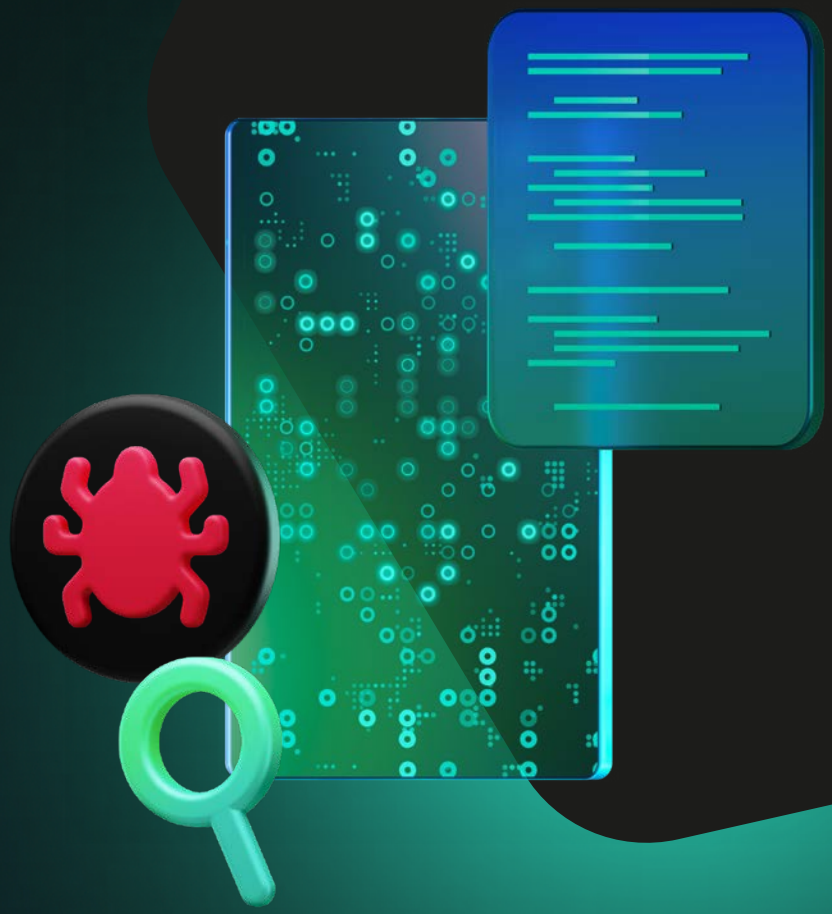
kaspersky



Busca ao IoC em ação: técnicas práticas de pivotagem

Este artigo foi escrito por Damir Shaykhelislamov, um funcionário que trabalha no departamento de Soluções de segurança especializadas da Kaspersky. Ele explora a importância da pivotagem do IoC na identificação proativa de ameaças moderna e demonstra como passar da detecção básica do IoC para a construção de uma imagem mais ampla da atividade nefasta.

O artigo inclui exemplos do mundo real que ajudarão os analistas a enriquecer indicadores e otimizar fluxos de trabalho com inteligência de ameaças, como:

- Pivotagem baseada em infraestrutura (por exemplo, IPs, domínios, certificados SSL)
- Descoberta de artefatos de malware usando sandboxing e análise de código
- Atribuição de ameaças e mapeamento de TTP com estruturas como MITRE ATT&CK

Essas e outras técnicas fornecem uma abordagem estruturada para transformar indicadores isolados em percepções que podem ser colocadas em prática, para que os analistas possam fazer mais detecções, responder mais rapidamente e se antecipar às ameaças cibernéticas.

A importância da busca a IoCs

Perder um único indicador no cenário de ameaças atual pode significar perder uma violação inteira. Portanto, a busca a indicadores de comprometimento (IoCs) continua sendo uma defesa importante da segurança cibernética, apesar dos avanços na análise comportamental.

IoCs são rastros digitais, como endereços IP suspeitos, hashes de arquivos maliciosos ou modificações de registro que atuam como pistas que levam à descoberta de um ataque maior.

Mas, a identificação de um IoC é apenas o começo. A verdadeira habilidade está na pivotagem: a expansão de uma única pista em uma rede mais ampla de indicadores relacionados. Essa técnica permite que os analistas descubram a infraestrutura oculta do invasor, detectem movimentações laterais e conectem eventos díspares a narrativas de ameaças coesas.

