TECNOLOGIA ESET

A abordagem multicamadas e sua eficácia

Autores:
Jakub Debski, Diretor de Desenvolvimento Tecnológico Central
Juraj Malcho, Diretor de Pesquisa
Peter Stančík, Gerente de Pesquisa em Segurança e Awareness

Versão do documento: 1.3

ENJOY SAFER TECHNOLOGY™

CONTEÚDOS

OBJETIVOS

Neste documento, resumimos as formas nas quais a ESET usa a tecnologia multicamadas para ir muito além das capacidades básicas de antivírus. Fazemos isso explicando quais camadas estão envolvidas na solução de problemas específicos e quais benefícios eles fornecem aos usuários.

SOLUÇÕES DE SEGURANÇA DA PRÓXIMA GERAÇÃO

A maioria das empresas de antivírus estabelecidas cresceram a partir de um desejo de ajudar as pessoas que têm problemas com vírus ou malware e sua tecnologia se desenvolveu para reunir uma ampla variedade de ameaças que os vendedores de segurança estavam começando a tratar. Hoje, o antivírus é percebido como um negócio de commodity e segurança é um assunto que atinge todas as pessoas, elas compreendendo ou não o que isso realmente significa. Mais recentemente, temos visto uma proliferação de empresas novas que se auto proclamam como "próxima geração" – ou como nós gostamos de chamá-las "pós verdade". Elas tipicamente têm pouca experiência no desenvolvimento de soluções antimalware, mas comercializam agressivamente suas soluções como "inovadoras", enquanto que deixam de lado vendedores estabelecidos por serem "dinossauros". Como todo vendedor com soluções milagrosas, muitas de suas alegações são enganosas e, ironicamente, suas capacidades de detecção normalmente são confiadas a um mecanismo de detecção terceirizado de um vendedor já estabelecido, já que apenas poucas dúzias de provedores de solução que estão agora no mercado têm a experiência ou a capacidade de conseguir desenvolver sua própria tecnologia de detecção central. As tecnologias da ESET são todas patenteadas e desenvolvidas pela própria empresa.

Contudo, a simples detecção por assinatura estática que – de acordo com os novatos – está comprometendo a efetividade da indústria antimalware estabelecida é, se não morta e enterrada, apenas um minúsculo componente da bateria de tecnologias que um produto de segurança moderno instala contra ameaças atuais.

MÚLTIPLAS AMEAÇAS, PROTEÇÃO MULTICAMADAS

As empresas de antimalware estabelecidas que ainda fazem negócios hoje têm mantido seu share de mercado evoluindo no encaminhamento de ameaças atuais.

Essas ameaças não são estáticas e sua evolução não parou no começo dos anos 2000. As ameaças de hoje não podem ser combatidas efetivamente somente investindo em tecnologia desde dos anos 90. Lutar contra os malwares modernos é um jogo de gato e rato no qual encaramos equipes de pessoas más que são qualificadas e (financeiramente) motivadas. Desse modo, as empresas de segurança precisam refinar seus produtos constantemente, tanto reativamente como proativamente, para fornecer soluções efetivas, adicionando camadas diferentes com as quais os malwares modernos possam ser detectados e/ou bloqueados. Um único ponto de proteção ou um único método de defesa é simplesmente pouco eficiente.

Essa é uma das razões pelas quais a ESET também evoluiu de um vendedor de antivírus para uma empresa de segurança em TI.

Múltiplas ameaças, múltiplas plataformas

Os sistemas operacionais Microsoft não são as únicas plataformas nas quais os malwares rodam hoje em dia. O campo de combate está mudando rapidamente e os hackers tentam tomar o controle de plataformas e processos previamente não explorados.

- Qualquer coisa que possa ser controlada para desempenhar atividades maliciosas pode ser usada por hackers.
- Qualquer coisa que rode um código executável para processar dados externos pode potencialmente ser sequestrada por dados maliciosos.

Os servidores Linux têm sido um grande alvo para os hackers (Operação Windigo, *Linux/Mumblehard*), Macs que rodam OS X hospedaram um dos maiores botnets de todos os tempos (*OSX/Flashback*), os telefones celulares são alvos comuns (*Hesperbot*) e os ataques em roteadores estão se tornando uma séria ameaça (*Linux/Moose*). Rootkits estão chegando cada vez mais perto do hardware (ataques em firmware ou usando o *rootkit UEFI*) e a virtualização abre novos vetores de ataque (Bluepill, vulnerabilidades de escape da máquina virtual). Também, os navegadores de web estão se tornando tão complexos quanto os sistemas operacionais e seus mecanismos de script são frequentemente usados com propósitos maliciosos (*Win32/Theola*).

Diferentes Vetores de Distribuição

Historicamente, o primeiro malware apareceu como um processo auto replicativo, primeiramente dentro de sistemas e depois como vírus que infectavam arquivos e discos, se espalhando de PC em PC. Como o uso da internet se tornou quase universal, também o número de caminhos para a distribuição de malware cresceu enormemente.

Objetos maliciosos podem também ser enviados por e-mail como anexos ou links, serem baixados de páginas na web, transmitidos por scripts em documentos, compartilhados em dispositivos removíveis, instalados remotamente levando vantagem sobre autorizações ruins e senhas fracas, executados por exploits ou instalados por usuários finais via técnicas de engenharia social.

Design de malware

A era em que os malwares eram escritos por adolescentes como uma piada ou para se exibirem já passou. Hoje em dia o malware é escrito com o objetivo de ganhar dinheiro ou roubar informações e uma alta quantia de dinheiro é investida em seu desenvolvimento tanto por criminosos quanto pelos governos.

Na esperança de tornar a detecção mais difícil, o malware é escrito em diferentes linguagens de compilação e interpretação. O código é ofuscado e protegido usando software customizado para tornar a detecção e a análise mais difíceis. O código é injetado dentro de processos limpos em uma tentativa de evitar monitoramento de comportamento – que é desenhado para localizar atividade suspeita – e dificultar a remoção, garantindo persistência no sistema. Os scripts são usados para evitar técnicas de controle de aplicativos e o malware "que fica somente na memória" contorna a segurança de arquivo.

Para ficarem por dentro das proteções no passado, os cibercriminosos inundavam a internet com milhares de variações de seus malwares. Outro método é distribuir o malware para um pequeno número de alvos para evitar atrair a atenção das empresas de segurança. Para evitar a detecção, componentes limpos de software são usados incorretamente ou códigos maliciosos são assinados usando certificados roubados de empresas legítimas, de modo que o código não autorizado seja mais difícil de perceber.

Também, no nível de rede, o malware faz menor uso dos servidores de comando e controle (C&C) codificados para enviar instruções e receber dados de sistemas comprometidos. Controle descentralizado de botnets

dos servidores de comando e controle (C&C) codificados para enviar instruções e receber dados de sistemas comprometidos. Controle descentralizado de botnets usando rede P2P é usado comumente e a comunicação criptografada torna a identificação dos ataques mais difícil. Algoritmos de geração de domínio reduzem a eficiência da detecção baseada em URLs conhecidas bloqueadas. Os hackers tomam o controle de sites legítimos que têm boa reputação e até mesmo os serviços de anúncio legal são usados para distribuir conteúdo malicioso.

