cryptocurrency transactions, companies of all sizes and even local and federal governments are giving in to the demands of these ransomware burglars.

These payments are financing cyber warlords, rogue states and criminal enterprises in the sums of hundreds of millions of dollars, with the average being $580,000 per extorted organization, giving the bad guys even more resources to improve their attacks. This affects every industry including manufacturing, pharmaceutical, energy, finance, and even the most sophisticated tech companies, many of which have dispersed remote workforces working solely in cloud environments. These cloud companies still need functioning equipment and networks to connect to their virtual workplaces.

None of us can look the other way or sit this fight out. The stakes for society are too high and even the highest levels of government around the world are imploring both public and private organizations to raise their posture against ransomware. The White House has issued an official warning for companies to act now on ransomware defenses. The official line and recommendation are never to pay, but many unfortunately cave when caught between a rock and a bricked PC.

SECTION 2

EXPLORING CRUCIAL RANSOMWARE DEFENSES

Ransomware protection is possible, but it requires a multi-layer defense across the cyber security spectrum . This goes from identifying attack methods and enemies to protecting data and machines with backups, detecting ongoing attacks, and responding with defensive measures. It can even involve deploying offensive measures and, ultimately having in place methods to recover from an attack.

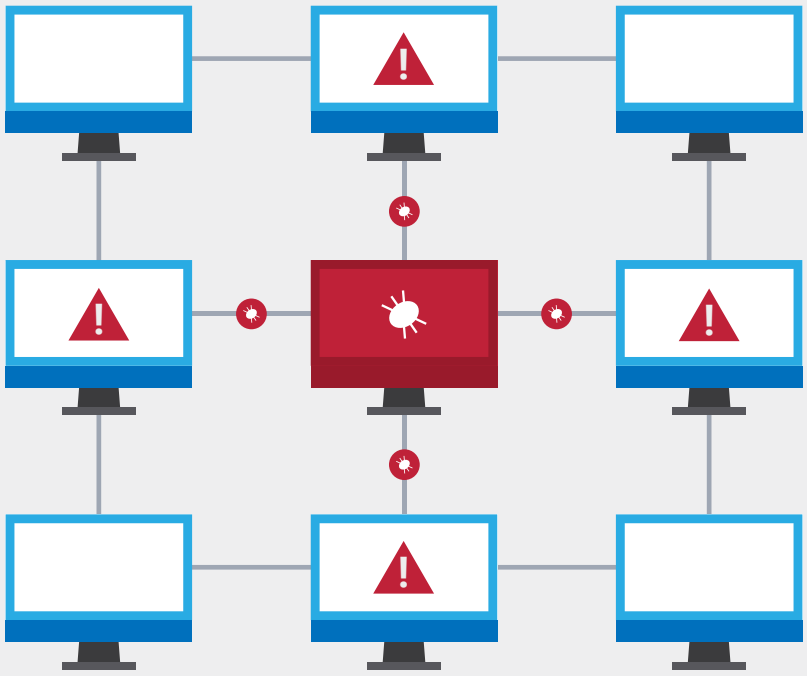
SCOPE AND INTRODUCTION

This paper explores how local offline backups on hardware-encrypted USB storage play a critical protective role in ransomware defense. Further, we'll see how secure USB devices are used as a trusted recovery mechanism to get machines up and running again. There are, for example, many solutions on the market that work to identify and attempt to protect machines against active attacks–could be traditional antivirus or nextgen behavioral engines, and they all play a part. So does implementing two-factor authentication to limit the risk of intrusions. But for the sake of brevity and clarity, we'll focus on the often overlooked part of the recovery from a ransomware attack. We will also see that having a plan B solidly in place will provide you with more options during an active attack.

SECTION 3

YOU HAVE RANSOMWARE. NOW WHAT?

Hey Siri: "How do I get rid of ransomware?" Sadly, it's not that easy. First, if your defenses are compromised, it's time to fight back. Regardless of whether it was a supply chain attack or an email payload that snuck by, it's time to act.



If attacked, most IT pros suggest the same advice: disconnect infected machines from networks and drives.

YOUR FIRST ACT IN THE RANSOM WAR

If attacked, most IT pros suggest the same advice: disconnect infected machines from networks and drives. And with good reason. Consider the story of the network engineers at Maersk that got caught up in the not Petya attack. These engineers were running through the hallways at the headquarters, yanking network cables out of every machine they could get their hands on, all while screens in the office were locking up in front of their eyes. Their gut reaction was correct.

Ok, let's linger on this for a while. If you're lucky, your entire network is offline–As in 1991 offline. Next is the process of disarming the ransomware bomb that's on parts of your network, all with your hands tied behind your back. No central dashboard, no SIEM, no package manager, and likely, no email (as was the case when the City of Baltimore was attacked). Yes, this is how bad it can get.

So, how did we do things before we put everything in the cloud? Let's go old school on these ransomware punks. Is there any method of getting clean machines up and running that does not include the network as we know it?

