CENÁRIO DE AMEAÇAS GERAIS

BAIXE AQUI O RELATÓRIO COMPLETO EM INGLÊS

O Talos observou várias tendências importantes no cenário de ameaças em 2022. De acordo com a telemetria e os estudos de caso entre os engajamentos de resposta a incidentes do Cisco Talos, observamos os agentes de ameaças que incorporam versões violadas/vazadas de ferramentas conhecidas de red-teaming, usando living-off-the-land binaries (LoLBins), como o PowerShell e o Microsoft PS Exec, e um aumento nos ataques de USB.

FERRAMENTAS DE DUPLA UTILIZAÇÃO

O desenvolvimento de ferramentas mal-intencionadas consome muitos recursos e pode permitir que um agente de ameaça seja rastreado. Para contornar esses custos elevados e fornecer uma camada adicional de anonimato, muitos oponentes recorrem a estruturas ofensivas e de red-team para oferecer suporte a uma série de ações em todo o ciclo de vida de um ataque.

O Cobalt Strike continua sendo uma opção conhecida para agentes de ameaças cibernéticas (Figura 1). Essa ferramenta legítima de defesa de rede e software de emulação de ameaças tem uma variedade de recursos, inclusive reconhecimento, atividade pós-exploração e diversas simulações de ataque, o que a torna uma ferramenta altamente funcional para oponentes.

O Talos e a comunidade de segurança lidam com o Cobalt Strike há anos, desenvolvendo continuamente detecções melhores e mais robustas. Ao longo do ano, também vimos agentes de ameaças se adaptarem a esses desenvolvimentos, recorrendo a outras estruturas ofensivas, como o Sliver e o Brute Ratel (Figura 2).

Além disso, o Talos descobriu duas estruturas ofensivas separadas, desenvolvidas por agentes de ameaças para seus próprios fins, chamadas de "Manjusaka" e "Alchimist". O Alchimist já está sendo usado em livre circulação e, embora não tenhamos observado o uso generalizado do Manjusaka até o momento, ele tem o potencial de ser adotado por agentes de ameaças em todo o mundo.

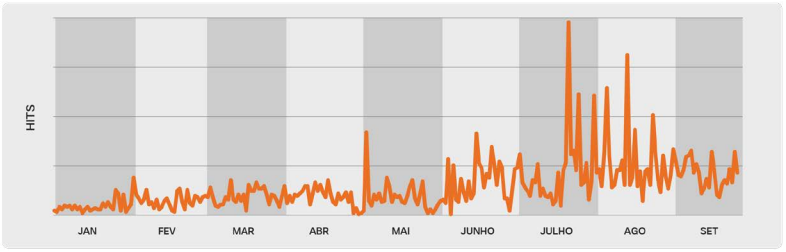

Figura 1. *Detecções do Cisco Secure Endpoint para uso do pipe nomeado Cobalt Strike.*

Cobalt Strike

- Uma ferramenta legítima de defesa de rede e um software de emulação de ameaças que tem uma variedade de recursos, inclusive reconhecimento, atividade pós-exploração e diversos pacotes de ataque, o que a torna uma ferramenta altamente funcional para oponentes.
- Beacon é o payload do Cobalt Strike para gerar ataques e criar tráfego de saída em HTTP, HTTPS ou DNS. Os beacons do Cobalt Strike podem ser comparados ao Meterpreter, que faz parte da estrutura Metasploit, e usados por testadores de penetração e pesquisadores de segurança ofensiva ao fornecer os serviços.

Brute Ratel

- Uma ferramenta de red-teaming legítima e avançada, lançada em 2020 como ferramenta de simulação de ataque. Desde então, tem sido utilizado por agentes de ameaças para facilitar vários estágios do ciclo de vida do ataque.
- O Brute Ratel foi criado especificamente para evitar que seja detectado por soluções de detecção e resposta de endpoint (EDR) e antivírus (AV).

Sliver

- Uma estrutura de red-teaming de código aberto e uma ferramenta de simulação de ataque que pode ser usada para realizar testes de segurança. Os implantes do Sliver são compilados dinamicamente com chaves de criptografia assimétricas por binário e são compatíveis com C2 em vários protocolos (mTLS, HTTP, DNS).
- Os implantes do Sliver são compatíveis com MacOS, Windows e Linux. O Sliver apresenta várias funcionalidades, inclusive payloads preparados e sem etapas, geração de código dinâmico, dinâmicas de pipe nomeado, execução de assembly do .NET de memória e muito mais.

Figura 2. *Comparação de ferramentas de duplo uso.*

CENÁRIO DE AMEAÇAS GERAIS

LIVING-OFF-THE-LAND BINARIES

Os living-off-the-land binaries (LoLBins) são ferramentas e utilitários legítimos pré-instalados em um sistema operacional, normalmente utilizados pelos oponentes. Como são ferramentas inerentemente confiáveis usadas para atividades de rotina, os defensores da rede podem não perceber os ataques que utilizam os LoLBins, ao monitorar comportamentos mal-intencionados. Continuamos a ver oponentes utilizarem ferramentas e utilitários legítimos em todos os estágios de um ataque para oferecer suporte às operações.

