SOPHOS

Ransomware remoto

A criptografia remota maliciosa é uma técnica popular de ransomware usada em cerca de 60% dos ataques de ransomware operados por humanos[1]. A maioria das melhores soluções de segurança de endpoint luta arduamente para se proteger contra essa abordagem, e se você não está usando o Sophos Endpoint, há grandes chances de você estar exposto a riscos. Leia este guia para saber sobre os riscos do ransomware remoto e a proteção da Sophos, que é líder do setor, para interromper esses ransomwares.

Documento técnico Sophos. Junho de 2024

O que é ransomware remoto?

Ransomware remoto, também conhecido por criptografia remota maliciosa, é quando um endpoint comprometido é usado para criptografar dados em outros dispositivos na mesma rede.

Em ataques conduzidos por humanos, os adversários normalmente tentam implantar um ransomware diretamente nas máquinas que desejam criptografar. Se a tentativa inicial for bloqueada (por exemplo, pelas tecnologias de segurança nos dispositivos de destino), raramente eles desistirão, optando por aplicar uma abordagem alternativa para fazer uma nova tentativa, e assim sucessivamente.

Quando os invasores conseguem comprometer o dispositivo com sucesso, eles podem se aproveitar da arquitetura do domínio da organização para criptografar os dados nas máquinas gerenciadas conectadas ao domino. Todas as atividades maliciosas, como entrada, execução de carga útil e criptografia, ocorrem na máquina já comprometida, evitando, assim, passar pelo moderno arsenal de segurança. A única indicação de comprometimento é a transmissão de documentos de e para as máquinas.

80% dos comprometimentos por criptografia remota se originam em máquinas não gerenciadas na rede[2], embora alguns tenham início em máquinas protegidas que carecem das defesas necessárias para interromper a entrada de invasores no dispositivo.

Por que o ransomware remoto é tão predominante?

Um fator-chave que dissemina o uso dessa abordagem é a sua escalabilidade: um único endpoint não gerenciado ou com pouca proteção pode expor o patrimônio digital de toda uma organização à criptografia remota maliciosa, mesmo que todos os outros dispositivos tenham em execução uma solução Next-Gen de segurança de endpoint.

Para piorar esse cenário ainda mais, os adversários têm uma lista ilimitada de opções de variantes de ransomware para esses ataques. Uma extensa lista de famílias de ransomwares admite a criptografia remota maliciosa, como é o caso do Akira, BitPaymer, BlackCat, BlackMatter, Conti, Crytox, DarkSide, Dharma, LockBit, MedusaLocker, Phobos, Royal, Ryuk e WannaCry.

Outro motivo significativo por trás da predominância do ransomware remoto é que a maioria dos produtos de segurança de endpoint é ineficiente nesse tipo de cenário porque se concentra em detectar arquivos de ransomware maliciosos e processos em endpoints protegidos. Entretanto, com os ataques de criptografia remota, os processos são executados em máquinas comprometidas, cegando a proteção do endpoint às atividades maliciosas.

Em contrapartida, a Sophos oferece a defesa de endpoint zero touch mais robusta contra ransomwares remotos, alimentada por nossa proteção CryptoGuard, líder do setor.

Proteção hermética contra ransomware com o Sophos CryptoGuard

O Sophos Endpoint contém várias camadas de proteção que defendem as organizações contra ransomwares, como o CryptoGuard, nossa exclusiva tecnologia anti-ransomware que vem incluída em todas as assinaturas do Sophos Endpoint.

Diferentemente de outras soluções de segurança de endpoint que buscam apenas arquivos e processos maliciosos, o CryptoGuard analisa arquivos de dados em busca de sinais de criptografia maliciosa independentemente de onde os processos estão operando. Essa abordagem o torna altamente eficiente para interromper todas as formas de ransomware, inclusive a criptografia remota maliciosa. Se ele detectar a criptografia maliciosa, o CryptoGuard bloqueia automaticamente a atividade e reverte os arquivos para o seu estado descriptografado.

