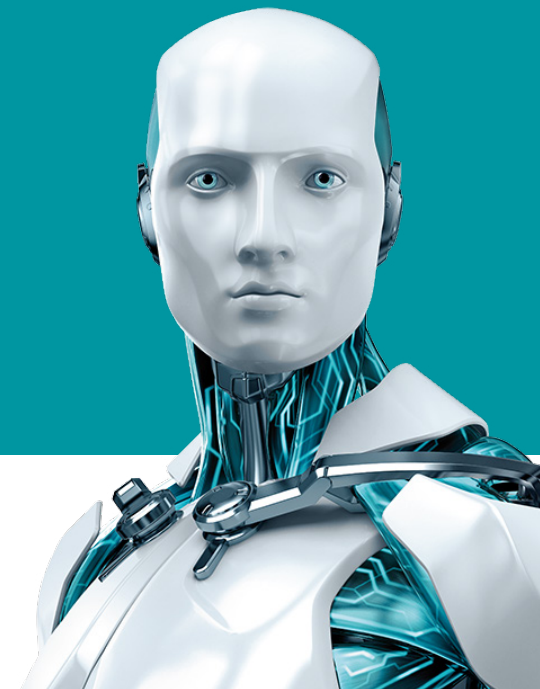


ESET vs. CRYPTO-RANSOMWARE

O quê, como e por quê?



ENJOY SAFER TECHNOLOGY™



CONTEÚDOS

Introdução	2
Todas as camadas ativadas	2
Escudo Ransomware ESET	3
Por que desse jeito e não de outro?	3
RanSim	4
Aplicar whitelist (lista branca) não é uma solução milagrosa.	4
A Shadow Copy é útil, mas não contra cripto-ransomware	4
Por que não fazer uma reversão como último recurso?	4
Outros modos como a ESET luta contra ransomware.	5
Recomendações fundamentais para se proteger contra ransomware	7

INTRODUÇÃO

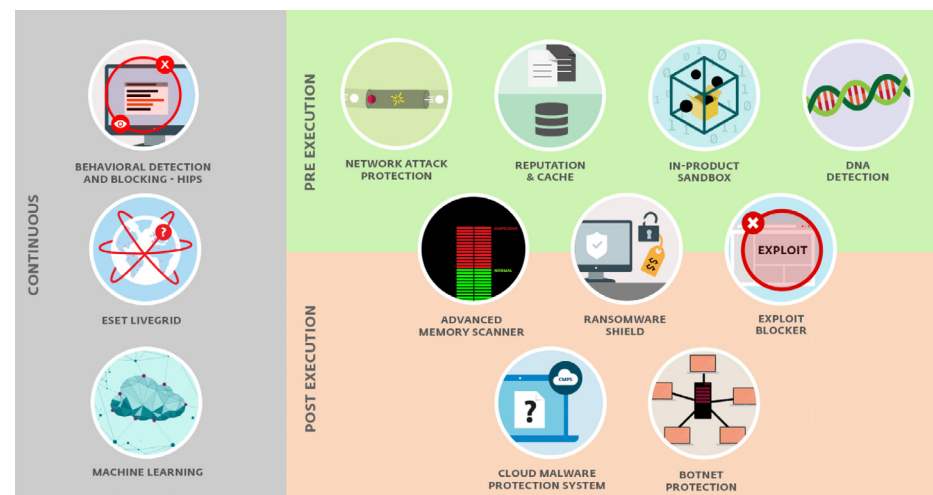
Cripto-ransomware (ou filecoders) estão em alta desde 2013 quando um notório CryptoLocker apareceu. Desde então, os cibercriminosos coletaram milhões de dólares extorquindo dinheiro das vítimas em troca de devolver acesso a seus dados. Em 2016, [estimativas baseadas em dados do FBI](#) sugeriram que o ransomware estava se tornando um crime de **1 bilhão de dólares ao ano**.

