



WTF

IS

DRP

A quick guide to
understanding how
your company looks
to attackers.

DIGITAL RISK PROTECTION

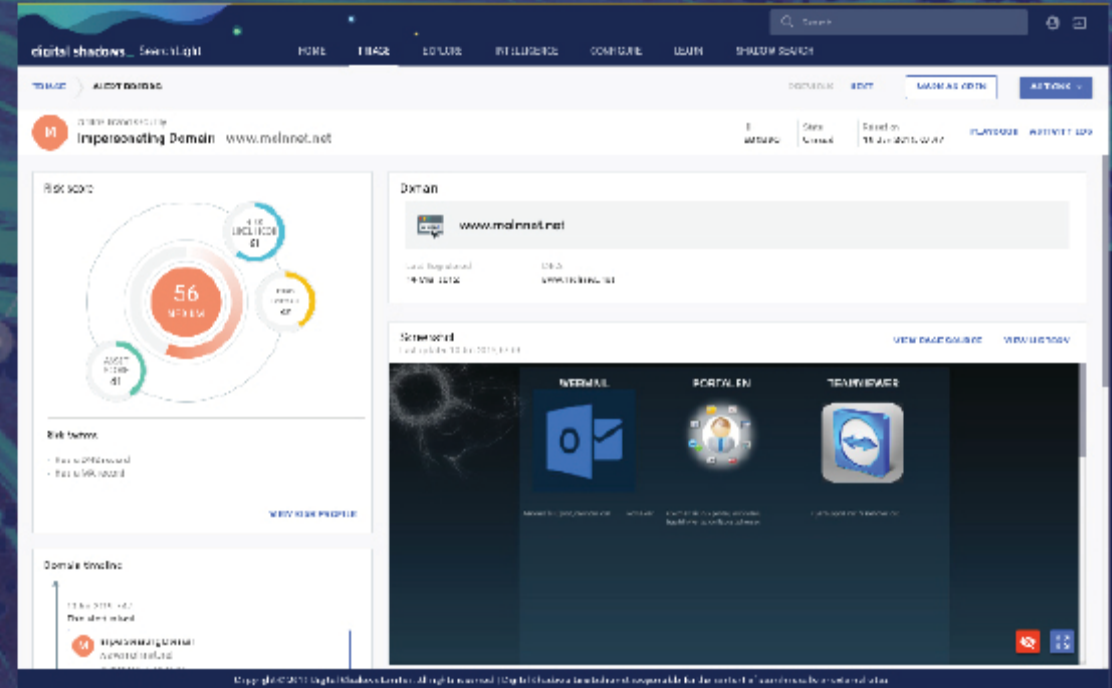
Understand the types of exposure that leave your business at risk.

PHISHING PROTECTION

Discover attackers impersonating your domains, social accounts, and mobile apps before they begin their campaigns targeting employees and customers.

240

SpooF Domains
detected every year for
the average company.

