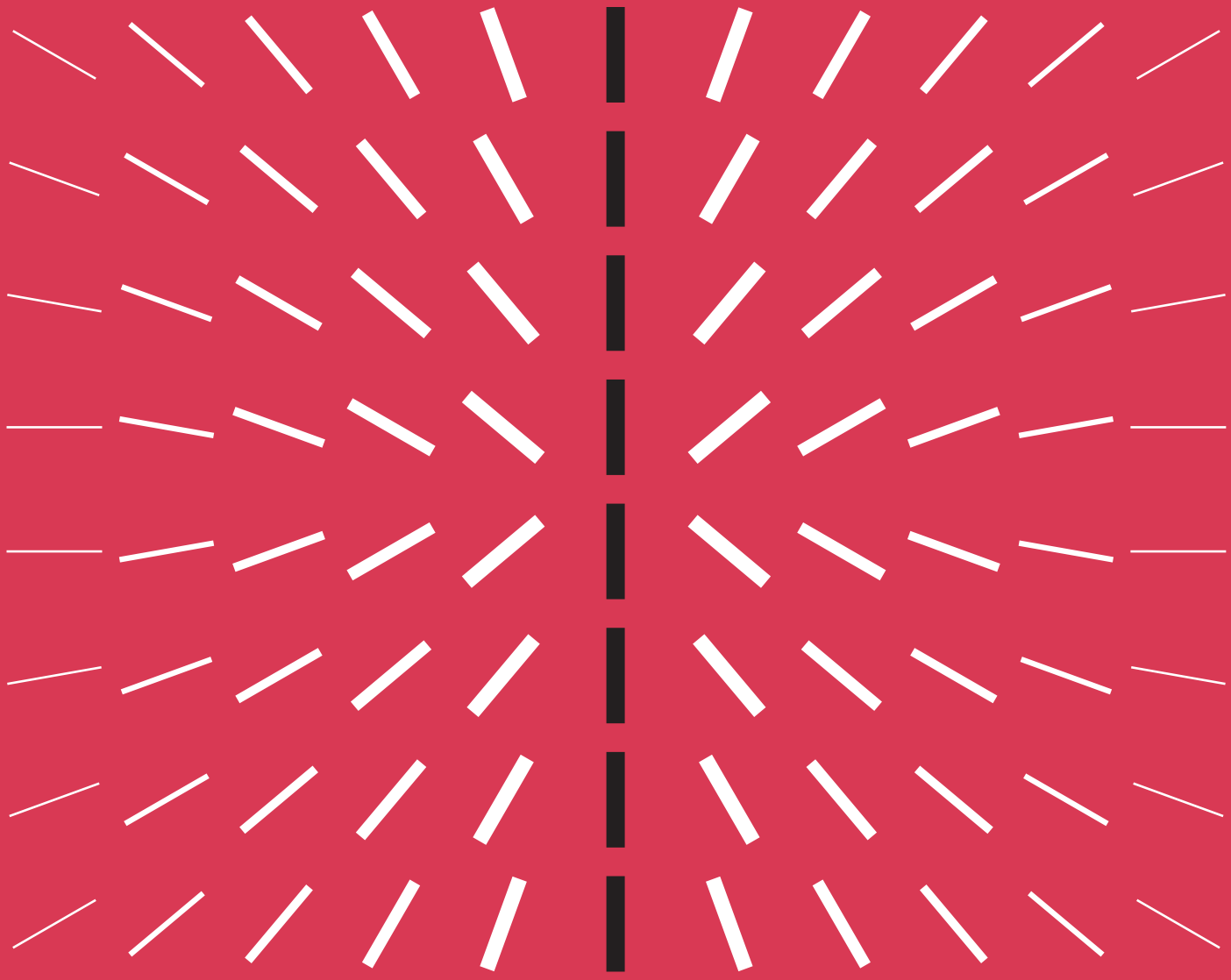
Como responder à ameaça crescente de ataques de *ransomware*

PwC *Cybersecurity*

Outubro de 2021



pwc

Conteúdo

Ataques de *ransomware*

Ataques de *ransomware* são hoje uma ameaça cibernética de alta prioridade enfrentada pela maioria das organizações.

Neste tipo de ataque, os cibercriminosos obtêm acesso às redes corporativas internas e implantam *ransomware* de maneira estratégica e deliberada. Eles criptografam dados e exigem resgates das organizações em valores substanciais como forma de recuperar o acesso e restaurar sistemas críticos ao seu negócio. Os invasores também roubam e ameaçam vazar dados confidenciais para adquirir uma vantagem adicional ao extorquir suas vítimas.

Esses ataques representam uma ameaça mais desafiadora do que variantes de *ransomware* conhecidas, como NotPetya e WannaCry.

Por trás desses crimes, estão pessoas qualificadas, flexíveis e motivadas financeiramente, que podem identificar e vencer defesas, além de desenvolver suas táticas para maximizar as chances de conseguir que as organizações paguem os resgates pedidos. Isso é diferente de ataques anteriores de grande visibilidade, que se baseavam em uma funcionalidade semelhante a um *worm* para disseminar *ransomware*.

Como os invasores começaram a roubar e vazar dados confidenciais, a maioria dos esforços de melhoria deve se concentrar na prevenção.

Enfatizar apenas estratégias de *backup* e recuperação não é mais uma opção viável, pois elas não evitam que o invasor roube dados, nem ajudam no enfrentamento das questões regulatórias resultantes. Mesmo quando essas estratégias estão em uso, uma recuperação de *backups* nas grandes organizações pode levar semanas e, em alguns casos, ser praticamente inviável.

