Shadow Search

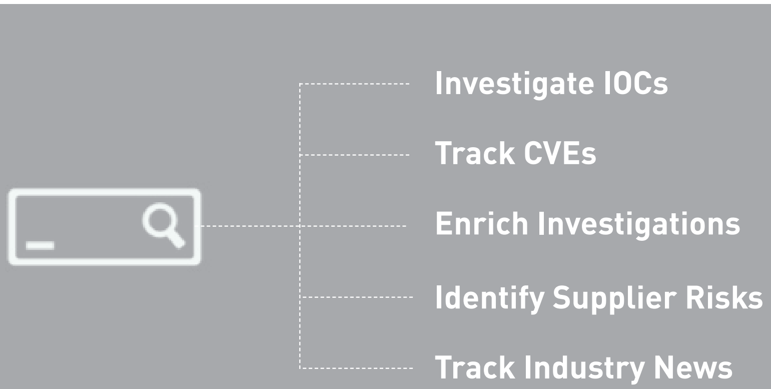
Shadow Search speeds up the security operations process, quickly enabling deeper research and faster investigation. The result is better decision making that gives back valuable time to security operations teams.

The Need for Rapid Research & Investigation

With the ever expanding threat landscape and rising mitigation costs, it is even more critical to detect and remediate threats quickly and effectively. However, security organizations struggle with the volume and lack of context provided by many event sources and require additional information to make the best decisions. With easy-to-interpret results, Shadow Search saves analyst time by putting the information they need at their fingertips, when they need it, all with an intuitive interface.

Shadow Search provides:

- **Immediate Access:** instant access to threat data and raw collections when you need it.
- **Coverage:** a vast repository of data including curated threat intelligence, content from open, deep and dark web sources, feeds, exploit and vulnerability information, all in one place available for searching.
- **Actionable information:** rich results with associated observables, an intuitive interface and full export, allowing users to make faster searches and more rapid decisions based on the results.
- **Relevant results:** smart filters and a powerful search syntax enable users to rapidly focus on the most relevant information.



Investigate IOCs

Track CVEs

Enrich Investigations

Identify Supplier Risks

Track Industry News

Most Popular Use Cases

Organizations use Shadow Search in a variety of different ways to help achieve their unique goals. Here are the most popular!

IOC Investigation

Gain additional context on IOCs, which can be useful to SOC teams during investigations. It can also be used to uncover further IOCs linked to malicious actions helping triage, and in configuration updates.

CVE Tracking

When clients are faced with a large number of CVEs which require patching, they use information found in Shadow Search to help prioritize – such as gaining an understanding of when exploits have been made public.

Enrich Investigations

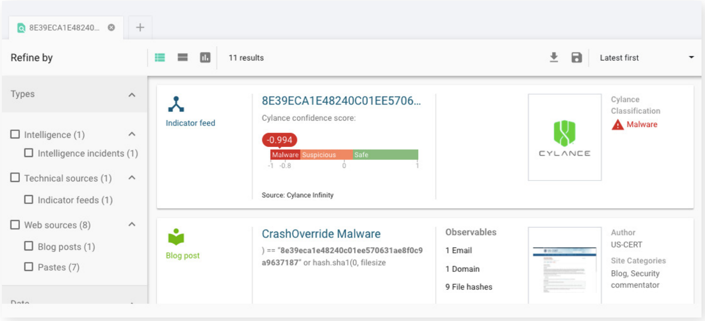
Shadow Search can be used within tactical investigations of technical indicators used in cyber-attacks such as business email compromise, phishing attempts, or denial of service attacks.

Identify Supplier Risks

Shadow Search is used by security teams to monitor potential third-party risks, such as vulnerabilities found in outsourced IT suppliers, or breaches of companies holding their sensitive data.

Track Industry News

For those who want to know as soon as possible whenever there's a new development related to their industry, Shadow Search is here to help.



8E39ECA1E48240C01EE5706...

Cylance confidence score: -0.994

Source: Cylance Infinity

Cylance Classification: Malware

CrashOverride Malware

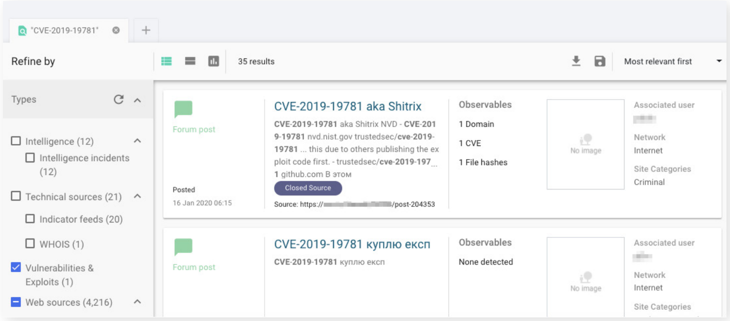
) == "8e39eca1e48240c01ee570631ae8f0c9a9637187" or hash.sha1(0, filesize

