Resumo de solução

Detenha o vazamento de dados

Certifique-se de que as "joias da coroa" estejam a salvo.

No **Relatório do McAfee Labs sobre ameaças: agosto de 2015**, abordamos em profundidade uma das etapas fundamentais do processo de roubo de dados: o vazamento de dados. Essa etapa consiste no ladrão ou perpetrador mover ou copiar dados da rede do proprietário para uma rede sob controle do atacante.

Nos últimos dez anos, o setor teve um crescimento sem precedentes em violações de dados e no volume de pessoas e organizações afetadas. As violações, que antes apenas coletavam números de cartões de crédito e de débito, agora roubam praticamente qualquer tipo de informação que colocamos on-line: nomes, datas de nascimento, endereços, números de telefones, informações de assistência médica, credenciais de contas e muito mais.

Infelizmente, pessoas não são os únicos alvos. A ciberespionagem praticada por governos de países, organizações criminosas e hacktivistas coloca em risco dados confidenciais de pessoas e organizações de qualquer lugar.

Os perpetradores de ameaças e suas motivações

Um perpetrador de ameaças é um indivíduo ou grupo que tenta obter acesso não autorizado a sistemas e redes de computadores. Na comunidade de segurança, tais ameaças são classificadas em três categorias principais: governos de países, crime organizado e hacktivistas. A tabela a seguir lança alguma luz sobre as motivações e possíveis tipos de dados que são valiosos para eles.

	Governos de países	Crime organizado	Hacktivistas
Razões em geral	Espionagem Influência	Ganho financeiro	Reputacionais Sociais
Exemplos de tipos de dados	Código-fonte E-mails Documentos internos Atividades militares Informações de identificação pessoal (PII) de funcionários do governo	Informações de contas bancárias Dados de cartões de crédito PII (incluindo números de identidade e dados de assistência médica)	E-mails Informações de funcionários Quaisquer dados internos confidenciais
Volume dos dados procurados	Pequeno a grande	Grande	Pequeno a grande
Sofisticação das técnicas de vazamento	Alta	Média a baixa	Média a baixa
Localização da rede	Desconhecida/ frequentemente dispersa	Conhecida	Tanto conhecida quanto desconhecida/ frequentemente dispersa

intel Security

Dados-alvo

Uma vez que um sistema da rede é comprometido por um atacante, este começa a explorar outros sistemas para descobrir os que abrigam os dados desejados. Uma rede complexa contém muitos tipos de dados, o que torna o processo demorado para qualquer perpetrador sem conhecimento privilegiado, aumentando as chances de detecção. Devido a isso, os atacantes tentam ser tão furtivos e persistentes quanto possível.

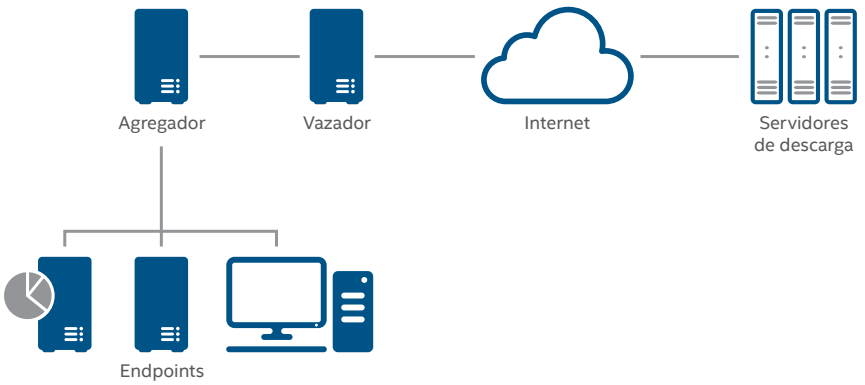
Os principais dados-alvo são:

Dados-alvo	Tipos de dados	Perpetradores interessados
Sistemas de banco de dados	Informações protegidas sobre saúde (PHI), informações de identificação pessoal (PII), cartões de crédito, dados bancários e contas de usuários	Crime organizado e hacktivistas
Repositórios de código-fonte	Código-fonte, credenciais e chaves	Governos de países e hacktivistas
Sistemas especializados	Variam	Todos, dependendo do tipo de endpoint
Compartilhamentos de arquivos e sistemas semelhantes	Código-fonte, projetos, comunicações, etc.	Governos de países e hacktivistas
E-mail e comunicações	Projetos e comunicações	Governos de países e hacktivistas

