Navegando pelo Ransomware em 2025:

Principais Insights e Estratégias de Prevenção

Digital Security
Progress. Protected.

Panorama do Ransomware: Como Prevenir e Ir Além

O *ransomware* continua sendo uma das ameaças cibernéticas mais urgentes em 2025, evoluindo constantemente em sofisticação e impacto. Apesar de anos de avanços em cibersegurança, organizações de todos os tamanhos e setores ainda enfrentam ataques persistentes que ultrapassam suas defesas por meio de técnicas cada vez mais refinadas. Um dos avanços mais recentes nessa batalha contínua é o uso dos chamados **EDR killers**, *malwares* projetados para desativar soluções de detecção e resposta em endpoints (EDR) antes da implantação do ransomware. Isso demonstra como os agentes de ameaça se adaptam aos avanços em segurança para explorar brechas nas defesas das empresas.

A motivação por trás dos ataques de ransomware continua elevada, impulsionada não apenas por incentivos financeiros, mas também por objetivos táticos e estratégicos. Embora grupos de cibercriminosos utilizem ransomware principalmente para obter lucro, grupos APT podem usá-lo para encobrir rastros ou como ferramenta destrutiva para interromper infraestruturas críticas — frequentemente com consequências geopolíticas. Esse uso em constante evolução adiciona ainda mais complexidade ao cenário de ameaças. Tanto os grupos motivados financeiramente quanto os atores APT refinam continuamente suas técnicas, explorando comprometimentos na cadeia de suprimentos, vulnerabilidades zero-day e campanhas de *phishing* assistidas por IA para ampliar seu alcance e impacto.

$4.91 milhões

O custo médio de um ataque de ransomware em 2024.
Fonte: *IBM: Cost of a Data Breach Report 2024*

Neste cenário de ameaças em constante evolução, a prevenção continua sendo a medida mais eficaz que as organizações podem adotar para fortalecer sua postura de segurança. Embora a resposta a incidentes e a recuperação sejam fundamentais, impedir que o ransomware se estabeleça desde o início reduz tanto a interrupção das operações quanto as perdas financeiras.

Uma estratégia de segurança preventiva — que inclua uma gestão de correções eficaz, arquitetura de confiança zero, proteção nativa com IA, políticas de gerenciamento de senhas, autenticação multifator (MFA), conscientização dos colaboradores e monitoramento contínuo de ameaças — pode reduzir significativamente o risco de infecção por ransomware.

À medida que avançamos em 2025, a capacidade de antecipar, prevenir e neutralizar ameaças de ransomware antes que se concretizem é mais crucial do que nunca. Isso inclui contar com tecnologias de remediação poderosas, prontas para ajudar 24 horas por dia, 7 dias por semana, durante todo o ano.

Últimas Observações sobre o Ransomware

Várias tendências-chave de ransomware em 2024 devem moldar o cenário de ameaças e as estratégias de defesa em 2025. Manter o foco nessas tendências é essencial para se manter à frente dos riscos em evolução.

Um dos eventos mais notáveis de 2024 foi o desmantelamento do LockBit, que era o grupo líder de ransomware-as-a-service (RaaS), responsável pela disseminação da variante de ransomware mais implantada no mundo. A interrupção do LockBit criou um vácuo significativo no cenário de ransomware. Esse espaço foi rapidamente preenchido por outros atores de ransomware, com o **RansomHub** surgindo como o **mais bem-sucedido até agora**.

Até o final do segundo semestre de 2024, o RansomHub havia listado quase 500 vítimas, consolidando-se como um jogador dominante no ecossistema de ransomware. Até agora, o RansomHub criptografou e exfiltrou dados de vítimas de uma ampla gama de setores: TI, serviços e instalações governamentais, saúde, serviços de emergência, alimentos e agricultura, serviços financeiros, instalações comerciais, manufatura crítica, transporte e setores de infraestrutura crítica, como comunicações.

Embora o RaaS seja um ambiente altamente competitivo para cibercriminosos, onde as quadrilhas inovam continuamente e ajustam seus programas de afiliados para atrair mais parceiros e aumentar a lucratividade, a ESET espera que o RansomHub mantenha sua posição dominante ao longo de 2025. Isso se deve não apenas às suas táticas agressivas e métodos sofisticados para manter o controle sobre redes comprometidas e explorar vulnerabilidades nos sistemas, mas também à sua **capacidade de atrair afiliados** anteriormente associados ao LockBit e ao BlackCat.

