RANSOMWARE: DO SURGIMENTO AOS ATAQUES AS A SERVICE

José Eduardo de Souza Pimentel, FATEC-AM, jespimentel@uol.com.br
Diego Antunes Cabrera, FATEC-AM, diego.cabrera@fatec.sp.gov.br
Cleberson Eugênio Forte, FATEC-AM, cleberson.forte@fatec.sp.gov.br

Resumo

Os r*ansomwares* são armas eficazes de grupos de cibercriminosos altamente especializados. Têm se mostrado cada vez mais complexos e efetivos no objetivo de fomentar extorsões, particularmente quando os ataques se apresentam *as a service* e/ou são direcionados a alvos específicos. O presente artigo aborda questões ligadas à evolução do *ransomware*, suas espécies, formas de ataque – nomeadamente na modalidade *as a service*, que desponta como ainda mais desafiadora – e medidas específicas de defesa contra *ransomwares* recomendadas pela comunidade de cibersegurança, propiciando ao leitor uma visão panorâmica do tema. O método de pesquisa empregado foi o bibliográfico.

Palavras-chave: *ransomware*, cibercrime, defesa cibernética.

Abstract

Ransomware is an effective weapon for highly specialized cybercriminal groups. They have become increasingly complex and effective in the objective of extortion, particularly when it presents itself "as a service" and / or is directed to specific targets. This article addresses issues related to the evolution of ransomware, its species, forms of attack - namely in the "as a service" modality, which emerges as even more challenging - and specific measures of defense against ransomware recommended by the cybersecurity community, providing give the reader a panoramic view of the topic. The research method used was the bibliographic.

Keywords*: ransomware, cybercrime, cyber defense.*

1. Introdução

Os ciberataques vêm ganhando cada vez mais notoriedade, tanto pela sua crescente sofisticação, quanto pela importância das vítimas que alcançam. Mesmo corporações de prestígio, incluindo empresas especializadas em tecnologia da informação, estão sujeitas a essas ameaças e podem, em alguns cenários, ceder às extorsões de atores que comprometem a integridade, a confidencialidade ou a disponibilidade de seus dados.

Nesse cenário, os *ransomwares* se apresentam como importantes vetores de ataques, consistindo em armas eficazes e cada vez mais complexas de grupos de cibercriminosos altamente especializados, com aptidão para colocar em alerta a sociedade, governos e instituições, diante da possibilidade concreta de que informações e sistemas informáticos, dos quais dependem o *core business*, sejam atingidos.

O presente artigo se propõe a estudar os *ransomwares*, de sua concepção teórica à evolução para a modalidade *as a service*, explicando de que forma esse *malware* se transformou numa das maiores ameaças à cibersegurança e se apresenta, em 2021, com as características de uma indústria criminosa. Descrevem-se, em acréscimo, os procedimentos defensivos genéricos para a mitigação dos ataques de *ransomware*, adaptáveis a quaisquer redes de computadores, independentemente de sua dimensão e arquitetura.

O método de pesquisa empregado foi o bibliográfico, consistente na busca de informações em livros, teses, artigos científicos e demais publicações.

2. Do surgimento dos vírus de computador aos ataques de *ransomware*

Desde o final da década de 80, diversos softwares têm sido desenvolvidos com objetivos maliciosos. São conhecidos como *malwares* e, de acordo com Barão e Vilar (2016, p. 410), têm a finalidade "de se infiltrar em um sistema computacional e realizar a coleta de informações sem autorização ou simplesmente causar um dano". Nos dias atuais, a principal motivação para a construção de *malwares* é a obtenção de lucro, mas os precitados autores concordam que os objetivos podem ser outros, incluindo causas sociais e ideológicas.

A concepção teórica dos vírus de computador – códigos capazes de danificar as máquinas, copiar a si mesmo e infectar novos hospedeiros – parece ter nascido no final dos anos 1940, nas palestras do matemático John von Neumann, e consagrada no artigo *Theory of Self-Reproducing Automata* ("Teoria de autômatos autorreprodutores"), por ele publicado em 1966 (KASPERSKY, 2021; AVG, 2021).

