CYFIRMA
DECODING THREATS

INDUSTRY
Retail

SOLUTION
Threat Visibility & Intelligence and Cyber Incident Analytics

BENEFITS
Prioritized recommendations to mitigate the impending attack and corrective actions to detect any further compromise

Retail Conglomerate turns to CYFIRMA for Advanced Threat Analytics Outside the Wire

The client is a Retail Conglomerate operating F&B, convenience stores and supermarkets in multiple locations across Asia. CYFIRMA Threat Intelligence team witnessed a growing number of state-sponsored hackers from different countries targeting the retail sector. The heightened interest among different threat actors looking to inflict financial and reputational damage was a cause for concern for the Retail Conglomerate. The retail sector has always been targeted by hackers as its nature of business involve the direct handling of customer data and financial records, both highly valuable assets in the dark web marketplace.

THE THREAT ACTORS AND THEIR METHODS

CYFIRMA Threat Visibility and Intelligence platform showed conversations picked up from Hackers' groups, deep and dark webs, and closed communities. They cast the light on a particular group using Phishing and social engineering attacks to access private data. CYFIRMA's observation showed the group using SNS (Amazon Simple Notification Service is a notification service for the mass delivery of messages) to approach the Retail Conglomerate engineers and attempted to compromise their credentials in order to get IP details.

CYFIRMA's threat intelligence also further revealed the Retail Conglomerate's point-of-sale terminals were susceptible to malware intrusions and brute-force attack. The threat actors were identified as 'Stone Panda' and 'Red Apollo'. Further analysis showed the hacker groups intended to utilize several methods of attack.

Power Shell: The group has been known to use PowerShell to perform various actions which include information discovery and code execution. One such example is Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet.

Credential Dumping: The group also use credential dumping to obtain confidential personal information from the target machine. It would further utilize this information for lateral movement across the network and access restricted information.

Remote System Discovery: It is used for lateral movement from the current system across the network. Information such as IP address, hostname or any other logical identifier on a network can be found by using RSD.

Remote Desktop Protocol: RDP has been a common technique used by Stone Panda to move across the victim's network.

CYFIRMA's analysis also showed the threat actors intention to use two types of malware, ChChes and Poison Ivy, to infiltrate the Retail Conglomerate's IT systems.

ChChes malware was disguised as word documents and once opened, it would execute in victim's machine.

Poison Ivy malware was a backdoor malware designed to provide covert access to a compromised system, exfiltrating data and download additional payload.

THE SOLUTIONS AND REMEDIATIONS

CYFIRMA's Threat Intelligence immediately provided a set of recommendations to mitigate the impending attack, and corrective actions to detect any further compromise.

MITIGATION

- Perform a review to assess the impact to the IT environment upon removal of PowerShell.
- To counter credential dumping, monitor/harden access to Local Security Authority Subsystem Service (LSASS) process and Security Account Manager (SAM) tables in Microsoft Windows operating systems.
- Disable or restrict NTLM traffic.
- Block malicious software and redundant systems which can be assessed remotely to gather information using whitelisting tools like AppLocker or software restriction policies.
- Disable RDP service if not required and enable firewall rules to block RDP traffic.

DETECTION

- Have a policy set to define execution of PowerShell through command line or registry. It would help in detecting malicious use of PowerShell.
- Enabling PowerShell logging capabilities help in getting the details when PowerShell is executed for further analysis.
- Monitor processes and command-line arguments for program execution that may be indicative of credential dumping.
- Monitoring of processes and command-line arguments for script execution and its behavior.
- Monitoring of user accounts logged into systems using RDP and analyze the logs for any anomalous activities.

With the above recommendations, the Retail Conglomerate was able to avoid heavy financial penalties and reputation loss. The advantages of having quality cyber intelligence have been significant, giving the client increased confidence in how they can run and grow their business.

To learn more, visit **CYFIRMA.COM**

About CYFIRMA

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provides the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks.

CYFIRMA is headquartered in Singapore with offices in APAC, EMEA and the US. The company is funded by Goldman Sachs, Zodius Capital, and Z3 Partners.

CYFIRMA
DECODINGTHREATS

twitter.com/cyfirma
facebook.com/Cyfirma/
linkedin.com/company/cyfirma
www.cyfirma.com