As organizações que ainda não tomaram medidas para entender os riscos cibernéticos e reduzir sua vulnerabilidade devem agir agora.

As melhorias necessárias para reduzir o risco de ataques não são nada surpreendentes para as equipes de segurança cibernética e devem estar na agenda da alta administração. Provavelmente essas questões já fazem parte dos planos de melhoria existentes nas organizações. No entanto, a escalada de ameaças deve fazer as organizações voltarem a priorizar atividades em andamento ou planejadas e considerar as ações a serem tomadas para gerir e reduzir riscos.

Como funcionam os ataques de *ransomware*?

Os autores de ataques de *ransomware* geralmente trabalham com grupos criminosos que usam técnicas automatizadas e de amplo alcance para acessar as redes corporativas, por exemplo, distribuindo e-mails de *phishing* com códigos ou instruções maliciosas (*malware*). Em muitos casos investigados pela área de resposta a incidentes da PwC, essas técnicas, às vezes conhecidas, são eficazes para comprometer as organizações, ainda envolvidas na solução de problemas de negócios, como a restrição de macros do Microsoft Office.

Depois de ter acesso inicial à organização alvejada, os invasores comprometem contas privilegiadas e outros sistemas, usando uma combinação de ferramentas comuns à administração de sistemas e de teste de segurança (por exemplo, Cobalt Strike, PowerShell Empire e BloodHound). Elas são suficientes para dar acesso privilegiado a redes corporativas devido a problemas generalizados de TI, tais quais a ausência de atualizações de segurança (patches), configurações não alinhadas às melhores práticas de segurança e fragilidades do Active Directory e a recursos que falham em detectar as técnicas usadas nesses ataques.

Quando ganham acesso privilegiado à rede do alvo, os invasores extraem dados confidenciais e implantam *ransomware* da forma mais ampla possível, na maioria dos casos provocando um distúrbio grande e prolongado nas operações do negócio.

O número de agentes de *ransomware* cresceu constantemente em 2020, incentivado pelos lucros nos ataques de grande visibilidade.

Jornada de um ataque de *ransomware*

O que está impulsionando o crescimento dos ataques de *ransomware*?

O rápido crescimento de ataques de *ransomware* foi impulsionado por vários fatores, como:

Número crescente de invasores, atraídos pela promessa de receita fácil.

O número de agentes de *ransomware* cresceu nos últimos anos, incentivado pelos lucros derivados de ataques de grande visibilidade. Por exemplo, o programa de afiliados do NetWalker – uma variante de *ransomware* lançada em março de 2020 – supostamente acumulou US$ 4,5 milhões nas primeiras seis semanas de existência. Após quatro meses de operação, essa receita teria aumentado para US$ 25 milhões.

Popularidade dos programas de afiliados, que reduzem a barreira de entrada para os recém-chegados.

12 esquemas bem conhecidos são executados como programas de afiliados nos quais os desenvolvedores de *ransomware* alugam acesso a seu *malware* em troca de uma participação nos lucros. Essa tendência reduz significativamente a barreira de entrada, pois o desenvolvimento de *malware* não é mais um requisito. Isso permite que eles se especializem na disseminação pelos ambientes de TI das organizações e na implantação de *ransomware* em grande escala.

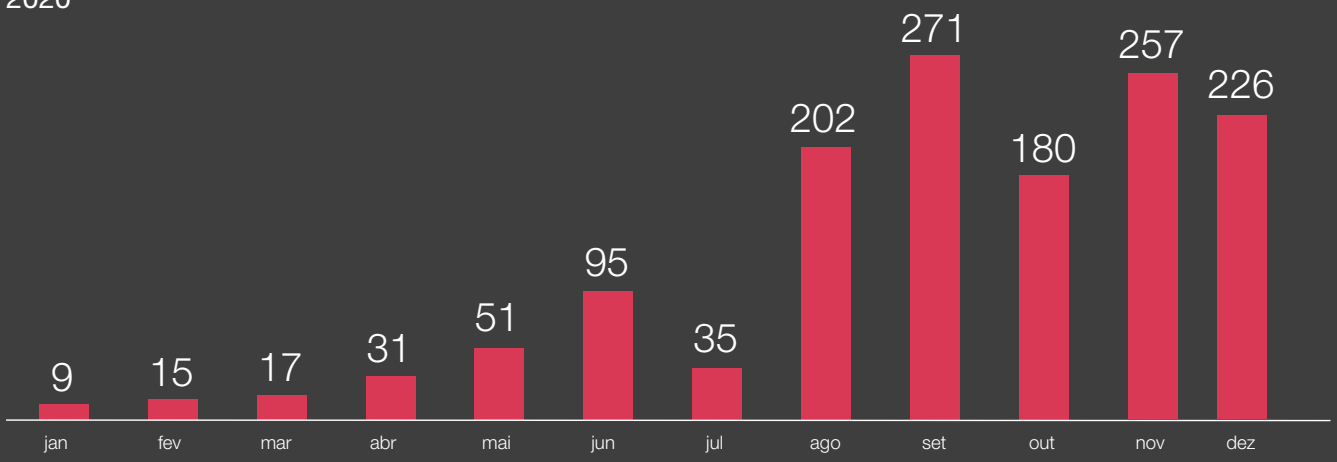
Surgimento de sites de vazamentos, exercendo pressão adicional sobre as vítimas para que paguem os pedidos de resgate.

