



CYBERSECURITY  
EXPERTS ON YOUR SIDE

# RDP: CONFIGURANDO A SEGURANÇA PARA UM FUTURO REMOTO, MAS NÃO DISTANTE

Alavancar RDP para administrar sua rede através de uma crise? Então tenha certeza de que você está limitando seu risco com boas práticas, ferramentas de autenticação e alavancando a base de conhecimento existente.

A pandemia do corona fez com que empresas ao redor do mundo enviassem as pessoas para casa e alavancassem o trabalho remoto em massa usando quaisquer meios possíveis. Isso inclui o uso de tecnologia RDP, que esteve sujeita a abuso nos últimos anos. Muitas instâncias emergiram, especialmente quando atacantes descobriram meios de explorar configurações mal planejadas ou senhas fracas para obter acesso a redes da empresa.

Assim que entram, os atacantes têm porta aberta para fazer quase tudo, incluindo, por exemplo, o roubo de propriedade intelectual ou outras informações sensíveis, criptografando-as para resgate.

AUTOR: Aryeh Goretsky  
CONTRIBUIÇÃO: James Shepperd

Abril 2020

# 1.

## O que os atacantes fazem com RDP?

Nos últimos anos, a ESET viu um número crescente de incidentes onde os atacantes se conectavam remotamente a servidores Windows a partir da internet usando RDP e faziam login como administrador do computador. Isso implica em vários vetores incluindo: vulnerabilidades (como BlueKeep CVE-2019-0708), phishing, roubo de credenciais, spray de senha, força bruta ou acesso mal configurado a sistemas internos.

Assim que os atacantes estão logados no servidor como administrador, eles geralmente irão realizar algum reconhecimento para determinar para que o servidor é usado, por quem e quando é usado. Então, eles podem começar a realizar ações maliciosas.

Essa não é uma lista completa de tudo o que eles podem fazer, nem eles irão necessariamente realizar todas estas atividades. A frequência exata, sequência e natureza do que os atacantes irão fazer varia muito.

### ATIVIDADES MALICIOSAS COMUNS QUE VIMOS INCLUEM:

- limpar arquivos de log contendo evidência de sua presença no sistema
- desabilitar backups agendados e cópias de sombra
- desabilitar software de segurança ou configurar exclusões nele (que é permitido para administradores)
- fazer download e instalar vários programas no servidor
- apagar ou sobrescrever backups antigos, se eles estiverem acessíveis
- exfiltrar dados do servidor

### TRÊS DAS MAIS COMUNS SÃO:

- instalar programas de mineração de moedas para gerar criptomoedas, como o Monero
- instalar ransomware para extorquir dinheiro da organização, frequentemente para ser pago usando criptomoeda, como o bitcoin
- em alguns casos, os atacantes podem instalar software de controle remoto adicional para manter acesso (persistência) a servidores comprometidos, caso as atividades RDP sejam descobertas e encerradas

## ATIVIDADE RDP MALICIOSA NOTÁVEL E RECENTE

Um ransomware prolífico, [GandCrab](#), que operou até maio de 2019, usou um modelo de negócio de *Ransomware* como Serviço (RaaS) no qual os desenvolvedores alavancaram muitos atores maliciosos afiliados para distribuir ainda mais o *malware*. O GandCrab, em particular, teve como alvo MSPs usando [RDP](#) para conectar as ferramentas de gerenciamento remoto e extorquir múltiplos clientes de uma vez.

Ainda que os operadores de ransomware do GandCrab [tenham anunciado](#) sua aposentadoria após o FBI liberar as chaves para descriptografar seu *ransomware*, nossos especialistas acreditam que o código fonte do GandCrab pode ter sido vendido para um grupo diferente que agora está executando o Sodinokibi, (devido a alterações no código, sua estrutura e atualizações subsequentes). O *ransomware* Sodinokibi apareceu quando o GandCrab começou a [suspender](#) suas operações, essencialmente [substituindo o GandCrab](#) e usando táticas, técnicas e procedimentos similares a seu predecessor para alvejar MSPs via RDP.

