

ESET Glossary

Guia do Usuário

[Clique aqui para exibir a versão da Ajuda deste documento](#)

Direitos autorais ©2023 por ESET, spol. s r.o.

ESET Glossary foi desenvolvido por ESET, spol. s r.o.

Para obter mais informações, visite <https://www.eset.com>.

Todos os direitos reservados. Nenhuma parte desta documentação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravação, digitalização, ou de outra forma sem a permissão por escrito do autor.

A ESET, spol. s r.o. reserva-se o direito de alterar qualquer software aplicativo descrito sem prévio aviso.

Suporte técnico: <https://support.eset.com>

REV. 19-04-2023

1 Introdução ao Glossário ESET	1
1.1 Adware	1
1.2 Botnet	1
1.3 Falso positivo (FP)	2
1.4 Compactador	2
1.5 Aplicativo potencialmente não seguro	2
1.6 Aplicativos potencialmente indesejados	2
1.7 Ransomware	7
1.8 Rootkit	7
1.9 Programação orientada para retorno	8
1.10 Spyware	8
1.11 Trojan	8
1.12 Vírus	9
1.13 Worm	9
1.14 Recheamento de credencial	10
1.15 Envenenamento de DNS	10
1.16 Ataque DoS	10
1.17 Ataque ICMP	10
1.18 Rastreamento de portas	11
1.19 SMB Relay	11
1.20 Dessincronização TCP	11
1.21 Ataque de worm	12
1.22 Envenenamento de Cache ARP	12
2 Ameaças por email	12
2.1 Propagandas	13
2.2 Hoaxes	13
2.3 Roubo de identidade	14
2.4 Reconhecimento de fraudes em spam	14
2.4 Regras	14
2.4 Lista de permissões	15
2.4 Lista de proibições	15
2.4 Exceção	16
2.4 Controle pelo servidor	16
2.5 Rastreamento de memória avançado	16
2.6 Proteção para bancos & pagamentos	16
2.7 Proteção contra botnet	17
2.8 Detecções de DNA	17
2.9 ESET LiveGrid®	18
2.10 Bloqueio de Exploit	18
2.11 Bloqueio de Exploit do Java	19
2.12 ESET LiveSense	19
2.13 Aprendizado de máquina	19
2.14 Proteção contra ataque de rede	20
2.15 Escudo Anti-ransomware	20
2.16 Proteção contra ataques baseados em script	20
2.17 Navegador protegido	21
2.18 Escaner UEFI	21
2.19 Arquivo canário	22
2.20 Bloqueio	22

Introdução ao Glossário ESET

O Glossário ESET oferece uma visão geral abrangente das ameaças atuais e das tecnologias ESET que trabalham para sua proteção.

Os tópicos são divididos nos capítulos a seguir, que descrevem:

- [Detecções](#) – Incluem vírus de computador, worm, trojan, Aplicativo potencialmente indesejado, etc.
- [Ataques remotos](#) – Ameaças que ocorrem através de uma rede local ou da Internet
- [Ameaças por e-mail](#) – incluem hoaxes, phishing, scam, etc.
- [Tecnologias ESET](#) – recursos de produto disponíveis nas soluções de segurança da ESET

Adware

Adware é abreviação de “advertising-supported software” (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a página inicial do mesmo. O adware é frequentemente vinculado a programas freeware, permitindo que seus criadores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso - os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware, ou, se forem, as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, aconselhamos removê-lo, uma vez que há grande possibilidade de que ele contenha códigos maliciosos.

Botnet

Um bot, ou um robô da web, é um programa de malware automatizado que rastreia blocos de endereços de rede e infecta computadores vulneráveis. Isso permite que hackers tomem o controle de vários computadores ao mesmo tempo e transformem esses computadores em bots (também conhecido como um zumbi). Normalmente os hackers usam bots para infectar um grande número de computadores, que formam uma rede ou um botnet. Quando um botnet está no seu computador, ele pode ser usado em ataques distribuídos de negação de serviço (DDoS), proxy e também podem ser usados para realizar tarefas automáticas na Internet sem o seu conhecimento (por exemplo: enviar spam, vírus ou roubar informações pessoais e particulares, como credenciais bancárias ou números de cartão de crédito).

Falso positivo (FP)

Realisticamente, não há garantia de uma taxa de detecção de 100% nem uma chance de 0% de evitar a categorização incorreta de objetos limpos como detecções.

Um falso positivo é um arquivo/aplicativo limpo que é classificado erroneamente como malware ou PUA.

Compactador

Empacotador é um executável de extração automática do tempo de execução que realiza vários tipos de malware em um único pacote.

Os empacotadores mais comuns são UPX, PE_Compact, PKLite e ASPack. O mesmo malware pode ser detectado de forma diferente quando compactado usando outro empacotador. Empacotadores também têm a capacidade de tornar suas "assinaturas" mutáveis ao longo do tempo, tornando o malware mais difícil de ser detectado e removido.

Aplicativo potencialmente não seguro

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. A ESET fornece a opção de detectar tais aplicativos.

Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

Aplicativos potencialmente indesejados

Grayware ou Aplicativo potencialmente indesejado (PUA) é uma categoria ampla de software, cujo objetivo não é tão claramente nocivo quanto outros tipos de malware, como vírus ou cavalos de Troia. Porém ele pode instalar software indesejado adicional, alterar o comportamento do dispositivo digital ou realizar atividades não aprovadas ou esperadas pelo usuário.

Categorias que podem ser consideradas grayware incluem: software de exibição de propagandas, empacotadores de download, barras de ferramentas de vários navegadores, software com comportamento enganoso, bundleware, trackware, proxuware (aplicativos de compartilhamento de internet), mineradores de criptomoedas, limpadores de registro (apenas nos sistemas operacionais Windows) ou qualquer outro software limítrofe, ou software que use práticas comerciais ilícitas ou no mínimo antiéticas (mesmo se parecer legítimo) e que pode ser considerado indesejável por um usuário final que se tornou ciente do que o software poderia fazer se a instalação fosse permitida.

Um [Aplicativo potencialmente inseguro](#) é um aplicativo que é um software legítimo (possivelmente comercial) por si só mas que também pode ser usado por um agressor. A detecção desses tipos de aplicativos pode ser ativada ou desativada por usuários do software ESET.

Existem algumas situações em um usuário pode sentir que os benefícios do aplicativo potencialmente indesejado superam os riscos. Por isso, a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso, como cavalos de Troia ou worms.

