PROWL SECURITY
Cyber Security Services

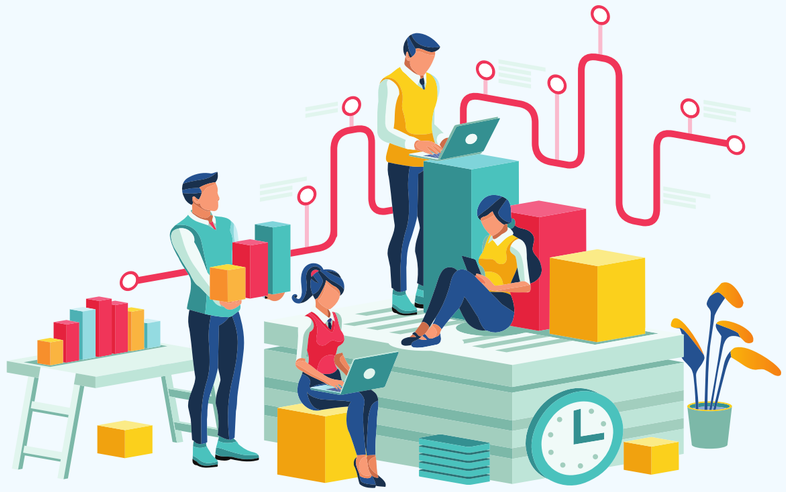
powered by:

LinkAmerica

Ransomware Attack Case Study

Prowl Security 2020 © All Rights Reserved

BACKGROUND INFORMATION



The client is a IT services company giving support to global organizations. They have over 200 employees worldwide working in their offices or remotely; our client needed visibility, control and management tools to enforce their policies.

At the end of 2019, we started giving them cybersecurity support to alert them of any malicious traffic or violation of corporate policy.

PROWL SECURITY
Cyber Security Services

Work Flow

On Saturday, April 4th 2020, a major attack was identified. At the right, you can see the steps taken to protect our client.

Total time to identify and mitigate: 2 hours

4:30 pm

Issue is identified

Our SOC Services issued an alert about a Canadian IP address trying to access a server and block access to the client's documents.

5 pm

Client is notified

Our client was notified via email and text message to verify they were aware of the cyberthreat.

5:30 pm

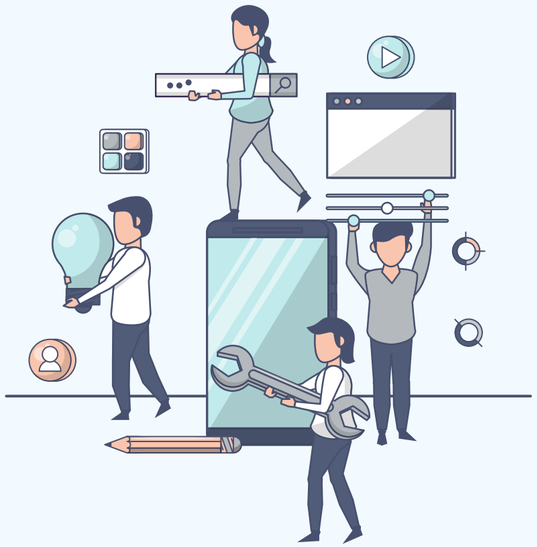
"War Room" is opened

The appropriate parties got together to discuss and identify the server.

6:30 pm

Equipment Identified and Taken Care Of

The equipment is identified and carefully turned off. Our SOC team monitored the event closely for the following 24 hours.



PROWL SECURITY
Cyber Security Services

Forensic Study

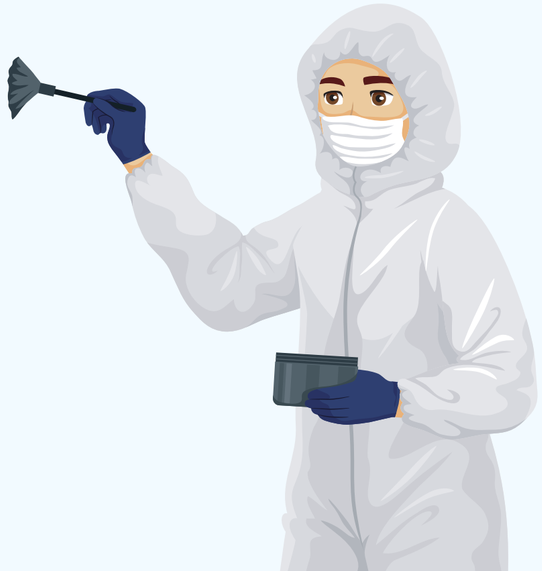
After the attack was resolved, we met with our client to help them understand more about the nature of this attack and analyze the steps taken.

1. Equipments from third parties open vulnerabilities in their network.

2. The third party server was an easy target since it didn't have security policies implemented.

3. Timing was quintessential to identify and mitigate.

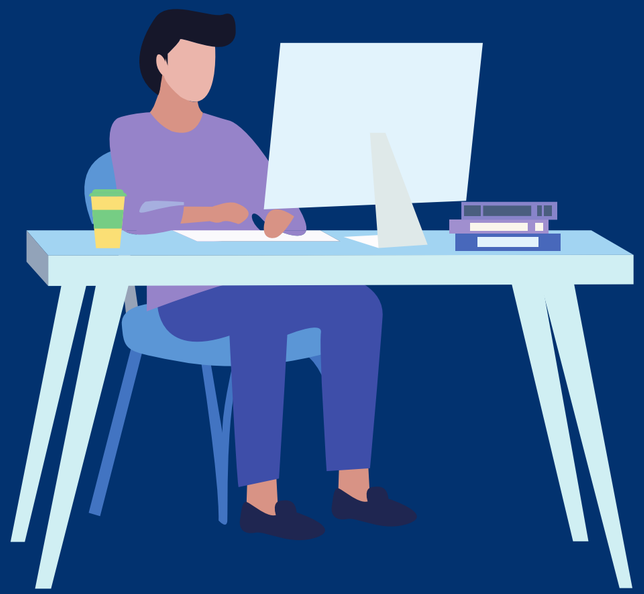
4. Notifying the right parties was beneficial and instrumental in resolving the incident.



PROWL SECURITY
Cyber Security Services

Other Attacks

As a IT services company, this was only one of many attacks our client had received.



Targeted System/Application Scan

There was a targeted System/Application Scan attack. An external IP was trying to enter one of client's ports. This IP address was recognized as a malicious IP address with a history of scanning and force brute attacks. The attack was registered back to China.

Crypto-mining

Our services were able to identify possible crypto-mining to one of our client's IP addresses. Through our database, we were able to identify the malicious website and appropriately recommend next steps to avoid harm. The attack was registered back to Nigeria.

P2P Traffic

Unlike the other attacks, we were able to identify P2P traffic from an internal host. The event triggered an alarm for potential corporate violation. We proceeded to contact the client, verify the event to either move forward with preventative measures or whitelist the activity.