NOTA IMPORTANTE
Há muitas formas dos hackers evitarem a detecção, de modo que uma solução simples, com camada única, não é suficiente para fornecer proteção. Na ESET, nós acreditamos que a proteção constante, em tempo real e multicamadas é requisito para assegurar o mais alto nível de segurança.

OS BENEFÍCIOS DA TECNOLOGIA CENTRAL DA ESET

A ferramenta de escaneamento da ESET é o centro de nossos produtos e, enquanto que a tecnologia de base foi herdada do "antivírus à moda antiga", ela se estendeu, melhorou grandemente e está constantemente sendo desenvolvida para cobrir ameaças modernas.

O propósito da ferramenta de escaneamento é identificar possíveis malwares e tomar decisões automáticas sobre como possivelmente o código inspecionado pode ser malicioso.

Por muitos anos, a performance da ESET foi baseada em algoritmos inteligentes e códigos agrupados criados manualmente para tratar de congestionamentos na performance causados por análises profundas de códigos usando a tecnologia de sandbox integrada no produto. Contudo, nós melhoramos essa abordagem. Agora, para uma performance máxima, nós usamos tradução binárias em conjunto com emulação interpretada.

Com o sandbox dentro do produto, você tem que emular diferentes componentes do hardware e do software do computador para executar um programa em um ambiente virtualizado. Estes componentes podem incluir memória, sistema de arquivo, APIs do sistema operacional e CPU (unidade de processamento central).

No passado, a CPU era emulada usando código de agrupamento sob medida. Contudo, era um "código interpretado", o que significa que cada uma das instruções tinha que ser emulada separadamente. Com a tradução binária você executa instruções emuladas de forma nativa em uma CPU real. Isso é muito mais rápido, especialmente no caso de loopings no código. Introduzir múltiplos loopings é uma técnica de proteção comum a todos os executáveis, onde medidas têm sido aplicadas para protegê-los de análises feitas pelos produtos de segurança e pesquisadores.

Os produtos ESET analisam centenas de diferentes formatos de arquivo (executáveis, instaladores, scripts, arquivos, documentos e bytecodes) para detectar de forma precisa componentes maliciosos incorporados.

A figura abaixo mostra várias tecnologias centrais da ESET e uma aproximação de quando e como elas podem detectar e/ou bloquear uma ameaça durante seu ciclo de vida no sistema:

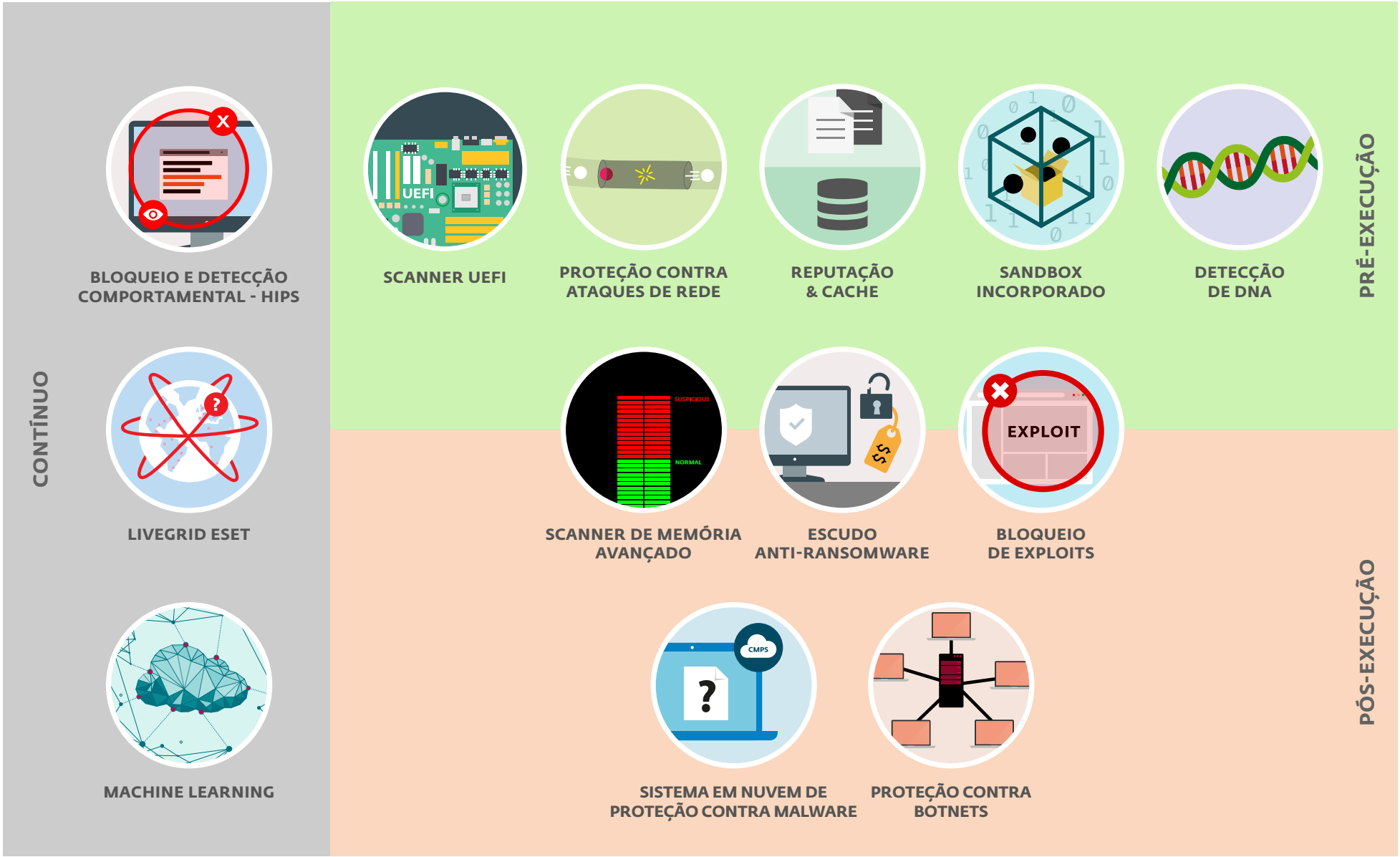
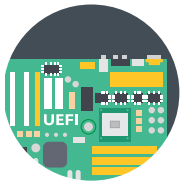


Fig. 1: Camadas de proteção ESET

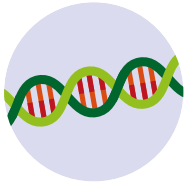


Scanner UEFI

A ESET é a primeira provedora de segurança de internet a adicionar uma camada dedicada dentro de suas soluções que protege a Interface de Firmware Extensível Unificada (UEFI). O UEFI Scanner da ESET checa e reforça a segurança do ambiente pré-inicialização que é compatível com as especificações UEFI. É desenhado para monitorar a integridade do firmware e, caso alguma modificação seja detectada, ele notifica o usuário.