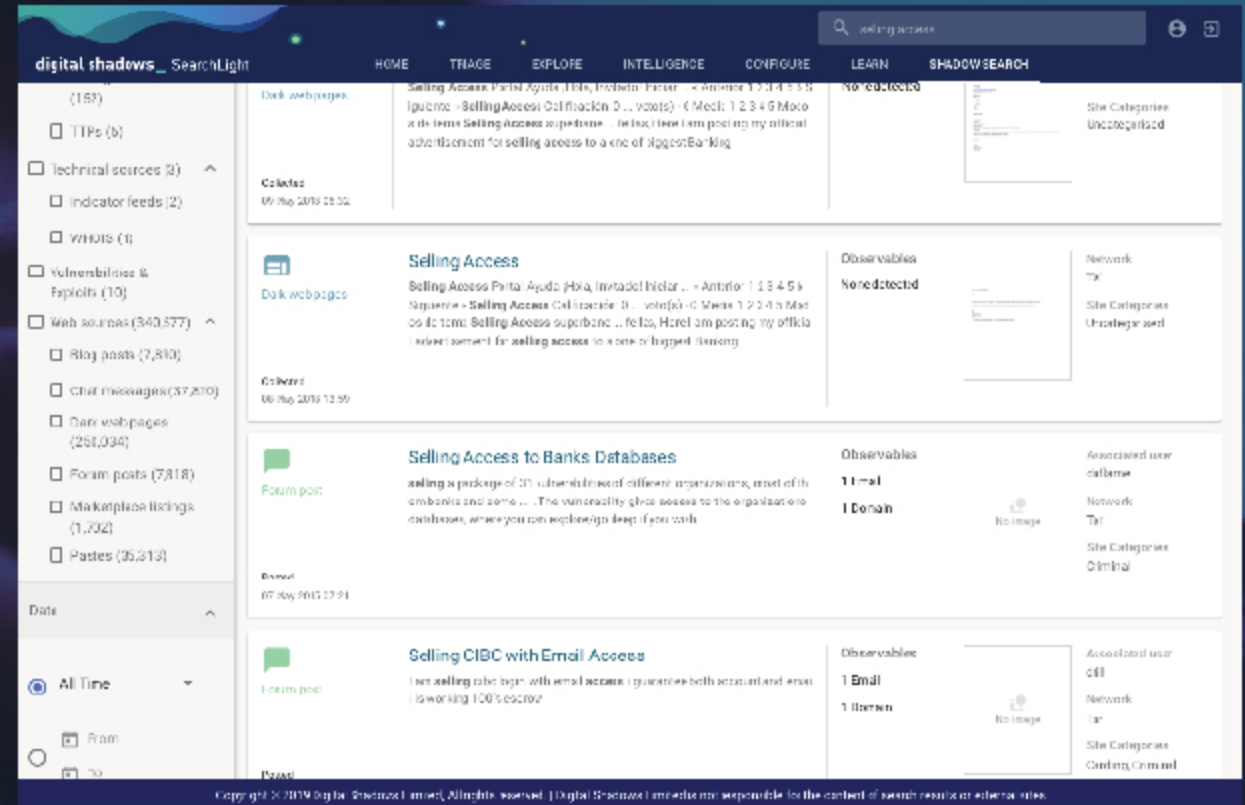


DARK WEB MONITORING

Gain visibility into criminal and fraudulent activity impacting your brand on the deep and dark web.

\$1B

Bitcoin to be spent on
Darknet activity in 2019.



The screenshot displays the 'digital shadows SearchLight' web application interface. The top navigation bar includes links for HOME, TRIAGE, EXPLORE, INTELLIGENCE, CONFIGURE, LEARN, and SHADOW SEARCH. A search bar at the top right contains the query 'selling access'. The left sidebar provides filters for various data types: Dark webpages (157), TTPs (6), Technical sources (2), Indicator feeds (2), WHOIS (6), Vulnerabilities & Exploits (10), Web sources (340,577), Blog posts (7,810), Chat messages (37,200), Dark webpages (251,034), Forum posts (7,818), Marketplace listings (1,792), and Pastes (35,313). The main content area shows three search results for 'selling access':

- Selling Access**: A dark webpage snippet dated 06 May 2019 12:52. The snippet mentions 'Selling Access Portal Ayuda (Hix, Invitado) Hixlar ...' and 'Selling Access Colibras (Hix, Invitado) Hixlar ...'. It also includes a 'Collect' button.
- Selling Access to Banks Databases**: A forum post snippet dated 07 May 2019 12:51. The snippet mentions 'selling a package of 31 vulnerabilities of different organizations, most of them are banks and some ...'. It includes a 'Collect' button.
- Selling CIBC with Email Access**: A forum post snippet dated 07 May 2019 12:51. The snippet mentions 'I am selling cbc login with email access i guarantee both account and email is working 100% escrowed'. It includes a 'Collect' button.

Each result card displays a title, a brief description, a date, and a 'Collect' button. The interface also shows a 'No image' placeholder for the results.