- [Alerta - Aplicativo potencialmente indesejado detectado](#)
- [Configurações](#)
- [Wrapper de software](#)
- [Limpadores de registro](#)
- [Conteúdo potencialmente indesejado](#)

Instruções ilustradas

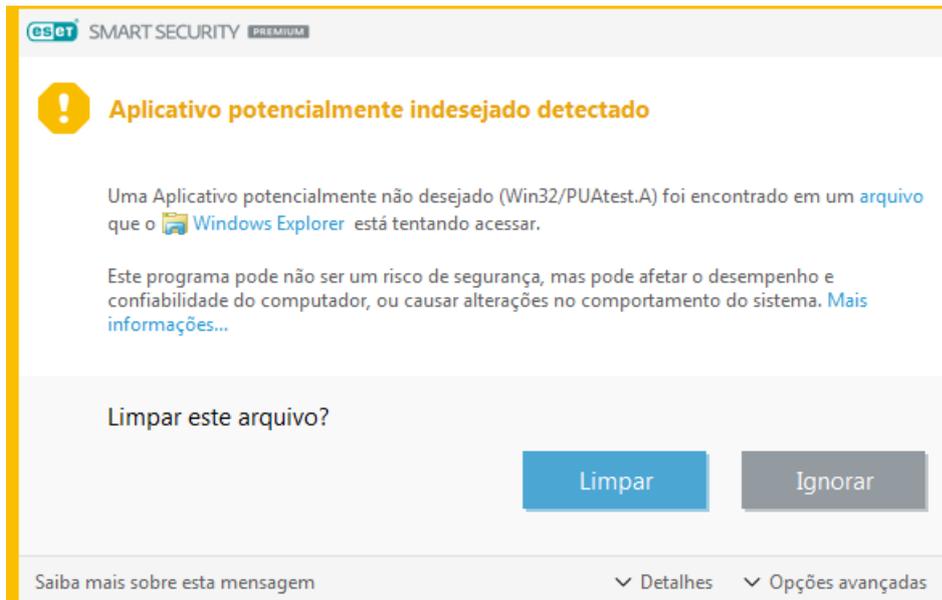


Para escanear e remover Aplicativos potencialmente indesejados (PUAs) nos produtos ESET Windows domésticos, consulte nosso [artigo da base de conhecimento ESET](#).

Alerta - Aplicativo potencialmente indesejado detectado

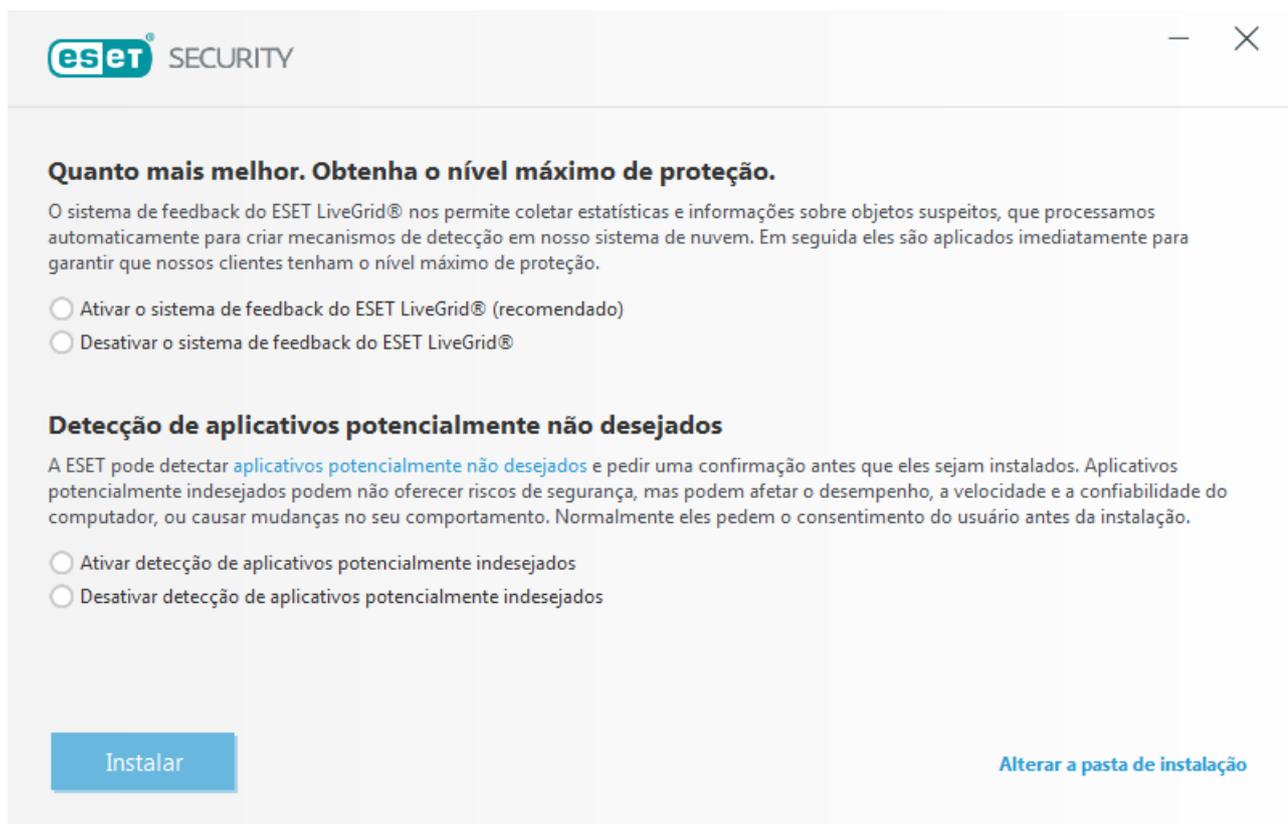
Quando um aplicativo potencialmente indesejado é detectado, você pode decidir qual ação realizar:

- 1.Limpar/Desconectar:** Esta opção encerra a ação e evita que uma PUA entre no sistema. Você verá a opção **Desconectar** para notificações de PUA durante o download de um site da web e a opção **Limpar** para notificações para um arquivo no disco.
- 2.Ignorear:** Essa opção permite que a PUA entre em seu sistema.
- 3.Excluir da detecção:** Para permitir que o arquivo detectado que já está no seu computador seja executado no futuro sem interrupções, clique em **Opções avançadas** e selecione a caixa de seleção ao lado de Excluir da detecção e clique em **Ignorear**.
- 4.Excluir assinatura da detecção:** Para permitir que todos os arquivos identificados por um nome de detecção (assinatura) específico sejam executados no seu computador no futuro sem interrupção (de arquivos existentes ou de um download da web), clique em **Opções avançadas**, selecione a caixa de seleção ao lado de **Excluir assinatura da detecção** e clique em **Ignorear**. Se janelas de detecção adicionais com um nome de detecção idêntico forem exibidas imediatamente depois, clique em Ignorear para fechá-las (quaisquer janelas adicionais são relacionadas a uma detecção que ocorreu antes de você ter excluído a assinatura da detecção).



Configurações

Ao instalar seu produto ESET, é possível decidir se vai ativar a detecção de aplicativos potencialmente não desejados, conforme exibido abaixo:



