CASE STUDY

MAHNOMEN COUNTY SHERIFF'S OFFICE

AppGuard Defeats Polymorphic Malware Attack, Prevents Spread to other Systems, Protects Against Future Zero-Day Attacks

Mahnomen County Sheriff's Office provides public safety services to 16 townships in Minnesota, covering 576 miles within the White Earth Indian Reservation. The Office consists of 14 full-time deputies who respond to a variety of emergencies, handling inbound 9-1-1 calls and investigating crime activity.

In 2019, the Sheriff's Office was hit by a malware attack that originated in another state agency. Once inside the Sheriff's network, it moved fast, crippling activities and rapidly jumping from computer to computer. After initial attempts to remove the malware failed, the Mahnomen County Sheriff's Office sought a cybersecurity solution that could quickly restore its systems, while better protecting its network from future attacks.

Challenges

Traditional Antivirus Protections Proved Useless

As the scope of the malware attack became better known, it was clear that the traditional signature-based antivirus software employed by the Sheriff's Office had completely failed. That's not surprising, as traditional antivirus solutions typically depend on a prepopulated database of known attack vectors. These databases are often not up to date and, even when they are, are mostly useless defending against never-before-seen zero-day attacks. As a result, they're largely ineffective and poorly suited to protect against today's rapidly evolving cyber threats.

Unfortunately, this was the case for the Mahnomen County Sheriff's Office. The malware had an unrecognized signature that didn't exist within their antivirus solution's database. This forced the Sheriff's Office into a highly reactive mode, as the malware continued on a destructive path, even attempting to access banking and other private information. The Sheriff's Office IT team jumped into action, doing ongoing scans and wiping infected machines, but the malware proved impossible to contain and morphed into different forms as it moved across the network.

Client

Mahnomen County Sheriff's Office

Deployment

AppGuard

Key Benefits

- Contained malware propagation within just five hours
- Experienced organizational savings from reduced IT service calls and cyber hygiene maintenance
- Gained set and forget protection from future, advanced zero-day attacks

A Losing Game of Cat and Mouse

An initial scan revealed four machines were infected, giving the Sheriff's Office hope that the virus could quickly be stopped. IT workers wiped every machine within the department, fearful the virus could spread to critical servers that support public services and safety, including 9-1-1 equipment.

Despite these efforts, every time a clean system was connected to the network it was quickly re-infected, with the virus skipping to new endpoints. The Sheriff's Office also rebuilt its servers, but still could not contain the attack.

This cat-and-mouse game continued for more than three weeks, with machines re-infected just hours after being cleaned. "We kept rebuilding machines and the malware would pop up again, jumping from machine to machine," said Josh Guenther, Sheriff with Mahnomen County. "IT was trying everything, but there seemed to be no end in sight."

Crippling Department Activities

From answering inbound calls to responding to emergencies in the field, much of the Sheriff's Office's day-to-day activities depend on computer-based applications. The virus' impact was widespread, hindering employees' abilities to communicate with other state and neighboring agencies and preventing critical information, such as arrest warrants, from being recorded in the department's database. To maintain critical services, the Sheriff's Office had to move 9-1-1 dispatch activities to a neighboring county.

"This outbreak crippled our department, since nearly everything we do relies on secure computer access and digital communications," said Guenther "The chain of custody was also impacted, as deputies struggled to capture information."

Solution

Mahnomen County Sheriff's Office turned to CHIPS, a Technology Success Provider and partner of Blue Ridge Networks, for help. The company recommended that the Sheriff's Office move quickly to deploy AppGuard, an advanced cybersecurity solution that defends against new, emerging, and one-of-a kind attacks that are frequently missed by traditional, detection-based cybersecurity methods.

AppGuard's patented "zero-trust" isolation technology assumes that endpoints may have unknown exploitable vulnerabilities, or even contain previously undetected advanced persistent infections and prevents all non-policy conforming actions at the process level to protect the system from every type of attack. Since AppGuard doesn't rely on scanning for known signatures or patterns to identify good from bad files, the solution provides protection without the need for constant patching.

Benefits

Malware Immediately Identified and Contained

With Blue Ridge Networks' and CHIPS' support, the Sheriff's Office deployed AppGuard in two phases. Since AppGuard isolates and protects networks, even those with already-infected systems, the Sheriff's Office could immediately install the solution on every machine. Within the first five hours, AppGuard isolated the malware and held it powerless inside each infected workstation, preventing the virus from spreading or executing any nefarious processes.

"We could tell the computers were insulated and protected because we could see the malware trying to get back into the machine without success," said Guenther. "The malware was useless once it was quarantined and isolated by AppGuard, cutting off the ecosystem it needed to carry out its actions."

Systematic Approach to Eliminate Threats, Today and Tomorrow

Once the initial crisis was over and the attack was isolated and contained, the team inventoried all endpoints, establishing a baseline so they could then undertake a clean installation of each machine. With data collected by AppGuard, it was determined that the malware was indeed polymorphic, changing signatures to stay hidden and jump from machine to machine. This is a tactic that is increasingly being employed by bad actors since traditional, signature-based antivirus solutions simply can't stop it.

With AppGuard installed, the same network isolation technology that stopped the existing outbreak now keeps the Sheriff's Office protected from future threats, cutting off attack vectors to ensure no new breaches occur, even previously unknown, zero-day attacks.

"With AppGuard, we aren't chasing signatures but rather isolating our environment, eliminating blind spots that could wreak further havoc," said Guenther. "It's a huge load off of our shoulders to know that our systems are safe from future attacks."

Fast Return to Daily Activities

Today, AppGuard is protecting the Sheriff's Office's servers and endpoints, including the laptops and devices that travel in and out of patrol cars. With AppGuard in place, deputies can now get back to performing their normal daily routines, providing a huge sense of relief for the entire department.

"The four-week period when the malware was spreading was one of my most stressful times in this office," said Guenther. "Within 30 hours of deploying AppGuard, we were back to normal operations."

In addition to a quick return to business as usual, the Sheriff's Office benefitted from a monthly reduction in IT service calls and decreased requirements for routine cybersecurity and system management, delivering significant cost savings to the organization.

"My advice to other public safety organizations: do not go through the same headaches and panic that we experienced and take a proactive stance now," said Guenther. "Get AppGuard in place immediately to prevent endpoint compromises in a true set and forget manner."

To learn more about how AppGuard prevents cyberattacks for public safety, government and enterprise organizations, visit https://www.blueridgenetworks.com/appguard.

Why Blue Ridge Networks

- Eliminate unsecure network entry points, even from unprotected, uncontrolled access points
- Isolate networks, applications, and critical operations from threats
- No need to scan for threats or constantly check alerts
- No patching or update hassles
- Trusted reputation

About Blue Ridge Networks

Based in Northern Virginia, Blue Ridge Networks is a visionary cybersecurity pioneer that provides cybersecurity for the connected world. Blue Ridge Networks' LinkGuard Cybersecurity Suite protects organizations from vulnerabilities posed by connected devices, endpoints, networks, and people. Blue Ridge solutions have protected critical operations for some of the largest US government, financial, healthcare, and other critical infrastructure customers for more than twenty years with no reported breaches.

Contact Us:

1-800-722-1168

sales@blueridgenetworks.com

Headquarters:

14120 Parke Long Court Suite 103
Chantilly VA, 20151