A conexão MSP é notável para grandes corporações também, já que os MSPs detêm as ["chaves do reino"](#) para milhares de PMEs (e relacionamentos de negócios de PMEs), e até mesmo algumas grandes corporações.

Do lado do cliente MSP, os negócios encaram dependências similares já que ambos, equipes e usuários individuais, dependem dos administradores para ajudar com tudo, do licenciamento e atualizações até a segurança.

## A VULNERABILIDADE RDP ABRE UMA GRANDE PORTA PARA O RISCO

Os ataques via RDP têm aumentado lenta e consistentemente, e estão sujeitos a muitos avisos governamentais do [FBI](#), do [NCSC](#) do Reino Unido, [CCCS](#) do Canadá e ACSC da Austrália, para citar alguns.

Em maio de 2019 as comportas se abriram com a chegada do [CVE-2019-0708](#) também conhecido como "BlueKeep", uma vulnerabilidade de segurança no RDP que afetou o Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 e Windows Server 2008 R2.

Ainda que esses possam ser sistemas legados e, na maioria dos casos não tenham mais suporte ou apenas tenham um suporte limitado para o fornecedor, a telemetria sugere que ainda haverá muitos sistemas vulneráveis em uso.

A [vulnerabilidade BlueKeep](#) permite que os atacantes executem um código de programa arbitrário nos computadores das

**A ESET OFERECE UMA FERRAMENTA DE DETECÇÃO GRATUITA BLUEKEEP (CVE-2019-0708) PARA AJUDAR A IDENTIFICAR SISTEMAS VULNERÁVEIS A EXPLORAÇÃO VIA RDP. PARA INSTRUÇÕES SOBRE SEU USO E PARA FAZER DOWNLOAD DE UMA CÓPIA**

*\*Observe: as versões do Windows 8 e Windows Server 2012 e superiores são relatadas como não afetadas no momento da publicação.*

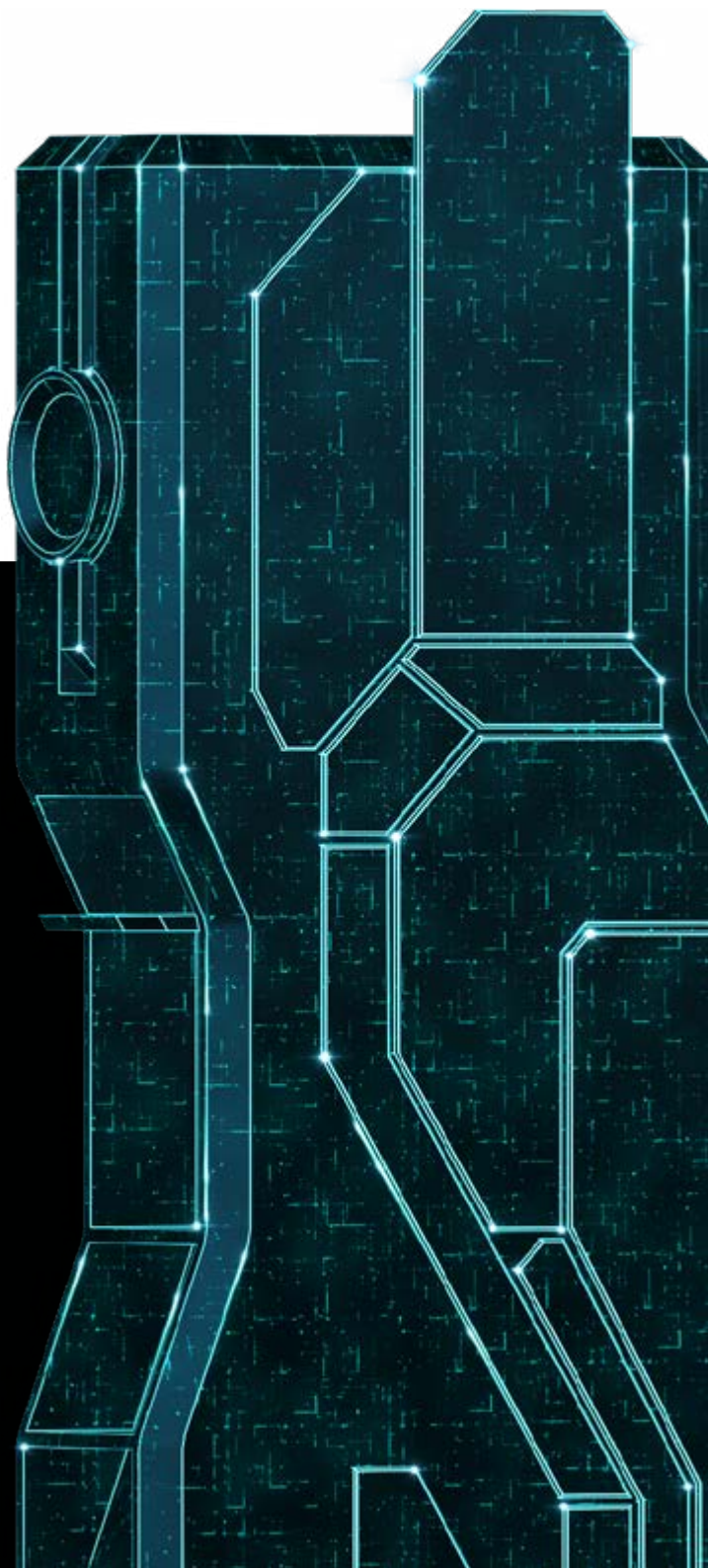
vítimas. Ainda que mesmo atacantes individuais possam ser uma ampla ameaça usando ferramentas automatizadas para ataques, esta vulnerabilidade é “tipo worm,” o que significa que um ataque poderia se espalhar automaticamente através das redes sem qualquer intervenção pelos usuários, assim como os worms Win32/Diskcoder.C (conhecido como NotPetya) e Conficker fizeram no passado.