O primeiro vírus de que se tem notícia foi chamado de *Creeper*. Foi criado em 1971, por Bob Thomas, da *BBN Technologies*, sem objetivo malicioso. Foi feito com o intuito de se replicar e, a cada nova infecção, removia-se do *host* anterior (KASPERSKY, 2021).

Em 1982 surgiu o *Elk Cloner*, primeiro vírus de propagação massiva entre os populares Apple II da época. Era executado após 50 inserções do disquete infectado no leitor. O resultado era a exibição de um poema na tela do usuário (AVG, 2021).

A partir de 1984, os vírus passaram a comprometer a memória RAM dos computadores, com a criação, nos laboratórios da *Bell Computers*, dos *Core Wars*, posteriormente difundidos nas universidades americanas (MEYER, 2015).

Em 1986, surgiram os *malwares Brain* e *Bouncing Ball*, os primeiros a infectarem o setor de *boot* dos disquetes. Na mesma época surgiram os vírus que infectavam arquivos com extensão exe e com. O *Brain* é considerado o primeiro vírus de PC (AVG, 2021) e, para fazer frente a ele, John McAfee criou o famoso antivírus *McAfee*, fundando a empresa homônima que, em 1992, estaria entre as 100 maiores dos EUA, segundo a Forbes (OFICINA DA NET, 2015).

Seguiu-se o *Bouncing Ball* (que ficou conhecido no Brasil como Ping Pong), com função não destrutiva (fazia com que uma bolinha percorresse a tela). Instalava-se no primeiro setor do disquete que, quando inserido, contaminava o computador e se copiava em outros disquetes conforme eram utilizados (MEYER, 2015).

De acordo com a AVG (2021), os vírus de computador não causaram maiores problemas até 1989. Nesse ano, porém, Joseph Frank Popp, um biólogo de Harvard, lançou o primeiro *ransomware*: o cavalo-de-troia AIDS (também conhecido como *PC Cyborg Trojan*). O *malware* possuía um contador que era incrementado a cada reinicialização do sistema operacional. Depois de 90 inicializações, o vírus ocultava os arquivos da máquina infectada, tornando-os inacessíveis ao usuário mediante o uso de

criptografia simétrica (uma única chave era usada para criptografar e descriptografar os arquivos), e exigia 189 dólares para restaurá-los. O dinheiro deveria ser enviado a uma caixa postal no Panamá. Popp acabou sendo preso sob acusação de chantagem, mas foi considerado inimputável no processo, tendo alegado aos investigadores que os lucros com o *ransomware* seriam destinados a pesquisas sobre o vírus (biológico) HIV.

Em 1992, apareceu o vírus *Michelangelo*, que permanecia inativo e indetectável até 6 de março, data do aniversário do referido artista, quando, então, corrompia os arquivos, neles sobrescrevendo caracteres aleatórios (AVG, 2021).

No ano de 1999 surgiu o vírus de macro *Melissa*, cuja importância reside no fato de ser o primeiro *malware* a usar engenharia social para a sua difusão, dado que se propagava por e-mail supostamente enviado por um dos contatos do alvo. Seu criador foi David L. Smith (AVG, 2021).

No ano 2000, o vírus *Iloveyou* infectou milhões de usuários do *Windows*, incluindo o Pentágono e a CIA. Era difundido por um e-mail com um arquivo anexo denominado *Love-letter-for-you*, que, ao ser executado, retransmitia a mensagem para todos os contatos do usuário (AVG, 2021).

Soares Filho (2020) informa que, no período compreendido entre 1989 (criação do AIDS) e 2005, não houve registro de ataques importantes de *ransomware*. O *ransomware* reapareceu, segundo o autor, em 2005, manifestando-se de forma mais agressiva. À época, porém, não havia criptomoedas (a concepção teórica da *bitcoin*, primeira moeda virtual, é datada de 2007) e não era fácil ao atacante lucrar com a extorsão. O panorama mudou, entretanto, em 2013, quando os resgates em *bitcoin* passaram a ser adotados e, em 2017, os ataques se tornaram verdadeiramente frequentes.

Na atualidade, o *ransomware* é considerado uma das maiores ameaças às redes de computadores e tem servido como vetor de extorsão em escala jamais vista em toda a história (SAVAGE, COOGAN e LAU, 2015).