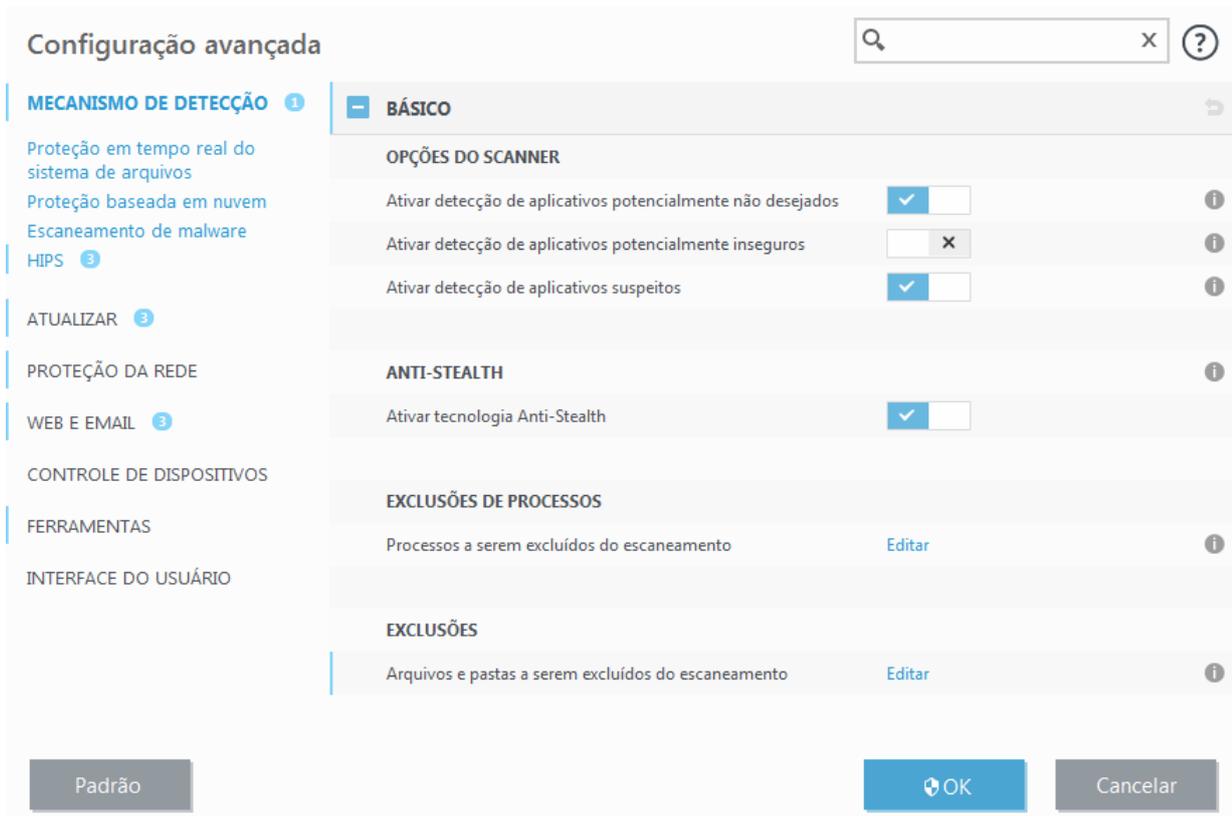
Aviso

- ⚠ Aplicativos potencialmente indesejados podem instalar adware, barras de ferramentas ou ter outros recursos de programa indesejados e inseguros.

Essas configurações podem ser modificadas nas suas configurações de programa a qualquer momento. Para

ativar ou desativar a detecção de Aplicativos potencialmente indesejados, inseguros ou suspeitos, siga essas instruções:

1. [Abra seu produto ESET.](#)
2. Pressione a tecla **F5** para acessar a **Configuração avançada**.
3. Clique em **Mecanismo de detecção** (em versões anteriores, também conhecido como **Antivírus** ou **Computador**) e ative ou desative as opções **Ativar detecção de aplicativos potencialmente não desejados**, **Ativar detecção de aplicativos potencialmente inseguros** e **Ativar detecção de aplicativos suspeitos** de acordo com suas preferências. Confirme clicando em **OK**.



Instruções ilustradas

Para instruções mais detalhadas sobre como configurar produtos para detectarem ou ignorarem PUAs, visite os artigos da Base de conhecimento da ESET:

- ✓ [ESET NOD32 Antivirus / ESET Internet Security / ESET Smart Security Premium](#)
- [ESET Cyber Security para macOS / ESET Cyber Security Pro para macOS](#)
- [ESET Endpoint Security / ESET Endpoint Antivirus for Windows](#)
- [ESET Mobile Security para Android](#)

Wrapper de software

Um wrapper de software é um tipo especial de modificação de aplicativo que é usado por alguns sites de hospedagem de arquivos. É uma ferramenta de terceiros que instala o programa que você planejou baixar, mas adiciona outros software, como barras de ferramentas ou [adware](#). O software adicional também pode fazer alterações na página inicial do seu navegador ou nas configurações de pesquisa. Além disso, sites de hospedagem

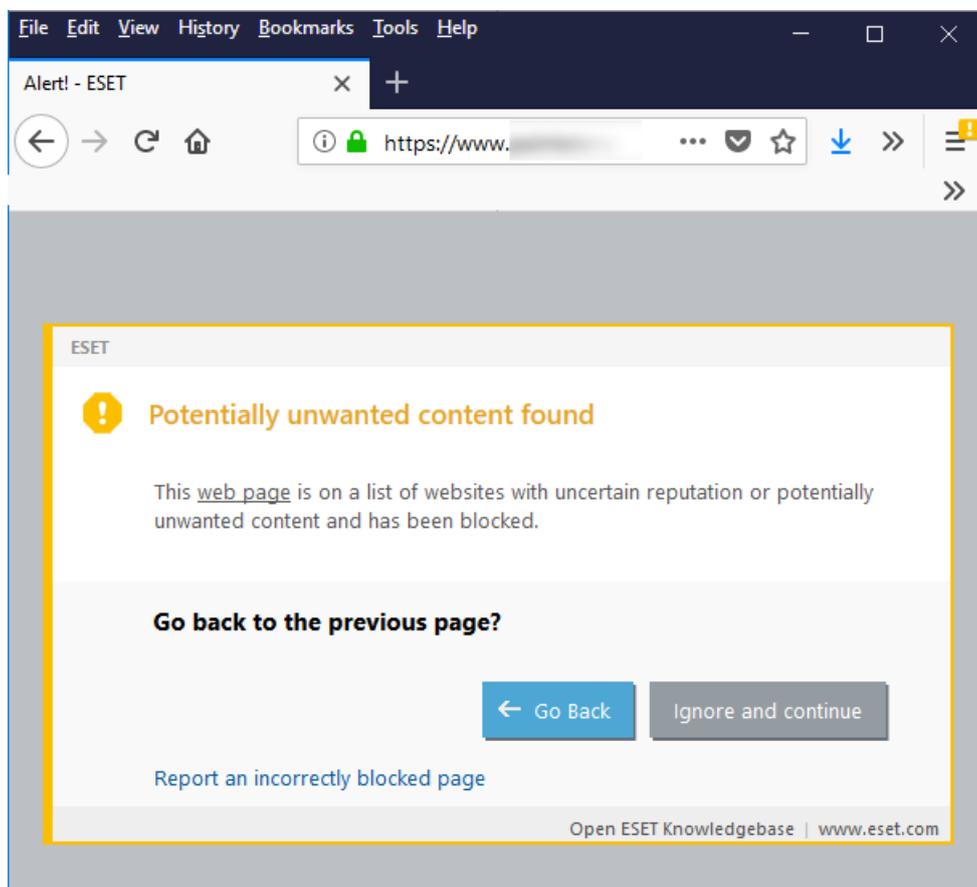
de arquivos muitas vezes não notificam o fabricante do software ou receptor do download que modificações foram feitas e muitas vezes oculta as opções de não realizar tais modificações. Por esses motivos, a ESET classifica o wrapper de software como um tipo de aplicativo potencialmente indesejado para permitir aos usuários aceitarem ou não seu download.

Limpadores de registro

Limpadores de registro são programas que podem sugerir que o banco de dados de registro do Windows precisa de manutenção regular ou limpeza. Usar um limpador de registro pode introduzir alguns riscos ao seu sistema de computador. Além disso, alguns limpadores de registro fazem declarações não qualificadas, que não podem ser verificadas ou em geral incompatíveis sobre seus benefícios e/ou geram relatórios enganosos sobre um sistema de computador com base nos resultados de um "escaneamento gratuito". Essas declarações e relatórios enganosos buscam persuadir você a comprar uma versão ou assinatura completa, normalmente sem permitir que você avalie o limpador de registro antes do pagamento. Por isso, a ESET classifica esses programas como PUA e oferece a você a opção de permiti-los ou bloqueá-los.