A UEFI é uma especificação padronizada da interface de software que existe entre um sistema operacional de um dispositivo e seu firmware, substituindo o Basic Input/Output System (BIOS) usado nos computadores desde meados dos anos 70. Graças a seu layout bem documentado, a UEFI é mais fácil de analisar, permitindo ainda aos desenvolvedores construir extensões para o firmware. Contudo, isso abre a porta também para que os desenvolvedores malware e hackers que infectam a UEFI com seus módulos maliciosos.

Segue com "Detecções de DNA". Colocar negrito em "Detecções de DNA ESET" no primeiro parágrafo e negrito de "definições complexas..... (até) características de malware".



Detecções de DNA

Os tipos de detecção variam de hashes muito específicos (úteis, por exemplo, em ter como alvo binários maliciosos específicos ou versões específicas de malware, para propósito estatístico ou simplesmente para dar um nome de detecção mais precisa para o malware que encontramos previamente de forma heurística) até as Detecções de DNA ESET, que são definições complexas de comportamento malicioso e características de malware.

O padrão de combinação usado pelos produtos antivírus da velha escola podem ser contornados facilmente por modificações simples do código ou o uso de técnicas de ofuscação. Contudo, o comportamento dos objetos não podem ser mudados tão facilmente. As Detecções de DNA ESET são precisamente desenhadas para tirar vantagem deste princípio. Nós fazemos análises profundas de código, extraindo os "genes" que são responsáveis por este comportamento. Estes genes de comportamento contêm muito mais informação do que os indicadores de comprometimento (IOCs) que algumas das chamadas soluções da "próxima geração" alegam ser a "melhor alternativa" para detecção de assinatura. Os genes de comportamento da ESET são usados para construir Detecções de DNA, que são usados para avaliar códigos suspeitos em potencial, sendo eles achados no disco ou na memória que está em processamento.

Adicionalmente, nossa ferramenta de escaneamento extrai muitos genes discriminatórios que são usados para detecção de anomalias: qualquer coisa que não pareça legítima é potencialmente maliciosa.

Dependendo do nível de limite ajustável e condições correspondentes, as Detecções de DNA podem identificar amostras específicas de malware conhecido, novas variáveis de uma família de malware conhecido ou até mesmo malware nunca visto ou conhecido que contenha genes que indiquem comportamento malicioso. Em outras palavras, uma única descrição de comportamento de DNA bem feito pode detectar dezenas de milhares de

variáveis de malwares relacionados e permitir que nosso software antivírus não apenas detecte malware que já conhecemos ou tenhamos visto antes, como também novas variáveis previamente desconhecidas. Além disso, uma clusterização automatizada e a aplicação de algoritmos de aprendizado de máquina em nosso conjunto de amostras maliciosas permite que identifiquemos novos genes maliciosos e padrões de comportamento para detecção através de nossa ferramenta de escaneamento. Tais genes podem ser facilmente combinados com uma grande lista branca para assegurar que falsos positivos não foram criados.

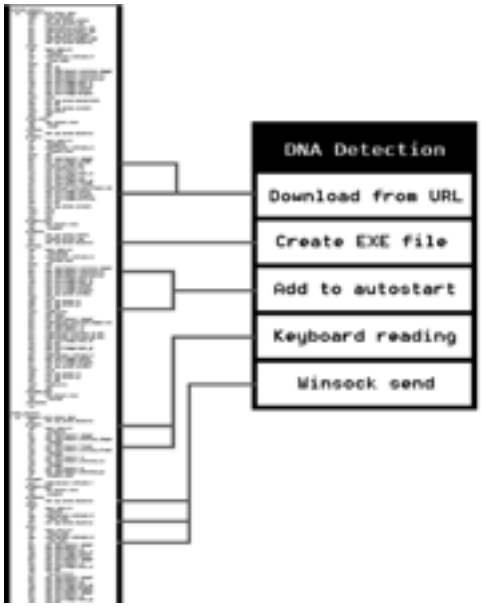


Fig. 2: Exemplo de detecção de DNA

Machine Learning

A ESET tem feito experiências com algoritmos de aprendizado de máquina para detectar e bloquear ameaças desde 1990, com redes neurais abrindo espaço dentro de nossos produtos já em 1998. Desde então, implementamos essa tecnologia promissora dentro de toda nossa abordagem multicamadas.

Isso inclui nossas detecções de DNA, que usam modelos baseados em aprendizado de máquina para trabalhar efetivamente com ou sem conexão com a nuvem. Os algoritmos de aprendizado de máquina são também uma parte vital da escolha inicial e classificação das amostras recebidas, bem como de sua colocação no "mapa de cibersegurança" imaginário.

Mas mais importante, a ESET desenvolveu seu próprio mecanismo de aprendizado de máquina chamado ESET Augur. Ele usa o poder combinado de redes neurais (como aprendizado profundo e memória longa de curto prazo) e um grupo escolhido a dedo de seis algoritmos de classificação. Isso permite gerar um resultado consolidado e ajudar a rotular corretamente as amostras que chegam como limpas, potencialmente indesejadas ou maliciosas.

O mecanismo ESET Augur é ajustado para cooperar com outras tecnologias protetivas como o DNA, o sandbox e a análise de memória, bem como com a extração de funcionalidades comportamentais para oferecer as melhores taxas de detecção e o número mais baixo possível de falsos positivos.

Fig. 3: Esquema do mecanísmo augur de machine learning da

LiveGrid ESET

O meio mais simples de fornecer proteção usando um sistema na nuvem é exatamente fazendo uma lista negra usando hashs. Isso funciona melhor para ambos arquivos e URLs, mas é capaz de bloquear somente objetos que combinem exatamente com a hash. Essa limitação tem levado à invenção de uma hash obscura. Essas hashs obscuras levam em consideração a similaridade binária de objetos, como objetos similares terem uma hash igual ou parecida.

A ESET colocou as hashs obscuras em outro nível. Nós não fazemos hashs de dados, mas do comportamento descrito nas Detecções de DNA.

Usando a hash de DNA, podemos bloquear milhares de variáveis diferentes de malware instantaneamente. Veja gráficos à direita.

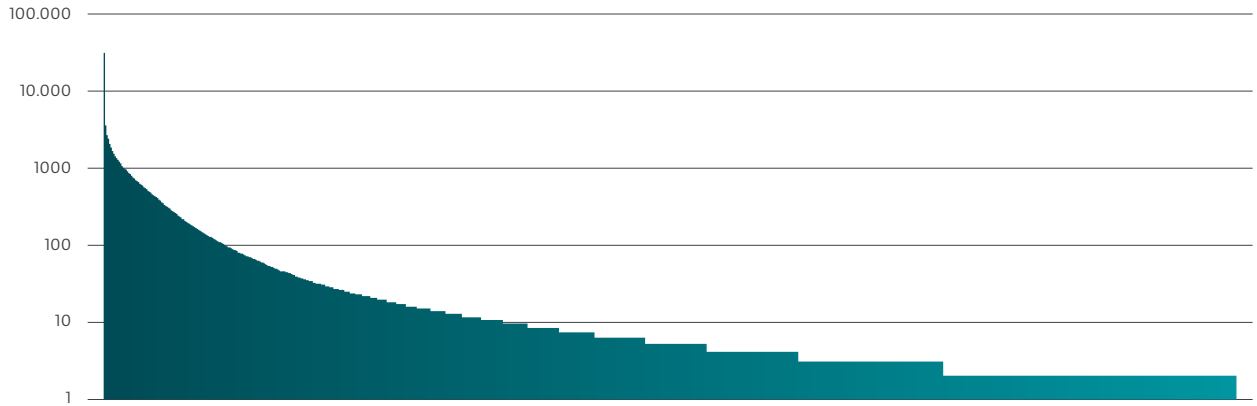


Fig. 4: Número de arquivos únicos (eixo y) detectados por hashes de DNA individuais (eixo x).

