SONICWALL

CMIT Solutions of Metrolina Mitigates Cyberattack with SonicWall Capture Client

CMIT Solutions relies on SonicWall to protect their customers with complete cybersecurity platform.

Founded in 1996 as a personal IT training and support provider, the CMIT Solutions team today includes more than 900 business leaders and technical staff delivering IT support across North America. In 2008, CMIT Solutions embraced the managed service provider model, and has since focused on serving local small and medium-sized businesses (SMBs).

Business need

Due to the ever-growing threat of ransomware and other attacks, MSSPs like CMIT Solutions have faced an increasing need for an endpoint security solution offering complete centralized management and reporting for all the businesses they serve.

Solution

To mitigate cyberattacks and other threats, CMIT Solutions of Metrolina began installing SonicWall Capture Client at all customer sites. One of CMIT Solutions' longtime customers, which relies on the CMIT Solutions team to manage and support their 9 physical locations, 150 endpoints and 15 servers, had opted to deploy as part of their IT managed services a complement of SonicWall products including nine SonicWall TZ Series NGFWs and SonicWall remote access appliances. The solution also included SonicWall Capture Client, a behavior-based anti-malware solution designed to stop attacks before and during execution and remediate even after malware execution.

What happened

In May 2021, this customer was the target of a ransomware campaign that ultimately attempted to launch 4,021 attacks against 162 endpoints and servers. The attack began when an employee opened a supplier email with a malicious Excel attachment, and then enabled the content within. From this single endpoint, the attack quickly mapped the network, downloaded additional files to propagate the attack, and — through a Windows SMB exploit — attempted to move throughout the organization to other locations, attacking PCs and servers. At the same time, it attempted to move through the network to servers in other locations through Windows Netlogin Privilege Elevations. Within two minutes, the malware made over 1,000 attempts to connect to three Command-and-Control (C&C) servers in Eastern Europe.

CMIT Solutions®
Your Technology Team

> ***"Defense in depth works! We are pleased with the performance of Capture Client and the other components in our security stack in helping our team contain and recover from this attack. CMIT's mission is to prevent bad actors from destroying business value, while also providing excellent customer support and keeping systems running efficiently. But if an attacker manages to defeat our security controls, we work equally hard to be ready to recover systems and information so our clients will have the option of not paying a ransom to access their data."***

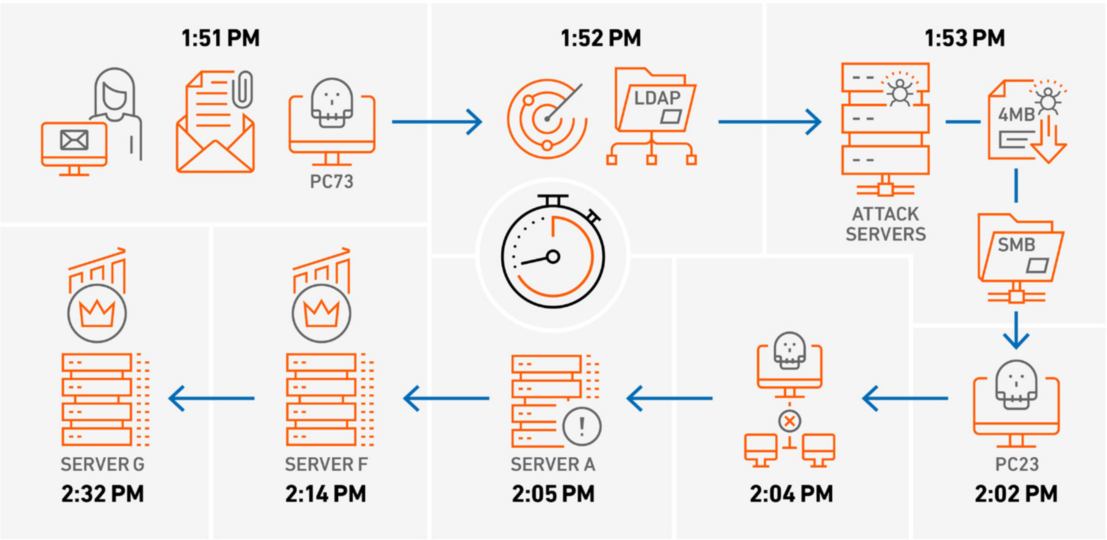
Emory Simmons
President

Customer Profile

Company	CMIT Solutions of Metrolina
Industry	MSSP
Country	US
Website	cmitsolutions.com/metrolina

CASE STUDY

4,021 Attacks on 162 Endpoints & Servers in 41 Minutes



Results

In the end, the attack failed to encrypt a single endpoint. While a third-party DNS security service initially blocked access to the C&C server, the CMIT Solutions team began receiving notifications that SonicWall Capture Client had stopped and eliminated ransomware "Win32/Teerac - f91e9b0.exe," followed by another notification that "HackTool.Win32.LAZAGNE.AC" had been stopped and removed from both a server and the original infected PC.

Ultimately, the attack was stopped through a mixture of advanced technology and the immediate response from CMIT Solutions team. CMIT Solutions immediately started their response process, taking machines offline via the Capture Client disconnect feature, dropping VPN tunnels between sites and allowing Capture Client to kill lateral movement between sites and servers. The original infected PC alone attempted 4,021 attacks on 162 endpoints and servers. SonicWall Capture Client detected and killed lateral movement, killed the ransomware, and killed the HackTool.

What They Learned

While the attack was quickly stopped, it still offered four lessons that would have further decreased the time the CMIT Solutions team needed to respond to the incident:

1. Setting Capture Client to disconnect endpoints when malware is detected would have contained the first server threat 49 minutes sooner. It would have also contained the initial infected PC 81 minutes sooner, allowing it less time to scan for other victims across the wide area network.
2. Enabling SonicWall Geo-IP filtering for source countries would have prevented the initial download of malware.
3. Setting IPS on SonicWall firewalls to block medium-level threats instead of just high-level ones would have blocked the Windows login exploit attempts.
4. Improved end-user awareness could have prevented this attack altogether.

While not a direct learning from this attack, CMIT also plans to further strengthen endpoint security by enabling the enforcement feature on SonicWall NGFWs. This will ensure only computers with Capture Client installed are allowed to access the Internet.

SonicWall Capture Client Benefits

- **Stops advanced attacks before and during execution**
- **Offers ransomware protection and remediation**
- **Gives visibility into application vulnerabilities**
- **Enforces web usage policies away from the network**
- **Allows users to easily view and manage tenant health**

Download a Free Trial of Capture Client:

www.sonicwall.com/capture-client

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com