Conteúdo potencialmente indesejado

Se a detecção de PUA estiver ativada em seu produto ESET, sites que tenham uma reputação de promover PUAs ou uma reputação de enganar os usuários para que eles realizem ações que poderiam ter implicações negativas em seu sistema ou experiência de navegação serão bloqueados como conteúdo potencialmente indesejado. Se você receber uma notificação de que um site que está tentando visitar é categorizado como tendo conteúdo potencialmente indesejado, você pode clicar em **Voltar** para sair da página da web bloqueada ou clicar em **Ignorar e continuar** para deixar o site carregar.



Mais informações sobre esse tópico podem ser encontradas neste [artigo da Base de conhecimento da ESET](#).

Ransomware

Ransomware (também conhecido como filecoder) é um tipo de malware que bloqueia seu dispositivo ou criptografa o conteúdo no seu dispositivo e extorque dinheiro de você para restaurar o acesso ao seu conteúdo. Esse tipo de malware também pode ter um timer incorporado com um prazo de pagamento pré-programado que deve ser cumprido. Se o prazo não for atendido, o preço aumentará ou o dispositivo se tornará definitivamente inacessível.

Quando o dispositivo é infectado, o filecoder pode tentar criptografar as unidades compartilhadas no dispositivo. Esse processo pode fazer com que pareça que o malware está se espalhando pela rede, mas na verdade ele não está. Essa situação acontece quando a unidade compartilhada em um servidor de arquivo está criptografada, mas o próprio servidor não contém uma infecção de malware (a menos que seja um servidor terminal).

Os autores de ransomware geram um par de chaves, uma pública e uma privada, e inserem a chave pública no malware. O ransomware em si pode ser parte de um trojan ou parecer ser um arquivo ou imagem que você pode receber em um email, em redes sociais ou aplicativos de mensagens instantâneas. Depois de infiltrado no seu computador, o malware vai gerar uma chave simétrica aleatória e criptografar os dados no dispositivo. Ele usa a chave pública no malware para criptografar a chave simétrica. Então o ransomware demanda um pagamento para retirar a criptografia dos dados. A mensagem demandando pagamento exibida no dispositivo pode ser um alarme falso de que seu sistema foi usado para atividades ilegais ou contém conteúdo ilegal. É solicitado que a vítima do ransomware pague um resgate usando vários métodos de pagamento. As opções geralmente são aquelas que são difíceis de rastrear, como moedas digitais (crypto currencies), mensagens de SMS com tarifa premium ou vales pré-pagos. Depois de receber um pagamento, o autor do ransomware deve desbloquear o dispositivo ou usar sua chave privada para retirar a criptografia da chave simétrica e retirar a criptografia dos dados da vítima, mas essa operação não é garantida.

Mais informações sobre a proteção contra ransomware

i Os produtos ESET usam tecnologias em várias camadas que protegem os dispositivos contra ransomware. Consulte nosso [artigo da Base de conhecimento ESET](#) para descobrir as melhores práticas para proteger seu sistema contra ransomware.

Rootkit

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

- 1.Quando eles tentam acessar um sistema: Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
- 2.Quando estão ocultos para os testes usuais: os usuários ESET têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

Programação orientada para retorno

A programação orientada para retorno (ROP) é um ataque típico de reutilização de código, onde um invasor controla diretamente o fluxo através do código existente com um resultado malicioso. O ataque ROP representa uma versão avançada de um ataque de empilhamento. Um transbordamento de pilha de buffer ocorre quando um programa escreve para um endereço de memória na pilha de chamada do programa fora da estrutura de dados pretendida, normalmente com um buffer de comprimento fixo.

ROP é uma técnica de exploit que permite a execução de código no sistema de destino. Ao obter controle da pilha de chamada, o invasor controla o fluxo de software confiável existente em execução no computador e manipula-o para realizar uma tarefa que não a pretendida.

Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

Como uma subcategoria de spyware, os keyloggers podem ser baseados em hardware ou software. Keyloggers baseados em software são capazes de coletar apenas as informações digitadas em um único site ou aplicativo. Keyloggers mais sofisticados podem registrar tudo que você digita, inclusive as informações que você copia/colar. Alguns keyloggers destinados a dispositivos móveis podem gravar chamadas, informações de aplicativos de mensagens, locais ou até mesmo capturas de microfone e câmera.

Trojan

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de ameaças que tentam se apresentar como programas úteis, enganando assim os usuários para executá-los.

Dado que Cavalos de Troia são uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- Downloader – Programas maliciosos com a capacidade de fazer o download de outras ameaças da

Internet.

- Dropper – Programas maliciosos com a capacidade para instalar outros tipos de malware em computadores comprometidos.
- Backdoor – Programas maliciosos que se comunicam com atacantes remotos, permitindo que eles acessem o computador e assumam o seu controle.
- Keylogger - (keystroke logger) - Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- Dialers - Programas maliciosos projetados para se conectar aos números premium-rate em vez do provedor de serviços de Internet do usuário. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modems discados que não são mais usados regularmente.

Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele contém códigos maliciosos.

Vírus

Um vírus de computador é uma parte de um código malicioso que é pré-anexado ou anexado a arquivos existentes no computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um lugar para outro. Quanto ao termo "vírus", ele é frequentemente usado de maneira incorreta para significar qualquer tipo de ameaça. Essa utilização está gradualmente sendo superada e substituída por um termo mais preciso "malware" (software malicioso).

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o código malicioso é chamado e executado antes da execução do aplicativo original. Um vírus pode infectar qualquer arquivo que tenha permissão de gravação dada pelo usuário.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositadamente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

Se o computador estiver infectado com um vírus e a limpeza não for possível, envie-o para o Laboratório de pesquisa da ESET para análise. Em certos casos os arquivos infectados podem ser modificados a ponto de uma limpeza não ser possível e os arquivos precisarem ser substituídos por uma cópia limpa.

Worm

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se propagar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms propagam-se para os endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de horas ou mesmo minutos após sua liberação. Essa

capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Recheamento de credencial

O recheamento de credenciais é um ataque cibernético que usa dados de banco de dados de credenciais vazados. Os agressores usam bots e outros métodos de automatização para fazer login em contas em vários sites usando os dados vazados. Os agressores aproveitam-se dos usuários que reutilizam suas credenciais de login em vários sites e serviços. Quando o ataque for bem sucedido, os agressores podem obter acesso total à conta e aos dados do usuário armazenados nesta conta. Os agressores podem explorar esse acesso para roubar dados pessoais para roubo de identidade, transações fraudulentas, distribuição de spam ou outras ações maliciosas.

Envenenamento de DNS

Através do envenenamento de DNS (Domain Name Server), os hackers podem levar o servidor DNS de qualquer computador a acreditar que os dados falsos que eles forneceram são legítimos e autênticos. As informações falsas são armazenadas em cache por um determinado período de tempo, permitindo que os agressores reescrevam as respostas do DNS dos endereços IP. Como resultado, os usuários que tentarem acessar os websites da Internet farão o download de vírus ou worms no lugar do seu conteúdo original.

