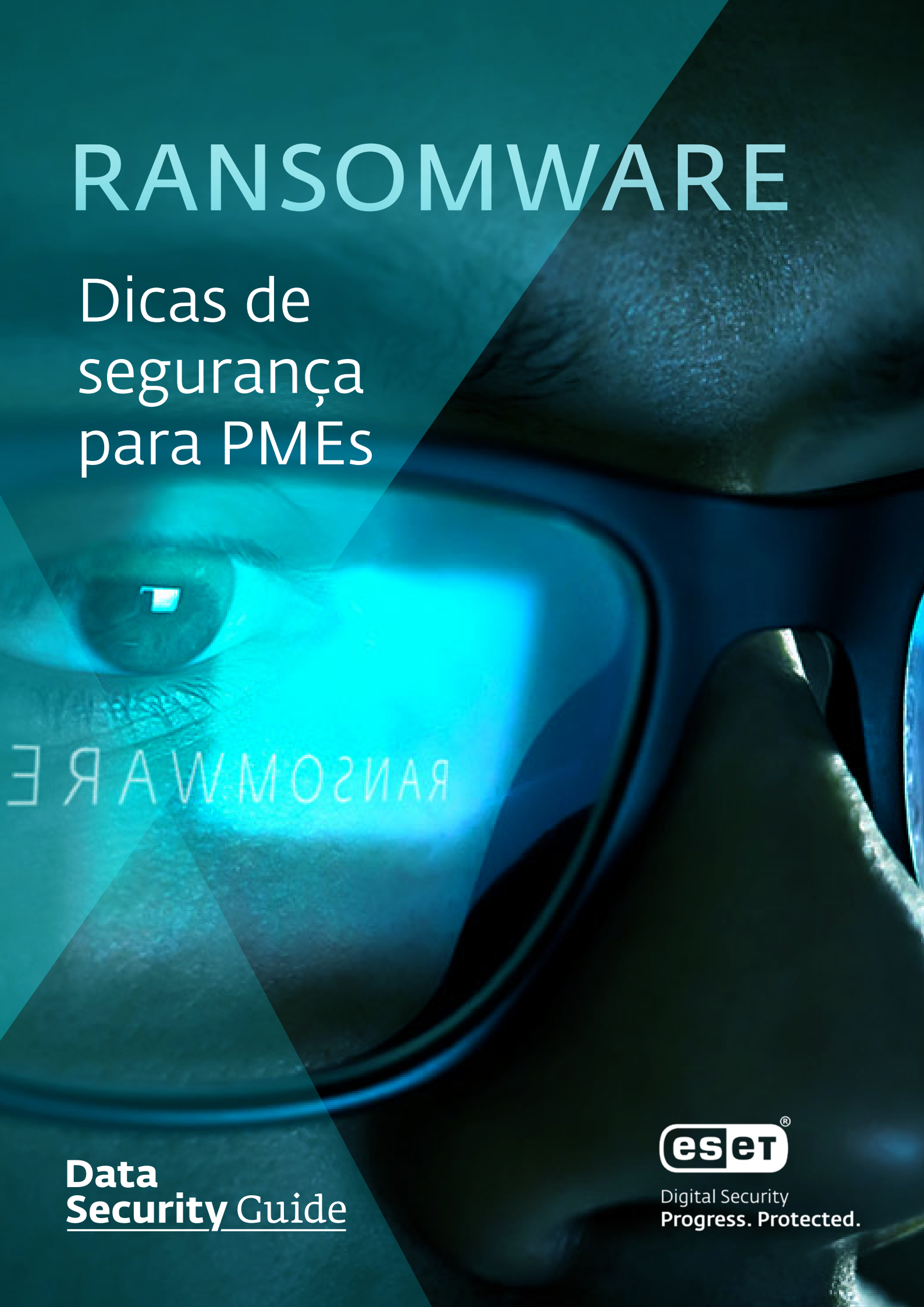
RANSOMWARE

Dicas de segurança para PMEs



Data Security Guide

ESET
Digital Security
Progress. Protected.

ÍNDICE

INTRODUÇÃO

RANSOMWARES EM ASCENSÃO

Nos últimos anos, grupos criminosos que desenvolvem esse tipo de malware e executam ransomwares como serviço têm evoluído para uma abordagem diferente e mais direcionada para esses ataques, tornando as métricas dessas operações mais difíceis de serem coletadas.

Os cibercriminosos têm demonstrado abordagens mais agressivas e esforços persistentes na busca por vulnerabilidades nos sistemas de cibersegurança, atacando bancos de dados, servidores web e smartphones. Ataques de força bruta ao protocolo de desktop remoto (RDP) ou ataques DDoS contra sites de empresas são apenas uma parte do que vemos acontecendo.

RANSOMWARES COMO AMEAÇA PARA PEQUENAS E MÉDIAS EMPRESAS

As pequenas e médias empresas (PMEs) têm se tornando alvos cada vez mais atrativos para ataques de ransomwares.
Por quê? Porque essas empresas acumulam dados mais valiosos do que consumidores individuais e, ao mesmo tempo, carecem das medidas de segurança robustas utilizadas por grandes corporações ou instituições.

Assim, esses fatores funcionam como um "ponto ideal" para cibercriminosos, elevando o risco de ataques de ransomwares às PMEs.