Embora a abrangência desses métodos em diferentes tipos de indicadores seja vasta (muito além do escopo deste artigo), os exemplos a seguir destacam abordagens práticas e impactantes que podem ser aplicadas pelos analistas.

Inteligência de ameaças como o principal facilitador

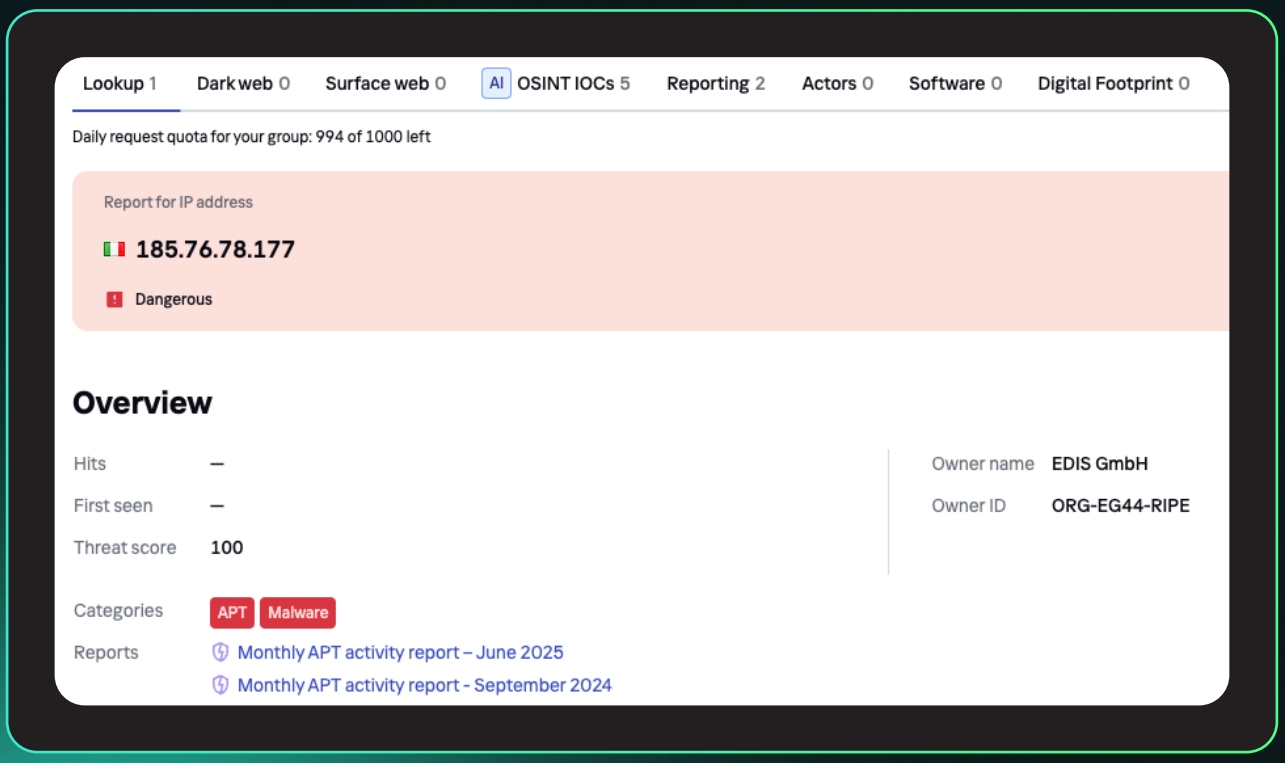
A pivotagem e a inteligência de ameaças (TI) estão profundamente interconectadas. A pivotagem extrai valor da inteligência de ameaças, enquanto a TI fornece o contexto e o enriquecimento que tornam a pivotagem eficaz. As plataformas modernas de TI oferecem capacidades automatizadas de correlação, visualização e enriquecimento que simplificam os fluxos de trabalho de pivotagem.

