heimdall

security research

A DIVISION OF ISH

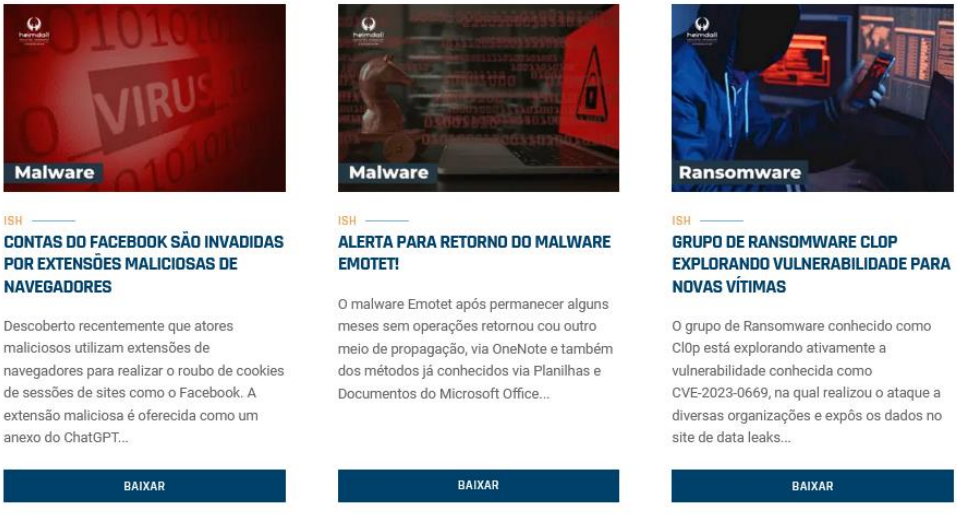
Riscos e Recomendações para serviços RDP expostos!

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Figuras

1 RDP (Remote Desktop Protocol)

O Protocolo de Área de Trabalho Remota (RDP), também conhecido como Remote Desktop Protocol em inglês, é um protocolo de comunicação desenvolvido pela Microsoft que permite o acesso remoto a computadores em uma rede. Ele é amplamente utilizado para permitir que os usuários acessem e controlem computadores remotamente, independentemente da localização física. O RDP funciona estabelecendo uma conexão entre um cliente e um servidor. O cliente RDP, geralmente um computador ou dispositivo móvel, inicia uma solicitação de conexão para um servidor RDP remoto. Após a autenticação e a autorização, uma sessão de área de trabalho remota é estabelecida entre o cliente e o servidor.

Durante a sessão remota, a interface gráfica do computador remoto é transmitida para o cliente, permitindo que o usuário interaja com o ambiente de trabalho remoto como se estivesse sentado fisicamente em frente ao computador remoto. O RDP transmite os gráficos, áudio e entrada do usuário através da rede, garantindo uma experiência de uso em tempo real. O RDP oferece recursos avançados, como redirecionamento de áudio e impressão, compartilhamento de área de transferência, redirecionamento de portas locais e suporte a múltiplas telas. Isso permite que os usuários executem aplicativos e acessem recursos do computador remoto de forma conveniente e eficiente.

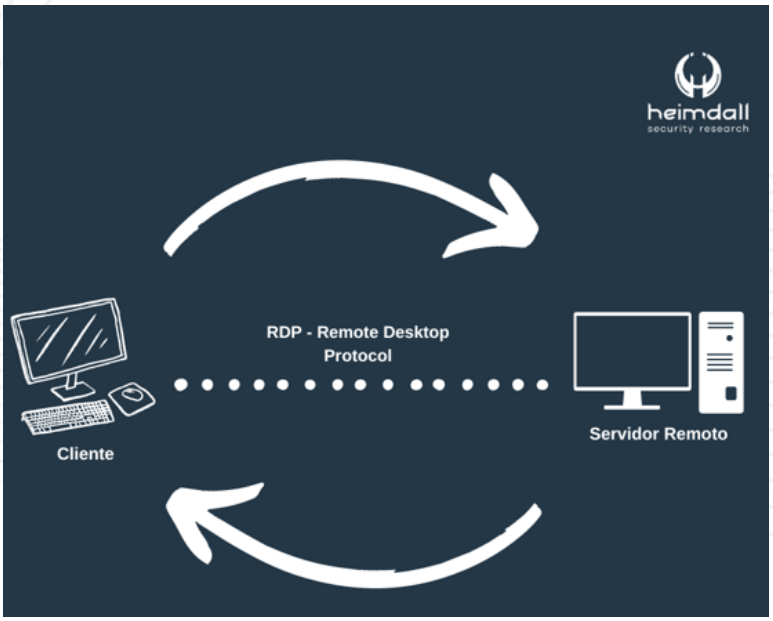


Figura 1 – Funcionamento do RDP.

