MORPHUS
SEGURANÇA DA INFORMAÇÃO

Incidente Lojas Renner

Malware Overview: **RansomExx**

1.0 | 21/08/2021

Índice

1. SUMÁRIO EXECUTIVO

No dia 19 de agosto de 2021, as Lojas Renner S.A emitiu um comunicado informando que sua infraestrutura teria sido afetada por um ataque cibernético que teria causado indisponibilidade em parte da sua operação.

Segue a nota:

LOJAS RENNER S.A.
Companhia Aberta
CNPJ/MF n° 92.754.738/0001-62
NIRE 43300004848

COMUNICADO AO MERCADO

LOJAS RENNER S.A. ("Companhia"), em observância ao disposto na Instrução da Comissão de Valores Mobiliários ("CVM") n.º 358, de 30 de janeiro de 2002, conforme alterada, vem informar aos seus acionistas e ao mercado em geral que, nesta data, sofreu um ataque cibernético criminoso em seu ambiente de tecnologia da informação, que resultou em indisponibilidade em parte de seus sistemas e operação e prontamente acionou seus protocolos de controle e segurança para bloquear o ataque e minimizar eventuais impactos.

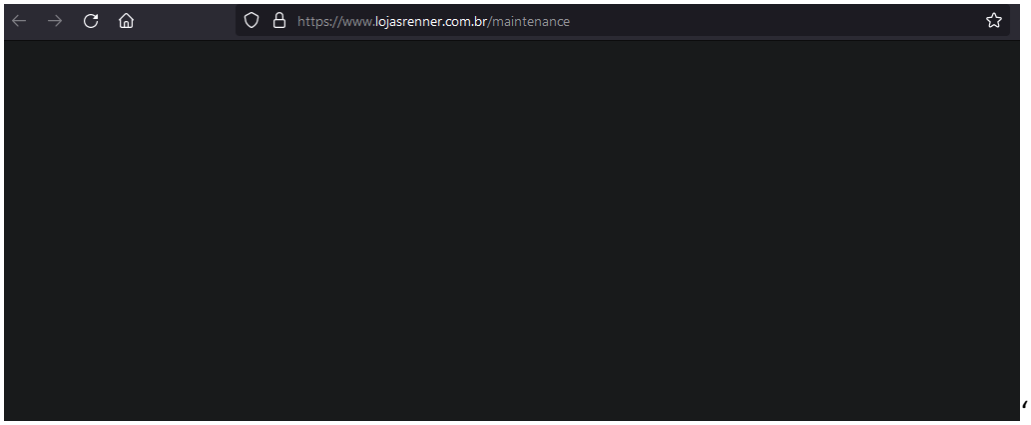
Neste momento, a Companhia atua de forma diligente e com foco para mitigar os efeitos causados, com a maior parte das operações já restabelecidas e tendo sido verificado que os principais bancos de dados permanecem preservados. Cabe ressaltar que em nenhum momento as lojas físicas tiveram suas atividades interrompidas. A Companhia ressalta ainda que faz uso de tecnologias e padrões rígidos de segurança, e continuará aprimorando sua infraestrutura para incorporar cada vez mais protocolos de proteção de dados e sistemas.

A Companhia manterá o mercado informado de qualquer informação relevante relacionada a este evento, e informará as autoridades competentes nos próximos dias.

Porto Alegre, RS, 19 de agosto de 2021.

