SONICWALL

RESUMO EXECUTIVO: O RESGATE DO ENSINO SUPERIOR

Melhores práticas de defesa contra ransomware e outros ataques cibernéticos

Resumo

Ataques coordenados estão atingindo as instituições de ensino superior por toda a nação e pelo mundo. Cibercriminosos ainda consideram as redes de faculdades e universidades um alvo lucrativo para ransomware. No entanto, há alguns passos que você pode seguir para evitar ser uma vítima.

Introdução

Há uma preocupação crescente quanto a ataques de ransomware nas redes de ensino superior. Serviços acadêmicos foram bloqueados e os custos cumulativos de ransomware foram de milhões.

Uma tendência preocupante

De acordo com o Relatório de Ameaças Cibernéticas da SonicWall 2020, os pesquisadores do SonicWall Capture Labs registraram 187,9 milhões no volume total de ransomware durante 2019, uma queda de 6% em relação ao volume recorde de 2018. Mas o volume não deve ser confundido com eficácia.

Organizações de cibercrimonosos que usam ransomware continuam a se concentrar mais na qualidade de seus ataques do que na quantidade. O que importa não é o tamanho da organização, mas sim a probabilidade de pagar. Esta é a razão porque as instituições de ensino superior ao redor no mundo continuam sendo alvos de ransomware. É uma epidemia global.

Esta tendência é extremamente prejudicial para a educação. De acordo com um relatório recente, o setor da educação foi o maior afetado entre todos os setores empresariais nos EUA em 2018 e no primeiro semestre de 2019. Ameaças vão desde aborrecimentos com adware até malware mais perigosos como trojans, backdoors e naturalmente ransomware – um arquivo malicioso que encripta arquivos do sistema e informações em endpoints e servidores. As universidades atingidas por ataques de ransomware são impedidas de acessar informações vitais até que paguem um resgate em criptomoeda (geralmente Bitcoin).

Além do prejuízo financeiro direto causado por este tipo de ataque, a incapacidade de acessar os sistemas de computador paralisa a instituição acadêmica. O custo dos danos aumenta quanto mais tempo a escola não pode enviar e-mails, registrar as horas de trabalho ou alocar as salas de aula e recursos de estudo, o que inclui os computadores da escola e o acesso à internet necessários para muitas atividades de aprendizagem. Escolas que se recusam a pagar podem ficar inoperantes por um período prolongado.

O famoso Emotet malware também tem atingido escolas, com atacantes usando spearphishing para infectar sistemas com o malware trojan. Hoje em dia, como muitos serviços são inteiramente computadorizados, até mesmo a infraestrutura, como aquecimento, refrigeração, serviços de cafeteria e sistemas de segurança é afetada.

Uma preocupação global

Muitas das universidades e faculdades dos EUA vivenciaram ataques de ransomware, vazamento de informações e contas de e-mail comprometidas. As universidades e institutos acadêmicos têm sido alvos de atacantes mais sofisticados, interessados em roubar a propriedade intelectual (IP) e dados de pesquisa que essas instituições produzem.

A situação em outras partes do mundo é igualmente ruim. Na Austrália, o chefe da agência de inteligência local foi chamado para explicar às universidades sobre ataques cibernéticos e meios de prevenção. Esta foi uma das iniciativas que teve lugar depois que um ator de ameaças altamente sofisticado comprometeu Universidade Nacional da Austrália (ANU) e permaneceu na rede da universidade por meses.

Em abril deste ano no Reino Unido um teste de intrusão feito pelo Comitê JISC, a agência do governo que fornece muitos serviços computadorizados para órgãos acadêmicos britânicos, testou as defesas de mais de 50 universidades britânicas. Os resultados foram críticos: os pentesters obtiveram 100% de sucesso: conseguiram simplesmente acessar todos os sistemas testados. Em alguns casos, em apenas uma hora, os sistemas de defesa foram contornados, e os hackers éticos foram capazes de ter acesso a informações, tais como dados de pesquisa, sistemas financeiros bem como dados pessoais de funcionários e estudantes.

Análise: Tendência geral

Bill Conner, CEO da SonicWall afirma: "É muito fácil exigir e receber pagamento de resgate sem riscos associados à exfiltração de dados tradicional. Enquanto as organizações não levarem a sério a proteção contra ransomware, estes tipos de ataques de ransomware de grande alcance continuarão. Como pudemos constatar nas escolas no ano passado, os ataques de ransomware são altamente preocupantes. As redes distribuídas hoje em dia podem ser comprometidas em minutos. As operações diárias ficam presas em troca de resgate de valores altos."

Não é mera coincidência que as escolas estão entre os alvos mais atacados. As instituições de educação superior lidam com grandes somas de dinheiro, armazenam informações pessoais de estudantes e do corpo docente, se conectam com organizações externas e provedores e naturalmente com pais, que usam e-mail como forma de se comunicar com a escola. Isto significa que a escola tem uma superfície de ataque muito grande.

Além das recompensas atraentes, os estudantes são vítimas fáceis de phishing scams. A falta de experiência dos estudantes juntamente com a tendência de se usar senhas simples em vários serviços os torna suscetíveis a ataques de coleta de credenciais e difusão de senha. Em setembro passado, em um incidente, mais de 3.000 e-mails de alunos no estado de Kent foram hackeados desta forma. Além disso, a conscientização dos pais, professores e faculdade em relação aos riscos cibernéticos é geralmente bem menor do que em outros setores.