A exploração de vulnerabilidades tipo worm é geralmente considerada um problema grave. A Microsoft atribuiu à vulnerabilidade seu mais alto grau de severidade, Crítico, em sua orientação publicada para clientes, e na Base de Dados de Vulnerabilidade Nacional do governo dos EUA, a entrada para CVE-2019-0708 obteve uma pontuação de 9.8 de 10. A Microsoft fez uma [publicação no blog](#) recomendando fortemente que os usuários instalem seus patches, incluindo aqueles para sistemas operacionais fora do suporte como o Windows XP e Windows Server 2003. Preocupações sobre um exploit tipo worm eram tão grandes que, no começo de junho de 2019, a Agência de Segurança Nacional dos Estados Unidos emitiu uma orientação rara recomendando a instalação de patches da Microsoft para a falha.

Enquanto fazia as rodadas em vários equipamentos de *pentesting* ao redor do mundo, nenhuma grande escalação na atividade BlueKeep foi relatada até novembro de 2019, quando relatórios em massa de uso do exploit vieram a público, conforme percebido pela ZDNet e WIRED. Os ataques foram notadamente menos do que bem-sucedidos com cerca de 91% de computadores vulneráveis travando com um erro de parada (conhecido como verificação de *bug* ou tela azul da morte)

quando o atacante tenta explorar a vulnerabilidade BlueKeep. No entanto, nos restantes 9% dos computadores vulneráveis, esses atacantes instalaram com sucesso o software de criptomineração Monero. Ainda que não seja o temido ataque tipo worm, o grupo criminoso automatizou a exploração, ainda que sem uma alta taxa de sucesso.

Como o tempo é escasso, vamos evitar uma descrição muito detalhada da vulnerabilidade e, ao invés disso, focar no que deverá ser feito para proteger as redes contra essa ameaça.



# 2.

## Defesa contra atacantes RDP

Então o que você pode fazer? Bem, a primeira coisa é parar de se conectar direto com seus servidores pela internet usando RDP ou ao menos minimizar isso sempre que possível. Isso pode ser problemático para muitos negócios, especialmente agora que muitos colaboradores podem estar trabalhando remotamente sob vários regimes de quarentena.