3. Anatomia dos ataques

O *ransomware* é, segundo Hassan (2019, p. 25), "um *malware* de computador que se instala silenciosamente na máquina do usuário". O objetivo desse software é negar

acesso aos arquivos, às vezes criptografando o HD e outras unidades de disco, podendo atingir as contas de armazenamento em nuvem conectadas. Em seguida, prossegue o autor, "ele demanda que o usuário pague um resgate para que seu criador remova a restrição e o usuário ganhe acesso novamente ao sistema e aos ativos armazenados (*stored assets*)".

Os *ransomwares* se classificam em dois tipos, segundo suas principais características: *Locker-ransomware* e *Crypto-ransomware* (SAVAGE, COOGAN e LAU, 2015).

O *Locker-ransomware* impede o acesso aos recursos do computador, normalmente bloqueando a interface do usuário. O pedido de resgate é a condição para que o acesso à máquina seja restaurado. Os computadores bloqueados geralmente ficam com recursos limitados, às vezes permitindo que o usuário interaja apenas com o *malware* e use o equipamento para pagar a extorsão. O *Locker* pode, geralmente, ser removido da máquina infectada. É comum, portanto, que o ataque incorpore ações de engenharia social para incentivar o pagamento do resgate. Citam-se os casos em que o *malware* assume a identidade de autoridades policiais e cogita da emissão de multas por indiscrições ou atividades criminosas *on-line* (SAVAGE, COOGAN e LAU, 2015).

Esse tipo de *ransomware*, todavia, pode ser muito eficaz em dispositivos que fornecem interação limitada aos usuários, como os da categoria Internet das Coisas (IoT).

O *Crypto-ransomware*, por sua vez, é destinado a criptografar dados gravados no computador, tornando-os inacessíveis a menos que o usuário obtenha a chave que os decriptografa.

Muitos usuários não fazem backups regulares, cuja realização, convenhamos, não é trivial. Quando vitimados pelos ataques, podem se sujeitar à extorsão, dada a importância dos dados eventualmente atingidos.

Uma característica inerente aos *crypto-ransomwares* é que sua remoção do sistema operacional não restaura os arquivos comprometidos. No geral, os atacantes que se valem desse vetor cobram valores de resgate mais baixos, apostando na avaliação que a vítima tende a fazer da relação custo-benefício de tentar obter de volta a disponibilidade de seus dados (EVEO, 2019).

A exceção ocorre quando o *ransomware* compromete o funcionamento da empresa. Dependendo do tamanho da corporação, os criminosos podem cobrar dezenas de milhões de dólares, como ocorreu com a Acer, em março de 2021 (SOARES, 2021).

Savage, Coogan e Lau (2015) observam que os ataques de *ransomware* estão incorporando maior sofisticação. O sucesso da infecção depende do gerenciamento adequado das chaves usadas na criptografia. Citam, como exemplo de uma concepção mais simplista e já superada pelos *malwares* atuais, o *Trojan.Gpcoder.E*, surgido em 2007, que operava com uma chave de 32 bits e a deixava armazenada no registro do computador comprometido, tornando possível a restauração dos arquivos.

Outras arquiteturas optaram pelo armazenamento de chaves no próprio código do *ransomware* ou pelo uso da mesma chave para todas as variantes do software. Neste último caso, se um alvo obtivesse o código, poderia compartilhá-lo e ele serviria a outras amostras.

Os mesmos autores afirmam que, em meados de 2008, os atacantes passaram a adotar nos *ransomwares* algoritmos de criptografia padrão da indústria, como *RSA*, *Triple Data Encryption Standard* (3DES) e *Advanced Encryption Standard* (AES). O *Trojan.Gpcoder.F* (2008) usava RC4 para criptografar arquivos; depois criptografava a chave de criptografia RC4 usando uma chave pública RSA-1024; na sequência, apagava a chave original. Assim, ainda que a chave RC4 permanecesse no computador infectado, estava protegida por uma criptografia de chave pública forte, tornando-a imune ao uso de força bruta naquela época (SAVAGE, COOGAN e LAU, 2015).

Nem todos os ataques são dotados da mesma sofisticação. Muitos deixam algum espaço de manobra para seus alvos. Savage, Coogan e Lau (2015) suspeitam que o ambiente dos fabricantes de *ransomware* esteja fragmentado, com muitos novos atores tentando se estabelecer em um mercado já dominado por grupos de cibercriminosos profissionais.