Fluxos de trabalho de pivotagem comuns

Endereço IP para domínios

Um cenário comum envolve a investigação de um endereço IP suspeito que foi sinalizado em alertas de segurança. Por exemplo, os alertas podem realçar consultas DNS para o endereço IP 185.76.78.177. A consulta de fontes de DNS passivo (pDNS) pode ajudar a identificar domínios historicamente associados a esse IP.

Para avaliar sua relevância, verifique a reputação do domínio usando plataformas de TI e pesquise qualquer tráfego relacionado a esse domínio nos seus logs internos de DNS e proxy.



Relatório de pesquisa de ameaças para endereços IP suspeitos: Portal do Kaspersky Threat Intelligence

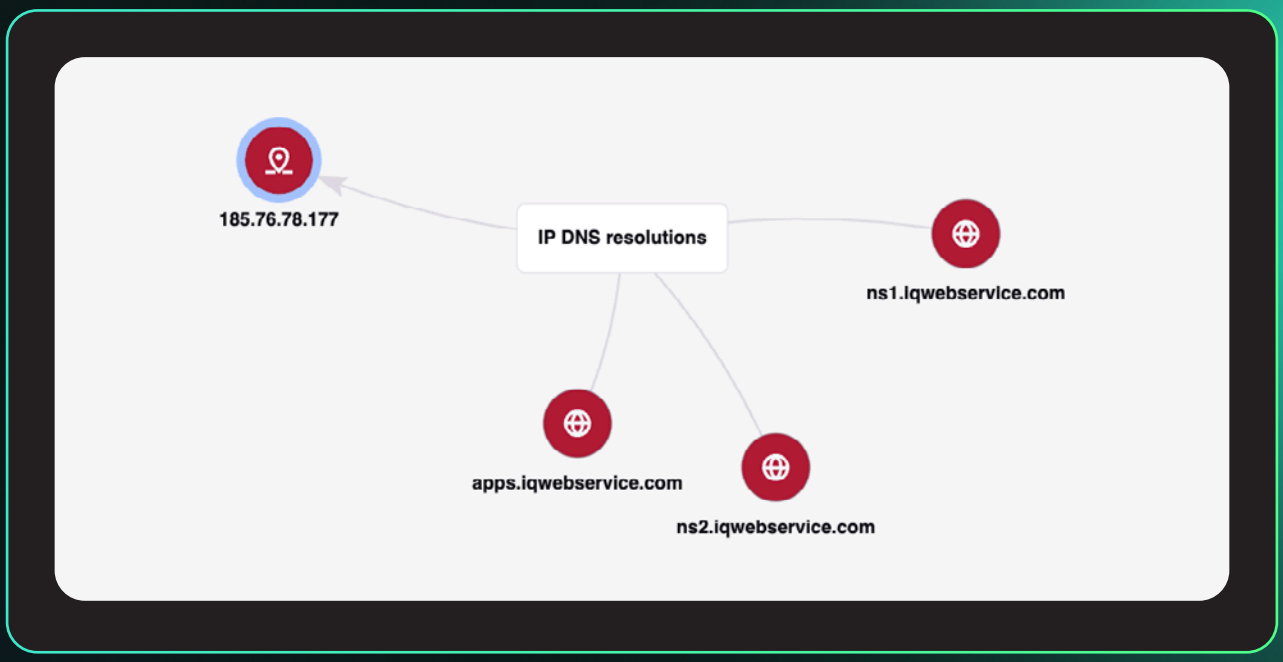


Gráfico de resolução de DNS passivo para o IP 185.76.78.177 - Portal do Kaspersky Threat Intelligence

Endereço IP para amostras de malware

Um endereço IP suspeito identificado em logs e alertas de rede pode exigir uma investigação mais aprofundada. A pivotagem do IP pode ajudar a determinar se ele está:

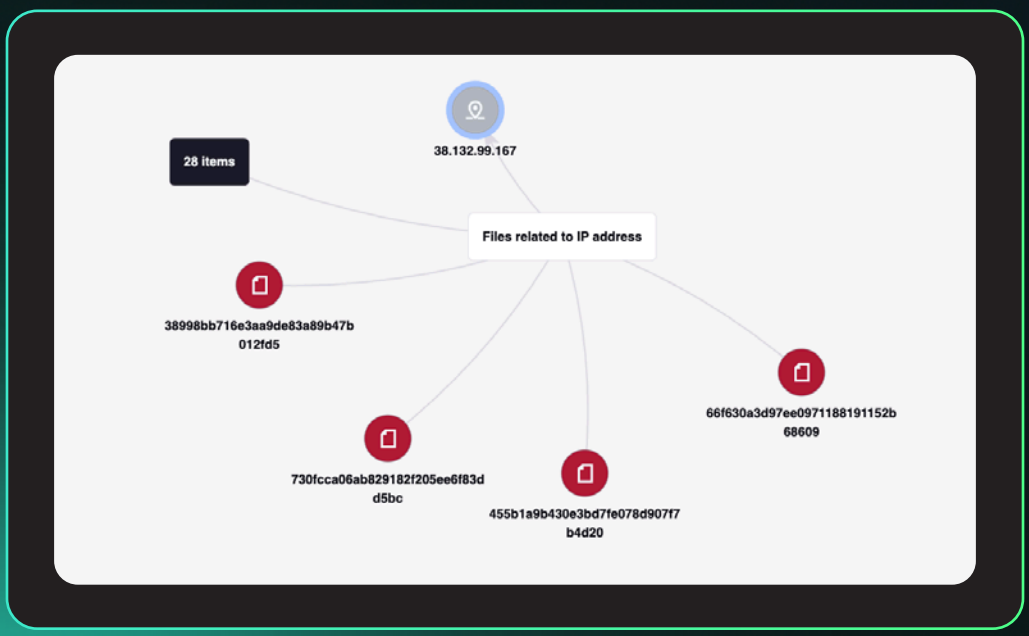
1

Hospedando amostras de malware conhecidas

2

Funcionando como um servidor de comando e controle (C2), etc.

As plataformas de TI públicas e comerciais fornecem capacidades suficientes para correlacionar endereços IP com atividades de malware observadas e campanhas relacionadas.



Hashes de arquivo associados ao IP 38.132.99.167 - Portal do Kaspersky Threat Intelligence

Certificados SSL

Os certificados SSL/TLS servem como pontos de pivotagem muito valiosos na identificação proativa de ameaças. Os agentes de ameaças frequentemente reutilizam certificados em vários servidores e domínios na sua infraestrutura, e geralmente recorrem a autoridades certificadoras gratuitas, como a Let's Encrypt, que fornecem emissão automatizada com validação mínima.

Pode-se repetir os mesmos campos de assunto do certificado em diferentes domínios e campanhas. Um padrão reutilizado típico pode ser semelhante a: "C=US, ST=Califórnia, L=San Francisco, O=Microsoft Corporation, OU=Divisão de Segurança, CN=(nome de domínio)", em que o Nome Comum (CN) é alterado, mas os detalhes organizacionais permanecem os mesmos.

Isso cria fortes oportunidades de pivotagem, permitindo que os analistas identifiquem endereços IP que anteriormente hospedavam servidores usando certificados com padrões de assunto idênticos ou semelhantes.

Além dos certificados, os metadados de handshake TLS, incluindo impressões digitais JA3, JA3S e JARM, podem ser usados para pivotar e agrupar a infraestrutura do invasor. Esses valores servem como impressões digitais exclusivas que identificam como um cliente ou servidor se comunica por TLS. Os agentes de ameaças geralmente reutilizam as mesmas configurações ou estruturas de malware em vários servidores, produzindo impressões digitais idênticas ou quase idênticas.

Por exemplo, pesquisar a assinatura JA3 **b742b407517bac9536a77a7b0fee28e9**, que corresponde à estrutura Cobalt Strike C2, e combinar essa impressão digital em conjuntos de dados de telemetria de rede ou inteligência de ameaças pode revelar hosts mal-intencionados adicionais operados pelo mesmo adversário.

Domínio → Registro TXT DNS

Embora os domínios sejam um ponto de partida comum nas investigações de IoC, consultar seus registros TXT DNS associados oferece uma oportunidade de pivotagem poderosa e, muitas vezes, negligenciada. Os comandos de consulta DNS podem ser usados nativamente, sem a necessidade de malware. Ao pivotar de um domínio suspeito para seu registro TXT, os analistas podem:

Extrair domínios adicionais, endereços de fallback do C2 ou comandos de botnet.