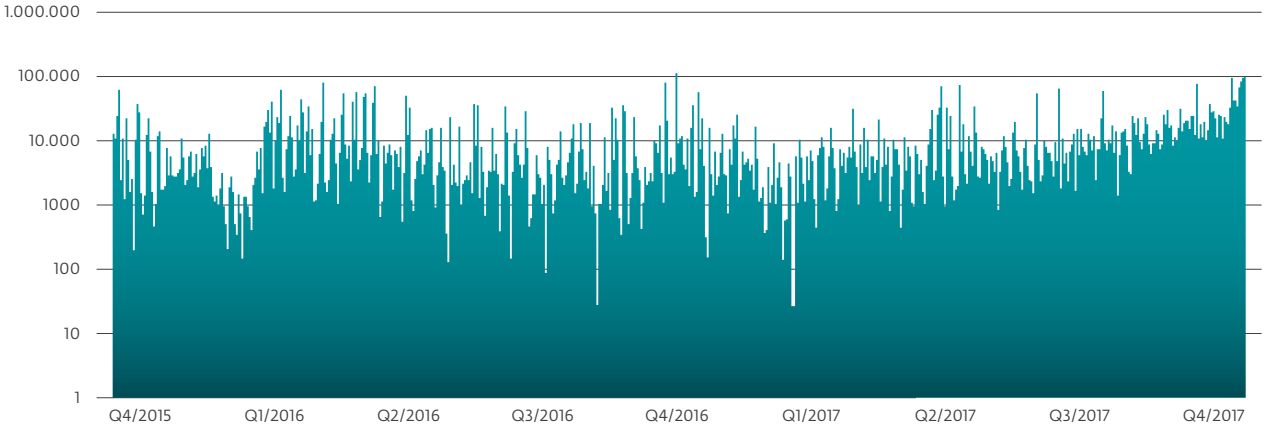


Fig.5 Número de arquivos únicos (eixo y) detectados por hashes de DNA individuais por dia (eixo x)

Sistema de proteção contra malware na nuvem

O Sistema de Proteção contra malware na nuvem da ESET é uma das diversas tecnologias baseadas no sistema de nuvem da ESET, o ESET LiveGrid. Aplicativos desconhecidos e potencialmente maliciosos e outras possíveis ameaças são monitoradas e submetidas à nuvem da ESET através do Sistema de Feedback do ESET LiveGrid. As amostras coletadas são submetidas a um sandbox automático e análise de comportamento, que resulta na criação de detecções automáticas se características maliciosas forem confirmadas. Os clientes da ESET aprendem sobre detecção automática através do Sistema de Reputação do ESET LiveGrid sem a necessidade de esperar pela próxima atualização da ferramenta de detecção. Esse mecanismo de reviravolta de tempo é tipicamente menor que 20 minutos, o que permite detecção efetiva de ameaças emergentes mesmo antes que detecções regulares sejam enviadas aos computadores dos usuários.

Fornecer lista negra (blacklist) instantânea aos usuários não é o único propósito do Sistema de Proteção contra malware na nuvem da ESET. Se um usuário decide participar do processo de envio de amostras, sempre que uma amostra com reputação questionável é identificada, ela é enviada para a ESET para uma análise profunda. Para fazer uso do potencial total do Sistema de Proteção contra malware na nuvem, os usuários devem também habilitar o Sistema de Feedback do ESET LiveGrid, que nos permite coletar quaisquer amostras suspeitas com reputação questionável para que uma análise profunda seja conduzida.

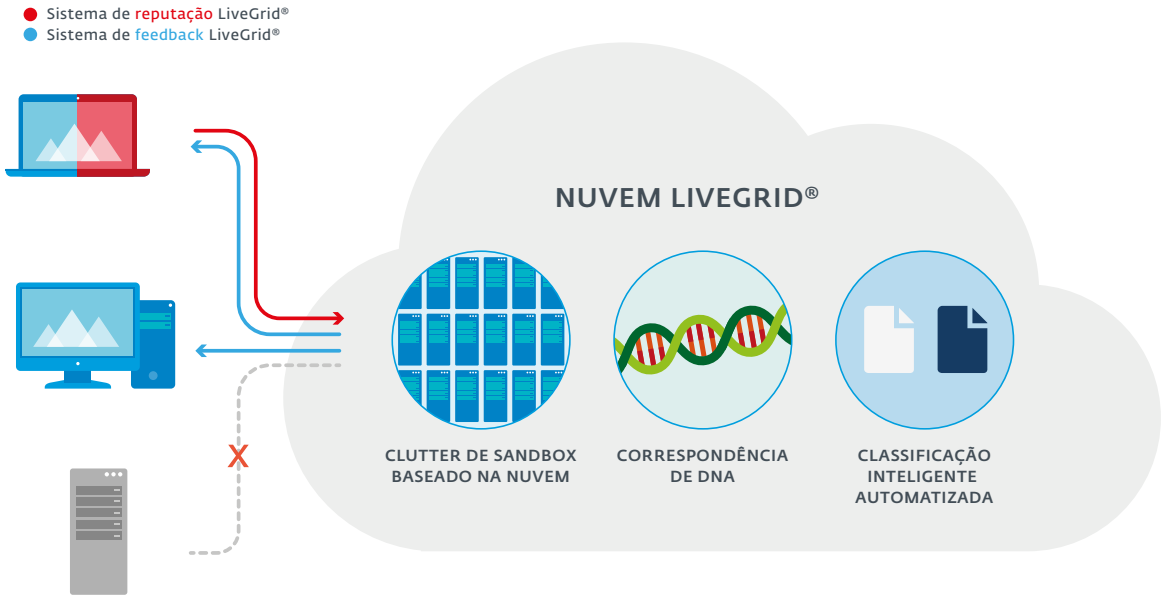


Fig. 6: Sistema de Proteção ESET Contral Malware na Nuvem

Reputação & Cache

Quando inspecionando um objeto como um arquivo ou uma URL, antes de se fazer qualquer escaneamento, nossos produtos checam o cache local (e o ESET Shared Local Cache no caso do ESET Endpoint Security) para objetos maliciosos conhecidos ou colocados em lista branca como benignos. Isso melhora a performance do escaneamento. Em seguida, nosso Sistema de Reputação do ESET LiveGrid é questionado sobre a reputação do objeto (isto é, se o objeto já foi visto em algum outro lugar e classificado como malicioso ou o contrário). Isso melhora a eficiência do escaneamento e permite um compartilhamento mais rápido da inteligência do malware com nossos clientes. Aplicar lista negra em URLs e checar a reputação previne os usuários de acessar sites com conteúdo malicioso e/ou sites de phishing.