Além disso, a propensão da gerência de PMEs a não considerar suas empresas como alvos potenciais pode resultar na falta de backups regulares de seus dados essenciais, deixando os negócios desprevenidos em caso de ataques

eset Digital Security Progress. Protected.

FUNCIONAMENTO TÉCNICO

Um ataque de ransomwares pode ser definido como uma tentativa de extorquir dinheiro de uma organização por meio da restrição de acesso aos seus próprios dados.
Perceber que você foi vítima de ransomware costuma ser rápido. Geralmente, ransomwares enviam notificações logo após afetar seus dispositivos, seja exibindo um aviso de resgate na tela, adicionando um arquivo de texto nas pastas afetadas ou alterando a extensão dos arquivos criptografados.

Tipos de ransomwares

Screen locker

Bloqueia o acesso ao seu dispositivo por meio de um bloqueador de tela, permitindo apenas o uso de uma interface de usuário maliciosa.

PIN locker

Altera o código PIN do seu dispositivo, tornando seu conteúdo e funcionalidade inacessíveis.

Disk coding

Criptografa o MBR (Master Boot Record) e/ou estruturas críticas do sistema de arquivos, impedindo o seu acesso ao sistema operacional.

Crypto ransomware

Criptografa os arquivos em seu disco..

eset Digital Security Progress. Protected.

FUNCIONAMENTO TÉCNICO

Durante a pandemia de covid-19, o escopo dos ataques de ransomwares se expandiu. As sequências de lockdowns resultaram em um aumento nos e-mails de phishing, direcionados principalmente a funcionários que migraram para o trabalho remoto, com acesso a sistemas e serviços internos da empresa por meio do RDP, tornando-se um vetor frequente na propagação de ransomwares.

Além disso, os cibercriminosos que operam esquemas de ransomwares como serviço (RaaS) costumam explorar vulnerabilidades para obter acesso ao dispositivo e, em seguida, movem-se lateralmente para um servidor e para a rede em geral, decidindo posteriormente se ransomwares serão utilizados.

Esses agentes também podem realizar ataques à cadeia de suprimentos para acessar ecossistemas de TI inteiros. Ao assumir o controle de plataformas populares de provedores de serviços gerenciados (MSP) e ferramentas de produtividade, agentes de ameaças podem disseminar ransomwares em diversas redes em escala. Outra tendência é que dispositivos de armazenamento conectados à rede (NAS), que fornecem dados a diferentes usuários e costumam ser utilizados para compartilhar arquivos para backups também têm despertado a atenção de grupos de ransomwares focados neste tipo de ameaça.

eset Digital Security
Progress. Protected.

FUNCIONAMENTO PSICOLÓGICO

A pressão psicológica é a principal tática empregada por operadores de ransomwares. A pressão se intensificam quando indivíduos ou organizações enfrentam danos reais à reputação, interrupções nos negócios ou até mesmo penalidades legais e financeiras.

Também é bastante provável que ocorra algum tipo de manipulação. Frequentemente, as vítimas observam diversos pontos de seus ambientes digitais sendo afetados, desde ataques de negação de serviço (DDoS) em seus sites até demonstrações infames da presença criminosa em uma rede. Alguns exemplos dessas abordagens alarmantes:

- Print bombing, no qual com que diversas impressoras em uma rede imprimam uma nota de resgate, comprometendo a capacidade da administração de controlar a comunicação interna e externa.

- •Acesso aos dados dos clientes de uma empresa, seguido de contato direto ou até mesmo chamadas com os clientes, envolvendo ameaças adicionais e a exposição pública das vítimas, enquanto seus departamentos de TI trabalham para mitigar os impactos do ataque.

AUMENTANDO A PRESSÃO SOBRE AS VÍTIMAS

Para garantir o recebimento da quantia solicitada, os cibercriminosos frequentemente multiplicam os métodos de extorsão.

Dupla extorsão

Essa estratégia combina criptografia e exfiltração de dados. Os cibercriminosos não apenas impedem o acesso aos arquivos valiosos ou críticos da vítima, como também podem realizar vazamentos ou vender os dados para outros agentes maliciosos. Um exemplo é o método chamado doxing, no qual cibercriminosos buscam dados sensíveis nos sistemas de suas vítimas, ameaçando divulgá-los, a menos que uma taxa adicional seja paga, além do resgate.

eset Digital Security Progress. Protected.

FUNCIONAMENTO PSICOLÓGICO

Tripla extorsão

Alguns operadores de ransomwares entram em contato com parceiros comerciais ou clientes das vítimas que não pagaram o resgate, informando que seus dados sensíveis foram acessados como parte do ataque. Em seguida, sugerem que esses parceiros pressionem a organização que foi vítima a realizar o pagamento, a fim de evitar a divulgação desses dados, ou exigem o pagamento diretamente dos parceiros.