O CryptoGuard examina ativamente o conteúdo de todos os documentos conforme os arquivos são gravados e lidos usando análises matemáticas para determinar se foram criptografados. Essa abordagem universal é única na indústria e permite que o Sophos Endpoint bloqueie ataques de ransomware que outras soluções não conseguem, inclusive ataques remotos e variantes de ransomwares ainda não observadas.

O CryptoGuard é uma das funcionalidades exclusivas do Sophos Endpoint e está incluído em todas as assinaturas do Sophos Intercept X Advanced, Sophos XDR e Sophos MDR. Além disso, a funcionalidade é habilitada automaticamente por padrão, assegurando às organizações a proteção total contra ataques de ransomwares remotos e locais imediatamente, sem a necessidade de ajustes ou configurações. **A defesa de endpoint zero touch mais robusta contra ransomwares remotos.**

- **Detecção de criptografia maliciosa pela análise de conteúdo de arquivo**

  Diferentemente de outras soluções que veem os ransomwares sob a perspectiva de um anti-malware, concentrando-se em detectar códigos maliciosos, o CryptoGuard se concentra na criptografia rápida e em massa dos arquivos, analisando seu conteúdo usando algoritmos matemáticos.

- **Bloqueio de ataques de ransomwares remotos e locais**

  Como o CryptoGuard direciona seu foco ao conteúdo dos arquivos, ele pode detectar a criptografia de ransomware mesmo quando o processo malicioso não está em execução no dispositivo da vítima.

- **Reversão automática de criptografia maliciosa**

  O CryptoGuard cria backups temporários de arquivos e os reverte automaticamente quando detecta a criptografia em massa. A Sophos usa uma abordagem proprietária, diferentemente de outras soluções que usam Cópias de Sombra de Volume do Windows, que os adversários já comprovaram que podem burlar. Não há limites em tamanhos e tipos de arquivos que podem ser recuperados, minimizando o impacto na produtividade dos negócios.

- **Bloqueio automático de dispositivos remotos**

  Em um ataque de ransomware remoto, o CryptoGuard bloqueia automaticamente o endereço IP do dispositivo remoto que está tentando criptografar os arquivos no computador da vítima.

- **Proteção do registro mestre de inicialização (MBR)**

  O CryptoGuard também protege o dispositivo contra ransomwares que criptografam registros mestres de inicialização (impedindo a inicialização) e contra ataques que apagam o disco rígido.

Descoberta de dispositivos sem proteção

Um único endpoint sem proteção pode deixar toda a sua organização vulnerável a ataques de criptografia remota. Implantar o Sophos Endpoint oferece proteção robusta contra ransomwares universais e criptografia maliciosa, mas como identificar se você tem dispositivos desprotegidos na sua rede?

É aqui que Sophos Network Detection and Response (NDR) pode ajudar. O Sophos NDR monitora o tráfego da rede em busca de fluxos suspeitos e, durante esse processo, identifica os dispositivos sem proteção e os ativos ilegítimos no seu ambiente.

Para ter uma proteção forte contra ataques de ransomware remotos, instale o Sophos Endpoint em todas as máquinas em seu ambiente e implante o Sophos NDR para encontrar os dispositivos sem proteção na sua rede.

Eleve sua proteção contra ransomwares remotos hoje mesmo

A criptografia remota maliciosa é uma técnica popular de ransomware que a maioria das melhores soluções de segurança de endpoint luta arduamente para bloquear. Se você não está usando o Sophos Endpoint, há grandes chances de você estar exposto a riscos.

Para saber mais sobre o Sophos Endpoint e como ele pode ajudar a sua organização a se defender melhor contra os atuais ataques avançados, incluindo ransomware remoto, fala com um consultor da Sophos ou com o seu parceiro Sophos hoje mesmo. Você também pode experimentá-lo no seu próprio ambiente fazendo uma avaliação gratuita de 30 dias sem compromisso.

1 Relatório de Defesa Digital da Microsoft. https://www.microsoft.com/pt-br/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (5 de outubro de 2023). Espionage fuels global cyberattacks. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2024-14-06 (WP-NP)

SOPHOS