Recuperar chaves ou tokens de criptografia.

Detectar padrões de abuso de DNS, como tunelamento ou entrega furtiva de carga útil.

Remontar fragmentos de arquivo ou componentes de carga útil.

Exemplo: uma investigação em um domínio de phishing descobre um registro TXT com IPs codificados em base64 para servidores C2 de backup, permitindo que o SOC os bloqueie antes de serem ativados.

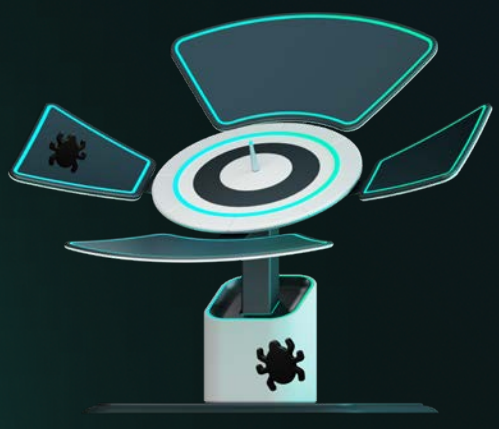
Padrões de temporização de beacon

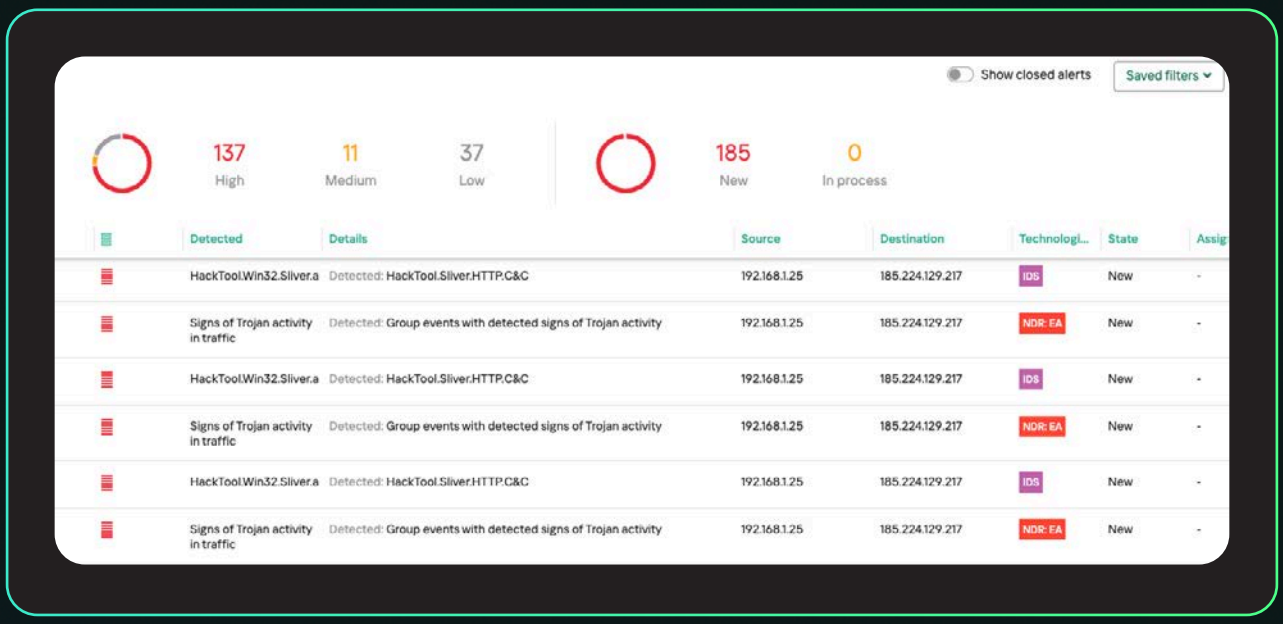
Beacons são sinais periódicos enviados por hosts comprometidos para seus servidores C2. Esses sinais atuam como um "batimento cardíaco", indicando uma infecção ativa e permitindo que o invasor mantenha o controle.