De acordo com nossa telemetria, 4 das 25 assinaturas mais ativas do Cisco Secure Endpoint Behavioural Protection estão relacionadas ao PowerShell, destacando a dependência constante dos agentes de ameaças no uso desse utilitário nativo do Windows para fins mal-intencionados (Figura 3). Os oponentes geralmente usam o PowerShell para oferecer suporte a uma ampla gama de atividades, inclusive a instalação de adware, como o ChromeLoader, o download de mineradores de criptomoeda ou a exploração de vulnerabilidades em software, como o Elasticsearch.

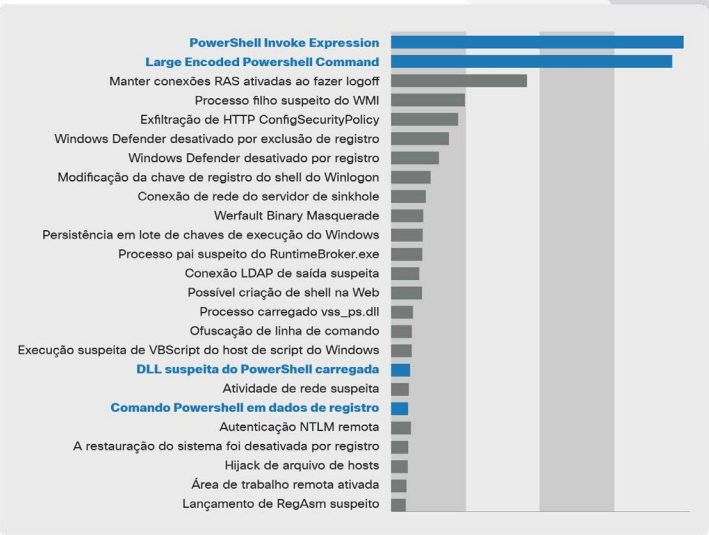

***Figura 3.** As 25 principais assinaturas mais ativas da Cisco Secure Endpoint Behavioural Protection.*

AMEAÇAS USB

A propagação de malware por meio de dispositivos de armazenamento removíveis remonta aos dias das unidades de disquete. Ao longo de 2022, o Talos observou um aumento nas detecções no Cisco Secure Malware Analytics para vários comportamentos associados a USBs e unidades externas, destacando que os oponentes fazem uso contínuo dessa tática antiga, mas eficaz. Esses comportamentos incluem a gravação de executáveis em uma unidade USB ou a configuração de atributos ocultos para arquivos em uma unidade USB para que não sejam detectados (Figuras 4 e 5).

O aumento pode ser parcialmente explicado pelo malware Raspberry Robin, que é disseminado entre dispositivos usando unidades USB compartilhadas. No entanto, observou-se também que os grupos de APT usam o acesso à unidade USB como parte dos ataques.

O ano de 2022 mostrou que os ataques USB estão de volta e que os oponentes adaptarão suas táticas para tirar proveito das empresas, desviando a atenção delas dos vetores de ataque mais antigos.

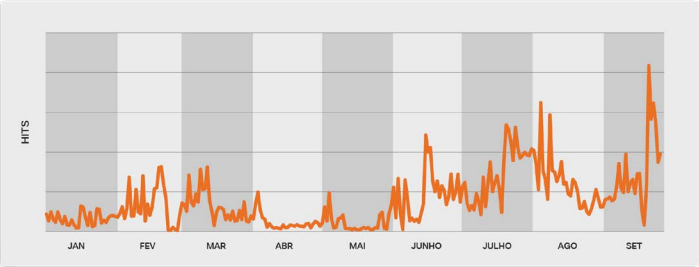

***Figura 4.** Detecções do Cisco Secure Malware Analytics para executáveis gravados em USB.*

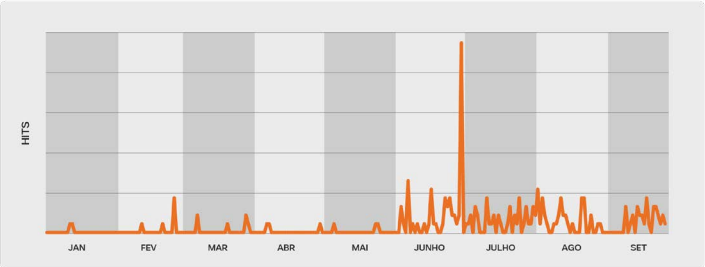

***Figura 5.** Detecções do Cisco Secure Malware Analytics para definir atributos ocultos para arquivos em um USB.*