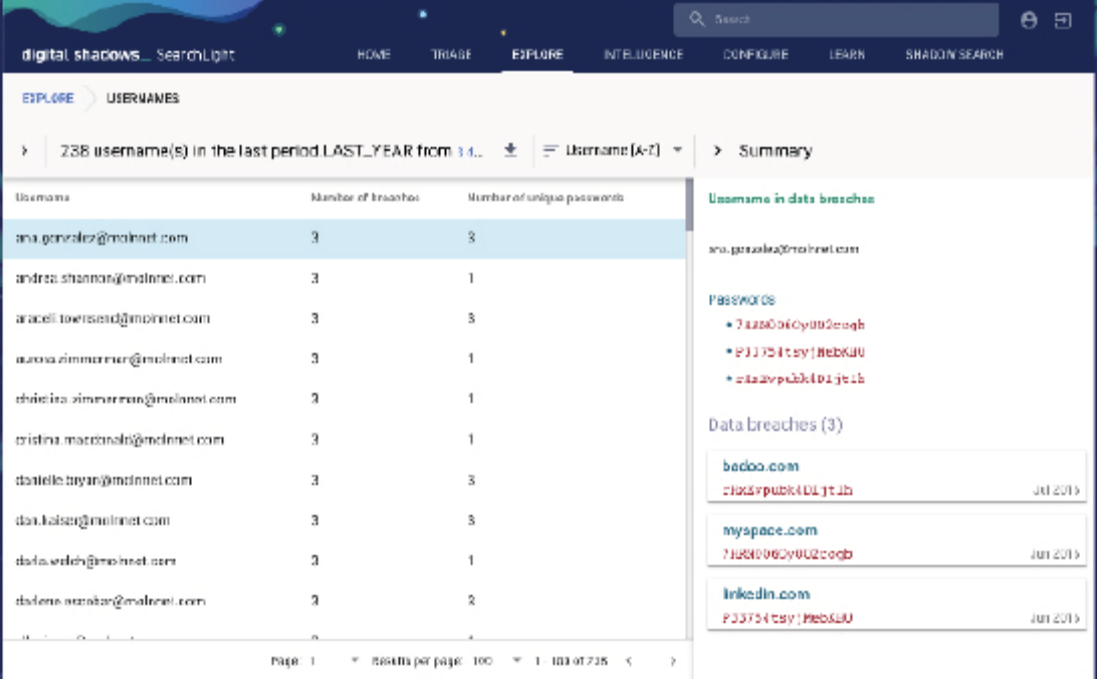
Copyright © 2019 Digital Shadows Limited. All rights reserved. | Digital Shadows Limited is not responsible for the content of search results or external sites.

ACCOUNT TAKEOVER PREVENTION

Detect exposed
employee credentials
before attackers do.

80%

of hacking-related breaches
still involve compromised and
weak credentials.



The screenshot shows the 'digital shadows SearchLight' interface. The top navigation bar includes links for HOME, TRIAGE, EXPLORE (active), INTELLIGENCE, CONFIGURE, LEARN, and SHADOW SEARCH. A search bar is located on the right. The main content area is titled 'EXPLORE > USERNAMES'. It displays a summary of '238 username(s) in the last period LAST_YEAR from 14...'. Below this is a table with three columns: Username, Number of breaches, and Number of unique passwords. The table lists several usernames and their associated breach counts and unique password counts. To the right of the table, there is a 'Summary' section with a 'Username in data breaches' list, a 'PASSWORDS' section with a list of passwords, and a 'Data breaches (3)' section with a list of breaches.

Username	Number of breaches	Number of unique passwords
ana.gonzalez@molinet.com	3	3
andrea.shannon@molinet.com	3	1
araceli.towers@molinet.com	3	3
awana.zimmerman@molinet.com	3	1
chrislin.zimmerman@molinet.com	3	1
crislin.mcdonald@molinet.com	3	1
danielle.bryan@molinet.com	3	3
dani.hansen@molinet.com	3	3
david.welch@molinet.com	3	1
shelene.walker@molinet.com	3	2

Page 1 Results per page: 100 1 of 238

Username in data breaches

- ana.gonzalez@molinet.com

PASSWORDS

- 7428096Cy002eugh
- P33754tsy|HebKdU
- 7428096Cy002eugh

Data breaches (3)