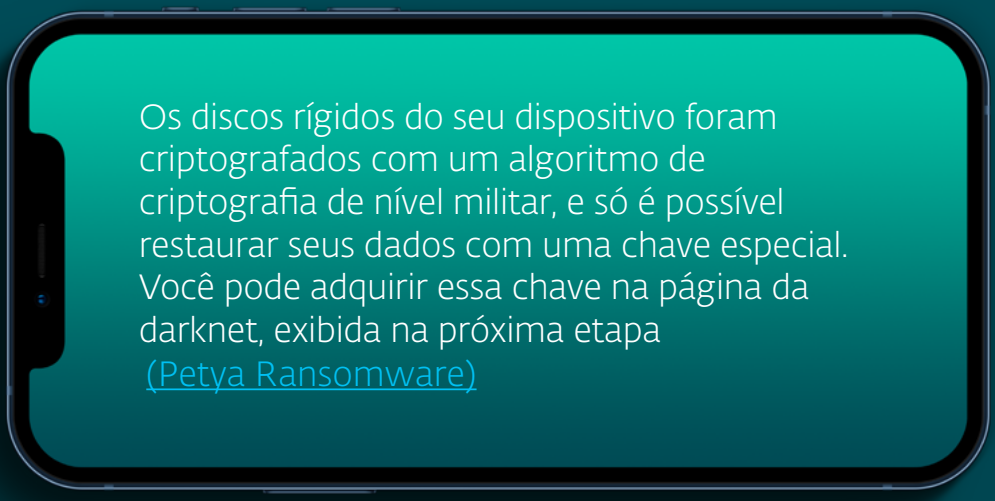
Em outras palavras, os ransomwares podem transformar um incidente de malware em uma guerra psicológica para forçar as vítimas a agirem contra sua própria vontade e melhores interesses. Esses ataques não precisam ser realizados por meio de malware personalizado, ameaças de dia zero ou ataques persistentes de longo prazo. Também podem acontecer como resultado de práticas de segurança inadequadas por parte de funcionários, configuração inadequada do RDP e outras ferramentas de acesso remoto, ou falhas nas práticas e processos, tanto dentro de sua organização quanto de seus provedores de serviços e outros agentes em sua cadeia de suprimentos.

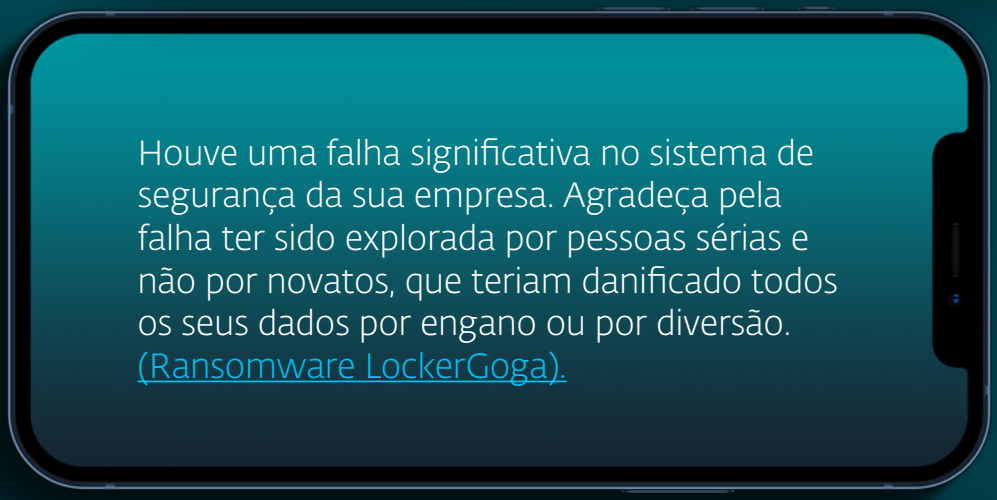
A segurança é uma responsabilidade compartilhada, por isso, o treinamento de cibersegurança das equipes de funcionários deve estar atualizado e abordar as últimas tendências em ciberameaças.
Informar os funcionários sobre o que procurar e evitar em relação a phishing e outros conteúdos maliciosos pode ser eficaz para reduzir o número de incidentes de malware enfrentados pela empresa.

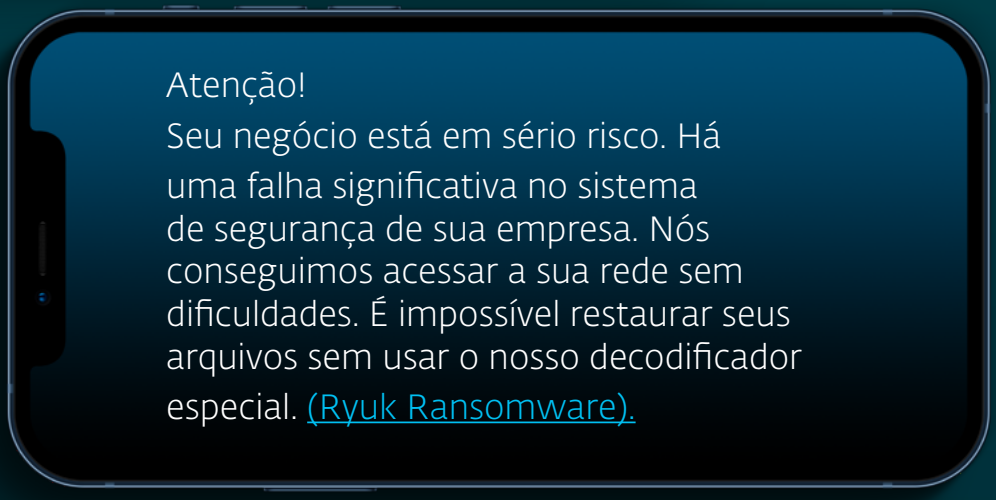
eset Digital Security Progress. Protected.

FUNCIONAMENTO PSICOLÓGICO

Exemplos de notas de resgate







eset Digital Security Progress. Protected.

