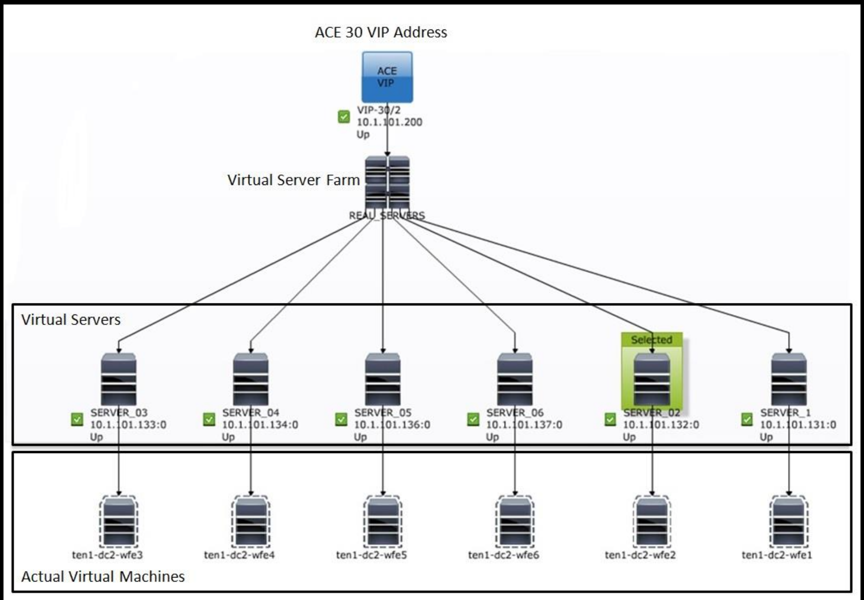
RANSOMWARE ATTACKS ONLINE CASINO

For several online casinos, their business usually peaks as their online gambler’s come home from work and log into their favorite blackjack tables or Texas HoldEm. However, on Tuesday February around 5:00PM the house did not favor the odds. This particular casino that has tens of millions of dollars upon virtual transaction data, several thousands of gamblers profiles, and even more millions that has been invested into the infrastructure. This casino was hit with a ransomware that had brought a very thriving online company to a directly encrypted cyber-crime scene.

The master mind criminals behind the direct attack, could have not asked for a better target. The, legal, online casino that is located outside of the United States just happens to be one of a few of the largest operations in the field of online gambling and other entertainment business. However, the casino wishes to remain anonymous for the safety of their organization as well as the protection of their users, they were provided with an extremely rare taste of high-stakes ransomware attacks that had served as a cautionary story for any company.

While ransomware was upon their radar, the business, in which uptime is very crucial for their success, and any DDoS attacks as well as APT attacks had always been upon their brink of security concerns. To be on the clearer side, the casino had invested extensively onto security protocols that where in place and other tools in order to aid in the protection of their network.