O uso crescente de sites de vazamentos, onde os dados das vítimas são divulgados se o resgate não for pago, aumenta ainda mais a pressão sobre as organizações para atender aos pedidos e eleva, por sua vez, a lucratividade desses ataques. Depois que o grupo Maze hospedou um site de vazamentos em janeiro de 2020, outros 18 criminosos seguiram o exemplo. Em sete meses, mais de 750 organizações tiveram dados expostos.

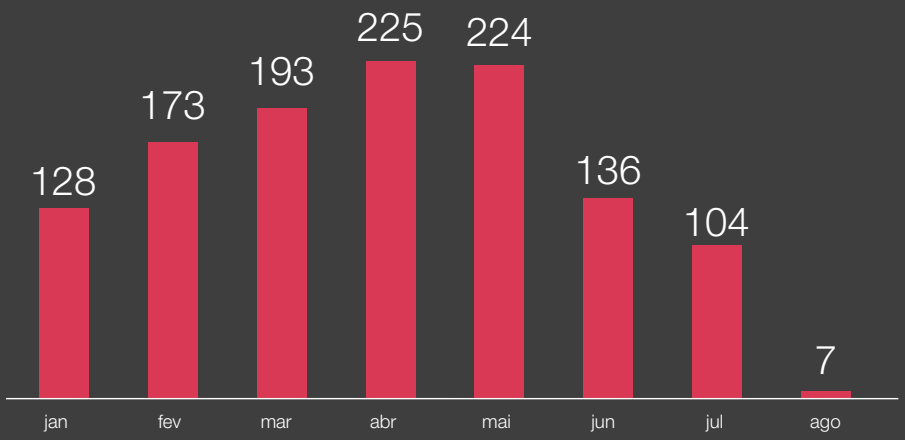
Chegada de novos invasores, alguns extremamente agressivos.

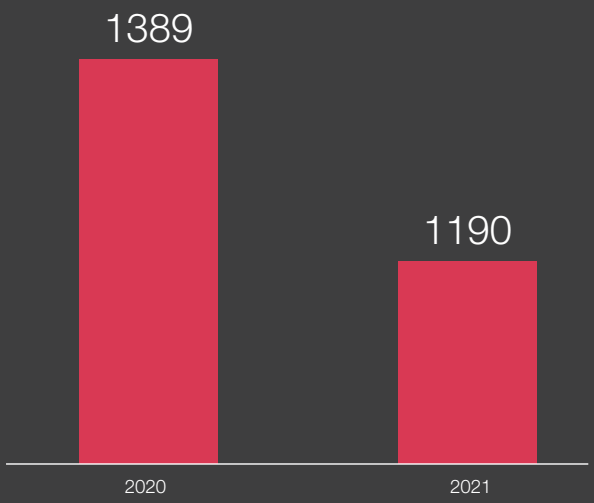
Apesar de sua chegada recente ao cenário do *ransomware*, operações como o Suncrypt divulgaram dados com mais frequência e em maior número do que alguns de seus rivais mais tradicionais. O Conti, que avaliamos ser o substituto do notório *ransomware* Ryuk, lançou seu site de vazamentos em agosto de 2020 e divulgou dados sobre mais de 100 vítimas nas primeiras oito semanas de atividade.

Total de vazamentos de dados de *ransomware*
2020



2021 - de janeiro a agosto





Fonte: Darktracer.

Por que as organizações são vulneráveis?

Nossa experiência em ajudar organizações a responder a ataques de *ransomware* mostrou que os invasores exploram várias falhas comuns de TI e segurança. Descrevemos a seguir os temas que mais observamos em nosso trabalho de resposta a esses incidentes e no apoio aos clientes para promover melhorias de segurança direcionadas.

O sistema legado de TI cria vulnerabilidades de segurança que os invasores podem explorar.

A maioria das organizações tem e depende de algum tipo de sistema legado de TI, o que gera impactos de segurança importantes. O risco de sistemas operacionais sem suporte aumenta com o tempo, uma vez que vulnerabilidades são identificadas e permanecem sem correção. Além disso, sistemas operacionais legados são quase sempre incompatíveis com as ferramentas de segurança modernas e não dispõem de recursos de segurança necessários para se proteger de ataques de *ransomware*. Em muitos casos, os sistemas legados hospedam alguns dos aplicativos mais essenciais de uma organização, que geralmente são os mais visados.

A tecnologia não está configurada de forma segura para evitar técnicas comuns de ataque cibernético.

Na maioria dos casos, o acesso inicial dos ataques resulta do comprometimento de estações de trabalho com o uso de e-mails ou servidores de *phishing* que exploram vulnerabilidades não corrigidas em serviços expostos à Internet. Os invasores se aproveitam da configuração inadequada desses sistemas, que têm controles de segurança ineficazes. Esses problemas geralmente permanecem sem solução devido à falta de consciência sobre as boas práticas de segurança, à falta de priorização por parte das equipes de TI nas correções de segurança e ao impacto percebido ou desconhecido dessas correções para os negócios.

A proteção insuficiente de contas privilegiadas permite que invasores comprometam as credenciais.

Vimos operadores de *ransomware* qualificados obterem funções de administrador de domínio em 72 horas, pois as organizações não tinham protegido adequadamente as contas com privilégios. Os problemas mais comuns são um grande número de contas com privilégios excessivos, práticas operacionais arriscadas por parte de administradores de domínio e o uso de senhas e mecanismos de autenticação inseguros. A causa disso geralmente é o fato de o Active Directory (e outros sistemas de gerenciamento de identidade e acesso) ser visto como uma ferramenta de TI – e não como ferramenta de segurança essencial para impedir ataques.

