SILENT PUSH

WHAT ARE INDICATORS OF FUTURE ATTACK™?

Indicators of Future Attack (IOFA)™ are actionable threat intelligence datapoints (hostname, domain, IP etc.) that reveal where an attack will be launched from in the future, based on how an adversary manages and deploys their infrastructure.

IOFA™ are used to create digital fingerprints of attacker activity, which security teams can use to track and monitor the searchable patterns that emerge as threat actors initialize and weaponize their infrastructure.

Indicators of Future Attack

Hostnames, domains and IP addresses that preemptively indicate attacker behavior and intent.

- Real-time, quick to search
- Provide behavioral fingerprints
- Fewer false positives
- **Preempts what WILL happen**

We'll delve a little deeper into what **IOFA™** are, how they expose threat actor infrastructure, how to use them to stop attacks, and why they're so effective when attempting to locate and block known and hidden threats.

WHAT PROBLEMS DO INDICATORS OF FUTURE ATTACK™ SOLVE?

There is an urgent need for preemptive cybersecurity solutions that minimize risk by stopping attacks at source, instead of waiting for an adversary to fully weaponize their infrastructure in a directed attack.

Today's security leaders are challenged to find the most effective threat intelligence solution for their organization, often searching through hundreds of options that almost always focus on traditional IOC-led cyber defense strategies that aren't equipped to fulfil this need.

Enter stage right: **Indicators of Future Attack™**.

The clue's in the name. It's not about where an attack has BEEN, it's about where an attack is coming FROM – whether it's a threat actor attempting to impersonate your organization online, inject malware onto machines to harvest and steal data, exploit your DNS records, or nation state-backed threat activity aimed at disrupting critical infrastructure.

WHAT DO INDICATORS OF FUTURE ATTACK™ EXPOSE?

IOFA™ preemptively reveal attacker intent and counteract threat infrastructure **as it's being setup** by focusing on an adversaries Tactics, Techniques and Procedures (TTPs), rather than waiting for an attack to be launched and the information to be publicly known – by which time it's often too late, and the damage is done.

Would you rather be alerted when a burglar is on their way to your house, or at your door, looking through the window for ways to break in? **IOFA™** act as digital roadblocks, allowing you to take proactive steps to ensure they never arrive at your property.

As well as emerging domains and IPs that are yet to be fully deployed, **IOFA™** can also be used to locate and block infrastructure that has already been involved in an attack.

WHY ARE INDICATORS OF FUTURE ATTACK™ SO EFFECTIVE?

Threat actors operate like a business, and like any other business, they adhere to a set of verifiable rules that produce results (i.e. a successful breach). To achieve this, APT groups setup and manage their infrastructure to a series of identifiable patterns.

IOFA™ allow security teams to turn the tables and use an adversary's own attack strategies against them, by shadowing their deployment techniques and blocking infrastructure the moment it's setup.

Threat actors recycle through hostnames and IPs at a rapid rate to evade detection, rendering most IOC-based feeds obsolete the moment they're setup.

By targeting the rules that govern how those same hostnames and IPs are deployed, **IOFA™** are not only able to counteract the thin end of the wedge – infrastructure involved in an attack – but any associated infrastructure that's lurking in the background, ready to strike.