Detecção de comportamento e bloqueio – HIPS

O Sistema de Prevenção contra Intrusão baseado em Host da ESET (HIPS) monitora a atividade do sistema e usa um conjunto de regras predefinidas para reconhecer comportamento de sistema suspeito.

Quando este tipo de atividade é detectada, o mecanismo de autodefesa do HIPS detém o programa ofensivo ou o processo de executar atividade potencialmente prejudicial. Os usuários podem definir um conjunto de regras customizado para ser usado ao invés de um conjunto padrão de regras; contudo, isso requer conhecimento avançado dos aplicativos e sistemas operacionais.

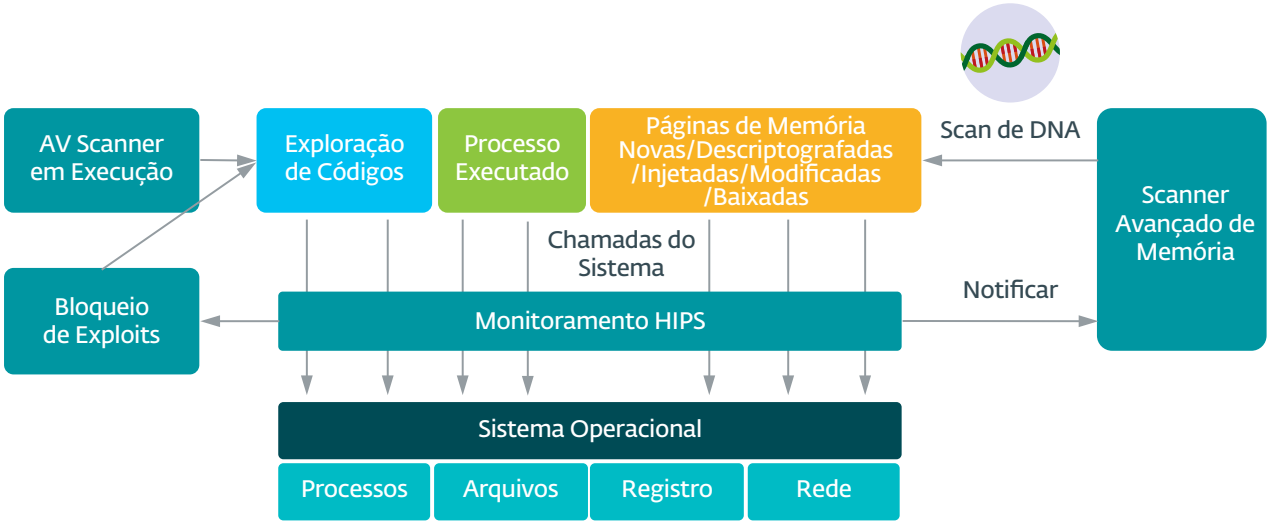
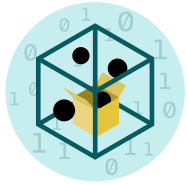


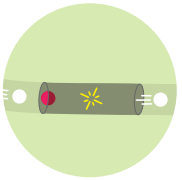
Fig. 7: Como a Detecção de Comportamento da ESET funciona



Sandbox no produto

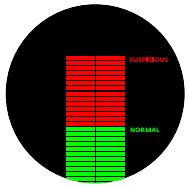
A ESET dividiu a detecção de DNA em duas. Ela ajuda com a compreensão do processo como um todo. É algo que surgiu em 1995 com nosso primeiro emulador utilizado em um produto – foi possível rodar o famoso jogo Doom neste emulador. Isso é o que fazemos para extrair metadados comportamentais que utilizamos em nossas Detecções de DNA. O malware está ficando cada vez mais ofuscado e vem tentando burlar a detecção e nós da ESET estamos tentando enxergar além, para saber como ele se comporta internamente e podermos focar no comportamento real do malware. Também estamos usando traduções binárias para isso, por isso não deixamos a máquina mais lenta.

Fig. 8: Porquê a ESET usa Sandbox incorporado



Proteção contra ataque de rede

A Proteção contra ataque de rede é uma extensão da tecnologia de firewall e melhora a detecção de vulnerabilidades conhecidas no nível da rede. Implementando a detecção para vulnerabilidades comuns em protocolos largamente usados, como SMB, RPC e RDP, isso constitui uma outra importante camada de proteção contra o malware que se espalha, ataques conduzidos via rede e exploração de vulnerabilidades para as quais um patch ainda não tenha sido lançado ou instalado.



Escaneador avançado de memória

O Escaneador de memória avançado é uma tecnologia única da ESET que efetivamente encaminha uma questão importante do malware moderno – uso pesado de ofuscação e/ou criptografia.

Estas táticas de proteção de malware, frequentemente usadas em compressores executáveis e protetores de códigos, causam problemas na detecção que emprega técnicas de extração, tais como emulação e sandbox. E mais, sendo a checagem feita usando um emulador e/ou sandbox físico/virtual, não há garantia de que durante a análise o malware demonstrará comportamento malicioso que permitirá que ele seja classificado como tal.

O malware pode ser ofuscado de modo que nem todos os caminhos de execução possam ser analisados, pode conter gatilhos condicionais ou de tempo para o código e, muito frequentemente, pode baixar novos componentes durante seu tempo de vida. Para lidar com essas questões, o Escaneador de Memória Avançado monitora o comportamento do processo malicioso e o escaneia assim que ele aparece na memória. Isso complementa a funcionalidade mais tradicional de pré-execução ou a análise de código proativa em execução.

Também, processos limpos podem de repente tornarem-se maliciosos por causa de expoits ou injeção de código. Por estas razões, fazer a análise apenas uma vez não é suficiente. Monitoramento constante é necessário e esse é o papel do Escaneamento de Memória Avançado. Sempre que um processo fizer uma chamada de sistema a partir de uma nova página executável, o Escaneamento de Memória Avançado fará uma análise de código de comportamento usando as Detecções de DNA ESET.

A análise de código é feita não somente na memória executável padrão, mas também no código .NET MSIL (Microsoft Intermediate Language) usado por autores de malware para atrapalhar a análise dinâmica. Devido à implementação do cache inteligente, o Escaneamento de Memória Avançado não tem quase despesa e não causa nenhuma deterioração notável nas velocidades de processamento.

O Escaneamento de Memória Avançado trabalha bem com o Bloqueador de Exploit. Ao contrário do anterior, é um método de pós-execução, o que significa que há um risco de que alguma atividade maliciosa já possa ter ocorrido. Contudo, ele entra na cadeia de proteção como um último recurso caso um hacker consiga contornar outras camadas de proteção.