Os ataques mais preocupantes são produzidos por *crypto-ransomwares* de alto nível de maturidade. Suas variantes geram uma nova chave assimétrica individual para cada infecção e apagam a chave de sessão da memória após o uso. Usam criptografia assimétrica (par de chaves pública e privada), de uso industrial, combinada com bons procedimentos operacionais, tornando teoricamente impossível a descriptografia sem o

pagamento do resgate. Somam-se a isso o uso de ferramentas de anonimização, como o Tor, e a opção pelo pagamento em criptomoedas (SAVAGE, COOGAN e LAU, 2015).

4. Evolução dos ataques: *as a service*

Os crimes cibernéticos sempre estiveram associados a *hackers*, pessoas com conhecimento diferenciado em tecnologia. No imaginário popular, tais atores consumiam considerável tempo de suas existências estudando arquiteturas de hardware ou sistemas com o objetivo de encontrar vulnerabilidades e explorá-las em seus ataques. Movia-os o desafio ou a diversão.

Na atualidade, todavia, não se exige o tal conhecimento para a prática do cibercrime, que, por sinal, tem atraído muita gente pelo potencial de lucro e anonimato. Diversas ferramentas têm sido oferecidas no mercado clandestino para a realização de ataques por leigos. Algumas consistem em softwares bastante amigáveis e de fácil uso. Muitas delas procuram suas vítimas de forma automatizada, o que acarreta um problema adicional à segurança cibernética.

Jesus e Milagre (2016, p. 163) consideram se tratar de uma nova tendência do cibercrime a modalidade *as a service*, na qual o ator encomenda um ataque contra um alvo específico.

Essa possibilidade é preocupante porque amplia o rol dos potenciais atacantes, incluindo entre eles pessoas com escasso conhecimento técnico. Também é um complicador para a investigação forense, porque o serviço pode ter sido contratado em algum país onde as autoridades têm pouca disposição em fornecer dados que contribuam para a identificação dos envolvidos no ataque.

De fato, o escaneamento de vítimas potenciais aumenta a distância psicológica entre autor e ofendido, mitigando o dilema moral que aquele possa ter em decorrência da prática do delito. Como observa Ayling (s.d.): quem rouba uma carteira se lembra com algum remorso do rosto da mulher que a possuía, mas o mesmo não ocorre com o fraudador cibernético, que não a vê.

Não é difícil encontrar plataformas que negociam essas ferramentas. São sites que contêm uma diversidade de produtos, classificações de clientes, ranking de popularidade

e até *help desk* (RIVA, s.d.). Tal realidade constitui um desafio de enormes proporções para indivíduos, corporações, governos e, particularmente, para as instituições incumbidas da repressão criminal.

Outra acepção da modalidade tem sido observada na formação de *startups* dedicadas à personalização de *malwares*.

É tendência mundial, principalmente nos EUA, o seguro voltado a ataques cibernéticos. A novidade fomenta um novo ramo de negócios, o *malware as a service*. Nele, *startups* criam os vírus e distribuem versões personalizadas e identificáveis a seus clientes para atacar vítimas institucionais. Havendo o pagamento do resgate pela vítima ou seguradora, os clientes são bonificados com parte do lucro, que pode chegar a 70% (SOARES FILHO, 2020).

O modelo parece ter sido inaugurado no ano de 2015. Neste ano, um *ransomware* foi disponibilizado como serviço em site da rede Tor, mediante o pagamento de comissão de 20% sobre o lucro obtido (MAURYA, 2018).

Embora os ataques-padrão de *ransomware* – assim considerados os difusos – rendam lucros de centenas de milhões de dólares aos seus operadores, há riscos e custos significativos na criação e manutenção de infraestruturas para ataques persistentes. Os criminosos também têm que lidar com questões diversas para que não sejam descobertos, incluindo mudanças de IPs, domínios, hospedagens e procedimentos para que não sejam bloqueados (TALOS, 2016).

De outra forma, um ataque empresarial direcionado pode ser realizado com ferramentas de código aberto, de forma rápida e eficaz. O sucesso de um ataque desse tipo pode levar ao pagamento do resgate em questão de dias. Os custos de infraestrutura são reduzidos e os recursos empregados no ataque podem ser removidos com bastante agilidade, de modo a dificultar a perseguição ao invasor e mantê-lo incógnito (TALOS, 2016; OSSAMU, 2020).

