ITENS DE NOTÍCIAS RELEVANTES

INFORMATIVO TÉCNICO

CIBERNÉTICA

RECRUDESCIMENTO DOS ATAQUES DE CRIPTOGRAFIA DE DADOS

Luiz Paulo Lopes dos Santos
Pós-Graduado, lato sensu, em Guerra Cibernética

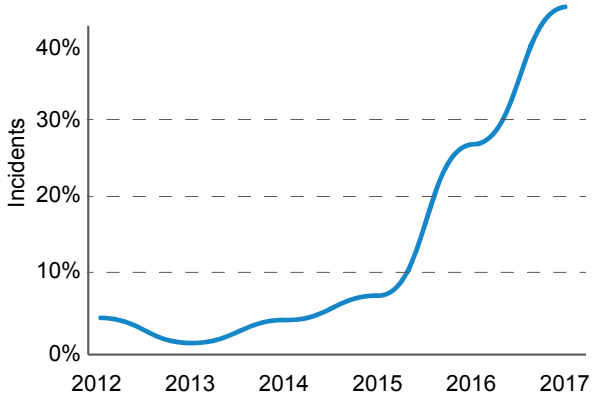
RESUMO: Um estudo recente de investigações sobre violação de dados revelou que o ransomware era a variedade mais prevalente de malware em 2017. De acordo com o "Relatório de Investigações de Violações de Dados (DBIR) de 2018 da Verizon", os profissionais de segurança identificaram o malware chamado ransomware em quase 40% dos incidentes de segurança que envolviam malware como uma de suas variedades de ataques. Esse tipo de ataque foi maior do que spywares, cavalos de Troia e outras formas de softwares mal-intencionados ao longo do ano. Os pesquisadores classificaram o ransomware como a quinta variedade de ação mais prevalente, com 787 incidentes, e observaram que o malware foi utilizado como uma tática em 30% dos eventos de segurança.

Palavras-chave: Phishing. Wannacry. Malware. Ransomware.

INTRODUÇÃO

Em maio de 2017, um ransomware, chamado de WannaCry, infectou mais de 200 mil computadores, fruto de um ataque que começou na Espanha e no Reino Unido, segundo HIGA (2017).

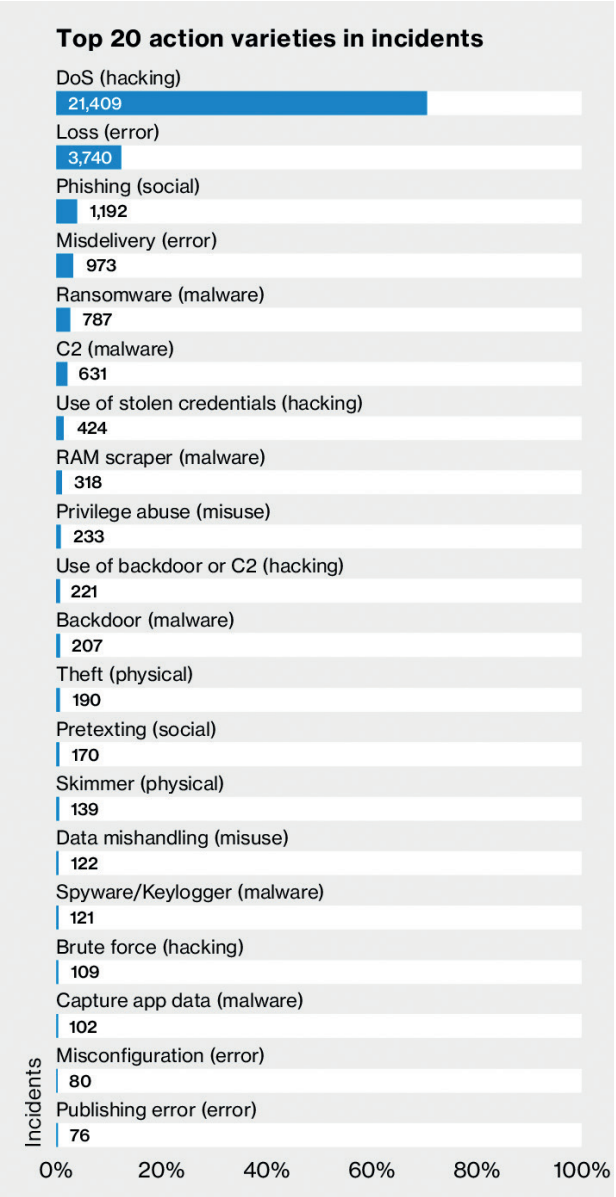
FIGURA 1 Ataque de rasomware nos últimos anos