Ataque DoS

DoS, ou Denial of Service (negação de serviço), é a tentativa de impedir que o computador ou a rede sejam acessados por seus usuários. A comunicação entre os usuários afetados é obstruída e não pode mais continuar de modo funcional. Os computadores expostos aos ataques DoS geralmente precisam ser reinicializados para que voltem a funcionar adequadamente.

Na maioria dos casos, os alvos são servidores web e o objetivo é torná-los indisponíveis aos usuários por um determinado período de tempo.

Ataque ICMP

O ICMP (Protocolo de Controle de Mensagens da Internet) é um protocolo de Internet popular e amplamente utilizado. Ele é utilizado primeiramente por computadores em rede para enviar várias mensagens de erro.

Os atacantes remotos tentam explorar a fraqueza do protocolo ICMP. O protocolo ICMP é feito para comunicação unidirecional que não requer qualquer autenticação. Isso permite que os atacantes remotos disparem ataques chamados de DoS (negação de serviço) ou ataques que dão acesso a pessoas não autorizadas aos pacotes de entrada e de saída.

Exemplos típicos de um ataque ICMP são ping flood, flood de ICMP_ECHO e ataques de smurfs. Os computadores

expostos ao ataque ICMP são significativamente mais lentos (isso se aplica a todos os aplicativos que utilizam a Internet) e têm problemas para conectarem-se à Internet.

Rastreamento de portas

O rastreamento de portas é usado para determinar se há portas abertas no computador em um host de rede. Um rastreador de porta é um software desenvolvido para encontrar tais portas.

Uma porta de computador é um ponto virtual que lida com os dados de entrada e saída - ação crucial do ponto de vista da segurança. Em uma rede grande, as informações reunidas pelos rastreadores de porta podem ajudar a identificar as vulnerabilidades em potencial. Tal uso é legítimo.

O rastreamento de porta é frequentemente usado pelos hackers na tentativa de comprometer a segurança. Seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar quais portas estão em uso. O rastreamento por si só não causa danos, mas esteja ciente de que essa atividade pode revelar as vulnerabilidades em potencial e permitir que os agressores assumam o controle remoto dos computadores.

Os administradores de rede são aconselhados a bloquear todas as portas não usadas e proteger as que estão em uso contra o acesso não autorizado.

SMB Relay

O Relé SMB e o Relé SMB 2 são programas especiais capazes de executar um ataque contra computadores remotos. Os programas se aproveitam do protocolo de compartilhamento de arquivo Server Message Block que é embutido no NetBios. Se um usuário compartilhar qualquer pasta ou diretório dentro da LAN, provavelmente ele utilizará esse protocolo de compartilhamento de arquivo.

Dentro da comunicação de rede local, as criptografias da senha são alteradas.

O Relé SMB recebe uma conexão nas portas UDP 139 e 445, detecta os pacotes trocados pelo cliente e o servidor e os modifica. Após conectar e autenticar, o cliente é desconectado. O Relé SMB cria um novo endereço IP virtual. O novo endereço pode ser acessado usando o comando "net use \\192.168.1.1". O endereço pode então ser usado por qualquer uma das funções de rede do Windows. O Relé SMB detecta a comunicação do protocolo SMB, exceto para negociação e autenticação. Os agressores remotos podem usar o endereço IP enquanto o computador cliente estiver conectado.

O Relé SMB 2 funciona com o mesmo princípio do Relé SMB, exceto que ele usa os nomes do NetBios no lugar dos endereços IP. Os dois executam ataques "man-in-the-middle". Esses ataques permitem que os agressores remotos leiam, insiram e modifiquem as mensagens trocadas entre dois pontos finais de comunicação sem serem notados. Os computadores expostos a tais ataques frequentemente param de responder ou reiniciam inesperadamente.

Para evitar ataques, recomendamos que você use senhas ou chaves de autenticação.

Dessincronização TCP

A dessincronização TCP é uma técnica usada nos ataques do TCP Hijacking. Ela é acionada por um processo no qual o número sequencial dos pacotes recebidos difere do número sequencial esperado. Os pacotes com um

número sequencial inesperado são dispensados (ou salvos no armazenamento do buffer, se estiverem presentes na janela de comunicação atual).

Na dessincronização, os dois pontos finais da comunicação dispensam os pacotes recebidos; esse é o ponto onde os agressores remotos são capazes de se infiltrar e fornecer pacotes com um número sequencial correto. Os agressores podem até manipular ou modificar a comunicação.

Os ataques TCP Hijacking têm por objetivo interromper as comunicações servidor-cliente ou peer-to-peer. Muitos ataques podem ser evitados usando autenticação para cada segmento TCP. Também é aconselhável usar as configurações recomendadas para os seus dispositivos de rede.

Ataque de worm

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. Os worms da rede exploram as vulnerabilidades de segurança dos diversos aplicativos. Devido à disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de algumas horas após sua liberação.

A maioria dos ataques dos worms (Sasser, SqlSlammer) podem ser evitados usando-se as configurações de segurança padrão do firewall, ou bloqueando as portas não usadas e desprotegidas. Também é fundamental manter o sistema operacional atualizado com os patches de segurança mais recentes.

Envenenamento de Cache ARP

O Protocolo de Resolução de Endereço (ARP) converte entre endereços na camada de link de dados (endereços MAC) e a camada de rede (endereços IP). Um ataque de envenenamento de cache ARP permite que os invasores interceptem a comunicação entre dispositivos de rede corrompendo as tabelas ARP da rede (mapeamentos de dispositivo MAC para IP).

O invasor envia uma mensagem de resposta ARP falsa para o gateway de rede padrão, informando que o endereço MAC está associado ao endereço IP de outro destino. Quando o gateway padrão recebe essa mensagem e transmite as alterações para todos os outros dispositivos na rede, todo o tráfego do destino para qualquer outro dispositivo de rede passa pelo computador do invasor. Essa ação permite que o invasor inspecione ou modifique o tráfego antes de encaminhá-lo para o destino pretendido.

Ameaças por email

Email é uma forma de comunicação que traz muitas vantagens.

Infelizmente, com seus altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso – [malware](#). A inconveniência e o perigo para você são aumentados pelo fato de que os custos de envio são mínimos e os autores de spam têm muitas ferramentas para obter novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam.

Algumas dicas de prevenção:

- Se possível, não publique seu endereço de email na Internet

- Forneça seu email apenas a pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou à sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".
- Use emails "especializados" – por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- Altere seu endereço de e-mail periodicamente
- Utilize uma solução antispam

Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. As suas principais vantagens de marketing são o custo mínimo e um alto nível de objetividade. Além disso, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por email para comunicar de forma eficaz com os seus clientes atuais e prospectivos.

Esse tipo de publicidade é legítimo, desde que você tenha interesse em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o limite razoável e se torna spam.

Hoje em dia a quantidade de emails não solicitados é um problema e não demonstra sinais de que vá diminuir. Geralmente, os autores dos emails não solicitados tentam mascarar o spam como mensagens legítimas.

Hoaxes

Um hoax é uma informação incorreta que é propagada pela Internet. Normalmente, os hoaxes são enviados por email ou por ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes solicitam aos destinatários que encaminhem mensagens aos seus contatos, perpetuando-os. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Na maioria dos casos, é impossível identificar a intenção do criador.

Se você receber uma mensagem solicitando que a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não. Antes de encaminhar, faça uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (por ex. instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, companhias de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

Reconhecimento de fraudes em spam

Geralmente, há alguns indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam.

