Case Study

LANTELLIGENCE
We make the NETwork!

CYBERDNA™
A VIGILANT TECHNOLOGY

POS System Update With The Infected Code

Attack Attempt to a Large Auto Dealership

Executive Summary

The Nature Of The Attack

On a Saturday morning, an update was released by a major POS vendor that unbeknown to them included code changes placed there by an attacker that had infiltrated their own code repository. This attack would ultimately allow a malefactor to gain full credit card information from each card swipe at every customer site that had updated their specific POS system.

POS systems attacks are designed to listen and capture unprotected data in transit and others that will attempt to modify the way that the POS system works allowing an attacker to copy or re-route traffic. This specific attack was the type that re-routes traffic, it was specifically dangerous because the attacker didn't infect the individual POS system at the customer, they infected the code at the vendor. By doing that, it allowed them to significantly increase the amount of organizations they could attack in a short period of time.

Detecting the Threat

In this case, one of the Vigilant's customers, an automotive dealer with double digit dealership locations, was performing routine maintenance on their POS systems and upgraded them to the most recent infected firmware. Being tasked with the protection of customer networks for both known and unknown threats, Vigilant team is able to identify when things are not as they should be whether we know about them first or not. Once the customer finished upgrading their POS system and placed it back into service the attack went into full force.

Vigilant immediately noticed that this specific POS had two changes to its behavior:

1. In addition to sending DNS requests internally like it normally would it began sending DNS traffic outbound to Europe and
2. Each outbound DNS packet was slightly larger in packet size than the request to the Customer's internal server. *(DNS is used to point computers to host names and websites by translating an IP address to an easier to remember host name.)*

Vigilant's analyst team went to work, inspected the traffic, looked at all recorded network traffic and quickly identified that the reason the DNS packet was slightly larger is that there was credit card information from a card swipe located in clear text within the credit card packet.

"When someone uses third party software or devices like POS Systems, medical devices etc., they are at the mercy of the levels of security the vendors have built into them.

Vigilant CyberDNA can give you visibility into remote devices without needing to have any agents installed on them.

We keep your vendors honest about security and reduce your risk and we do it 24/7."

Preventing The Worst

Having a confirmation of the attack, Vigilant Analysts notified the Customer's IT staff. At that point Vigilant was informed that the Customer had just updated the specific point of sale system. Vigilant advised the customer to roll back the update from the vendor to not update the remaining POS systems and to notify the manufacturer immediately who performed their own investigation.

There were two problems here:

1. The POS vendor did not know they had been attacked and
2. With the malicious code changes embedded in the update and the update easily downloadable it is no telling how many POS systems could have been infected.

The dealership had the device removed, rolled back the update and cleaned up the network, they also contacted their vendor and informed them of the issue.

About Vigilant

Vigilant Technology Solutions is a Cyber Security Firm based out of Cincinnati, Ohio providing Security Solutions and its Patent Pending CyberDNA Network Security Monitoring Solution to Customers in the Financial, Healthcare, Automotive, Manufacturing and Construction industries.

Vigilant has been operating since 2009, is privately held (and will remain that way) with no outside investment funding.

VIGILANT
TECHNOLOGY SOLUTIONS

Detection Approach and Process

This attack was not detected by the customer's firewalls or their Anti-Virus, Vigilant CyberDNA saw it immediately and stopped what could have been a very expensive and damaging attack.

In order to detect attacks like this Vigilant places their collection devices very carefully as an attacker that is working remotely has to travel across the network at some point on their way out to the Internet. This allows for an interesting vantage point as no matter what way the attacker tries to change the way they look they still have to travel the network and are detectable if you are able to look at the data the right way.

Vigilant's approach gives immediate visibility and can inform a customer in near-real-time of what is happening in the deepest parts of their network. It's like turning the lights on late at night to see if there is a monster in the room, although you hope there isn't one whether there is one or not you at least know and can take the appropriate action. Within minutes of turning on Vigilant's CyberDNA service our analyst team was able to detect in an agent-less way that something had changed on this POS system and that something was allowing valuable data to leave.

Steps of Detection

1. An attacker infiltrated the code repository of the POS vendor.
2. Customer downloads and installs POS update.
3. CyberDNA was operating within the environment and in an agentless way detected both the behavior change of the device and the Credit Card information in the DNS packet.
4. All Firewall based IDS/IPS and detection methods available within Customer network did not detect the attack.
5. Vigilant's Analyst team notified the customer of the compromised system, the customer removed the systems from the network, cleaned them and notified the manufacturer of the vulnerability.

