Business Intelligence Brief

Don't Let RANSOMWARE Hold You Hostage

cyberstreams

In Partnership with datto

Ransomware is a rapidly evolving malware threat that was a $1 billion business in 2016 – and it's growing at epidemic proportions. Ransomware victims end up paying from several hundred dollars to tens of thousands of dollars to get the code to access their locked data. This eBook will tell you how to defend your organization from ransomware and other malicious threats.

Chapter 1

What is Ransomware?

Ransomware is a malicious software (malware) that's deployed in a cyberattack. It locks your data with an encryption key that the attacker keeps secret until you pay a ransom via a cryptocurrency like Bitcoin. Unfortunately, paying the ransom doesn't guarantee that your data can be recovered. Ransomware-as-a-Service (RaaS) can now be purchased for a small fee, or a portion of the paid ransom. So, it's easy for criminals to get and use ransomware.

In 2016, a school district in California paid $10,000 ransom, and a hospital $17,000. The FBI reported that in the first quarter of 2017, cybercriminals received more than $200 million from these attacks. So, you can see that ransomware is a very lucrative endeavor.

You may remember the ransomware attacks on the Office of Personnel Management (OPM), Anthem Blue Cross Blue Shield, Target and Home Depot. The rise of ransomware is now one of the most pervasive threats to both businesses and individuals.

Locky is a very dangerous form of ransomware. It's believed to infect as many as 90,000 victims each day.

It has the potential to infect 33 million victims in 12 months, resulting in $300 to $500 million in paid ransom. The Ponemon Institute reports that the average cost of a data breach from ransomware is approximately $6.5 million. Loss estimates are based on costs to the organization that's been targeted.

These losses include:

- Loss of business due to interruptions in productivity, credibility and damage to a business's reputation.
- Regulatory penalties and fines from entities like the Payment Card Industry (PCI).
- Legal fees for litigation.
- Remediation for response and recovery from the incident, public relations, breach notifications and credit-monitoring services (for individuals).

How Ransomware Works

Criminals typically get access to an IT system through:

- Social engineering/phishing where an unsuspecting person exposes his or her network credentials, or unknowingly installs malware on the system.
- Exploiting a vulnerability in an Internet application or service.

Ransomware is typically delivered through waterhole attacks and exploit kits. After it's delivered, ransomware identifies what files and data to encrypt and hold for ransom. Then, a notification is delivered to the victim with instructions on how to pay the ransom.

Once it's paid, the criminal will hopefully release the files. Although, this isn't guaranteed. You can pay ransom and then find that additional files are encrypted because other malware and exploit kits have been installed on your endpoints or other networked systems. This way, the criminal can extort more money from you.

Chapter 2

What's the Answer? – Prevention

Ransomware must be prevented whenever possible. If it does breach your network, you and your staff should know how to detect it to limit potential damage. Training is essential, as is the new best-of-breed solutions that span your IT architecture, with endpoint security for all your devices, even mobile ones no matter where they're used. Android phones are a popular target, and MacOS is now a target. It won't be long before Apple iOS is targeted as well.

The best way to prevent ransomware attacks is to use these best-of-breed solutions to keep the attackers out of your network. An architectural approach to IT is the most effective way to prevent a ransomware attack from succeeding in the first place. With these protections in place, the criminal will move on to another, much-easier IT system to attack.

To prevent you or your staff from unknowingly being targets of ransomware you should do the following:

- Ask your Managed Service Provider (MSP) to conduct security-awareness training sessions on a regular basis. They should provide information on the latest threats and tactics, and train your staff on incident-reporting procedures, so they feel comfortable relaying that they've been targeted.

- Reinforce your security policies, such as not revealing or sharing user credentials (usernames/passwords). Plus, your staff should only use company-sanctioned software and applications.

- Sign up for Software-as-a-Service (SaaS) applications to share files, exchange documents, and collaborate on projects, rather than relying on email that might contain malicious attachments.

- Make sure your staff never enables macro in Microsoft documents. Macro-based malware is on the rise and is very difficult to detect.

- Use non-native document rendering for pdfs and Microsoft Office files in the cloud. Applications for desktops aren't patched regularly, where cloud applications are.

- Don't forget about physical security. Shred paper documents, keep track of who is in your office, and prevent practices like shoulder surfing, piggybacking, and dumpster diving.