Vazamento de dados

Uma vez que perpetradores de ameaças tenham localizado e obtido os dados desejados, começa a parte mais difícil da tarefa: o vazamento do tesouro. Os atacantes tiram proveito do ambiente do host para atuar como intermediários entre as redes da vítima e do atacante. Essa infraestrutura atuante pode ser simples ou complexa, dependendo do quão profundos e segmentados estão os dados-alvo na rede. Algumas das funções que os sistemas podem adotar na infraestrutura atuante podem envolver:

- **Endpoints:** dados-alvo simples ou múltiplos no mesmo segmento ou em um segmento roteável para o agregador.
- **Agregador:** atua como um ponto de coleta para os dados dos endpoints-alvo e transfere os dados para o vazador. O agregador pode ou não ter acesso à Internet. Em campanhas sofisticadas, múltiplos agregadores podem transferir dados para vários vazadores para ocultar o caminho de saída dos dados.
- **Vazador:** pega dados de um agregador e promove a transferência dos mesmos para o servidor de descarga do atacante. Pode ser uma transferência simples ou o vazador pode hospedar os dados para que o atacante os apanhe.



Arquitetura típica de vazamento de dados.

Independentemente de ser um trabalho simples ou complexo, o objetivo do atacante é transferir os dados visados para um servidor que esteja fora da rede da vítima. Servidores de descarga são os primeiros pontos nos quais as informações roubadas residem fora do controle da vítima e podem ser facilmente acessadas pelos atacantes. Esses servidores podem ser:

- **Sistemas comprometidos:** sistemas que foram comprometidos pelo atacante durante uma campanha separada. Esses sistemas podem ser de qualquer tipo, desde blogs pessoais no WordPress a servidores pertencentes a empresas com parcos controles de segurança.
- **Sistemas hospedados em países específicos:** países com leis rigorosas sobre privacidade são atraentes para os atacantes porque estes podem hospedar sistemas sem serem incomodados e ainda ter um certo nível de proteção.
- **Sistemas hospedados temporariamente:** sistemas de vida curta hospedados na nuvem através de provedores como Amazon Web Services, Digital Ocean ou Microsoft Azure.
- **Serviços de compartilhamento de arquivos na nuvem:** sites de compartilhamento de arquivos on-line de uso geral, como DropBox, Box.com ou Pastebin.
- **Serviços hospedados em nuvem:** outros serviços baseados na Internet, como Twitter e Facebook, que permitem aos usuários postar dados.

Transportadores de dados

Transportadores de dados são os protocolos e métodos que os ladrões usam para copiar dados de um lugar ou sistema para outro, sejam de interno para interno (de endpoint para agregador) ou de interno para externo (de vazador para servidor de descarga). Veja a seguir um resumo dos protocolos de transporte mais comuns:

Transportador	Descrição	Interno	Externo
HTTP/HTTPS	O predomínio do HTTP nas comunicações em rede torna-o um protocolo ideal para ocultação de dados vazados em meio a outros tipos de tráfego. Ele é utilizado como transportador de vazamentos em geral por meio da incorporação de comandos em cabeçalhos de HTTP e dentro de métodos GET/POST/PUT.		■
FTP	O FTP frequentemente está disponível em servidores corporativos e é de fácil interação por meio de comandos nativos do sistema, o que o torna um transportador descomplicado.	■	■
USB	Dispositivos de armazenamento USB são frequentemente utilizados para vazamento de dados entre redes fisicamente isoladas (air-gap). Vimos exemplos de malware que procuram por um dispositivo de armazenamento USB de um determinado fabricante e, então, copiam os dados a serem vazados para um setor oculto do dispositivo. Quando o dispositivo é colocado em um outro sistema infectado com acesso à rede, o vazamento tem início. Dispositivos de armazenamento USB também podem ser utilizados por elementos internos para copiar grandes quantidades de dados e removê-los fisicamente da organização.	■	■
DNS	Registros de DNS específicos, como TXT ou mesmo A e CNAME podem, até certo ponto, armazenar dados. Com o controle de um domínio e um servidor de nomes, um atacante pode transmitir pequenas quantidades de dados fazendo pesquisas específicas no sistema do vazamento.		■
Tor	O uso da rede Tor está se tornando mais popular. Ela permite que os atacantes postem dados vazados em servidores de difícil rastreamento. Contudo, o tráfego Tor em redes corporativas raramente é legítimo e, portanto, pode ser facilmente detectado e interrompido.		■
SMTP/e-mail	Servidores de SMTP, da empresa ou não, podem ser utilizados para enviar dados para fora da organização na forma de anexos ou no corpo de mensagens de e-mail.		■
SMB	SMB é um protocolo extremamente comum em ambientes Microsoft Windows que pode já estar ativado nos sistemas.	■	

