



Relatório sobre ameaças

McAfee Labs

Roubo de informações

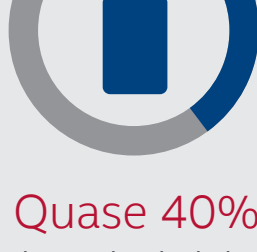
Vazamento de dados: o quê, como e quem.



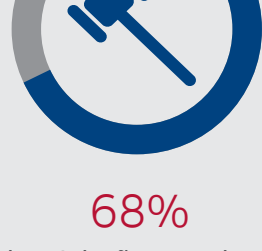
53% das violações são descobertas por alguém de fora da organização violada.



62% das violações envolvem dados pessoais de clientes ou funcionários.



Quase 40% das perdas de dados envolvem algum tipo de mídia física.



68% das violações envolvem perdas de dados que exigem relatórios regulamentares.



Mais de 25% das empresas não monitoram o acesso a informações de clientes ou funcionários.



Somente 37% das empresas utilizam monitoramento de endpoints, incluindo atividades dos usuários e mídias físicas.

Crise na sala de emergências

O ransomware infecta os hospitais.

Os autores de ransomware visam hospitais porque



Sistemas legados
Eles possuem sistemas legados com segurança fraca.

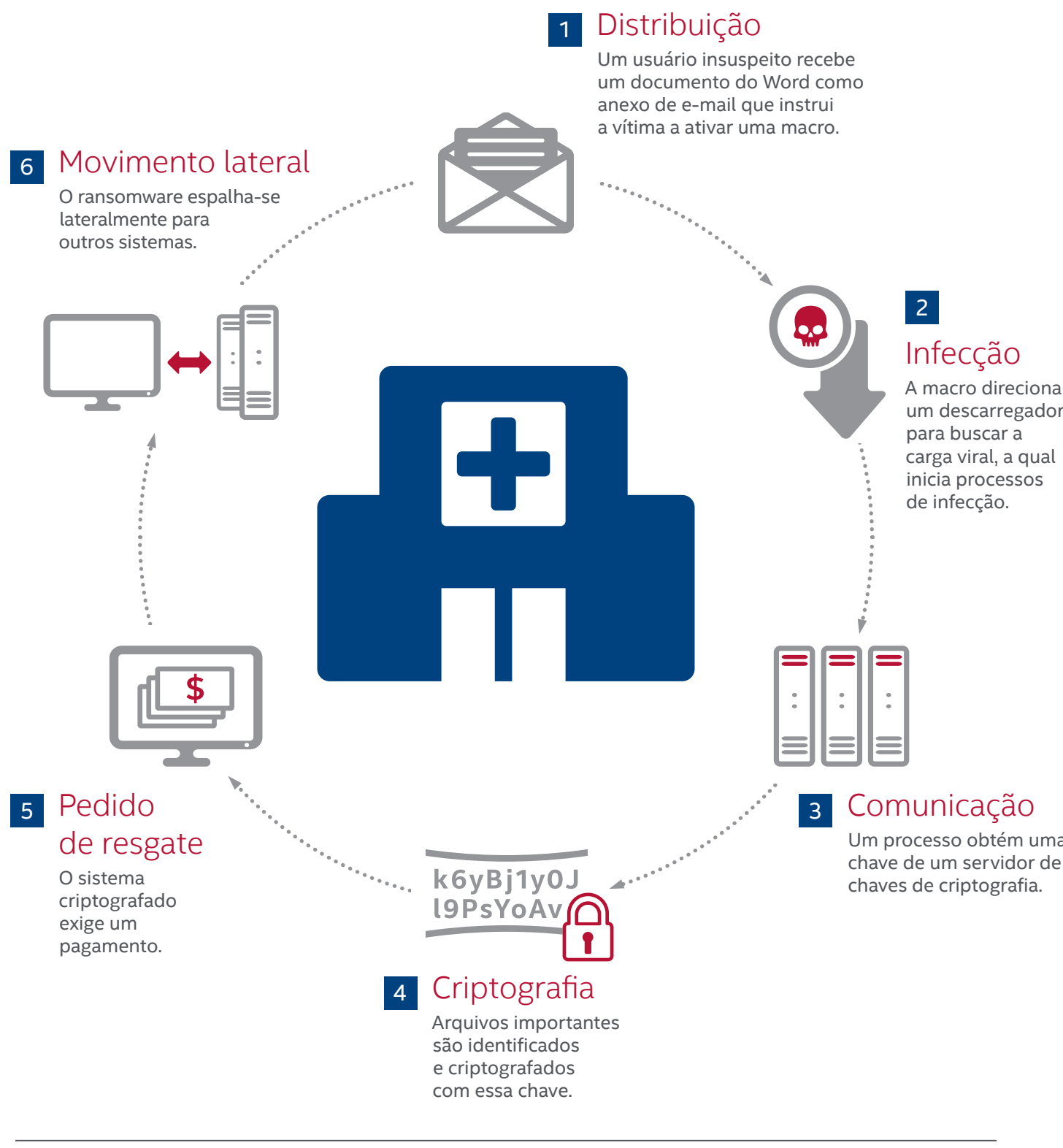


Dispositivos médicos
Eles possuem dispositivos médicos com segurança fraca ou nenhuma segurança.

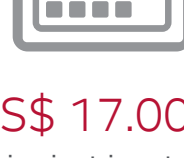