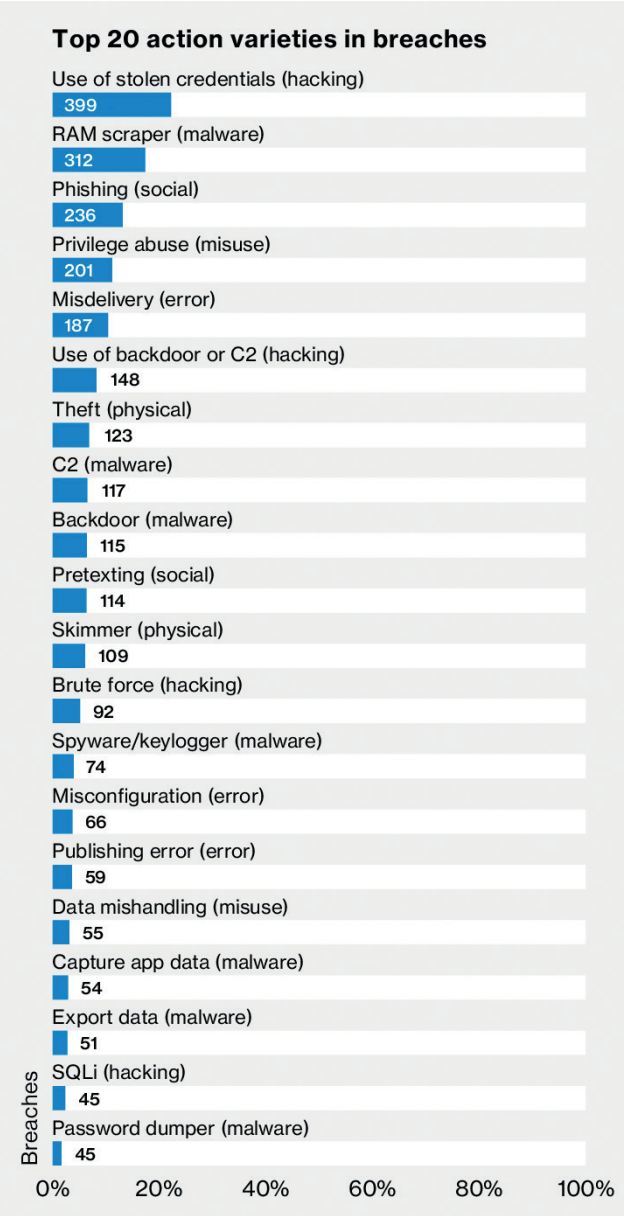


Fonte: DBIR 2018 – Verizon

Em 2018, de acordo com o relatório anual de informações da empresa Verizon, divulgado em 3/4/2018, podemos constatar que este tipo de malware ainda continua realizando seus ataques. A ameaça foi encontrada em 39% das violações de dados, o dobro em comparação com o ano passado, tornando-se a maior variedade de software malicioso.

FIGURA 2 As 20 principais variedades de ações em incidentes e violações





Fonte: DBIR 2018 - Verizon.

A 11ª edição do relatório analizou mais de 53.000 incidentes de segurança e 2.216 violações de 65 países. O relatório da Verizon aponta que os incidentes relacionados com o ransomware dobraram em relação a 2017.

O motivo pelo qual estamos vendo essa incrível prevalência do ransomware sob as demais formas de ataques está vinculado ao grande valor agregado capturado pelo invasor (ZDNET, 2018).

Os atacantes não precisam usar rotinas ou sistemas complexos para que se consiga infectar um computador. Uma vez “solto” dentro da máquina, o malware trabalha sozinho para infectar o alvo original e quaisquer outros periféricos conectados a mesma rede.

Antes era difícil para hackers configurarem a criptografia necessária para implantar o ransomware, porém, hoje eles podem simplesmente comprar o software de que precisam.

