WHITEPAPER

WHEN RANSOMWARE STRIKES

A Look at Two Dramatically Different Business Outcomes.

888-435-7986 | www.getgds.com

GLOBAL® DATA SYSTEMS

INTRODUCTION

Ransomware has emerged in recent years as one of the most significant threats to businesses.

What is Ransomware?

In a typical ransomware attack, a hacker will send a phishing email to one or more users within a company. The email will appear to be from a legitimate sender, and will instruct the recipient to click a link, open an attachment, or take some other action. This enables the hacker to drop malware onto the user's device and propagate it across the network to other systems.

Some ransomware attacks use compromised administrator credentials that have been cracked through a brute-force attack or bought on the dark web. Administrator-level privileges give the attacker full rights to distribute and execute malware on the organization's systems.

The malware may contain encryption keys or communicate with command-and-control servers to obtain them. It then encrypts all the files it can find across the network, essentially locking the organization out of its systems. In a worst-case scenario, the organization's backups are also encrypted and the data cannot be restored.

Your Data Held For Ransom

Once the damage is done, the attacker will display a message explaining how the victim can regain access to the data by paying a ransom, using cryptocurrency that can't be traced. The ransom demand is typically for thousands or hundreds of thousands of dollars, although an attacker recently demanded more than $5 million.

However, there's no guarantee that hackers will do what they promise, which is why the FBI advises victims to not pay the ransom. Paying the ransom also supports the cybercriminal enterprise, perpetuating the attacks.

Ransomware attacks can be devastating

A study conducted by Osterman Research found that more than one-third of businesses had experienced a ransomware attack in the preceding year. Almost one-quarter (22 percent) had to immediately shut down operations for a period of time. Approximately 17 percent said their systems were down for 25 hours or more, with some reporting more than 100 hours of downtime. However, organizations that have invested in advanced security tools and around-the-clock monitoring can avoid these dire consequences.

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

The following two case studies will compare the outcomes of one organization that was inadequately prepared and one that was protected by managed security services from GDS.

Case Study No. 1

Significant Downtime and Data Loss

Company No. 1 had an on-premises data center with servers and storage to support its accounting software and other business-critical applications.

Ransomeware Strikes

The environment was protected by a firewall and antivirus solution, and the data was backed up daily. The company had been talking with GDS about managed security services **but had not moved forward with implementation.**

The company was hit with malware that infiltrated most of the applications, files and backups, and remained dormant for an estimated six to nine months. When the malware went live, users started receiving notifications that the files they were trying to access had been encrypted. **The company then received a ransom demand for several hundred thousand dollars.**

MIllions of Dollars in Costs

The ransomware continued to propagate and the entire business was soon shut down. The company was unable to bill its customers or access email. At one point, the IT team unplugged all the systems from the Internet to make sure the situation didn't get any worse. The company then engaged GDS to begin remediation.

However, because the backups had been encrypted there wasn't much that could be done. In essence, **the entire data center had to be rebuilt from scratch.**

Major Downtime

The company had a week of downtime, during which everything had to be done on paper. For a couple days, employees didn't even come to the office because they couldn't do their work. Conservative estimates was that the attack cost the business $1 million to $3 million.

After the attack was resolved, Company No. 1 bought GDS managed security services and managed secure SD-WAN. The organization's environment is now safe and GDS has remediation services in place in the event that another attack occurs in the future.

Case Study No. 2

No Downtime or Data Loss

On Dec. 20, 2018, a GDS managed security services customer fell victim to a Ryuk ransomware attack.

Ryuk is a targeted attack in which the cybercriminals conduct extensive reconnaissance in order to gain access to administrator credentials. The attackers use the credentials to log into the organization's systems, embed the malware and allow it to propagate. When the malware goes live it quickly infiltrates the victim organization's environment, and because the attackers have admin-level access they can turn off security systems.

Rapid Detection

GDS first detected the infection at 1:34 a.m. on Dec. 20 in a file called 202.exe. It was successfully quarantined. Shortly thereafter, the malware continuously tried to download the same file and another similar file to four other servers but was stopped by GDS.

The malware then used a privileged account to remove GDS security tools from the systems so that the malicious payload could be downloaded and executed. This supported the theory that Company No. 2 had been targeted and that the malware had been dormant for some time.

The investigation also uncovered several issues that allowed the attackers to gain a foothold in the organization's systems before GDS security tools had been implemented.

Incident Response & Recovery

The GDS incident response team began reviewing the organization's firewall event logs for signs of the attack. GDS identified at least one compromised account and several infected machines, and was able to successfully clean those systems. The incident response team also took steps to block malicious IP addresses and geo-locations, and had users change their passwords before logging in again.

The next step was to recover data that had been encrypted on the infected server. Because the company made regular backups that were protected from attack, GDS was able to restore the data and get the server back up and running.

GDS proved that the right tools and rapid response can minimize the impact of a ransomware attack. Company No. 2 lost access to one application for less than 24 hours and never suffered any business downtime.

CONCLUSION

Ransomware is one of the top threats that organizations face today. Cybercriminals can obtain thousands of dollars from organizations desperate to regain access to their data. Even if an organization refuses to pay the ransom, it is likely facing millions of dollars in downtime, data loss and business disruption.

The outcome of a ransomware attack isn't a foregone conclusion, however. While ransomware can get past basic defenses, a **fully managed and monitored security solution can detect attacks and quickly eradicate the threat.**

Managed security services from GDS are proven effective at stopping a ransomware attack.

With GDS working behind the scenes, organizations can rest assured that their systems and data are protected.

GDS can help you protect your data
Contact Global Data Systems: 888-435-7986