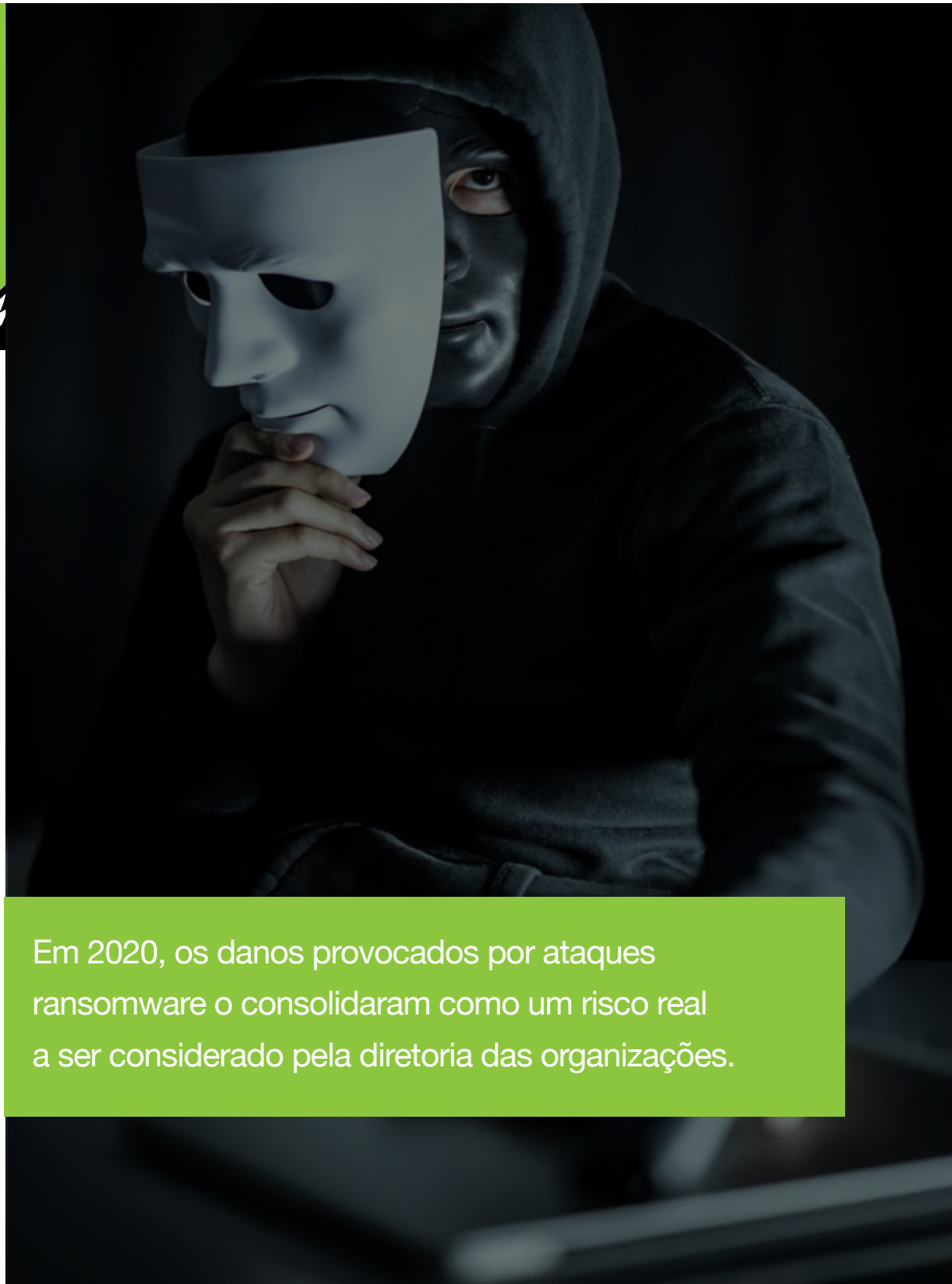
A Avalanche de Ataques Ransomware em 2020 —Como Sobreviver em 2021

RIDGE SECURITY



Em 2020, os danos provocados por ataques ransomware o consolidaram como um risco real a ser considerado pela diretoria das organizações.

A Avalanche de Ataques Ransomware em 2020 —Como Sobreviver em 2021

O ataque ransomware é uma forma de extorsão, tendo o valor dos resgates aumentado drasticamente em 2020. Notícias sobre empresas atingidas por ataques ransomware que resultaram em consequências devastadoras, com valores de resgate exorbitantes, tornaram—se recorrentes nos noticiários especializados.

Em 2020, os danos provocados por ataques ransomware o consolidaram como um risco real a ser considerado pela diretoria das organizações. Todos os aspectos desse tipo de ataque cibernético estão em alta.

- Número de vitímas
- Número de resgates
- Valor dos resgates
- Dano às organizações
- A extorsão pelos dados roubados, além do resgate pela sua descriptografia

De acordo com o relatório “The State of Ransonware in 2020” da BlackFog: “ataques ransomware são um grande negócio, tão grande que as pesquisas demonstram que uma empresa é atacada por cibercriminosos a cada 11 segundos, de modo que os danos daí decorrentes deverão atingir cerca de USD 20 bilhões até 2021.” Um ciberataque ao Hospital Universitário de Düsseldorf na Alemanha, em setembro de 2020, resultou no falecimento de um paciente da emergência que, em decorrência do ataque criminoso, precisou ser transferido para outra unidade hospitalar não conseguindo ser socorrido a tempo.

Tendências Sobre Ransomware

As tendências apontam para um rápido crescimento tanto na frequência quanto no tamanho dos ataques em 2021. Os cibercriminosos vêm atualizando seu roteiro de ataque visando resgates maiores e mais certeiros.

Tendências que Acarretam no Crescimento dos Ataques Ransomware

As tendências empresariais e da indústria em geral aumentaram drasticamente a superfície de ataque nas redes das corporações, entidades governamentais e pequenas empresas. Novas tendências abriram novas oportunidades.