Transportador	Descrição	Interno	Externo
RDP	O protocolo RDP possibilita diversas atividades, como copiar/colar, compartilhamento de arquivos e, em alguns casos, sistemas que permitem o RDP podem ficar expostos à Internet.	■	■
Transportadores personalizados	Transportadores personalizados são ocasionalmente utilizados em comunicações de servidores de controle e malware sofisticado. Um transportador robusto demanda muito trabalho e sua natureza peculiar torna o protocolo fácil de identificar na rede — fazendo a balança pender para um transportador mais consolidado.	■	■

Manipulação de dados

Os atacantes fazem tudo o que podem para não revelar suas intenções a suas vítimas ao manusear e vazar dados confidenciais. A manipulação dos dados antes de sua transferência pode ajudar a evitar detecções, a reduzir o tempo da transferência e até a tornar mais demorada a detecção. Algumas das técnicas comuns nesse estágio:

Técnica	Descrição
Compactação	A utilização do formato de arquivo ZIP padrão não apenas proporciona um grau de ocultação, como também acelera as transferências de arquivos.
Organização em blocos (chunks)	A divisão dos dados em pequenas partes antes do envio ajuda a esconder a transferência em meio à atividade normal da rede.
Codificação/ocultação	O tipo mais comum de manipulação de dados é um algoritmo básico de codificação ou ocultação. Com técnicas simples, como realizar uma operação XOR com uma chave estática, codificação Base64 ou simplesmente converter cada caractere em hexadecimal, os dados podem ser manipulados apenas o suficiente para evitar detecção.
Criptografia	É surpreendente que nem sempre se use criptografia durante o vazamento. Talvez isso se deva ao baixo desempenho ou apenas por não haver necessidade. Quando utilizada, a criptografia mais comum é RC4 ou AES.

Como a Intel Security pode ajudá-lo a se proteger contra vazamento de dados

McAfee DLP Discover

A primeira etapa para proteger adequadamente os dados é compreender onde residem as informações e o que são exatamente esses dados. O **McAfee DLP Discover** protege contra vazamento de dados simplificando essa primeira etapa através das seguintes capacidades:

- **Identificar e controlar informações confidenciais:** inventário e indexação de todo o conteúdo com a varredura automatizada do McAfee DLP Discover de todos os recursos disponíveis, o que permite compreender os seus dados confidenciais, onde quer que eles residam. Com o McAfee DLP Discover, você pode consultar e garimpar informações para saber como elas são utilizadas, a quem pertencem, onde são armazenadas e para onde se propagaram.
- **Revisão e correção de violações:** descobre violações de conteúdo, registra e gera assinaturas e envia notificações de alerta para proteger os dados confidenciais com mais eficácia. A integração com fluxos de trabalho de gerenciamento de casos e resposta a incidentes limita a proliferação de material confidencial.
- **Fácil definição de políticas de proteção:** oferece gerenciamento, geração de relatório e criação de políticas unificadas e intuitivas para proporcionar mais controle sobre a sua estratégia de proteção da informação.

McAfee DLP Monitor

O **McAfee DLP Monitor** coleta, rastreia e gera relatórios sobre dados transmitidos em toda a rede. Você pode descobrir com facilidade ameaças desconhecidas aos dados, tomar providências para protegê-los e assegurar que a sua empresa não sofra uma grande violação.

- **Examine o tráfego de rede:** examine o tráfego de rede em um nível mais profundo com a capacidade de varredura e análise de dados do McAfee DLP Monitor, líder do setor.
- **Identifique os dados rapidamente:** a descoberta em tempo real permite ver em detalhes como os dados estão sendo usados, quem os está usando e para onde estão indo, fornecendo informações suficientes com base nas quais agir. O McAfee DLP Monitor identifica com rapidez mais de 300 tipos de conteúdo sendo transportados por qualquer porta ou protocolo, garantindo visibilidade para a sua empresa.
- **Faça análises forenses detalhadas:** realiza análises forenses para correlacionar eventos de risco atuais e passados, detectar tendências de risco e identificar ameaças. O McAfee DLP Monitor permite que você entenda a situação rapidamente e desenvolva regras e políticas para lidar com o problema.

McAfee DLP Prevent

O **McAfee DLP Prevent** protege contra a perda de dados assegurando que os dados só deixem a rede quando for apropriado, seja por e-mail, webmail, mensagens instantâneas, wikis, blogs, portais, HTTP/HTTPS ou transferências FTP. Frequentemente, a capacidade de identificar e mitigar tentativas de vazamento com rapidez é a diferença entre manter seus valiosos dados seguros e fazer parte do próximo grande escândalo.

