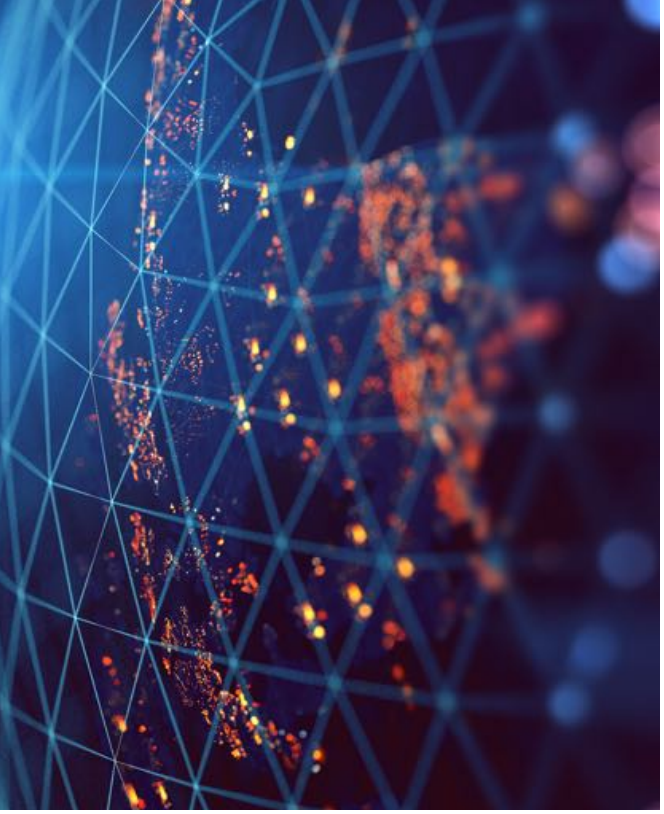


SONICWALL

A CMIT Solutions da Metrolina mitigou um ataque cibernético com o SonicWall Capture Client

A CMIT Solutions confia na SonicWall para proteger seus clientes com uma plataforma completa de segurança cibernética.

Fundada em 1996 como uma prestadora de serviços de treinamento de pessoal e suporte em TI, a equipe da CMIT Solutions atualmente conta com mais de 900 líderes comerciais e profissionais técnicos que prestam serviços de suporte em TI em toda a América do Norte. Em 2008, a CMIT Solutions adotou o modelo de prestadora de serviços gerenciados, e desde então se concentrou no atendimento a empresas locais de pequeno e médio porte (PMEs).

Necessidades das empresas

Devido à ameaça em franco crescimento dos ransomwares e outros tipos de ataques, MSSPs como a CMIT Solutions têm enfrentado uma necessidade cada vez maior de ter uma solução de segurança para seus endpoints, que permita a gestão completa e centralizada, além de relatórios para todas as empresas clientes.

Solução

Para mitigar ataques cibernéticos e outras ameaças, a CMIT Solutions da Metrolina começou instalando o SonicWall Capture Client em todas as instalações de seus clientes. Um dos clientes mais antigos da CMIT Solutions, que confia na equipe da CMIT Solutions para gerenciar e prestar suporte a seus 9 estabelecimentos físicos, 150 endpoints e 15 servidores, havia optado pela implementação como parte de seus serviços gerenciados de TI, um complemento dos produtos da SonicWall, incluindo nove NGFWs série TZ da SonicWall e appliances de acesso remoso da SonicWall. A solução também inclui o SonicWall Capture Client, uma solução antimalware baseada em comportamento, projetada para impedir ataques antes e durante a execução, além de reparar danos mesmo depois da execução do malware.

O que aconteceu

Em maio de 2021, esse cliente foi alvo de uma campanha de ransomware que, em última instância, tentou lançar 4.021 ataques conta 162 endpoints e servidores da empresa. O ataque começou quando um funcionário abriu o e-mail de um fornecedor com um anexo de Excel infectado, e em seguida habilitou o conteúdo desse anexo. A partir desse único endpoint, o ataque rapidamente mapeou a rede, baixou arquivos adicionais para propagar o ataque, e – por meio de um mecanismo de SMB no Windows – tentou se difundir pela organização e para outros locais, atacando PCs e servidores. Ao mesmo tempo, ele tentou se movimentar pela rede até os servidores em outros locais, por meio do Windows Netlogin Privilege Elevations. Em apenas dois minutos, o malware fez mais de 1.000 tentativas de se conectar a três servidores de Comando e Controle C&C no leste europeu.