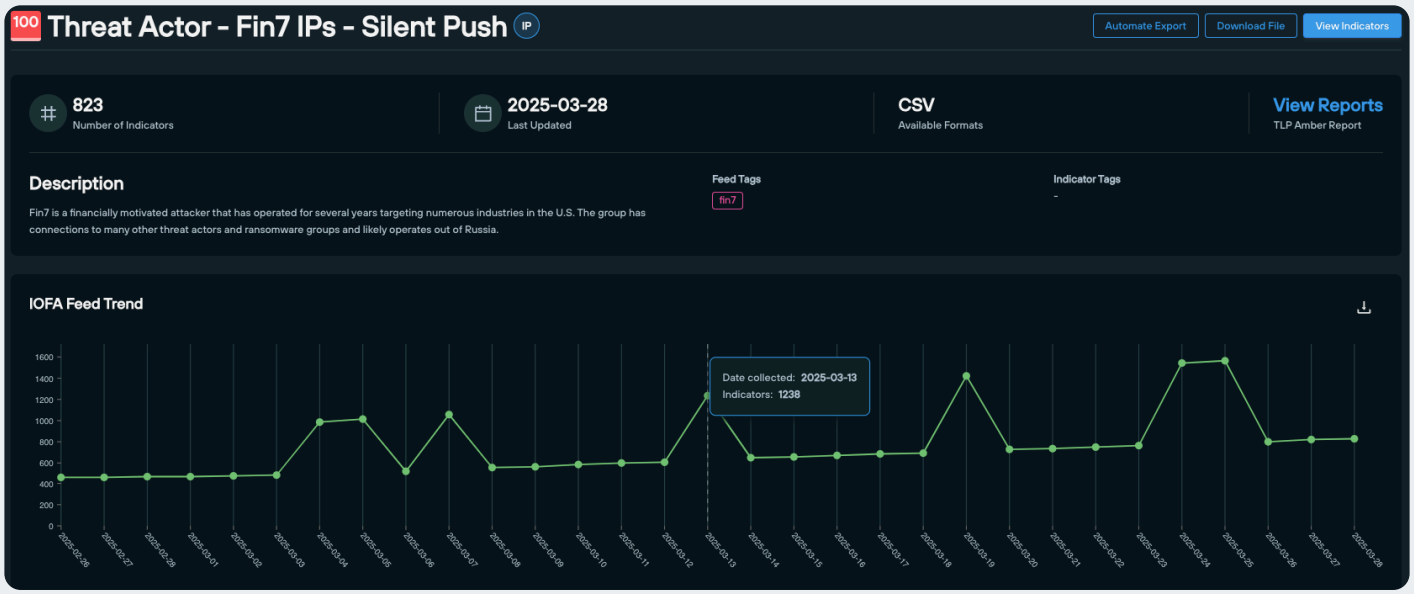
HOW ARE INDICATORS OF FUTURE ATTACK™ USED TO STOP ATTACKS?

IOFA™ have numerous practical uses that fulfil a range of cybersecurity functions, with the end goal of providing security teams with an early warning system that alerts them to emerging attacks.

Here's a few notable applications:

EARLY DETECTION FEEDS

Domain and IP **IOFA™** are used to construct automated threat feeds in Silent Push Enterprise, containing hidden elements of attacker infrastructure as well as known malicious datapoints.



Silent Push Threat Analysts create and update **IOFA™** Feeds that counteract high-profile named APT groups (e.g. Lazarus, Scattered Spider), which Enterprise customers use as finished intelligence within their detection and blocking mechanisms.

Enterprise users are also able to create their own feeds, built on Silent Push queries that output **IOFA™** relevant to their organization and area of operation.

DATA CORRELATION VIA INTEGRATIONS

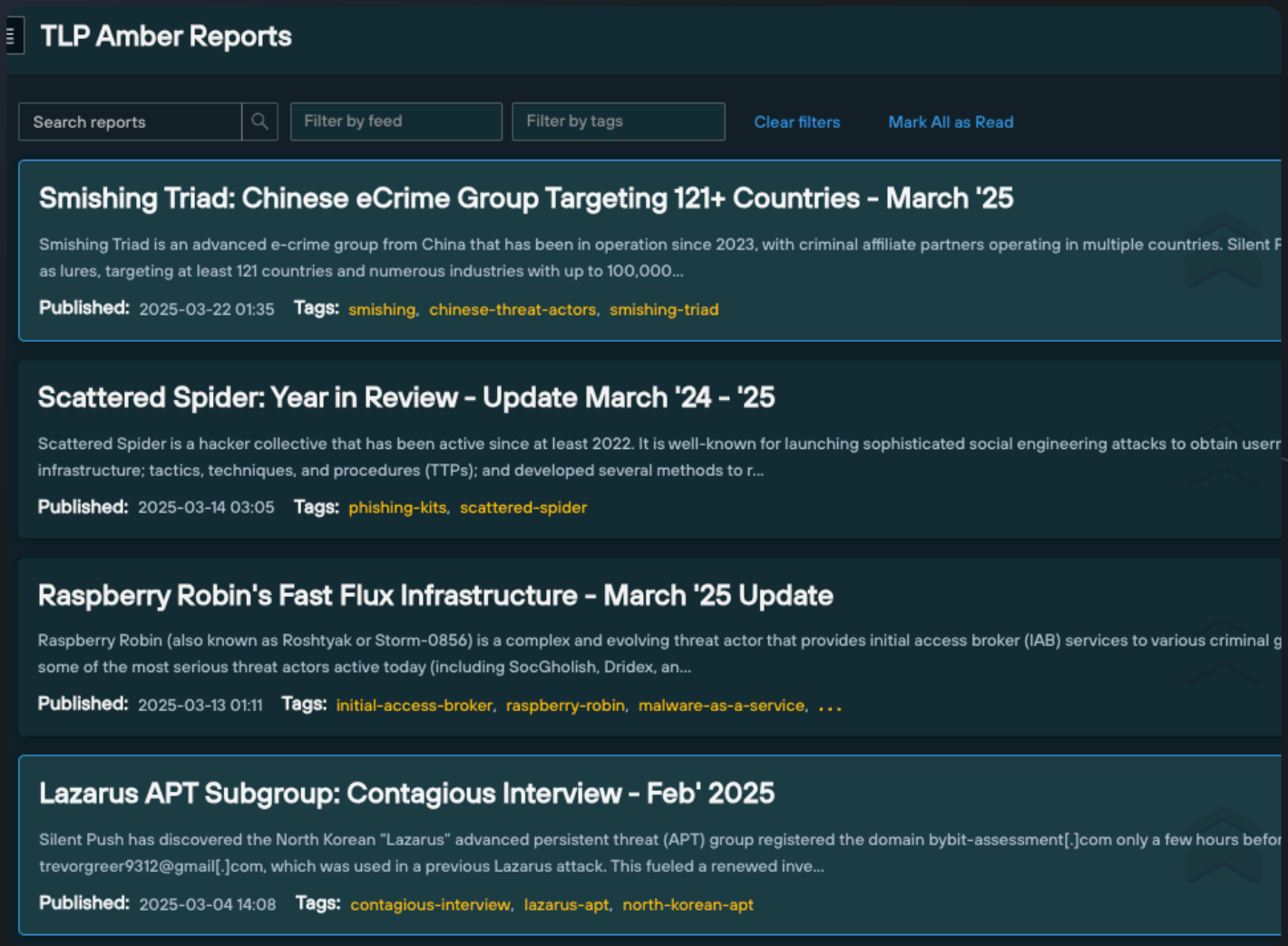
IOFA™ can be passed through an organization's security stack using the Silent Push API and a range of native integrations with leading cybersecurity vendors, to enrich existing datastreams with a wealth of DNS and content-based categorization.