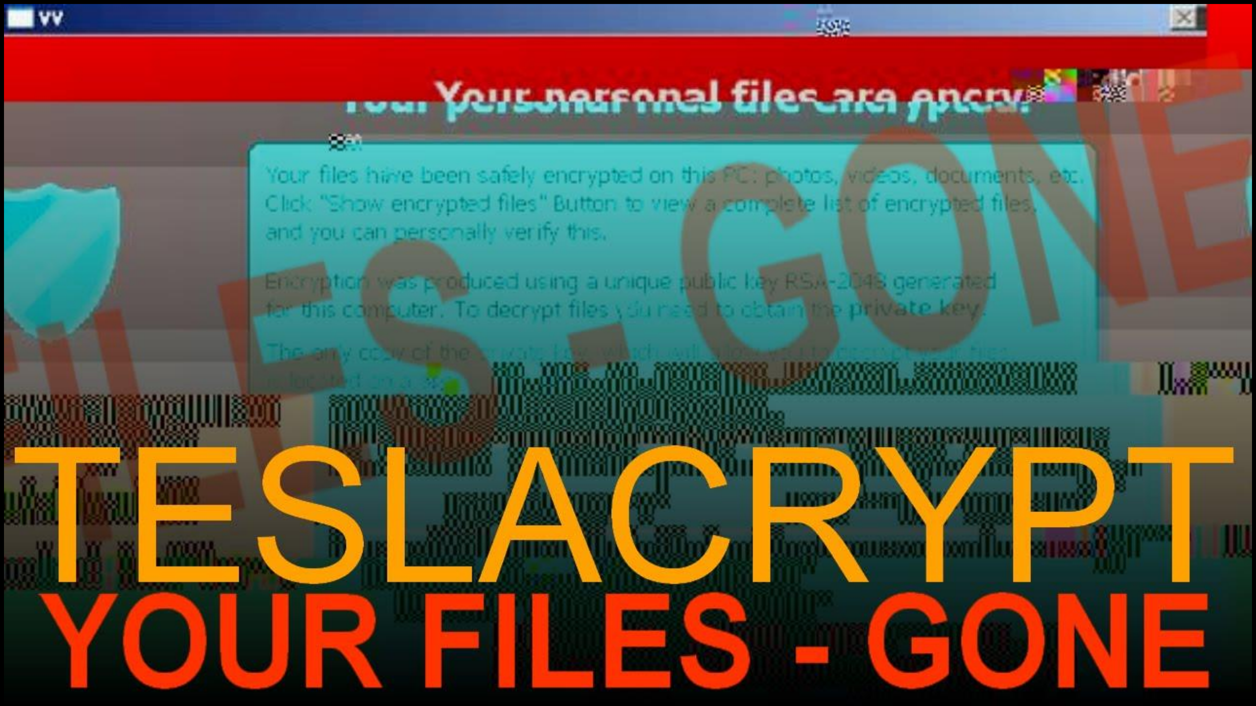
This casino in which holds 1,000 employees, possess 2 extremely large infrastructure data centers, and also a large cloud infrastructure. Relaying upon heavy security, the casino utilizes a firewall from a reputable top-tier supplier. The data center security comes from that of another leading vendor and possess the clients AV (Antivirus) protection had come from a mixture of other leading providers. This was also contracted to operate in a real-time network in order to perform the correct monitoring from yet another outside service provider.



Needless to say, I believe it would be considered an understatement in which if someone said that security was of their top concern. And protecting thousands of user's data, as well as the casino's infrastructures as well as revenue, is of the utmost concern.

However, with that being stated, there are no perfect security solutions. And upon that Tuesday evening as their usual gamblers were logging on, their servers went through a whirled and then spun into a massive overdrive. This casino soon learned the most extreme way, that nothing is bulletproof.

The attack of the ransomware started a 5:00PM with the starting point of the hook of a simple Phishing email, which possess a bogus invoice that had been sent to another external consultant that was working in-house. While the software was working just behind the casino's firewall onsite, the consultant had received an email in which had a subject line "Requested Receipt ID: 084C9F"
The consultant paid no attention to the email, and didn't suspect anything wrong with the email, or the emails attachment that had been labeled as "segreteriagenerale_request_084C9F.zip.js".
In this section, "JS" of the attachment's extension was obfuscated by the attacker. And naturally, the JavaScript was that of a malicious attachment. However, in this case, the payload was in fact the "TeslaCrypt 3" ransomware.



Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

Utilizing a Windows 7 Sony Laptop, that was bestowed to him by the casino, the consultant proceeded onto opening the email message and even double-clicked upon the email's attachment. Thus leading onward to unleashing the horrifying ransomware. Completely unaware by the casino, was the fact that their consultant's laptop did not possess any security software in order to aid in preventing this from happening. Moreover, making things even worse for the company, the consultant's laptop was also misconfigured with "C:\Users\username\Public" folder that had been wrongly setup in order to be completely shared upon the casino's network.