Recursos de detecção e resposta ineficazes dão aos invasores liberdade para operar.

Os invasores geralmente permanecem nas redes corporativas por dias ou semanas, adquirindo privilégios e expandindo sua presença antes de implantar um *ransomware* destrutivo. Há muitas oportunidades de detecção e resposta que não são detectadas pelas organizações. Na maioria das vezes, isso ocorre porque as ferramentas de segurança tradicionais baseadas em assinaturas são ineficazes para detectar as técnicas usadas nos ataques. Além disso, os alertas se perdem, uma vez que as equipes de operações de segurança estão sobrecarregadas resolvendo falsos positivos, e os processos de contenção não são eficientes. O uso de *trojans* comuns – tipo Emotet, Dridex ou Qakbot – como um vetor de infecção inicial geralmente é muito eficaz, já que a detecção e remediação dessas infecções de "*malware* comum" não são priorizadas pelas equipes de segurança.

As organizações mantiveram uma infraestrutura local e tiveram dificuldade para adotar a nuvem SaaS.

Aplicativos comerciais de "software como serviço" em nuvem (por exemplo, e-mail, armazenamento de arquivos e CRM) podem reduzir significativamente o impacto de um ataque de *ransomware*, mas muitas organizações continuam a confiar e investir em infraestrutura e aplicativos locais. Esse tipo de ambiente raramente é projetado com padrões de segurança (ou mesmo para evitar ameaças modernas). Isso significa que os invasores podem usar ferramentas de segurança ofensivas amplamente disponíveis para explorar as fragilidades. Não há soluções rápidas, pois a atualização eficaz dos controles modernos de segurança cibernética na infraestrutura de TI pode ser custosa e complexa, exigindo que a TI se modernize antes que possa ser protegida.

Que perguntas você deve fazer para avaliar sua vulnerabilidade?

As equipes de administração devem questionar suas equipes de segurança para saber o quanto são suscetíveis a ataques de *ransomware*, fazendo perguntas do tipo:

Como estamos usando controles técnicos de segurança para limitar o risco de uma estação de trabalho ser comprometida por ataques de *phishing*?

Como estamos usando práticas de administração seguras e restringindo o uso de contas de administrador de domínio para limitar o risco de ataques de roubo de credenciais?

Como ainda poderemos acessar nosso e-mail e mensagens se um ataque de *ransomware* impactar nossa infraestrutura de TI local?

Com que rapidez e abrangência estamos detectando e corrigindo infecções de "*malware* comum" nas estações de trabalho?

Até que ponto confiamos que é possível detectar o comprometimento de contas privilegiadas por um invasor?

Como restringimos a conectividade e as relações de confiança do Active Directory entre diferentes áreas da empresa para desacelerar e limitar a propagação de ataques de *ransomware*?

Acreditamos que é possível detectar o uso de ferramentas comuns de invasores em nossa rede, como Cobalt Strike ou BloodHound?

Como estamos mitigando o risco de sistemas legados de TI para garantir que não constituam uma vulnerabilidade e permitam que um invasor comprometa todo o nosso ambiente?

O que fizemos para validar se todos os controles de segurança de rede ainda são eficazes com cada vez mais profissionais trabalhando remotamente?

Como as organizações devem responder?

Dada a crescente ameaça cibernética representada por ataques de *ransomware*, recomendamos que as equipes de segurança cibernética adotem uma abordagem em três etapas para reduzir de forma imediata e duradoura a vulnerabilidade de sua organização:

1 Entender e comunicar as vulnerabilidades da organização

Use testes de segurança para avaliar se as técnicas utilizadas em ataques de *ransomware* podem ser evitadas e detectadas por defesas em vigor. Eles ajudam a identificar também as vulnerabilidades e fraquezas que podem ser exploradas por agentes de *ransomware*. As equipes de segurança devem fornecer informes contínuos sobre riscos à administração, usando os resultados dessa abordagem de teste com foco em ameaças.

2 Promover melhorias direcionadas para reduzir imediatamente o risco e validar sua implementação

Melhorias direcionadas servem para prevenir e detectar as técnicas usadas em ataques e abordam as vulnerabilidades e fraquezas identificadas. Vimos clientes conseguirem alcançar esse objetivo reunindo equipes de TI e segurança para colaborar no desenvolvimento de correções apropriadas para o ambiente. Os testes de segurança devem ser usados para validar se as melhorias foram corretamente implementadas para lidar com os riscos identificados.

3 Desenvolver competências para reduzir o risco cibernético de forma duradoura

Nas situações em que a causa das fraquezas e vulnerabilidades de segurança não tiver sido corrigida nas etapas anteriores, as iniciativas estratégicas devem ser projetadas para fornecer redução duradoura do risco cibernético. Por exemplo, abandonando sistemas legados de TI ou reformulando a maneira como o acesso privilegiado é gerenciado dentro da organização.

