EMERGENCY RESPONSE TO
RANSOMWARE INFECTION

Understand the symptoms, treatment, and cure for one of the greatest modern threats to data security.

# TABLE OF CONTENTS

The prevalence of security threats engineered to take advantage of unsuspecting users is on the rise. Modern threats are diverse, and continually evolving to evade our protective counter-measures. Ransomware specifically is considered to be one of the most destructive, causing millions of dollars in damage and massive disruption to businesses. Utilize this whitepaper for steps that ensure a fast return to business in the event of infection.

www.novabackup.com

What are the risks of Ransomware infection?

Ransomware is a common type of malware that after gaining access, encrypts system files using a secret key or otherwise prevents you from accessing data. As the name implies, the user is ordered to pay money via untraceable methods (usually BitCoin) within a limited time frame or face permanent loss of their data. For a business to suddenly face their operations being held hostage by a criminal enterprise, the effects can be catastrophic and often business-ending.
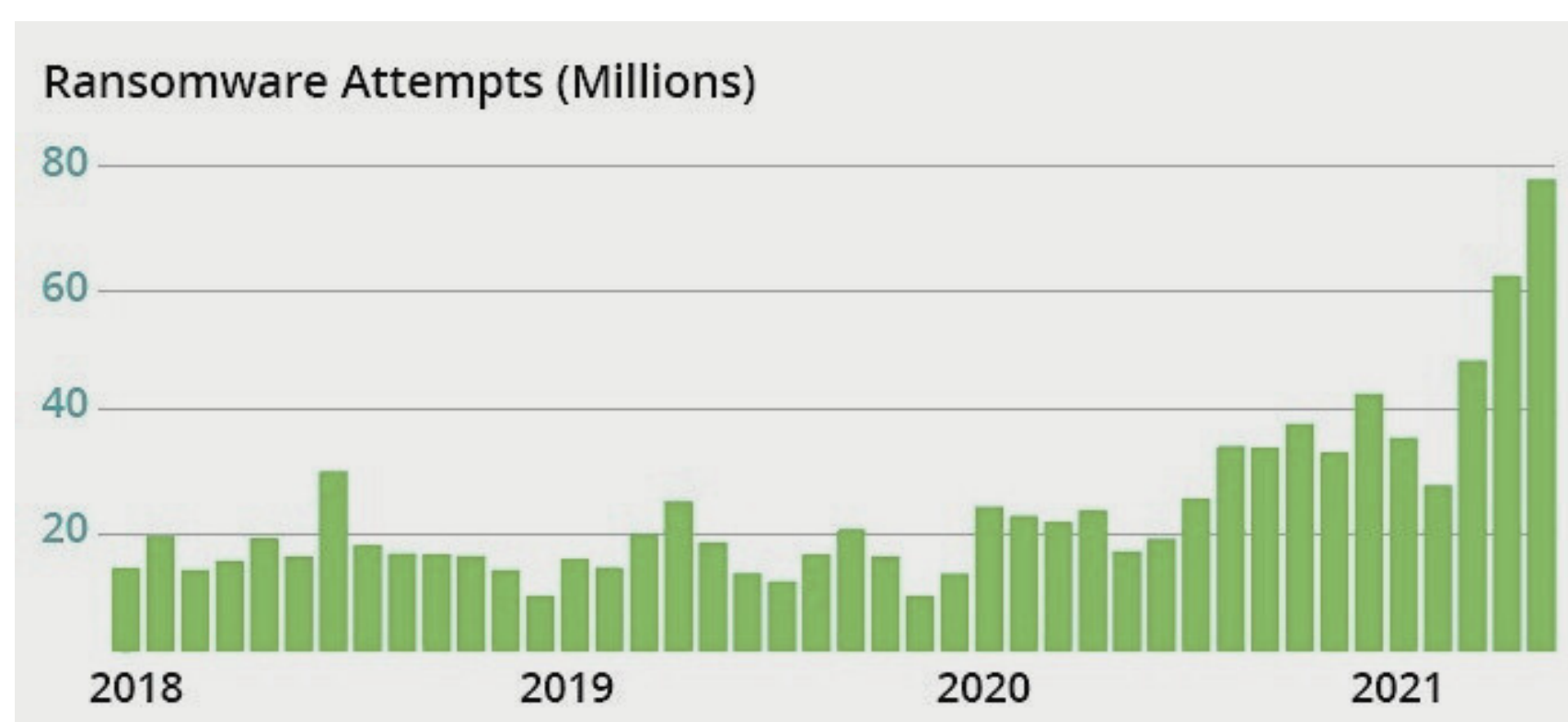
Sources: Sonicwall

Even if a business is able to recover from the loss of data and downtime, far more remains at risk. Damage to reputation can cause long-term effects, and for many industries there are also legal ramifications. Ransomware has infected institutions ranging from small businesses, to hospitals, universities, and government institutions. It can spread throughout networks and even to mobile devices at shocking speeds. Defensive measures are an important part of a ransomware security strategy, however it is quite difficult to achieve 100% preventability. This is why the NovaBACKUP team works with organizations to build a rapid response plan, outlining the emergency actions that must take place in the unfortunate event of infection.