Os ganhos dos cibercriminosos demonstram o impacto dessa tendência exponencial e são a principal razão pela qual o cripto-ransomware se tornou o malware de escolha em muitas campanhas. Não deveria ser uma surpresa que a maioria das campanhas de ransomware use kits de exploit e e-mails de engenharia social como seu vetor de infecção, que também contribui para sua prevalência. De fato, de acordo com o [serviço PhishMe](#), *“mais de 97% dos e-mails de phishing entregues em 2016 continham ransomware...”*

A ESET tem monitorado o cenário de ransomware de perto e responde rápido à sua evolução. Em 2016, houve poucos dias nos quais os pesquisadores da ESET não tenham encontrado uma família de ransomware nova em folha.

Contudo, apesar de ser um dos tipos mais sérios de malware que ainda não foi contido, ele é somente um outro tipo de malware. Isso significa que a ESET está combatendo-o como faz com qualquer outro tipo de malware, através de múltiplas camadas.

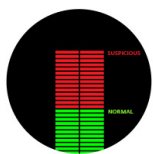
TODAS AS CAMADAS ATIVADAS



A vasta maioria dos ataques de ransomware são bloqueados pela [tecnologia multicamadas da ESET](#) antes mesmo que a infecção efetiva por ransomware atinja os computadores das vítimas. Um bom exemplo disso é a detecção de mensagens de e-mail contendo malwares que eventualmente baixam e executam o ransomware.



Um outro exemplo é a detecção de tentativas de exploração que permitem aos hackers conseguir controle remoto sobre as máquinas das vítimas e em muitos casos levam à extorsão pelo ransomware. As detecções de rede da ESET são desenhadas para prevenir tais tentativas, tendo como alvo vulnerabilidades de rede e kits de exploit. Adicionalmente, o **Bloqueador de Exploits da ESET** monitora os processos de aplicativos que rodam e busca anormalidades em seu comportamento. Seu desenho permite que o produto ESET detecte e bloqueie efetivamente a exploração de vulnerabilidades – mesmo aquelas que são previamente desconhecidas, as chamadas o-days – que podem ser usadas pelo cripto-ransomware para entrar em sistemas alvo.



Para fortalecer mais os sistemas dos usuários, o **Escaneamento Avançado de Memória** é desenhado para descobrir a verdadeira natureza de processos pesadamente ofuscados, frequentemente detectando cripto-ransomware antes que ele criptografe arquivos

valiosos. Tais malwares ofuscados constituem uma parte significativa do tráfego malicioso de hoje, principalmente por causa de serviços automatizados de empacotamento e ofuscação, disponíveis nos mercados negros. Mas mesmo o código mais ofuscado do mundo precisa se revelar em algum momento para ser executado. E esse é exatamente o momento no qual ele será pego pelo nosso Escaneamento Avançado de Memória, que é disparado pelo Sistema de Prevenção contra Intrusão baseado em Host (HIPS) no momento certo.



Adicionalmente, cada uma das camadas da tecnologia multicamadas da ESET usa diferentes meios para ser parte de um bloqueio efetivo do cripto-ransomware. Além disso, metadados de cada uma dessas camadas podem ser enviados para fora dos nossos sistemas de nuvem do **ESET LiveGrid®** fornecendo mais inteligência aos nossos algoritmos de aprendizado de máquina. Estes sistemas

automatizados, combinados com a experiência de nossos pesquisadores e engenheiros, nos permite diminuir o tempo de reação a novas ameaças emergentes para minutos.

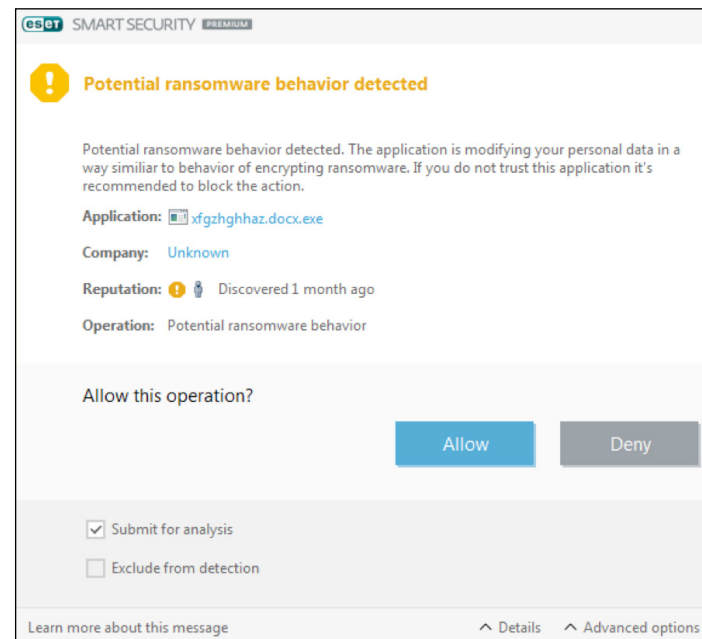
Em um esforço para ficar o mais próximo possível da segurança perfeita, a ESET ainda adicionou uma outra camada para direcionar o fenômeno do ransomware.



