McAfee
Together is power.

Relatório sobre ameaças

McAfee Labs

Técnicas e tendências de evasão de malware

As técnicas de evasão de malware estão amplamente disponíveis e estão se tornando mais poderosas.

A história das técnicas de evasão

1980
Vírus Cascade
Primeiro vírus a utilizar criptografia para embaralhar seu conteúdo.

1990
Família de vírus Chameleon
Primeiros vírus polimórficos.

1998
Malware metamórfico
O Regswap utiliza metamorfismo por meio de registros diferentes para as mesmas funções.

Anos 1990
Compactadores
Compactadores que criptografam ou compactam dados popularizaram-se devido ao tamanho menor dos discos e RAM.

1999-2003
Rootkits
Em 1999 surge o primeiro rootkit para Windows, o NTRootkit, seguido pelo HackerDefender em 2003.

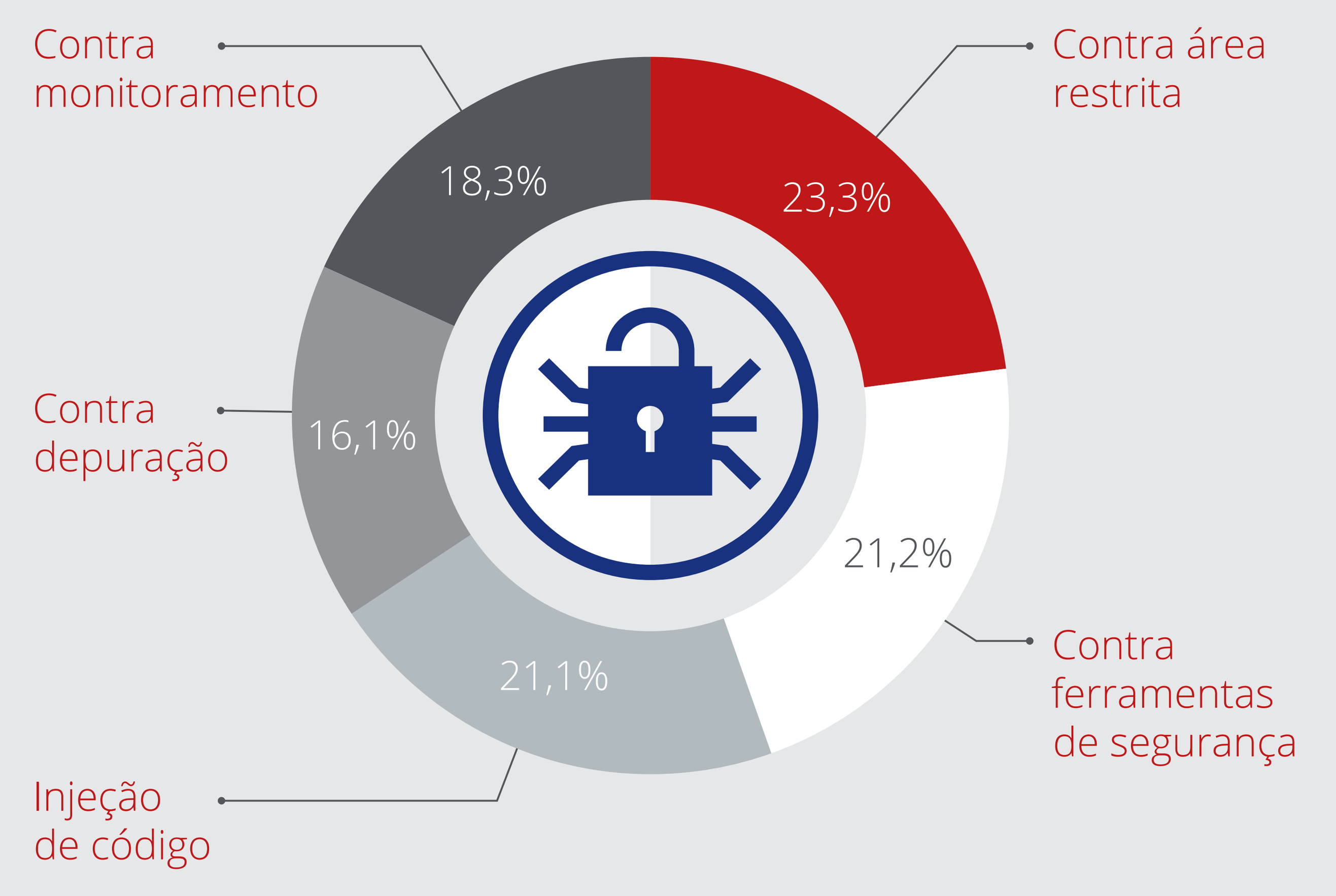
2008
Algoritmos de geração de domínios
O worm Conficker utiliza um algoritmo de geração de domínios (DGA) para evadir detecção de rede.