À medida que o modelo RaaS continua a evoluir, os atores de ransomware estão adotando técnicas especializadas para evitar a detecção e aumentar os danos. Embora os "EDR killers" já sejam usados por grupos de ransomware há bastante tempo, sua prevalência aumentou, com algumas quadrilhas agora desenvolvendo ferramentas personalizadas e oferecendo-as como parte de seus programas de RaaS. Ao mesmo tempo, muitos atores

de ransomware que entram no ecossistema RaaS seguem tendências definidas por grupos estabelecidos, frequentemente programando seus criptografadores em Rust ou Go para garantir compatibilidade entre plataformas e um alcance mais amplo.

EDR KILLERS: são malwares especializados projetados para desativar soluções de segurança ao utilizar técnicas de BYOVD (Bring Your Own Vulnerable Driver). Os atacantes primeiro instalam drivers legítimos, mas vulneráveis, e então os exploram para executar ações privilegiadas a partir do espaço do kernel. Isso permite que eles contornem os controles de segurança, finalizem processos de segurança e desativem os mecanismos de detecção e proteção.

À medida que os EDR killers se tornam uma parte comum dos ataques de ransomware, a ESET espera que os atores mais avançados melhorem esse tipo de ferramenta em 2025, tornando-a cada vez mais sofisticada, protegida e mais difícil de detectar. O que essa tendência mostra é que ferramentas de segurança, como **os EDRs, são um incômodo para os cibercriminosos**, que irão se esforçar ao máximo para removê-las ou, pelo menos, desativá-las.

O modelo RaaS e as técnicas avançadas não devem ser discutidos sem reconhecer o envolvimento e o papel dos grupos de Ameaças Persistentes Avançadas (APT). Esses grupos utilizam o ransomware não apenas para ganho financeiro, mas também para alcançar objetivos estratégicos mais amplos. Os seguintes grupos APT têm se envolvido mais recentemente em ataques de ransomware:

ChamelGang (China-aligned)

Este grupo foi observado utilizando ransomware para distrair de suas operações secretas, dificultando a detecção de suas atividades principais pelos defensores.

Esse grupo, às vezes também conhecido como CamoFei, tem utilizado a variante de ransomware CatB em ataques que impactam organizações de alto perfil em todo o mundo, incluindo organizações governamentais, como a Presidência do Brasil, ou infraestruturas críticas, como o All India Institute of Medical Sciences (AIIMS), uma universidade pública de pesquisa médica e hospital.

Moonstone Sleet (North Korea-aligned)

Conhecido por desenvolver e implantar seu próprio ransomware, o FakePenny, o Moonstone Sleet usa ransomware principalmente

➜ para ganho financeiro. Anteriormente conhecido como Storm-17, o Moonstone Sleet foi identificado como alvo de setores financeiros e de ciberespionagem. Seus métodos incluem o uso de software trojanizado, como o PuTTY, para acesso inicial, distribuição de jogos maliciosos e pacotes do Node Package Manager (NPM), implantação de carregadores personalizados de malware e criação de empresas falsas de desenvolvimento de software, como StarGlow Ventures e C.C. Waterfall.

Essas empresas falsas interagem com potenciais vítimas por meio de plataformas como LinkedIn, Telegram, redes de freelancers e e-mail.

Pioneer Kitten (Iran-aligned) y Andariel (North Korea-aligned)

Esses grupos têm sido associados a ataques de ransomware, principalmente como fornecedores de acesso inicial. É provável que vendam esse acesso para outros cibercriminosos em busca de ganho financeiro. O primeiro grupo tem invadido principalmente setores como defesa, educação, finanças e saúde, enquanto o segundo foca em infraestruturas críticas e organizações de saúde, especialmente nos Estados Unidos.

O Pioneer Kitten também é conhecido pelos nomes Fox Kitten, UNC757, Parisite, RUBIDIUM e Lemon Sandstorm, e utiliza uma ampla gama de técnicas. Andariel é considerado um subgrupo do Lazarus Group e tem sido atribuído ao Bureau Geral de Reconhecimento da Coreia do Norte.