Utilizing **IOFA™** data within other software platforms alerts teams to infrastructure that isn't on their radar, and allows for faster and more effective discovery of all the hostnames and IPs associated with a given threat, including those lurking under the surface of an attack.

TLP AMBER REPORTS

Silent Push Enterprise edition customers have access to TLP Amber reports, written and curated by our team of Threat Analysts, that perform a deep dive into high profile APT activity and contain lists of **IOFA™** associated with a given campaign.

Our TLP Amber reports contain proprietary information on named threat campaigns, including the queries used to track how infrastructure is being setup and managed, that SOC and IR teams use as immediately actionable intelligence to stop emerging attacks, and gather intelligence on known threats.



WHY ARE INDICATORS OF FUTURE ATTACK™ UNIQUE TO SILENT PUSH?

Silent Push is the only cybersecurity vendor that outputs **IOFA™**.

No other platform has the same ability to map out the relationship between billions of disparate hostnames and IPs in a way that reveals adversary TTPs at the earliest possible stage, allowing teams to stay one-step ahead of a given campaign before it's fully initialized without needing to rely on post-breach IOCs.

Our data is all our own. **IOFA™** are generated from a powerful first-party dataset that scans and correlates the global IP range, and joins the dots across the IPv4 range in a way that makes it immediately obvious where the next digital assault is likely to originate from.

CATEGORIZATION

IOFA™ aren't used in isolation. We apply 150+ proprietary categories to each **IOFA™** the platform outputs, that allows teams to understand the relationship a domain or IP address has with the rest of the Internet, including how it's moved between hosts, its risk level, and how it's managed in relation to known malicious indicators.

LEARN MORE ABOUT OUR UNIQUE APPROACH TO PREEMPTIVE THREAT INTELLIGENCE

If you're interested in learning about how **IOFA™** can help you to locate hidden and known threat infrastructure, and stop digital assaults at source before they occur, contact us for more information.

ABOUT US

Silent Push provides preemptive cyber defense exposing threat actor infrastructure as it's being set up. Our **Indicators Of Future Attack (IOFA)™** act as an early warning system to defend against threats. We go beyond stale IOCs and create a unique digital fingerprint of adversary behavior enabling you to proactively block hidden attacks before they're launched.

Get started today.

SILENT **PUSH**

PREEMPTIVE CYBER DEFENSE WITH INDICATORS OF FUTURE ATTACK™

CONTACT US TO LEARN MORE

silentpush.com