cpl.thalesgroup.com

THALES
Building a future we can all trust

Como os ataques ransomware usam RDPs desprotegidos e o que você pode fazer quanto a isso

Os ataques ransomware contra empresas de diversos setores dispararam nos ultimos anos. Os criminosos estão tirando proveito de nossa confiança nas comunicações digitais e no trabalho remoto com fins mal-intencionados. Como resultado, a maioria dos incidentes de ransomware pode ser atribuída a um número limitado de vetores de intrusão, sendo os três principais: terminais mal protegidos do remote desktop protocol (RDP), phishing por e-mail e a exploração de vulnerabilidades de dia zero do VPN.

Relatórios das empresas Coveware, Emsisoft e Recorded Future destacam que o "RDP é considerado como o maior vetor de ataque ransomware", tendo sido a fonte da maioria dos incidentes de ransomware em 2020 Algumas pessoas acham que o RDP é o principal vetor de intrusão de ransomware devido ao home office Entretanto, essa presunção está errada. O RDP está entre os principais vetores de intrusão desde o ano passado, quando os hackers de ransomware deixaram de visar os consumidores e passaram a visar empresas e infraestruturas críticas.

Qual é a principal causa disso?

O RDP é a tecnologia mais popular para conexão a sistemas remotos, e é geralmente considerado como uma ferramenta segura e protegida quando usado em uma rede privada. Entretanto, quando as portas do RDP são deixadas abertas na internet e acessíveis com senhas simples, elas podem causar sérios problemas de segurança. As senhas podem ser facilmente comprometidas, abrindo o caminho para o acesso criminoso e não autorizado às redes corporativas através de RDPs desprotegidos. O acesso não autorizado via RDPs permite que os hackers tenham acesso aos servidores corporativos e atuem como plataforma de lançamento de ataques ransomware.

Há milhões de computadores com suas portas do RDP expostas online sem qualquer proteção, o que faz do RDP um enorme vetor de ataque a todos os tipos de atividades cibernéticas criminosas, e cada vez mais ataques ransomware. Os criminosos que procuram explorar esses pontos de acesso podem encontrá-los gratuitamente nos "mercados de RDP". A partir daí, o trabalho deles é o mesmo de sempre. Eles procuram senhas fracas usando técnicas conhecidas como força bruta ou engenharia social. Uma vez que o hacker tenha obtido acesso ao sistema desejado, ele se concentra em tornar a rede tão insegura quanto possível.

Após os sistemas de segurança terem sido desativados e a rede ficar desprotegida, os criminosos ficam livres para atacar. Isto pode ser qualquer coisa, desde a instalação de ransomware, keyloggers, o uso de máquinas comprometidas para distribuir spam, o roubo de dados confidenciais ou a instalação de backdoors para futuros ataques.

Melhores práticas para mitigar os ataques ao RDP

Como mencionado acima, os RDPs são pontos de acesso para entrar em redes corporativas e não devem ser vistos na internet ou publicados sem proteção. A publicação de áreas de trabalho remoto para conveniência do usuário não justifica o aumento da ameaça à qual as empresas ficam expostas.

Para empresas que requerem o RDP, as seguintes melhores práticas se concentram no fortalecimento do ponto de acesso e são úteis para proteger o RDP contra ataques por força bruta.

- Como regra geral, não publique áreas de trabalho remoto desprotegidas na internet. Se isso for extremamente necessário, certifique-se de que o ponto de acesso do RDP esteja protegido com autenticação multifator (MFA) para garantir que somente usuários validados possam entrar no RDP.
- Use gateways de RDP. As áreas de trabalho remoto devem ser protegidas atrás de gateways proxy reversíveis para ofuscar a porta padrão 3389 do RDP padrão. Os gateways de RDP são acessados através de conexões HTTPS (porta 443) protegidas através do protocolo de criptografia TLS.
- Utilize a MFA para acessar o gateway de RDP. Mesmo as senhas mais fortes podem ser comprometidas. Embora não seja uma panaceia, a MFA oferece uma camada extra de proteção ao exigir que os usuários forneçam pelo menos duas formas de autenticação para entrar em uma sessão de RDP.
- Utilize a MFA para o login na rede. Uma vez dentro da área de trabalho remota, implemente outra camada de segurança, aplicando a MFA ao ponto de login na rede.

Como o Thales SafeNet Trusted Access ajuda a mitigar ataques

O Thales SafeNet Trusted Access pode ajudar a proteger seu ambiente de negócios contra ataques ransomware baseados em RDP. O SafeNet Trusted Access permite que as empresas protejam efetivamente o acesso remoto aos RDPs, gateways de RDP, bem como a aplicativos adicionais de nuvem e legados, independentemente do dispositivo final utilizado. SafeNet Trusted Access

- Suporte para uma ampla gama de opções de autenticação, incluindo autenticação adaptativa e de passo a passo, MFA e tokens de hardware.
- Políticas de acesso flexíveis para todos os sistemas operacionais (Windows/Mac/Linux) - isso significa que você pode usar um único serviço de gerenciamento de acesso e autenticação para proteger aplicativos baseados em nuvem e todas as áreas de trabalho remotas, independentemente do sistema operacional em que eles são executados.
- Gerencie centralmente os aplicativos de nuvem e logins de rede a partir de um único serviço de gerenciamento de acesso/MFA.

Sobre a Thales

As pessoas em quem você confia para proteger sua privacidade confiam na Thales para proteger seus dados. Em termos de segurança de dados, as organizações enfrentam cada vez mais momentos decisivos. Seja na criação de uma estratégia de criptografia, migração para a nuvem ou cumprimento de normas de conformidade, você pode confiar na Thales para proteger sua transformação digital.

Tecnologia decisiva para momentos decisivos.