CyberDNA Solution Overview

Vigilant's CyberDNA Managed Network Security Monitoring Service leverages a distributed network of passive network security sensors and takes a different approach to monitoring customer infrastructure.

CyberDNA is a fully managed service with certified information security analysts pro-actively hunting for compromises and security risks in your organization. We serve as an extension to your existing team, notifying you in record time about the security events that matter, while providing clear and easy to understand recommended courses of action, so you can address the issue and get back to running your business.

CyberDNA is a fast and affordable Enterprise Security Monitoring Solution. After a 15-minute installation, you can have a detection capability that rivals many of the leading security conscious organizations. We know because our team has experience protecting some of the largest Fortune-500 global enterprises in the world.

CyberDNA will:

- Give your IT Staff more time: CyberDNA will give them specific, timely information that reduces the amount of time they need to search for issues and helps them fix the problem fast.
- Minimize your incident costs by finding attacks when they happen, not the industry average of 205-240 days after the fact.
- Give you access to a Cyber Security team at a fraction of the cost.

CyberDNA offers:

- US Based Analysts – Fully Vetted
- Unlimited Incident Response (Unique to Vigilant)
- 24x7 Full Forensic Analysis, Network DVR (PCAP) and Detection
- Full Logging and Distributed Sensors
- Elite Analyst team with White Glove Approach with full Threat Hunting
- Invisible and Undetectable protection
- 4 Free Quarterly Assessments
- No hardware to purchase
- A sentry making sure that all your defenses are working.

Vigilant Analysts

Many of our analysts are GIAC certified and carry multiple industry certifications. Our backgrounds range from small business to global Fortune-10 and span numerous industries including Finance, Healthcare, Automotive, Manufacturing, Aerospace & Defense, and Telecommunications.

Our analysts are all US Citizens, many of which hold Secret or TOP Secret US Department of Defense security clearances, and undergo extensive background, reference, and drug screen checks.

Managed Endpoint:

Vigilant's Managed Endpoint brings direct containment and remediation to your endpoints.

Features:

- Uses a broad suite of McAfee Products
- Agent points to Vigilant for added threat intelligence beyond McAfee default
- Integrates with CyberDNA for Host Verification
- Managed Host Based Firewall
- Dynamic Application Containment
- Machine Learning with Dynamic File Analysis
- Global File Reputation Checking
- Managed Client Web Control
- Endpoint Detection & Response (EDR) Capability
- Remotely investigate & respond by our Analysts
- Active Response and Remediation
- Supports all cloud environments
- Virtualization friendly, supports all major hypervisors
- Cross platform - supports all major Operating Systems

Combined with CyberDNA, Managed Endpoint provides the ability to determine the trusted nature of devices on your infrastructure 24x7 with a localized containment strategy.

Assessment Scope and Approach

The CyberDNA trial is an opportunity for customers to try our service for free to make sure they absolutely love it before they buy it. Our engineers first meet with your team to decide on the best location to install our sensor into your network. The sensor is then provisioned and sent to your site. After installation our Analysts immediately go to work inspecting your traffic for threats. If we find any active threats, we'll contact you immediately. Otherwise, on the 5th day of the trial we compile a report, which encapsulates our most noteworthy findings.

It's truly amazing the level of visibility and insights one can obtain over their network by passive monitoring. This is why we also make a significant amount of information from your sensor(s) available to you in real time on our Customer Portal.

The portal is a great place to see what versions of software are running in your environment, and which ones are out of date. You can know without a doubt when your company policies and regulatory requirements are not being met. You can even track your organization's true bandwidth usage, and explicit content usage. The customer portal is your one stop shop for managing tickets and incidents, and keeps you on the pulse of your overall security posture.

Deciding to retain our services beyond the trial is as simple as "Yes". We simply convert your existing sensor to a permanent one and immediately go to work fine-tuning it to your specific network environment and organizational monitoring needs. There's no time wasted on deploying replacement equipment, or additional software licenses to hassle with.

Contact LANtelligence team to learn how to get your 5-day free CyberDNA trial

866-510-8547

contactme@lantelligence.com