Atendimento aos pacientes
Eles precisam de acesso imediato às informações para oferecer o melhor atendimento possível aos pacientes.

Estágios de um ataque de ransomware contra um hospital



19 hospitais
Pelos menos 19 hospitais foram infectados por ransomware no primeiro e no segundo trimestres.



US\$ 17.000
No primeiro trimestre, um hospital da Califórnia (EUA) pagou US\$ 17.000 para restaurar seus arquivos e sistemas, sofrendo uma paralisação de cinco dias úteis.



US\$ 100.000
A Intel Security descobriu que um grupo relacionado de ataques direcionados contra hospitais gerou aproximadamente US\$ 100.000 em pagamentos de resgate no primeiro trimestre.

Análises

Uso de autoaprendizagem para deter os atacantes.

A autoaprendizagem consiste em uma automatização de análises que utilizam computadores para aprender ao longo do tempo.



Análise prescritiva
"Isto é recomendado porque aquilo vai acontecer."



Análise descritiva
"O que aconteceu?"

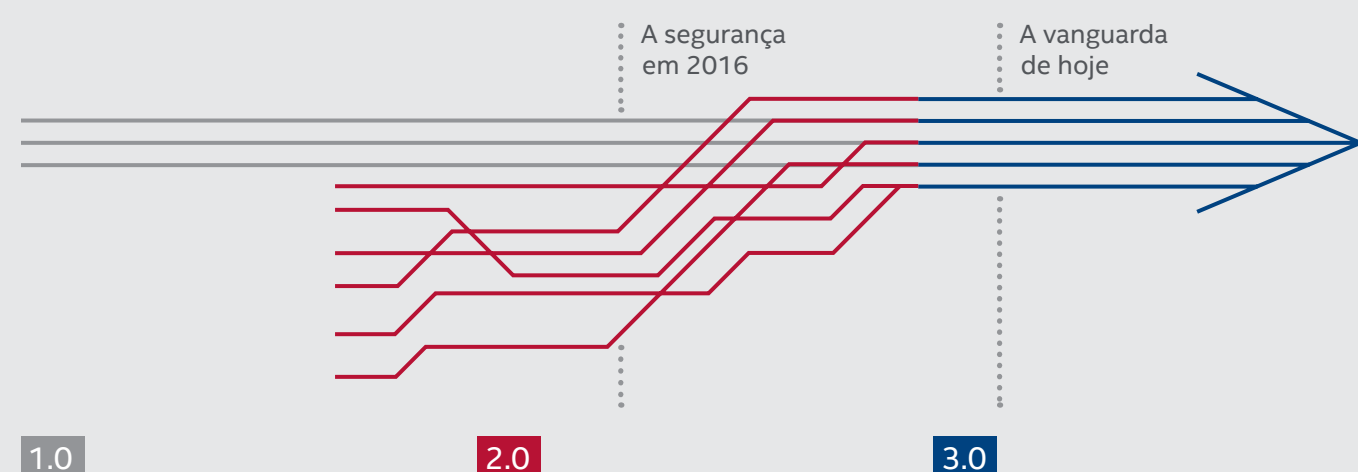


Análise preditiva
"O que vai acontecer?"