Além disso, há uma nova tendência no malware avançado: alguns códigos maliciosos agora operam "apenas na memória", sem a necessidade de componentes persistentes no sistema de arquivo que possam ser detectados convencionalmente. Inicialmente, tal malware apareceu apenas nos servidores, devido ao seu longo tempo de atividade – já que os sistemas de servidor se mantêm funcionando por meses ou anos seguidos, os processos maliciosos podem se manter na memória indefinidamente sem a necessidade de sobreviver a um reboot – mas ataques recentes em empresas indicaram uma mudança nessa tendência e vemos que endpoints também viraram alvo nesse sentido. Apenas o escaneamento de memória pode descobrir com sucesso tais ataques maliciosos e a ESET está pronta para essa nova tendência com seu Escaneamento de Memória Avançado.

Bloqueador de Exploit

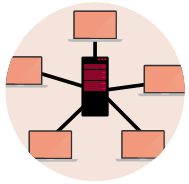
As tecnologias da ESET protegem contra vários tipos de vulnerabilidades em diferentes níveis: nossa ferramenta de escaneamento cobre exploits que aparecem em arquivos de documentos mal formados; a Proteção contra ataque de rede visa o nível de comunicação; e, finalmente, o Bloqueador de Exploit bloqueia a exploração dos processos em si.

O Bloqueador de exploits monitora tipicamente aplicativos exploráveis (navegadores, leitores de documento, clientes de e-mail, Flash, Java e mais) e ao invés de somente visar identificadores de vulnerabilidade e exposição comuns (*CVE*), ele foca em técnicas de exploração. Cada exploit é uma anomalia na execução do processo e nós procuramos por anomalias que sugerem a presença de técnicas de exploração. Como a tecnologia está sob constante desenvolvimento, novos métodos de detecção são adicionados regularmente para cobrir as novas técnicas de exploração. Quando disparado, o comportamento do processo é analisado e, se é considerado suspeito, a ameaça pode ser bloqueada imediatamente na máquina, com os demais metadados relacionados ao ataque sendo enviados para nosso sistema na nuvem ESET LiveGrid. Essa informação é posteriormente processada e correlacionada, o que nos permite identificar ameaças previamente desconhecidas e os chamados ataques de dia zero, e fornecer ao nosso laboratório valiosa inteligência contra ameaças.

O Bloqueador de exploit adiciona uma outra camada de proteção, um passo mais próximo dos hackers, usando uma tecnologia que é completamente diferente das técnicas de detecção que focam em analisar o código malicioso em si.d to protect their end users as well. Based on the needs of the organization, ESET systems and experts can generate custom botnet and targeted malware reports based on YARA rules, phishing reports or offer real time data feeds in STIX/TAXII format, which can be seamlessly integrated into existing SIEM tools.

Escudo Anti-Ransomware

O Escudo Ransomware ESET é uma camada adicional que protege usuários contra ameaças também conhecidas como malware de extorsão. Essa tecnologia monitora e avalia todos os aplicativos executados usando comportamento e reputação baseados em heurística. Sempre que um comportamento que lembra um ransomware é identificado ou o malware em potencial tenta fazer modificações indesejadas em arquivos existentes (por exemplo, para criptografá-los), nossa funcionalidade notifica o usuário que pode bloquear a atividade. O Escudo Ransomware é ajustado para oferecer o maior nível de proteção contra malware possível, juntamente com outras tecnologias ESET, incluindo o Sistema de Proteção contra malware na nuvem, Proteção contra ataque de rede e Detecções de DNA.



Proteção contra botnet

Um elemento do malware que é caro para que seus autores fiquem mudando é a comunicação com os servidores C&C.

A Proteção contra botnet da ESET comprovou ter detectado com sucesso comunicação maliciosa usada por botnets e ao mesmo tempo identificou processos ofensivos.

As Detecções de Rede da ESET estendem a tecnologia de Proteção contra Botnet no encaminhamento de problemas gerais associados com a análise de tráfego de rede. Elas permitem detecção mais rápida e mais flexível de tráfego malicioso. Assinaturas padrão da indústria como o Snort ou o Bros permitem a detecção de muitos ataques, mas as Detecções de Rede da ESET são especificamente desenhadas para mirar as vulnerabilidades de rede, kits de exploit e comunicação de malware avançado em particular.

A habilidade de fazer análise de tráfego de rede em endpoints tem vantagens adicionais. Nos permite identificar exatamente qual processo ou módulo é responsável pela comunicação maliciosa, permite que uma ação seja tomada contra um objeto identificado e às vezes até permite que a criptografia da comunicação seja contornada.

Rastreador de botnet

Se uma amostra ou um despejo de memória é identificado pelos sistema da ESET como um "botnet, eles são enviados para o Rastreador de Botnet da ESET, que identifica a variante exata de malware e usa unpackers/decodificadores específicos para o caso para extrair informação sobre seus servidores C&C e chaves de criptografia/comunicação. Quando eles são obtidos, se inicia uma comunicação falsa a partir de várias geolocalizações. Todos os dados extraídos são então processados posteriormente e usados para proteger os clientes ESET ao redor do mundo, por exemplo, bloqueando URLs, criando novas detecções para payloads, bem como informando os clientes do Threat Intelligence da ESET.