2011
Mercado de produtos prontos
Silkroad foi o primeiro mercado darknet a vender produtos e serviços para evasão de malware.

2015-2017
Dridex, Locky
Primeiros casos de ocultação em grande escala, uso de PowerShell e evasão de área restrita.

2015-2017
Malware de firmware
Vazamentos do Equation Group e do Hacking Team revelam o uso de malware de firmware para evitar detecção.

Uso de técnicas de evasão pelo malware



Evasão
O código das técnicas de evasão pode ser adquirido pronto, às vezes gratuitamente.

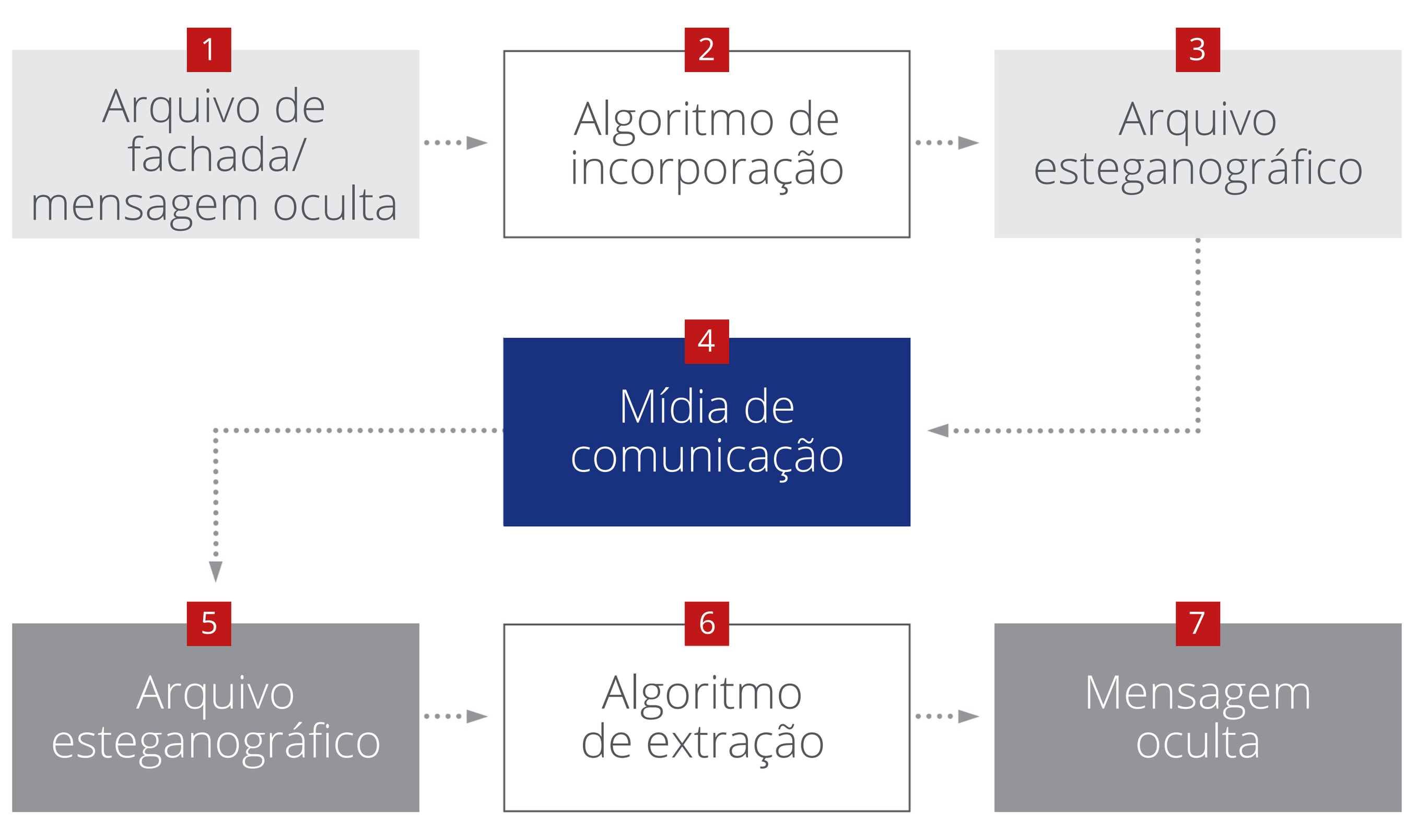
Firmware
A infecção de firmware é um método cada vez mais utilizado para evitar detecção.

