SILENT PUSH

KNOW FIRST WITH IOFA™

DISCOVER ATTACKER INFRASTRUCTURE BEFORE IT'S WEAPONIZED

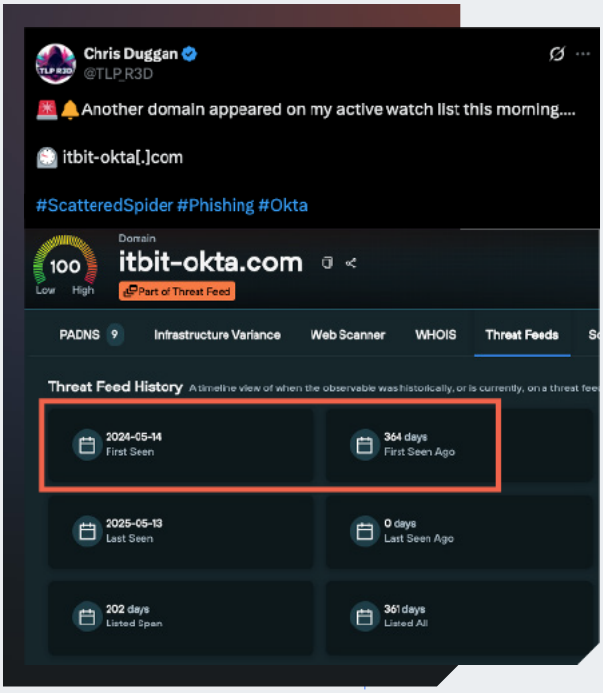
Preemptive cyber intelligence that exposes threat actor infrastructure as it's being set up with **Indicators of Future Attack (IOFA)**™.

IOFA™ are actionable threat intelligence datapoints revealing where an attack will be launched based on how an adversary manages their infrastructure; plus where attacks already occurred.

IOFA™ are created by discovering malicious domains and IPs that share the same characteristics, such as hosting clusters, and various on-page elements. Silent Push operates with a proprietary DNS and content scanning engine that takes every public domain and IP address, and applying over 200 categories that uncovers the relationship between billions of observable datapoints on the Internet.

PROACTIVE THREAT DETECTION FOR SOC, IR, AND CTI TEAMS

- **IOFA**™ replace traditional post-breach IOC-led detection.
- Know attacker infrastructure from their unique digital fingerprints.
- **IOFA**™ reduce false positives enabling you to proactively defend your organization.



USE CASE

EARLY DETECTION OF SCATTERED SPIDER PHISHING

KNOW FIRST 5 MONTHS EARLIER WITH IOFA™

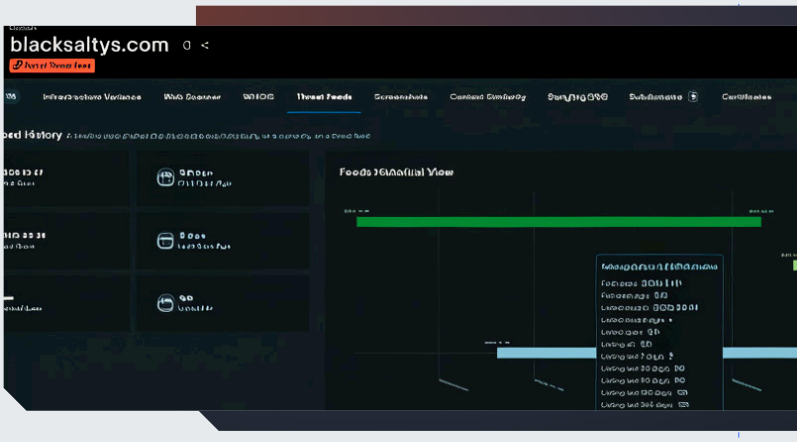
Scattered Spider target Okta users primarily through social engineering tactics, including phishing domains, to access systems protected by Okta's Identity and Access Management platform and bypass MFA protections.

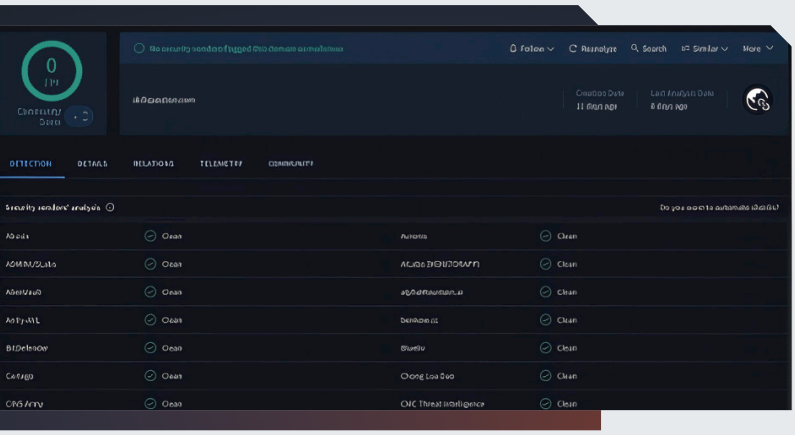
The first public mention of itbit-okta[.]com domain was on 20/9/24. We had it tagged in a Scattered Spider threat feed five months earlier on 15/5/24.

USE CASE

DETECTED TA569 MALWARE

The sites used for the initial web inject campaign to drop SocGholish Javascript malware applied fake browser updates to lure users into downloading the payload. Silent Push first identified the infrastructure 4 months prior to published research by tracking the bullet proof hosting provider used to serve the content.





USE CASE

REVEALED UNKNOWN LAZARUS GROUP ATTACKS

A campaign associated with the North Korean group, Lazarus, utilized several domains for phishing and malware delivery. Silent Push created a behavioral fingerprint of the traceable deployment patterns, and an **IOFA**™ feed to automatically track and collect associated domains.

KNOW FIRST WITH IOFA™ TO STOP ATTACKS

ATTACKER'S DIGITAL FINGERPRINT IDENTIFIES INTENT

These unique fingerprints enable SOC, IR and CTI teams to quickly make informed and timely decisions in high-pressure situations where every second counts.

The moment a new domain or IP address is spun up to engage in a fresh assault, it's detected in the Silent Push platform and flagged as malicious before the attacker has time to engage with their target.

AUTOMATED PREEMPTIVE INTELLIGENCE REDUCES RISK

IOFA™ Feeds contain lists of true positive domains and IPs that can be utilized for detection and blocking purposes. These feeds counteract high-profile named APT groups and other threats.

This finished intelligence enables faster response to emerging threats, improving MTTD and MTTR.

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™

REQUEST A DEMO

silentpush.com