LOJAS RENNER S.A.
Alvaro Jorge Fontes de Azevedo
Diretor de Relações com Investidores

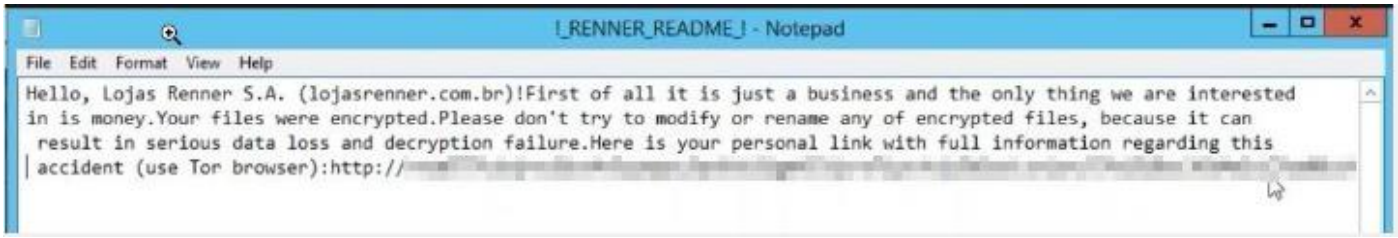
O site da Lojas Renner ficou indisponível desde quinta-feira (19/08/2021) à tarde, até pelo menos o início da noite da sexta-feira (20/08/2021).



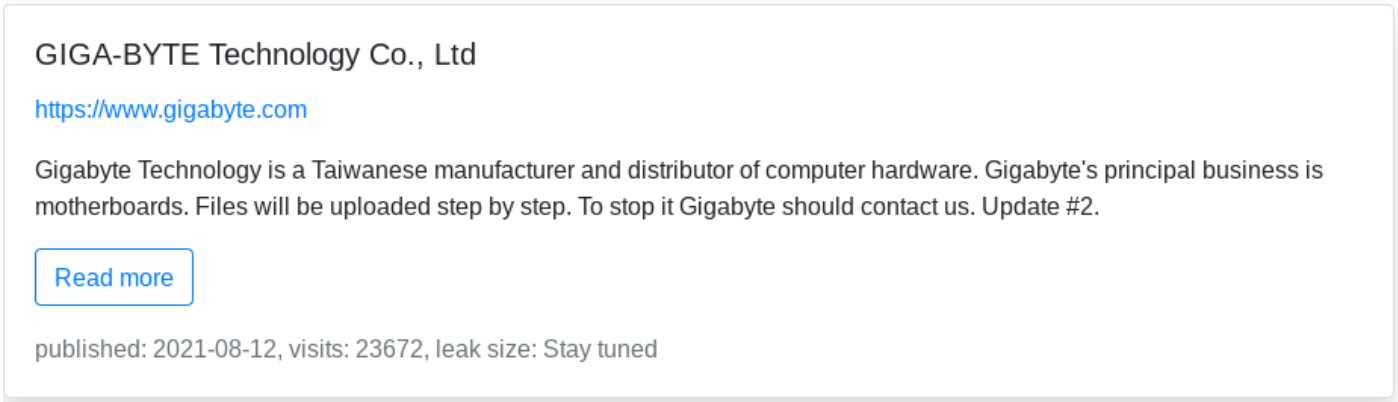
Fonte: https://www.lojasrenner.com.br/maintenance

Até o momento não podemos confirmar à atribuição da ameaça responsável por tal incidente, porém, devido a circulação de uma suposta nota de resgate, em que há a menção de um portal na Dark Web utilizado pelo ransomware RansomExx, cria-se uma hipótese de que o grupo por trás de tal ransomware, teria sido o autor de tal ataque.

Segue a nota de resgate em circulação:



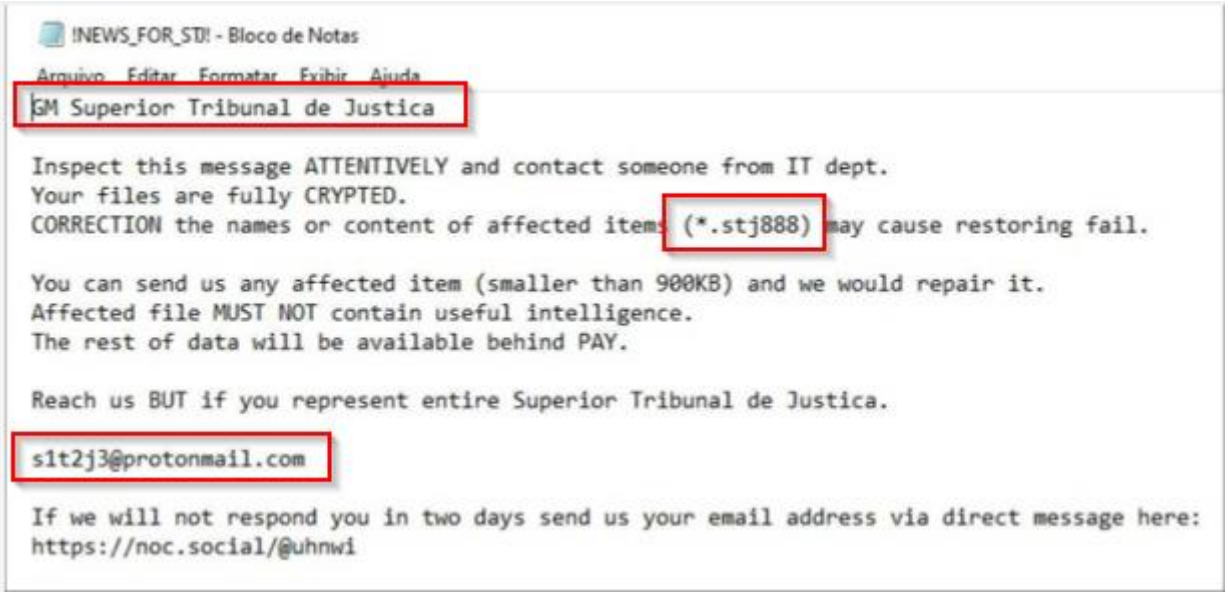
O portal mencionado é utilizado pelo grupo para publicar os dados exfiltrados de suas vítimas, caso o resgate não seja pago. Até o momento, não há qualquer menção à Renner neste portal, sendo a última publicação a da empresa Gigabyte Technology no dia 12 de agosto de 2021.



É importante destacar que o RansomExx é operado de maneira diferente de um Ransomware-as-a-Service (Raas). Um RaaS é um modelo de negócio utilizado por desenvolvedores de ransomware, no qual eles alugam variantes de seus ransomwares, da mesma forma que desenvolvedores de software legítimos alugam produtos SaaS. Assim, os desenvolvedores do ransomware, fornecem um painel de controle central para grupos afiliados criarem artefatos do ransomware, gerenciarem suas vítimas, postarem em blogs e compilarem estatísticas sobre o sucesso e o fracasso de seus ataques, ou seja, neste modelo a infraestrutura do malware é reutilizada para outras vítimas. Os ransomwares Lockbit e REvil são exemplos de RaaS.

No caso do RansomExx, este é operado por um grupo APT conhecido por Gold Dupont ou Sprite Spider, que realizam ataques manuais e personalizados para cada vítima, isto é, toda sua infraestrutura, binários, extensão de arquivos e até mesmo suas notas de resgate são personalizados para uma vítima específica.

Segue o exemplo de uma nota de resgate personalizada para o STJ:



2. THREAT PROFILE

O RansomExx, considerado uma variante do Defray777, é um ransomware de dupla extorsão que foi identificado pela primeira vez em junho de 2020, em um incidente onde comprometeu o Departamento de Transporte do Texas. Até então, o RansomExx somente criptografava os dados da vítima, atualmente os operadores exfiltram os dados da vítima e publicam no seu próprio portal, caso não seja realizado o pagamento.

Este Ransomware é utilizado em ataques mais elaborados nos quais os atacantes fazem uma parte do trabalho de invasão de forma manual — principalmente as fases de elevação de privilégios e movimentação lateral, além de personalizar seus ataques, de modo que até a extensão da nota de resgate remete ao nome da empresa vítima do incidente.

