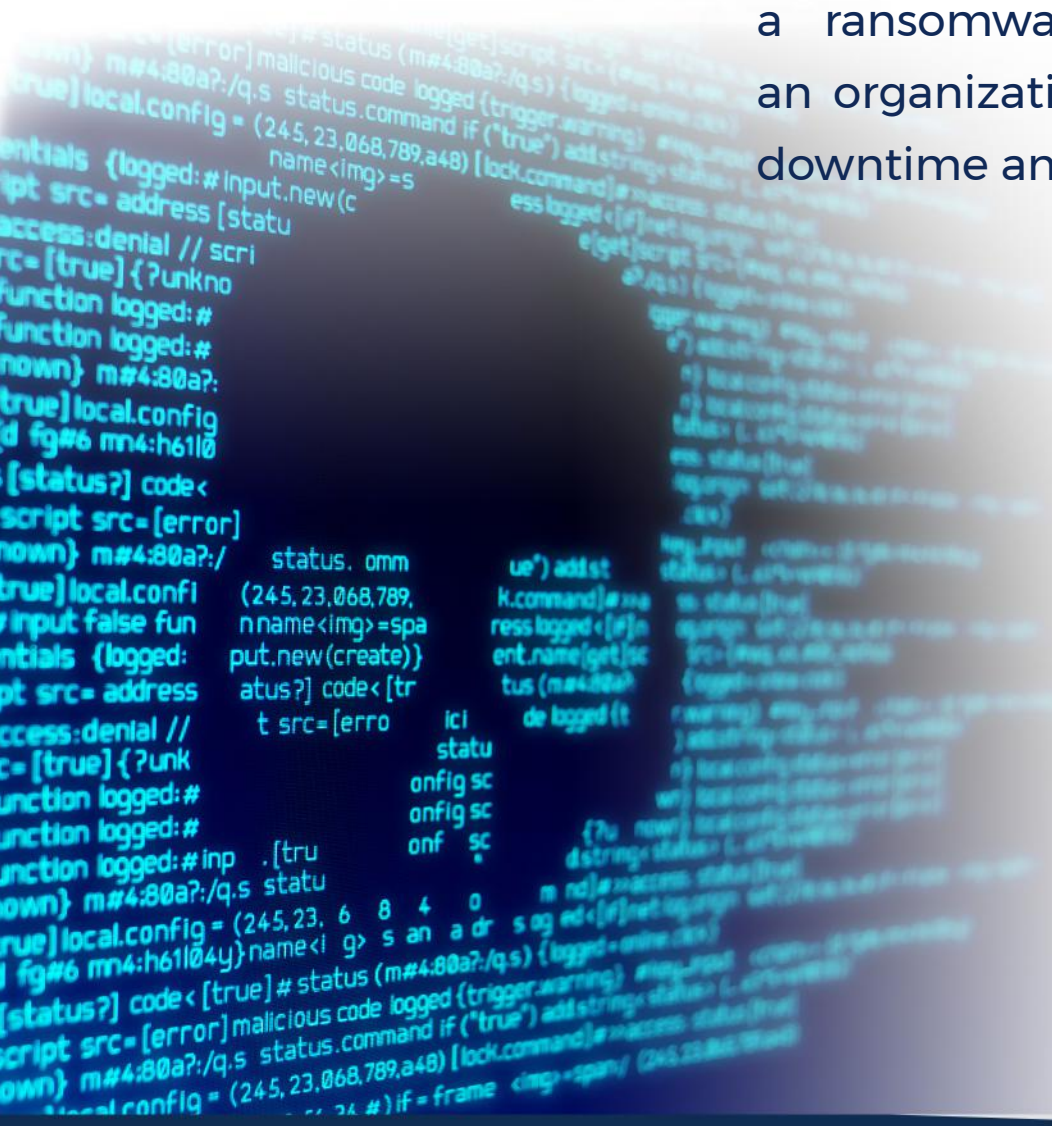
Case Study:
Ransomware Incident Response

GDS detects and rapidly contains a ransomware attack, helping an organization avoid significant downtime and data loss.