- Have your MSP conduct ongoing risk assessments to find any vulnerabilities in your IT system:

    - o Conduct periodic port and vulnerability scans.
    - o Centralize your data logging and event-management platforms (SIEM).
    - o Practice timely patch management.
    - o Stop using unnecessary services and follow system-hardening guidance.
    - o Practice strong password requirements, and use two-factor authentication whenever possible.

Chapter 3

How to Mitigate the Effects of a Successful Ransomware Attack

Implement the following best practices:

- Use domain-name-system (DNS) layered protection so you can identify malicious domains, IP addresses and Internet Infrastructure.
- Employ a system of the least privilege necessary for staff members, to limit an attacker's ability to gain privileges.
- Use automatic firewall, advanced malware protection, encryption and data-loss protection on all your endpoints, including your staff members' mobile devices and USB drives. This protects your system whether your staff works at home, in the office or on the road.
- Use security products and services that analyze Internet traffic, emails and files to prevent infection and data exfiltration.
- Enable security on email gateways with sender-policy framework verification (SPF), including the removal or blocking of executable files that could be malicious.
- Deploy a robust, secure IT architecture that uses micro segmentation to block an attacker's movement throughout your network environment.

If you suspect an attack has occurred, do the following:

- Communicate this to your stakeholders and executives to ensure adequate resources are committed to block the attack and remediate any potential damage.
- Communicate this to your employees, law enforcement, customers, shareholders and the general public.
- Automatically share new security intelligence throughout your IT architecture. You can do this by bringing together critical data from various systems, such as SIEM, threat intelligence and sandboxing tools. This allows your response team to handle high-impact security incidents.
- If malware is detected on an endpoint, it should automatically be sent to a cloud-based threat intelligence platform for analysis. Once this is done, new countermeasures should be automatically deployed and enforced.

Once the threat has been contained:

- Restore your data from your backups and resume normal business operations.
- Preserve any evidence for law enforcement and audit officials.
- Perform a root-cause analysis and identify lessons learned to prevent another attack in the future.

Chapter 4

How the New Best-of-Breed Security Architecture Helps to Prevent Ransomware Attacks

To safeguard your businesses from ransomware and other malicious threats, your MSP can leverage a new best-of-breed security architecture with a layered protection that extends from the DNS layer to email, network and endpoints.

There are numerous phases to a ransomware attack. The criminal must first design an Internet infrastructure to support the execution with command-and-control (C2) phases. Your MSP can implement an umbrella-like protection that blocks this before a connection is established – one that can block the C2 callbacks and stop your system from releasing data.

With the right solution, you can stop phishing and malware infections earlier in the chain, identify infected devices, and prevent data exfiltration. Cloud services protect endpoints both on and off your network. It's the best way to protect all of your users, and can be deployed in under 30 minutes.

The right solution will:

- Automatically protect your IT system with an integrated, umbrella-like approach that correlates with your other security products and services, both on-premise and in the cloud.
- Provide better integration with new and existing security solutions, and reduce complexity so it provides transparency across your entire IT architecture.