RANSOMWARES VS. INFRAESTRUTURA DE TI

PROTOCOLO DE DESKTOP REMOTO

Para o acesso remoto de funcionários aos sistemas da sua empresa, é fundamental ter o RDP habilitado. É necessário estabelecer um acesso mais restritivo , tanto para funcionários quanto para administradores acessarem a plataforma por meio da autenticação multifator (MFA). Após a autenticação, os funcionários podem se conectar com segurança a esses sistemas.

caixa de informações

De que formas as organizações podem usar o RDP?

1) Para gerenciar programas em execução em um servidor, como um site ou banco de dados de back-end.

2)Para permitir o acesso remoto a desktops corporativos ou máquinas virtuais que têm acesso a recursos não disponíveis fora da rede corporativa. O acesso a esses sistemas via RDP elimina a necessidade de expor servidores internos sensíveis à internet de forma direta.

PROTEÇÃO EQUILIBRADA IDEAL PARA AS EMPRESAS

ESET PROTECT Advanced

Proteja seus endpoints contra ransomwares e ameaças de dia zero com um console baseado na nuvem, fácil de usar..

SAIBA MAIS

RANSOMWARES VS. INFRAESTRUTURA DE TI

Porque que a descoberta de sistemas externos e o seu uso indevido é tão fácil?

- Sistemas RDP vulneráveis são fáceis de encontrar (por exemplo, por meio de mecanismos de busca especializados como o Shodan);
- Agentes invasores conseguem acesso em sistemas RDP mal configurados de forma muito fácil;
- As ferramentas e técnicas para escalação de privilégios e obtenção de direitos de administrador em sistemas RDP comprometidos são amplamente conhecidas e disponíveis.

71 bilhões

Número de detecções em que o RDP apareceu como vetor de ataque, entre janeiro de 2020 e junho de 2021, segundo a telemetria da ESET..

Número total de resultados para a porta padrão 3389 do RDP aberta no mecanismo de pesquisa Shodan.io.

Mais de 4 milhões

eset Digital Security Progress. Protected.

RANSOMWARES VS. INFRAESTRUTURA DE TI

Infográfico

Tendência de detecção de ataques de força bruta ao RDP, média de 7 dias.

Embora o aumento mais expressivo tenha sido registrado no primeiro semestre de 2020, o ano de 2021 apresentou os números mais elevados até agora. Ao comparar o primeiro semestre de 2020 ao mesmo período de 2021, a ESET observou um crescimento seis vezes maior nas detecções de ataques de força bruta ao RDP. Além disso, ataques via RDP podem passar despercebidos por diversos métodos de detecção, resultando em menos métricas e, portanto, uma menor percepção das ameaças.

.

eset Digital Security Progress. Protected.

RANSOMWARES VS. INFRAESTRUTURA DE TI

COMO PROTEGER SUA EMPRESA CONTRA ATAQUES DE RANSOMWARES AO RDP

- Estabeleça políticas para a segurança de acesso remoto. É possível exigir que todo acesso RDP seja roteado por uma VPN (rede virtual privada), protegida por MFA (autenticação multifator), ou limitado a funções específicas, em sistemas específicos configurados com segurança, com a aplicação constante de patches de correções, monitoramento constante, firewall apropriado e backups regulares.
- Certifique-se do cumprimento das regras pela equipe, além da sua preparação para lidar com um ataque bem-sucedido, apesar das regras.
- Faça um inventário de seus ativos voltados para a internet. Nossas pesquisas apontam que o seguinte cenário não é tão incomum: uma organização é atacada por meio de um ativo conectado à internet, sobre o qual a equipe de segurança não tinha conhecimento até depois do ataque.
- Não permita que um contratante ou funcionário conecte um servidor físico ou virtual à rede da organização e à internet, a menos que esse servidor esteja configurado de forma segura. A configuração deve ocorrer antes de o servidor entrar em operação, principalmente caso o servidor esteja executando RDP com uma conta de administrador de domínio.
- Faça um levantamento dos ativos voltados para a internet que têm acesso remoto habilitado e avalie se esse acesso é necessário. Caso o acesso seja realmente necessário, exija senhas longas para as contas habilitadas e avalie a possibilidade de limitar esses sistemas à rede interna, permitindo o acesso remoto por meio de uma VPN corporativa.
- Caso seja necessário acessar um sistema a partir da internet pública via RDP, e uma VPN não for viável, implemente autenticação multifatorial (MFA), para não depender apenas de senhas. Certifique-se, porém, de usar uma solução de MFA que não seja baseada em SMS. Agentes do cibercrime têm diversas formas de contornar a autenticação baseada em SMS. Caso dependa apenas de senhas, estabeleça um limite de três tentativas de login inválidas, bloqueando as tentativas seguintes por um período determinado, por exemplo, três minutos.
- Reforce e aplique correções a todos os dispositivos com acesso remoto. Além de garantir a identificação e correção de todas as vulnerabilidades de segurança, certifique-se de que todos os serviços e componentes não essenciais tenham sido removidos ou desativados e que as configurações estejam definidas para a maior segurança.

eset Digital Security Progress. Protected.

RANSOMWARES VS. INFRAESTRUTURA DE TI

E-MAIL

Alguns criminosos ainda utilizam anexos de e-mail para instalar malwares que servem como estágio inicial de comprometimento, que acabam culminando em ransomwares.