Autoaprendizagem
Os atacantes estão desenvolvendo técnicas para evadir a segurança por autoaprendizagem.

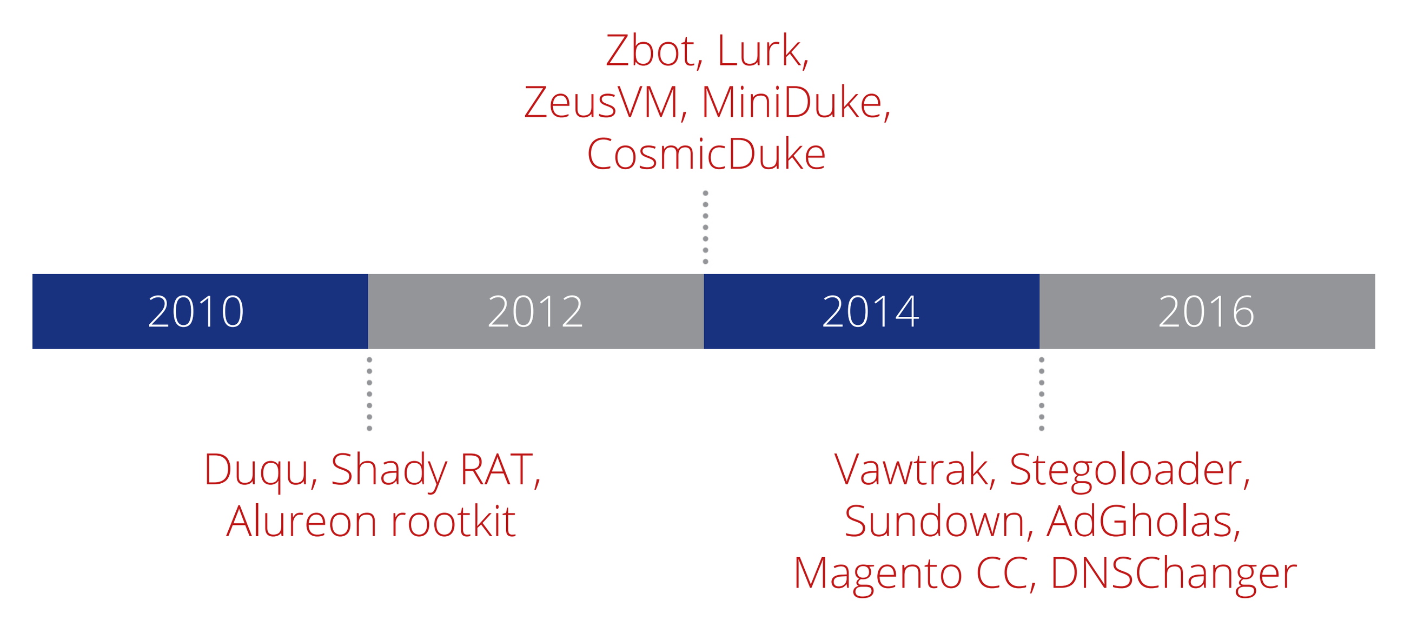
Escondido em plena vista: a ameaça oculta da esteganografia

Esteganografia — a arte e a ciência da ocultação de segredos.

O processo de esteganografia digital



Esteganografia digital no malware



Mensagem secreta
A esteganografia esconde uma mensagem secreta dentro de uma mensagem aparentemente legítima.