How do I know if I'm at risk?

Understanding the common methods in which ransomware infiltrate systems and propagates itself is critical to preventing infection. The methods commonly used to gain access can offer us valuable hints as to how we can protect ourselves. Quick identification of how the malware gained access can help contain the spread and prevent future infections.

There are many actions that a Systems Administrator can take to help secure a network and connected devices; such as updating software, firmware, and creating secure passwords. But technology measures alone are simply not enough. Equally challenging is a business's ability to deliver employee education about modern cyber threats, to introduce security protocols and to maintain the correct behaviors.

Exploiting Vulnerabilities

If you have data that you can't afford to lose, then you are a potential target for ransomware. Cyber-criminals know that numerous weaknesses commonly exist within hardware infrastructure, software and various network devices. One common method to exploit these weaknesses is by tricking users into an action that delivers malicious software to your system. Once in place, this "Trojan" horse takes advantage of the security hole in order to deliver the ransomware and extort victims. This misstep is often preventable through regular employee education and awareness training.

Phishing

As unsolicited spam email has become commonplace in modern times, attackers and their Ransomware has evolved to become more sophisticated. Messages are received that appear to come from business partners, coworkers, and friends to establish trust and lure users into downloading attachments or clicking dangerous links. Multi-phase attacks might first target your Office 365 environment, then send spoofed emails throughout your organization, or even worse throughout your client base. Modern methods have even shown the ability to mimic the styles and behaviors of trusted email contacts. *Note: Recent advances in deepfake technologies have made it possible to use computer generated audio (voice) and video to impersonate humans (Example: Company CEO) in order to initiate bank transfers.*

Malicious Advertising

Malicious advertisements can be embedded within legitimate websites in order to trick users into clicking on dangerous links. These links may even appear as websites that have been visited before, but lead users towards downloading exploit packages that introduce ransomware. These links may appear as helpful software such as Antivirus and other utilities. But clicking is not always required. A method known as "drive-by-download" can infect a system by simply loading the compromised website and launching malicious code upon your visit.

As these types of criminal groups are rarely brought to justice, malicious advertising continues to grow in popularity with estimates of about 1 in 100 advertisements containing malicious code. Current trends show that weaknesses in mobile devices applications and 3rd party storefronts becoming popular sources of infection.

Self-Propagation

Ransomware is designed to reach as many victims as possible, and accordingly hackers build in creative measures for self-propagatation. Whether spreading to additional systems on your network or accessing your email contacts as a method of infecting others, there are numerous paths that malware takes to spread itself. You may even see such methods as SMS messages to your contacts, or infection of removable drives.

Ransomware-As-A-Service

If ransomware wasn't successful, it wouldn't be growing at such a rapid pace. Cyber criminals have created organizations from which countless ransomware variants can be purchased, and online extortion services may be acquired. These Ransomware-As-A-Service (RaaS) groups have structured themselves with set roles and services, in order to spread rapidly and allow even non-technical criminals to now take part in cybercrime. The popularity of RaaS sites is one of the leading causes of the staggering ransomware growth witnessed in recent years.

What are the symptoms?

There is a there is a brief window of time between infection and the demand for a ransom in which you may recognize symptoms that a serious problem has occurred. Reacting swiftly to signs of ransomware can help to mitigate damage. Check with your organizations members to verify if any of the following indications have taken place.

- Missing files, unexplained files, or data in unexpected places
- Reduced system performance, or unexpected lag during operation
- System boot-up suddenly taking longer than usual

- A locked desktop, or limited access from certain files or programs
- Applications crashing or failing to launch altogether
- Antivirus programs inexplicably deactivated, bypassed or removed
- System crashes occurring more frequently than usual
- Reports of unexplained messages from your contacts (malware propagation)

If you suspect that your system has been infected, immediately disconnect from network and storage devices, run an updated virus scan and proceed to your emergency response plan.

I feel it coming on;
What can I do to cut it off?

If you have even a small suspicion that one of your systems has been infected, the time to take action is now. Not unlike a real virus, ransomware could be replicating and encrypting or deleting files at this very moment.

Isolate

The first step is to isolate the system from all other devices. You should remove it from the network, disconnect any attached storage devices (placing any recently removed storage into quarantine), locking down any NAS devices, and temporarily disconnecting from the Internet. These actions are to prevent the further spreading of ransomware to additional systems.

Scan & Identify

Ensure that an up-to-date antivirus and anti-malware software has scanned your system to identify the specific type of ransomware you are dealing with. If you have already received a message or note, use the content within the ransom note to help identify the type of ransom- ware. You may be able to find helpful details online about how to stop or reverse its progress. If caught early enough, some strains may be removed without ill effects.

