APPGUARD
The Malware Disruptor

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

CASE STUDY: MAHNOMEN COUNTY SHERIFF'S OFFICE

About:

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.

Situation:

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:

- Protecting against advanced cyber attacks
- Ensuring critical systems operate effectively in order to protect citizens

OUTCOMES:

- Malware that bypassed anti-virus tool was contained and propagation prevented
- Cost savings due to reduction of IT service calls and hygiene maintenance
- Greater security with less effort
- Protection against future advanced attacks including zero-day

Traditional Anti-virus Failed to Thwart Attack

As the scope of the malware attack became better known, it was clear that the traditional signature-based anti-virus software employed by the Sheriff's Office had completely failed. That's not surprising, as traditional anti-virus solutions typically depend on a prepopulated database of known attack vectors. These databases are often not up to date and, even when they are, they are unable to defend 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 anti-virus solution's database. This forced the Sheriff's

> *Once AppGuard was installed, we could tell the computers were insulated and protected because we could see the malware trying to get back into the machine without success,*
>
> — *Josh Guenther, Sheriff with Mahnomen County*

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.

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. 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.

Malware Crippled County 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.

Solution

To restore operations and prevent further damage, the Mahnomen County Sheriff's Office turned to AppGuard's advanced pre-compromise 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.

AppGuard Immediately Identified and Contained Malware

Since AppGuard isolates and protects networks, even those with already-infected systems, the Sheriff's Office immediately installed 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. "Once AppGuard was installed, 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." AppGuard enabled the Sherriff's Office to resume business, while preventing malware from doing what it wanted to do. AppGuard provides the county peace of mind knowing their endpoints can no longer be compromised.

About AppGuard

AppGuard is a cyber security company on a mission to set a new standard: true cyber protection for all. AppGuard's patented technology prevents compromises before they happen by disrupting malware activity from causing harm without having to recognize it. Unlike detection-based solutions, AppGuard outsmarts malicious actors to ensure businesses can do what they need to do, and malware can't do what it wants to.

APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us