No uso dessa abordagem, recomendamos seis áreas de foco prioritárias para reduzir o risco de ataques de *ransomware*:

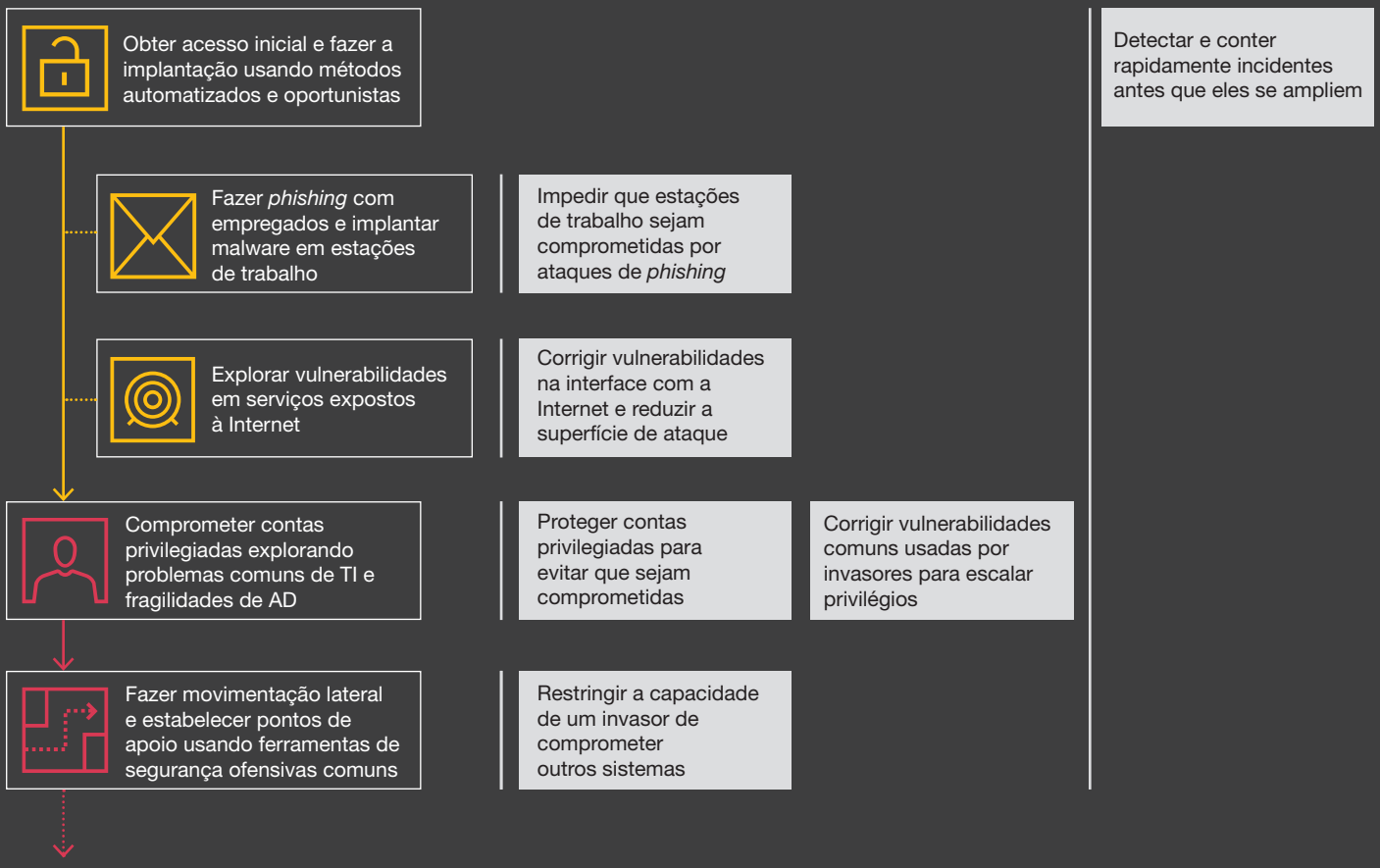
1. **Impedir que estações de trabalho sejam comprometidas por ataques de *phishing***
2. **Corrigir vulnerabilidades na interface com a Internet e reduzir a superfície de ataque**
3. **Proteger contas privilegiadas para evitar que sejam comprometidas**
4. **Corrigir vulnerabilidades comuns usadas por invasores para escalar privilégios**
5. **Restringir a capacidade de um invasor de comprometer outros sistemas**
6. **Detectar e conter incidentes rapidamente antes que eles se ampliem**

Para cada uma das áreas, listamos várias melhorias direcionadas que, com as abordagens certas de execução e priorização, podem ser realizadas em três meses. Embora muitas dessas melhorias pareçam óbvias à primeira vista, seu valor (ou o desafio de execução) não deve ser subestimado. São os "conceitos básicos" de segurança que ainda representam o principal desafio e oferecem os maiores benefícios.

Como o "diabo mora nos detalhes" do processo de redução do risco, recomendamos que as organizações que já implementaram essas melhorias ainda tomem medidas para validar se as ações efetivamente detectam e previnem as técnicas usadas nos ataques. Em casos investigados pela área de resposta a incidentes da PwC, observamos regularmente uma desconexão entre os níveis reais e percebidos de redução de risco ocasionada por melhorias que foram implementadas (por exemplo, a implantação de ferramentas sem configuração adequada).

Jornada típica de um ataque de *ransomware*

Seis áreas prioritárias de foco para reduzir o risco de ataques



Legenda

Automatizado e em grande escala

Executado por humanos

Área de foco prioritária

Impedir que estações de trabalho sejam comprometidas por ataques de *phishing*

Além de aumentar a conscientização dos empregados sobre os e-mails de *phishing*, as organizações devem implementar controles técnicos de segurança para evitar que e-mails de *phishing* com arquivos maliciosos comprometam as estações de trabalho. São ações cada vez mais importantes considerando os vários criminosos cibernéticos que sequestram *threads* de e-mail legítimas para distribuir arquivos maliciosos, enfrentando muitas iniciativas comuns de treinamento para conscientização de empregados. Principais ações:

Confirmar se as ferramentas de filtragem de e-mail estão configuradas adequadamente para bloquear e-mails de *phishing*.