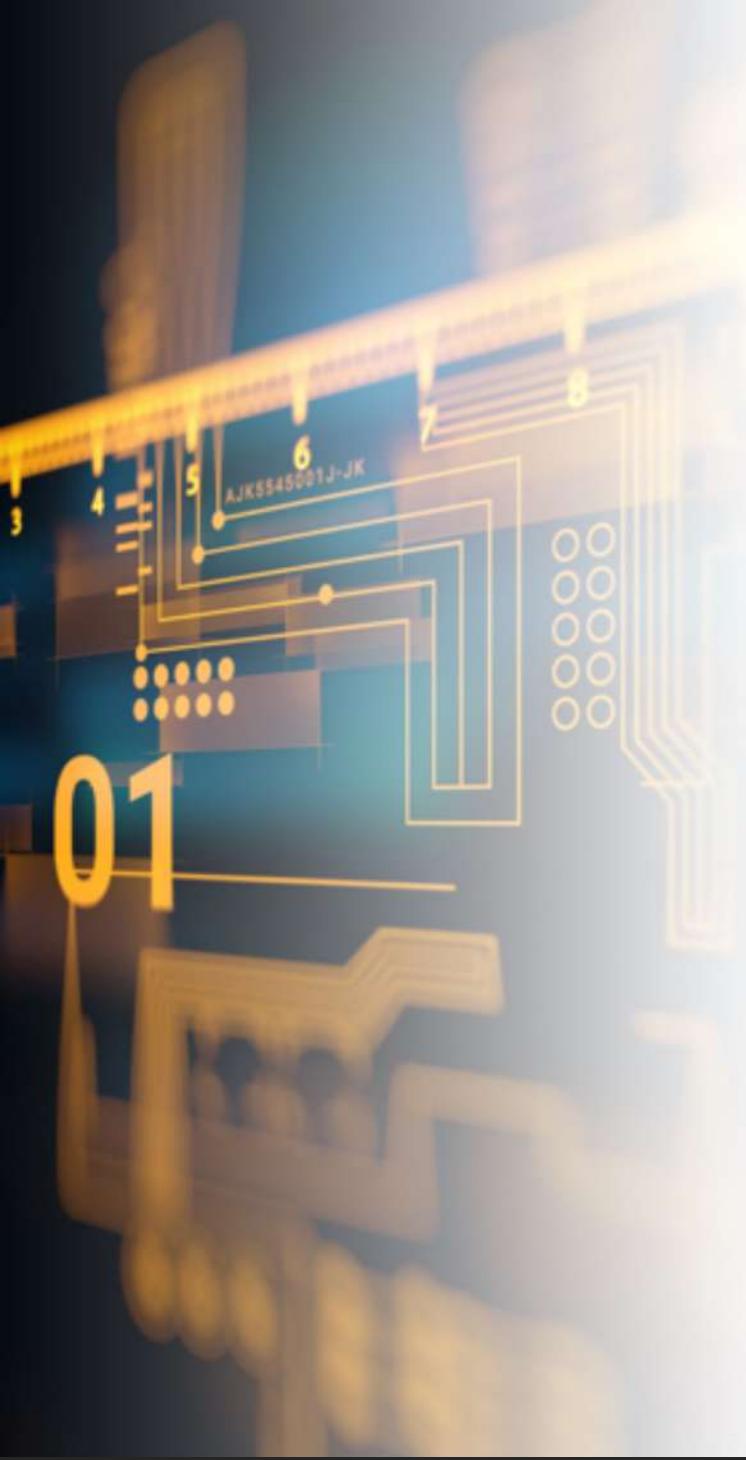
A Best-of-Breed Security Architecture consists of:

- Next-generation firewalls, cloud-based threat intelligence, and intrusion protection that identifies who is doing what on your network.
- A DNS layer that extends protection beyond your firewalls.
- Software defined network segmentation that works regardless of location, device or IP (Internet Protocol) address.
- Email and web security, along with advanced malware protection with sandboxing capabilities to secure endpoints and address email threats.

Chapter 5

In Closing – 7 Things to Remember About Ransomware.

1. It's always evolving and getting smarter. One example of this is CryptoWall. There have been three different versions, each one smarter than the rest. Plus, the pace of evolution is accelerating due to the wide use of Android phones (a prime target), Bitcoin (enabling untraceable payments to cybercriminals), and RaaS (Ransomware as a Service) which makes it easy for anyone to use ransomware.



2. Paying a ransom isn't the answer. Even if your files are decrypted, when you pay the ransom there's no guarantee that the criminal didn't install additional malware on your system. Plus, a copy of your files may have already been exfiltrated and sold on the dark web.

3. Remember to always backup your files to a secure cloud, so they can be easily restored. And be sure to run regular restoration testing to ensure you can retrieve your information in the event of data loss.

4. Ask your MSP to build a layered, umbrella-like security architecture that deploys best-of-breed solutions. This will reduce the complexity in your security environment and improves your overall security posture.

5. Use Cloud-Based, Real-Time Threat Intelligence. This will help you defend against the ever-changing landscape of cyber threats, and to quickly deploy the latest countermeasures as new threats emerge.

6. Ensure your security actions are automated to reduce response time. Such as anti-malware, and intrusion prevention system (IPS) signature files.

7. Always report ransomware or other attacks to the FBI. The FBI doesn't advocate paying a ransom. To report an attack, go to: www.ic3.gov and provide the following:

- The date of infection, and information about your company (your industry and business size).
- The type of ransomware that was detected.
- How the infection occurred (email, browsing on the web).
- The Bitcoin address provided.
- Your overall losses (including any ransom paid, and the impact on your business).

Don't let ransomware hold you hostage.

cyberstreams
Advancing business via smart technology

In Partnership with datto

Contact CyberStreams.
Our Security Experts can help.
425-274-1121
sales@CyberStreams.com