440 A.C.
A esteganografia tem sido utilizada de várias formas desde pelo menos 440 A.C.

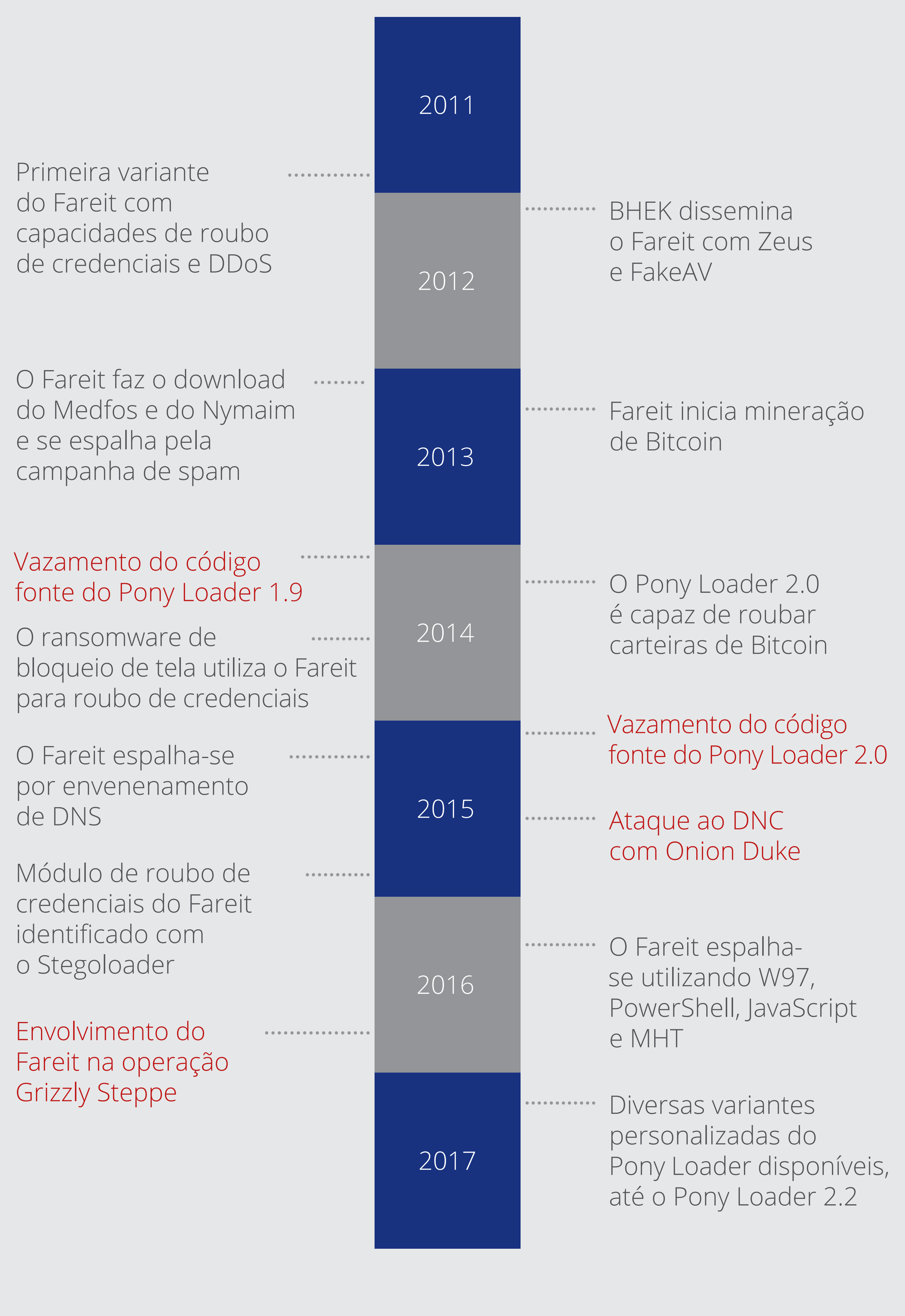
2011
A esteganografia digital foi utilizada pela primeira vez pelo Duqu em 2011.

Rede
Esteganografia de rede é o tipo mais recente de esteganografia digital utilizado por malware.

O perigo crescente do ladrão de senhas Fareit

Ladrões de senhas são utilizados nos estágios preliminares de praticamente todas as principais ameaças persistentes avançadas. O Fareit foi provavelmente utilizado na violação do Comitê Nacional do Partido Democrata (DNC) em 2016.