As empresas e diversas organizações não são os únicos alvos esperados para ataques de ransomware. Os atores de ameaça estão novamente explorando e mirando de forma sistemática os usuários domésticos. Em agosto de 2024, o ransomware Magniber lançou uma campanha global em larga escala, direcionada a usuários comuns e criptografando seus dispositivos ao redor do mundo.

Embora ações como essa já tenham sido observadas no passado, essa campanha marcou uma mudança significativa nas estratégias de segmentação de ransomware, principalmente devido à escala e distribuição ampla do ataque, que foca em usuários individuais que frequentemente não possuem medidas robustas de cibersegurança.

O ransomware Magniber foi distribuído por meio de downloads de software malicioso, atualizações falsas e geradores de chaves, exigindo resgates que variam de $1.000 a $5.000 para descriptografar. Os métodos usados para distribuir o Magniber incluem zero-days do Windows, atualizações falsas do Windows e do navegador, e cracks de software trojanizados e geradores de chaves.

Usuários domésticos, portanto, devem permanecer vigilantes e proativos em suas práticas de cibersegurança. Ao adotar medidas preventivas, os indivíduos podem reduzir significativamente o risco de se tornarem vítimas de ataques de ransomware.

Os pedidos de resgate direcionados a usuários individuais aumentaram para até

$5,000

em 2024.

Fonte: *BleepingComputer: Surge in Magniber ransomware attacks impact home users worldwide*

Prevenir Mais, Gerenciar Menos

O ransomware é normalmente o payload final, precedido por outras ameaças, incluindo phishing, exploração, ataques de força bruta, credenciais comprometidas, downloaders ou malwares personalizados. Muitos ataques de ransomware em potencial são identificados precocemente no ciclo de vida do ataque, e somente se os atacantes conseguirem contornar as defesas de suas vítimas e finalmente tentarem implantar o ransomware é que podemos falar de um ataque de ransomware.

Para prevenir eficazmente os ataques de ransomware, as organizações devem adotar uma abordagem de segurança em camadas, incorporando automação que aborde cada estágio do ciclo de vida do ataque. Isso pode ser considerado uma **abordagem preventiva**, que muitas organizações e empresas cada vez mais reconhecem como uma estratégia com grande potencial — e os motivos são indiscutíveis.

Primeiro, o mais importante: o **treinamento e a conscientização dos funcionários** são cruciais, pois o phishing continua sendo um dos principais vetores para o ransomware. Os funcionários devem estar cientes dos sinais comuns de phishing e entender a importância de não clicar em links desconhecidos ou baixar anexos não solicitados.

Educar regularmente a equipe sobre como reconhecer tentativas de phishing, usar senhas fortes e habilitar autenticação multifatorial pode reduzir significativamente os riscos. A proteção de endpoints, por meio de soluções robustas de antivírus, anti-malware e ferramentas de Detecção e Resposta em Endpoints (EDR), também é importante, pois é essencial para detectar e bloquear atividades maliciosas.

Nenhuma solução de EDR é totalmente imune aos EDR killers, pois os atacantes exploram vulnerabilidades em drivers assinados legitimamente para executar código

malicioso no espaço do kernel. Esses drivers, uma vez carregados no Windows, podem ser usados para desativar ferramentas de segurança. Os produtos da ESET bloqueiam de forma eficaz muitos desses drivers vulneráveis, e os analistas e administradores da ESET podem ajudar os clientes a fortalecer ainda mais suas defesas. Ao configurar políticas rigorosas para aplicações potencialmente indesejadas (PUA), apenas os drivers mais recentes são permitidos — uma abordagem que se beneficia do suporte especializado.

Reforçar o sistema operacional com regras WDAC (Windows Defender Application Control) também é importante, somando-se a uma estratégia de prevenção de longo prazo que, por si só, já é necessária. Esse tipo de orientação especializada pode fazer toda a diferença quando se trata de lidar com os EDR killers.

Outros passos importantes incluem **medidas de segurança de rede** como firewalls, sistemas de detecção de intrusões (IDS) e segmentação de rede, que ajudam a controlar e monitorar o tráfego, prevenir acessos não autorizados e limitar a propagação do ransomware.

