SophosLabs revela que nenhuma plataforma é imune ao Ransomware

- Ransomware prefere sistema Windows, mas ataques a Android, Linux e MacOS também aumentaram em 2017
- Apenas duas variedades de ransomware foram responsáveis por 89,5% dos ataques interceptados nos computadores de clientes Sophos em todo o mundo

Lisboa, 14 de novembro de 2017 – A Sophos (LSE: SOPH), líder global de segurança na rede e em endpoint, apresenta o mais recente SophosLabs 2018 Malware Forecast, um relatório que sumariza a atividade de ransomware e em outras tendências de cibersegurança com base na informação recolhida de computadores de clientes Sophos em todo o mundo, entre 1 de abril e 3 de outubro de 2017. Uma das principais conclusões mostra que os sistemas Windows foram os mais atacados por ransomware nos últimos seis meses, mas as plataformas Android, Linux e MacOS não estão imunes.

"O ransomware tornou-se agnóstico em relação a plataformas. Embora ataque principalmente computadores Windows, este ano o SophosLabs viu um aumento no número de cripto-ataques em diferentes dispositivos e sistemas operativos utilizados pelos clientes mundialmente", disse Dorka Palotay, investigadora do SophosLabs e colaboradora na análise do ransomware no SophosLabs 2018 Malware Forecast.

O relatório também monitoriza os padrões de crescimento do ransomware, indicando que o WannaCry, libertado em maio de 2017, foi o ransomware mais interceptado pelos computadores dos clientes, destronando o líder histórico Cerber, que surgiu no início de 2016. O WannaCry representou 45,3% de todo o ransomware identificado através do SophosLabs, e o Cerber 44,2%.

"Pela primeira vez, vimos um ransomware com características de 'verme', o que contribuiu para a rápida expansão do WannaCry. Este ransomware aproveitou-se de uma conhecida vulnerabilidade do Windows para infetar e se espalhar pelos computadores, tornando-o difícil de controlar" explica Palotay. "Ainda que os nossos clientes estejam protegidos e o WannaCry tenha sido desativado, ainda vemos a ameaça que representa devido à sua natureza inerente de continuar a monitorizar e atacar computadores. Estávamos à espera que os cibercriminosos replicassem o que foi conseguido pelo WannaCry e o NotPetya, o que é já evidente com o mais recente ransomware Bad Rabbit, que mostra muitas semelhanças ao NotPetya".

O SophosLabs 2018 Malware Forecast reporta com detalhe o aparecimento e desaparecimento do NotPetya, o ransomware que causou o caos em junho de 2017. O NotPetya foi inicialmente distribuído através de um pacote de software de contabilidade Ucraniano, o que limitou o seu impacto geográfico. Espalhou-se através do EternalBlue, tal como o WannaCry, mas como o WannaCry já tinha infetado as máquinas mais expostas, foram poucas as que ficaram vulneráveis. O motivo por detrás do NotPetya ainda não é claro, pois existem vários erros, cracks e falhas neste ataque. Por exemplo, a conta de e-mail que as vítimas deviam utilizar para contactar os atacantes, não funcionava e as vítimas não puderam desencriptar e recuperar a sua informação, de acordo com Palotay.

"O NotPetya espalhou-se de forma rápida e agressiva, e afetou negócios porque destruiu permanentemente a informação dos computadores que atingiu. Felizmente, o NotPetya parou quase tão rapidamente como começou", diz Palotay. "Suspeitamos que os cibercriminosos estavam ou a fazer testes ou então o seu objetivo não era um ransomware, mas algo mais destrutivo como eliminar dados. Independentemente da sua intenção, a Sophos aconselha fortemente não pagar por ransomware e recomenda antes algumas boas práticas, incluindo fazer um *back up* da informação e manter as patches atualizadas".

O Cerber, vendido como um kit ransomware na Dark Web, continua a ser uma ameaça perigosa. Os criadores do Cerber atualizam continuamente o código e cobram uma percentagem do resgate que os atacantes intermediários recebem das vítimas. Novas funcionalidades regulares tornam o Cerber não só uma ferramenta de ataque eficiente, como permanentemente disponível para os cibercriminosos. "Este modelo de negócio da Dark Web infelizmente está a funcionar e à semelhança de uma empresa legitima está a financiar o desenvolvimento da Cerber. Podemos assumir que os lucros estão a motivar os autores deste ransomware a manter o código", diz Palotay.

O ransomware no Android está também a atrair os cibercriminosos. De acordo com a análise do SophosLabs, o número de ataques a clientes Sophos a utilizar dispositivos Android aumentou praticamente todos os meses em 2017.

"Só em setembro, 30,4% do malware malicioso presente em Android processado pelo SophosLabs, era ransomware. Estamos a prever que este valor aumente para os 45% em outubro", diz Rowland Yu investigador do SophosLabs e colaborador na análise do ransomware no SophosLabs 2018 Malware Forecast. "Uma razão pela qual acreditamos que o ransomware em Androids está a aumentar é por ser uma forma fácil dos cibercriminosos fazerem dinheiro em vez de roubar contactos e SMS, colocar anúncios pop up e preparar ataques de phishing bancário, que requerem técnicas de hacking mais sofisticadas. Importa reforçar que o ransomware Android é descoberto maioritariamente em mercados que não têm o Google Play – outra razão para os utilizadores terem cuidado com o tipo de apps que descarrega e onde o fazem".

O relatório SophosLabs revela outros dois tipos de métodos emergentes de ataque a Androids: bloqueio de telemóvel sem informação encriptada, e bloqueio do telemóvel enquanto encriptam a informação. A maioria dos ransomware em dispositivos Android não encripta a informação do utilizador, mas apenas o ato de bloquear um ecrã em troca de dinheiro é suficiente para deixar as pessoas a sofrer, especialmente considerando a quantidade de informação acedida diariamente num dispositivo pessoal. "A Sophos recomenda fazer *back up* dos dispositivos regularmente, tal como ao computador, para proteger a informação e evitar pagar resgate apenas para voltar a ter acesso à mesma. Prevemos que os ataques de ransomware a Androids continue a crescer e se torne o maior tipo de malware a atacar estes sistemas móveis no próximo ano", conclui Yu.

Para acesso ao relatório completo e ao infográfico, entre em SophosLabs 2018 Malware Forecast

Visite a Sophos News para mais informação detalhada 2018 Malware Forecast Ransomware Hits Hard Crosses Platforms e 2018 Malware Forecast Questions and Answers

# # #

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
Nanci Martinez
910 939 847
nanci.martinez@teamlewis.com

Ana Luzia
914 377 330
ana.luzia@teamlewis.com