No organization is immune to cyberattacks. Large enterprises, including many of the world's most respected brands, have had their reputations seriously damaged by security breaches.

Small to midsize businesses with tighter budgets and weaker defenses have become popular targets, and many never recover from a breach.

Ransomware attacks can be particularly 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.

On Dec. 20, 2018, a Global Data Systems (GDS) customer fell victim to a Ryuk ransomware attack. GDS immediately initiated its malware/ransomware incident response plan to confirm that an incident had occurred, stop the malware from spreading, investigate the source and scope of the attack, remove the malware from the network, and restore affected systems to their normal operating state. Thanks to these actions, the customer suffered minimal downtime and no data loss due to the incident.

Challenge

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, such as a vendor, service provider or government agency. The email will instruct the recipient to click a link, open an attachment, or take some other action that enables the hacker to drop malware onto the user's device and propagate it across the network to other systems.

The malware then takes control and encrypts all files, essentially locking the victim out of the system. The attacker will display a message explaining how the victim can regain access to the data by paying a ransom before a specified deadline, using cryptocurrency that can't be traced. However, there's no guarantee that hackers will do what they promise, which is why the FBI advises victims to not pay the ransom.

In the Dec. 20, 2018, incident, the GDS team determined that the attack was executed using the Ryuk ransomware variant. Unlike common ransomware strains that are distributed via massive spam campaigns, Ryuk is used for targeted attacks and only encrypts critical assets and resources. **The attackers conduct extensive reconnaissance prior to the attack, collecting information on day-to-day business operations, email addresses and credentials, and the network architecture.** The malware is manually downloaded by the attackers onto a compromised system rather than by an end-user through the web or email.

Once the ransomware is loaded onto the system and executed, it stops antivirus, backup and other software from running and writes itself to the Run registry key to ensure that it will execute after reboot. It then attempts to elevate its privileges and create files containing a public encryption key and unique hardcoded ID.

Once these files are successfully created, the encryption process begins using a three-tier model. The first tier uses a global RSA encryption key pair held by the attackers, which means they are the only ones who can decrypt the files. The second tier uses an RSA key-pair that is generated specifically for the victim, and the third tier uses a standard AES symmetric encryption key generated for the victim then encrypted using the second-tier key.

Ryuk performs a recursive sweep of every drive and network share on the victim's system, and encrypts every file and directory except for those containing the words "Windows," "Mozilla," "Chrome," and "RecycleBin," among others. The ransomware also tries to encrypt network resources. Finally, Ryuk destroys its encryption key and deletes shadow copies and various backup files from the disk.

Solution

GDS first detected the infection at 1:34 a.m. on Dec. 20, 2018, 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 the victim company had been targeted.

The GDS incident response team began reviewing the company's firewall event logs for signs of the attack. The highest occurrence of security events occurred two days before the attack began. However, because GDS security tools had not yet been fully deployed throughout the network at that point, investigators suspected that the company's environment had been compromised for some time.

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 encrypted data on the infected server. Because the company made regular backups, GDS was able to restore the data and get the server back up and running.

Results

GDS proved that the right tools and rapid response can minimize the impact of a ransomware attack. The investigation also uncovered several issues that allowed the attackers to gain a foothold in the company's systems.

GDS is working with the company to deploy GDS security tools throughout the environment, and recommended that the company implement a layered security solution that can quickly detect and disrupt an attack. The GDS team also recommended a review of the company's security policies and practices and the development of an internal incident response plan.

An external and internal vulnerability scan can identify exploitable vulnerabilities, while a baseline of system, application and network performance makes it possible to detect unusual behavior. By developing standardized images of servers and desktops, the company can recover infected systems faster.

Because regular backups are the best hedge against a ransomware attack, GDS recommended a review of the company's backup systems and processes to ensure that backups are completed and tested. The GDS team also advised the company to develop and regularly review a comprehensive disaster recovery plan.

For More Information

Contact Us:
- getgds.com/contact-us
- facebook.com/getgds

Call Us:
- 888-435-7986

About This Solution:
- getgds.com/services/security/advanced-infrastructure-security