O RansomExx é operado por um grupo APT conhecido por Gold Dupont ou Sprite Spider, grupo de cibercriminosos com motivação exclusivamente financeira que também é responsável pelos ransomwares 777 e Defray777.

O grupo Gold Dupont está ativo desde 2018 e tem como característica estabelecer um acesso inicial através de credenciais válidas para serviços de acesso remoto como infraestrutura de desktop virtual (VDI) ou redes privadas (VPN). Em ocasiões, o acesso inicial já foi realizado através do malware Trickbot e do IcedID, que são distribuídos através de e-mail *phishing.*

Após o incidente que atingiu o Supremo Tribunal de Justiça (STJ) em novembro de 2020, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR) confeccionou um relatório no qual algumas vulnerabilidades teriam sido exploradas no ambiente. Segue a lista das CVEs:

- **CVE-2020-3992**– Vulnerabilidade RCE crítica que afeta o ESXi, **CVSS v3 9.8.**
- **CVE-2019-5544** – Vulnerabilidade RCE crítica que afeta o ESXi, **CVSS v3 9.8.**
- **CVE-2020-1472** – Falha crítica conhecida como Zerologon, é uma vulnerabilidade de escalação de privilégio no NetLogon. **CVSS v3 10.0. Há exploit público.**
- **CVE-2018-13379 –** Vulnerabilidade crítica que permite o download de informações e configurações de dispositivos Fortinet. **CVSS v3 9.8. Há exploit público.**

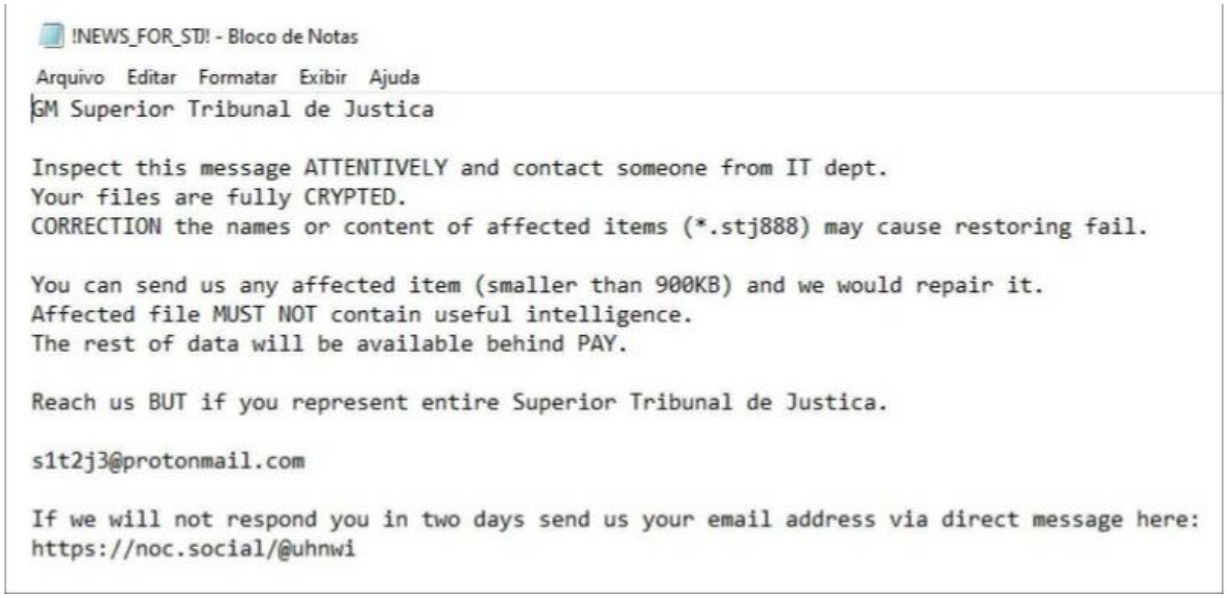
3. VITIMOLOGIA

O RansomExx não foca em nenhuma geolocalização ou setor específico, portanto, qualquer empresa pode ser um alvo do grupo que opera o ransomware. Pelo menos 4 grandes empresas brasileiras teriam sido vítimas deste ransomware.