Escudo Ransomware ESET

O Escudo Ransomware ESET monitora e avalia aplicativos executáveis usando heurística de comportamento. É desenhado para detectar e bloquear comportamentos que se assemelhem ao ransomware.

A tecnologia é ativada por padrão. Se o Escudo Ransomware ESET for disparado por uma ação suspeita, então será pedido ao usuário que aprove/negue uma ação de bloqueio.



Além disso, a janela de diálogo permite ao usuário submeter aplicativos suspeitos para análise – ou excluí-los de detecções futuras.

POR QUE DESSE JEITO E NÃO DE OUTRO?

Entre diversas possibilidades de abordagem para combater o ransomware, acreditamos que nossa abordagem multicamadas é a correta. E isso não é apenas nossa crença; sua eficiência foi provada em incontáveis testes independentes por organizações que aplicam testes de alta reputação. Por exemplo, em um [teste de uma organização de terceiros independente, a SE Labs, focada na detecção de ransomware, a ESET pontuou em 100%](#). A palavra “conceituada” é muito importante: há testes lá fora que não fornecem valor internacional de forma alguma. Alguns deles são, inclusive, enganosos, como por exemplo, o chamado [RanSim](#).

RanSim

O software pode ser um simulador, mas certamente NÃO simula o comportamento de um cripto-ransomware. A partir do momento que ele modifica apenas os arquivos que ele mesmo criou, ele de fato simula apenas o “ransomware” que exige pagamento para descriptografar seus próprios arquivos. Se todas as milhares de famílias de ransomware para as quais uma solução ainda não tenha sido lançada ou encontrada compartilhassem um design tão engenhoso, não haveria de forma alguma qualquer ransomware efetivo.

Os produtos ESET não detectam – e nem nunca detectarão – este comportamento como malicioso, e então “falham” repetidamente em tais testes. Na verdade, se eles fossem detectar este comportamento, eles também teriam que detectar técnicas de gerenciamento de direitos digitais usadas por plataformas de distribuição digitais, como o Steam. Essas técnicas se comportam similarmente, fazendo o download de seus próprios arquivos criptografados – jogos no caso do Steam – e descriptografando-os no momento certo.

Mas vamos voltar para o tópico desta seção e discutir por que nós não abordamos o cripto-ransomware de forma diferente.

Aplicar whitelist (lista branca) não é uma solução milagrosa

A ideia de uma lista branca de aplicativos benignos conhecidos é frequentemente discutida como uma candidata a ser um tratamento poderoso contra o cripto-ransomware. Independentemente da tarefa de manter o número de falsos positivos tão baixo quanto possível, há diversas questões que precisam ser tratadas.

Casos problemáticos incluem, por exemplo, cripto-ransomware que se injeta dentro de um processo pertencente a um aplicativo que foi colocado em lista branca. Ou quando alguns aplicativos colocados em lista branca possam ser intérpretes, como o wscript, o autoit ou o cmd, e possa ser desafiador decidir quando permitir ou bloquear sua execução, já que o código que eles estão prestes a interpretar (executar) pode ser malicioso.

Isso não quer dizer que a lista branca de aplicativos não faz sentido. Ela contribui para as capacidades de detecção como um todo dos produtos ESET. Contudo, sem outras camadas de proteção, ela seria significativamente mais fraca.

A Shadow Copy é útil, mas não contra cripto-ransomware

A Shadow Copy é uma tecnologia que permite cópias backup automáticas ou manuais ou snapshots dos arquivos de computador ou volumes, mesmo quando estiverem em uso. Contudo, há alguns fatos que devem ser considerados antes de tentar usar isso como uma solução de reversão após o ataque de cripto-ransomware.