A ferramenta de filtragem de e-mails deve ser configurada para verificar arquivos e links maliciosos em anexos, bloquear tipos de arquivos comumente usados por invasores (por exemplo, arquivos de *script* como HTA e PS1) e detectar técnicas usadas para fingir legitimidade (por exemplo, *spoofing* de endereços de e-mail internos ou envio a partir de domínios registrados recentemente). Essa ferramenta também deve ser integrada à inteligência de ameaças atualizada (incluindo indicadores anatômicos e comportamentais) para bloquear e-mails de *phishing* suspeitos.

Implantar e configurar ferramentas de filtragem da web para evitar que os usuários baixem arquivos maliciosos.

As ferramentas de filtragem devem ser configuradas para bloquear o download de arquivos comumente usados em *malware* e verificar todos os outros em busca de conteúdos maliciosos. Os sites devem receber uma classificação de risco e ser bloqueados de acordo com ela. Entre os sites de alto risco podem estar aqueles categorizados como maliciosos e os que usam domínios recém-registrados ou domínios de alto nível que costumam sofrer abusos.

Restringir macros do Microsoft Office

As macros do Microsoft Office devem ser desabilitadas sempre que possível para empregados, equipes e departamentos que não apresentam uma justificativa de negócios adequada. Quando isso não for possível, deve-se bloquear sua execução em documentos baixados da Internet. Ela deve ser permitida apenas para documentos de locais confiáveis ou para macros assinadas. Em organizações com licenças do Microsoft 365 E5, o Application Guard for Office deve ser habilitado sempre que possível.

Restringir a execução de scripts em estações de trabalho

O uso de *scripts* em estações de trabalho deve ser contido, por exemplo, com a implantação do modo de linguagem restrito do PowerShell para limitar o uso completo desse recurso aos usuários autorizados. As extensões de arquivo de *script* comuns devem ser configuradas para serem abertas em editores de texto por padrão. Isso reduz o risco de os usuários executarem arquivos maliciosos enviados por e-mails de *phishing*.

Corrigir as vulnerabilidades na interface com a Internet e reduzir a superfície de ataque

Muitos dos grupos recentemente envolvidos em ataques de *ransomware* exploram vulnerabilidades em serviços expostos à Internet a fim de obter acesso inicial às redes corporativas. No entanto, em muitos casos, vemos que essas vulnerabilidades permanecem sem solução, pois há problemas na cobertura e configuração das ferramentas de verificação de vulnerabilidades. Além disso, os esforços de correção não são priorizados, monitorados nem escalonados de forma eficaz. Veja as principais ações:

Realizar verificação e monitoramento de vulnerabilidades para garantir que elas sejam corrigidas rapidamente.

As ferramentas de verificação devem ser configuradas para realizar varreduras regulares e alertar para novas vulnerabilidades na interface com a Internet ou para serviços expostos. As equipes de segurança também devem garantir que todos os intervalos de endereços IP expostos à Internet sejam cobertos por ferramentas de verificação, além de revisar as exceções existentes para garantir que não tenham vulnerabilidades que possam ser exploradas por invasores.

Desativar ou restringir o acesso a serviços expostos à Internet para reduzir a superfície de ataque.

Os sistemas que permitem acesso externo devem ser auditados regularmente e as organizações devem procurar desabilitar ou restringir o acesso a quaisquer serviços expostos à Internet (por exemplo, RDP, SSH e SMB) que não sejam estritamente necessários. Isso atenua o risco de vulnerabilidades futuras, reduzindo a superfície geral de ataque. Nos casos em que os serviços sejam necessários, devem ser implementados controles de compensação para mitigar o risco (por exemplo, lista de permissões de endereços IP e autenticação forte).

Aplicar autenticação multifator para reduzir o impacto de credenciais comprometidas.

A autenticação baseada em risco multifatorial deve ser configurada em todos os sistemas que permitem acesso remoto e serviços expostos à Internet. Os registros de autenticação desses serviços também devem ser coletados e monitorados para casos de uso que possam representar contas comprometidas, por exemplo, eventos de login indicando “viagem impossível” do usuário ou logins realizados de países e dispositivos inesperados.

Proteger contas privilegiadas

Depois de comprometerem as estações de trabalho com ataques de *phishing*, os invasores buscam adquirir privilégios. A principal forma de dificultar essa ação é proteger as credenciais de contas privilegiadas para evitar que sejam expostas aos sistemas com maior risco de comprometimento. Principais ações:

Restringir o uso de contas de administrador de domínio.

As equipes de segurança devem trabalhar com as equipes de TI para desenvolver práticas de administração seguras que reduzam o risco de ataques de roubo de credenciais. Por exemplo, é preciso restringir o login de contas de administrador de domínio em estações de trabalho e servidores e apenas usar contas com privilégios de administrador de domínio quando estritamente necessário. As contas de administrador de domínio devem ser controladas por uma ferramenta de gerenciamento de acesso privilegiado que administre credenciais de forma segura e isole sessões de administrador.

Identificar e corrigir percursos de ataque para contas privilegiadas no Active Directory.

