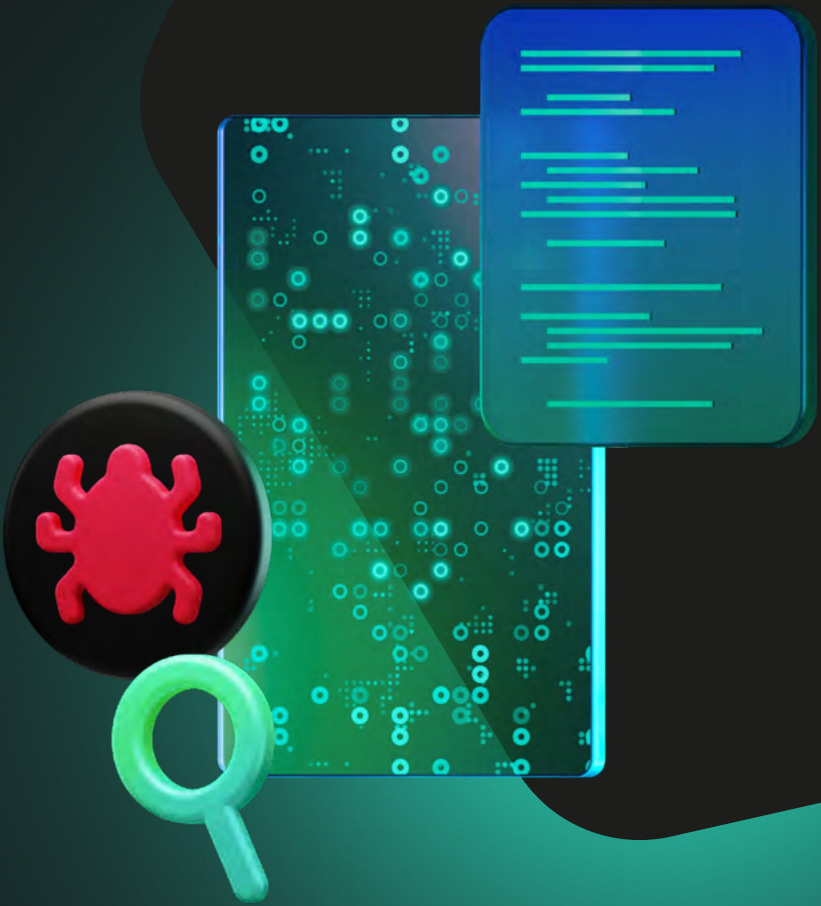
kaspersky



IoC hunting in action: practical pivoting techniques

This article was written by Damir Shaykhelislamov, an employee working within Kaspersky's Expert Security Solutions department. It explores the importance of IoC pivoting in modern threat hunting and demonstrates how to move from basic IoC detection to building a broader picture of nefarious activity.

The article includes real-world examples that will help analysts to enrich indicators and optimize workflows with threat intelligence, such as:

- Infrastructure-based pivoting (e.g., IPs, domains, SSL certificates)
- Malware artifact discovery using sandboxing and code analysis
- Threat attribution and TTP mapping with frameworks such as MITRE ATT&CK

These, among other, techniques provide a structured approach to turn isolated indicators into actionable insights, so analysts can detect more, respond faster and get ahead of cyberthreats.

Importance of IoC hunting

Missing a single indicator in today's threat landscape can mean missing a breach entirely. Indicator of compromise (IoC) hunting therefore remains a key cybersecurity defense, despite advances in behavioral analytics.

IoCs are digital traces such as suspicious IP addresses, malicious file hashes or registry modifications that act as breadcrumbs leading to a larger attack surface.

But identifying an IoC is only the beginning. The real skill lies in pivoting: the expansion of a single clue into a broader network of related indicators. This technique allows analysts to uncover hidden attacker infrastructure, detect lateral movement and connect disparate events into cohesive threat narratives.

While the range of these methods across different types of indicators is vast (far beyond the scope of this article), the following examples highlight practical, impactful approaches that analysts can apply.