3.1 SUPREMO TRIBUNAL DE JUSTIÇA (STJ)

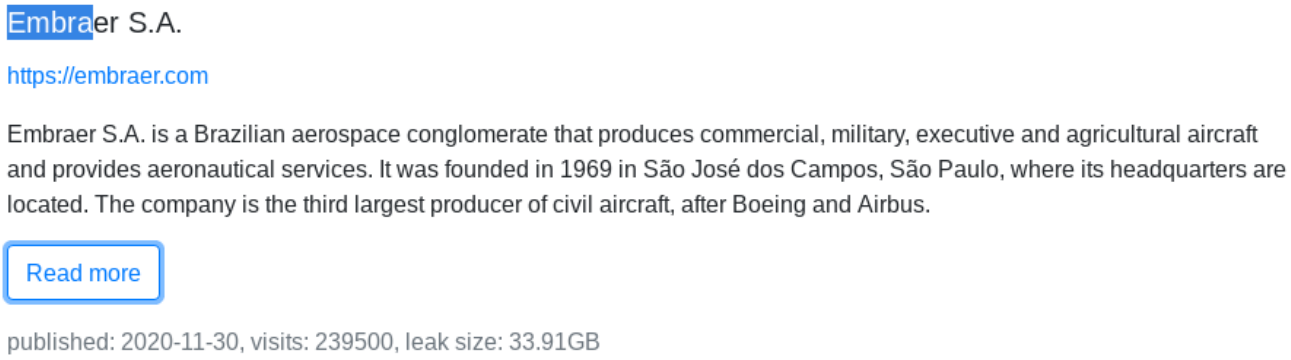
O primeiro caso de repercussão no Brasil foi o incidente no Supremo Tribunal de Justiça (STJ) ocorrido em novembro de 2020, porém, até o momento, o ransomware não realizava a exfiltração dos dados, mas somente os criptografava.

Segue a nota de resgate personalizada:



3.2 EMBRAER

O segundo caso de repercussão nacional foi o incidente na empresa de aviação Embraer. Neste momento, o RansomExx já possuía seu portal para a publicação de dados exfiltrados das vítimas. Um post mencionando a Embraer foi publicado no dia 30 de novembro de 2020, no qual informava que cerca de quase 34GB de dados poderia ser baixadas gratuitamente.



3.3 ULTRAPAR

No início de 2021, o grupo Ultrapar também teria sido vítima do RansomExx. De acordo com a publicação no portal do malware, quase 36GB foram exfiltrados e publicados para download.

Ultrapar Participações S.A.

https://www.ultra.com.br

Ultra is a Brazilian company operating in the sectors of fuel distribution, through Ipiranga and Ultragaz; in the production of specialty chemicals, through Oxiteno; in the storage of liquid bulk, through Ultracargo; and in pharmacies, through Extrafarma, all of which are subsidiaries entirely controlled by Ultrapar holding. The company is publicly traded under the name Ultrapar on São Paulo's stock exchange (B3) and on New York's (NYSE).

Read more

published: 2021-01-24, visits: 315253, leak size: 35.52GB

4. CONCLUSÕES

Ainda não podemos afirmar a autoria do incidente, pois, a **única suposta evidência** que temos é a nota de resgate que está circulando em grupos de mensagens instantâneas e redes sociais e, não podemos garantir que esta é verídica. Caso esta nota realmente seja verídica, o incidente teria sido causado pelo ransomware RansomExx, o mesmo que já afetou o STJ, Embraer, Grupo Ultra, entre outros. Porém, ainda não há não há qualquer menção à Renner no portal do RansomExx ou em nenhum outro portal de ransomware de dupla extorsão em que monitoramos.