67%

dos CISOs relataram aumento nos orçamentos de cibersegurança em 2024 em comparação com 2023.
Fonte: *IANS, 2024 Security Budget Benchmark Report*

Dificilmente qualquer uma dessas medidas pode ser executada com eficácia sem uma **gestão regular de atualizações**, que garante que todos os sistemas e softwares estejam atualizados com os patches de segurança mais recentes, fechando vulnerabilidades que poderiam ser exploradas por atacantes

Implementar controles de acesso com base no princípio do menor privilégio e adotar um **modelo de segurança de confiança zero (zero trust)** reduz ainda mais o risco de acessos não autorizados e, atualmente, faz parte dos padrões comuns de prevenção em cibersegurança. O mesmo vale para **backups regulares** de dados críticos, armazenados offline ou em ambientes de nuvem segura, que são vitais para a recuperação em caso de um ataque. Esses backups devem, é claro, ser testados regularmente para garantir sua eficácia.

Quando falamos das operações do dia a dia e de como a prevenção pode ser útil nesse contexto, medidas de **segurança de e-mail**, como filtragem e proteção contra spam, ajudam a bloquear e-mails e anexos maliciosos antes que cheguem aos usuários. Muitos incidentes ainda ocorrem devido a erro humano, e o e-mail continua sendo um dos principais vetores de ataque

Como há muitas outras aplicações utilizadas no cotidiano corporativo, a **lista de permissões**

de aplicações (application whitelisting) também é de grande importância. Ela garante que apenas aplicativos aprovados possam ser executados na rede, impedindo a execução de softwares não autorizados.

Ter um plano de resposta a incidentes bem desenvolvido e realizar simulações regulares garante que as organizações estejam preparadas para responder de forma eficaz a ataques de ransomware.

Todas essas medidas contribuem para a construção de uma postura robusta de cibersegurança por meio de estratégias de defesa proativas, baseadas no entendimento de que prevenir é sempre melhor do que remediar.

Por que não pagar o resgate?

Não sejamos ingênuos — mesmo com uma abordagem preventiva sólida, um ataque de ransomware ainda pode acontecer. Os agentes de ameaça refinam constantemente suas táticas, explorando vulnerabilidades zero-day, fragilidades na cadeia de suprimentos ou erros humanos para contornar até mesmo boas defesas.

Mas, embora um ataque possa ser disruptivo, ele não é uma situação sem solução. Organizações que agem rapidamente, utilizam planos de resposta a incidentes e contam com backups seguros podem se recuperar sem ceder à extorsão. Isso nos leva a um ponto crucial — por que pagar o resgate não é a solução correta.

63%

63% foi a parcela de vítimas de ransomware que envolveram as autoridades e evitaram o pagamento de resgate em 2024.
Fonte: *IBM, Cost of a Data Breach Report 2024*

Pagar criminosos que criptografaram seus dados significa:

- Validar o modelo de negócio por trás do crime.
- Incentivar a continuidade da atividade criminosa ao financiá-la, ainda que involuntariamente.
- Permitir que gangues de ransomware pesquisem vulnerabilidades zero-day e desenvolvam novos exploits.
- Estar sujeito a novos ataques e novas exigências de pagamento no futuro.

Pagar o resgate não oferece nenhuma garantia de que os cibercriminosos fornecerão uma chave de descriptografia funcional — afinal, não há como responsabilizá-los ou tomar medidas legais contra eles. Existem várias razões pelas quais o pagamento pode não resultar na recuperação dos dados:

- Alguns dados podem ter sido corrompidos durante a criptografia, tornando-os irrecuperáveis.
- A ferramenta de descriptografia fornecida pode vir acompanhada de malwares adicionais, apresentar falhas ou ser significativamente mais lenta do que a restauração a partir de backups.
- Existem várias maneiras pelas quais o processo de entrega da chave de descriptografia pode falhar, incluindo bugs no código de descriptografia, esquemas de criptografia excessivamente complexos, complicações no processamento do pagamento (especialmente com criptomoedas) ou táticas de dupla extorsão exigindo pagamentos adicionais.
- O atacante pode simplesmente agir de má-fé, sem qualquer intenção de fornecer uma chave de descriptografia.