Threat intelligence as the key enabler

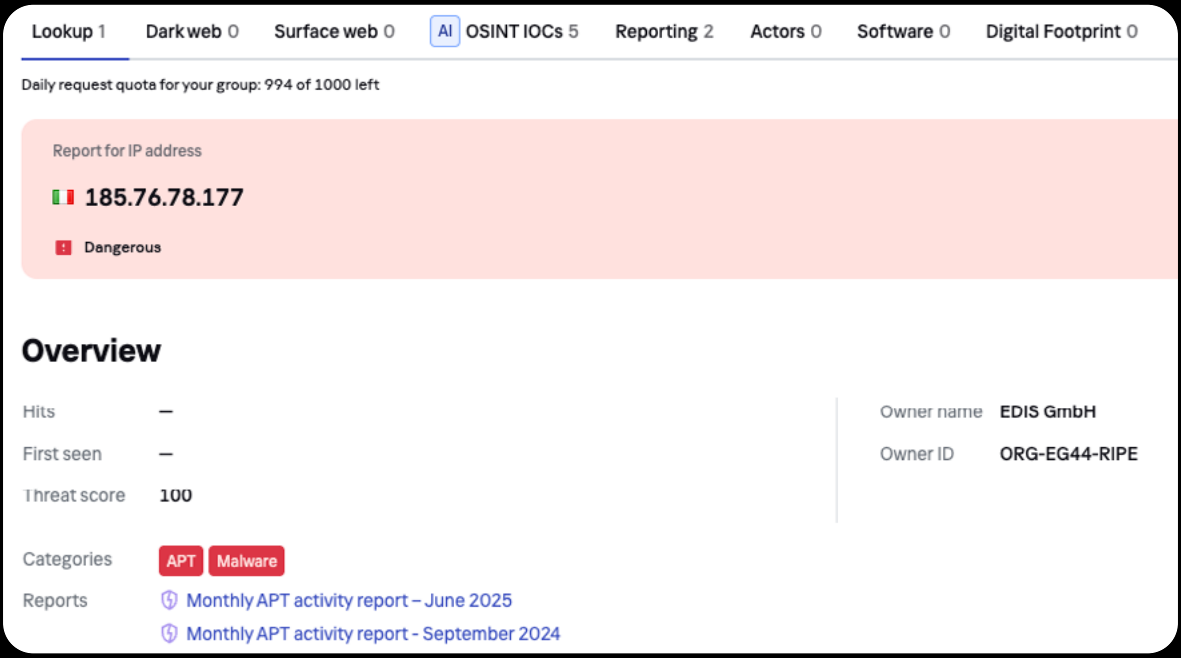
Pivoting and threat intelligence (TI) are deeply interconnected. Pivoting extracts value from threat intelligence, while TI provides the context and enrichment that makes pivoting effective. Modern TI platforms offer automated correlation, visualization and enrichment capabilities that streamline pivoting workflows.

Common pivoting workflows

IP address to domains

A common scenario involves investigating a suspicious IP address flagged in security alerts. For example, alerts may highlight DNS queries to the IP address 185.76.78.177. Querying passive DNS (pDNS) sources can help identify domains historically associated with this IP.

To assess their relevance, check the domain reputations using TI platforms and search your internal DNS and proxy logs for any traffic related to these domains.