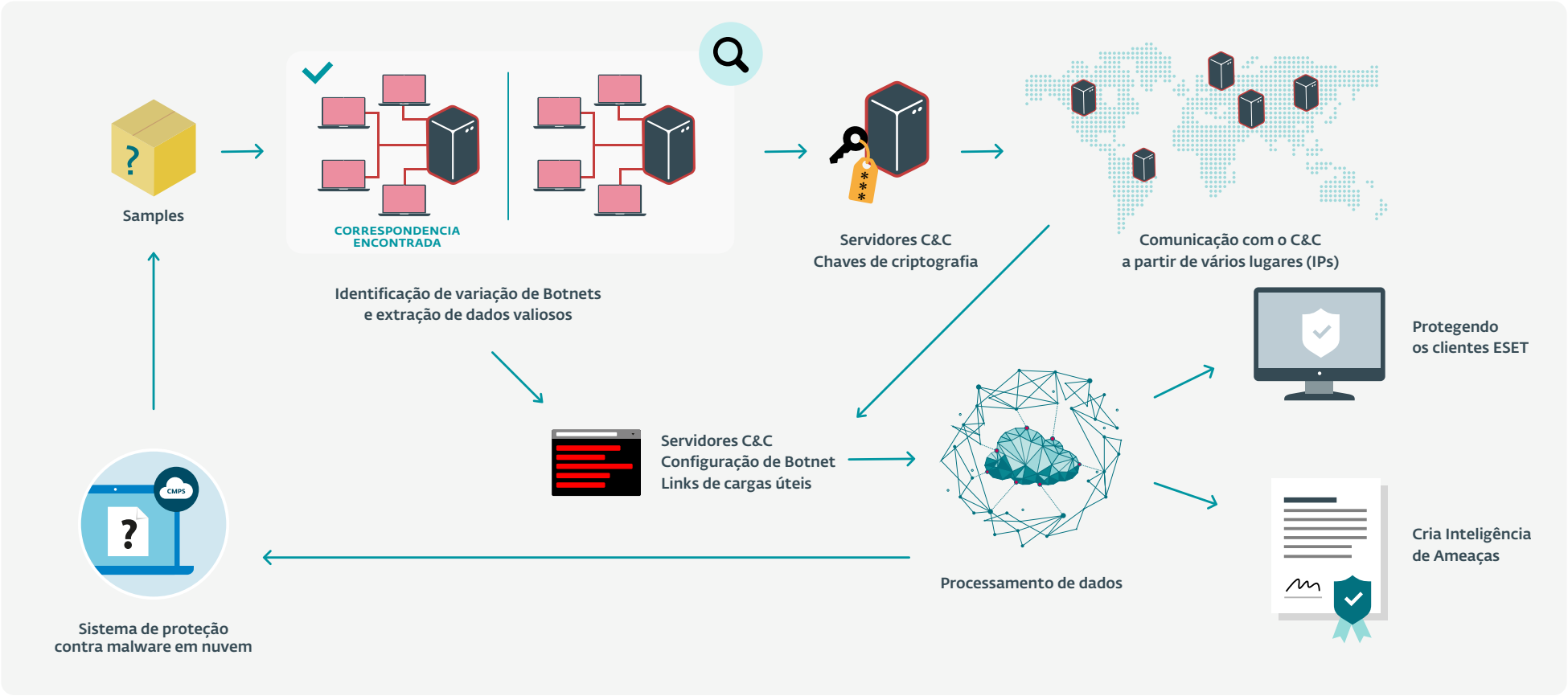


Fig. 9: Como o Rastreador de Botnet funciona

Threat Intelligence

O ESET Threat Intelligence (ETI) ajuda as empresas a se adaptarem a um mundo onde as ameaças a cibersegurança são frequentemente direcionadas e ocultas. Oferecendo coleta de informação de mais de 100 milhões de sensores, esse serviço fornece às organizações um melhor panorama das ameaças, ajuda a prever e prevenir ataques antes que eles aconteçam e oferece estes dados para um diagnóstico de incidente mais eficiente e efetivo na fase pós-ataque. Esse conhecimento único fortalece não somente a segurança das empresas em si, mas pode ser usado para proteger os usuários finais também. Baseada nas necessidades da empresa, os sistemas e os especialistas da ESET podem gerar relatórios customizados sobre botnet e malware direcionado baseado nas regras YARA, relatórios de phishing ou oferecer feed com dados em tempo real no formato STIX/TAXII, que podem ser usados continuamente integrados às ferramentas SIEM existentes.

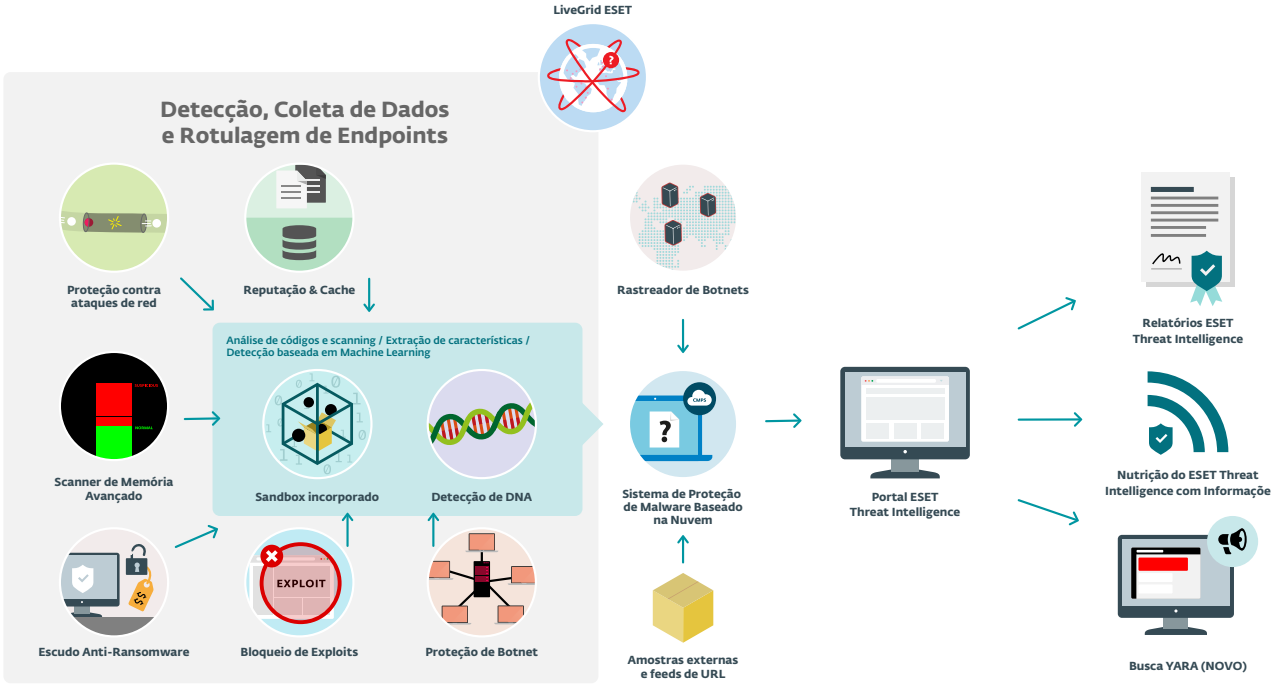


Fig. 10: Coleta de inteligência de ameaças com as tecnologias ESET

PROTEÇÃO REATIVA VS PROTEÇÃO PROATIVA HOJE

Enquanto as Detecções de DNA são excelentes para detectar até mesmo famílias inteiras de malware, elas devem ser distribuídas aos usuários para protegê-los. É o mesmo caso da ferramenta de escaneamento, heurística ou qualquer mudança no foco de novas ameaças. Hoje em dia, a comunicação com o sistema LiveGrid na nuvem da ESET é necessária para assegurar o mais alto nível de proteção por muitas razões:

• O escaneamento off-line é principalmente reativo. Ser proativo hoje em dia não significa mais ter a melhor heurística em seu produto. Enquanto suas ferramentas de proteção estiverem disponíveis para um hacker, não importa se você está usando assinatura, heurística ou classificadores de aprendizado de máquina: um autor de malware pode experimentar sua tecnologia de detecção, modificar o malware até ele não ser mais detectado e apenas então lançá-lo. O ESET LiveGrid antecipa essa estratégia do malware.

• As atualizações não são em tempo real. As atualizações podem ser lançadas mais frequentemente e podem até mesmo ser enviadas aos usuários a todo minuto. Mas isso pode ser feito de uma maneira melhor? Sim: o ESET LiveGrid permite proteção instantânea, fornecendo informações sempre que necessário.

• O malware tenta voar abaixo do radar. Os autores de malware, especialmente no caso de ciberespionagem, tentam evitar a detecção o máximo possível. Ataques direcionados – em oposição às distribuições em massa como os worms de e-mail – instalam pedaços únicos de malware em um pequeno número de alvos, algumas vezes apenas um. Nós usamos este fato contra os autores do malware: objetos que não são populares e não tem uma boa reputação são assumidos como potencialmente maliciosos e analisados no detalhe mesmo no endpoint ou submetidos a análise automática detalhada através do nosso Sistema de Feedback do ESET LiveGrid. O Sistema de Reputação do ESET LiveGrid contém informação sobre arquivos, suas origens, similaridades, certificados, URLs e IPs.