Na prática, geralmente existem dois principais argumentos a favor do pagamento do resgate. O primeiro é a incapacidade de restaurar os dados criptografados a partir de backups — seja porque os backups não existem, estão incompletos ou foram corrompidos. No entanto, pode haver alternativas ao pagamento. Antes de tomar qualquer decisão, consulte o fornecedor da sua solução de segurança:

(a) para verificar se existe uma ferramenta de descriptografia disponível para a variante específica do ransomware, o que pode permitir a recuperação sem pagamento.

(b) para confirmar se o pagamento do resgate é conhecido por ser ineficaz contra aquela variante em particular.

O segundo argumento comum para o pagamento do resgate é que ele seria mais barato do que restaurar a partir dos backups. Embora isso possa ser tecnicamente verdade em termos de tempo e esforço, continua sendo uma decisão fundamentalmente falha por vários motivos.

Como mencionado anteriormente, as promessas de descriptografia são pouco confiáveis, há uma alta probabilidade de ser atacado novamente após o primeiro pagamento — lembre-se: você não está lidando com pessoas que seguem a lei — e, ao pagar, você está financiando uma operação criminosa, o que, no fim das contas, aumenta a probabilidade de novos ataques contra outras vítimas. Em alguns casos, o pagamento é inclusive ilegal, principalmente quando os atacantes estão sob sanções.

Como a ESET pode ajudar com ransomware e remediação?

Uma **ferramenta de remediação**, confiável, como parte de uma estratégia preventiva e proativa, pode ser sua melhor defesa diante de decisões difíceis — como investir pesadamente na recuperação de dados ou até considerar o pagamento de um resgate. Com uma tecnologia poderosa de remediação contra ransomware, você se mantém alguns passos à frente.

A *Remediação de Ransomware da ESET* é uma camada de segurança totalmente automatizada dentro do módulo moderno de proteção de endpoints da plataforma ESET PROTECT. Desenvolvida para fortalecer a defesa contra ransomware, ela atua em conjunto com o Ransomware Shield, que detecta e bloqueia comportamentos suspeitos. Essa solução combina prevenção e remediação em uma abordagem multietapas abrangente no combate à criptografia.

Ao contrário das soluções tradicionais de remediação e reversão, que dependem do Serviço de Cópia de Sombra de Volume do sistema operacional — frequentemente um

94%

das organizações entrevistadas relataram tentativas de cibercriminosos de comprometer seus backups durante o ataque em 2024.
Fonte: *SC World, Compromised backups send ransomware recovery costs soaring*

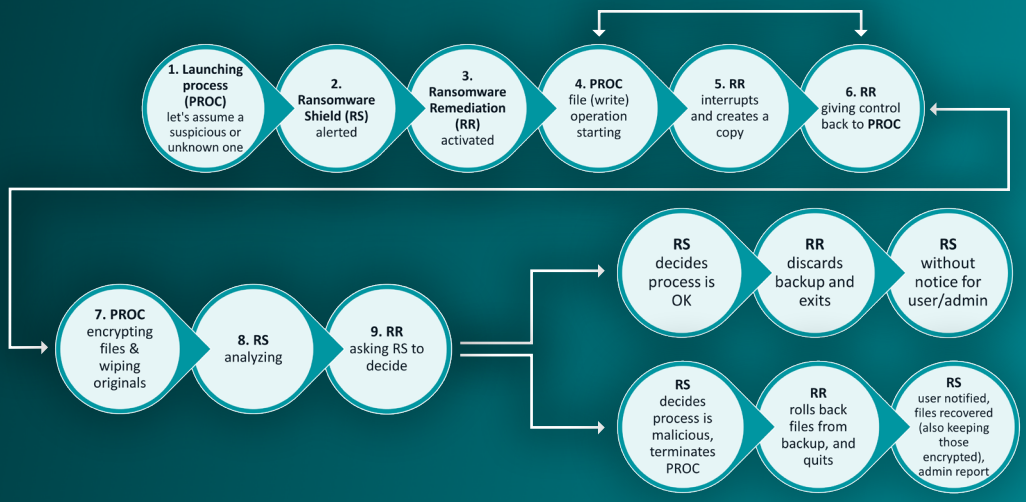
alvo principal para os atacantes — a ESET utiliza uma solução própria de armazenamento em cache de arquivos, oferecendo maior flexibilidade e confiabilidade. Os operadores de ransomware frequentemente excluem ou sobrescrevem as cópias de sombra para impedir a recuperação, tornando os métodos tradicionais de reversão ineficazes.