Caso realmente tenha sido o RansomExx, este é operado por um grupo APT conhecido por Gold Dupont ou Sprite Spider, que realizam ataques manuais e personalizados para cada vítima, isto é, toda sua infraestrutura, binários, extensão de arquivos e até mesmo suas notas de resgate são personalizados para uma vítima específica. Sendo assim, os indicadores de comprometimento (IOCs) coletados a partir de um incidente que envolve o RansomExx, tende a não ser mais efetível em outro cenário. O foco deve ser na busca contínua por uma melhor postura na defesa cibernética das organizações, visando ações que mitiguem técnicas e ferramentas que geralmente são utilizadas em ataques de ransomware de dupla extorsão.

5. RECOMENDAÇÕES

Como ainda não podemos chegar a uma atribuição do incidente, seguem algumas recomendações que já publicamos em um artigo no Blog do Morphus Labs no final de 2020. Estas recomendações são mais estruturais e não focam em uma família de ransomware ou grupo específico, porém, se aplicadas, já fornecem grande efetividade na mitigação de riscos e impactos associados a incidentes de ransomware. Antes de aplicar as recomendações abaixo, é importante avaliar os impactos e realizar validações das mudanças em ambientes de homologação para evitar problemas no seu ambiente de produção.

5.1 Dê especial atenção a vulnerabilidades exploradas rotineiramente por atores maliciosos em 2020 e aquelas que estão sendo amplamente explorados até o momento em 2021.
Além das já citadas anteriormente, busque corrigir, caso ainda não tenha feito, as vulnerabilidades mais exploradas por atores maliciosos em 2020: CVE-2019-19781, CVE-2019-11510, CVE-2018-13379, CVE-2020-5902, CVE-2020-15505, CVE-2020-0688, CVE-2019-3396, CVE-2017-11882, CVE-2019- 11580, CVE-

2018-7600, CVE 2019-18935, CVE-2019-0604, CVE-2020- 0787, CVE-2020-1472, CVE-2019-19781, CVE-2019-11510, CVE-2018-13379. Sendo o CVE-2019-19781 a falha mais explorada em 2020.

Da mesma forma, priorize a correção dos CVEs mais explorados em 2021:
- Microsoft Exchange: CVE-2021-26855, CVE-2021-26857, CVE-2021- 26858 e CVE-2021-27065.
- Pulse Secure: CVE-2021-22893, CVE-2021-22894, CVE-2021-22899 e CVE-2021-22900.
- Accellion: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE2021-27104
- VMware: CVE-2021-21985.
- Fortinet: CVE-2018-13379, CVE-2020-12812 e CVE-2019-5591

5.2 É comum que as campanhas maliciosas com forte impacto no ambiente, com criptografia de múltiplos dispositivos, executem a coleta de credenciais com privilégios elevados na rede Microsoft. Um dos caminhos conhecidos é a obtenção de hashes, tokens e tickets armazenados na memória (processo LSASS) de dispositivos aos quais o atacante tenha privilégios locais elevados (ex: Mimikatz) para efetuar elevação de privilégios no domínio, mapeamento de compartilhamentos e movimentação lateral. Para evitar que o atacante tenha sucesso nesta estratégia, o melhor é não deixar credenciais com privilégios elevados disponíveis em hosts do ambiente. Para isso, recomendamos:

5.2.1 Não usar sessões interativas remotas com credenciais com privilégios elevados: RDP, *console logon*, *run-as*. Esta recomendação é especialmente útil para os servidores, normalmente acessados por vários usuários;

5.2.2 Finalizar as sessões RDP remotas ao encerrar o uso. Os hashes e tokens das credenciais ficarão disponíveis no sistema enquanto a sessão interativa estiver aberta. Se a conexão for desconectada, mas não finalizada (logout), o hash permanecerá no sistema e poderá ser roubado;