Os ataques direcionados seguem um padrão, no qual se identificam 5 fases[1]: a) **implantação**: nela os atores distribuem códigos essenciais para infectar, criptografar ou

[1] A MITRE Corporation, agência de consultoria sem fins lucrativos, descreve o ataque de *ransomware* em 12 etapas, a saber: acesso inicial, execução, persistência, escalonamento de privilégios, evasão de defesa, acesso à credencial, descoberta, movimento lateral, coleção, comando e controle (C2), exfiltração e impacto

bloquear o sistema. O *phishing* é uma forma bem conhecida para a realização desse passo; b) **instalação**: uma vez instalada a carga útil, os componentes são executados automaticamente. Buscam ganhar persistência, alterar chaves de registro e conceder a permissão para que os atacantes controlem a máquina infectada remotamente; c) ***Command-and-Control* (C2)**: ocorre quando o *malware* se conecta ao servidor de comando e controle (C2) e passa a receber instruções. Nessa fase, a chave de criptografia assimétrica é depositada em local inacessível à vítima; d) **Destruição**: neste momento, os arquivos são criptografados e são excluídas as cópias do sistema. O objetivo é que a decriptografia seja o único meio de restaurar os arquivos visados; e e) **Extorsão**: na última fase, a vítima toma conhecimento de que seus arquivos foram comprometidos e da possibilidade de reavê-los mediante o pagamento do resgate. Técnicas adicionais são empregadas para persuadir o alvo ao pagamento. As polícias não encorajam a submissão às exigências e não há garantia de que as informações sejam restauradas com o pagamento (THE HACKER NEWS, 2021).

Esse modelo permite ataques contra corporações com objetivos específicos. Inicialmente, o invasor busca adquirir credenciais de administrador de domínio do *Active Directory* e extrair informações do banco de dados *NTDS.dit*. Na sequência, os esforços podem ser voltados à identificação dos sistemas de *backup*, incluindo as plataformas que os executam, visando dificultar a recuperação dos arquivos. Esse passo é bastante importante para a obtenção do resgate. Outros procedimentos incluem a identificação dos sistemas com dados e arquivos críticos, incluindo bancos de dados, folha de pagamentos, aplicativos web, repositórios de códigos, pastas compartilhadas etc. A ação pode abranger a identificação dos servidores de mensagens (*VoIP*, *e-mail*, *Enterprise Messenger* etc) e sistemas de missão crítica, bem como os sistemas responsáveis pelos *pushes* de atualização de softwares e antivírus. Estes últimos sistemas, aliás, podem ser utilizados para distribuir a carga útil do *ransomware*, fazendo com que se espalhe mais rapidamente pela corporação atacada (TALOS, 2016).

O sucesso dessas ações reclama bastante especialização e, de fato, os grupos de cibercriminosos têm se mostrado mais colaborativos entre si.

(MILLER, 2020). Optamos, no entanto, por um framework simplificado e com menos fases para a melhor generalização dos casos (nota dos autores).

Os ataques mais sofisticados têm humanos no comando de todas as etapas da invasão, que se adaptam e reagem às ações defensivas eventualmente tomadas pelos alvos. Nesses cenários, o *ransomware* pode se manifestar como "a carga útil final" de um processo mais longo e para deixar explícito que o atacante já tem o controle da rede e está prestes a concluir o ataque (ROBERTS, 2021).

No ano de 2020, os atacantes incorporaram ao seu arsenal uma estratégia inédita, que lhes permitiu potencializar suas receitas. Os operadores do *ransomware Maze* conseguiram coletar dados de suas vítimas antes de criptografá-los e anunciaram que os divulgariam se o resgate não fosse pago. Essa tática foi acrescida ao ataque para atingir organizações mais bem preparadas para restaurar seus recursos, mas que temem a divulgação de suas informações. Supõe-se que o procedimento tenha se mostrado eficiente porque outros grupos que atuam por meio de *ransomwares* passaram a adotá-lo em suas investidas (OSSAMU, 2020). A modalidade vem sendo chamada de "ataque de dupla extorsão".

Em 2021, a nova versão do r*ansomware Darkside* surgiu com novidades. De acordo com fóruns especializados *XSS* e *Exploit* (apud: CISO ADVISOR, 2021), o *Darkside 2.0* para *Windows* se mostra capaz de criptografar arquivos com mais eficiência do que qualquer outro *ransomware as a service*, incluindo a versão anterior do mesmo *malware*, e oferece *multithreading* nas versões *Windows* e *Linux*. Outra notável inovação é a concepção de um site da marca *Darkside* com aspecto profissional, que inclui área de assessoria de imprensa para a divulgação de futuros vazamentos e com capacidade para estabelecer contatos com vítimas e jornalistas. No site são oferecidos serviços de decriptografia de empresas parceiras, são anunciadas doações a instituições de caridade, são publicadas análises de negócios das empresas vítimas e há lugar até mesmo para um questionável código de ética dos responsáveis pelo *malware*. Todos esses recursos foram pensados, certamente, para estimular o pagamento dos resgates. Para a Kaspersky, são indícios seguros de que os *ransomwares* estão se tornando uma indústria (DEDENOK, 2021).

5. Defesa

Os ataques de *ransomware* são, como visto, extremamente sofisticados. Muitos são bem planejados e empreendidos por grupos criminosos altamente especializados ou associados entre si. Os objetivos visados são claros e potencialmente aptos a causar prejuízos materiais e imateriais às corporações, às vezes atingindo a reputação das empresas construída ao longo de décadas.

A defesa contra a modalidade envolve o conhecimento do problema, da anatomia do ataque e dos possíveis cenários em desdobramento. A Cisco recomenda como ponto de partida a consideração dos seguintes fatores: a) os *ransomwares* estão evoluindo; b) *ransomwares as a service* são uma ameaça emergente; c) pagar o resgate não resolve problemas de segurança; d) a arquitetura de segurança deve ser estabelecida em camadas e baseada em padrões abertos; e) a defesa do ambiente deve ser exercida em profundidade (e não com produtos de segurança pontuais ou autônomos); f) a segurança deve abranger todo ambiente de rede; g) a complexidade do seu ambiente de segurança deve ser reduzida; h) deve-se preferir a nuvem para a inteligência contra ameaças cibernéticas em tempo real; i) deve-se automatizar as ações de resposta *antimalware* e contra intrusão para reduzir o tempo de resposta; j) por fim, deve-se adotar a máxima “viu algo, diga algo”, estabelecendo-se, com isso, a cultura de reportar as infecções aos órgãos competentes (MILLER, 2020)

No que diz respeito às estratégias de mitigação do problema, o *framework* da Talos Intelligence (TALOS, 2016) figura-se como bem adequado, dada sua abordagem genérica e completude. As ações sugeridas compreendem: a) a prevenção do acesso inicial; b) o fortalecimento da rede de perímetro (DMZ); c) o controle de *phishing* e engenharia social; d) a restrição ao movimento lateral e da propagação do *malware*; e e) recuperação do *backup*.

A prevenção do acesso inicial é a primeira e mais importante medida sugerida. Parte do pressuposto de que alguns atacantes são oportunistas e, encontrando obstáculos, podem desistir da invasão. As atitudes em relação a esse aspecto incluem a atenção a atitude dos colaboradores internos em relação à política de segurança da empresa (TALOS, 2016).

O fortalecimento da rede de perímetro (*Delimitarized Zone* ou DMZ) abrange verificações periódicas dos serviços e sistemas que a organização está expondo à Internet. Nesse campo vige a regra de que quanto menos serviços disponibilizados, menor será a superfície de ataque disponível. No tocante aos serviços essenciais, convém que sejam realizadas varreduras de rotina para a identificação de vulnerabilidades e que, uma vez descobertas, sejam imediatamente corrigidas (TALOS, 2016).

O controle de *phishing* e engenharia social envolve o conhecimento do problema por todos os colaboradores e treinamento constante. O compartilhamento de arquivos deve ser preferível à sua anexação em e-mails. Especial atenção deve ser dada ao formato pdf, dado ser conhecido que softwares de leitura desses formatos podem conter vulnerabilidades. Os usuários devem ser orientados a relatar incidentes ao departamento de segurança sem qualquer constrangimento ou temor (TALOS, 2016).