Evolução do Fareit



5.599
O Fareit foi descoberto em 2011. Houve 5.599 incidentes do Fareit com usuários no ano passado.

O Fareit tem diversas capacidades:

- Roubar senhas
- Fazer o download de outro malware e executá-lo
- Realizar ataques DDoS
- Roubar carteiras de criptomoedas
- Roubar credenciais de FTP

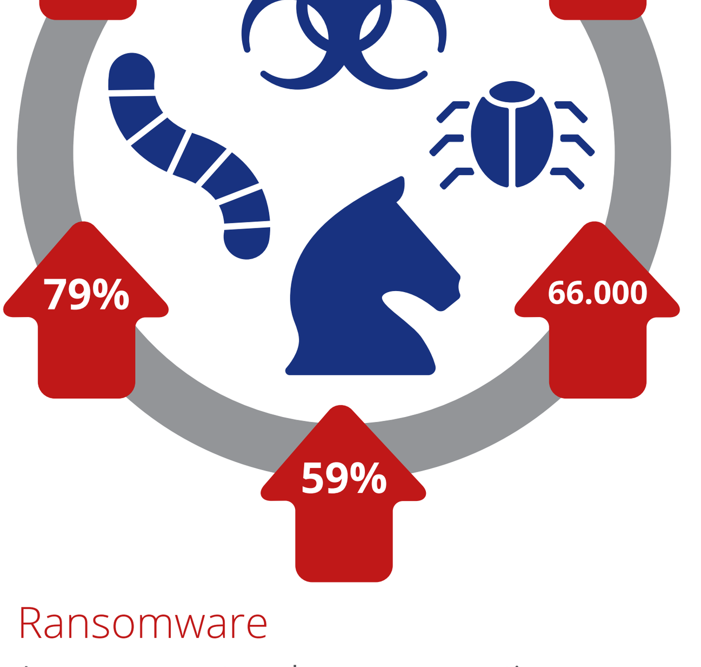
Estatísticas sobre ameaças

No primeiro trimestre, houve 244 novas ameaças a cada minuto, mais de quatro por segundo.

Incidentes
Contamos 301 incidentes de segurança divulgados publicamente no primeiro trimestre, um aumento de 53% em relação ao quarto trimestre. Os setores de saúde, serviços públicos e educação representaram mais de 50% do total. 78% de todos os incidentes de segurança divulgados publicamente no primeiro trimestre ocorreram nas Américas.

Malware
As novas amostras de malware tiveram uma recuperação no primeiro trimestre, chegando a 32 milhões. **O número total de amostras de malware aumentou 22% nos quatro trimestres passados, atingindo 670 milhões de amostras.**

Malware móvel
Os relatos de malware móvel da Ásia dobraram no primeiro trimestre, contribuindo para um aumento de 57% nas taxas globais de infecção. **O total de malware móvel cresceu 79% nos quatro trimestres passados, atingindo 16,7 milhões de amostras.**



Malware para Mac OS
Nos últimos três trimestres, o malware para Mac OS foi incrementado por uma enxurrada de adware. Embora ainda pequeno em comparação com as ameaças para Windows, **o número total de amostras de malware para Mac OS cresceu 53% no primeiro trimestre.**

Malware de macro
O malware de macro novo recuou para sua média de três anos. **66.000 novas amostras de malware de macro foram vistas no primeiro trimestre.**

Ransomware
As novas amostras de ransomware tiveram uma recuperação no primeiro trimestre, principalmente devido aos ataques do ransomware Congur contra dispositivos Android. **O número total de amostras de ransomware aumentou 59% nos quatro trimestres passados, atingindo 9,6 milhões de amostras.**

McAfee Global Threat Intelligence

O McAfee GTI recebeu, em média, 55 bilhões de consultas por dia no primeiro trimestre.

95 milhões
As proteções do McAfee GTI contra URLs de risco médio **caíram de 107 milhões por dia no quarto trimestre para 95 milhões por dia no primeiro trimestre** devido a um aumento na precisão.

56 milhões
As proteções do McAfee GTI contra programas potencialmente indesejados apresentaram um **aumento de 37 milhões por dia no quarto trimestre para 56 milhões por dia no primeiro trimestre.**

McAfee GTI

34 milhões
As proteções do McAfee GTI contra arquivos maliciosos **diminuíram de 71 milhões por dia no quarto trimestre para 34 milhões por dia no primeiro trimestre** devido à detecção antecipada de malware e a uma inteligência local melhor.

59 milhões
As proteções do McAfee GTI contra endereços IP arriscados **caíram de 88 milhões por dia no quarto trimestre para 59 milhões por dia no primeiro trimestre** devido à detecção antecipada.

Relatório do McAfee Labs sobre ameaças: junho de 2017

Visite www.mcafee.com/June2017ThreatsReport para ler o relatório completo.

McAfee
Together is power.

3181_0517_info-threat-report-malware-evasion