Esse vetor pode ser utilizado para disseminar downloaders que instalam malware no dispositivo do destinatário do e-mail, ou para estabelecer uma posição em um dispositivo conectado à rede dentro de uma organização. Essa posição pode servir como base para tentativas de roubo de dados valiosos e criptografia de arquivos em toda a organização, antes mesmo de exigirem um resgate alto, como é frequente em casos de ataques de ransomwares direcionados via RDP.

O e-mail também é um dos principais vetores para botnets, como Trickbot, Qbot e Dridex, que costumam utilizar documentos do Microsoft Office com macros maliciosas para a o acesso inicial e ransomwares como payload final.

Certifique-se de que as equipes entendam o dever de relatar mensagens e anexos suspeitos à equipe de suporte ou segurança de forma imediata. O alerta precoce pode auxiliar a organização a ajustar seus filtros de spam e conteúdo e reforçar seus firewalls e demais defesas..

exemplo

De um e-mail à uma porta eletrônica inutilizável em um hotel

A criptografia dos dados de seus dispositivos não é o único risco quando falamos de ransomwares.
Um diretor executivo de um hotel quatro estrelas nos Alpes da Áustria recebeu um e-mail de ransomwares, disfarçado como uma fatura da Telekom Austria. Após clicar em um link do e-mail, as portas eletrônicas do hotel ficaram inutilizáveis, não sendo possível emitir novas chaves de cartão para os hóspedes. Para retornar às operações, ele decidiu pagar um resgate de dois Bitcoins.

Depois, o hotel foi hackeado mais três vezes, comprovando que, ao pagar o resgate, você está mostrando aos criminosos sua disposição para pagar e, portanto, aumentando as chances de novos ataques.

Source: BBC

eset Digital Security Progress. Protected.

RANSOMWARES VS. INFRAESTRUTURA DE TI

CADEIA DE SUPRIMENTOS

Uma cadeia de suprimentos é uma rede de conexões entre uma empresa e seus fornecedores para produzir e distribuir um produto ou serviço específico. Um ataque à cadeia de suprimentos em qualquer um desses pontos terá consequências em toda a sua extensão.

Quando os ataques à cadeia de suprimentos ocorrem por meio digital em vez de físico, os efeitos são igualmente prejudiciais. Ao violar apenas um dos participantes da cadeia de suprimentos, é possível que agentes mal-intencionados obtenham acesso irrestrito e de difícil detecção a grande parte dos parceiros comerciais e da base de clientes.

exemplo

O que pode acontecer em caso de ataque à cadeia de suprimentos?

Em 2017, a ESET descobriu o uso de um software de contabilidade legítimo pelo cibercrime para propagar o malware NotPetya/DiskCoder.C. Agentes invasores conseguiram se infiltrar nos servidores de atualização da empresa de software, introduzindo seu próprio código aos arquivos legítimos de atualização do aplicativo. Quando os usuários do software de contabilidade clicavam para instalar as atualizações do programa, também estavam instalando um malware backdoor, dando início ao que se tornou o ciberataque mais destrutivo da história.

Fonte: WeLiveSecurity.

A crescente intensidade dos ataques à cadeia de suprimentos também é evidenciada pelo número de artigos de pesquisa publicados pela ESET em que esse vetor de ataque foi utilizado. Entre novembro de 2020 e fevereiro de 2021, quatro casos de ataques à cadeia de suprimentos foram identificados de forma exclusiva pela ESET, um número bastante alto em comparação aos anos anteriores.

A defesa contra esse tipo de ataque envolve acompanhar atualizações e correções de software, utilizar software de proteção de endpoints, aproveitando também as soluções EDR e instruir os usuários sobre e-mails não solicitados que os incentivam a acessar sites desconhecidos.

eset Digital Security Progress. Protected.

RANSOMWARES VS. INFRAESTRUTURA DE TI

OUTRAS VULNERABILIDADES

Os cibercriminosos podem se beneficiar tanto de vulnerabilidades conhecidas e como desconhecidas, mas a exploração de vulnerabilidades de dia zero costuma ser realizada especificamente por grupos de APT e agentes patrocinados pelo Estado. Ainda assim, o uso malicioso dessas vulnerabilidades segue sendo uma grande preocupação para administradores de segurança e proprietários de empresas.

A maior parte dos fornecedores de cibersegurança ainda detecta atividades relacionadas à ameaça EternalBlue (2017) e suas diversas variantes, bem como explorações contínuas com base no protocolo de compartilhamento de arquivos SMBv1 da Microsoft. A persistência de vulnerabilidades e ameaças como WannaCryptor (também conhecido como WannaCry) costuma estar relacionada à falta de atualizações e gerenciamento de patches adequados em empresas e instituições.

Por fim, as VPNs também exigem proatividade por parte dos administradores de TI, que devem atualizar os produtos de cibersegurança conforme necessário. Essa ênfase em atualizações adequadas deve ser complementada com uso de autenticação multifator para logins no serviço de VPN. Em casos de suspeita de uso indevido de credenciais, a organização deve efetuar redefinições abrangentes das contas.
.

exemplo

Exploração de vulnerabilidades no Microsoft Exchange Server

Em março de 2021, a Microsoft lançou atualizações de emergência para resolver quatro falhas de dia zero afetando as versões 2013, 2016 e 2019 do Microsoft Exchange Server. Os agentes de ameaças foram observados explorando as vulnerabilidades em ambientes reais, para acessar servidores Exchange locais, resultando no roubo de e-mails, download de dados e comprometimento de dispositivos com malware para acesso de longo prazo às redes das vítimas.