2 RISCOS ASSOCIADOS A UTILIZAÇÃO DO RDP

Mesmo com todos os recursos e benefícios associados ao uso do serviço de conexão remota, o mesmo traz vários riscos de segurança para as organizações e governos ao deixarem os serviços RDP expostos à Internet. Alguns dos principais riscos de segurança associados ao RDP são listados abaixo:

Acesso não autorizado, ao expor o serviço RDP diretamente à Internet, as organizações aumentam a probabilidade de acesso não autorizado por parte de invasores. Hackers podem realizar ataques de força bruta ou explorar vulnerabilidades para obter acesso a sistemas e redes corporativas.

Roubo de informações confidenciais, um invasor que ganha acesso não autorizado a um sistema RDP pode acessar informações confidenciais, como dados de clientes, segredos comerciais, informações financeiras ou propriedade intelectual. Isso pode levar a violações de privacidade, roubo de identidade e danos à reputação da organização.

Ransomware e ataques destrutivos, os cibercriminosos podem usar o acesso RDP para implantar ransomware ou executar ataques destrutivos nos sistemas corporativos. Eles podem criptografar dados, bloquear o acesso aos sistemas ou causar danos irreparáveis, resultando em perda de dados e interrupção significativa dos negócios.

Espalhamento de malware, se um sistema RDP for comprometido, os invasores podem usar essa porta de entrada para espalhar malware para outros sistemas dentro da rede da organização. Isso pode resultar em infecções generalizadas, roubo de dados e interrupção dos sistemas.

Fraude e atividades criminosas, um invasor com acesso a um sistema RDP pode usar esses privilégios para realizar atividades criminosas, como fraude financeira, roubo de informações pessoais, lavagem de dinheiro ou acesso indevido a recursos sensíveis.

Comprometimento da rede, se um atacante ganhar acesso a um sistema RDP, ele pode tentar escalar seus privilégios e se mover lateralmente pela rede corporativa, comprometendo outros sistemas e servidores. Isso pode levar ao comprometimento generalizado da rede e dificultar a detecção e a resposta ao incidente de segurança.

3 VULNERABILIDADES EXISTENTES PARA O RDP

O Protocolo (RDP) já foi alvo de várias vulnerabilidades ao longo dos anos. Essas vulnerabilidades podem permitir que invasores explorem falhas no RDP para obter acesso não autorizado a sistemas remotos ou executar códigos maliciosos. Segue algumas das vulnerabilidades conhecidas associadas a explorações no protocolo:

BlueKeep (**CVE-2019-0708**): Uma vulnerabilidade crítica descoberta em 2019 que afetou várias versões do Windows. Ela permitia que invasores executem código remotamente sem autenticação, podendo resultar em ataques de ransomware em grande escala. A Microsoft lançou patches de segurança para corrigir essa vulnerabilidade, destacando a importância de manter os sistemas atualizados.

Pontuação base: 9.8 – Crítica

DejaBlue (**CVE-2019-1181**, **CVE-2019-1182**, **CVE-2019-1222**, **CVE-2019-1226**): Essas vulnerabilidades foram descobertas em 2019 e afetaram diferentes versões do Windows. Elas permitiam a execução remota de código malicioso por meio de conexões RDP, explorando falhas no processamento de pacotes RDP. A Microsoft lançou patches para corrigir essas vulnerabilidades.

Pontuação base: 9.8 – Crítica

CredSSP Encryption Oracle Remediation (**CVE-2018-0886**): Essa vulnerabilidade, descoberta em 2018, afetou a autenticação do RDP. Um invasor poderia explorar essa falha para realizar ataques de interceptação de dados ou obter acesso não autorizado a sistemas RDP.

Pontuação base: 7.0 – Alta

4 RDP EXPOSTO NO BRASIL

No Brasil, assim como em outros países, muitas organizações podem inadvertidamente expor serviços RDP diretamente na Internet, sem as devidas configurações de segurança. Isso pode ocorrer devido a configurações incorretas, falta de conscientização sobre os riscos ou negligência no gerenciamento de sistemas e redes.

Foi realizado uma busca de inteligência pelo time de CTI da ISH e foi possível encontrar um grande número de serviços RDP expostos no Brasil, essa verificação foi realizada através da porta padrão do RDP (3389). Porém esse número de exposição pode ser maior no país.

Figura 2 – Serviços RDP expostos no Brasil.