O BloodHound (uma ferramenta de segurança ofensiva) deve ser usado para identificar, investigar e eliminar percursos de ataque para contas privilegiadas. Eles muitas vezes existem devido a relações de confiança ocultas e não intencionais em ambientes do Active Directory. Por exemplo, permissões herdadas complexas ou configuradas incorretamente. Essa também deve ser a oportunidade para as equipes de segurança adquirirem confiança de que o uso do BloodHound é detectado de forma eficaz.

Restringir contas em grupos de administradores locais para reduzir a superfície de ataque de identidades para os *endpoints*.

É preciso revisar usuários e grupos no grupo de administradores locais em estações de trabalho e servidores, para assegurar que a inclusão de contas seja feita apenas quando estritamente necessário. Isso reduz o número de contas que, se comprometidas, podem conferir a um invasor acesso administrativo amplo aos sistemas. Os grupos de administradores locais também devem ser monitorados para assegurar a detecção de quaisquer modificações.

Monitorar o Active Directory para detectar o uso inseguro, o comprometimento e o abuso de contas privilegiadas.

As equipes de segurança devem implantar ferramentas, como o Microsoft Defender for Identity, para monitorar e detectar anomalias envolvendo contas privilegiadas, por exemplo, por meio do login a partir de um novo local. Contas com suspeitas de comprometimento devem ser bloqueadas e investigadas minuciosamente antes de ter seu acesso restabelecido.

Corrigir vulnerabilidades comuns usadas por invasores para escalar privilégios

A maneira mais comum que os invasores usam para adquirir privilégios em ambientes de TI corporativos é explorando vulnerabilidades e fraquezas resultantes de problemas de TI e fragilidades no AD. Essas questões predominam em redes corporativas internas extensas e pouco conhecidas, que evoluíram com o tempo sem governança de segurança nem investimentos adequados. Principais ações:

Impor senhas fortes nas contas de serviço para evitar que sejam quebradas.

Senhas fortes devem ser configuradas em todas as contas de serviço, priorizando as associadas a Nomes de Entidade de Serviço (SPNs, na sigla em inglês). Antes disso, é necessário fazer a auditoria e a manutenção de um inventário de contas de serviço para identificar os proprietários das contas, confirmando se eles ainda são necessários e assegurando sua identificação adequada e a aplicação de uma política de senha forte. Contas de serviço de longo prazo devem ser integradas a uma ferramenta de gerenciamento de contas privilegiadas.

Remover as credenciais armazenadas em compartilhamentos de rede para evitar que invasores façam uso delas para violar contas.

Em muitos casos investigados pela área de resposta a incidentes da PwC, as organizações, sem saber, têm credenciais privilegiadas armazenadas como texto sem formatação em compartilhamentos de arquivos de rede (ou outros locais de fácil acesso) que são explorados por invasores. Ferramentas de segurança ofensivas, como *scripts* do PowerShell, devem ser usadas para verificar a existência de credenciais em compartilhamentos de arquivos, para que elas sejam removidas e que as senhas expostas sejam redefinidas. O acesso aos compartilhamentos de rede também deve ser restrito ao máximo, pois essa é uma maneira comum de os invasores acessarem dados confidenciais.

Usar testes de segurança e o Microsoft Secure Score para identificar problemas de TI e fragilidades do Active Directory.

Testes de segurança simulando técnicas de ataque cibernético devem ser usados para identificar fraquezas e vulnerabilidades que um invasor poderia explorar. Para organizações que usam o Microsoft 365, o Secure Score também deve ser usado para identificar correções para melhorar a postura de segurança e reduzir a superfície de ataque. Por exemplo, é possível fazer isso com a habilitação do Credential Guard para melhorar a configuração segura da estação de trabalho.

Restringir a capacidade de um invasor de comprometer outros sistemas

Os invasores tentam comprometer outras estações de trabalho e servidores para adquirir privilégios e ter o acesso necessário para implantar *ransomware* em todo o ambiente. Dificultar o tráfego lateral de um invasor aumenta a chance de detectá-lo antes que ele possa implantar o *ransomware*. Principais ações:

Corrigir vulnerabilidades exploráveis em sistemas internos para remover rotas triviais que comprometam outros sistemas.

A verificação de vulnerabilidades deve ser usada para identificar esses problemas na rede interna. O escopo e a cobertura das ferramentas de verificação de vulnerabilidades devem ser revisados, e todas as exceções, investigadas. Nos casos em que a estabilidade do sistema for uma preocupação, testes de penetração personalizados ou manuais devem ser realizados para verificar vulnerabilidades. É preciso isolar os sistemas da rede quando eles não puderem ser corrigidos.

Prevenir e detectar técnicas comuns para implantação em massa de *ransomware*.

Firewalls baseados em host devem ser configurados por padrão em estações de trabalho para bloquear conexões de entrada, a fim de evitar a implantação em escala de *ransomware* em estações com o uso de tráfego SMB lateral. Mecanismos legítimos de implantação de software (por exemplo, SCCM) e ferramentas de administração remota (por exemplo, PsExec, WMI e GPO) devem ser monitorados para detectar o uso não autorizado. É preciso monitorar também os controladores de domínio quanto à execução de arquivos de *script*, comumente usados por invasores para implantar *malware* e desabilitar ferramentas de segurança.

Segmentar unidades de negócios e redes de alto risco para limitar o raio de ação dos ataques de *ransomware*.

