Data Leak Prevented:

CYREBRO Brute-Force Case Study

National Nonprofit Organization

Brute-Force

DFIR Case

Data Leak Threat

About the Company

CYREBRO launched an investigation for a large nonprofit client after the SOC detected suspicious activity on the organization's database server. This led to the discovery of an attacker who established an RDP connection leveraging an admin account through port 3389. Further analysis revealed clear signs of a conventional brute-force attack, and the CYREBRO team quickly responded to contain and mitigate the potential impacts as well as prevent any further lateral movement in the organization's environment.

This nonprofit organization has been running for 50 years, providing aid, and distributing relief on a national level. With over 15,000 volunteers, a supply chain reaching 4,000 distributors, countless files containing personal data, confidential financial details, along with sensitive donor and distributor details, a cyber-attack can cause serious damage to the organization and its continuity.

The CYREBRO SOC Solution

The nonprofit recognized the need for a SOC because of the difficulty of monitoring, correlating between, and responding to events across its siloed environments. The nonprofit chose CYREBRO because of its wide coverage, which provides 24/7 monitoring, detection, and response, thousands of proprietary detection rules and event correlations, hundreds of integrations, as well as the ability to swiftly conduct investigations while communicating simple and real-time recommendations.

The Incident: Database Server Attack

CYREBRO initially identified an alert indicating suspicious activity on a SentinelOne EDR that was installed on the nonprofit's machines. Due to CYREBRO's automated prioritization algorithms, the severity of the EDR alert was raised and the SOC immediately began investigating and uncovered a malicious file.

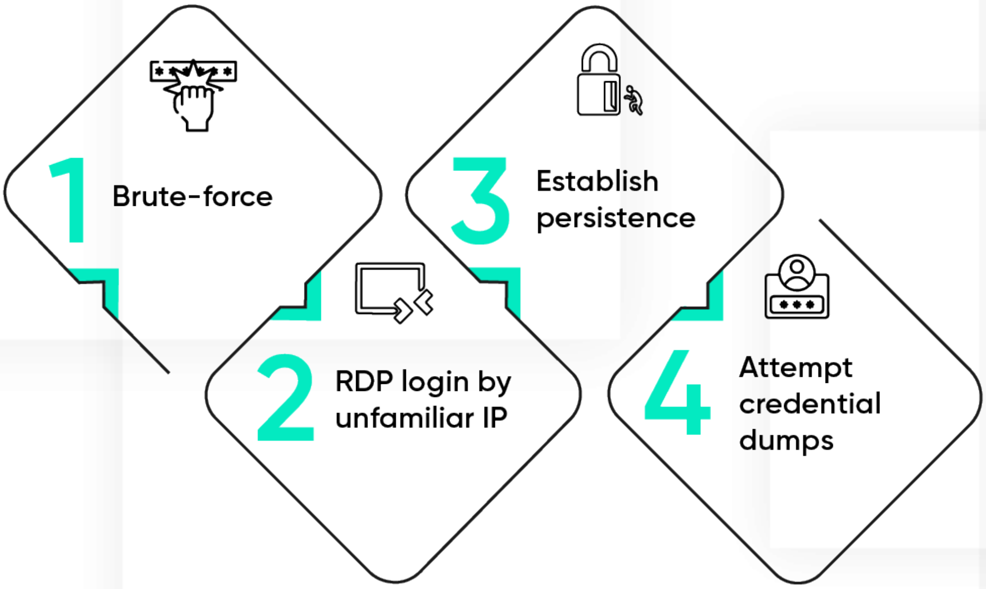
Additional suspicious activity was found surrounding the malicious file, which further escalated the severity of this investigation to critical, and triggered CYREBRO's expert DFIR team.

To get a better understanding of how the attacker first gained access, the DFIR team requested forensic evidence from the client for analysis, such as Windows events logs. They analyzed logs of the login attempts and uncovered thousands of failed logins along with one successful attempt, revealing the brute force access vector and patient zero. Additionally, the DFIR team traced a malicious RDP login from an external unfamiliar IP that was leveraging an admin user.

Further investigation revealed that the attacker connected to a database server from an unfamiliar IP which OSINT later found to be a known offender with numerous prior offenses such as brute-force attacks and web app attacks.

The attacker used different tools to attempt to deploy batch scripts to automate malicious tasks such as network scanning to reveal vulnerabilities, credential dumping, database server credential dumps, and more.

Brute-Force Attack Timeline



CYREBRO Response & Remediation

Events logged by SentinelOne and evidence that was collected directly from the infected host were correlated to determine the incident's root cause and further attacker activity.

Evidence such as Windows events logs, registry hives that show recent execution of files, MFT (the drive's master file table), and other execution evidence was investigated to provide a larger understanding of the incident and help contain and mitigate it.

To contain and mitigate the incident, the CYREBRO DFIR team first recommended that the client disable the compromised user. The team also blacklisted relevant hashes, recommended blocking traffic from outside the network from reaching the affected database server, and recommended deleting all relevant malicious files as well. All of the attacker's manipulations and backdoors were identified and closed to purify the network.

CYREBRO's Swift Response Prevents Data Leak

Once CYREBRO detected the threat and classified its prioritization, the CYREBRO DFIR team acted fast and caught up with the attacker before any significant damage could occur.

Although asset compromise was possible, there was no evidence of exfiltration of the client's assets or critical data, which could have had devastating consequences for the nonprofit, considering their dependency on donors and distributors.

Once the investigation was concluded, CYREBRO provided best practices to follow which would prevent such a time-sensitive incident in the future. The nonprofit has not been following best practices for internet-facing servers, like closing accessible and open ports, which became a major factor in this case. If port 3389 was closed, the attacker would never have been able to brute-force their way into the network in the first place.

An EDR or antivirus are vital tools, but alone they simply do not provide the visibility needed to monitor a business nor investigate an event or incident. Enlisting a capable SOC solution and integrating the organization's reporting systems into a single, centralized brain like CYREBRO's Platform provides complete visibility, enabling the earliest detection and rapid investigation when it's most needed and from any attack vector.