Um Script Kiddie, nome atribuído de maneira depreciativa aos hackers inexperientes que procuram alvos fáceis para aplicar seus poucos conhecimentos técnicos (DORKSLAB, 2017), geralmente usa ferramentas prontas na internet para realizar ataques, já que o risco é baixo, dada a facilidade de obtenção da ferramenta e alta recompensa vinculada ao êxito.

FIGURA 3 Script kiddie

IMPACTO

O ransomware também começou a impactar os sistemas críticos de negócios, acarretando em demandas de resgate maiores, fazendo com que os cibercriminosos obtenham mais dinheiro por menos trabalho.

Hoje, com a facilidade da criptomoeda, qualquer ataque hacker bem-sucedido de criptografia de dados terá o pagamento irrastreável (CCMTECNOLOGIA, 2018).

As pequenas e médias empresas/lojas são as mais impactadas com uma criptografia de dados. A título de exemplo, o hospital de Câncer de Barretos teve todas as suas unidades de prevenção espalhadas pelo Brasil afe-

tadas como registrou o portal de notícias G1. GLOBO (2017).

Isso significa que uma empresa que tenha todo o seu histórico de consultas, pagamentos, contas, devedores e diversas informações criptografadas, caso não possua um sistema de backup salvo do ataque, terá perda total de seus sistemas.

E esse tipo de ataque está fazendo diversas vítimas ao redor do mundo, de acordo com o site ZDNET (2018).

Essas empresas são coagidas a pagarem o resgate com criptomoedas, mesmo não tendo garantias de que os dados serão, de fato, devolvidos (FANTÁSTICO, 2017).

Também temos problemas e impactos causados às pessoas que continuam sendo vítimas de ataques de engenharia social, segundo o relatório. O email continua a ser o principal ponto de entrada para malware, com 96% dos ataques chegando através de caixas de entrada.

As empresas também têm quase três vezes mais chances de serem violadas devido a ataques de engenharia social do que com vulnerabilidades reais, destacando a necessidade de educação cibernética contínua dos funcionários.

O relatório também apontou que 78% das pessoas não estão caindo no golpe do phishing, alguns aplicados pelas próprias empresas para testar o treinamento de seus funcionários como esclarece Olenick (2017), e ensina Stu (2016), onde o primeiro fala que a melhor defesa é o ataque, e afirma que envia e-mails falsos para seus próprios funcionários, para testar o treinamento oferecido pela empresa contra o ataque, e estas por sua vez podem focar seus esforços de educação anti-phishing em pequenos grupos de empregados.

CONCLUSÕES

O ransomware, quando atua contra indústrias da área de saúde, apresenta um dano potencial, ainda, imensurável se confrontado com outras áreas industriais de significativa relevância.

O surto ocorrido em maio de 2017, deixando 34% dos hospitais do Serviço Nacional de Saúde do Reino Unido inoperantes exemplifica bem a suscetibilidade a ataques de malware. Essas informações coadunam com o relatório da Verizon, onde os dados apontam que 85% de todas as variedades de malware atingem os serviços de saúde (NHS, 2018).

O mesmo relatório observou que as organizações médicas são obrigadas por regulamentos federais a relatar ataques de ransomware como violações de dados e não como risco de dados. Portanto, é impossível saber se os hospitais e outros centros de saúde são mais suscetíveis a ransomware do que as organizações de outros setores, pois esses setores relatam os ataques como riscos de dados.

O relatório cita, ainda, boas práticas que buscam atenuar e erradicar os efeitos, tais como a autenticação de dois fatores, correção de vulnerabilidades de software e realização de treinos contínuos de conscientização de segurança aos usuários.

Por fim, embora tenha-se percebido, no ano de 2017, inúmeros ataques de rasonware a uma diversidade de setores, pouco foi feito no período de um ano, pois o novo relatório aponta carência de conscientização sobre a segurança de dados. É imprescindível que ações efetivas sejam tomadas, desde a atualização dos sistemas e softwares de proteção locais até a contratação de serviços de salvaguarda de dados, monitoramento e resolução de incidentes.