As unidades de negócios e redes de alto risco devem ser segmentadas para limitar o número de sistemas afetados por um ataque de *ransomware*. Isso deve ser feito por meio do bloqueio da conectividade de rede, especialmente os protocolos comumente usados para tráfego lateral, e por meio da quebra ou do fortalecimento das relações de confiança do Active Directory.

Detectar e conter rapidamente incidentes antes que eles se ampliem

Como a implantação de *ransomware* é o estágio final de um ataque que pode ter começado há meses, quase sempre há oportunidades para detectar e conter esses ataques antes que os dados sejam criptografados ou roubados. Ao detectar e conter efetivamente infecções de "*malware* comum", as organizações também podem evitar oportunidades de acesso para os invasores que usam recursos de *ransomware*. Principais ações:

Implantar um agente de segurança de *endpoint* capaz de detectar e impedir a atividade do invasor.

Um agente de *endpoint* deve ser escolhido para detectar e prevenir atividades suspeitas em estações de trabalho e servidores por meio de análise comportamental – e do suporte para a AMSI (*Antimalware Scan Interface*) na detecção do uso malicioso de linguagens de *script* – e para capacitar equipes de segurança com rápidos recursos investigativos e de resposta.

Incorporar um serviço de detecção e resposta gerenciadas (MDR) para automatizar a resposta a ameaças comuns e garantir a detecção e correção de "*malware* comum".

Muitas organizações não têm recursos para monitorar efetivamente sua situação e responder ao volume de alertas criados. Elas carecem de experiência, ferramentas ou pessoal. Uma solução rápida é incorporar um serviço de detecção e resposta gerenciadas, pois ele fornece ferramentas necessárias em termos de pessoas, processos e *wrappers* de automação/orquestração, além de uma cobertura de detecção abrangente e demonstrável das técnicas dos invasores.

Certificar-se de que ferramentas comuns de invasão sejam detectadas e os alertas sejam corrigidos com eficácia.

Os testes de segurança devem ser usados para garantir que uma organização possa detectar com eficácia as ferramentas comuns de invasão e que as pessoas e os processos necessários estejam disponíveis para investigar e responder aos alertas. As lacunas de recursos devem ser identificadas e corrigidas por meio da implantação e configuração de ferramentas de detecção e resposta, desenvolvimento de processos de resposta a incidentes e treinamento.

Como as organizações devem se preparar para responder a um ataque de *ransomware*?

Embora a maioria dos esforços deva se concentrar na prevenção desses ataques, também é essencial que as organizações planejem e executem sua resposta a um grande incidente de *ransomware*. Em muitos casos nos quais a equipe de resposta a incidentes da PwC foi chamada a ajudar, já tinham sido perdidos vários dias por causa da falta de planos claros de recuperação e resposta, além do desafio de demonstrar à liderança, de maneira clara e estruturada, a magnitude das ações necessárias para restabelecimento do ambiente de forma segura.

Observamos que a "realidade da recuperação" nas organizações é muito mais desafiadora do que elas preveem, pois os ambientes de TI são complexos e as informações sobre sistemas essenciais não são claras. Mesmo quando as organizações têm acesso às chaves de descriptografia, em muitos casos elas ainda não conseguem descriptografar grandes quantidades de dados porque eles foram corrompidos por ferramentas de *ransomware* ou porque elas não têm capacidade técnica para fazê-lo.

Recomendamos que as organizações realizem as seguintes ações como preparação para um grande ataque de *ransomware* e mobilização de uma resposta eficaz:

1. Desenvolver e exercitar planos de resposta a incidentes e crises que descrevam claramente como a resposta deve ser gerenciada e coordenada. Esses planos devem ser testados para assegurar sua eficácia em um cenário de *ransomware* catastrófico, no qual a segurança e as ferramentas de TI comuns talvez estejam indisponíveis e os esforços de recuperação possam ter que ser mantidos por semanas ou meses.

2. Compreender onde estão os dados críticos; quais seriam as implicações nesses dados se os sistemas não estivessem disponíveis; quais os requisitos regulatórios associados; e o que precisaria ser recuperado para criar uma "empresa mínima viável".

3. Assegurar a criação e a validação dos backups off-line para todos os sistemas e dados críticos, inclusive o Active Directory, com um procedimento de restauração bem definido e testado.

4. Desenvolver ou reter o conhecimento técnico para investigar e responder ao ataque (por exemplo, investigando a extensão do comprometimento, identificando o acesso do invasor e removendo-o do ambiente).

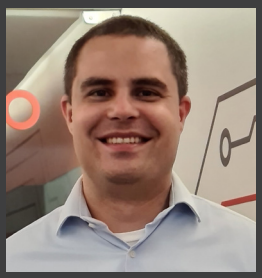
Como podemos ajudar

Nossa equipe multidisciplinar tem experiência na prevenção e detecção de ataques de *ransomware* e na resposta a eles.

Ajudamos organizações em diversos setores a compreender sua vulnerabilidade a essa ameaça, implementar melhorias táticas para reduzir imediatamente o risco e mobilizar programas estratégicos para resolver problemas que estão na raiz dessa questão, desenvolvendo recursos sustentáveis de segurança cibernética.

Contatos

Eduardo Batista
Sócio e líder de *Cybersecurity*
eduardo.batista@pwc.com



Rafael Cortes
Diretor, especialista em *Cybersecurity*
cortes.rafael@pwc.com

Para nossos *insights* e recursos mais recentes, visite:
https://www.pwc.com.br/pt/consultoria-negocios/ciberseguranca-privacidade.html

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil