CASE STUDY:

REGIONAL BANK

Concerned about unauthorised network traffic, a regional bank in the MD/DC/VA area contracted GBMS Tech Ltd to monitor the banks various security systems.

GBMS Tech Ltd uncovered a **bot net** being used in a denial of service attack. A common tactic used to force unauthorised entry.

Thanks to **Trident CMP**, **no breach was made**.

GBMSTECH

SECURED BUSINESS CONTINUITY

www.gbmstech.com

GBMSTECH

SECURED BUSINESS CONTINUITY

Best in class cyber security to combat **escalating threats**

Cybercriminals are finding ways to bypass layered security defenses, including those of highly IT security conscious organisations in more regulated industries such as financial services and healthcare.

Businesses need to understand how to defend themselves against these attacks. Yet, often the details of how the breach was conducted are not known or not disclosed to the public.

As these attacks are escalating, GBMS Tech, Ltd. a global cyber security consultancy works with its customers to provide best in class cyber security services and products. As such we have developed our Trident product line to create a multi-layered approach to cyber security. Our Trident product line consists of four approaches to cyber security defense as labeled below.

Introduction

A regional bank in the MD/DC/VA area contracted with **GBSM Tech, Ltd**. to install and monitor two Trident – Network Protection devices in their **corporate network and data center**.

The bank was concerned about unauthorized network traffic in their system and felt that there was not an adequate way for them to quickly detect the traffic and respond to it.

Until GBMS Tech, Ltd. was brought into consult the bank had augmented the cybersecurity expertise of its Computer Emergency Response (CERT) team with a host of firewalls, intrusion detection, vulnerability management, and log retention. However, the process in which alerts were generated was cumbersome and often led to delays in reacting to alerts often by days. The alert handoff from the alerting system to IT services took time and often involved miscommunication, leaving the attacker with unrestricted access to any resources they were engaged in.

On any given day the bank various security systems, firewalls, routers, servers, and other various hardware/software can generate up to 10 million lines of logs and alerts to review. Knowing that their staff was unable to determine which lines of logs/alerts were the most serious and what needed to be addressed right away the bank worked with GBMS Tech, Ltd. to use the GBMS Tech Trident – Network Protection to pass all the alerts and logs to the GBMS Tech data centres strategically placed around the word. Once the alerts are successfully passed to the GBMS Tech data centres our Security Operations Team (SOC) can review the alerts in conjunction with our machine learning algorithms to develop a pulse of the banks network traffic and reduce the alerts/logs noise by an immediate 95% of normal traffic.

Reducing the noise allows for the SOC analysts to convert any remaining alerts/logs into actual events that need to be researched. Upon an indication of finding an alert that has an immediate need to be acted upon the SOC team will immediately reach out to the appropriate resources at the bank to inform them of the potential breach/alert and what action we recommend that can be taken.

In most client settings GBMS Tech, Ltd. will work with the client to make sure the actions we recommended have been completed and then retest for the alert. In rare instances GBMS Tech, Ltd, also acts as the IT resource and can take responsibility for completing those actions. With the bank our responsibility is to work with the bank IT staff to confirm that they have implemented the fix we recommended and retest the alert to determine is the fix has made the correct changes.

Once those actions have been completed we close the ticket on our side and resume normal day to day alert/logging monitoring.

Trident – Network Protection

Trident Network Protection consist of an appliance device installed onto the banks network and allowed using a SPAN/Mirror port the ability to monitor all the network traffic that is being sent through the banks network.

Typical Trident – Network Protection standards of practice call for a two-week baselining period in which the GBMS Deployment team will examine the network traffic and learn the system.
The Trident – Network Protection devices were installed at both the datacenter and bank headquarters IT room. As all Internet and network traffic was routed through these locations therefore the Trident – Network Protection product could examine all traffic travelling through to the Internet from each bank branch.

What is a **Bot?**

A bot is a malicious software program often installed on a machine unknown to a user.

The often enables cybercriminals aka hackers to control your pc to distribute spam, phishing attacks, spyware, malware, or attempt unauthorized access to other machines.

A botnet is a collection of bot infested machines.

What is **Port 3389**

Port 3389 is registered for Microsoft WBT server, used for Windows Remote Desktop and Remote Assistance connections. Also used by Windows Terminal Services.

Port 3389 is vulnerable to Denial of Service attacks in which a remote attacker can quickly cause a server to reach full memory utilization by creating many normal TCP connections to the port. Connections will ultimately timeout, but a low bandwidth continuous attack will main the server at maximum memory usage and prevent new connections from legitimate sources from being made.

Legitimate connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

Often IT systems administrators will allow port 3389 from a vital server to pass through a firewall to have that port open so that they or another resource may access the server in an emergency to fix any issues that may arise.

This is considered bad security practice and ports being passed through a firewall should be limited or at a very minimum be changed so that another port number is being used on the outside of the firewall to prevent bot attacks.

The Attack

Shortly after **GBMS Tech Ltd.** installed and activated our Trident – Network Protection devices at the banks data centre we noticed many connections being attempted to an internal server on port 3389 from around several thousand different external sources.

While it is not uncommon for the SOC team to see connections to port 3389 from external sources, the SOC team was initially concerned about the sheer number of bad login connections that were being attempted.

In the span of 4 minutes, there were over **3.5 million connection attempts** made from 10,000 external sources. Further review of these sources indicated that most of the IPs were from legitimate companies that were infected with bots to create a large botnet.

Our SOC analyst immediately opened a case and let the GBMS CERT manager know the details of what was being reported to the GBMS SOC. Once in possession of the details the CERT manager immediately called the IT Support manager for the bank and let him know what was going on.

The IT Manager informed the CERT manager that they were in the middle of troubleshooting their web server and that the online banking web portal had gone down unexpectedly just a few minutes before. With the information about the port 3389 connection attempts and all the failed logins, the CERT manager indicated that there was a denial of service attack happening to that server and that the IT manager should have his team turn off port 3389 as a pass through on the firewall preventing anymore connections to that server and any other server that could be potentially using that port.

Once port 3389 was removed as being accessible from the outside the firewall the memory usage on the web server went **from 100% to 21% as was normal utilization.**

Further forensic follow up from the GBMS CERT team indicated that a **breach never occurred** and all the connection attempts were denied with bad username and password.

Aftermath and Conclusion

In the post Forensic and Incident follow up report GBMS noted to the bank that several bad practices had been followed by the bank and recommended immediate action to prevent further denial of service attacks.

The following actions were recommended:

- Permanently remove port 3389 from being used as outside of the network access.
- Consider deploying a reverse proxy for any server from the internal network that must be accessed from the outside world.
- Implement IDS protocols on the banks firewall system that will reject large quantities of duplicate attempts to access internal resources.
- Conduct an external penetration test to develop a plan for any future breaches and vulnerabilities that can still be exploited.

During our 3-month post assessment of the incident we noted in the GBMS SOC system that connections attempts to port 3389 were near nonexistent and that the correct use of a penetration test with the proper fixes increased the cybersecurity posture of the bank

Conclusion.

In conclusion GBMS Tech Ltd is very pleased with the outcome of this incident, though it could have been potentially far worse had an attacker actually gained control of a system or had been flooding the actual firewall to prevent an update.

Attackers have become very sophisticated and it's up to organisations like this bank to seek out and retain the best support they can get to keep their systems up to date and secure.

GBMSTECH

SECURED BUSINESS CONTINUITY


enquiries@gbmstech.com


+44 (0) 207 993 6949


www.gbmstech.com


1Berkeley Street
London
W1J 8DJ