Ransomware não infecta mais somente um dispositivo único, mas sim vários dispositivos com a intenção de infectar toda a rede. Primeiro famosos com o ataque WannaCry, os autores de ransomware agora tentam se aproveitar de vulnerabilidades, tais como SMB no Windows para se espalhar para outras unidades. Nem todos os computadores estão atualizados e isso oferece a oportunidade de se infectar não somente esse dispositivo, mas também todos outros.

Algumas instituições acadêmicas são ricas em dados e pobres em segurança, o que as torna um alvo principal. Faculdades têm informações sobre estudantes, incluindo graduações que são fundamentais para seus futuros empreendimentos e algumas jurisdições têm que manter esses dados por até 100 anos. As universidades que conseguiram digitalizar registros antigos e não têm backups apropriados estão se arriscando a perder esses dados ou a ter que digitalizá-los novamente. As escolas devem fazer backup constante de tudo e fazê-los fora da rede, seja em fitas LTO ou na nuvem.

Adicionalmente o que agrava a situação da segurança é que os estabelecimentos educacionais têm poucos funcionários dedicados à segurança. Ao contrário de bancos, as escolas normalmente não têm pessoal dedicado à segurança de informações com proteção 24/7.

"Você tem ransomware"

A maioria dos ataques de ransomware vem em e-mails não solicitados. Aparecem em anexos com linhas de assunto tais como:

- Aqui meu currículo
- Fatura não paga
- Aqui está a fatura de seu voo/ encomenda, etc. (na esperança de dar um susto nas pessoas e levá-las a pensar que as informações de seu cartão de crédito foram roubadas).

Também se usam URLs maliciosas. Parecem iguais aos URLs reais, mas levam a outros lugares na dark web. As linhas de assunto comuns são:

- Seu cartão foi debitado, revise
- É você neste vídeo?
- Sua encomenda chegou

Prepare-se com essas melhores práticas

A Agência de Segurança Cibernética e Segurança de Infraestrutura (CISA) do Departamento de Segurança Nacional dos EUA recomenda as seguintes precauções para proteger usuários contra a ameaça de ransomware:

- Atualize software e sistemas operacionais com os últimos patches. Aplicativos e sistemas operacionais desatualizados são os alvos da maioria dos ataques.
- Nunca clique em links ou abra anexos em e-mails não solicitados.
- Faça regularmente backup de seus dados. Mantenha estes backups em um dispositivo separado e armazene-os off-line.
- Siga práticas seguras quando navegar pela internet.

CISA também recomenda às organizações usarem as seguintes melhores práticas:

- Limite as permissões de usuários para instalar e executar aplicações de software e use o princípio de "menos privilégios" em todos os sistemas e serviços. A limitação desses privilégios pode prevenir a execução de malware ou limitar sua capacidade de se espalhar pela rede.
- Use aplicação whitelisting para permitir que somente programas autorizados possam ser executados em uma rede.
- Use filtros de spam fortes para evitar e-mails de phishing de chegarem até os usuários finais e autentique os e-mails de entrada para evitar spoofing.
- Verifique todos os e-mails que entram e saem para detectar ameaças e filtrar arquivos executáveis de chegar até os usuários finais.
- Configure firewalls para bloquearem o acesso a conhecidos endereços IP maliciosos.

Adicionalmente, SonicWall sugere os seguintes passos de melhor prática:

- Ensine os usuários sobre as melhores práticas de segurança cibernética
- Use um firewall de próxima geração para eliminar ameaças conhecidas na rede
- Implemente sandboxing eficaz nesses firewalls para identificar ameaças desconhecidas
- Implemente segurança de endpoint com IA avançada para deter ataques antes que aconteçam no endpoint.
- Evite pagar regaste; isso só encoraja mais ataques.

Conclusão

Infelizmente com abordagens diferentes para responder à demanda de ransomware sendo conduzidas por orçamento e recursos, os cibercriminosos constataram que faculdades e universidades são um alvo lucrativo para ataques de ransomware. Embora esses ataques de ransomware sejam muito difundidos, devem-se considerar algumas semelhanças. É imprescindível estar preparado com a implementação das melhores práticas conhecidas e das contramedidas de ransomware mais recentes.

Saiba mais. Leia nosso sumário: 7 Best Practices for Fighting Ransomware (7 melhores práticas para combater ransomware).

Sobre SonicWall

A SonicWall luta contra a indústria do crime cibernético há mais de 28 anos, defendendo empresas de pequeno e médio porte, grandes corporações e órgãos governamentais no mundo todo. Respaldadas pela pesquisa do SonicWall Capture Labs, nossas premiadas soluções de detecção e prevenção de violações em tempo real protegem mais de um milhão de redes e seus e-mails, aplicativos e dados em mais de 215 países e territórios. Essas organizações operam com mais eficácia e com menos receios quanto à segurança. Para mais informações, visite www.sonicwall.com ou nos siga no Twitter, LinkedIn, Facebook and Instagram.

Se tiver dúvidas com relação ao possível uso deste material, contate:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Faça referência ao nosso website para informação adicional.
www.sonicwall.com