A restrição ao movimento lateral do *malware* é de fundamental importância após a invasão, pois evita o maior comprometimento da rede corporativa. Nesse campo, destaca-se a importância da arquitetura da rede, que deve ser precedida de planejamento cuidadoso em termos de segmentação. Sugere-se que cada unidade de negócios disponha de sua própria VLAN e sub-rede, de forma a separar logicamente os dados. O uso de *firewalls* baseados em *hosts* é recomendado. Nesse âmbito, o adequado gerenciamento de senhas e credenciais também tem bastante valor, sugerindo-se o emprego da permissão de compartilhamento de rede baseada em função (menos privilégio). Pode-se pensar, em acréscimo, no uso da lista branca de aplicativos e/ou bloqueio de executáveis a partir de diretórios específicos (TALOS, 2016).

A recuperação do *backup* é o último recurso para se evitar o pagamento do resgate. Nesse ponto, deve-se considerar a capacidade de recuperação do ataque, com perda mínima de dados e o tempo necessário para essa operação. Conhecem-se muitos métodos de *backup*. Em alguns cenários, nos quais se verifique o comprometimento de todo o ambiente, os *backups* externos se apresentam como a única solução. É de se anotar que nem sempre a opção de *backup* em nuvem resolve completamente o problema. Essa alternativa exige bastante cuidado com as credenciais, pois o gerenciamento deficiente ou o reuso de senhas pode contribuir para que os arquivos em nuvem se tornem igualmente indisponíveis (TALOS, 2016).

6. Considerações finais

Os vírus de computador nasceram inofensivos, mas evoluíram ao longo de anos e, na atualidade, destinam-se, geralmente, a fins maliciosos. Dentre as diversas espécies de *malwares*, destacam-se, atualmente, os *ransomwares* que, no estado da arte, servem a grupos criminosos sofisticados e instrumentalizam a obtenção de lucros ilegais. Têm servido a extorsões de monta e representam ameaça concreta a cibersegurança.

O presente artigo descreveu a evolução dos *ransomwares*, da concepção à modalidade *as a service*, hoje patrocinada por *startups* e grupos criminosos altamente especializados.

Realçou, ainda, as operações cada vez mais frequentes de ataques de *ransomwares* direcionados a alvos específicos, que potencializam as possibilidades do ganho ilícito e representam um desafio adicional às organizações no objetivo de zelar pela reputação de suas marcas.

Por fim, apresentou uma visão macro das medidas de segurança que se supõem mais efetivas para a defesa contra os *ransomwares*.

O estudo nos permitiu concluir que os *ransomwares* devem ser considerados como ameaças das mais importantes para as redes de computadores. Essa realidade exige que o profissional de segurança da informação se mantenha atuante e muito bem-informado sobre a evolução, tipos, formas de infecção e demais aspectos relacionados ao problema, sem o que não será capaz de atuar com eficiência para prevenir e mitigar os ataques.

Como trabalho futuro, cogita-se minudenciar as etapas de defesa citadas no presente artigo e classificá-las segundo a efetividade que possam ter diante dos *ransomwares*.

Referências

AVG. “Uma breve história dos vírus de computador”. Disponível em: <https://www.avg.com/pt/signal/history-of-viruses>. Acesso em: 16 mar. 2021.

AYLING, Tim. “Cyberfraude and emotional detachment”. Buguroo. Disponível em:<https://www.buguroo.com/en/blog/cyberfraud-and-emotional-detachment>. Acesso em: 15 mar. 2021.

BARÃO, Rafael Eduardo e VILAR, Gustavo Pinto. Exames em malwares. In: Velho, Jesus Antonio (org.). "Tratado de computação forense". Campinas, SP: Millenium Editora, 2016, p. 409-445.

CISO ADVISOR. "Nova versão do ransomware Darkside pode sequestrar máquinas virtuais". 12 mar. 2021. Disponível em: <https://www.cisoadvisor.com.br/nova-versao-do-ransomware-darkside-pode-sequestrar-maquinas-virtuais-e-storage-nas/>. Acesso em: 25 abr. 2021.

EVEO. "Ransomware: saiba quais são os principais e como melhorar a sua segurança". 14 jun. 2019. Disponível em <https://www.eveo.com.br/blog/principais-tipos-ransomware/>. Acesso em: 29 mar. 2021.