Primeiramente, a degradação de performance em potencial relacionada à criação de uma shadow copy e seu armazenamento devem ser considerados. Segundo, as shadow copies podem ser apagadas ou criptografadas pelo ransomware se não estiverem protegidas. Além disso, se o ransomware começa repetidamente a criptografar os arquivos, o buffer dedicado a armazenar as mudanças incrementais de arquivo pode atingir seu limite. E mais importante, não devemos nos esquecer do ransomware de criptografia de disco (como o [Petya](#)) contra o qual as shadow copies seriam completamente inúteis.

Por que não fazer uma reversão como último recurso?

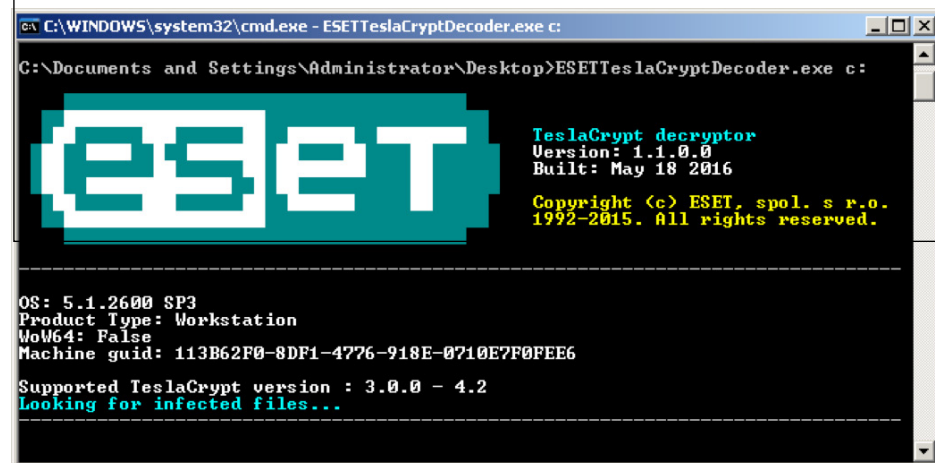
Há claramente benefícios quando se tem a funcionalidade de reversão implementada diretamente em uma solução de segurança. Estamos continuamente testando e avaliando o impacto geral de uma solução desse tipo e poderemos implementar uma no futuro. Neste momento, contudo, nossas análises sugerem que a abordagem atual – com o foco primariamente em medidas proativas – fornece resultados ótimos.

OUTROS MODOS COMO A ESET LUTA CONTRA RANSOMWARE


Nós na ESET sabemos que a luta contra o malware, especialmente tipos tão nocivos quanto o cripto-ransomware, precisa ir além de nossas soluções de segurança padrão e da tecnologia implementada dentro dele. É por isso que nossos pesquisadores estão em constante busca por oportunidades de acabar com as operações de cibercriminosos.

No caso do cripto-ransomware, isso significa encontrar erros em sua implementação ou brechas na infraestrutura dos cibercriminosos. Nós abraçamos cada oportunidade de criar descriptografia de ransomware que ajude aqueles que foram vítimas a recuperar seus dados. Na maioria