- **Visibilidade para incidentes de segurança:** proporciona visualizações resumidas e detalhadas dos incidentes de segurança e de suas ações de mediação através de visualizações personalizadas e relatórios de incidentes.
- **Imponha proativamente o cumprimento das políticas para todos os tipos de informações:** imponha políticas para informações reconhecidamente confidenciais e também para informações não tão óbvias que você talvez desconheça. Com uma ampla gama de políticas internas, que incluem desde a conformidade e o uso aceitável até a propriedade intelectual, você pode fazer a correspondência de documentos parciais ou integrais com um conjunto de regras para proteger todas as suas informações confidenciais.

McAfee DLP Endpoint

O **McAfee DLP Endpoint** permite monitorar e evitar instantaneamente o vazamento de dados nas dependências da empresa, fora dela e na nuvem. Monitore rapidamente eventos em tempo real, aplique políticas de segurança com gerenciamento centralizado e gere relatórios de proliferação e forenses detalhados sem prejudicar as operações do dia a dia.

- **Suporte aprimorado para virtualização:** impõe uma política específica por usuário para múltiplas sessões e infraestruturas de desktop virtual, proporcionando flexibilidade e melhor controle sobre os dados que fluem para terminais compartilhados.
- **Geração de relatórios e monitoramento de incidentes abrangentes:** coleta todos os dados necessários, como remetente, destinatário, data/hora e evidências de rede para devida análise, investigação e auditoria — bem como avaliações de riscos e correção.
- **Console de gerenciamento centralizado:** aproveita o console de gerenciamento do McAfee® ePolicy Orchestrator® (McAfee ePO™) para definir políticas, distribuir e atualizar agentes, monitorar eventos em tempo real e gerar relatórios para atender requisitos de conformidade.
- **Gerenciamento abrangente de conteúdo:** controla e bloqueia a cópia de dados confidenciais para dispositivos USB, unidades flash, smartphones e outros dispositivos de armazenamento removíveis, incluindo mídias óticas e cópias impressas. A integração do DLP com o gerenciamento de direitos digitais estende a proteção para além da sua rede.

McAfee Device Control

O **McAfee Device Control** protege contra vazamento de dados via mídias e dispositivos de armazenamento removíveis, como unidades USB, smartphones, CDs e DVDs. Ele permite que a sua organização monitore e controle transferências de dados de todos os desktops e laptops, independentemente da localização, nas dependências da empresa ou fora dela. O McAfee Device Control conta com recursos de bloqueio de dispositivos com reconhecimento de conteúdo e contexto, como:

- **Gerenciamento abrangente de dispositivos e dados:** controla como os usuários da sua organização copiam dados para unidades USB, smartphones, CDs e DVDs graváveis e muitos outros dispositivos que podem ser utilizados para vazamento de dados.
- **Controles granulares:** especificam quais dispositivos podem ou não ser utilizados e quais dados podem ou não ser copiados nos dispositivos permitidos, além de impedir os usuários de copiar dados de locais e aplicativos específicos.
- **Capacidades avançadas de geração de relatórios e auditoria:** simplificam a conformidade com registros detalhados em nível de usuário e de dispositivo. Detalhes como dispositivo, data/hora e evidências de dados são facilmente registrados e relatados como suporte a consultas de conformidade e auditoria.
- **Gerenciamento centralizado:** oferece monitoramento de eventos em tempo real e gerenciamento centralizado de incidentes e políticas através da integração com o software McAfee ePO.

McAfee Next Generation Firewall

Proteja-se contra vazamento de dados ou ataques que utilizam técnicas avançadas de evasão com o **McAfee Next Generation Firewall**. O McAfee Next Generation Firewall realiza uma inspeção profunda de pacotes especializada, bem como a normalização de pilha completa e inspeção com base em fluxos de dados horizontais, para expor as anomalias de tráfego, como comunicações entre o malware e seu servidor de controle ou tentativas de vazamento de informações da sua rede.

- **Derrota técnicas avançadas de evasão:** usa funções de normalização do tráfego de múltiplas camadas, impressões digitais com base em vulnerabilidades e correspondência de impressão digital independente de protocolo.
- **Detecta atividades de servidores de controle:** usa detecção com base em descriptografia e análise de sequência de tamanho de mensagem para detectar atividades de redes de bots e servidores de controle.
- **Bloqueia com base na localização geográfica:** nega conexões de entrada e saída a países com os quais a sua empresa não faz negócios. Isso reduz as possibilidades de que comandos de servidores de controle sejam recebidos de IPs que não têm motivos para se comunicar com o seu ambiente.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com