Update Antivirus Software

You may need to boot into safe mode to access or update your antivirus software:

Windows Laptop: Power button + S at startup
Windows Desktop: Restart + hold Shift at login
Mac: Restart + hold down Shift

Notify Team

Make sure that the members of your organization maintain heightened awareness about a possi- ble attack and exercise extraordinary caution. If it is known how the ransomware gained entry, this should be swiftly communicated to all parties, along with the strain type. Coworkers should verify that they have recently backed up their critical data. Use of portable / flash drives should be limited until it is determined that all devices are clean. Appropriate security team members should be ready to initiate an emergency data restore plan if necessary.

If I get it, what is the cure?

If you have been able to identify your infection quickly enough, it's possible that an anti-malware or antivirus program may be able to remove it. If however the ransomware has progressed too far, then more intensive measures will be required.

Restore

Ransomware is designed with the mission of disabling your systems before you can remove it. Therefore, it is quite likely you are unable to remove the infection and must resort to replacing your system data entirely. This is where a reliable and secure backup comes into play. By using software like NovaBACKUP to store data in an offsite location, it's possible to completely replace system files, applications and operating systems to a state prior to the infection.

Many storage device manufacturers like <u>Buffalo Technologies</u> include storage-level snapshot capability with their systems to compliment backup. If the NAS device is unaffected by ransomware, the snapshot can help to restore system data back to a previous point in time.

Notify Team

Make sure that the members of your organization maintain heightened awareness about a possi- ble attack and exercise extraordinary caution. If it is known how the ransomware gained entry, this should be swiftly communicated to all parties, along with the strain type. Coworkers should verify that they have recently backed up their critical data. Use of portable / flash drives should be limited until it is determined that all devices are clean. Appropriate security team members should be ready to initiate an emergency data restore plan if necessary.

Law Enforcement

You are a victim of a crime, and it must be reported to the authorities. This may include the police department or FBI. While they may not be able to do much to restore data, taking this action helps to inform others and ultimately deter future attacks. If you've elected to obtain insurance against such an event, providing clear documentation of your follow-up actions will help to expedite your claim. Locations for reporting cyber-crimes will vary by country, but victims in the US can submit their complaint online with the FBI at the <u>Internet Crime Complaint Center (IC3)</u>.

Evaluate the Source

Without understanding how ransomware gained access to your systems, you are unable to defend against additional breaches. Research the type and method of your ransomware infection and put policies into place that prevent this behavior moving forward. Patch any discovered security holes and ensure that software, firmware and all other security systems have been updated to the latest versions.

How do I prevent it from coming back?

Manage Rights and Files

The restriction of administrative rights can go a long way toward mitigating vulnerabilities. You will need to balance user access, network security, and productivity. Make file extensions visible, and utilize tools that let you block known ransomware file extensions. The creation or renaming of a file to a known ransomware extension should trigger an alert notification to the security team.

Penetration Testing

Penetration testing can help to locate and fix weaknesses within your IT environment, and serve to both educate and create a sense of urgency around the subject. Regular restore testing of backups can create confidence in recoverability, while running ransomware infection simulations can offer organizations a realistic idea of what to expect.

What is my emergency response plan?

Advanced preparation for ransomware infection can save valuable time in a situation where seconds count. By laying out your priorities for getting business up and running, you create a clear path forward and enable your team to take action. Once the primary systems are back online, less critical pieces can be addressed and reactivated.

Download and complete the Emergency Data Recovery Plan below and put your customized action plan in writing. An easily accessible printed version should be made available to the security team and system administrators for the fastest possible response during a worst-case-scenario.

DOWNLOAD: YOUR "**EMERGENCY DATA RECOVERY PLAN**" TEMPLATE

Questions about Ransomware? Our team of US based backup experts is ready to provide advice on how to better protect your environment.
Speak with us today.

ABOUT NOVABACKUP

For more than a decade, NovaBACKUP has been a trusted provider of flexible, all-inclusive data protection solutions for Managed Service Providers (MSPs) and professional offices worldwide. As industry leaders in Backup and Disaster Recovery, we bring extensive experience in helping specialized industries meet strict data protection goals.

At NovaBACKUP, our primary goal is to simplify and enhance data protection for our clients. More than just powerful backup technology, our team of backup experts is dedicated to providing unparalleled support. We take a people-first approach to backup, understanding that every unique environment requires a personalized approach to data protection.

With NovaBACKUP, our commitment to exceptional support ensures that you have a reliable partner in data protection. Learn more about NovaBACKUP and explore our comprehensive range of data protection solutions by visiting our website at www.novabackup.com.

Schedule a call with one of our backup experts today!

Our Service Promise

We promise to treat the protection and safety of your data like we do our own. Our job it to make data protection as simple and reliable as possible. You can count on us to provide professional, knowledgeable support that meets your data protection needs. Feel free to reach out to our team if you need assistance with your backup and recovery needs.

NovaBACKUP

NovaBACKUP
29209 Canwood Street
Agoura Hills, California
91301

Tel.: (805) 579-6700
Fax: (805) 579-6710

M-F 9am-5pm PT

Email: ols@novabackup.com

www.novabackup.com