dos casos, desenvolvemos decodificadores personalizados para o caso específico da vítima, já que existem muitas variáveis específicas de sistema para serem levadas em consideração. Contudo, sempre que possível, criamos esses decodificadores e os fornecemos sem custo para o público em geral. Nosso decodificador TeslaCrypt, que já foi baixado mais de 100.000 vezes, é um deles.



```
C:\WINDOWS\system32\cmd.exe - ESETTeslaCryptDecoder.exe c:
C:\Documents and Settings\Administrator\Desktop>ESETTeslaCryptDecoder.exe c:

 TeslaCrypt decryptor
Version: 1.1.0.0
Built: May 18 2016

Copyright (c) ESET, spol. s r.o.
1992-2015. All rights reserved.

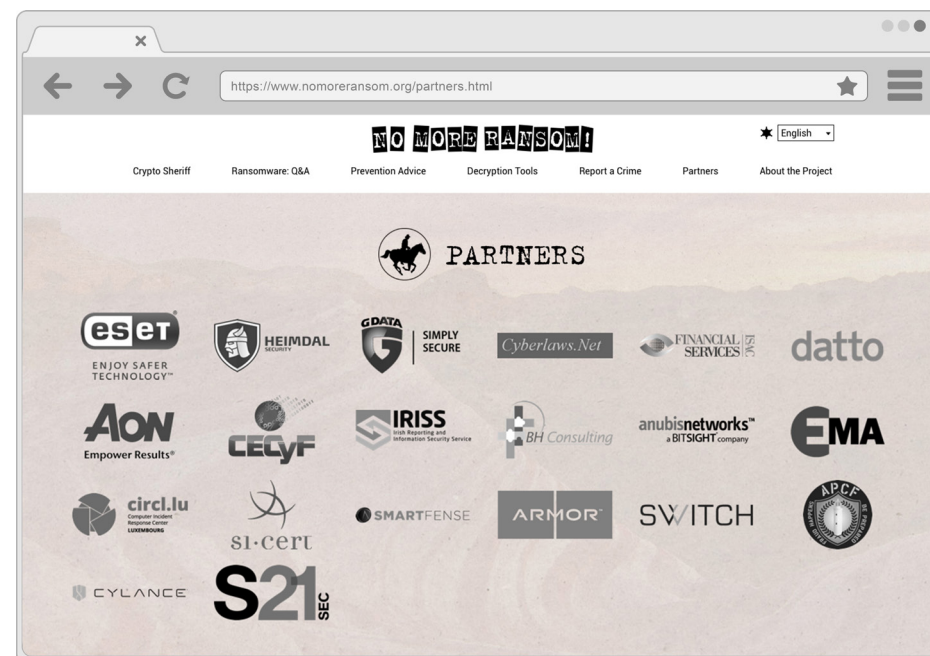
-----
OS: 5.1.2600 SP3
Product Type: Workstation
WoW64: False
Machine guid: 113B62F0-8DF1-4776-918E-0710E7F0FEE6

Supported TeslaCrypt version : 3.0.0 - 4.2
Looking for infected files...
```

Similar a uma abordagem proativa que nossos produtos assumem lidando com o cripto-ransomware, nós também proativamente compartilhamos os resultados de nossa pesquisa de cripto-ransomware, conduzida através de diversos centros de pesquisa da ESET.

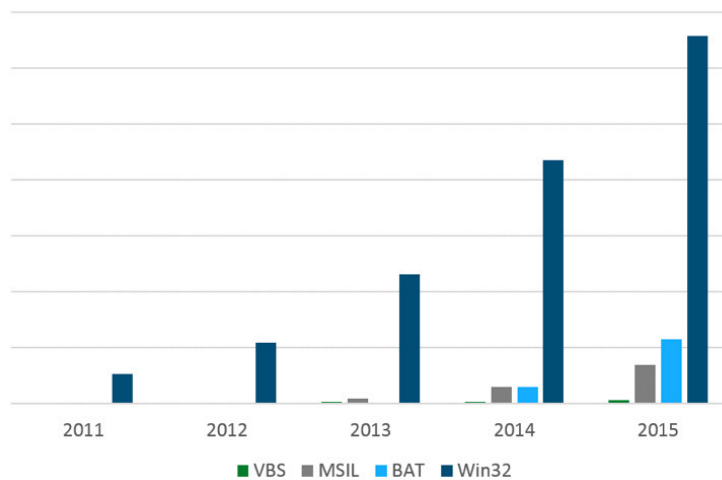
Nós frequentemente publicamos artigos e relatórios sobre cripto-ransomware no blog de nossa empresa www.WeLiveSecurity.com/br, presente no tópico de numerosas conferências internacionais, indo até mesmo em escolas para aumentar a consciência entre a geração mais jovem.

Compartilhamos nossos achados com pesquisadores de todo o mundo, mesmo que eles trabalhem para nossos maiores concorrentes ou para entidades de execução de leis, como o FBI. Ser uma das primeiras empresas a se tornar um parceiro de apoio ao Projeto ["No More Ransom"](http://www.nomore ransom.org) é um dos muitos modos com o qual a ESET tem provado sua dedicação na luta contra o cripto-ransomware.