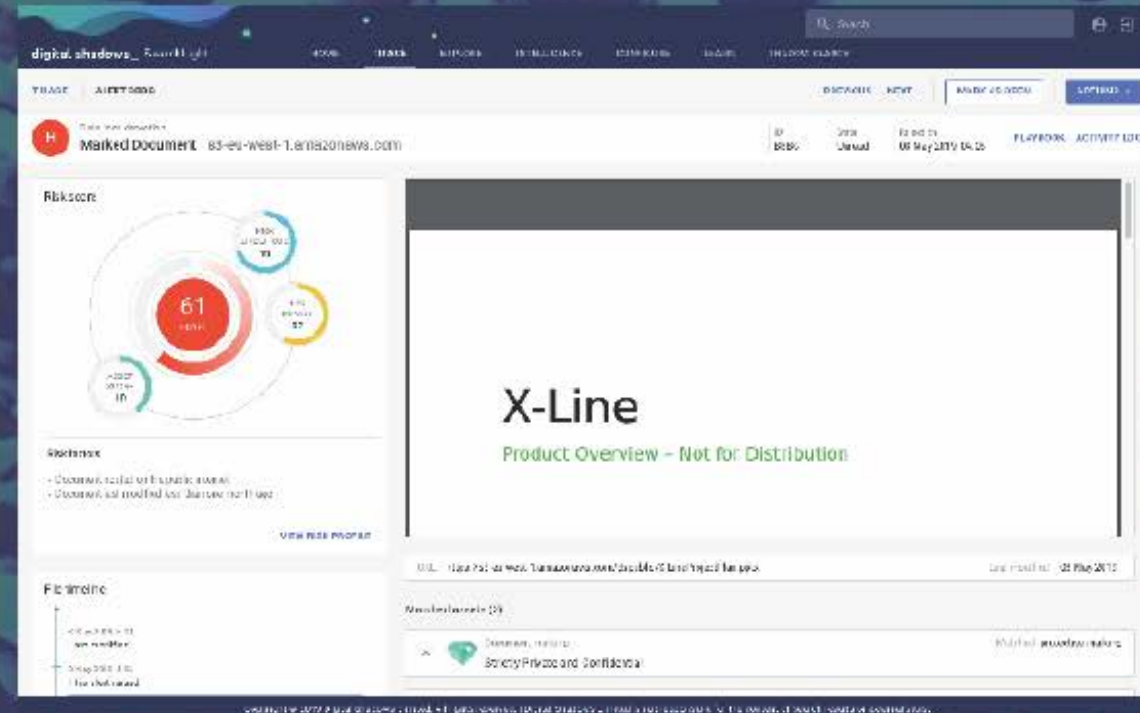
- badco.com
7428096Cy002eugh Jul 2015
- myspace.com
7428096Cy002eugh Jun 2015
- linkedin.com
P33754tsy|HebKdU Jun 2015

DATA LEAKAGE DETECTION

Detect sensitive data that's been exposed by employees, contractors, or third parties.

50%

of Companies
detect exposed
data every week.



DIGITAL FOOTPRINT MONITORING

Gain an attackers-eye-view
of your external-facing
infrastructure.

digital shadows_ SearchLight

HOME TRACE EXPLORE INTELLIGENCE CONFIGURE LEARN SHADOW SEARCH

TRACE INCIDENT: CVE-2006-3747

PREVIOUS NEXT ACTIONS

SEVERITY VERY HIGH Information: Common vulnerability exposure CVE-2006-3747 with 4 exploits detected on 192.168.222.200.

Status: Bad Based on: 11 Jul 2015, 10:12 ACTIVITY LOG

Description

Host IP: 192.168.222.200
CVE Number: CVE-2006-3747
CVSS Score: 7.5

Off-by-one error in the idag scheme handling in the Rewrite module (mod_rewrite) in Apache 1.3 from 1.3.28, 2.0.46 and other versions before 2.0.59 and 2.2, when RewriteEngine is enabled, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted URLs that are not properly handled using various rewrite rules.

4 different working exploits including one metasploit module indicate the severity of this vulnerability and the high rate of successful exploitation.

However this flaw does not affect a default installation of Apache HTTP Server. Users who do not use or have not enabled, the Rewrite module mod_rewrite are not affected by this issue.