Vamos enfatizar, se você ainda está executando o Windows Server 2008 ou Windows 7 (que não tem mais suporte desde janeiro de 2020) e tem máquinas executando estas plataformas que são acessíveis diretamente via RDP, então você está em risco sério de ataque e deverá tomar medidas para corrigir isso imediatamente. Ao executar essas plataformas, sua superfície de ameaça se multiplicou por um fator substancial, e [as recomendações abaixo devem fazer parte do seu negócio atualizando para plataformas que tenham suporte total dos seus fornecedores respectivos.](#)

Para aqueles executando plataformas de atualização, a situação não significa que você tem que parar imediatamente de usar RDP, mas que você precisa dar passos adicionais para protegê-la tão logo e tão detalhadamente quanto possível. Para este fim, criamos uma tabela com os [Top 12 passos que você pode dar para começar a proteger seus computadores de ataques baseados em RDP.](#)



# 12 RECOMENDAÇÕES PARA PROTEGER O RDP

Esta tabela é livremente baseada em ordem de importância e facilidade de implementação, mas isso pode variar dependendo da sua organização. Algumas podem não se aplicar ou podem ser mais práticas de executar em uma ordem diferente. Sua organização pode precisar de passos adicionais.

	RECOMENDAÇÃO	MOTIVO
1	Proibir conexões externas a máquinas locais na porta 3389 (TCP / UDP) no firewall do perímetro.*	Bloquear acesso RDP de toda a internet.
2	Testar e implementar patches para a vulnerabilidade CVE-2019-0708 (BlueKeep) e habilitar autenticação em nível de rede o mais rápido possível.	Instalar patch da Microsoft e seguir suas orientações de prescrição ajuda a garantir que os dispositivos estejam protegidos contra a vulnerabilidade BlueKeep.
3	Para todas as contas que puderem ser logadas via RDP, solicitar senhas complexas (uma frase de senha longa contendo 15+ caracteres sem frases relacionadas ao negócio, nomes de produto ou usuários é obrigatório).	Proteger contra adivinhação de senha e ataques de roubo de credencial. É muito fácil automatizar isso e o comprimento da senha os torna exponencialmente mais resistentes a ataques.
4	Para acessar servidores, use senhas únicas para contas locais com direitos administrativos (ex., usando LAPS ou um serviço de gerenciamento de senhas robusto). *Também: restringir direitos de acesso do servidor a um grupo limitado de usuários.	(conforme acima) Reduzir a superfície de ataque dos servidores limitando o número de usuários que podem ter acesso a eles.
5	Configurar o nível de criptografia de conexão do cliente RDP para "alto," se possível. Se não for, use o nível de criptografia mais alto disponível para conexões.	Usar criptografia de 128 bits para todas as comunicações cliente-servidor, se possível.

6

Instalar uma solução de autenticação multifatorial (MFA), como o [ESET Secure Authentication \(ESA\)](#), e requisitar isso para todas as contas que podem ser logadas via RDP, além de todas as contas de administrador.

Requer uma segunda camada de autenticação disponível apenas para colaboradores através do celular, token ou outro mecanismo para fazer login em computadores.

7

Instalar um gateway de rede virtual privada (VPN) para intermediar todas as conexões RDP de fora da sua rede local.

Prevenir conexões RDP entre a internet e sua rede local. Permitir que você aplique uma identificação mais forte e requisitos de autenticação para acesso remoto aos computadores.

8

Via seu painel de segurança, garantir que seu software de segurança de endpoint protegido por senha está usando uma senha forte não relacionada a contas de serviço e administrativas. O ESET Security Management Center (ESMC) permite um controle de política fácil e granular, e a criação de vários grupos de computador. Simultaneamente, o ESMC permite multi-inquilino e também é acessível por logins protegidos por MFA.

Fornecer uma camada adicional de proteção se um atacante obtiver acesso de administrador a sua rede.

9

Habilitar [bloqueio de exploração](#) no software de segurança endpoint, que é uma [tecnologia de detecção](#) de anomalia não baseada em assinatura, que monitora o comportamento de aplicativos que geralmente são o alvo

Muitos programas de segurança endpoint também podem bloquear técnicas de exploração. Verifique se essa funcionalidade está habilitada.