Observables: 1 Email, 1 Domain, 9 File hashes

Author: US-CERT

Site Categories: Blog, Security commentator

Investigating a suspicious file hash in Shadow Search



CVE-2019-19781 aka Shitrix

CVE-2019-19781 aka Shitrix NVD - CVE-2019-19781 nvd.nist.gov trustedsec/cve-2019-19781 ... this due to others publishing the exploit code first. - trustedsec/cve-2019-197... 1 github.com В этом

Closed Source

Source: https://[redacted]/post-204353

Posted: 16 Jan 2020 06:15

Observables: 1 Domain, 1 CVE, 1 File hashes

Associated user: [redacted]

Network: Internet

Site Categories: Criminal

CVE-2019-19781 куплю експ

CVE-2019-19781 куплю експ

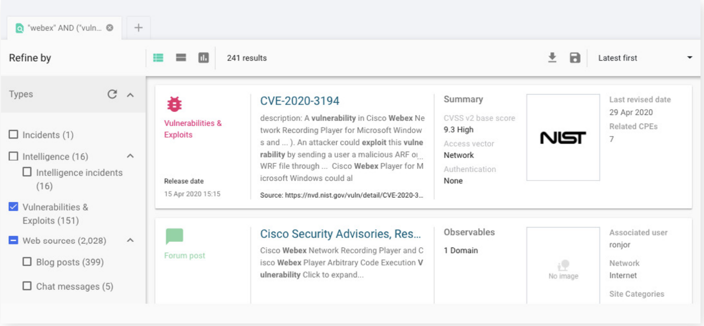
Observables: None detected

Associated user: [redacted]

Network: Internet

Site Categories

Tracking mentions of a CVE, with discussions across Closed Source criminal forums



CVE-2020-3194

description: A vulnerability in Cisco Webex Network Recording Player for Microsoft Windows and ...). An attacker could exploit this vulnerability by sending a user a malicious ARF or... WRF file through ... Cisco Webex Player for Microsoft Windows could al

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-3...

Release date: 15 Apr 2020 15:15

Summary

CVSS v2 base score: 9.3 High

Access vector: Network

Authentication: None

Last revised date: 29 Apr 2020

Related CPEs: 7

Cisco Security Advisories, Res...

Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerability Click to expand...

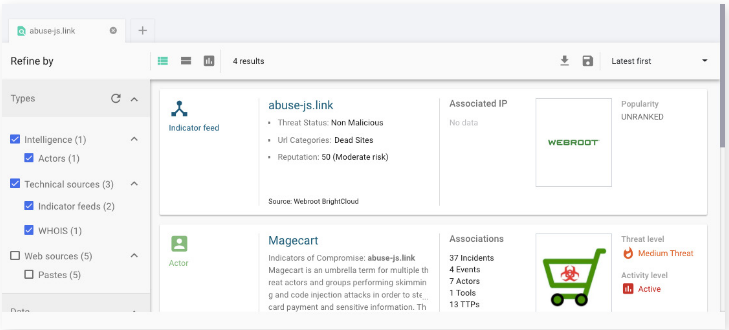
Observables: 1 Domain

Associated user: ronjor

Network: Internet

Site Categories

Monitoring for reports of exposure related to a technology supplier



abuse-js.link

- Threat Status: Non Malicious
- Url Categories: Dead Sites
- Reputation: 50 (Moderate risk)

Source: Webroot BrightCloud

Associated IP: No data

Popularity: UNRANKED

Magecart

Indicators of Compromise: abuse-js.link

Magecart is an umbrella term for multiple threat actors and groups performing skimming and code injection attacks in order to ste... card payment and sensitive information. Th

Associations: 37 Incidents, 4 Events, 7 Actors, 1 Tools, 13 TTPs

Threat level: Medium Threat

Activity level: Active

Investigating a suspicious domain, combining feeds, raw, and finished intelligence

Source Coverage

Organizations have direct access to the vast repository of technical, tactical and strategic threat intelligence, and raw web content, curated and collected by Digital Shadows to investigate threats and take immediate action. Each source will bring unique context to your investigations, but some of the most popular finds are displayed below.

Source Type	Source Examples	Common Finds
Criminal Forum Posts	Exploit, Raidforums, XSS, Torum*	Keep track of discussions on exploits, insiders, and criminals selling access.
Dark Web Marketplace Listings	Apollon, Empire**	Track databases and accounts offered for sale.
Chat Messages	IRC, Telegram	Immediately detect the trade of stolen credit cards and customer accounts.
Pastes	Pastebin	View IOCs posted by researchers, and detect leaked data.
Social Media	Twitter posts	View and export IOCs posted by researchers i.e. Emotet, Trickbot
Blogs	Security researcher blogs	Breaking industry news & exposure of third parties.
Threat Intelligence and Reputation Feeds	AlienVault, Webroot, Cylance Infinity, PhishTank	Enrich observables and give context to ongoing investigations.
Vulnerability and Exploits	ExploitDB, NIST NVD	Gain context on the latest vulnerabilities and exploits.
WHOIS Information	N/A	Launch investigations into domains of interest.
DNS Lookups	N/A	Identify DNS records associated with a domain.
Intelligence Incidents	Photon Analysis	Access Digital Shadows' finished intelligence.
Actor Profiles	Photon Analysis	Learn more about threat actor and drill down into IOCs.
Incidents and Alerts	All private alerts (i.e. Impersonating domain)	Gain vital context on your private incidents and alerts.

