Matrix desconstruído: a tendência para *ransomware* direcionado continua

- *A Sophos lançou um relatório que analisa o ransomware Matrix*
- *A forma de acesso principal ocorre através de firewalls que apresentam o protocolo de desktop remoto (RDP) ativado*
- *Como destacado no Threat Report da Sophos de 2019, os ataques de ransomware direcionados estão a ganhar relevo*

Lisboa, 31 de janeiro de 2019 – A Sophos (LSE:SOPH), líder global na segurança na rede e para endpoint, lançou um novo relatório sobre um grupo de *ransomware* conhecido como Matrix. Este *malware* tem estado em operação desde 2016 e a Sophos detetou 96 amostras. Tal como aconteceu com outros tipos anteriores de *ransomware* direcionado, incluindo o BitPaymer, o Dharma e o SamSam, os atacantes que utilizam o Matrix têm estado a infiltrar-se nas redes e a infetar computadores através do Remote Desktop Protocol (RDP), uma ferramenta de acesso remoto integrada nos computadores com sistema operativo Windows. No entanto, ao contrário de outros *ransomware*, o Matrix infeta apenas um único equipamento na rede, em vez de se propagar amplamente por toda a organização.

No seu último artigo, a SophosLabs submeteu o código e as técnicas, em constante evolução, assim como os métodos e as mensagens de extorsão de dinheiro às vítimas, a um processo de engenharia reversa. Os criminosos que criaram o Matrix fizeram evoluir os parâmetros dos ataques ao longo do tempo, adicionando um novo código e ficheiros que mobilizam diferentes tarefas e cargas na rede.

As notas de resgate do Matrix encontram-se introduzidas no código de ataque, mas as vítimas não sabem quanto terão de pagar até entrarem em contacto com os atacantes. Durante grande parte da existência do Matrix, os agressores utilizaram um serviço de mensagens instantâneas anónimas criptograficamente protegido, denominado bitmsg.me. Com a descontinuação deste serviço, os criminosos regressaram à utilização de contas de e-mail normais.

Os atacantes que utilizam o Matrix exigem o pagamento de um resgate em criptomoeda, em equivalentes a dólares americanos. Este facto é invulgar uma vez que, normalmente, cada criptomoeda vem com um valor específico na sua própria denominação, e não em equivalentes a dólares. Não é claro se esta exigência quanto ao resgate se trata de uma manobra deliberada de diversão, ou se resulta apenas de uma tentativa de navegar num cenário de taxas de câmbio de criptomoeda em forte flutuação. Com base nas interações que o SophoLabs teve com os atacantes, os resgates exigidos eram de 2500$ USD, apesar de este valor ter sido reduzido quando os investigadores deixaram de responder às exigências.

O Matrix é um pouco como o "canivete suíço" do mundo do *ransomware*, pois apresenta novas variantes capazes de pesquisar e identificar potenciais vítimas depois de infetada a rede. Apesar do volume da amostra ser reduzido, isto não torna esta ameaça menos perigosa, pelo contrário, o Matrix encontra-se em evolução e estão a surgir novas versões à medida que os criminosos aprendem com cada novo ataque.

No relatório de ameaças da Sophos de 2019, Sophos' 2019 Threat Report, destacamos que o *ransomware* dirigido será um dos fatores a influenciar o comportamento dos *hackers*, e as organizações devem permanecer atentas e trabalhar ativamente para assegurar que não são um alvo fácil de atingir.

A Sophos recomenda a implementação imediata de quatro medidas de segurança:

- Restrição do acesso a aplicações de controlo remoto tais como o Remote Desktop (RDP) e o VNC
- Verificação completa e regular da vulnerabilidade e testes de segurança em toda a rede. Se não realizou os testes de intrusão, está na altura de os fazer. Se continuar a ignorar os conselhos dos seus detetores de intrusão, os cibercriminosos serão bem sucedidos.
- Autenticação multifatores para sistemas internos sensíveis, mesmo para os colaboradores na LAN ou através de VPN.
- Criação de sistemas de back-up *offline* e *offsite*, bem como desenvolvimento de um plano de recuperação em caso de desastre, que abrange a restauração dos dados e dos sistemas para para todas as organizações, de uma vez só.

Para mais informações e análise, leia o relatório Matrix: "A Low-Key Targeted Ransomware" realizado pela Sophos: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-matrix-report.pdf.

# # #

Leia as últimas notícias sobre segurança na nossa página Naked Security News e saiba mais sobre a Sophos no nosso canal Sophos News.

Proteja todos os Mac e PC em sua casa com os softwares de segurança de próxima geração da Sophos Home.

Sobre a Sophos
A Sophos é uma empresa líder em soluções de segurança de '*next generation*' na rede e para *endpoint*. Enquanto pioneira na área da segurança sincronizada, a Sophos desenvolve um portfólio de soluções de segurança inovadoras para *endpoint*, rede, encriptação, web, email e mobile que trabalham perfeitamente em conjunto. Mais de 100 milhões de utilizadores em 150 países confiam nas soluções Sophos como a melhor proteção contra ameaças sofisticadas e perda de informação. Os produtos Sophos estão exclusivamente disponíveis através de um canal global com mais de 26.000 parceiros registados. A Sophos está sediada em Oxford, no Reino Unido e está cotada em bolsa na Stock Exchange de Londres, sob o símbolo "SOPH." Mais informação disponível em http://www.sophos.com/.

Siga a Sophos nas redes sociais: Twitter, LinkedIn, Facebook, Spiceworks, YouTube, Google+

Para mais informação, por favor contacte:

LEWIS

Clara Casanova Ferreira
910 928 302
clara.ferreira@teamlewis.com

Ana Marcelino
910 939 847
anacatarina.marcelino@teamlewis.com