Blue Bastion

Road to Recovery

How Blue Bastion Rebuilt The City of Washington's Entire Environment After a Ransomware Attack

OVERVIEW

In May 2019, a ransomware attack forced City of Washington, PA officials to take down their communication system and pay a $21,250 ransom to regain control of their environment.
A Blue Bastion investigation revealed that the cybercriminal attempted to break into the city's system 109,000 times before finally accessing the City Hall server.
The ransomware attack knocked out phones and emails for city workers for more than two weeks.

To restore the city's network and all of its data, Blue Bastion & Ideal Integrations needed to create a new network, provide new workstations, and prepare data to be introduced in a clean environment.

This approach allowed Blue Bastion to create a Security-as-a-Service solution designed to monitor the city's environment for threats and Indicators of Compromise (IoC) 24/7/365.

"Within 45 minutes of our initial phone call to Blue Bastion, a representative was in City Hall to discuss a plan for moving forward and fixing what seemed to be a dire situation."

Lynn Galluze
Computer Systems & Website Coordinator, City of Washington

Blue Bastion

APPROACH

At 10 p.m. on Saturday, day zero, the GlobeImposter 2.0 ransomware struck the City's computers. The attack encrypted the majority of the city's computing resources, rendering them offline and unavailable. Four days later, city officials contacted Blue Bastion for help. The team worked with the representatives and FBI agents to investigate, recover, remediate, and insure operational capacity.

While a negotiator worked with the attackers to obtain the decryption keys, Blue Bastion followed the four recommended phases of NIST SP 800-61:

- Preparation and fact gathering;
- Detection and analysis;
- Containment; and,
- Post-incident activity.

In the preparation and fact-gathering phase, investigators examined the encrypted computers and imaged them as potential evidence. Attacker's .exe and .bat files were located on the city's servers that had opened remote desktop on the Windows firewall and enabled the attack.

To execute containment, eradication, and recovery, the city's internal infrastructure team and Blue Bastion decided to execute several plans simultaneously: rebuild and recovery. Infected hardware was segmented off the network. Ideal Integrations provided replacement hardware to rebuild the environment on clean hardware. Carbon Black was installed on the replacement assets and monitored to ensure no repeat infection and to contain any potential malware activity.

Analysts used the decrpytion key obtained from threat actors to restore data to the original hardware. Once restored, analysts examined and sanitized the data for any known threats. Once the data was deemed clean, it was moved to the new hardware for the City of Washington's use.

Blue Bastion

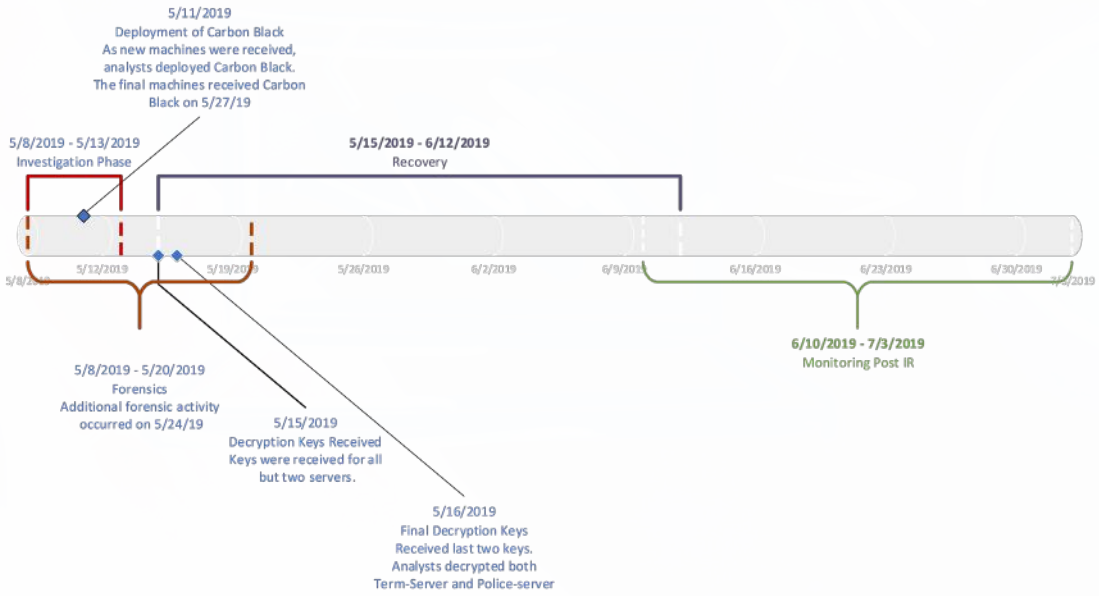
CONCLUSION

Post Incident Response, Blue Bastion continued to monitor the City of Washington's endpoints, using Carbon Black, to prevent further attacks. During the initial recovery, the devices run in a restrictive Incident Response mode; once the IT team is confident that the attack concluded, the software will be aligned to the communication needs of the client.

The Blue Bastion team continues to monitor the network using GuardiCore and Carbon Black Live Query. A centralized log management solution, Graylog, also has been introduced to permit capture, storage and real-time analysis of the computer logs generated by each device on the network.

To prevent future compromise, Blue Bastion continues to work with the City of Washington to ensure their security needs are met, not only with Carbon Black, but also with GuardiCore and Graylog.

Timeline of Events



Blue Bastion