Daily request quota for your group: 994 of 1000 left

Report for IP address

185.76.78.177

Dangerous

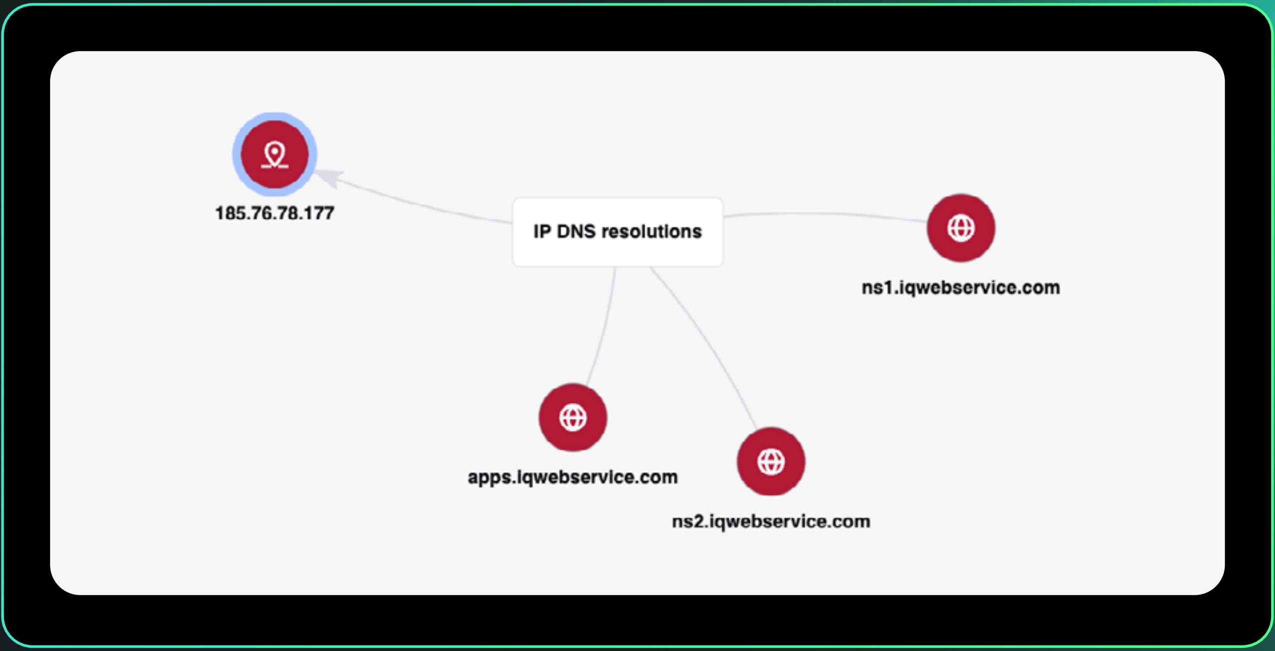
Overview

Hits	–	Owner name	EDIS GmbH
First seen	–	Owner ID	ORG-EG44-RIPE
Threat score	100		

Categories: APT Malware

Reports: Monthly APT activity report – June 2025
Monthly APT activity report - September 2024

Threat lookup report for suspicious IP address – Kaspersky Threat Intelligence Portal



Passive DNS resolution graph for IP 185.76.78.177 – Kaspersky Threat Intelligence Portal

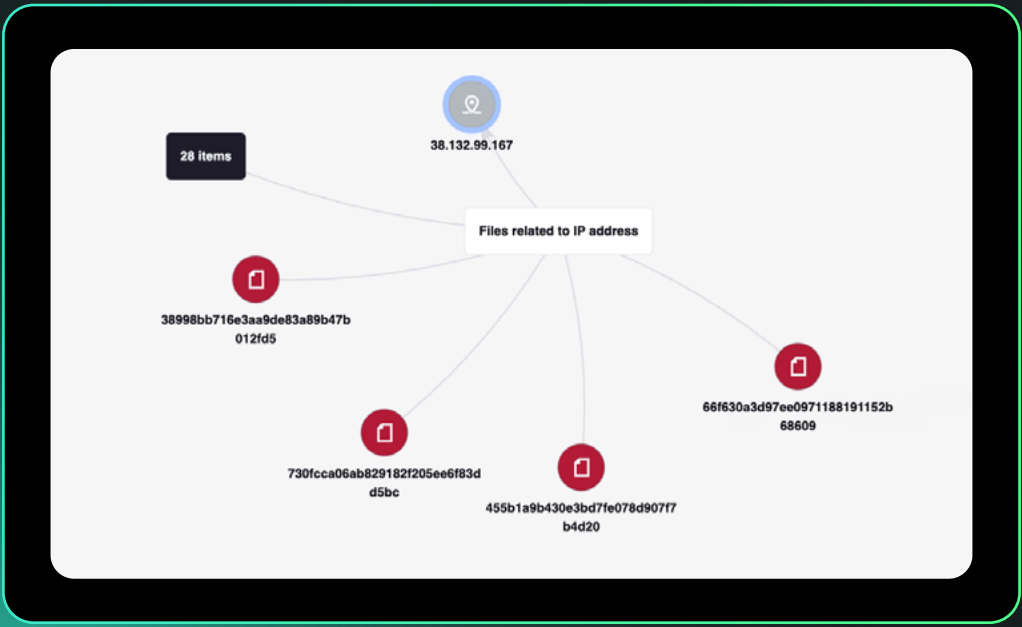
IP address to malware samples

A suspicious IP address identified in network logs and alerts may require further investigation. Pivoting from the IP can help determine whether it is:

1. Hosting known malware samples

2. Functioning as a command-and-control (C2) server, etc.

Public and commercial TI platforms provide sufficient capabilities to correlate IP addresses with observed malware activity and related campaigns.