Fonte: WeLiveSecurity.

eset Digital Security Progress. Protected.

ESTRATÉGIAS DE DEFESA CONTRA RANSOMWARES

USO DA NUVEM E SEGMENTAÇÃO DE REDE

Seja qual for o vetor de ataque empregado, caso ransomwares consigam entrar na sua organização, é provável que tentem se espalhar para o maior número possível de dispositivos, causando impactos a todas as operações da sua empresa.

Limitar a quantidade de dispositivo acessíveis em uma invasão desencadeada a partir de um único ponto de entrada traz benefícios significativos como estratégia de defesa. Existem diferentes abordagens para implementar essa estratégia, com destaque para a segmentação de rede.

Nos últimos anos, uma estratégia popular de arquitetura de sistemas tem sido a migração de dados para a nuvem. Entretanto, a nuvem não oferece proteção automática contra os ataques de ransomwares. Na verdade, o baixo custo e a relativa facilidade com que novos servidores podem ser provisionados na nuvem e conectados ao restante da infraestrutura digital da organização tornaram a nuvem um ambiente propício para ataques do cibercrime. Assim, fica evidente que o uso da nuvem por qualquer parte da organização precisa ser devidamente autorizado e configurado com segurança. Além disso, como todos os outros sistemas, aqueles na nuvem também devem estar cobertos por um plano adequado de backup e recuperação.

eset Digital Security Progress. Protected.

RANSOMWARE DEFENSE STRATEGIES

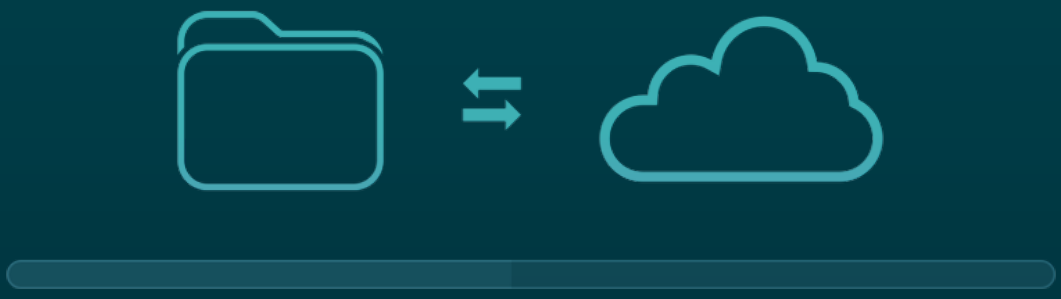
CORREÇÕES E BACKUP

Correções e backups são dois pontos fundamentais da operação e administração de sistemas na defesa contra ataques de ransomwares.

Ao corrigir os sistemas, possíveis vias de ataque são bloqueadas, prevenindo a entrada de ransomwares na sua organização ou, caso entre, os potenciais danos podem ser reduzidos. Já um programa de backup e recuperação bem gerenciado é um mecanismo de defesa crucial para seus esforços de recuperação em casos de invasão por ransomwares.

Esse aspecto, porém, pode ser mais complexo do que parece. Por quê? As atualizações e correções devem passar por testes antes da sua implementação. Alguns sistemas da sua organização podem ter dependências de software que são afetadas por atualizações para versões mais recente de um aplicativo ou sistema operacional.

Correções e backups devem, sim, ser considerados. Porém, é importante lembrar que alguns ataques de ransomwares são executados ao longo de um período prolongado, durante o qual podem ser incluídos junto a arquivos legítimos na rotina de backup, comprometendo a possibilidade de uma recuperação sem entraves. Por isso, o backup não é uma estratégia de segurança definitiva – deve ser monitorado e gerenciado, e o processo de recuperação deve ser testado frequentemente.



eset Digital Security Progress. Protected.

ESTRATÉGIAS DE DEFESA CONTRA RANSOMWARES

Atualmente, existe uma grande variedade de opções de backups e recuperação, com destaque para o armazenamento em nuvem, seja remoto, local ou híbrido. No entanto, também há um maior número de dados e locais de origem. Sem uma estratégia de backup abrangente, há um risco constante de os propagadores de ransomwares encontrarem aquele dispositivo que não foi incluído no backup.

Segundo especialistas em backup da Xopero, membro da ESET Technology Alliance, um backup abrangente deve incluir dados e estado do sistema em todos os endpoints, servidores, caixas de e-mail, unidades de rede, dispositivos móveis e máquinas virtuais. Há, porém, algumas ressalvas especificas para o caso dos ransomwares.

Por exemplo, armazenamentos que estão constantemente ativos podem estar vulneráveis a ataques de ransomwares, da mesma forma que o armazenamento local e outros conectados à rede.

caixa de informações

Como evitar a propagação de ransomwares

Opte por um armazenamento externo que:

- Não fique permanentemente ativo;.
- Proteja os dados de backup contra modificações ou substituições automáticas e silenciosas por malware quando a instalação remota estiver ativa;
- Proteja as versões anteriores dos dados de backup contra comprometimentos, garantindo que seja possível recuperar alguns dados (inclusive versões anteriores dos dados atuais) mesmo em casos de fatalidades nos backups mais recentes.
- Proteja o cliente ao exibir iformaçõe sosbre as responsabilidades legais/contratuais do provedor, o que acontece se o provedor sair do negócio, entre outros aspectos.