FOCO NO CRIPTO-RANSOMWARE PETYA

A ESET cobriu a [evolução do cripto-ransomware](#) previamente, mostrando a proeminência de seu crescimento. O número de famílias, variantes e plataformas-alvo aumentou significativamente desde 2011.



Número de programas de ransomware criptografados em arquivos Windows no período de 2011 a 2015.

Vamos ver de perto como a criptografia foi usada em uma nova infame família de cripto-ransomware, o Petya. Exploramos três famílias adicionais neste [this post do blog](#).

O [Petya](#) teve uma abordagem diferente daquela que outros cripto-ransoms têm. Ao invés de arquivos criptografados individualmente, ele tem como alvo o sistema de arquivos. O alvo é o [registro mestre de inicialização](#) (MBR) da vítima, que é responsável por carregar o sistema operacional.

Quando o Petya é executado, ele começa um ataque de dois estágios com o intuito de criptografar o MBR. O processo de criptografia do MBR começa com a modificação do MBR para fazer com que a [tela azul da morte \(BSOD\)](#) faça com que o sistema seja reinicializado.

Ele então mostra uma tela de [CHKDSK](#) falsa, enquanto faz a criptografia do MBR e, finalmente, reinicia o sistema. Quando isso acontece, aparece uma tela piscando com uma caveira e a mensagem de sequestro.



Evolução das telas de caveira do ransomware Petya e telas de sequestro (inicialmente vermelha e mais recentemente com variantes verde e dourada).

Enquanto que essa mensagem é, sem dúvida, amedrontadora, ainda é possível desfazer o dano causado, devido a diversas falhas no modo como o Petya lida com a criptografia.

Os desenvolvedores do Petya cometeram um erro de implementação no núcleo Salsazo, que reduz o nível de segurança da criptografia. Apenas metade da chave é aplicada de fato, reduzindo de uma segurança de 92 bits para uma de 46, o que é passível de quebrar dentro de alguns segundos usando-se força bruta.

Contudo, as versões mais recentes do ransomware não tem mais essas falhas, já que elas foram percebidas e consertadas pelos operadores de malware.

Saiba mais sobre a invasão do ransomware Petya em junho de 2017 [clikando aqui](#).

RECOMENDAÇÕES FUNDAMENTAIS PARA SE PROTEGER CONTRA RANSOMWARE

O ransomware é apenas mais um membro da família do malware. A única diferença é que ele vai atrás de seus arquivos – então, além de tudo o que você faz para não ser infectado (os vetores de ataque são e-mails e kits de exploit principalmente), você precisa ter uma política de backup razoável preparada, com a habilidade de rapidamente se restaurar. Soluções que registram todas as comunicações são pesadas para o disco/CPU e você não vai querer realmente usá-las até um problema de ransomware aparecer (o que em termos de tempo já é muito tarde). Para limitar os vetores de ataque:

1. Configure apropriadamente os endpoints e seu software de segurança.
2. Atualize e use um patch em seu sistema operacional e software regularmente, pois o ransomware frequentemente usa vulnerabilidades conhecidas. Dê atenção especial aos navegadores de internet nesse sentido.
3. As soluções de segurança de endpoint e de perímetro são ótimas e elas devem estar propriamente configuradas para serem capazes de usar o conjunto total de funcionalidades, como detecções rápidas baseadas em nuvem.
4. Use quaisquer capacidades que seu sistema operacional ofereça para dificultar:
 - remova a habilidade de rodar códigos não confiáveis com o AppLocker ou com as políticas de restrição de software;
 - desabilite o script em sistemas operacionais e navegadores;
 - desabilite serviços desnecessários como o RDP;
 - faça com que o sistema operacional mostre a extensão do arquivo;
 - considere usar o serviço de restauração de sistemas;
 - considere desabilitar o Windows Script Host;
 - configure "Abrir com..." para extensões frequentemente usadas para infecção com um leitor (como o Bloco de notas) ao invés de usar um intérprete;
 - bloqueie a execução de aplicativos das pastas %LocalAppData% e %AppData%.
5. Desabilite acesso desnecessário ao compartilhamento de rede.
6. Não use servidores como desktop padrão (por exemplo, para navegar na internet).



ENJOY SAFER TECHNOLOGY™