Beebe Healthcare Stops Cyber Attack With Red Canary

CHALLENGE

Beebe Healthcare needed the ability to defend against advanced threats as they entered its network and compromised endpoints.

REQUIREMENTS

- Extensive, accurate, and timely detection
- Rapid and easy-to-use response tools
- Hands-on support to supplement internal staff

SOLUTION

Red Canary's Managed Endpoint Detection and Response (MEDR) helps Beebe Healthcare secure its endpoints against attacks as they happen. Because Red Canary's security analysts continuously monitor and analyze endpoint activity, Beebe is instantly notified of threats and able to quickly stop them.

SNAPSHOT

Beebe Healthcare is an award-winning 210-bed community healthcare system with seven locations serving Sussex County in southern Delaware. It offers a wide array of inpatient, outpatient, emergency, and diagnostic services. When the hospital became the victim of a rapidly advancing zero-day malware attack, Red Canary was on hand to instantly notify the hospital and help prevent the attack from spreading.

MORE BOOTS ON THE GROUND

Beebe Healthcare has been able to multiply its security operations with Red Canary. The Managed Endpoint Detection and Response (MEDR) solution brings a team of deeply technical experts that the hospital can rely on to monitor and investigate potential threats across its endpoints. These analysts identified a never-before-seen attack as it began. Red Canary collaborated with Beebe's security, network, and operations teams to shut down all endpoints and stop the attack. Rapid response prevented the threat from spreading to hundreds of workstations.

TYPICAL 30-DAY PERFORMANCE

8	threats detected that bypassed existing security tools and processes
1,123	potential threats reviewed
3x	resources due to Red Canary's Security Operations Center

red canary

DIGGING DEEPER

Time Is of the Essence

In one dramatic incident, an employee downloaded and opened an email attachment that was infected with malware. Red Canary's behavioral detection technology quickly identified the malware and notified hospital security staff. It soon became apparent that the attack was a previously unknown variant. Worse, it included a network-spreading capability and propagated to 47 devices in 7 minutes.

Red Canary escalated the alert and worked with the hospital's team to isolate the affected endpoints. Quick action spared hundreds of workstations from falling victim to the attack. Clint Perkinson, Director of Information Technology, said: "It would have hit all our workstations if Red Canary had not caught it in time. You can't invest enough in that type of assurance."

RED CANARY IN ACTION

Threat Detection: Stage 1

2016-01-13 17:49:45 UTC	Process spawned by msiexec.exe `c:\users\          \appdata\local\temp\o71eeouu_1.exe` fadf4c1545c540477d34394a688dfc44
2016-01-13 17:49:50 UTC	Process spawned `c:\windows\regedit.exe` 8a4883f5e7ac37444f23279239553878

Regedit was used to make change to the system via registry keys, including disabling system restore.

Threat Detection: Stage 2

2016-01-13 17:50:01 UTC	Process spawned by 91155153517e7.exe `c:\windows\system32\net.exe` b9a4dac2192fd78cda097bfa79f6e7b2

Net.exe executed with the commandline `net.exe view`. This command list other computers in the domain.

2016-01-13 17:51:59 UTC	Process spawned by 91155153517e7.exe `c:\users\          \appdata\local\temp\wvomx.exe` 74054ce33d1c8e469c20a9735ab3ace6

At the time of this detection, this process had been spawned over 95 times, each targeting a different host attempting to execute `xtakr.exe`.