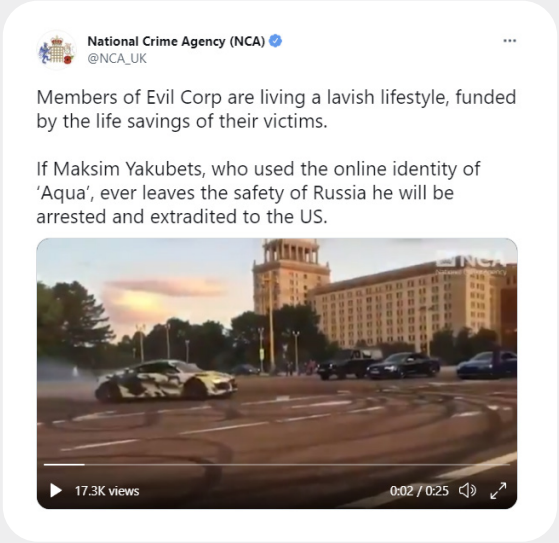
Recovery experts know the answer: boot up a clean environment on that ransomware-infected machine and start anew. This is exactly what Maersk ended up doing. Given the scale of their operation, they put a big dent in the market supply of USB drives getting machines online. To do it, they had to load up thousands of USB drives with clean images and ship them worldwide. This was a logistical and practical nightmare that took place over weeks of grinding work around the clock. But in the trenches, there was, as reported, still an energizing sense that the team was fighting back as every fresh machine showed up in the new infrastructure.

Many large-capacity encrypted drives can be configured as fully bootable drives.

Over and over, the story of booting up from USB drives and cleaning up is repeated. Even in the cases where companies pay up, it's still wise to wipe and restore a clean image on a machine, lest ransomware still be lurking deep in a machine where anti-virus can't find it. Or are you going to trust the word of the people at Evil Corp? Should you trust the burglar that they did not leave something that lets them return one day? Especially when they're trying to get another sports car to do donuts with?

What about that Windows reset capability? It exists, BUT (of course there is a but) it has been prone to get reinfected.

That means if there was ever a time to sing Happy Birthday twice and scrub hard, this is it. You and your employees need a steady-state to work from. So wipe that computer clean down to the last bit. Remember, plan B is now coming into play.



Cybercriminals are known for leaving a backdoor. Even if you pay a ransom and think everything is ok, can you be sure they won't be back?

Make sure to put a plan in place now, so you're not doing a Maersk-style shopping spree, cleaning out Best Buy of their USB drive stock on a Friday night, sweating through your Old Spice onto your favorite RSA giveaway t-shirt.

Nor is it a good idea to implore everyone to download a large data set onto whatever USB they can find lying around and stick it into their/your machines. Maybe that malware-laden USB drive is from the parking lot? Seriously, we can do better. Your employees shouldn't be allowed to use random USB drives anyway because USB port control exists (we'll get to this later). Breathe.

SECTION 4

THE SWISS ARMY KNIFE OF RANSOMWARE WARFARE - THE MANAGED SECURE USB DRIVE

CYBER INSURANCE PREMIUMS ROSE AN AVERAGE OF 18% IN THE FIRST QUARTER OF 2021[13]

Let's rewind, edit, and replay. Suppose we know that there is a calculated risk that we will be hit by ransomware, in fact so high that the cyber insurance industry is getting cold feet with premiums skyrocketing. In fact, cyber insurance premiums rose an average of 18% in the first quarter of 2021. In this case, we need to have a ransomware plan B in place no matter what our first line of defense looks like.

So, you have been hit by ransomware. But the difference now is that you came prepared. Each location that is now sitting there offline has a magic tool available for recovery; they even have the instructions to go with it.

SOME OF THEIR 800 STORES THAT GOT CAUGHT UP IN THE KASEYA SUPPLY CHAIN ATTACK HAD TO WAIT FOR 4 DAYS TO SERVICE A SINGLE CUSTOMER

EXAMPLE 1
THE GENERAL STORE

For example, if you can teach a general store manager to do emergency CPR on a customer, they can probably manage to plug in a USB drive into the store machines and follow a written procedure; it could be considered computer CPR. Central IT is asking you to run the prepared payload of the secure USB drive. This could be:

- A fully bootable environment that can run off the infected machine and connect to, preferably, an alternate central IT system to allow them to be guided from there.
- A pre-approved rollback image that a visiting engineer updates each week/month/quarter.

In the case of supermarket Coop, some of their 800 stores that got caught up in the Kaseya supply chain attack had to wait for 4 days to service a single customer. They had 100 engineers crisscrossing between stores, going from register to register to install a fresh image. The downtime would have been limited if they had a locally available recovery method using a managed secure USB drive.

EXAMPLE 2
THE LOCAL GOVERNMENT

The Bristol Police Department got hit by ransomware, describing their situation as being operational with no electronic capability. Well, that does hamper things. Again, ensuring that critical functions within a department had a rollback from a trusted environment, a managed secure USB drive would have meant that there was a way to fight back. Once you are up and running, you can hopefully access a clean backup, provided that it has not been infected.