10

Isolar qualquer computador desprotegido que precise ser acessado a partir da internet usando RDP.

Implementar isolamento de rede para bloquear computador(es) vulneráveis do resto da rede.

11

Substituir computadores desprotegidos.

Se não puder ser feito patch de um computador (contra a vulnerabilidade BlueKeep), planeje sua substituição oportuna.

12

Considere instituir bloqueio por GeolIP no gateway VPN.

Se a equipe e fornecedores estiverem no mesmo país ou entre uma pequena lista de países, considere bloquear acesso de países excluídos para prevenir conexões de atacantes estrangeiros.

# 3.

## Como a ESET ajuda a proteger seu RDP

Um bom primeiro passo é ter certeza de que seu software de segurança endpoint está a) atualizado e b) detecta a vulnerabilidade BlueKeep. Então, há um papel mais granular para a tecnologia em camadas. A BlueKeep é detectada como RDP / Exploit. O CVE-2019-0708 pelo [módulo de Proteção de Ataque à Rede](#) da ESET, que é uma extensão da tecnologia firewall da ESET presente nos [produtos de proteção endpoint da ESET](#), versão 7 e superior.

Outra camada de tecnologia crítica para a proteção de RDP é o [ESET Exploit Blocker](#), que monitora geralmente aplicativos exploráveis (navegadores, leitores de documento, clientes de e-mail, Flash, Java e outros). Ao invés de focar somente em identificadores particulares CVE, ela foca em técnicas de exploração. Quando ativada, a [ameaça é bloqueada](#) imediatamente na máquina.

Em paralelo à tecnologia, aconselhamos você a colocar processos adequados em ação, que devem ser o mais amigáveis possível, processos que por fim se beneficiem de ferramentas fáceis de usar. Já que proteger o RDP requer vários passos (procedurais), uma autenticação multifatorial (MFA) fácil de usar talvez seja o mais crucial porque ela age como uma proteção contra senhas fáceis de adivinhar ou força bruta. Ao focar em autenticação para um sistema ou plataforma, neste caso RDP, você protege um dos sistemas mais críticos que você tem no seu negócio para administrar a segurança de ambos, sua rede e usuários individuais.

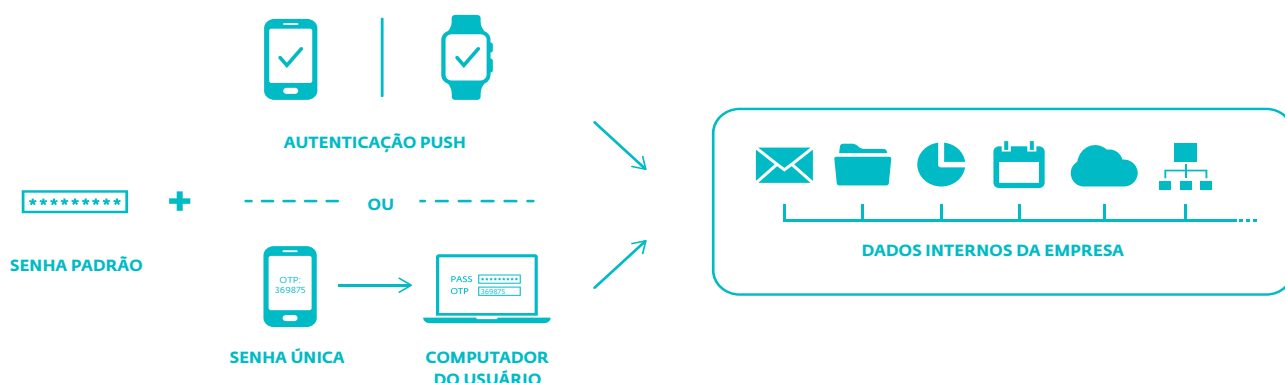
Nossa solução MFA [ESET Secure Authentication \(ESA\)](#) protege comunicações vulneráveis como Protocolo de Desktop Remoto ao adicionar autenticação multifatorial.