28 items
38.132.99.167
Files related to IP address
38998bb716e3aa9de83a89b47b012fd5
730fcca06ab829182f205ee6f83dd5bc
455b1a9b430e3bd7fe078d907f7b4d20
66f630a3d97ee0971188191152b68609

File hashes associated with IP 38.132.99.167 – Kaspersky Threat Intelligence Portal

SSL certificates

SSL/TLS certificates serve as highly valuable pivot points in threat hunting. Threat actors frequently reuse certificates across multiple servers and domains within their infrastructure and often leverage free certificate authorities such as Let's Encrypt, which provide automated issuance with minimal validation.

The same certificate subject fields can appear repeatedly across different domains and campaigns. A typical reused pattern might look like: "C=US, ST=California, L=San Francisco, O=Microsoft Corporation, OU=Security Division, CN=(domain name)," where the Common Name (CN) changes but organizational details remain constant.

This creates strong pivoting opportunities, allowing analysts to identify IP addresses that previously hosted servers using certificates with identical or similar subject patterns.

In addition to certificates, TLS handshake metadata – including JA3, JA3S and JARM fingerprints – can be used to pivot and cluster attacker infrastructure. These values serve as unique digital fingerprints that identify how a client or server communicates over TLS. Threat actors often reuse the same configurations or malware frameworks across multiple servers, producing identical or near-identical fingerprints.

For example, searching for the JA3 signature **b742b407517bac9536a77a7b0fee28e9**, which corresponds to the Cobalt Strike C2 framework, and matching this fingerprint across network telemetry or threat intelligence datasets can reveal additional malicious hosts operated by the same adversary.

Domain → DNS TXT record

While domains are a common starting point in IoC investigations, querying their associated DNS TXT records offers a powerful and often overlooked pivoting opportunity. DNS querying commands can be used natively – no malware needed. By pivoting from a suspicious domain to its TXT record, analysts can:

Extract additional domains, C2 fallback addresses or botnet commands.

Retrieve encryption keys or tokens.

Detect DNS abuse patterns such as tunneling or stealthy payload delivery.

Reassemble file fragments or payload components.

Example: an investigation into a phishing domain uncovers a TXT record with base64-encoded IPs for backup C2 servers, enabling the SOC to block them before they are activated.