EXAMPLE 3
THE REMOTE WORKFORCE

The modern remote workforce is susceptible to ransomware attacks in a particularly concerning way. Many remote workforces are serviced through remote management systems by some central IT function. This makes it extraordinarily difficult if a large percentage of the workforce were to go offline simultaneously due to a ransomware attack propagating through a shared service. One method to beat the adversary here would be to have a managed secure USB available per employee including the following:

Managed USB Recovery Drive

- Rescue Disk
- Recovery Disk
- Separate bootable operating system to keep on working
- All in one toolkit for recovery
- Offline backup taken daily/weekly/monthly

Paired with a clear procedure, this could allow staff to recover independently or in small clusters. Again, if your staff can handle working remotely everyday, they should be able to unlock and plug a secure USB into their machine; if everything comes prepared and prepackaged, it should allow central IT to get a good starting point.

SECTION 5

OFFLINE BACKUP IS THE ULTIMATE ANTI-RANSOMWARE WEAPON

This is worth repeating. If you have a central backup location, it should include having a complementary local backup, as long as it is encrypted properly. Having a local backup on a hardware encrypted USB drive provides a remote workforce with formidable resilience. It is affordable, does not weigh down the local network, and recovery and restoring can take place in a matter of minutes and hours, rather than days/weeks. There have also been many cases where the actual thing being held for ransom includes the central backup. Not even a highly motivated criminal enterprise will be able to reach into the desk drawer of your remote employees, making an offline backup on a hardware encrypted drive the ultimate anti-ransomware weapon. Simply put, if you are fighting ransomware, you should be packing hardware. And if you knew you had that ultimate weapon at your disposal, ready to go whenever needed, maybe that means you never pay a ransom.

CONCLUSION

Having a true plan B in place can provide you with a powerful comeback if ransomware sneaks through your defenses and knocks your organization to the floor. Unlike the ABC of ransomware protection, secure USB drives are not relying on the network for their operation. In fact they are truly isolated which makes them the perfect mechanism to activate if you have been hit by ransomware. They are reliable safeguards that can be activated, provided that you put procedures in place today. These procedures will stand the test of time as we are now adding an offline hardware component to our armory of defense mechanisms.

SECTION 6

DATALOCKER'S ARSENAL OF ANTI-RANSOMWARE TOOLS

TRUSTED HARDWARE ENCRYPTED DRIVES

Used by two-thirds of the Fortune 100 and trusted by elite government agencies, DataLocker has the broadest offering of hardware encrypted USB drives available in various sizes and capabilities. The firmware on the controller is cryptographically signed and verified on each run making it malware resistant, while our supply chain and production are under strict control. The device can be set to lock down based on a timer, ensuring it is kept offline once local backups are completed. It is even possible to configure and preload devices on a massive scale using our DeviceDeployer technology.

CENTRAL MANAGEMENT WITH SAFECONSOLE

DataLocker devices can be controlled, audited, and managed by our central management platform, SafeConsole. This provides inventory control with devices assigned to each user, device and file audit; remote password reset capabilities and management of onboard McAfee Anti-Malware and much more.

USB PORT CONTROL USING PORTBLOCKER

PortBlocker offers endpoint USB port control managed by SafeConsole. USB plays such a crucial role in ransomware attack recovery that the interface should be under strict scrutiny as your everyday network protocol. Ask yourself, if USB was handled in your network firewall, would you leave that GB/s barn door wide open? Yes, data might be leaving in an awful hurry, but malware can also walk right through that open door.

PROFESSIONAL SERVICES

If you do agree on the approach and idea of having managed secure USB drives as a recovery method but don't know where to start or how to put your plan together, DataLocker has a professional services team with niche expertise, understanding certified industry veterans that can help you address those challenges.

1 https://www.justice.gov/criminal-ccips/file/872771/download#:~:text=On%20average%2C%20more%20than%204%2C000,risk%20posed%20to%20your%20organization.

2 https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

3 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

4 https://www.foxnews.com/politics/top-cyber-security-official-warns-of-more-ransomware-attacks

5 https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/

6 https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html

7 https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/#:~:text=When%20announcing%20the%20DOJ's%20recovery,at%20U.S.%20East%20Coast%20gas

8 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

9 https://www.bbc.com/news/world-us-canada-48371476

10 https://gvnshtn.com/maersk-me-notpetya/

11 https://www.infopackets.com/news/10411/explained-if-i-reset-windows-10-will-it-remove-malware

12 https://www.theregister.com/2016/04/11/half_plug_in_found_drives/

13 https://qz.com/2036127/ransomware-hacks-are-driving-up-premiums-for-cyber-insurance/

14 https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

15 http://www.bristolpress.com/BP-Plymouth+News/346297/plymouth-officials-work-to-get-system-back-online-after-cyber-attack

DATALOCKER®

DATALOCKER
+1 913-310-9088

sales@datalocker.com
To find your local DataLocker Reseller please visit
datalocker.com