McAfee
Together is power.

Previsões sobre ameaças em 2019

McAfee Labs

Parceiros no crime cibernético

Os criminosos cibernéticos vão se associar entre si, criando famílias de malware como serviço em menor número, porém mais fortes.

Locais com toda sorte de ataques disponíveis

Os criminosos cibernéticos podem comprar malware, explorações, redes de bots e outros serviços ilícitos em mercados clandestinos. Criminosos com vários níveis de experiência e sofisticação podem lançar ataques facilmente.

Marcas fortes expandem seu alcance

Marcas cada vez mais poderosas impulsionarão uma mineração de criptomoedas mais sofisticada, além de aumentar o malware móvel e o roubo de credenciais e de cartões de crédito.

Consolidação do submundo

As famílias de malware como serviço trabalharão ativamente juntas. Tais alianças florescerão por meio de afiliações — por exemplo, kits de exploração impulsionando ransomware (GandCrab).

Exploração mais rápida

Os criminosos cibernéticos serão mais ágeis. Em 2019 eles explorarão vulnerabilidades de vida curta, reduzindo o tempo decorrido da detecção à armamentização.

Técnicas de evasão

O predomínio da terceirização de ataques levará ao uso de inteligência artificial em táticas de evasão.

Ferramentas de evasão

Ferramentas de compactação, encriptação e outras são componentes comuns para evitar detecção. Ao empregar inteligência artificial, os criminosos cibernéticos se tornarão mais ágeis e mais capazes de contornar as proteções.

Evasão ágil

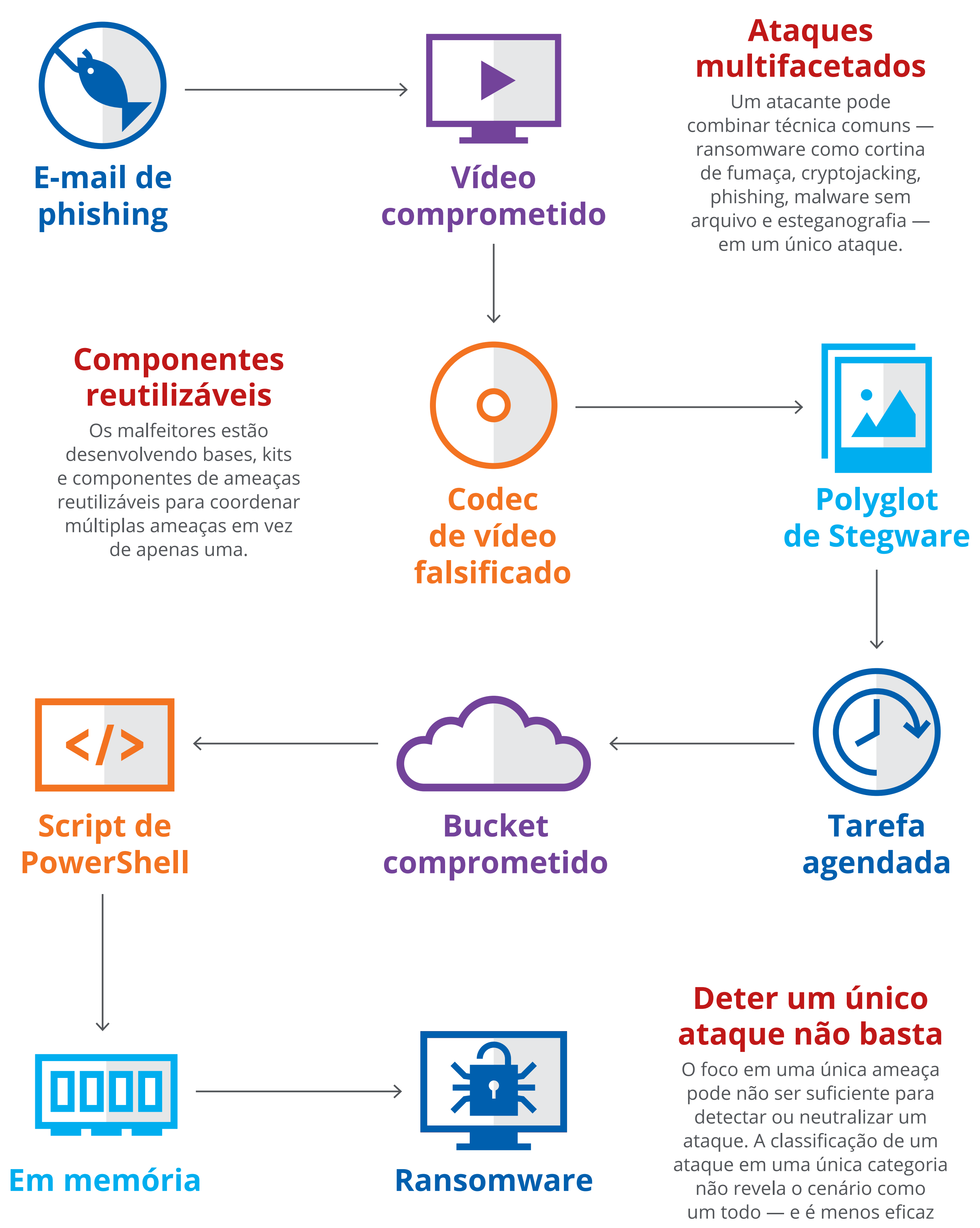
Exemplos de técnicas são um minerador de moedas que pare quando o Gerenciador de Tarefas é executado ou durante uma varredura, kits de exploração que utilizem injeção de processos ou manipulação do espaço de memória para inserir código, redes de bots que adicionem código ocultado para retardar uma engenharia reversa e APTs que usem certificados roubados para evitar detecção.