- O endereço do remetente não pertence a alguém da sua lista de contatos.
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma.
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais - números de contas bancárias, nomes de usuário e senhas, etc.
- Está escrito em um idioma estrangeiro.
- Você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original).
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo, "vaigra" em vez de "viagra".

Regras

No contexto das soluções antispam e dos clientes de email, as regras ajudam a manipular as funções do email. Elas são constituídas por duas partes lógicas:

1. Condição (por exemplo, uma mensagem recebida de um determinado endereço ou com um determinado assunto de email)
2. Ação (por exemplo, a exclusão da mensagem ou transferência para uma pasta especificada)

O número e a combinação de diversas regras com a solução antispam. Essas regras servem como medidas contra spam (email não solicitado). Exemplos típicos:

1. Condição: Uma mensagem de email recebida contém algumas palavras geralmente vistas nas mensagens de spam.
2. Ação: Excluir a mensagem.

1. Condição: Uma mensagem de email recebida contém um anexo com a extensão .exe.
2. Ação: Excluir o anexo e enviar a mensagem para a caixa de correio.

1. Condição: Uma mensagem de email recebida chega do seu patrão.
2. Ação: Mover a mensagem para a pasta "Trabalho"

Para facilitar a administração e filtrar os spams com mais eficiência, recomendamos que você use uma combinação de regras nos programas antispam.

Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceitos, ou para os quais foi concedida permissão de acesso. O termo "lista de permissões de e-mail" (endereços permitidos) define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de e-mail, nomes de domínio ou endereços IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço IP não serão recebidas. Se a lista de permissões não for exclusiva, tais mensagens não serão excluídas, mas filtradas de algum modo.

Uma lista de permissões baseia-se no princípio oposto de uma [lista de proibições](#). As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições: as criadas pelos usuários em seus aplicativos antispam e as listas de proibições profissionais atualizadas com frequência, criadas por instituições especializadas e que podem ser encontradas na Internet.

O uso dessas listas de proibições é um componente essencial da filtragem antispam bem-sucedida, mas é muito difícil mantê-la, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos o uso de uma lista de permissões e uma lista de proibições para filtrar os spams com a maior eficácia.

Exceção

A Lista de exceções (também conhecida como Lista de Exceções) geralmente contém endereços de e-mail que podem ser falsificados e usados para o envio de spam. As mensagens de e-mail de endereços relacionados na Lista de exceções serão sempre escaneadas quanto a existência de spam. Por padrão, a Lista de exceções contém todos os endereços de e-mail em contas existentes dos clientes de e-mail.

Controle pelo servidor

O controle pelo servidor é uma técnica para identificar os emails de spam em massa com base no número de mensagens recebidas e nas reações dos usuários. Cada mensagem deixa uma "marca" digital única com base no conteúdo da mensagem. O número de ID único não diz nada sobre o conteúdo do email. Duas mensagens idênticas terão marcas idênticas, enquanto mensagens diferentes terão marcas diferentes.

Se uma mensagem for marcada como spam, sua marca será enviada ao servidor. Se o servidor receber mais marcas idênticas (correspondendo a uma determinada mensagem de spam), a marca será armazenada no banco de dados de marcas de spam. Ao rastrear as mensagens recebidas, o programa envia as marcas das mensagens ao servidor. O servidor retorna as informações sobre que marcas correspondem às mensagens já marcadas pelos usuários como spam.

Rastreamento de memória avançado

O Rastreamento de memória avançado funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feita para evitar a detecção por produtos antimalware através do uso de ofuscação e/ou criptografia. Em casos em que a emulação comum ou heurística podem não detectar uma ameaça, o Rastreamento de memória avançado é capaz de identificar o comportamento suspeito e rastrear ameaças conforme elas se revelam na memória do sistema. Esta solução é eficaz contra malware que ainda esteja fortemente ofuscado.

Ao contrário do Bloqueio de exploit, O Escaneamento de memória avançado é um método de pós-execução, significando que existe um risco de que alguma atividade maliciosa possa ter sido realizada antes de uma ameaça ser detectada, porém no caso de outras técnicas de detecção terem falhado ele oferece uma camada adicional de segurança.

Proteção para bancos & pagamentos

A Proteção para bancos & pagamentos é uma camada adicional de proteção projetada para proteger seus dados financeiros durante transações online.

O ESET Smart Security Premium e o ESET Internet Security contêm uma lista embutida de sites pré-definidos que vão acionar a abertura de um navegador protegido. É possível adicionar um site ou editar a lista de sites na configuração do produto.

Ative Proteger todos os navegadores para iniciar todos os navegadores da web compatíveis no modo de segurança.

Para mais detalhes sobre este recurso, leia os seguintes artigos na Base de conhecimento ESET:

- [Como usar a Proteção para Bancos e Pagamentos ESET?](#)
- [Pausar ou desativar a Proteção para bancos & pagamentos nos produtos domésticos ESET Windows](#)
- [Proteção para bancos & pagamentos ESET — erros comuns](#)

O uso de comunicação criptografada HTTPS é necessário para realizar a navegação protegida. A Proteção para bancos & pagamentos é compatível com os navegadores a seguir:

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

Abra a Proteção para bancos & pagamentos no seu navegador da web preferido

Ao abrir a Proteção para bancos & pagamentos diretamente da guia **Ferramentas** no menu do produto, ela é aberta no navegador da web definido como padrão no Windows. Caso contrário, quando você abrir seu navegador da web preferido (não do menu do produto), os sites da lista de sites protegidos serão redirecionados para o mesmo tipo de navegador da web protegido pela ESET.

Proteção contra botnet

A proteção contra botnet descobre malware ao analisar seus protocolos de comunicação de rede. O malware de botnet é alterado frequentemente, em contraste com os protocolos de rede, que não foram alterados nos últimos anos. Essa nova tecnologia ajuda a ESET a combater qualquer malware que tente evitar ser detectado e tente conectar seu computador a uma rede botnet.

Detecções de DNA

Os tipos de detecção variam de hashes muito específicos até Detecções de DNA ESET, que são definições complexas de comportamento nocivo e características de malware. Enquanto o código nocivo pode ser modificado ou ofuscado facilmente pelos agressores, o comportamento dos objetos não pode ser alterado tão facilmente. A Detecção de DNA ESET é feita para tirar proveito desse princípio.

Realizamos uma análise profunda do código e extraímos “genes” que são responsáveis por seu comportamento, assim construímos as Detecções de DNA ESET, que são usadas para avaliar códigos potencialmente suspeitos sejam eles encontrados no disco ou na memória de execução de processos. As Detecções de DNA podem identificar amostras conhecidas de malware específicas, novas variantes de uma família de malware conhecida ou até mesmo malware desconhecido e nunca visto antes que contenha genes que indicam o comportamento nocivo.

ESET LiveGrid®

ESET LiveGrid® (construído sobre o sistema de alerta precoce avançado ESET ThreatSense.Net) usa dados que os usuários ESET enviaram em todo o mundo e envia-os para o Laboratório de pesquisa ESET. Ao fornecer amostras suspeitas e metadados originais, o ESET LiveGrid® nos permite reagir imediatamente às necessidades de nossos clientes e manter a ESET sensível às ameaças mais recentes.

Pesquisadores de malware da ESET usam as informações para construir um instantâneo preciso sobre a natureza e abrangência das ameaças globais, que nos ajuda a concentrar nos alvos corretos. Os dados do ESET LiveGrid® desempenham um papel importante na definição de prioridades do nosso processamento automatizado.