Em contraste, o processo de backup de Remediação de Ransomware da ESET não é um serviço local, mas opera dentro de sua própria seção protegida de armazenamento no disco, onde os arquivos não podem ser modificados, corrompidos ou excluídos pelos atacantes.

A tecnologia monitora continuamente todos os processos, interceptando modificações de arquivos em tempo real. No momento em que um processo de alteração de arquivo é detectado, o sistema de backup em tempo real da ESET cria cópias dos arquivos originais — mesmo antes dos sistemas de reputação comportamental, como o Ransomware Shield, determinarem se a atividade é maliciosa. Tudo funciona em conjunto com as

tecnologias ESET LiveSense, dissecando e analisando o malware até seu núcleo.

A Remediação de Ransomware da ESET, como uma abordagem proativa, garante que as organizações possam recuperar seus arquivos instantaneamente, eliminando a necessidade de pagar o resgate. A Remediação de Ransomware da ESET está incluída em todos os níveis da Plataforma ESET PROTECT, começando pelo ESET PROTECT Advanced. Uma versão de teste totalmente funcional de 30 dias também está disponível.



ESET Ransomware Shield e a Árvore de Processos Complexos da Remediação de Ransomware

QUAIS SÃO OS PRINCIPAIS BENEFÍCIOS DA REMEDIAÇÃO DE RANSOMWARE DA ESET?

- A ferramenta oferece uma reversão abrangente através da restauração automatizada e sem interrupções dos arquivos a partir de um cache seguro.
- Ela só protege os arquivos que são afetados por um processo suspeito, portanto, o espaço em disco é muito menos um problema.
- A ESET utiliza sua própria tecnologia exclusiva e não depende do recurso VSS (Volume Shadow Copy Service) fornecido nos sistemas operacionais Windows da Microsoft, como outras soluções fazem.
- O recurso está ativado por padrão nos níveis de assinatura do ESET PROTECT elegíveis; não há interação do usuário necessária, e os administradores podem configurar pastas e tipos de arquivos protegidos.

Conclusão

O ransomware continua sendo uma ameaça formidável à cibersegurança em 2025, com táticas em constante evolução e aumento de sofisticação. A queda do LockBit e o surgimento do RansomHub destacam a dinâmica em mudança do ecossistema RaaS, onde o sucesso é frequentemente medido pela capacidade de atrair e manter afiliados.

Após a desarticulação do LockBit pelas autoridades, muitos afiliados perderam confiança e migraram para o RansomHub, enfraquecendo significativamente a escala operacional do LockBit. Enquanto isso, técnicas avançadas como os EDR killers, juntamente com a participação de grupos APT, continuam a adicionar camadas de complexidade a essas ameaças.

As organizações devem adotar uma abordagem de segurança em camadas, preventiva-primeiro, para combater eficazmente o ransomware e as ameaças que o precedem. Isso inclui treinamento de funcionários, proteção robusta de endpoints e dados, backups regulares e soluções de segurança avançadas, como MDR ou XDR.

Com o conjunto abrangente de cibersegurança da ESET — incluindo a tecnologia de Remediação de Ransomware, uma solução proativa que permite recuperar rapidamente e minimizar o impacto dos ataques — você pode lidar com as ameaças de ransomware mais sofisticadas.

LEIA MAIS

Esta é a ESET

Defesa proativa. Nosso negócio é minimizar a superfície de ataque.

Fique um passo à frente das ameaças cibernéticas conhecidas e emergentes com nossa abordagem focada na prevenção, impulsionada por inteligência artificial e expertise humana.

Experimente uma proteção de alto nível, graças à nossa inteligência global de ameaças cibernéticas desenvolvida internamente, analisada e refinada ao longo de mais de 30 anos — base que impulsiona nossa ampla rede de P&D, liderada por pesquisadores reconhecidos mundialmente.

A ESET protege o seu negócio para que ele possa liberar todo o potencial da tecnologia.

Multicamadas, com foco em prevenção

IA de ponta combinada com expertise humana

Inteligência contra ameaças reconhecida mundialmente

Suporte hiperlocal e personalizado

eset®
Digital Security
Progress. Protected.