Não subestime a utilidade de mídias de gravação única para o arquivamento de dados. Os arquivos armazenados em mídias que não são regraváveis estão imunes aos ataques de ransomwares..

eset Digital Security Progress. Protected.

RESPONDENDO A ATAQUES DE RANSOMWARES

Mesmo estando ciente dos riscos oferecidos por ransomwares e tendo implementado todas as medidas preventivas possíveis, sua organização ainda precisa estar preparada para responder a um ataque de ransomwares que consiga ultrapassar suas defesas.
Aqui, oferecemos um panorama prático que pode auxiliar no seu planejamento de resposta a ataques de ransomwares.

caixa de informações

A sua equipe entende as políticas?

Questões para abordagem em uma empresa:

- A quem as equipes devem relatar suspeitas de ransomwares?
- Qual é a política da empresa em relação ao pagamento de resgates em ataques de ransomwares?
- Que medidas a organização é obrigada a tomar em casos de violação de dados?
- Quem está autorizado a pagar/negociar pagamentos de resgate?
- Qual é a política da empresa em relação ao desligamento de dispositivos afetados?
- Quem toma essas decisões? O desligamento dos dispositivos elimina possíveis evidências armazenadas na memória e pode ser considerado fora de conformidade com as regulamentações.

Problemas a evitar:

- Funcionários que não relatam suspeitas de ransomwares por medo de represálias;.
- Administradores de rede que pagam resgates por ser mais "fácil" do que recuperar sistemas a partir de backups;
- Divulgação não autorizada de informações sobre suspeitas ou ataques de ransomwares.

eset Digital Security Progress. Protected.

RESPONDENDO A ATAQUES DE RANSOMWARES

PLANO DE RECUPERAÇÃO

É uma recomendável incluir ao menos um cenário de ransomwares no seu manual de planejamento de crises e conduzir um exercício de simulação com a equipe pertinente, incluindo executivos.

Dessa forma, é possível identificar lacunas nos planos de backup e recuperação e prever melhor o impacto de não conseguir acessar serviços básicos devido à criptografia de sistemas, como e-mail, telefones VoIP e acesso à internet.

Exemplo de um plano eficaz de recuperação e resposta a incidentes:

1) Ao identificar os primeiros sinais de ataque, notifique o pessoal designado;
2) Isole e analise as máquinas afetadas;
3) Caso o isolamento dos dispositivos afetados não seja possível, faça uma captura de imagem e memória do sistema e, em seguida, desligue-os para evitar a propagação do ataque de ransomwares;
4) Uma vez confirmado o ataque, ative sua equipe de resposta a incidentes/crises;
5) Alerte o conselho jurídico;
6) Entre em contato com fornecedores que possam oferecer assistência;
7) Reforce com a equipe as políticas de imprensa e redes sociais da empresa para manter o controle das comunicações voltadas ao público;
8) Avalie o escopo do ataque e os detalhes dos ransomwares (por exemplo, determinar se há uma chave de descriptografia publicamente disponível);
9) Entre em contato com as autoridades policiais;
10) Prepare um comunicado de imprensa;
11) Caso os arquivos tenham sido criptografados, avalie a viabilidade de restauração a partir do backup;
12) Mantenha as equipes atualizadas sobre o status;

eset Digital Security Progress. Protected.

RESPONDENDO A ATAQUES DE RANSOMWARES

13) Caso seja necessário, ative o seu plano de continuidade de negócios;

14) Administradores de TI devem coletar logs relevantes e possíveis indicadores de comprometimento, como binários, notas de pedido de resgate, endereços IP, entradas de registro ou outros arquivos;

15) Documente a investigação inicial do ataque e as medidas tomadas para a remediação.

POR QUE NÃO PAGAR O RESGATE

Pagar o resgate aos criminosos que criptografaram seus arquivos não garante que você receberá a chave de descriptografia. Existem diversas razões pelas quais o pagamento pode não significar a recuperação dos seus arquivos

1) Alguns dos dados podem ter sido corrompidos no processo de criptografia e, portanto, não são recuperáveis;

2) A ferramenta de descriptografia fornecida pode conter outros malwares, não funcionar corretamente ou ser muito mais lenta do que a recuperação por meio de backups;

3) O processo de entrega da chave de descriptografia pode falhar;.

4) É possível que o invasor esteja agindo de forma desonesta e não tenha a intenção de fornecer as chaves de descriptografia;

5) Pagar o resgate pode ser ilegal. Por exemplo, em outubro de 2020, o Escritório de Controle de Ativos Estrangeiros (OFAC) do Departamento do Tesouro dos Estados Unidos declarou ser ilegal facilitar o pagamento a indivíduos, organizações, regimes e, em alguns casos, países inteiros que estão na lista de sanções.

Além disso, existem razões éticas para não pagar o resgate exigido. Porque, ao pagar, você...

... valida o modelo de negócios que sustenta o crime.
... incentiva novas atividades criminosas.
... possibilita que grupos de RANSOMWARES pesquisem vulnerabilidades de dia zero e desenvolvam novas ameaças.
... pode ser alvo de futuros ataques e novas exigências de dinheiro.

eset Digital Security Progress. Protected.

caixa de informações

Argumentos mais comuns para pagar o resgate:

"É mais barato do que restaurar a partir de backups."