- **Migração para nuvem:** As tecnologias baseadas em nuvem cresceram exponencialmente nos últimos anos, resultando em significativa economia de custos e agilidade nos negócios para organizações de todos os portes. As plataformas e os serviços em nuvem garantem cada vez mais flexibilidade em termos de recursos de armazenamento, computação, pagando-se pelo o que for utilizado, e escalando-se ou reduzindo-se conforme a demanda, em vez de realizarem-se investimentos de capital pesados na aquisição de infraestrutura.
- **Pandemia do COVID-19 e Trabalho Remoto:** A resposta global à pandemia resultou em uma mudança repentina de deslocamento da força de trabalho para ambientes móveis e remotos. Os urgentes esforços organizacionais para manter a continuidade dos negócios aceleraram a já crescente migração para a nuvem. De forma conjunta, a nuvem e o trabalho remoto dissolveram o tradicional e rígido perímetro de rede corporativa, substituindo-o por um perímetro definido por software (SDP) que funciona sobre qualquer superfície da rede com acesso à internet. As organizações vêm lutando para se adaptarem às novas habilidades e tecnologias necessárias para garantir a segurança desse novo perímetro baseado em software e do acesso remoto seguro via internet.
- **IoT:** Dispositivos não gerenciados de baixo custo estão se proliferando em redes para automação, monitoramento, reporte, medição e vigilância de uma ampla gama de recursos e situações empresariais, desde a manufatura até a agricultura. Muitos dispositivos de IoT normalmente utilizam cópias obsoletas de stacks TCP/IP de código aberto, os quais não possuem sequer capacidades rudimentares de segurança, além de não oferecerem metodologia para rastreamento ou instalação de patches para vulnerabilidades conhecidas.

Outras tendências mais específicas de ransomware também levaram a um aumento significativo em relação à sofisticação, severidade e eficácia financeira de tais ataques.

Ransomware-as-a-Service (RaaS): No passado, o número de alvos de ataques era naturalmente limitado, pois apenas uma pequena e especializada quantidadade de cibercriminosos possuíam a infraestrutura, habilidade técnica e metodologia para se infiltrarem em redes bem protegidas de grandes corporações.

No entanto, seguindo o mesmo racional de facilidade na implantação e pouco conhecimento técnico requerido que capitalizou os modelos de SaaS, IaaS e PaaS, o Ransomware-as-a-Service (RaaS) também migrou para a nuvem, onde kits de ransomware altamente customizáveis, adquiridos na dark web, podem ser implantados com facilidade. Isso diminuiu o nível de exigência requerido e permitiu a uma população muito maior de cibercriminosos lançar ataques sofisticados. O RaaS oferece diferentes tipos de programas de parcerias, dispondo de um portal web completo onde parceiros podem obter kits atualizados. REvil/Sodinokibi e Netwalker são exemplos do modelo RaaS.

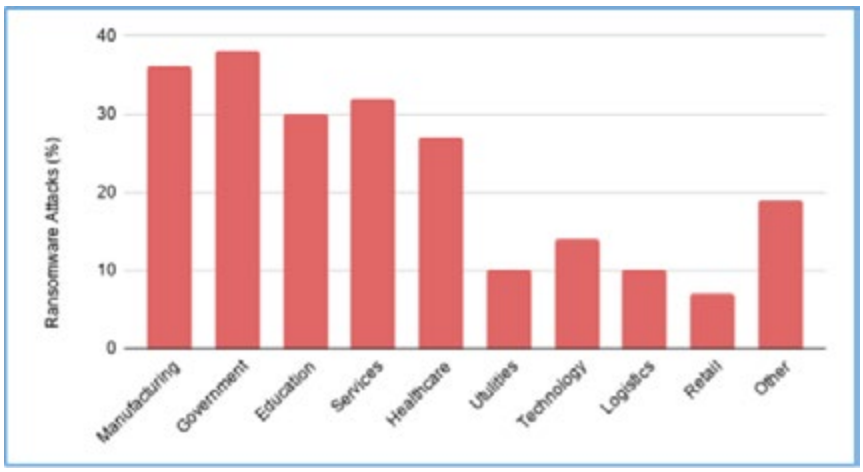
- **Spam and Phishing:** Esses são de longa data os mais bem sucedidos meios de entrada iniciais para malware, tendo a pandemia do COVID-19 acelerado estas tendências com novas oportunidades direcionadas a atacar o medo humano e a explorar as vulnerabilidades nas configurações de trabalho remoto. Os cibercriminosos se passam por organizações que fornecem informações e estatísticas sobre o COVID-19, programas de auxílio econômico-governamental, equipamentos de proteção pessoais e dados sobre vacinas.
- **Pagamentos em Bitcoin:** O aumento da popularidade e disponibilidade das criptomoedas tais como o bitcoin oferecem meios de pagamento para transações sem rastreabilidade e sem opções de contestação ou cancelamento.

Tendências emTentativas de Ataques Ransomwares

Os ransomware ocasionalmente ainda atingem consumidores, porém a grande maioria de tais ataques tem mudado de foco e vem sendo **direcionada a alvos corporativos e governamentais**. A infiltração inicial nos ativos é tão fácil quanto e as oportunidades de recebimento de resgates são enormes.

Em 2020, os cibercriminosos miraram especificamente organizações de grande porte e, frequentemente, aquelas com alta **exposição regulatória**. A possibilidade de serem impostas multas regulatórias e o dano de reputação resultante da violação legal às normas de proteção de dados aumentaram significativamente a taxa de sucesso no recebimento dos resgates, bem como dos próprios valores.

De acordo com relatório do SOCRadar Labs, as indústrias mais afetadas por ataques ransomware em 2020 foram manufatura, governo e serviços, pois são setores particularmente sensíveis a períodos de inatividade que são causados por tais ataques.



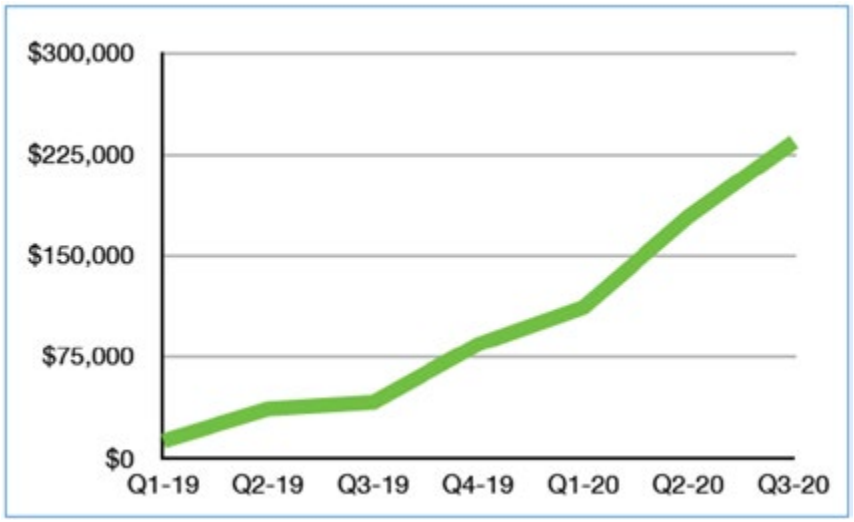
A **virulência dos ataques ransomware**, potencializada pelo RaaS, tem levado a um **crescimento vertiginoso da população de cibercriminosos** capazes de ameaçar um número cada vez maior de organizações.

Além de simplesmente reter os dados criptografados de uma organização em troca do resgate, um número cada vez maior de ataques tem **combinado criptografia com extorsão** no intuito de maximizar a probabilidade de pagamento. Nessa combinação de ataques, o cibercriminoso obtem acesso aos ativos da organização, extrai os seus dados e só então os criptografa. Se a organização se recusa a efetuar o pagamento do resgate em troca da chave de criptografia, o cibercriminoso expõe os dados extraídos, tornando-os públicos ou leiloando-os na dark web, causando danos imensuráveis ao status reputacional e financeiro da organização.

Essa tendência também leva os ataques ransomware a serem classificados como vazamento de dados. Isso força a gestão de segurança das organizações a reavaliarem a resposta a riscos e a incidentes, bem como a ajustarem as estratégias de recuperação de desastres e de continuidade dos negócios. Os grupos de ransomware continuam a se valer dessa tática de extração e extorsão, embora a expectativa de que os dados roubados sejam deletados está se esvaindo, já que o não cumprimento de tais promessas vem se tornando mais prevalente, apesar de o pagamento do resgate ter sido efetuado pela vítima.

Os cibercriminosos também têm tirado vantagem do fato de as **organizações encontrarem-se distraídas durante a pandemia da COVID-19**. Enquanto a reengenharia da rede e da computação vem sendo feita em regime de emergência para garantir a continuidade dos negócios, as vulnerabilidades de segurança expostas pela migração para a nuvem e para o trabalho remoto frequentemente permanecem sem resolução por um período de tempo. A proliferação de configurações de trabalho remoto utilizando RDP e outras tecnologias permite a cibercriminosos valerem-se de vetores de ataque antes inexistentes.

Nos últimos dois anos, a **média de valor dos resgates** aumentou significativamente de acordo com o Relatório Mensal sobre Ransomware elaborado pela BlackFog. O aumento é atribuído em parte ao fato de cibercriminosos estarem mirando cada vez mais grandes corporações.



Geograficamente, o Brasil foi um dos alvos mais afetados por ataques ransomware em 2020, seguido por outros países latino-americanos como **Colômbia, México, Equador e Peru**.

Tradicionalmente, cibercriminosos miraram sistemas Windows em razão de serem a maior **base de sistema operacional instalada**, porém à medida em que sistemas MacOS ganham mercado essas plataformas também têm se tornado alvo.

O último relatório de mercado da Coveware destaca as estatísticas do 3º Trimestre de 2020 com o top 10 dos tipos de ransomware.

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
1	Sodinokibi	16.2%	-
2	Maze	13.6%	-
3	Netwalker	9.9%	+1
4	Phobos	5.0%	-2
5	DopplePaymer	4.3%	New in Top 10
6	Snatch	4.0%	+2
6	Conti	4.0%	New in Top 10
8	Lockbit	3.6%	+1
9	Dharma	2.3%	-4
10	Nephilim	2.0%	New in Top 10
10	Avaddon	2.0%	New in Top 10

Tendências em Tradecraft de Ransomware

Em dezembro de 2020, no evento virtual da BlackHat Europe, apresentadores da Mandiant/FireEye discutiram as melhorias e mudanças no tradecraft de ransomware observadas em 2020.

- Mais discrição, menos barulho: Ataques ransomware são rápidos, porém ruidosos
- Melhoria de ferramentas: Menor dependência de ferramentas padrões de pentests, e maior utilização de malware customizados
- Maior rapidez na obtenção de credenciais de administradores de domínios
- Melhoria na metodologia de implantações de ransomware
- Maior efetividade na deleção de backups

Ações de Mitigação Recomendadas

Mesmo o ataque mais simples pode custar uma quantidade grande de tempo e dinheiro a uma organização. Ataques sofisticados, combinados com técnicas de extração-extorsão, podem paralisar ou destruir uma empresa. Dentre as recomendações gerais para minimizar os danos de um ataque ransomware estão:

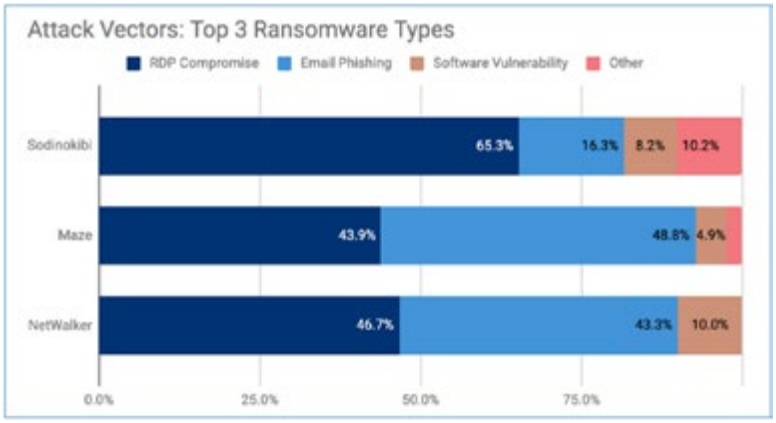
- Estabelecer e manter backups offline, bem como testá-los regularmente para assegurar que os sistemas podem ser restaurados com sucesso.
- Educar os colaboradores a respeito de técnicas de engenharia social e estratégias de phishing.
- Estabelecer uma estratégia de prevenção a roubo de dados—especialmente onde houver grande quantidade de dados armazenados ou transferidos em plataformas em nuvem.
- Instituir análise de comportamento do usuário para monitorar e identificar potenciais incidentes de segurança.
- Utilizar autenticação multifator (MFA) em todos os pontos de acesso remotos.
- Implantar pentests regulares ou contínuos para identificar pontos fracos, credenciais fracas e vulnerabilidades exploradas de forma frequente.
- Implantar tecnologia Secure Access Service Edge (SASE) para garantir a proteção do perímetro definido por software (SDP) ao redor de ativos em nuvem, no acesso direto à internet (DIA) pelos escritórios corporativos e no acesso dos usuários remotos.
- Ações específicas para mitigar vulnerabilidades de stack de protocolo TCP/IP (tanto para ativos corporativos em geral quanto para IoT): Desativar IPv6 quando/onde não for necessário; utilizar servidores DNS internos para dispositivos críticos; monitorar sua rede em busca de pacotes e comportamentos anômalos; segmentar sua rede para prevenir movimentação lateral de malware.
- Ser cauteloso em relação a serviços expostos publicamente, tais como Desktop Remoto (RDP, porta 3389), VPN, Virtual Network Computing (VNC), FTP e Server Message Block (porta 445).
- Não instalar software ou conceder-lhes privilégios de adminstrador a menos que sua organização saiba exatamente o que eles irão fazer.
- Garantir que todos os sistemas operacionais estejam com as atualizações em dia e instalar software antivírus em todos os lugares.

Técnicas e Fases Comumente Utilizadas

A maioria dos ataques ransomware utiliza um pequeno número de vetores comuns de infecção.

- **Phishing:** Anexos maliciosos de emails, também chamados de “malspam.”
- **Remote Desktop Protocol (RDP):** invasão de rede através de portas e serviços não protegidos.
- **Vulnerabilidades de Software e Rede:** Worms e outros formas de ransomware que exploram vulnerabilidades de rede.
- **Dual Malware:** Malware adicional introduzido via infecções de malware anteriores (por exemplo, uma infecção por TrickBot que leva a uma infecção subsequente por Ryuk).

O relatório de mercado da Coveware do 3º Trimestre de 2020 fornece detalhes sobre os vetores de infecção dos diferentes tipos de ransomware.



As táticas e técnicas mais comuns utilizadas por autores e operadores de ransomware são classificadas em diversas categorias.

- **Oportunísticas:** O modelo operacional oportunístico se vale de ransomware que se autopropagam, tais como o WannaCry. Os cibercriminosos ativam o malware—normalmente utilizando pontos de entrada de fácil acesso, tais como kits de exploits, backdoors, portas abertas, VPNs não seguras, sistemas operacionais e aplicações desatualizadas—e, após isso, a propagação do ransomware fica atrelada às ações do usuário, de modo que o cibercriminoso não sabe ao certo para onde o ransomware irá, para onde irá se mover, qual organização alvo se tornará uma vítima ou quais domínios e redes ele poderá acessar.

  Por vezes denominado spray-and-pray, esses ataques ocorrem em larga escala e são menos sofisticados, sendo hoje um método de operação em declínio.

- **Direcionadas:** Trata-se de uma técnica estratégica de menor volume e com mais sofisticação, resultando no pagamento de resgates de maior monta em geral. Os cibercriminosos lançam campanhas específicas para atingir uma determinada organização. Eles obtêm acesso à rede atráves de emails phishing, engenharia social, vulnerabilidades em sistemas operacionais e portas abertas, e então vasculham a rede antes de lançar as suas demandas por resgate. Há dois modelos de operações nesta técnica direcionada:
  - **Modelo de Parcerial:** Cibercriminosos profissionais criam o ransomware e então fornecem aos seus parceiros (por subscrição ou por um percentual do resgate) uma plataforma pela qual eles podem acessar as ferramentas e as instruções para executar os ataques. Este modelo não exige muito para que sejam lançados ataques altamente sofisticados.
  - **Modelo Autogerenciado:** Neste modelo de operação, o cibercriminoso profissional executa ele mesmo a fase inicial de comprometimento, ganha acesso ao sistema e ao ambiente, e então os vasculha antes de efetuar as demandas por resgate.

Proteja os Seus Ativos Contra Ransomware Utilizando o RidgeBot 3.2

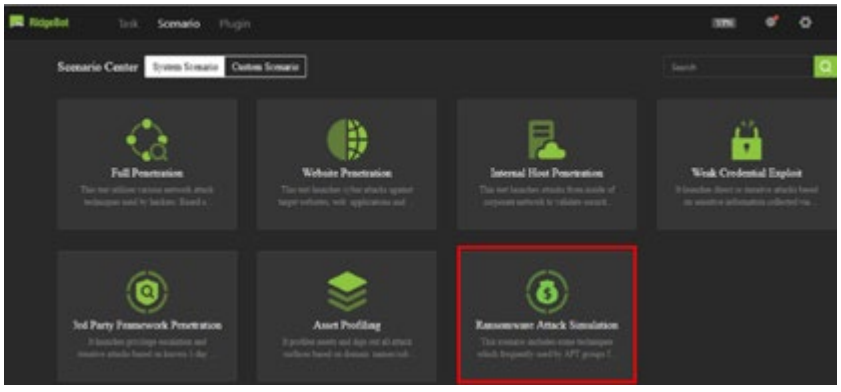
O RidgeBot descobre automaticamente os seus ativos, escanea-os e então procede à exploração das vulnerabilidades encontradas, da mesma forma que um hacker o faria. No seu relatório, o RidgeBot o alerta sobre os perigos encontrados nas vulnerabilidades exploradas, e também demonstra a exata rota de ataque que o permitiu comprometer o ativo. Com este conjunto de informações precisas e detalhadas, sua organização pode proativa e rapidamente corrigir todas as vulnerabilidades identificadas na sua rede e nos seus ativos.

RidgeBot 3.2—Proteção Contra Ransomware

A versão 3.2 disponibiliza um novo modelo focado especificamente no combate a ataques ransomware. Inicialmente, esse modelo inclui:

- Escaneamento das 27 principais vulnerabilidades em pontos de entrada para ransomware
- Habilidade de lançar ataques para explorar essas vulnerabilidades
- Relatório detalhado com os níveis precisos de sucesso atingidos pela exploração das vulnerabilidades

Definições de mais ataques ransomware serão adicionadas no decorrer to tempo e sua organização poderá adicioná-las ao seu arsenal de segurança por meio de downloads periódicos das atualizações do RidgeBot.



Ao utilizar os modelos de ransomware disponíveis no RidgeBot 3.2., sua organização executa fácil e rapidamente o escaneamento das vulnerabilidades que podem estar presentes nos seus ativos. Como parte integral da solução, o RidgeBot também executa ataques para comprovar que as vulnerabilidades encontradas são efetivamente exploráveis no ambiente atual da sua organização. Sua organização pode executar esses ataques e testes de intrusão sob demanda ou regularmente.

Assim como no caso de outras ferramentas e testes de vulnerabilidades, é recomendado que a sua organização reexecute o scan-and-exploit do RidgeBot quando houver qualquer alteração nos seus ativos, tais como adição de um novo servidor ou dispositivo de rede, atualização de software de um dispositivo, instalação de um patch em um dispositivo, mudança de scripts ou informações em um servidor web, ou qualquer outra alteração de software ou hardware que possa resultar no aparecimento de uma nova vulnerabilidade na sua rede. Sua organização deve estar particularmente atenta a dispositivos de IoT que possam estar conectados ou serem inseridos na sua rede.

A Abordagem do RidgeBot 3.2

Os modelos de ransomware disponíveis no RidgeBot 3.2 incluem o escaneamento e a exploração das seguintes classes de vulnerabilidades:

- Execução remota de código/comando (RCE)
- Stuffing de senhas e credenciais fracas (por exemplo, SSH, Redis e Servidor SQL)
- Server Message Block (SMB)
- WebLogic e outros uploads de arquivos

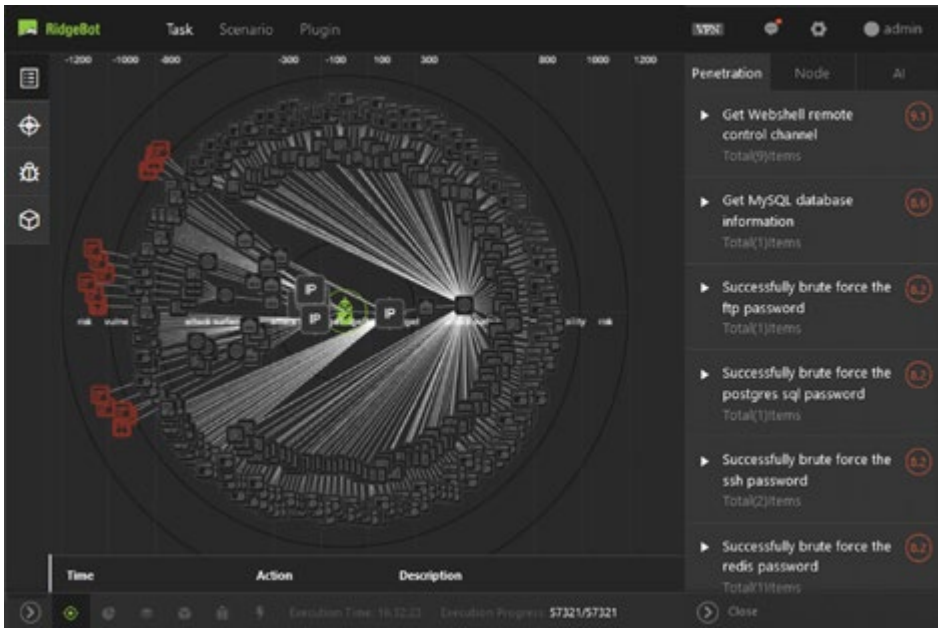
Escopo do RidgeBot 3.2

O robô de escaneamento e exploração RidgeBot cobre vulnerabilidades técnicas como credenciais fracas, portas abertas, uploads de arquivos, e vulnerabilidades de aplicações web WebLogic e Struts2. Ele não pode proteger sua organização contra engenharia social ou phishing, nem contra dados que já tenham sido criptografados por um ataque ransomware. Em vez disso, o RidgeBot identifica as vulnerabilidades na sua rede para impedir a intrusão de ransomware.

Se sua organização é um possível ou provável alvo de cibercriminosos, utilize as habilidades de escaneamento e exploração do RidgeBot 3.2 para protegê-la contra a fase inicial de comprometimento de um ataque orquestrado. Uma vez que o cibercriminoso tenha invadido a sua rede e estabelecido a sua presença, sua organização necessitará de ferramentas adicionais para detectar e remediar a intrusão.

Combatendo os PrincipaisAtaques Ransomware com o RidgeBot

O RidgeBot desenha uma estrutura de rede a partir dos ativos descobertos e disponibiliza uma lista de alvos (as caixas vermelhas do gráfico) e de exploits e vulnerabilidades (listadas ao lado direito da tela) que foram invadidas com sucesso. São demonstradas as precisas rotas do ataque que o RidgeBot seguiu para comprometer aquele alvo. Isto garante à sua organização informações claras e precisas sobre quais dispositivos no seu ambiente demandam quais tipos de ajustes ou atualizações para estarem devidamente protegidos contra ataques ransomware.



A seção abaixo fornece detalhes e exemplos das principais e mais facilmente exploráveis vulnerabilidades que podem existir no seu ambiente. O RidgeBot 3.2 pode proteger sua organização contra tais vulnerabilidades e outras mais.

A agência governamental estadounidense National Institute of Standards and Technology (NIST) mantém uma base de dados pesquisável, a National Vulnerability Database (NVD), na qual detalhes adicionais sobre quaisquer vulnerabilidades que tenham números de CVE alocados podem ser pesquisados.

Execução Remota de Código/Comando: EternalBlue

Os ataques massivos de ransomware ao redor do mundo em 2017 foram manchetes dos principais jornais, tendo paralisado empresas multinacionais por dias e custado a elas milhões de doláres em danos, reparação e recuperação. O ransomware WannaCry que se propagou em 2017 utilizava a vulnerabilidade EternalBlue para explorar computadores Windows não atualizados. Em junho de 2017, seguiu-se o ataque ransomware NotPetya, explorando a mesma vulnerabilidade.

Em março de 2017, a Microsoft disponibilizou o boletim de segurança MS17-010, detalhando a falha a segurança EternalBlue e anunciando os patches Windows para todas as versões suportadas ativas naquele momento, incluindo Windows Vista, Windows 7, 8.1, and 10, Windows Server 2008, 2012 e 2016. A EternalBlue também foi coberta pelas CVE-2017-0143 a CVE-2017-0148.

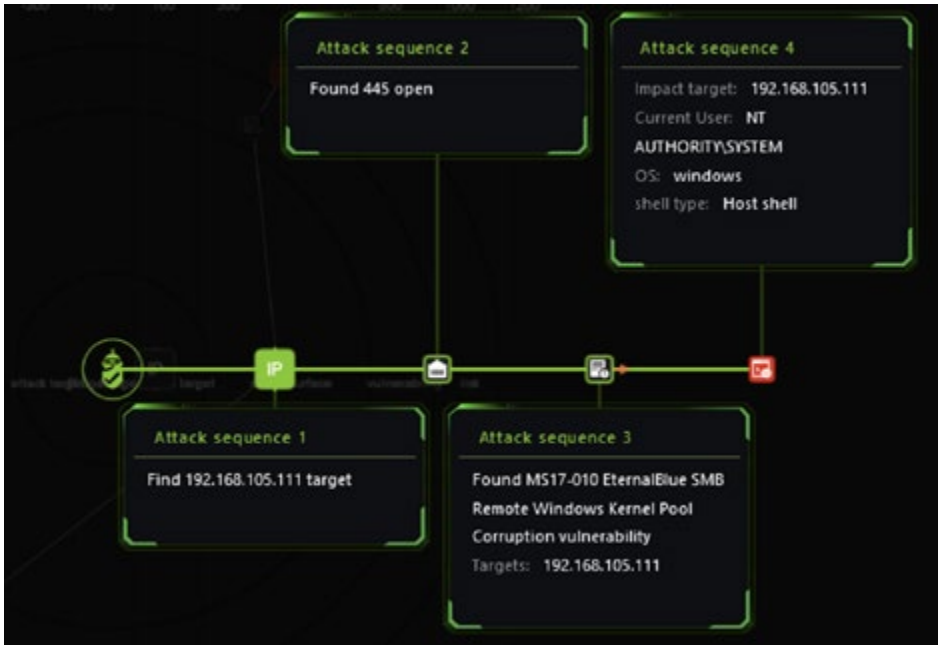
A EternalBlue é uma exploit que permite a cibercriminosos obter acesso a um ativo Windows, controlar o shell e executar remotamente códigos arbitrários ao enviar pacotes especialmente criados para um servidor utilizando Microsoft Server Message Block 1.0 (SMBv1). O SMB é um protocolo de compartilhamento de arquivos em rede que permite o acesso a arquivos em um servidor remoto.

Essa vulnerabilidade permite que cibercriminosos injetem malware que se autopropaga infectando uma rede inteira e todos os dispositivos a ela conectados, plantando o payload do criptoransomware em todos os lugares para o qual se espalha. A habilidade de se autopropagar tornou a EternalBlue uma exploit popular para vários outros malware, tais como Trickbot (um banking trojan modular), e também CoinMiner e WannaMine em que criptomineradores exploraram a EternalBlue para obter acesso a recursos computacionais e minar criptomoedas.

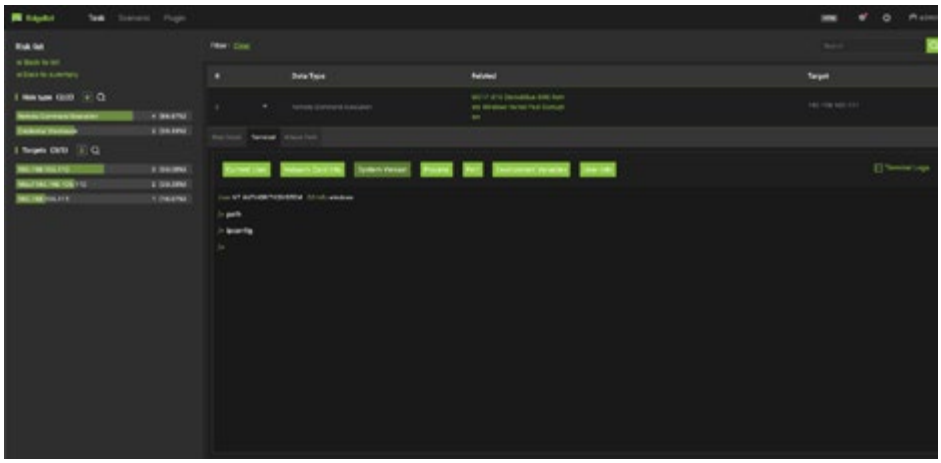
Apesar de a vulnerabilidade EternaBlue—e dos patches Windows para remediá-la—já terem sido anunciadas anos atrás, em março de 2017, ainda há, em 2021, muitas máquinas não atualizadas que tornam essa vulnerabilidade muito atrativa para cibercriminosos.

O RidgeBot 3.2 pode escanear sua rede, seus dispositivos e servidores para detectar quaisquer potenciais vulnerabilidades EternalBlue não atualizadas no seu ambiente. Em seguida, o RidgeBot pode lançar um ataque contra os dispositivos alvo, explorando a vulnerabilidade EternalBlue encontrada. No exemplo de ataque do Ridgebot mostrado abaixo contra o IP 192.168.105.111, a vulnerabilidade EternalBlue foi explorada com sucesso (caixa vermelha na borda externa).

Detalhando a rota do exploit (caixas verdes) até a máquina alvo (caixa vermelha), é destacado o caminho de ataque utilizado para atingir o alvo.



Para exploits EternalBlue, o RidgeBot pode controlar o host shell do dispositivo comprometido. Um exploit bem sucedido de uma vulnerabilidade EternalBlue pelo RidgeBot é destacada no Risk Table, demonstrando que o host alvo foi invadido e que o RidgeBot conseguiu enviar comandos a partir do shell.



Execução de Código/Comando Remotos: Struts2

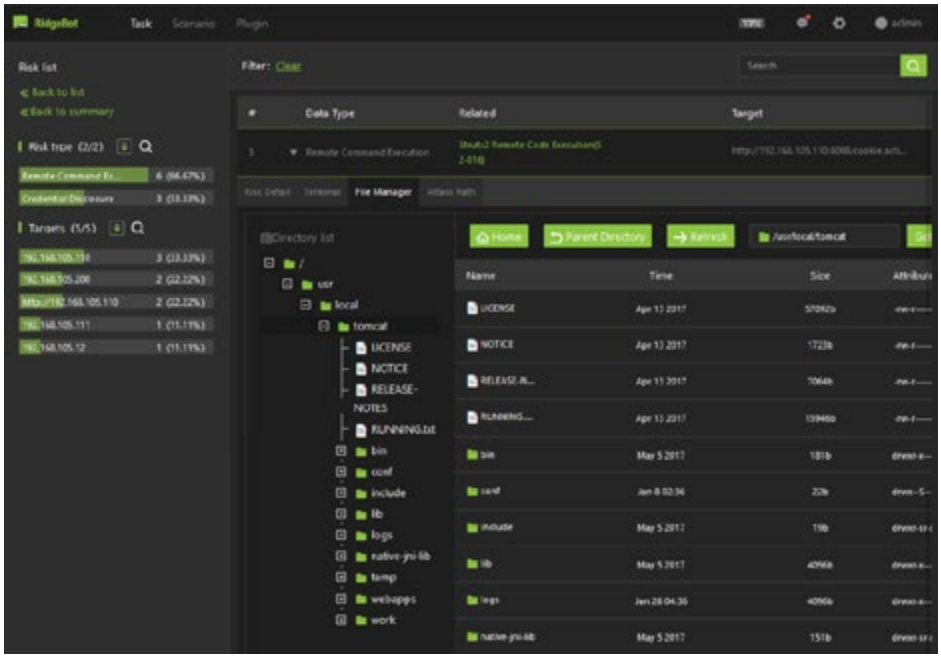
O Apache Struts2 é um open-source web application (Model-View-Controller ou MVC) framework gratuito para desenvolvimento de aplicações web Java, cross-platform. Ele possui uma arquitetura extensível utilizando Java Servlet API e plugins REST, AJAX e JSON para permitir fácil desenvolvimento de software.

Um série de vulnerabilidades para execução remota de códigos estão presentes no código do Struts2 e de seus plugins, incluindo os boletins de segurança Apache S2-008 (CVE-2012-0391), S2-016, S2-019 (CVE-2013-4316), S2-032, S2-037, S2-045, S2-048, S2-052, S2-057 e S2-059.

O RidgeBot 3.2 pode escanear sua rede, seus dispositivos e servidores para detectar quaisquer das vulnerabilidades do Struts2 destacadas acima no seu ambiente. Em seguida, o RidgeBot pode lançar um ataque contra o dispositivo alvo, explorando a vulnerabilidade do Struts2 encontrada. No exemplo de ataque do RidgeBot abaixo contra o IP 192.168.105.110, a vulnerabilidade Struts2 foi explorada com sucesso (caixa vermelha na borda externa).

Detalhando a rota do exploit (caixas verdes) até a máquina alvo (caixa vermelha), é destacado o caminho de ataque utilizado para atingir o alvo.

Para exploits Struts2, o RidgeBot consegue coletar o diretório de arquivos do host alvo. Um exploit bem sucedido de uma vulnerabilidade Struts2 pelo RidgeBot é destacada no Risk Table, demonstrando que o host alvo foi invadido e que o RidgeBot conseguiu visualizar o seu diretório de arquivos.



Ataques de Senhas Fracas e Credenciais Divulgadas

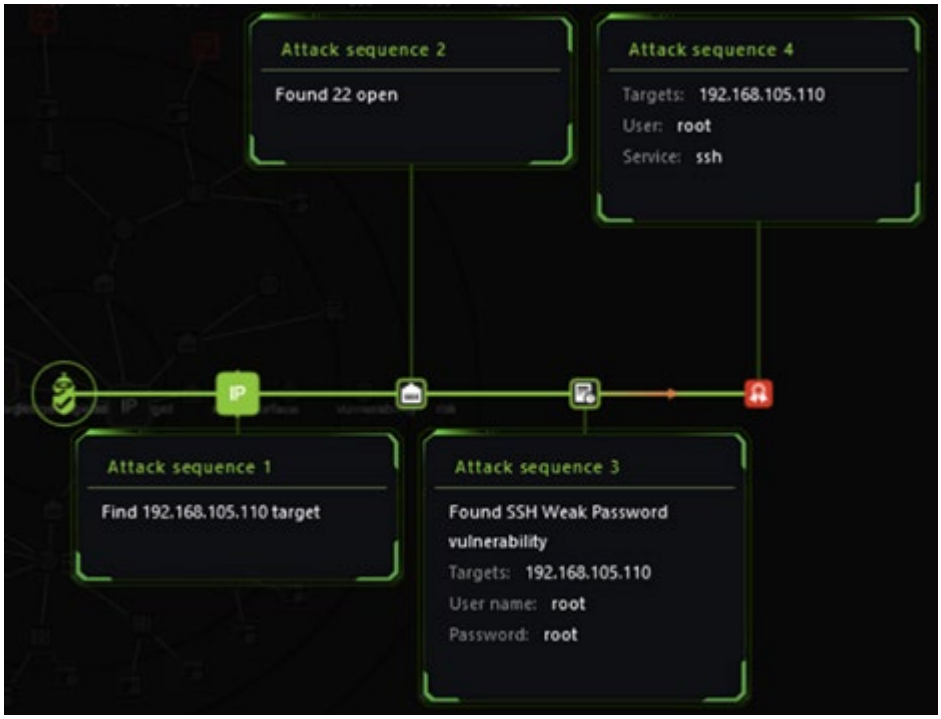
Existem inúmeras vulnerabilidades conhecidas na indústria que estão relacionadas a senhas fracas e divulgação de credenciais, incluindo as associadas a SSH, Redis, SQL Server, SMB e Microsoft Remote Desktop Server. Alguns dos exploits estão relacionados a divulgação de credenciais, outros a RCE abrindo “wormable opportunities” pelas quais o malware consegue se propagar de um computador vulnerável a outro, de maneira similar a como o ransomware WannaCry se propaga.

O RidgeBot 3.2 consegue escanear sua rede, dispositivos e servidores para detectar uma seção transversal de vulnerabilidades de senhas fracas no seu ambiente. Em seguida, o RidgeBot pode lançar um ataque contra o dispositivo alvo, explorando a vulnerabilidade de senha fraca encontrada. No exemplo de ataque do RidgeBot abaixo contra o IP 192.168.105.110, a vulnerabilidade de senha fraca do Redis foi explorada com sucesso (caixa vermelha na borda externa).

Detalhando a rota do exploit (caixas verdes) até a máquina alvo (caixa vermelha), é destacado o caminho de ataque utilizado para atingir o alvo.

No exemplo de ataque do RidgeBot abaixo contra o IP 192.168.105.110, a vulnerabilidade de senha fraca de SSH foi explorada com sucesso (caixa vermelha na borda externa).

Detalhando a rota do exploit (caixas verdes) até a máquina alvo (caixa vermelha), é destacado o caminho de ataque utilizado para atingir o alvo.



Ataques de Weblogic e deOutrosUploads de Arquivos

Vulnerabilidades em uploads de arquivos, como o próprio nome já diz, valem-se de arquivos para inserir códigos maliciosos de ativação de RCE na plataforma alvo.

- **Vulnerabilidade em upload local de arquivo:** Uma aplicação permite a um cibercriminoso fazer o upload de um arquivo malicioso diretamente, o qual é executado em seguida.
- **Vulnerabilidade em upload remoto de arquivo:** Uma aplicação se aproveita de uma ação do usuário para buscar um arquivo em um site remoto na internet e o armazenar localmente para ser executado em momento posterior.

O RidgeBot 3.2 consegue escanear sua rede, dispositivos e servidores para detectar as seguintes vulnerabilidades no upload de arquivos do seu ambiente.

- Apache Tomcat PUT Method Write File (CVE-2017-12615)
- WebLogic Service Test Configuration Page Has Arbitrary File Upload (CVE-2018-2894)
- WebLogic XML Decoder Deserialization (CVE-2017-10271)
- Apache ActiveMQ Arbitrary File Writing (CVE-2016-3088)

Implantando o RidgeBot 3.2 Ridge Security Demo

Uma vez que um cibercriminoso tenha conseguido invadir sua rede e tenha avançado para se estabelecer nos seus ativos, normalmente já é tarde para impedir o dano. Dessa forma, é indispensável tomar medidas preventivas para impedir que os cibercriminosos consigam encontrar quaisquer aberturas para ingressar na sua rede e nos seus ativos.

O RidgeBot 3.2 dispõe de habilidades críticas de escaneamento e exploração, desenvolvidas especificamente para combater vulnerabilidades relacionadas a ataques ransomware. Entre em contato conosco hoje para uma demonstração de como o RidgeBot pode auxiliar sua organização a sobreviver nesses tempos perigosos.

Company Profile

Ridge Security dispõe de soluções de pentesting éticas, eficientes e acessíveis para grandes, médias e pequenas empresas. Nós garantimos que nossos clientes estejam sempre em conformidade, alertas e protegidos a todo o momento no mundo cibernético. Nosso time executivo possui muitos anos de extensa experiência em redes e segurança. A Ridge Security está localizada no coração do Vale do Silício e vem se expandindo para outras áreas como América Latina, Ásia e Europa.

RidgeBot, um sistema robótico de pentests, automatiza completamente o processo de testagem ao combinar técnicas de hacking ético a algoritmos de tomada de decisão. O RidgeBot encontra, explora e documenta riscos de negócio e vulnerabilidades descobertos durante o processo de testagem, destacando o potencial impacto e dano.

Ridge Security Technology Inc.
www.ridgesecurity.ai