With this small unprotected laptop, the ransomware had completely attacked the notebooks default "My Folders" directory and then proceeded onto encrypting those files. This only took a matter of minutes. The consultant had noticed that he was unable to open any of the documents he just created, and they had new extensions that included; .XXX, .TTT, and even .MICRO in which had been appended onto those documents. Concerned about the technical issues bestowed upon his laptop, he called the casino's IT department in search of answers. While awaiting the phone call, he was searching for answers on his own in Google. After a half-hour of waiting, the IT department finally contacted him and instructed him to unplug his Ethernet cord as fast as he could.

The laptop in which belonged to the consultant was also linked to another 80 desktops and laptop computers. All of which were linked by a network of another 15 shared servers within the casino's operations. The servers had contained a full mixture of critical network elements that consisted of the companies Active Directory Domain Services, and even the companies treasure trove of several applications and valuable data.

Within just 60-Minutes, the casino's 3rd party security firm, that was based in London "DarkTrace", had not only received information that the casino was dealing with a massive ransomware attack, but had already detected it before the cyber security firm did. The casino's network, end points, and even the traffic was just busting open with odd behavior.

During the hour of damage, the casino thought that the ransomware had been contained strictly to the laptop in which was by now quarantined from the rest of the network. The damage that had been emitted from the TeslaCrypt 3 had also infected the primary laptop of the consultant files within the "C:\Users\username\Public" folder. However, the casino could not have been any further from being wrong.

While the casino's IT team was performing a local triage, the DarkTrace technicians had noticed something even bigger. DarkTrace noticed there was in fact a tsunami of network activities as well as anomalies upon the casino's network.

Dave Palmer, a directory of technology working for DarkTrace, had stated that they were watching the ransomware work its way through the network and scanning the file directories in an alphabetical order. They had spotted the unusual network traffic and the executables zipping around the casino’s network at lightning fast speeds. This caused a massive spike inside of the number of files that were being touched. The failed passwords attempts became off the charts, and they were also seeing traffic, that was coming into the network, from other outside domains. Such domains that no one from the company had even visited before.

Impressively, the ransomware had worked its way into the Hitachi shared storage server from inside the consultants main public file “C:\Users\username\Public” folder.

Now, time is extremely crucial for this thriving online casino. And this attack is not the kind in which you engulf yourself into a cup of coffee while you work out the situation at hand. Both DarkTrace as well as the casino’s IT division where working as fast as they can in order to cordon this horrible ransomware, and ultimately prevent it from infected the rest of the server, and limiting the TeslaCrypt 3’s ability to encrypt even more endpoints.

However, the casino’s nightmare is not of completely unique on its own. If fact there has been other reports of similar incidents of a successful “CryptoWall”, “TeslaCrypt”, “Pyta”, and even “Locky” ransomware attacks that has been steadily upon the rise of cyber-crime activities. Top security researchers at Cisco Talos is informing the public that they are seeing a large spike that is targeting attacks on hospitals as well as other niche industries that leads onto spear phishing and other forms of spam attacks.

As we look at past attempts of non-ransomware attacks, they happen cautiously and quietly.

However, ransomware is just the opposite. The main goal of a ransomware infection is to strategically grasp a stranglehold upon the respective organization as quickly as it possibly can. Then it goes on a hunt. It hunts down and proceeds to encrypt as many files as possible while utilizing as much of the organizations bandwidth as possible.

For the cyber-defense company, DarkTrace, the casino's ransomware was just a typical attack. Typically, other companies utilize a temp, contractor, and other suppliers such as 3rd party services in which they are plugged into a gap. Loaner laptops from companies are seldom operating on the most recent operating system and fail to have all of the patches up-to-date.

To prevent this from accruing again, the company is now double checking the correct access privileges upon every computer and server, while exercising extreme discretion when the time comes for others to have any access onto the back end. The casino is also spending more time on provide more education onto their employees and informing them on how to spot "Phishing" emails.

Sources: ThreatPost { } BleepingComputer { } Windows 7 { } DakrTrace { }