Embora essa afirmação possa estar tecnicamente correta, em termos de tempo e custos de mão de obra, a decisão de pagar ainda é fundamentalmente falha pelos motivos mencionados anteriormente. Além disso, remover ransomwares ativos com software de segurança não é o mesmo que recuperar dados. Remover ransomwares e então decidir realizar o pagamento significa que os dados podem não ser mais recuperáveis, mesmo com a cooperação dos criminosos, pois o mecanismo de descriptografia geralmente está junto do malware.

"Não é possível restaurar as informações criptografadas a partir dos backups."

Essa limitação pode ocorrer pela inexistência de backups ou no caso de backups incompletos ou danificados. No entanto, existem alternativas viáveis. Primeiro, verifique com o fornecedor do seu software de segurança sobre a disponibilidade de uma ferramenta de descriptografia, que possibilite a recuperação dos dados e que elimine a necessidade de pagar o resgate.

eset Digital Security Progress. Protected.

RANSOMWARES: CENÁRIOS FUTUROS

Os ransomwares se beneficiam da dependência das organizações em relação à tecnologia. Assim, a menos que ocorram mudanças inesperadas na política global e na economia, a perspectiva é que os ransomwares sigam existindo e evoluindo no futuro.

Com base na nossa experiência com códigos maliciosos desde o final da década de 1980, podemos afirmar que as ameaças de malware tendem a evoluir da seguinte forma:

- Descobrem-se vulnerabilidades em uma nova tecnologia/ software, e seu potencial para uso criminoso é abordado;
- As tentativas de uso malicioso de tecnologias mais recentes são raras em um primeiro momento, pois os criminosos estão lucrando facilmente com estratégias já estabelecidas;
- Iniciam-se os esforços para a remediação e mitigação dessas vulnerabilidades;.
- Na ausência de uso criminoso generalizado, os esforços de remediação e mitigação perdem força;
- Por fim, agentes do cibercrime menos habilidosos descobrem que essa "nova" tecnologia está pronta para ser explorada.

Esses cenários de ransomwares em evolução têm múltiplas implicações para as pequenas e médias empresas. É preciso começar a abordar essas potenciais ameaças dentro da sua própria estratégia e planejamento de gerenciamento de riscos.

Comece a controlar os ativos vulneráveis a ransomwares agora mesmo: dispositivos IoT, roteadores SOHO, robôs, sistemas de controle e sistemas autônomos. Acompanhe os relatórios de vulnerabilidades relacionadas a esses ativos e também as atualizações de correções e firmware disponíveis para esses dispositivos.Além disso, segmente dispositivos IoT e outras novas tecnologias das redes de produção.

Devido à maior eficácia das técnicas de extorsão e aos novos canais de distribuição de ransomwares, estima-se que centenas de milhões de dólares tenham entrado nas contas desses cibercriminosos tecnicamente qualificados, permitindo o desenvolvimento de um modelo de negócios de ransomwares como serviço (RaaS) e a integração de diversos novos afiliados (criminosos com menos habilidades e experiência). Além disso, presume-se que alguns grupos de cibercriminosos tenham começado a adquirir vulnerabilidades de dia zero e estejam comprando credenciais roubadas, ampliando ainda mais o número de potenciais vítimas.
.

eset Digital Security Progress. Protected.

CONCLUSÃO

Com recursos, ambição e foco, principalmente por parte dos grupos de ransomwares, aprender com as histórias e análises alarmantes relatadas diariamente na mídia se tornou obrigatório para qualquer administrador de TI, profissional de segurança e líder empresarial. Tem sido demonstrado repetidas vezes que a aplicação de políticas, configurações adequadas e senhas fortes, combinadas com autenticação multifator, podem ser elementos decisivos na proteção contra ransomwares.

Para combater vulnerabilidades de dia zero, botnets, malspam e outras técnicas mais avançadas, são necessárias tecnologias de segurança adicionais. Essas tecnologias começam com uma solução de proteção de endpoint multicamadas, capaz de detectar e bloquear ameaças recebidas por e-mails, por meio de links da web, RDP e outros protocolos de rede. Além disso, devem-se utilizar ferramentas de detecção e resposta de endpoints para monitorar, identificar e isolar anomalias e sinais de atividade maliciosa no ambiente de uma organização.

Proteja seus endpoints contra ransomwares com as soluções da ESET. Para mais informações, acesse o nosso site https://www.eset.com/br/.

eset Digital Security Progress. Protected.

SOBRE A ESET

Há mais de 30 anos, a ESET® vem desenvolvendo softwares e serviços de cibersegurança líderes do setor, protegendo empresas, infraestruturas críticas e consumidores do mundo todo contra ameaças digitais cada vez mais sofisticadas. Desde a segurança de endpoints e dispositivos móveis até a detecção e resposta de endpoints, passando pela criptografia e autenticação multifator, as soluções de alto desempenho e uso descomplicado da ESET garantem a proteção e o monitoramento discretos em tempo integral, com a atualização das defesas em tempo real para manter a segurança dos usuários e o funcionamento das operações empresariais sem interrupções. As ameaças em constante evolução demandam uma empresa de cibersegurança também em constante evolução, possibilitando o uso seguro da tecnologia. Contamos com o apoio dos centros de P&D da ESET em todo o mundo, trabalhando a serviço do nosso futuro compartilhado. Para mais informações, acesse https://www.eset.com/br/ ou nos siga no LinkedIn, Facebook e YouTube.

© 1992 - 2022 ESET, spol. s r.o. - All rights reserved.
Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.

Digital Security
Progress. Protected.