Além disso, ele implementa um sistema de reputação que ajuda a melhorar a eficiência global de nossas soluções antimalware. Um usuário pode verificar a reputação de [processo em execução](#) e arquivos diretamente da interface do sistema ou do menu de contexto, com informações adicionais disponíveis do ESET LiveGrid®. Quando um arquivo executável está sendo inspecionado no sistema de um usuário, seu hashtag é comparado primeiro contra um banco de dados de itens na lista de permissões e lista de proibições. Se ele for encontrado na lista de permissões, o arquivo inspecionado é considerado limpo e sinalizado para ser excluído de escaneamentos futuros. Se ele estiver na lista de proibições as ações apropriadas serão tomadas com base na natureza da ameaça. Se nenhuma correspondência for encontrada o arquivo é verificado completamente. Com base nos resultados deste escaneamento, os arquivos são classificados como ameaças ou não ameaças. Esta abordagem tem um impacto positivo significativo no desempenho do escaneamento. Este sistema de reputação permite uma detecção eficaz de amostras de malware, mesmo antes de suas assinaturas serem entregues para o computador do usuário por meio de um banco de dados de vírus atualizado (o que acontece várias vezes ao dia).

Além do sistema de reputação ESET LiveGrid®, o sistema de feedback ESET LiveGrid® coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Servidores ESET LiveGrid®

i Nossos servidores ESET LiveGrid® estão localizados na Bratislava, Viena e San Diego, mas esses são apenas os servidores, que respondem a solicitações dos clientes. As amostras enviadas são processadas na Bratislava, Eslováquia.

Ativar ou desativar o ESET LiveGrid® em produtos ESET

✓ Para instruções mais detalhadas e ilustradas sobre como ativar ou desativar o ESET LiveGrid® em produtos ESET, visite nosso [artigo da Base de conhecimento da ESET](#).

Bloqueio de Exploit

O Bloqueio de Exploit é feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de e-mail e componentes Microsoft Office, e proteger contra [Ataques ROP](#). O Bloqueio de Exploit está disponível e é ativado por padrão em todos os produtos domésticos ESET Windows, produtos ESET para Windows Server e produtos ESET endpoint para Windows.

Ele funciona monitorando o comportamento de processos em busca de atividades suspeitas que possam indicar um exploit.

Quando o Bloqueio de Exploit identifica um processo suspeito, ele interrompe o processo imediatamente e

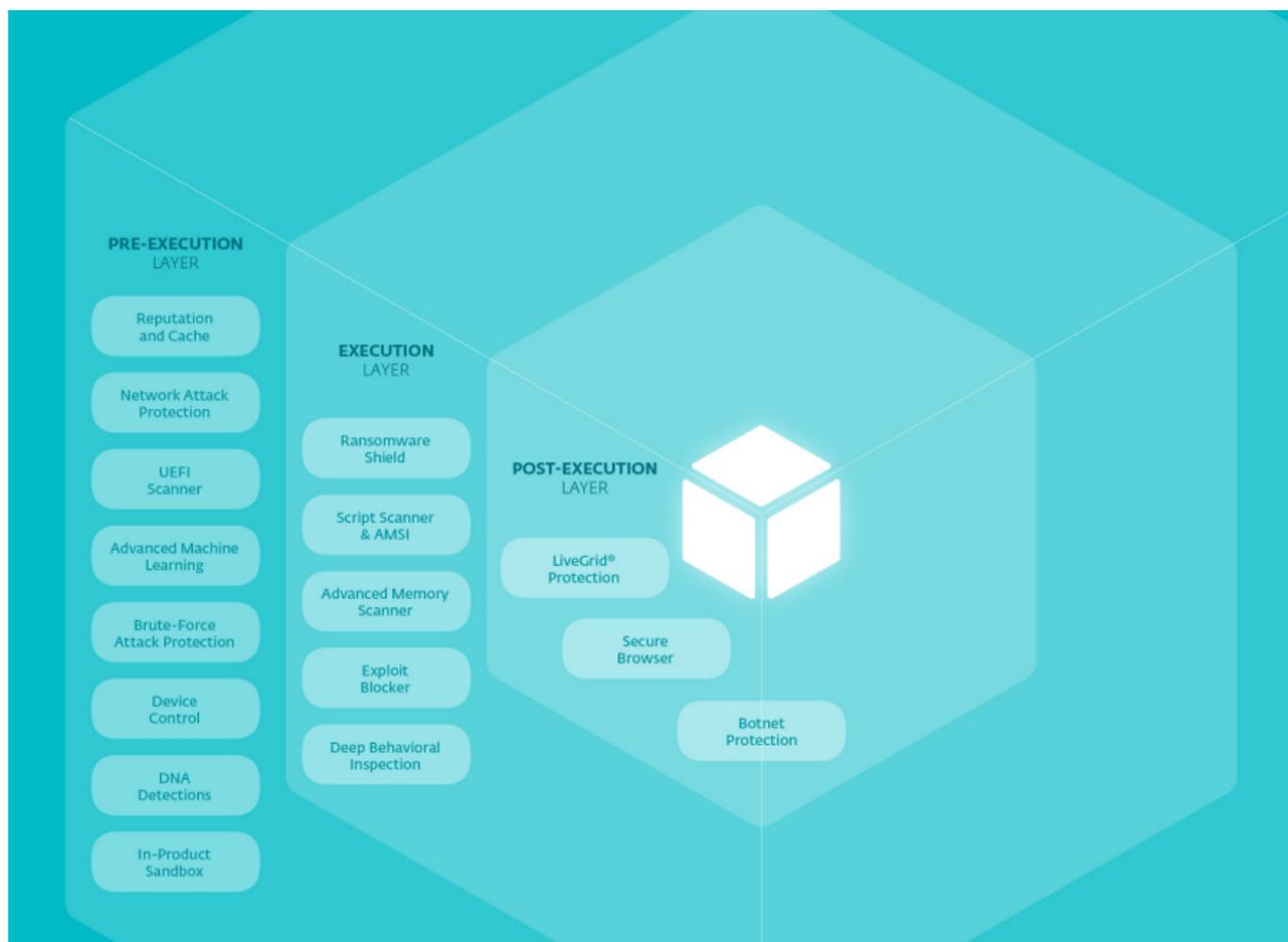
registra e envia os dados sobre a ameaça ao sistema de nuvem do ESET LiveGrid®. Estes dados são processados pelo Laboratório de pesquisa da ESET e usados para proteger melhor todos os usuários contra ameaças desconhecidas e ataques de dia zero (de malware recém-lançado para o qual não há solução pré-configurada).

Bloqueio de Exploit do Java

O Bloqueio de Exploit do Java é uma extensão para a [tecnologia de Bloqueio de Exploit](#) existente. Ele monitora o Java e procura comportamentos semelhantes aos de exploit. Amostras bloqueadas podem ser encaminhadas para analisadores de malware, para que eles possam criar assinaturas para bloqueá-los em camadas diferentes (bloqueio de URL, download de arquivos, etc.).

ESET LiveSense

A ESET usa muitas tecnologias únicas, proprietárias e de proteção em camadas que funcionam juntas como o ESET LiveSense. A figura a seguir mostra algumas das tecnologias principais da ESET e indica aproximadamente quando e onde elas podem detectar, e eventualmente bloquear, uma ameaça durante seu ciclo de vida no sistema.