Uma solução como a ESA dá suporte a todas as VPNs (por si só um acesso de segurança de proteção crítica), logins em dispositivos críticos que contém dados sensíveis e serviços na nuvem como o Office 365, Google Apps ou Dropbox e muitos outros usando [ADFS 3.0](#) ou [SAML](#).

Gerenciado centralmente a partir do navegador, a ESA foi projetada para funcionar em todos os dispositivos iPhone e Android e também funciona bem com múltiplos tipos de autenticadores, incluindo notificações push fáceis de usar, aplicativos móveis, tokens de hardware, chaves de segurança FIDO e outros métodos personalizados (via a SDK ESA). Paralelamente, a ESA ajuda a proteger ambos, os dados da empresa e da nuvem de uma forma simples, mas poderosa, ela também ajuda a atender requisitos de conformidade para regulamentações como GDPR.

**POR EL COVID-19, Y PARA AYUDAR A LAS EMPRESAS A PROTEGER SUS SISTEMAS CRÍTICOS Y DATOS PERSONALES, ESET EXTIENDE EL PERÍODO DE PRUEBA GRATUITA A 90 DÍAS.**

Por último, adicionar [criptografia completa de disco](#) como um acompanhamento para o MFA também é um grande passo. O ESET Full Disk Encryption (EFDE) fornece uma criptografia poderosa de discos de sistema, partições ou drives inteiros. Eles são gerenciados nativamente por consoles de administração [ESET Security Management Center](#) e ESET Cloud Administrator, melhorando ainda mais a segurança dos dados de sua organização.





## CONHECIMENTO É PODER... SEGURANÇA TOTAL TAMBÉM

VÁRIAS [técnicas e táticas RDP também podem ser examinadas na base de conhecimento MITRE ATT&CK®](#). Ainda que referenciada por muitos pesquisadores de fornecedores, a base ATT&CK traz muita experiência para um espaço compartilhado. Alavancar ferramentas (EDR) e ATT&CK pode ser muito útil para examinar em detalhes ameaças a sua rede. Ferramentas como o [ESET Enterprise Inspector \(EEI\)](#) permite que administradores de segurança examinem detecções e façam referência direta à base ATT&CK para mais informações, configurando alarmes personalizados para sua rede.

Outra possibilidade com ameaças RDP é ter detecções (parciais), mas que permanecem desprotegidas. A EDR também pode ter um papel em cenários onde [detecções claras não podem ocorrer](#). Por exemplo, em alguns casos, o exploit BlueKeep travou imediatamente o sistema alvo porque ele se mostrou não confiável.

Então, para o exploit RDP funcionar, ele precisa ser pareado com outro exploit, como uma vulnerabilidade de revelação de informações (por exemplo, via arquivos php Flash) que mostram endereços de memória kernel para que eles não mais precisem ser adivinhados. Isso poderia reduzir a probabilidade de um travamento, já que o exploit atual realiza uma grande pilha de spray. Esses comportamentos associados podem ser sinalizados com regras personalizadas criadas dentro do EEI, objetivando por fim um alarme e chamando a atenção do administrador. Inteligência de rede adicional também pode ser fornecida via teste de penetração regular, e verificando comportamento suspeito via SIEM, [IPS](#), [IDS](#).

## CONCLUSÃO

**O COVID-19 mudou a forma que as organizações trabalham, não apenas temporariamente ao longo da pandemia, mas para sempre. Os empregadores precisam ajustar não apenas as demandas de colaboradores trabalhando de casa agora, mas também no futuro.**

**Uma coisa que a pandemia nos mostrou é que muitos trabalhos e tarefas que anteriormente se pensava que eram necessários ser feitos presencialmente pelos colaboradores no escritório serão agora vistos como ótimos candidatos para serem remotos. Mas, para que isso possa ocorrer, os trabalhadores remotos precisam ter acesso seguro ao escritório. A ESET oferece uma variedade de soluções que pode ajudar as empresas a fornecer acesso seguro para recursos corporativos.**