DEDENOK, Peter. "Cinco sinais de que os ransomwares estão se tornando uma indústria". 19 abr. 2021. Kaspersky Daily. Disponível em: <https://www.kaspersky.com.br/blog/darkside-ransomware-industry/17323/>. Acesso em: 25 abr. 2021.

HASSAN, Nihad A. "Perícia forense digital". Traduzido por Aldir Coelho Corrêa da Silva. São Paulo: Novatec Editora Ltda, 2019.

JESUS, Damásio de; MILAGRE, José Antonio. "Manual de crimes informáticos". São Paulo: Saraiva, 2016.

KASPERSKY. "Um breve histórico dos vírus de computador e qual será o seu futuro". Disponível em: <https://www.kaspersky.com.br/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>. Acesso em: 15 mar. 2021.

MAURYA, A. K, et. al. Ransomware: Evolution, Target and Safety Measures. In: "International Journal of Computer Sciences and Engineering", vol. 6, issue 1. 31 jan. 2018, p. 81-85. Disponível em: <https://www.researchgate.net/publication/325777408_Ransomware_Evolution_Target_and_Safety_Measures>. Acesso em: 19 mar. 2021.

MEYER, Maximiliano. "Os primeiros vírus de computador da história". Disponível em: <https://www.oficinadanet.com.br/post/13962-os-primeiros-virus-de-computador-da-historia>. 2015. Acesso em 25 set. 2021.

MILLER, Lawrence. "Ransomware defense" [Cisco 2nd Special Edition]: for dummies. Hoboken, NJ: John Wiley & Sons, Inc. 2020 [e-book].

OFICINA DA NET. John McAfee. "O maior badass do mundo da tecnologia" (parte 1). Disponível em: <https://www.oficinadanet.com.br/post/14006-john-mcafee-o-maior-badass-da-tecnologia>. Acesso em: 15 mar. 2021.

OSSAMU, Carlos. "Symantec prevê ataques mais agressivos de ransomware". 20 nov. 2020. Inforchannel. Disponível em: <https://inforchannel.com.br/symantec-preve-ataques-mais-agressivos-de-ransomware/>. Acesso em: 29 mar. 2021.

RIVA, Pablo de la. “Cybercrime.org. Cybercrime as a business”. Buguroo. Disponível em: <https://www.buguroo.com/en/blog/cybercrime-org-cybercrime-as-a-business>. Acesso em: 9 mar. 2021.

ROBERTS, Paul. “Netfilim and Ransomware’s Long Fuse”. 29 jan. 2021. QOMPLX Blog. Disponível em: <https://www.qomplx.com/netfilim-and-ransomwares-long-fuse/>. Acesso em: 25 abr. 2021.

SAVAGE, Kevin; COOGAN, Peter; e LAU, Hon. “The evolution of ransomware”. Version 1.0. 6 ago. 2015. Symantec. Disponível em <https://docs.broadcom.com/docs/the-evolution-of-ransomware-15-en>. Acesso em: 16 mar. 2021.

SOARES FILHO, Gilberto. “Ransomwares: da insanidade ao modelo de negócios”. 2020. Tecnoblog. Disponível em: <https://tecnoblog.net/324768/ransomwares-da-insanidade-ao-modelo-de-negocios>. Acesso em: 17 mar. 2021.

SOARES, Lucas. “Hackers invadem Acer com ransomware e exigem U$ 50 milhões como resgate”. 19 mar. 2021. Olhar Digital. Disponível em: <https://olhardigital.com.br/2021/03/19/seguranca/hackers-invadem-acer-com-ransomware-e-exigem-us-50-milhoes-como-resgate/>. Acesso em: 29 mar. 2021.

TALOS. “Ransomware: past, presente and future”. 11 abr. 2016. Cisco Talos Intelligence Group. Disponível em: <https://blog.talosintelligence.com/2016/04/ransomware.html>. Acesso em: 29 mar. 2021.

THE HACKER NEWS. “Everything You Need to Know About Evolving Threat of Ransomware”. 24 fev. 2021. Disponível em: <https://thehackernews.com/2021/02/everything-you-need-to-know-about.html>. Acesso em: 5 abr. 2021.