SLASHNEXT

# Real-Time Phishing Threat Intelligence

## The Industry's Broadest, Most Up-to-the-Minute Intelligence on Phishing Threats

SlashNext enables organizations to better understand and protect themselves from zero-hour phishing and social engineering threats on the web. Through multiple sources, SlashNext proactively inspects millions of suspicious URLs daily. Unlike other anti-phishing technologies, SlashNext patent-pending SEER™ technology uses virtual browsers to dynamically inspect page contents and server behavior to detect tens of thousands of new phishing URLs per day with extreme accuracy. Together with fully automated URL re-checking and retirement, security teams get the most comprehensive, real-time phishing threat intelligence available.

### OVER 90% OF BREACHES START WITH PHISHING

Phishing and social engineering threats have become so numerous, convincing, and evasive that many bypass multi-layer security controls and deceive even cyber-savvy employees. While email phishing remains a common tactic, phishing attack vectors have expanded to target people through ads, pop-ups, social media, search, IM, SMS, rogue apps, and more.

### PHISHING THREATS: MORE NUMEROUS, SOPHISTICATED, FAST-MOVING

- Tens of thousands of new phishing sites go live each day
- Most disappear in 4 to 8 hours, often faster than they become known or blacklisted
- Growing sophistication makes malicious sites virtually indistinguishable from legitimate sites
- Threat actors increasingly use compromised sites, URL obfuscation, and other tactics to evade detection

### DEFINITIVE REAL-TIME PHISHING THREAT INTELLIGENCE POWERED BY SEER

SlashNext Real-Time PhishingThreat Intelligence is powered by SEER threat detection technology. SEER (Session Emulation and Environment Reconnaissance) uses virtual browsers in a purpose-built cloud to dynamically inspect sites with advanced computer vision, OCR, NLP, and active site behavioral analysis. Machine learning enables definitive verdicts—malicious or benign—with exceptional accuracy and near-zero false positives.

### COMPREHENSIVE PHISHING THREAT DETECTION

Unlike other anti-phishing technologies and threat feeds, SlashNext Real-Time Phishing Threat Intelligence covers all six major categories of phishing and social engineering threats.

**CREDENTIAL STEALING**
Fake login pages, etc.

**PHISHING EXPLOITS**
Weaponized documents, etc.

**SCAREWARE**
Tech support scams, fake virus alerts, etc.

**SOCIAL ENGINEERING SCAMS**
Credit card and Bitcoin fraud, money transfer scams, fake deals, prizes, etc.

**ROGUE SOFTWARE**
Rogue apps, browser extensions, fake AVs, etc.

**PHISHING CALLBACKS (C2s)**
Data exfiltration, C2 callbacks, etc.

### THE SLASHNEXT ADVANTAGE

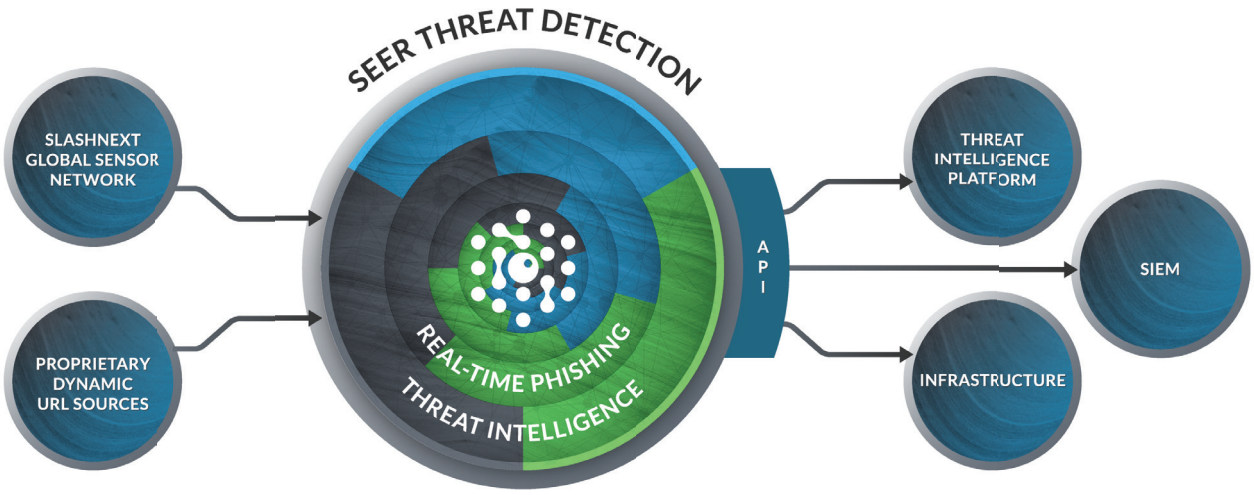
- **Comprehensive:** covers all six types of types of phishing threats (not just fake log-in pages)
- **Real-Time:** continuously updated list of zero-hour phishing URLs, domains, and IPs with IOCs
- **Accuracy:** automated URL re-checking and retirement results in dynamic list of active phishing threats with near-zero false positives
- **SEER Technology:** detects phishing sites that evade URL inspection and domain reputation analysis
- **Preemptive:** global, proactive threat hunting provides advance visibility of threats
- **Easily Accessible:** web API access to threat data in multiple machine-readable formats
- **SlashNext Expertise:** technology and quarterly threat intelligence reports from the specialists in modern phishing threats

## THREAT INTEL API

SlashNext Real-Time Phishing Threat Intelligence is accessed via a RESTful API that returns phishing threat feed types. Each is available in JSON, CSV, or plaintext formats. API access enables organizations to pull down just domains, IPs, Wildcard URLs, and/or full URLs to suit their own specific needs.

| SIX THREAT INTELLIGENCE FEEDS | | OPTIONS | FORMATS |
|---|---|---|---|
| Credential stealing | Phishing Exploits | Full URLs | JSON |
| Scareware | Social Engineering Scams | Domains | CSV |
| Rogue Software | Phishing Callbacks (C2s) | IPs | Plaintext |
| | | Wildcard URLs | |

## SLASHNEXT SEER TECHNOLOGY PROVIDES THE MOST COMPREHENSIVE, ACCURATE, REAL-TIME PHISHING THREAT DETECTION AND INTELLIGENCE




Through multiple live sources, SlashNext proactively scans billions of global Internet transactions and millions of suspicious URLs on a daily basis.

Suspect URLs are rendered with millions of virtual browsers in the SlashNext threat detection cloud. SEER technology inspects the site with advanced computer vision, OCR, NLP, and active site behavior analysis.

SEER analysis features are fed into machine learning algorithms which deliver a single definitive verdict: malicious or benign. There are no inconclusive threat scores and near-zero false positives.

Malicious URLs, Domains, and IPs are continuously added to the SlashNext Real-Time Phishing Threat Intelligence feed and available in multiple machine-readable formats via Web APIs.

## QUARTERLY THREAT INTELLIGENCE REPORT

SlashNext customers also receive our quarterly Threat Intelligence Report highlighting key threats and trends detected by our platform and analyzed by our security research team. Each report provides insights and useful intelligence to help organizations better understand and manage protections against the changing threat landscape.

**START YOUR FREE, NO HASSLE TRIAL TODAY AT WWW.SLASHNEXT.COM/TRIAL-REQUEST**

© 2019 SlashNext, Inc. All rights reserved. All other trademarks are the property of their respective owners.

4301 Hacienda Drive, Pleasanton, CA 94588 | slashnext.com | info@slashnext.com | 800.930.6843

022019