Os beacons geralmente ocorrem em intervalos consistentes ou semi-consistentes, por exemplo, a cada poucos minutos, o que se destaca em relação à variabilidade típica da rede. Para evitar a detecção direta, os invasores podem adicionar uma leve randomização (jitter) aos intervalos de beacon. No entanto, a análise de padrões estatísticos como o intervalo médio e o desvio padrão ainda pode revelar algo suspeito.

Ao analisar intervalos médios e jitter, os analistas podem detectar anomalias e pesquisar logs em busca de padrões correspondentes, descobrindo hosts infectados adicionais ou malware relacionado.

Exemplo: durante uma investigação de incidentes, os analistas observam conexões de rede de saída ocorrendo em intervalos regulares, um padrão consistente com um perfil de beacon Sliver C2.





Padrão de beacon Sliver C2 regular detectado - Kaspersky Anti Targeted Attack Platform (NTA)

Dos marcadores de código à expansão de IoCs

O binário contém traços de código distintos, ou "marcadores genéticos", vinculados a um ataque direcionado conhecido ou campanha APT. Ao adotar uma abordagem de atribuição de ameaças, como o Kaspersky Threat Attribution Engine (KTAE), os analistas podem comparar esses fragmentos de código com um repositório de amostras de malware avançadas.

Para operacionalizar essas percepções, os analistas podem criar regras YARA com base nos padrões de código identificados, permitindo a detecção automatizada de binários semelhantes em sistemas internos, repositórios de malware ou ambientes de sandbox. Essa análise pode revelar IoCs adicionais, ajudando a identificar amostras relacionadas implementadas no ambiente ou remanescentes de atividades de ataque anteriores.

Isso representa uma forma de pivotagem de atribuição baseada em código, em que marcadores binários exclusivos são rastreados até campanhas APT conhecidas, facilitando a descoberta de IoCs vinculados e a reconstrução dos rastros históricos dos ataques.

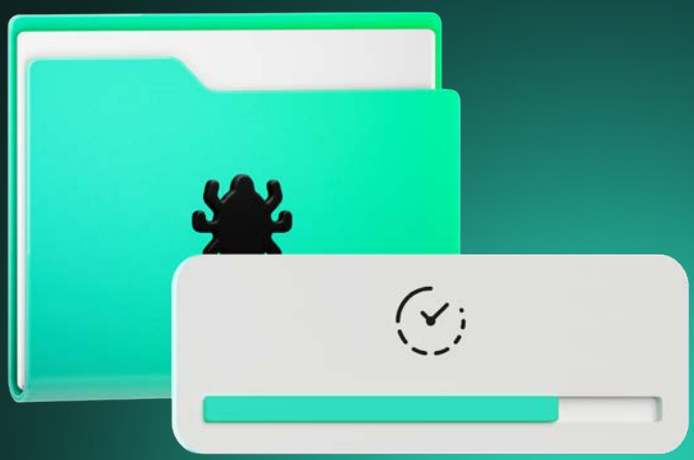
Pivotagem de artefatos de sandbox

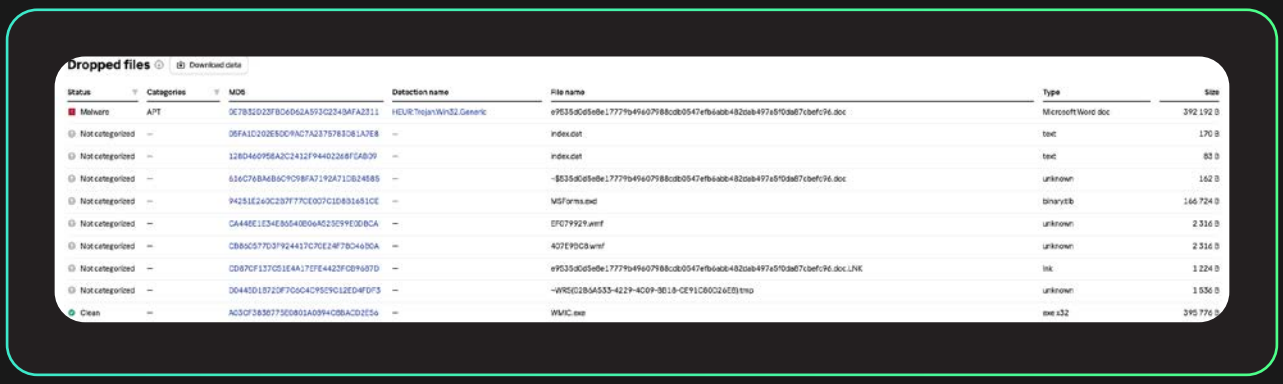
Alguns indicadores de comprometimento (IoCs) só surgem quando um objeto suspeito é executado em um ambiente controlado. Muitas ameaças modernas não têm arquivos ou são realizadas em etapas, o que significa que a carga útil inicial é benigna ou mínima, enquanto o comportamento mal-intencionado real é acionado de forma dinâmica durante a execução.