Aprendizado de máquina

A ESET trabalha com algoritmos de aprendizado de máquina para detectar e bloquear ameaças desde 1990. Redes neurais foram adicionadas ao mecanismo de detecção dos produtos da ESET em 1998.

O aprendizado de máquina inclui [detecções de DNA](#), que usa modelos baseados em aprendizado de máquina para trabalhar de maneira eficaz com ou sem conexão com a nuvem. Algoritmos de aprendizado de máquina também são parte vital da classificação de amostras de entrada, e também para colocá-las no "mapa de segurança cibernética" imaginário.

A ESET desenvolveu seu próprio mecanismo de aprendizado de máquina interno. Ele usa o poder combinado de redes neurais (como o aprendizado profundo e a memória a curto prazo longa) e um grupo selecionado de seis algoritmos de classificação. Isso permite que o mecanismo gere uma saída consolidada e ajuda a rotular adequadamente a amostra de entrada como limpa, potencialmente indesejada ou maliciosa.

O mecanismo de aprendizado de máquina da ESET é adaptado para cooperar com outras tecnologias de proteção como DNA, sandbox e [análise de memória](#), e também com a extração de recursos comportamentais, para oferecer as melhores taxas de detecção e o menor número possível de [falso positivos](#).

Configuração do escaneador na Configuração avançada do produto ESET

- [Produtos domésticos para Windows da ESET](#) (a partir da versão 13.1)
- [Produtos endpoint para Windows da ESET](#) (a partir da versão 7.2)

Proteção contra ataque de rede

A Proteção contra ataque de rede é uma extensão para o Firewall que melhora a detecção de exploits para vulnerabilidades conhecidas no nível da rede. Ao implementar detecções para exploits comuns em protocolos amplamente utilizados como o SMB, RPC e RDP, ele constrói uma outra camada de proteção importante contra a propagação de malware, ataques conduzidos pela rede e explorações de vulnerabilidades para os quais um ainda não foi lançado ou implantado um patch.

Escudo Anti-ransomware

O Escudo Anti-ransomware é uma técnica de detecção baseada em comportamento que monitora o comportamento de aplicativos e processos que tentam modificar arquivos de uma maneira que é comum para [ransomware/filecoders](#). Se o comportamento de um aplicativo for considerado malicioso ou se o escaneamento baseado em reputação mostrar que um aplicativo é suspeito, o aplicativo será bloqueado e o processo será interrompido, ou o usuário será solicitado a bloquear ou permitir.



O ESET LiveGrid® deve estar ativado para que o Escudo Anti-ransomware funcione adequadamente. Consulte nosso [artigo da Base de conhecimento ESET](#) para certificar-se de que o ESET LiveGrid® ele está ativado e funcionando no seu produto ESET.

Proteção contra ataques baseados em script

A Proteção contra ataques baseados em script consiste em proteção contra javascript em navegadores da web e proteção da Interface de Escaneamento Antimalware (AMSI) contra scripts em PowerShell.



HIPS
O HIPS deve estar [ativado](#) para que esse recurso funcione.

A Proteção contra ataques baseados em script é compatível com os seguintes navegadores da Web:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

Use um navegador da web compatível

i As versões mínimas compatíveis de navegadores da web podem variar, pois a assinatura de arquivo dos navegadores muda frequentemente. Porém, a versão mais recente do navegador da web é sempre compatível.

Navegador protegido

O Navegador protegido é uma camada adicional de proteção projetada para proteger seus dados confidenciais enquanto navega pela internet (por exemplo, dados financeiros durante transações online).

O ESET Endpoint Security 8 e versões posteriores contém uma lista embutida de sites pré-definidos que vão acionar a abertura de um navegador protegido. É possível adicionar um site ou editar a lista de sites na configuração do produto. O Navegador protegido está desativado por padrão depois da instalação.

Para mais detalhes sobre este recurso, leia o seguinte [artigo na Base de conhecimento ESET](#).

O uso de comunicação com criptografia HTTPS é necessário para realizar a navegação protegida. Para usar a navegador protegido, seu navegador da internet deve cumprir com os requisitos mínimos listados abaixo:

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

i Apenas o Firefox e o Microsoft Edge são compatíveis com dispositivos com processadores ARM.

Abrir o Navegador protegido ESET no seu navegador da web preferido

Ao abrir o Navegador protegido ESET diretamente da guia **Ferramentas** no menu do produto, o Navegador protegido ESET é aberto no navegador da web definido como padrão. Caso contrário, quando você abrir seu navegador da web preferido (não do menu do produto), a lista interna da ESET será redirecionada para o mesmo tipo de navegador da web protegido pela ESET.

Escaner UEFI

O Escaner de Interface de Firmware Unificada e Extensível (UEFI) faz parte do Sistema de prevenção de intrusos baseado em host (HIPS) que protege o firmware UEFI no seu computador. O firmware UEFI é carregado na memória no início do processo de inicialização. O código está em um chip de memória flash soldado na placa mãe. Ao infectá-lo, os agressores podem implantar um malware que sobrevive a reinstalações e reinicializações do sistema. O malware também pode passar despercebido por soluções antimalware, já que muitos deles não

escaneiam essa camada.

O Escaner UEFI é ativado automaticamente. Você também pode iniciar um escaneamento no computador manualmente a partir da janela principal do programa clicando em **Escaneamento do computador > Escaneamentos avançados > Escaneamento personalizado** e selecionando o destino **Setores de inicialização/UEFI**.



Se o seu computador já foi infectado por malware UEFI, leia o Artigo da Base de conhecimento ESET a seguir:

[Meu computador foi infectado por malware UEFI, o que devo fazer?](#)

Arquivo canário

Um arquivo canário é um documento de computador falso colocado entre documentos reais para ajudar na detecção antecipada de acesso, cópia ou modificação de dados não autorizados.

Bloqueio

Um bloqueio é uma situação onde cada processo do computador aguarda um recurso que está atribuído a outro processo. Neste caso, nenhum dos processos será executado, já que o recurso necessário está bloqueado por outro processo que também está aguardando a liberação de outro recurso. É importante impedir um bloqueio antes que ele possa ocorrer. Uma ocorrência de bloqueio pode ser detectada pelo agendador de recursos, o que ajuda o sistema operacional a acompanhar todos os recursos alocados a processos diferentes. O bloqueio pode ocorrer se as quatro condições a seguir existirem simultaneamente:

- **Nenhuma ação preventiva** – um recurso só pode ser liberado voluntariamente pelo processo que o mantém depois do processo ter concluído sua tarefa.
- **Exclusão mútua** – um tipo especial de semáforo binário usada para controlar o acesso ao recurso compartilhado. Permite que tarefas atuais de prioridade superior sejam mantidas bloqueadas pelo menor tempo possível.
- **Manter e esperar** – nessa condição, os processos devem ser impedidos de manter recursos individuais ou múltiplos enquanto aguardam simultaneamente um ou mais outros.
- **Espera circular** – impõe uma ordem total de todos os tipos de recursos. A espera circular também requer que todos os processos solicitem recursos em uma ordem da enumeração que vai aumentando.

Existem três formas de lidar com um bloqueio:

- Não deixe o sistema em um estado de bloqueio.
- Deixe o bloqueio acontecer, então faça a prevenção para lidar com isso quando ocorrer.
- Se ocorrer um bloqueio, reinicie o sistema.