Inteligência artificial

Os criminosos utilizarão inteligência artificial para automatizar a seleção de alvos e verificar os ambientes infectados antes de distribuir os estágios mais avançados e, com isso, evitar detecção.

Que ataque é esse?

Ataques sinérgicos envolvendo múltiplas ameaças trabalhando juntas atuam como uma cortina de fumaça, impedindo os defensores de identificar o objetivo final do agressor.



E-mail de phishing

Vídeo comprometido

Codec de vídeo falsificado

Polyglot de Stegware

Tarefa agendada

Bucket comprometido

Script de PowerShell

Em memória

Ransomware

Ataques multifacetados

Um atacante pode combinar técnica comuns — ransomware como cortina de fumaça, cryptojacking, phishing, malware sem arquivo e esteganografia — em um único ataque.

Componentes reutilizáveis

Os malfeitores estão desenvolvendo bases, kits e componentes de ameaças reutilizáveis para coordenar múltiplas ameaças em vez de apenas uma.

Deter um único ataque não basta

O foco em uma única ameaça pode não ser suficiente para detectar ou neutralizar um ataque. A classificação de um ataque em uma única categoria não revela o cenário como um todo — e é menos eficaz em sua neutralização.

Os ataques de vazamento de dados vão visar a nuvem

Mais dados para roubar

Conforme as empresas dão continuidade à adoção plena de múltiplos modelos de nuvem (SaaS, PaaS, IaaS), a quantidade de dados que residem na nuvem atinge níveis recordes. Os ataques seguirão esses dados e serão cada vez mais direcionados contra esses serviços de nuvem.

Informações confidenciais

21% dos dados na nuvem são confidenciais — como propriedade intelectual e dados pessoais e de clientes — segundo o Relatório da McAfee sobre adoção de nuvem e riscos.

Ataques de interceptação

GhostWriter: aproveitou a nuvem como ponto de partida de ataques de interceptação nativos de nuvem **para lançar ataques de cryptojacking ou ransomware**.

Office 365 como alvo

KnockKnock: com a adoção crescente do Office 365, houve um surto de ataques — especialmente tentativas de comprometer e-mail, como **a rede de bots KnockKnock, que visou contas de sistema sem autenticação por múltiplos fatores**.

Assistentes digitais controlados por voz

Entrada nova para a casa

Os assistentes digitais controlados por voz, cada vez mais utilizados para gerenciar todos os dispositivos IoT de uma residência, serão um ponto de entrada preferencial para criminosos cibernéticos invadirem uma rede domiciliar.

Conexão pelo telefone

Os autores de malware vão se aproveitar de telefones e tablets para assumir o controle sobre dispositivos IoT quebrando senhas e explorando vulnerabilidades.

Dispositivo confiável

Como o tráfego vem de um dispositivo confiável, ele não parece suspeito e isso dificulta a identificação das rotas de ataque.

Falando alto

Atividades maliciosas, como abrir portas e conectar servidores de controle, poderão ser acionadas por comandos de voz do usuário (“Tocar música” e “Qual é a previsão do tempo para hoje?”).

Recrutamento de redes de bots

Dispositivos IoT infectados fornecerão redes de bots, as quais poderão lançar ataques DDoS, bem como roubar dados pessoais.

Plataformas de identidade e dispositivos periféricos sitiados

Plataformas de identidade de grandes proporções oferecem autenticação e autorização seguras e centralizadas de usuários, dispositivos e serviços em diversos ambientes de TI — e também um alvo para os criminosos.

Mídias sociais

Apesar do empenho cada vez maior por parte dos provedores de plataformas no que se refere à segurança, seus ambientes repletos de dados continuarão a ser um alvo lucrativo para os criminosos cibernéticos. Esse será o próximo grande campo de batalha.

Dispositivos periféricos

Os adversários continuarão a lançar ataques remotos contra dispositivos periféricos — qualquer hardware de sistema conectado em rede ou qualquer protocolo dentro de um produto de IoT — devido ao uso de senhas estáticas e segurança limitada.

Quebra de confiança

O modelo de confiança da IoT baseia-se em uma fundação frágil de confiança presumida e segurança de perímetro. A maioria dos dispositivos periféricos de IoT não possui autodefesa por padrão, bastando uma única exploração bem-sucedida para que o dispositivo seja capturado.

Proteção de nossos sistemas

A autenticação por múltiplos fatores e a inteligência de identidade tornar-se-ão os melhores métodos para oferecer segurança nessa guerra cada vez mais acirrada.

Ascensão da desinformação contra corporações

Campanhas de extorsão e notícias falsas (fake news) em mídias sociais, oriundas não só de estados-nação, mas também de grupos criminosos, atacarão marcas.

Conteúdo enganoso

Contas de redes de bots disseminam e promovem mensagens, frequentemente em AMBOS os lados de uma história para instigar debates. As mensagens de melhor desempenho são amplificadas ainda mais para extorquir as empresas, ao ameaçar suas marcas.

Disseminação rápida

Uma única conta de bot com 279 seguidores, em sua maioria outros bots, começou a assediar uma organização. Por amplificação, essa conta ganhou 1.500 seguidores adicionais em apenas quatro semanas, simplesmente tuitando conteúdo malicioso sobre seu alvo.

Leia a versão completa do *Relatório de previsões do McAfee Labs sobre ameaças*
Visite: www.mcafee.com/2019Predictions
para ler o relatório completo.

McAfee
Together is power.

Dezembro de 2018