Impact

Exploit details:

- (<https://www.exploit-db.com/exploits/1237/>)
- (<https://www.exploit-db.com/exploits/1996/>)
- (<https://www.exploit-db.com/exploits/1680/>)

This module requires RENDIRPATH option to be set accurately. In addition, the target must have RewriteEngine on, configured, with a specific RewriteRule condition enabled to allow for exploitation. The flaw affects multiple platforms, however this module currently only supports Windows based installations. (<https://www.exploit-db.com/exploits/1575/>)

4 different working exploits including one metasploit module indicate the severity of this vulnerability and the high rate of successful exploitation.

192.168.222.200

10 Active DITs by Shadow

Network details

CVE-2006-3747

CVSS	Auth
7.5	None
Access	Unauthenticated
Network	28 Jul 2006

Apache (mod_rewrite) < 1.3.37 / 2.0.59 / 2.2.3 - Remote Overflow (PoC)

Apache 2.0.58 mod_rewrite (Windows 2003) - Remote Overflow



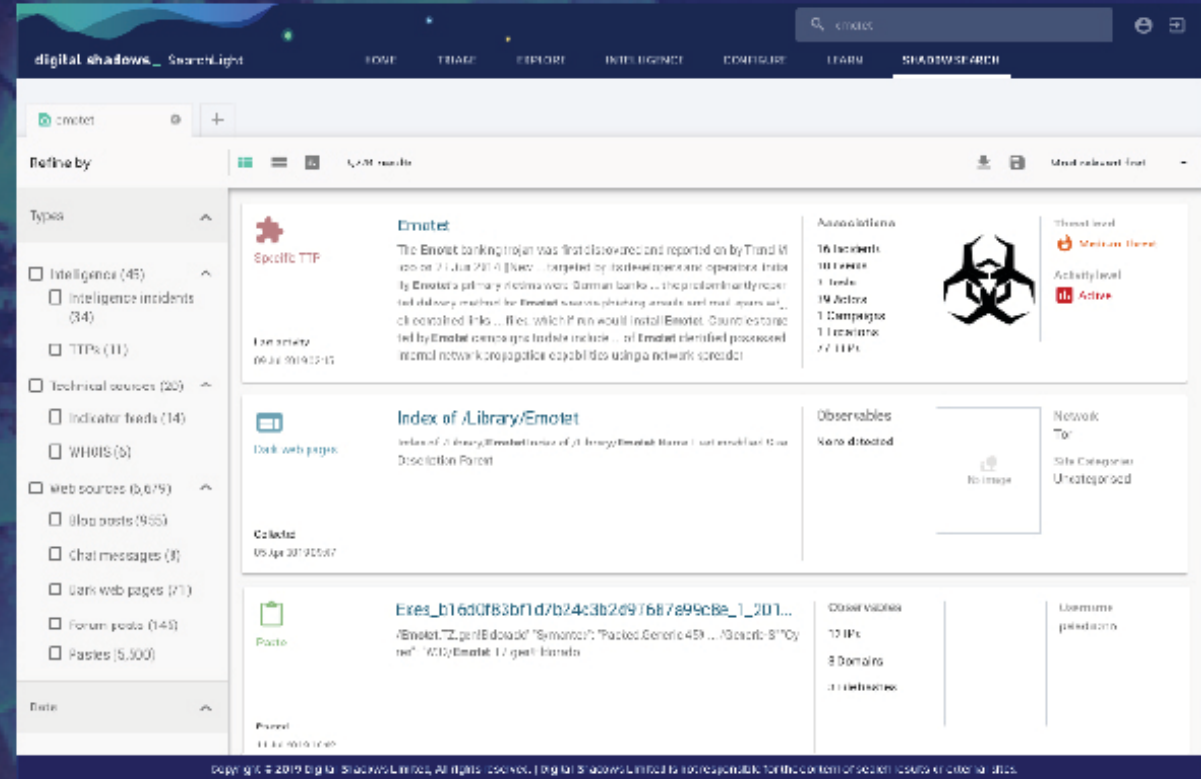
of organizations do not have sufficient understanding of their attack surface.

THREAT INTELLIGENCE

Understand threat actors,
their behavior, and the assets
they target.

72%

of companies
produce or
consume Cyber
Threat Intelligence.



ABOUT DIGITAL SHADOWS

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats.

Ready to get started understanding your risk and protecting your business?

Visit

www.digitalshadows.com