Phobos Ransomware Impact On Small Business, New Study Released By 2Secure Corp

Cybercriminals are zeroing in on large enterprises, and SMB's - The Size Does Not Matter Anymore.

Ransomware Attack

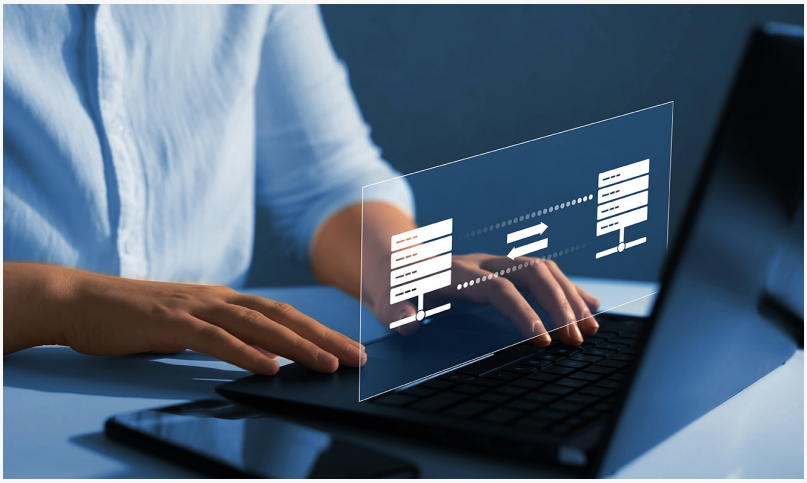

Ransomware Chain Attack

OCEAN, NJ, USA, July 26, 2022 /EINPresswire.com/ -- For anyone who thinks that cyber protection is being overblown by security firms who have a vested interest in offering their services and products, it might be instructive to take a close look at what happened in the recent 'See it in the Eyes' Ransomware attack. When the attack occurred, it took approximately 16 hours to detect it, and it involved the Phobos Ransomware, aka Eight Virus. The victim, a jewelry company were unable to open their business the next day following the attack. All servers with files, emails, and databases were encrypted.

By the time a resolution had been reached, 71 days passed, and it cost the owners $25,000 to rebuild entire digital presence, the virtual servers, and the applications which used to processes in-store and e-commerce orders. An estimate of $275,000 paid out in as soft costs, and $25,000 which was paid directly to the attackers. Making matters worse, the backups for the applications and data were also encrypted, because they were not stored offsite for safety, but on the same system as the business-critical files.

Many people also have come to believe that Cyberattackers primarily target big corporations, because of the potential for big money being paid out. This example should totally refute that kind of thinking, because the targeted company was a small jewelry store in Georgia, with only

Thirty employees. The company was targeted because its cybersecurity measures were inadequate, as can be seen by the fact that backups were located on-site and on the same network as the primary data and networking mis- configuration.



Ransomware Chain Attack - BEC

TIMELINE OF THE ATTACK

The attack occurred on a Sunday at 6:45 on the evening of April 10, 2022, when the store was closed. The servers were completely unprotected and vulnerable to attack. The encryption was carried out overnight, and by Monday morning, the IT manager called in to report a blue screen on the VM host, which led her to think there was a problem with the operating system. They contacted 2Secure Corp, which had previously helped them migrate their email system to a current system, and described the issue.

All workstations were affected, as well as the virtual host server and the Network-Attached Server (NAS). Action taken by 2Secure Corp was to reinstall Windows in the hope of recovering access to the servers. By Monday afternoon, it was apparent that the client should contact their insurance company, as well as the FBI to begin an investigation into what was happening. Tuesday, recovery has started by the Forensic company by shipping drives and software utility to image the servers and start analyzing the cause of the breach.

All servers were imaged and the images were shipped back to the forensic company headquarters for further analysis. On Wednesday, a temporary email Microsoft Exchange was setup, so the victimized company could have some communication with clients and business associates. It took until June 23rd before the company had recovered to the point where they once again had a fully functioning system and could carry on business as usual.

However, even then all was not normal, because during the 71-day period of recovery, the company's website suffered an attack and was significantly defaced. Clearly, the website also lacked adequate protection from Cyberattack, and was just as vulnerable as the host network for the business. When files were recovered, it was also found that many emails had been corrupted and had Malware included in them which could be capable of launching a secondary attack. All these were successfully removed, and any further disaster was thus thwarted.

So how did the Phobos Ransomware enter the victim's system? Eventually, it was discovered that an improperly configured firewall left a port open to attack, and this provided the entry point for the Ransomware to penetrate the system. The firewall had actually been configured with security in mind, and some of the ports were changed so as to thwart a Cyberattack. But Cybercriminals

are much more persistent than to skip over a firewall which has unconventional port assignments.

They will go through the entire port range until they find something that appears vulnerable, and that is exactly what happened in the case of the firewall for the jewelry store. This should point up the fact that nothing and no one is immune from attack, because any really committed Cybercriminal will keep working until they find a way to breach your system. The fact that saves most companies is that cybercriminals just haven't heard about you yet, and haven't focused on carrying out any attack on your system.

THE LINGERING DAMAGE
Any business large or small, which is forced to shut down for over two months will suffer serious financial loss. In addition, any breach like this quickly becomes public knowledge and results in a loss of confidence in the company that was attacked. Casual observers feel that the company lacks adequate security measures, and are hesitant to do business with them. That loss of confidence translates to ongoing loss of business for a company, because customers prefer to patronize more secure companies.

To continue to read the full release, please follow this link:
https://www.2secure.biz/2022/07/see-it-in-the-eyes-ransomware-attack-case-study-2/

Yigal Behar
2Secure Corp
+1 646-560-5083
cyber@2secure.biz
