SILENT PUSH

KNOW FIRST WITH IOFA™

DISCOVER ATTACKER INFRASTRUCTURE BEFORE IT'S WEAPONIZED

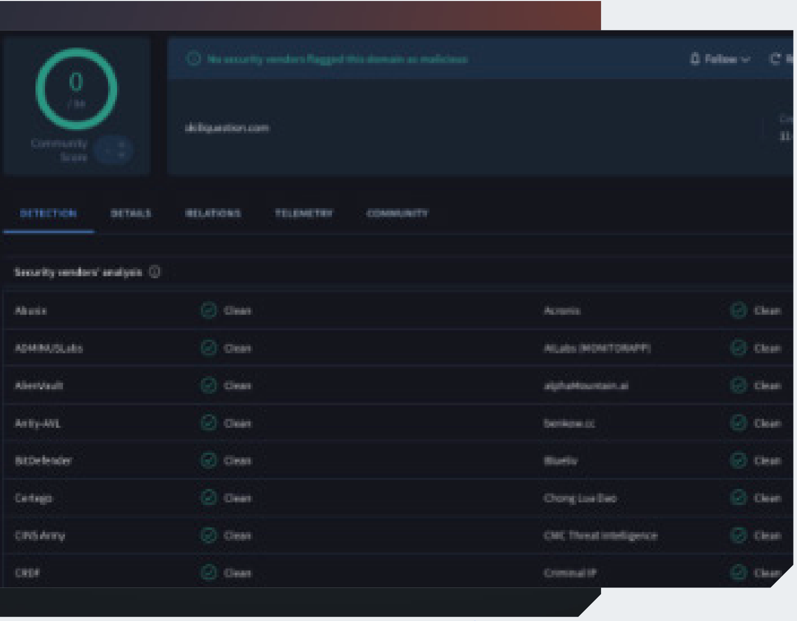
Preemptive cyber intelligence that exposes threat actor infrastructure as it's being set up with Indicators of Future Attack (**IOFA**)™.

IOFA™ are actionable threat intelligence datapoints that reveal where an attack will be launched from in the future based on how an adversary manages and deploys their infrastructure, as well as revealing where attacks have already occurred.

Silent Push operates with a proprietary DNS and content scanning engine that takes every public domain and IP address and applies over 200 categories that reveal 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 intent from their unique digital fingerprints created from **IOFA**™.
- **IOFA**™ reduce false positives enabling you to proactively defend your organization.



No security vendors flagged this domain as malicious

skillquestion.com

Security vendors' analysis

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean
CRDF	✓ Clean	Criminal IP	✓ Clean

USE CASE

KNOW FIRST
3 MONTHS EARLIER
WITH IOFA™

LOCATED SOCGHOLISH MALWARE

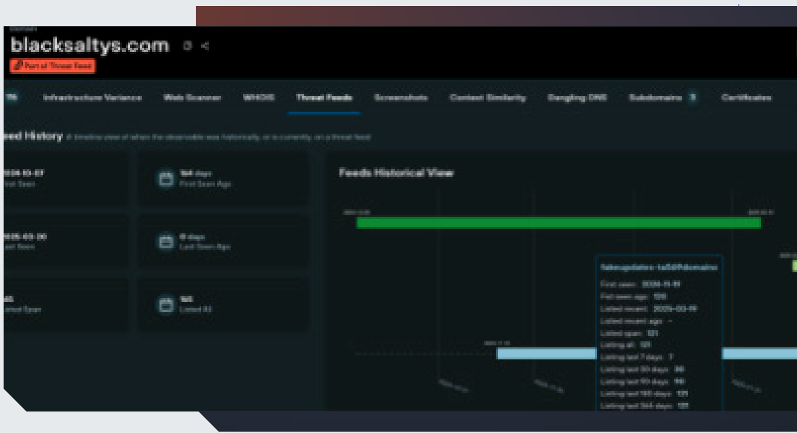
After reviewing the IOCs listed in a SocGholish public report that included a list of true positive domains and IPs associated with the attack vector, Silent Push found most had already been tagged as malicious in the platform 3 months prior. Silent Push had previously informed its customers through a 'Fake Browser Update' **IOFA**™ feed.

KNOW FIRST
4 MONTHS EARLIER
WITH IOFA™

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.



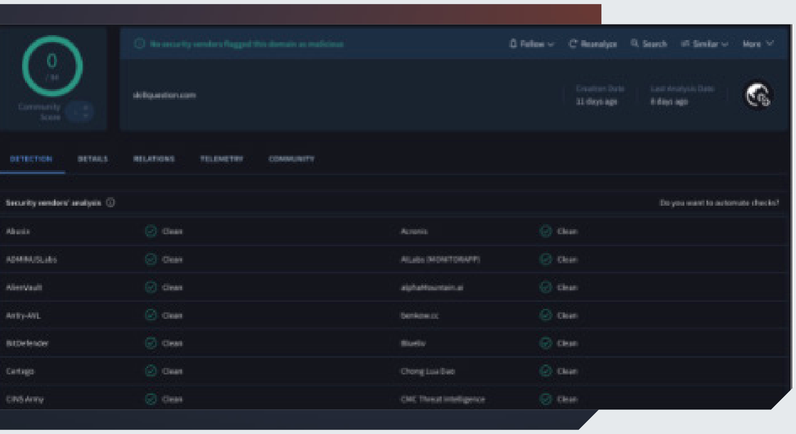
2024-10-07 First Seen

164 days First Seen Ago

2025-03-20 Last Seen

8 days Last Seen Ago

Listed At



No security vendors flagged this domain as malicious

skillquestion.com

Creation Date 11 days ago

Last Analysis Date 8 days ago

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Bluelivv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean

USE CASE

REVEALED UNKNOWN LAZARUS GROUP ATTACKS

KNOW FIRST
3 MONTHS EARLIER
WITH IOFA™

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 intelligence 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 INTELLIGENCE WITH
INDICATORS OF FUTURE ATTACK™

REQUEST A DEMO

silentpush.com