Ao executar esses objetos em uma sandbox, os analistas podem observar comportamentos de tempo de execução, incluindo comunicações de saída, arquivos gerados, modificações de registro e atividade de processo, que não são visíveis apenas por meio de análise estática. Eles podem então usar esses artefatos comportamentais para gerar novos IoCs, enriquecendo a inteligência de ameaças e expandindo a abrangência da detecção em todo o ambiente.

Um endereço de hash/URL de arquivo pode servir como ponto de partida para identificar artefatos adicionais. A pesquisa por meio de um hash de arquivo (MD5, SHA1, SHA256) ou endereço de URL é uma das técnicas de pivotagem mais eficazes na análise de inteligência de ameaças e malware.

Quando um arquivo malicioso é executado em uma sandbox, ele geralmente gera objetos adicionais no disco (arquivos executáveis, DLLs, scripts, configurações). Eles geralmente fazem parte de um ataque realizado em várias etapas.





Hashes de arquivo gerados da amostra analisada (**0e7b32d23fbd6d62a593c234bafa2311**) - Portal do Kaspersky Threat Intelligence

Saber o que foi gerado ajuda a determinar a extensão do incidente, entender a cadeia de eliminação do ataque e desenvolver regras YARA com base nas assinaturas, nomes e características comportamentais dos arquivos gerados.

Chave de registro para mapeamento TTP (MITRE ATT&CK)

Modificações de registro que enfraquecem as defesas do sistema ou expõem dados confidenciais geralmente são exemplos de IoCs fortes. Um exemplo comum é a alteração maliciosa das configurações de autenticação do **WDigest**, que permite o armazenamento de credenciais de texto simples na memória do sistema. Essa alteração aparentemente pequena pode aumentar de forma drástica a superfície de ataque, permitindo que os adversários extraiam senhas em texto não criptografado diretamente do LSASS (Serviço de Subsistema de Autoridade de Segurança Local).

Por padrão, as versões modernas do Windows desativam o **WDigest (UseLogonCredential = 0)** para evitar esse risco. No entanto, quando um invasor modifica o registro e define esse valor como 1, o sistema começa a armazenar em cache as credenciais do usuário na memória, fornecendo aos invasores um caminho direto para o roubo de credenciais por meio de ferramentas como o Mimikatz.

Esses IoCs baseados em registro podem revelar a intenção e a técnica do invasor. Para contextualizar esses IoCs dentro do comportamento conhecido do adversário, o MITRE ATT&CK Navigator pode ser utilizado. Por exemplo, um IoC de acesso a credenciais, como o **UseLogonCredential = 1** em WDigest, corresponde diretamente à técnica T1003.001 - Despejo de credenciais do SO: memória do LSASS.

Ferramentas como EDR e SIEM são úteis para detectar IoCs e mapeá-los para táticas adversárias.

Aceleração da descoberta de IoC por meio da IA

Embora a pivotagem tradicional dependa muito da experiência do analista, a IA pode trazer escala ao processo:

Correlação automatizada: os modelos de aprendizado de máquina podem vincular IoCs relacionados em conjuntos de dados massivos em segundos, mesmo quando os indicadores diferem ligeiramente (por exemplo, variações de subdomínio, anomalias de certificado).

Descoberta de padrões: a IA pode detectar padrões de infraestrutura recorrentes que foram ignorados pela busca manual.

Redução de ruído: modelos inteligentes filtram falsos positivos, permitindo que os analistas se concentrem nos pivôs de alto risco mais prováveis.

A combinação da experiência humana para validação e IA faz com que as descobertas de IoC sejam mais rápidas e precisas.

