WannaCry Ransomware Worm

CYREBRO IR Case Study

North American Casino

Incident Summary

The CYREBRO Digital Forensics and Incident Response (DFIR) team initiated an investigation for a large North American casino after CYREBRO's SOC identified a network traffic spike of Server Message Block (SMB) connection (port 445) to external IP addresses coming from multiple hosts. The team conducted a swift investigation to minimize the impact of what looked like a case of vulnerable machines (point of sale endpoints) being exposed to the internet, leaving the casino's environments susceptible to infection.

The Attacker's Initial Access Vector - EternalBlue Exploit

One of the casino's NRT machines (POS endpoint), which was running on Windows 7, was exposed to the internet through SMB version 1 protocol, leaving it vulnerable to the EternalBlue exploit. The attacker was then able to exploit the vulnerability and gain local system privileges on the compromised host, obtaining full control over the machine. At this stage, the attacker deployed botnet binaries and scripts, and began to spread laterally to other vulnerable machines, clearing a path for the WannaCry infection.

Potential Consequences
of WannaCry on a Casino (without CYREBRO)

Casino operations start and end with financial transactions moving from A to B, making them an attractive target for attackers. These are some of the consequences of an attack of this type:

FINANCIAL LOSS: This casino was hit with a WannaCry ransomware worm, infecting NRT (ATM) machines, and risking customers' CC information as well as other personally identifiable information, potentially leading to both financial losses for the casino as well as the customers.

SIGNIFICANT DOWNTIME: Dealing with the incident and removing the WannaCry worm requires the affected machines to be shut down for some time. Systems and networks need to be isolated to safely enable containment and purification. These two situations can lead to signification operational downtime, impacting the casino's services and causing reputational damage and revenue loss.

SPREAD OF INFECTION: The attack originated from an unsecure configuration change of an NRT (ATM) machine, exposing it to the internet by adding a secondary public NIC (Network Interface Card), allowing the attackers to exploit the machine externally and infect it. The WannaCry ransomware worm is designed to spread rapidly across networks and exploit vulnerabilities, infecting as many machines as possible, further worsening the incident.

CYREBRO DFIR Investigation and Threat Eradication

CYREBRO was monitoring and collecting logs from the casino's network and identified an unusual network traffic spike. This triggered CYREBRO to initiate an investigation, revealing the presence of the notorious WannaCry ransomware worm, which had infiltrated the casino's environment through vulnerable machines exposed to the internet.

The primary focus was to identify patient zero from which the infection spread throughout the environment.

With CYREBRO already in place as the casino's SOC solution, once the initial network traffic spike of SMB connection was detected, the SOC was able to immediately begin investigating the threat. Since the casino was connected to the CYREBRO SIEM and was forwarding logs to it, the investigation process was substantially accelerated.

A rapid response is important because even slight delays in an investigation can have significant consequences. For example, information may be missing because attackers clean their footprints to harm the investigation process, or ransomware can have a specific trigger it waits for to then be executed, unleashing its destructive payload.

CYREBRO traced the progression of the malware, uncovering how the attackers gained access and exploited the compromised machine using the Server Message Block (SMB) exploit "EternalBlue" and were able to manipulate system data.

The initial attack vector stemmed from an outdated Windows 7 OS with several vulnerabilities. The addition of an external NIC (Network Interface Card) exposed the machine to the web, leading to infection.

The CYREBRO DFIR team was successful in eradicating the remaining malware samples in the environment, including malware samples that had the potential to steal resources for Bitcoin mining and compromise regulated patient records.

Remediation and Reinforcement

After completing the investigation and purifying the casino's network from infected machines and attacker footprints, CYREBRO provided the casino with several recommendations to strengthen its security posture moving forward.

The main recommendations CYREBRO provided were:

1

ONLY ALLOW EXTERNAL ACCESS WHEN NECESSARY

Unnecessary open ports and internet access introduces an organization to countless threats. If it's not necessary, external access should always be closed.

2

UPDATE AND PATCH ALL LEGACY COMPUTING

Legacy machines are not safe but if they must remain in the organization, updating and patching them must be a routine practice.

3

SUPERVISE 3rd PARTY VENDORS

Avoid third-party vendors implementing untested changes in the production environment without proper controls/guidelines.

4

EDR DEPLOYMENT

Fully implement and deploy an EDR across all devices in order to increase visibility and reduce risk.