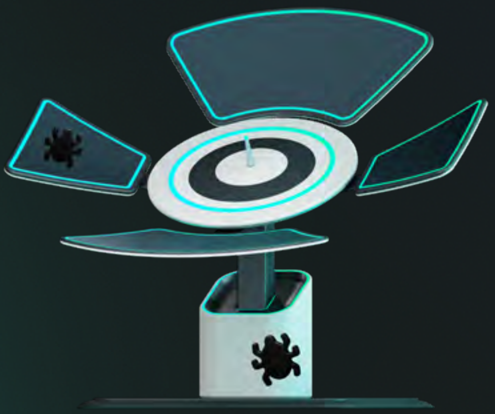
Beacon timing patterns

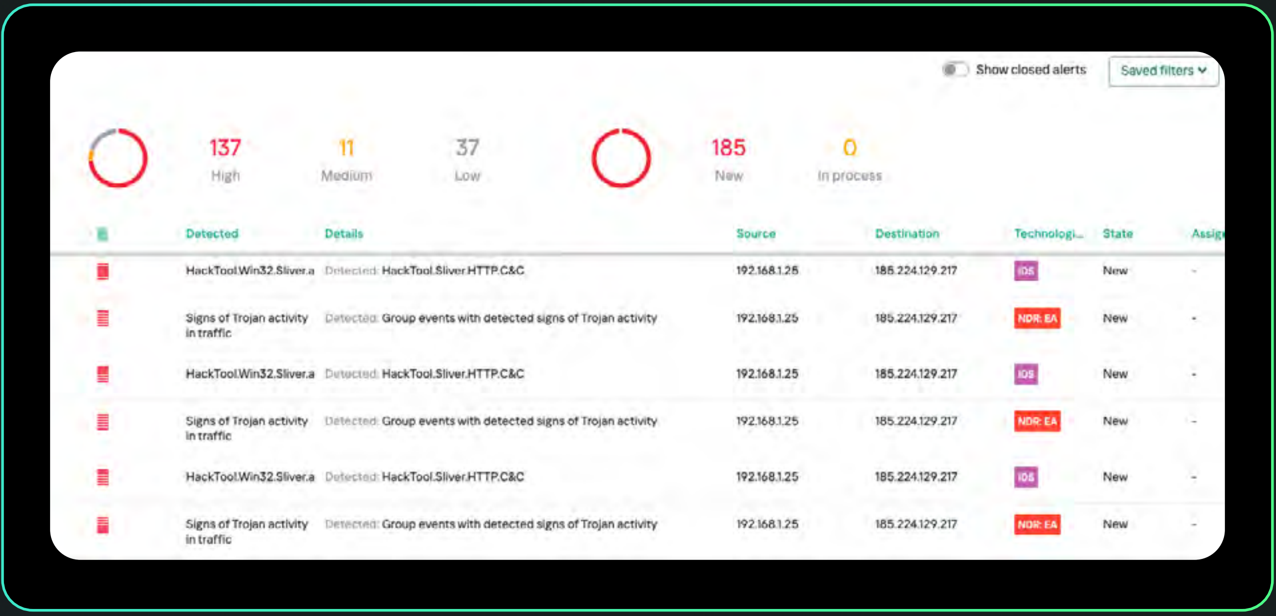
Beacons are periodic signals sent by compromised hosts to their C2 servers. These signals act as a "heartbeat," indicating active infection and allowing the attacker to maintain control.

Beacons often occur at consistent or semi-consistent intervals; for example, every few minutes, which stands out against typical network variability. To evade straightforward detection, attackers may add slight randomization (jitter) to beacon intervals. However, analyzing statistical patterns like the average interval and standard deviation can still reveal suspicious timing.

By analyzing average intervals and jitter, analysts can detect anomalies and search logs for matching patterns, uncovering additional infected hosts or related malware.

Example: during an incident investigation, analysts observe outbound network connections occurring at regular intervals, a pattern consistent with a Sliver C2 beacon profile.





	Detected	Details	Source	Destination	Technologi...	State	Assig
	HackTool.Win32.Sliver.a	Detected: HackTool.Sliver.HTTP.C&C	192.168.1.25	185.224.129.217	IDS	New	-
	Signs of Trojan activity in traffic	Detected: Group events with detected signs of Trojan activity	192.168.1.25	185.224.129.217	NDR: EA	New	-
	HackTool.Win32.Sliver.a	Detected: HackTool.Sliver.HTTP.C&C	192.168.1.25	185.224.129.217	IDS	New	-
	Signs of Trojan activity in traffic	Detected: Group events with detected signs of Trojan activity	192.168.1.25	185.224.129.217	NDR: EA	New	-
	HackTool.Win32.Sliver.a	Detected: HackTool.Sliver.HTTP.C&C	192.168.1.25	185.224.129.217	IDS	New	-
	Signs of Trojan activity in traffic	Detected: Group events with detected signs of Trojan activity	192.168.1.25	185.224.129.217	NDR: EA	New	-

Regular Sliver C2 beacon pattern detected – Kaspersky Anti Targeted Attack Platform (NTA)

From code markers to IoC expansion

The binary contains distinctive code traits, or "genetic markers," linked to a known targeted attack or APT campaign. Leveraging a threat attribution approach, such as the [Kaspersky Threat Attribution Engine (KTAE)](), allows analysts to compare these code fragments against a repository of advanced malware samples.

To operationalize these insights, analysts can create YARA rules based on the identified code patterns, enabling automated detection of similar binaries across internal systems, malware repositories or sandbox environments. This analysis can reveal additional IoCs, helping to identify related samples deployed in the environment or remnants of earlier attack activity.

This represents a form of code-based attribution pivoting, where unique binary markers are traced back to known APT campaigns, facilitating the discovery of linked IoCs and the reconstruction of historical attack footprints.

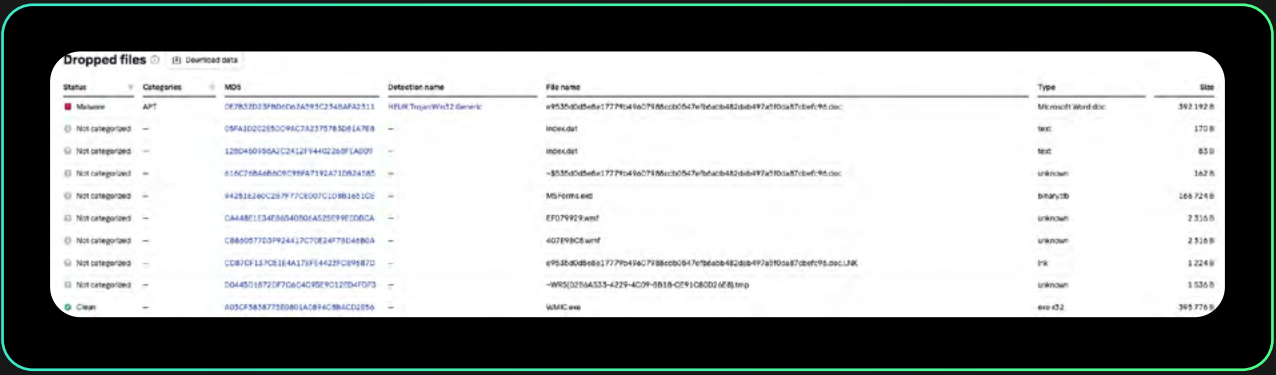
Sandbox artifact pivoting

Some indicators of compromise (IoCs) only emerge when a suspicious object is executed in a controlled environment. Many modern threats are fileless or staged, meaning the initial payload is benign or minimal, while the actual malicious behavior is triggered dynamically during execution.

By detonating such objects in a sandbox, analysts can observe runtime behaviors, including outbound communications, dropped files, registry modifications and process activity, which are not visible through static analysis alone. They can then use these behavioral artifacts to generate new IoCs – enriching TI and expanding detection coverage across the environment.

A file hash/URL address can serve as a starting point for identifying additional artifacts. Searching via a file hash (MD5, SHA1, SHA256) or URL address is one of the most effective pivoting techniques in TI and malware analysis.

When a malicious file is detonated in a sandbox, it often drops additional objects (executables, DLLs, scripts, configs) onto the disk. These are usually part of a multi-stage attack.



Dropped files ⓘ Download data

Status	Categories	MD5	Detection name	File name	Type	Size
🟥 Malware	APT	0E7B32D23FBD6D62A593C234BAFA2311	HEUR:Trojan.Win32.Generic	e9535d0d5e8e17779b49607988ccb0547efb6abb482dab497a5f0da87cbefc96.doc	Microsoft Word doc	392 192 B
Not categorized	–	05FA1D202850C9AC7A2375783D61A7E8	–	index.dat	text	170 B
Not categorized	–	128D460956A2C2412F94402268F1AD07	–	index.dat	text	83 B
Not categorized	–	616C768A6B6C9C98FA7192A71D824585	–	~$535d0d5e8e17779b49607988ccb0547efb6abb482dab497a5f0da87cbefc96.doc	unknown	162 B
Not categorized	–	94251E260C267F77CE007C10BB1651CE	–	MSForms.exd	binary.tlb	166 724 B
Not categorized	–	CA448E1E34E86540B06A525E99E0DBCA	–	EF079929.wmf	unknown	2 316 B
Not categorized	–	CB860577D3F924417C70E24F78D46B0A	–	407E9BC8.wmf	unknown	2 316 B
Not categorized	–	CD87CF137C81E4A178FE4422FC89587D	–	e9535d0d5e8e17779b49607988ccb0547efb6abb482dab497a5f0da87cbefc96.doc.LNK	lnk	1 224 B
Not categorized	–	D044501872DF7C6C4C95E9C12ED4FDF3	–	~WRS{D2B6A533-4229-4C09-8B18-CE91C80D26E8}.tmp	unknown	1 536 B
Clean	–	A05CF5838775E0801A0894C8B4CD2E56	–	WMIC.exe	exe x32	395 776 B

Dropped file hashes from analyzed sample (**0e7b32d23fbd6d62a593c234bafa2311**) – Kaspersky Threat Intelligence Portal

Knowing what was dropped helps in determining the extent of the incident, understanding the attack kill chain, and developing YARA rules based on the dropped files' signatures, names and behavioral traits.