Exemplo de pivotagem aplicado

A pivotagem de um único hash pode expor um caminho de infecção completo, permitindo tanto a contenção quanto o enriquecimento do IoC. Suponha que uma equipe de operações de segurança detecte um arquivo executável suspeito ("agent.exe") em um endpoint do departamento financeiro. O hash exclusivo para este arquivo é sinalizado pelo sistema EDR. Os analistas enviam o hash para plataformas de inteligência de ameaças, que o vinculam a uma família de malware conhecida especializada em roubo de dados e tunelamento DNS. O relatório de inteligência de ameaças identifica os hashes relacionados, os domínios associados (por exemplo, "corp-updates[.]com") e as campanhas anteriores que utilizam DNS para exfiltração.

Com os indicadores enriquecidos do pivô de hash, os analistas consultam os logs DNS em busca de domínios suspeitos e padrões de subdomínio longos e aleatórios vinculados a "corp-updates[.]com". Eles observam centenas de solicitações de DNS de saída de vários endpoints para subdomínios longos e aleatórios de "corp-updates[.]com.". O padrão se assemelha a técnicas de exfiltração de DNS bem documentadas, em que o malware codifica dados roubados em subdomínios de solicitação de DNS.

Os analistas montam a linha do tempo:

O ataque de spear phishing entregou um documento malicioso que gerou o arquivo "agent.exe".

O agente coletou arquivos confidenciais e os exfiltrou via DNS, combinando isso com consultas normais.

A análise de hash e IoC relacionada descobriu mais endpoints infectados ao consultar “helper[.]corp-updates[.]com” e “auditlogs[.]corp-backups[.]com”.

O SOC bloqueia todas as solicitações de saída para "corp-updates[.]com" e domínios relacionados na camada de firewall e isola todas as máquinas com hashes correspondentes ou consultas DNS suspeitas para realizar uma revisão forense.

Resumo

A pivotagem do IoC é **cíclica e iterativa**. Cada novo indicador pode levar à descoberta de outros. Seja por meio de indicadores estáticos, como hashes e domínios de arquivos, ou artefatos dinâmicos surgidos durante as execuções de sandbox, a pivotagem permite que os analistas rastreiem a infraestrutura do invasor, descubram infecções relacionadas e enriqueçam a telemetria interna.

Desafio do analista: selecione um IoC de uma investigação recente (de preferência uma vinculada à atividade maliciosa confirmada) e divida-o em pelo menos três dimensões: infraestrutura (por exemplo, DNS passivo, JA3/JA3S), artefatos de malware (por exemplo, arquivos gerados em sandbox, correspondências YARA) e comportamento do adversário (por exemplo, mapeamento MITRE ATT&CK TTP).

No entanto, apesar de seus pontos fortes, a pivotagem do IoC tem limitações:

Indicadores de curta duração: os indicadores (por exemplo, domínios C2) são alternados com frequência e a infraestrutura do invasor pode desaparecer em poucas horas.

Falsos positivos: comuns ao confiar em feeds comunitários sem verificar as informações.

Sobrecarga de informações: a pivotagem pode gerar dados excessivos.

Técnicas de evasão: adversários sofisticados usam cada vez mais a entrega de cargas úteis maliciosas criptografadas, domain fronting e ofuscação em tempo de execução.

Portanto, embora a pivotagem do IoC tenha um papel significativo nas estratégias de detecção e resposta, ela deve ser complementada por análises comportamentais, detecção de anomalias e identificação proativa de ameaças baseada em TTP.

Sobre a Kaspersky

A Kaspersky é uma empresa de privacidade digital e segurança cibernética global fundada em 1997. Com mais de um bilhão de dispositivos protegidos contra ameaças cibernéticas emergentes e ataques direcionados, a inteligência de ameaças profunda e a expertise em segurança da Kaspersky estão constantemente se transformando em soluções e serviços inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. O portfólio abrangente de segurança da empresa inclui proteção de endpoint líder, produtos e serviços de segurança especializados, bem como soluções de imunidade cibernética para combater ameaças digitais sofisticadas e em constante evolução. Ajudamos mais de 200.000 clientes corporativos a proteger o que mais importa para eles. Saiba mais em www.kaspersky.com.

www.kaspersky.com.br