Análise de diagnóstico
"Por que isso aconteceu?"

A evolução da análise



1.0

Análise 1.0

- Conjuntos de dados estruturados e gerados internamente
- Análise descritiva e de diagnóstico
- Reativa, mas útil

2.0

Análise 2.0

- Big Data: dados em grande volume, complexos e desestruturados
- Dados de fontes internas e externas

3.0

Análise 3.0

- Utiliza autoaprendizagem com Big Data, aprendizagem profunda e computação cognitiva
- Descoberta e insights rápidos e proativos

Fonte: adaptado do International Institute for Analytics.

Estatísticas sobre ameaças

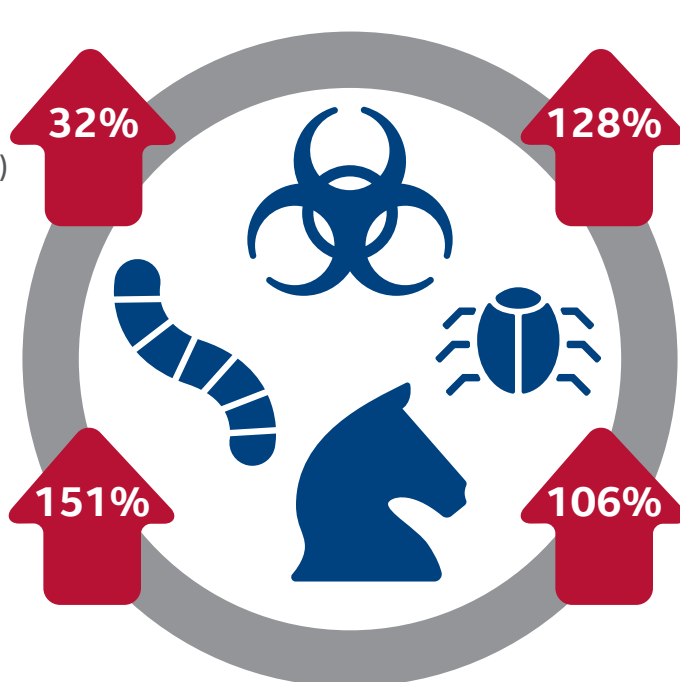
Surgem 316 novas ameaças a cada minuto ou mais de cinco por segundo.

Malware

A quantidade de novas amostras de malware no segundo trimestre (41 milhões) é a segunda maior já registrada. O "zoológico" de malware do McAfee Labs cresceu 32% no ano passado, chegando a 600 milhões de amostras.

Malware móvel

A quantidade de novas amostras de malware móvel (quase 2 milhões) foi a maior já registrada no segundo trimestre. O total de malware móvel cresceu 151% no ano passado.



Ransomware

A quantidade de novas amostras de ransomware (mais de 1,3 milhão) foi a maior já registrada no segundo trimestre. O total de ransomware cresceu 128% no ano passado.

Malware de macro

Os novos cavalos de Tróia descarregadores são responsáveis por um aumento de mais de 200% no novo malware de macro no segundo trimestre. O total de malware de macro cresceu 106% no ano passado.

McAfee Global Threat Intelligence

O McAfee GTI recebeu, em média, 48,6 bilhões de consultas por dia.



100 milhões
As proteções do McAfee GTI contra URLs maliciosos aumentaram levemente de um ano para outro, chegando a 100 milhões por dia no segundo trimestre.



30 milhões
As proteções do McAfee GTI contra programas potencialmente indesejados caíram 83% de um ano para outro, chegando a 30 milhões por dia no segundo trimestre.



104 milhões
As proteções do McAfee GTI contra arquivos maliciosos caíram 77% de um ano para outro, chegando a 104 milhões por dia no segundo trimestre.



29 milhões
As proteções do McAfee GTI contra endereços IP arriscados atingiram o mais alto número nos últimos dois anos, 29 milhões por dia, um aumento de 128% de um trimestre para outro.



Relatório do McAfee Labs sobre ameaças: Setembro de 2016

Visite www.mcafee.com/September2016ThreatsReport para ler o relatório completo.