Registry key to TTP mapping (MITRE ATT&CK)

Registry modifications that weaken system defenses or expose sensitive data often serve as strong IoCs. A common example is the malicious alteration of **WDigest** authentication settings, which enables the storage of plaintext credentials in system memory. This seemingly minor change can dramatically increase the attack surface, allowing adversaries to extract cleartext passwords directly from the Local Security Authority Subsystem Service (LSASS).

By default, modern Windows versions disable **WDigest (UseLogonCredential = 0)** to prevent this risk. However, when an attacker modifies the registry and sets this value to 1, the system begins caching user credentials in memory, providing attackers with a straightforward path to credential theft using tools like Mimikatz.

Such registry-based IoCs can reveal the attacker's intent and technique. To contextualize these IoCs within known adversary behavior, the MITRE ATT&CK Navigator can be used. For example, a credential access IoC such as **UseLogonCredential = 1** under WDigest maps directly to T1003.001 – OS Credential Dumping: LSASS Memory.

Tools such as EDR and SIEM are useful for detecting IoCs and mapping them to adversary tactics.

Accelerating IoC Discovery with AI

While traditional pivoting relies heavily on analyst expertise, AI may bring scale to the process:

Automated correlation: Machine learning models can link related IoCs across massive datasets in seconds, even when indicators differ slightly (e.g., subdomain variations, certificate anomalies).

Pattern discovery: AI can detect recurring infrastructure patterns that manual hunting might overlook.

Noise reduction: Intelligent models filter false positives, allowing analysts to focus on the most probable high-risk pivots.

The combination of human expertise for validation and AI produces faster and more accurate IoC discovery.

Applied pivoting example

Pivoting from a single hash may expose a complete infection path, supporting both containment and IoC enrichment. Suppose a security operations team detects a suspicious executable (“agent.exe”) on a finance department endpoint; the unique hash for this file is flagged by the EDR system. Analysts submit the hash to TI platforms, which link it to a known malware family specialized in data theft and DNS tunneling. The TI report identifies related hashes, associated domains (e.g., “corp-updates[.]com”) and previous campaigns using DNS for exfiltration.

With the enriched indicators from the hash pivot, analysts query DNS logs for suspicious domains and long, randomized subdomain patterns tied to “corp-updates[.]com”. They observe hundreds of outbound DNS requests from several endpoints to long, random subdomains of “corp-updates[.]com.”. The pattern resembles well-documented DNS exfiltration techniques, where the malware encodes stolen data into DNS request subdomains.

Analysts piece together the timeline:

Spear-phishing delivered a malicious document that dropped “agent.exe”.

The agent harvested sensitive files and exfiltrated them via DNS, blending this with normal queries.

Related hash and IoC analysis uncovered more infected endpoints querying “helper[.]corp-updates[.]com” and “auditlogs[.]corp-backups[.]com”.

The SOC blocks all outbound requests to “corp-updates[.]com” and related domains at the firewall layer, and isolates all machines with matching hashes or suspicious DNS queries for forensic review.

Summary

IoC pivoting is **cyclical and iterative** – every new indicator can lead to more. Whether through static indicators like file hashes and domains or dynamic artifacts surfaced during sandbox detonations, pivoting enables analysts to trace attacker infrastructure, uncover related infections and enrich internal telemetry.

Analyst challenge: select an IoC from a recent investigation – ideally one linked to confirmed malicious activity – and pivot it across at least three dimensions: infrastructure (e.g., passive DNS, JA3/JA3S), malware artifacts (e.g., sandbox-dropped files, YARA matches), and adversary behavior (e.g., MITRE ATT&CK TTP mapping).

However, despite its strengths, IoC pivoting has limitations:

Short-lived indicators: indicators (e.g., C2 domains) are frequently rotated, and attacker infrastructure can disappear within hours.

False positives: common when relying on community feeds without verification.

Information overload: pivoting can generate excessive data.

Evasion techniques: sophisticated adversaries increasingly use encrypted payload delivery, domain fronting and runtime obfuscation.

Therefore, while IoC pivoting holds a significant role in detection and response strategies, it should be complemented by behavioral analytics, anomaly detection and TTP-based threat hunting.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

www.kaspersky.com