RECRUDESCENCE DATA ENCRYPTION ATTACK

ABSTRACT. A RECENT STUDY OF DATA BREACH INVESTIGATIONS REVEALED THAT RANSOMWARE WAS THE MOST PREVALENT VARIETY OF MALWARE IN 2017. ACCORDING TO VERIZON'S "DATA VIOLATIONS INVESTIGATION REPORT (DBIR) 2018, SECURITY PROFESSIONALS HAVE IDENTIFIED THE MALWARE CALLED RANSOMWARE IN NEARLY 40% OF SECURITY INCIDENTS INVOLVING MALWARE AS ONE OF ITS VARIETIES OF ATTACKS. THIS TYPE OF ATTACK WAS GREATER THAN

spyware, Trojans and other forms of malicious software throughout the year. The researchers ranked ransomware as the fifth most prevalent action variety, with 787 incidents, and found that malware was used as a tactic in 30% of security events.

Keywords: Phishing. Wannacry. Malware. Ransomware.

REFERÊNCIAS

CCMTECNOLOGIA. Veja como o sequestro de dados afeta pequenas e médias empresas, 2018. Disponível em: < https://www.ccmtecnologia.com.br/blog/veja-como-o-sequestro-de-dados-afeta-pequenas-e-medias-empresas/> Acesso em: 10 Maio. 2018.

DORKSLAB. Os tipos de hackers, 12 junho 2017. Disponível em: < http://www.dorkslab.com.br/2017/06/os-tipos-de-hackers.html/> Acesso em: 11 Maio. 2018.

FANTASTICO. G1.GLOBO. Hackers pedem resgate em moedas virtuais como o bitcoin, 14 maio 2017. Disponível em: <http://g1.globo.com/fantastico/noticia/2017/05/hackers-pedem-resgate-em-moedas-virtuais-como-o-bitcoin.html>Acesso em: 11 Maio. 2018.

G1.GLOBO. Após ciberataque, Hospital de Câncer de Barretos estima 5 dias para normalizar atendimentos em todo o país, 27 março 2018. Disponível em: <https://g1.globo.com/sp/ribeirao-preto-franca/noticia/apos-ciberataque-hospital-de-cancer-de-barretos-estima-5-dias-para-normalizar-atendimentos-em-todo-o-pais.ghtml/> Acesso em: 11 Maio. 2018.

HIGA, PAULO. Ransomware WannaCry já infectou 200 mil computadores em 150 países, Janeiro 2017. Disponível em: <https://tecnoblog.net/214656/wannacry-ataque-disseminacao-150-paises/>. Acesso em: 10 Maio 2018.

NHS. Lessons learned review of the WannaCry Ransomware Cyber Attack, 01 fevereiro 2018. Disponível em: <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf/> Acesso em: 11 Maio. 2018.

OLENICK, DOUG. Top 5 anti-phishing training programs, 10 outubro 2017. Disponível em: <https://www.scmagazine.com/top-5-anti-phishing-training-programs/article/699119/> Acesso em: 11 Maio. 2018.

STU. How To Phish Your Employees, janeiro 2016. Disponível em: <https://www.knowbe4.com/resources/how-to-phish-your-employees/> Acesso em: 11 Maio. 2018.

TECHPRORESEARCH. Cybersecurity spotlight: The ransomware battle, Agosto 2016. Disponível em: <http://www.techproresearch.com/downloads/cybersecurity-spotlight-the-ransomware-battle/>. Acesso em: 04 março 2018.

VERIZON ENTERPRISE. 2018 Data Breach Investigations Report, 09 Abril 2018. Disponível em: <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf>. Acesso em: 10 Maio 2018.

ZDNET. Atlanta, hit by ransomware attack, also fell victim to leaked NSA exploits, 27 março 2018. Disponível em: <https://www.zdnet.com/article/atlanta-hit-by-ransomware-attack-also-fell-victim-to-leaked-nsa-exploits/> Acesso em: 06 Março. 2018.

ZDNET. Cybercriminals switching from ransomware to mining malware attacks, 06 março 2018. Disponível em: <https://www.zdnet.com/video/cryptocurrency-mining-malware-now-as-lucrative-as-ransomware-for-hackers/> Acesso em: 04 Março. 2018.

O autor é graduado em Ciências Militares pela AMAN e pós-graduado em Guerra Cibernética pelo CIGE. Atualmente, exerce a função de Chefe de Seção de Ensino a Distância na Escola de Comunicações e pode ser contactado pelo email luizpaulo.santos@eb.mil.br