*A small selection of the forum coverage

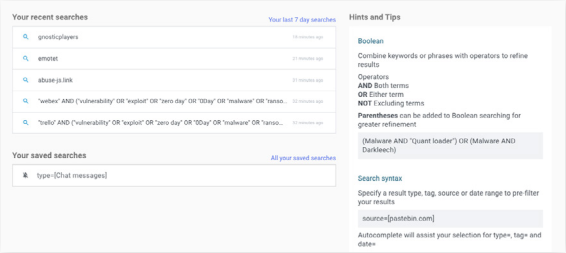
** Marketplace are in a state of flux; markets will disappear and others will emerge, so the latest live marketplaces will change.

Features

Shadow Search provides analysts with fast access to raw and curated intelligence that frees up time for other security responsibilities. It also complements internal hunting and incident response efforts.

Some of the many features include:

Search Guidance



Your recent searches — Your last 7 day searches

- gnosticplayers — 18 minutes ago
- emotet — 21 minutes ago
- abuse-js.link — 31 minutes ago
- "webex" AND ("vulnerability" OR "exploit" OR "zero day" OR "0Day" OR "malware" OR "ranso... — 32 minutes ago
- "trello" AND ("vulnerability" OR "exploit" OR "zero day" OR "0Day" OR "malware" OR "ranso... — 32 minutes ago

Your saved searches — All your saved searches

- type=[Chat messages]

Hints and Tips

Boolean

Combine keywords or phrases with operators to refine results

Operators
AND Both terms
OR Either term
NOT Excluding terms

Parentheses can be added to Boolean searching for greater refinement

(Malware AND "Quant loader") OR (Malware AND Darkleech)

Search syntax

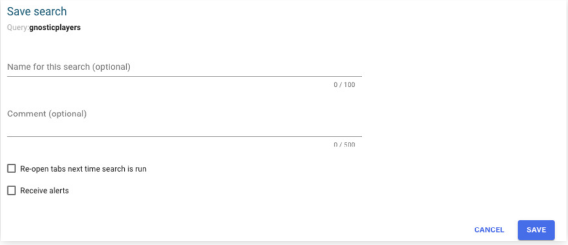
Specify a result type, tag, source or date range to pre-filter your results

source=[pastebin.com]

Autocomplete will assist your selection for type=, tag= and date=

Clicking into the search bar will provide an overview of recent searches, saved searches, and Hints and Tips for searching.

Alert Subscriptions



Save search

Query:**gnosticplayers**

Name for this search (optional) 0 / 100

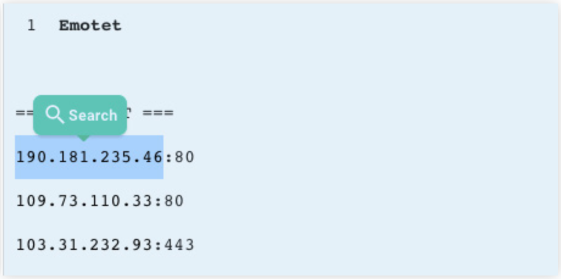
Comment (optional) 0 / 500

☐ Re-open tabs next time search is run

☐ Receive alerts

Users can subscribe to "Google-like" alerts on new matches. These alerts can be immediate, daily, weekly, or monthly and are editable at any point.

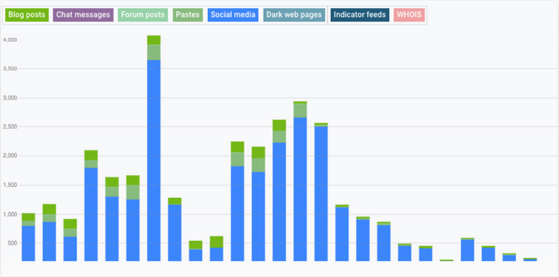
Pivot Feature



```
1   Emotet

==  Search  ===

190.181.235.46:80

109.73.110.33:80

103.31.232.93:443
```

Pivot off any term in results from intuitive multi-tab interfaces. For ease of discovery, observables will be automatically displayed in the search results.

Different View Options



Filter by date, source, and display results as a timeline, summary, or results view. These different views are perfect for including in reports.

Contact Us to Get Started and Learn More

Email info@digitalshadows.com

Call us at US 1-888-889-4143
UK +44 (0)203 393 7001

Visit www.digitalshadows.com
for more information

digital shadows_