Processamento de amostras automatizadas e manuais

Todos os dias, a ESET recebe centenas de milhares de amostras que são processadas automaticamente, semiautomaticamente e manualmente depois do pré-processamento e clustering. A análise automática é feita por ferramentas desenvolvidas internamente em uma variedade de máquinas virtuais e reais. A classificação é feita usando diversos atributos extraídos durante a execução, de acordo com a análise de código dinâmica e estática, mudanças introduzidas no sistema operacional, padrões de comunicação de rede, similaridade com outras amostras de malware, funcionalidades de DNA, informação estrutural e detecção de anomalia.

Todos os classificadores automáticos têm desvantagens:

• Escolher funcionalidades discriminatórias para classificação não é trivial e deve ser feita usando o conhecimento de humanos que sejam especialistas na área de malware.

• Classificadores de aprendizado de máquina requerem a participação de especialistas humanos para verificar as inserções usadas para o aprendizado. Com um processo totalmente automatizado, onde as amostras classificadas pelo sistema seriam usadas como inserções ao sistema, um efeito bola de neve a partir de um looping de feedback positivo o tornaria rapidamente instável. "Lixo dentro – lixo fora".

• Os algoritmos de aprendizado de máquina não entendem os dados e mesmo que a informação esteja estatisticamente correta, isso não significa que ela seja válida.

Por exemplo, o aprendizado de máquina não pode distinguir um atualizador conectado a um aplicativo limpo de um downloader usado pelo malware e não pode reconhecer quando os componentes de um software limpo são usados com propósitos maliciosos.

• Com o aprendizado de máquina, adicionar novas amostras ao processo de aprendizado pode causar falsos positivos e remover falsos positivos pode reduzir a eficácia da detecção de verdadeiros positivos.

• Enquanto o processo automático permite respostas instantâneas a novas ameaças pela detecção através do ESET LiveGrid, o processamento adicional de amostras por engenheiros de detecção é crucial para assegurar a mais alta qualidade e taxa de detecção e o menor número de falsos positivos.

Serviços de reputação

O ESET LiveGrid também fornece reputação para objetos. Nós julgamos a reputação de várias entidades, incluindo arquivos, certificados, URLs e IPs.

Conforme descrito acima, a reputação pode ser usada para identificar novos objetos maliciosos ou fontes de infecção. Há, contudo, outros usos.

Escaneamento de lista branca

O escaneamento de lista branca é uma funcionalidade que reduz o número de vezes que uma ferramenta de escaneamento precisa inspecionar um objeto. Se temos certeza que um objeto não foi modificado e está limpo, não há necessidade alguma de fazer o escaneamento. Isso tem um impacto muito positivo na performance e ajuda a tornar os produtos da ESET tão discretos. Como nós dizemos, "o código mais rápido é o código que não é executado de forma alguma". Nossas listas brancas são constantemente adaptadas para a realidade sempre em mutação do mundo de software.

Coleta de inteligência

Se um usuário decidir participar enviando estatísticas para o ESET LiveGrid, nós usamos essa informação para um rastreamento global e monitoramento de ameaças. Essa informação nos dá dados abundantes de pesquisa para trabalhar e nos permite focar nos casos mais urgentes e problemáticos, observar as tendências em malware e planejar e priorizar o desenvolvimento de tecnologias de proteção.

SOBRE FPS E IOCS

Indicadores de comprometimento (IOCs) são percebidos como muito importantes na segurança corporativa contemporânea, mas eles estão longe de ser especiais ou avançados, mesmo sendo algumas vezes enfatizados pela "próxima geração" dos provedores de segurança.

Retratado aqui temos uma análise detalhada dos IOCs mais prevalentes e em que eles são baseados*. Como podemos ver, as funcionalidades que eles carregam são extremamente básicas: um quarto dos casos é a respeito de MD5 conhecidas, e então de nomes de arquivos, etc. Os resultados deixam claro que este não é um método que serve para prevenir e bloquear, embora possa ser útil na área forense. É irônico que alguns vendedores da "próxima geração", que desprezam detecções baseadas em assinatura "obsoletas" usadas em "velhos antivírus", elogiem tanto os IOCs, embora eles sejam na verdade o modo baseado em assinatura mais fraco para detectar arquivos ou eventos maliciosos.

*Fonte dos dados: IOC Bucket, Abril de 2015. IOC Bucket é uma plataforma livre dirigida pela comunidade, dedicada a prover uma comunidade segura como um modo de compartilhar a inteligência de ameaças.

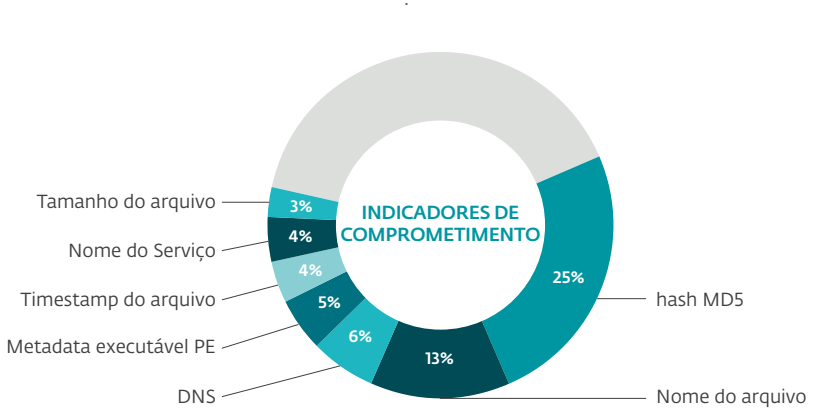


Fig. 11: Análise de indicadores de comprometimento do IOC Bucket (amostra de Abril de 2015)

CONCLUSÃO

Não há mágica em segurança. O malware de hoje, sendo dinâmico e frequentemente direcionado, requer uma abordagem multicamadas baseada em tecnologias proativas e inteligentes que levam em conta os petabytes de inteligência coletados durante muitos anos pelos pesquisadores experientes. Voltando 20 anos, a ESET reconheceu que o antivírus – com abordagem tradicional – era uma solução incompleta, o que nos fez começar a incorporar tecnologias proativas em nossa ferramenta de escaneamento e gradualmente implementamos diferentes camadas de proteção para lutar em diferentes estágios da cadeia de ataques cibernéticos.

A ESET é um dos poucos vendedores de segurança capazes de fornecer um alto nível de proteção baseado em mais de 25 anos de pesquisa. Isso nos permite ficar à frente do malware, constantemente fazendo nossa tecnologia evoluir para ir além do uso da assinatura padrão estática.

Nossa combinação única de tecnologias baseadas em endpoint e em nuvem expandida fornece a mais avançada segurança contra malware no mercado.


ENJOY SAFER TECHNOLOGY™