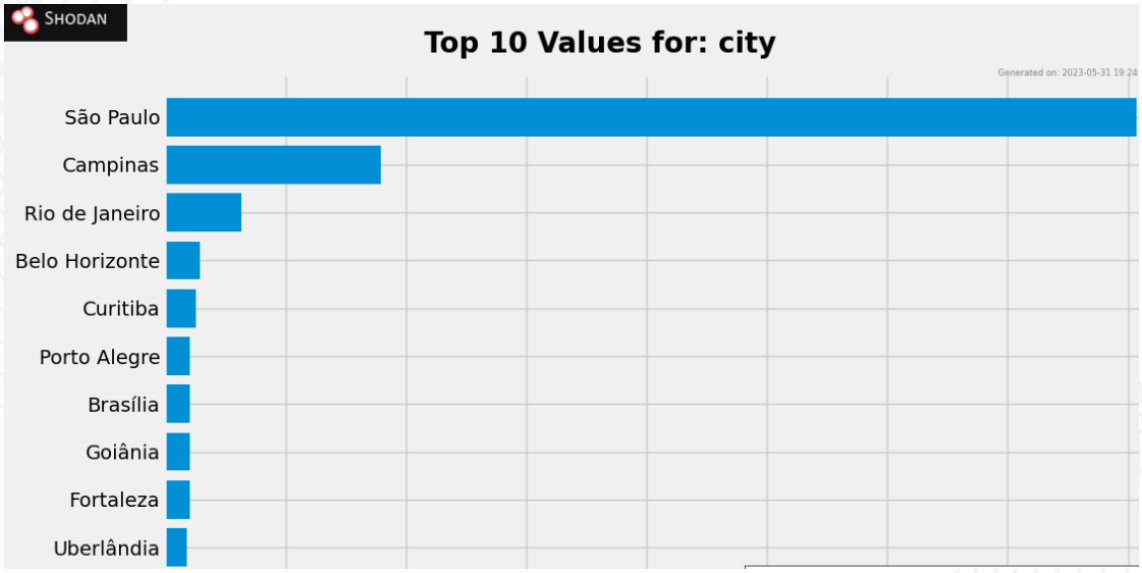


Figura 3 – Exposições por cidades no país.

Muitos profissionais de segurança recomendam alterar a porta do RDP de 3389 para uma porta não padrão em uma tentativa de mascarar o uso do RDP. Não há nada de errado em usar essa técnica, mas realizar essa alteração sem também implementar medidas de segurança necessárias, não fornece nenhuma segurança adicional.

Os IABs (indivíduos ou grupos que vendem acesso inicial a sistemas comprometidos para outras pessoas ou grupos que buscam lançar ataques cibernéticos, incluindo ataques de ransomware) estão bem cientes desses truques e verificam o serviço RDP em todas as portas pois eles estão bem mais interessados na resposta fornecida no banner do que em qual porta está aberta.

5 Conclusão

A exposição de serviços RDP (Remote Desktop Protocol) na Internet é uma prática arriscada podendo tornar as organizações e governos mais vulneráveis, levando a potenciais vulnerabilidades e vários ataques cibernéticos, conforme mencionados neste relatório, especialmente se medidas adequadas de segurança não forem implementadas. Portanto, é altamente recomendado não expor diretamente os serviços RDP à Internet.

6 RECOMENDAÇÕES

Para mitigar esses riscos de segurança, é fundamental adotar práticas de segurança adequadas ao usar o RDP, como por exemplo:

- Considerar o uso de soluções VPN para acessar remotamente os sistemas internos, em vez de expor diretamente o serviço RDP à Internet.
- Configurar firewalls para restringir o acesso ao serviço RDP, permitindo apenas conexões de IP confiáveis.
- Usar autenticação de dois fatores para aumentar a segurança das credenciais de acesso.
- Atualizar regularmente o software RDP e os sistemas operacionais com as últimas correções de segurança.
- Implementar monitoramento de segurança para detectar atividades suspeitas ou tentativas de acesso não autorizado.
- Educar os usuários sobre boas práticas de segurança e a importância de proteger as credenciais de acesso.
- Limite os privilégios concedendo apenas os privilégios necessários aos usuários que acessam o RDP. Evite conceder privilégios de administrador, a menos que seja absolutamente necessário.
- Utilize senhas fortes, defina senhas complexas e exclusivas para as contas de usuário do RDP. Evite senhas óbvias ou fáceis de adivinhar. Considere o uso de uma frase de senha longa em vez de uma senha curta.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Shodan.io**

heimdall
security research

A DIVISION OF ISH