cmit Solutions® Your Technology Team

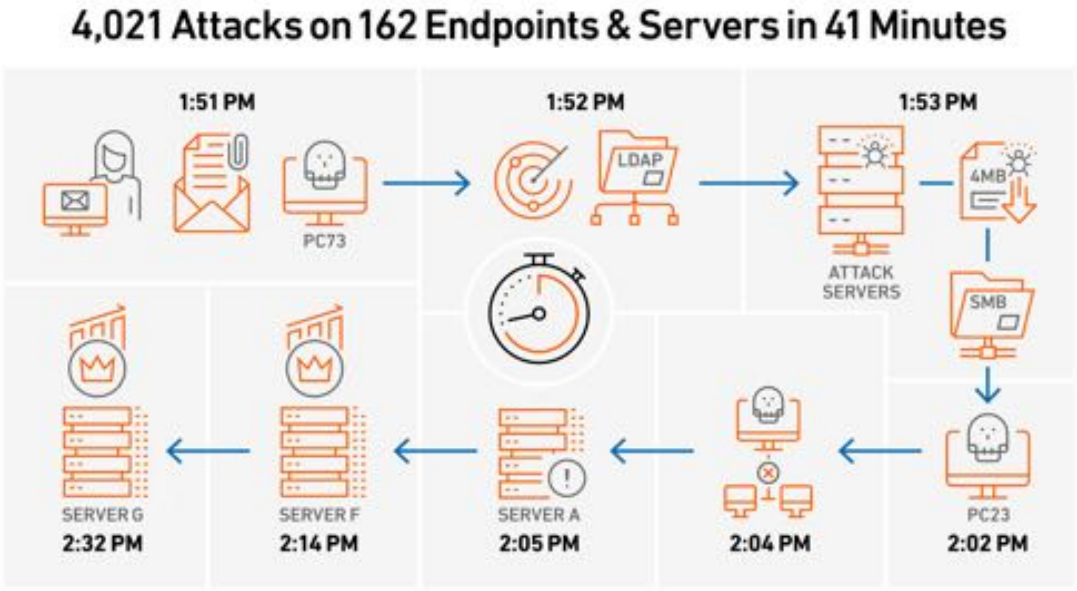
"Defesa profunda funciona! Estamos satisfeitos com o desempenho do Capture Client e dos demais componentes do nosso sistema de segurança, que ajudaram nossa empresa a conter esse ataque e se recuperar em seguida. A missão da CMIT é evitar que pessoas mal-intencionadas destruam valores da empresa, ao mesmo tempo oferecendo um excelente suporte aos clientes e mantendo os sistemas em execução de forma eficiente. Mas se um golpista consegue derrotar nossos controles de segurança, trabalhamos com o mesmo afinco para estarmos preparados para recuperar os sistemas e as informações, para que nossos clientes não se obriguem a pagar um resgate para terem acesso aos seus dados novamente".

Emory Simmons
Presidente

Perfil do cliente

Empresa	CMIT Solutions da Metrolina
Setor	MSSP
País	EUA
Site	cmitsolutions.com/metrolina

ESTUDO DE CASO



Resultados

No final, o ataque não foi capaz de criptografar um único endpoint. Embora um serviço de segurança DNS de terceiros DNS tenha sido capaz de bloquear o acesso no início do ataque, a equipe da CMIT Solutions começou a receber notificações de que o SonicWall Capture Client havia interrompido e eliminado o ransomware "Win32/Teerac - f91e9b0.exe," seguida de outra notificação de que o "HackTool.Win32.LAZAGNE.AC" havia sido interrompido e removido tanto de um servidor quando do PC originalmente infectado.

Finalmente, o ataque foi interrompido por uma mescla de tecnologia avançada e a resposta imediata da equipe da CMIT Solutions. A CMIT Solutions iniciou imediatamente seu processo de resposta, desconectando as máquinas da rede com os recursos de desconexão do Capture Client, gerando túneis VPN entre os sites e permitindo que o Capture Client eliminasse a movimentação lateral entre sites e servidores. O PC originalmente infectado tentou sozinho realizar 4.021 ataques em 162 endpoints e servidores. O SonicWall Capture Client detectou e eliminou a movimentação lateral, eliminou o ransomware, e eliminou o HackTool.

Lições aprendidas

Embora o ataque tenha sido rapidamente interrompido, ele ainda assim representou quatro lições sobre fatores que poderiam ter reduzido o tempo que a equipe da CMIT Solutions levou para reagir ao incidente:

1. A configuração do Capture Client para desconectar endpoints quando um malware é detectado teria contido a ameaça ao primeiro servidor 49 minutos mais cedo. Também teria contido o PC inicialmente infectado 81 minutos mais cedo, conferindo menos tempo para que ele fizesse a varredura de outras vítimas pela rede ampla.
2. A habilitação dos filtros SonicWall Geo-IP nos países de origem teria impedido que o malware inicial fosse baixado.
3. A configuração IPS no firewall da SonicWall para bloquear ameaças de nível médio em vez de atuar apenas sobre as ameaças de alto nível teria bloqueado as tentativas de explorar os recursos do Windows.
4. Uma conscientização aperfeiçoada dos usuários teria evitado o ataque por completo.

Embora não tenha sido um aprendizado direto desse ataque, a CMIT também planeja fortalecer ainda mais a segurança dos endpoints, habilitando o recurso de fiscalização nos NGFWs da SonicWall. Esta medida vai assegurar que somente computadores com o Capture Client instalado tenham permissão para acessar a internet.

Benefícios do SonicWall Capture Client

- **Interrompe ataques avançados antes e durante a execução**
- **Oferece proteção contra ransomware e reparação de danos**
- **Permite a visibilidade das vulnerabilidades das aplicações**
- **Fiscaliza as políticas de utilização da internet fora do ambiente de rede**
- **Permite aos usuários visualizar e gerenciar facilmente a saúde do computador hospedeiro**

Baixe um teste gratuito do Capture Client:

www.sonicwall.com/capture-client

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso site na internet pata obter informações adicionais.
www.sonicwall.com

CaseStudy-CMIT-Metrolina-COG-4874