5.2.3 Ao executar atividades remotas de gerenciamento, dê preferência ao uso de *Powershell Remoting via Invoke-Command* ou *Enter-PSSession*. Desta forma, a credencial administrativa não ficará disponível no sistema remoto;

5.2.4 Ative o Credential Guard no Windows 10. Este recurso vai impedir a coleta de hashes e tokens diretamente do processo LSASS;

5.2.5 Utilize o Domain Protected Users. Este recurso vai fazer com que os usuários do grupo *Protected Users* não possam criar tokens delegados — mesmo em sessões interativas. Isso vai evitar a exposição desnecessária de tokens nos hosts da rede. É importante notar, no entanto, que as contas deste grupo não terão permissão para qualquer tarefa administrativa;

5.2.6 Senhas com privilégios elevados do domínio também podem ser obtidas nos serviços ou tarefas agendadas do Windows. As senhas dos serviços ficam armazenadas de forma criptografada no registro do Windows (LSA *Secrets*) e podem ser acessadas e decriptadas pelo administrador local. Evite ao máximo o uso de contas privilegiadas no domínio em serviços ou tarefas agendadas. Caso tenha que fazer, reforce o monitoramento da conta e use o recurso *Group Managed Service Accounts* para facilitar a troca da senha constante destas contas;

5.2.7 Certifique-se de que as contas locais de administrador são únicas para cada computador/servidor. O recurso LAPS (*Local Administrator Password Solution*) da própria Microsoft poderá ajudá-lo na tarefa de gerenciamento das contas de administração local para os computadores do domínio.

5.3 Habilite o recurso de senha para desativação/desinstalação da solução de *endpoint protection* dos computadores. É comum que os atacantes tenham que desinstalar o antivírus para executar o ransomware. A senha adicional pode não impedir totalmente, mas será uma barreira adicional;

5.4 Reforce o monitoramento de ações suspeitas como a autenticação em computadores que nunca foram utilizadas por uma determinada conta antes. Este poderá ser um indicador de movimentação lateral na rede;

5.5 Para os servidores que não precisarem iniciar conexões para a internet, desabilite ou restrinja ao máximo as conexões de saída. Esta ação poderá dificultar o download de novos componentes ou ferramentas necessárias para o ataque;

5.6 Restrinja ao máximo o compartilhamento via SMB (TCP/445). Geralmente, a comunicação envolvendo tal protocolo só se faz necessário entre estações de trabalho e controladores de domínio ou servidores de arquivos. A comunicação entre estações de trabalho, deve ser restringida. Tal restrição deve ser feita via segmentação de rede e restrição entre a comunicação destas. Isso pode ser feito via ACLs (*Access Control Lists*), regras de firewall de rede ou até mesmo em políticas de firewall do próprio Windows. As políticas de firewall do Windows podem ser aplicadas localmente ou de forma centralizada via GPO (*Group Policy*). Além da restrição do protocolo SMB entre segmentos de rede, restrinja também os seguintes protocolos:

- Protocolo de Área de Trabalho Remota (TCP/3389);
- Gerenciamento Remoto do Windows / PowerShell Remoto (TCP/80, TCP/5985, TCP/5986);
- WMI (faixa de porta dinâmica atribuída por DCOM);

Permita a comunicação destas portas aonde for estritamente necessário.

5.7 Considerando que, mesmo com a aplicação das boas práticas, seu ambiente foi comprometido por um ransomware, será de grande valia que você tenha previamente habilitado e preservado os registros de logs do Windows. São especialmente importantes os logs dos *Domain Controllers*, mas não economize na geração e na preservação de logs. Por exemplo, se você tiver logs de auditoria de acesso aos objetos do File Server, em uma resposta ao incidente poderá descobrir quais objetos foram lidos em massa pelo atacante e possivelmente exfiltrados. Ainda no quesito registro de logs, lembre-se que a habilitação de logs de tráfego (fluxos) também pode ajudar no trabalho de post-mortem.