ENTERPRISE RECON FOR PURPLE TEAMS

Jordan Drysdale @rev10d

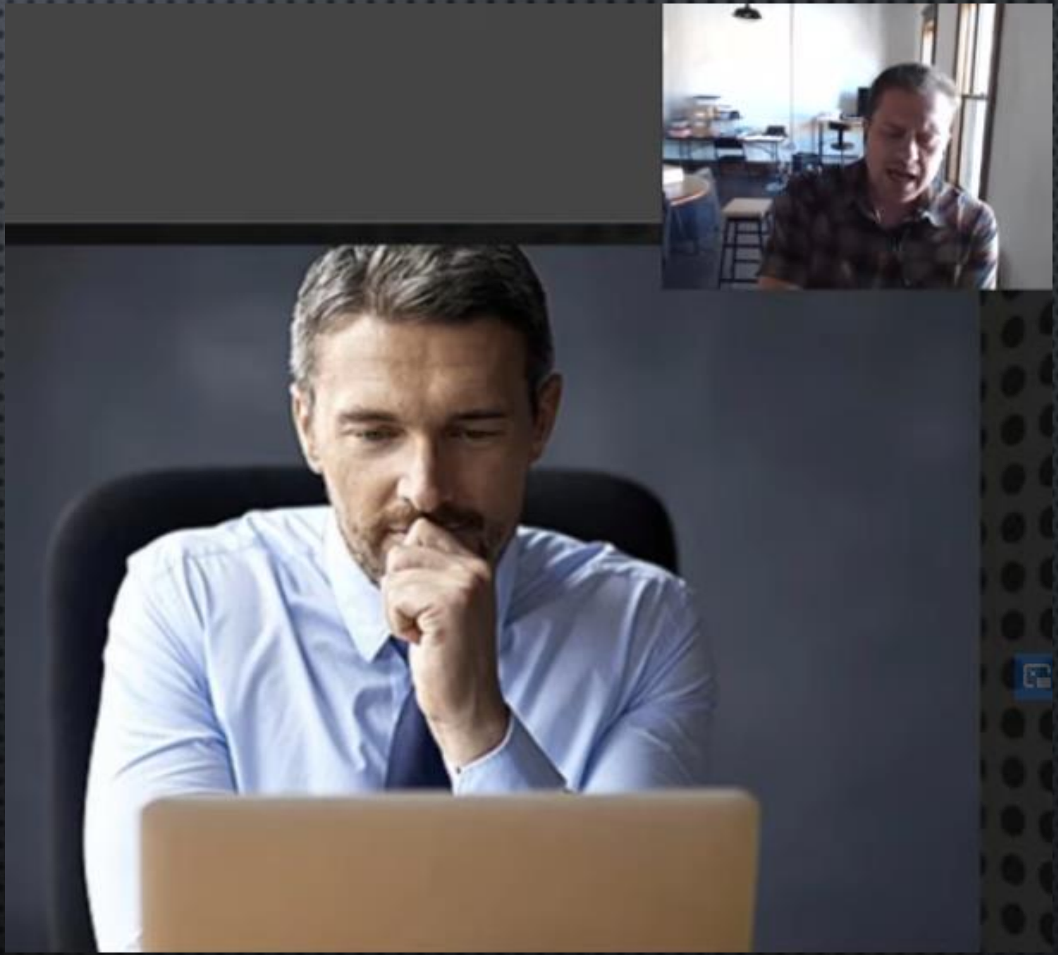
Kent Ickler @krelkci

Black Hills Information Security @BHInfoSecurity

EXECUTIVE PROBLEM STATEMENT

So Much information On the Internet

- Organization
- Employees
- Leadership
- Technologies
- Security
- Partnerships, Vendors, Clients



RECON YOU SAY?

What can be found about your…

- Organization
- Employees
- Leadership
- Technologies
- Security
- Partnerships, Vendors, Clients

RECON YOU SAY?

- OSINT
  - Opensource Intelligence
  - Using Publicly available data with context to abstract useful information
  - Media, Internet, Public Government Data
  - Professional / Academic Publications
  - Commercial Data,"grey Literature"
  - Unintentional other disclosures

CONTROL OF OSINT IS DIFFICULT

Sources can be difficult to control

- Social Media of Employees. Leadership
- Posts to 3rd part services may require legal intervention
- Can be Unintentional slips by Marketing, Human Resources, Development

INTERNALLY, HR IS YOUR FRIEND… SOMETIMES

POLICIES?

- CAN WE REALLY TELL AN EMPLOYEE WHAT THEY CAN'T DO ON THEIR PERSONAL PROFILE?
- COMPANY HADNBOOK LAYS SOME GROUND RULES

AND…

- DID WE MENTION HIRING MANAGERS TOO OFTEN ADD SPECIFIC TECHNOLOGY REQUIREMENTS TO JOB POSTINGS?

INTERNALLY, MARKETING IS YOUR FRIEND… SOMETIMES

All that communication management!

- Marketing sets the feel for the organization. They can manage PR and be your goto SME on Social media
- Can help coordinate reduction of OSINT related to the public website and external communication platforms.

And…

- Marketing doesn't always think that the latest post might disclose something sensnstive.
- Example: Photo of employee's industry recognition , badges visible and all.

BUT WHAT CAN A ~~BLUE~~ PURPLE TEAM DO?

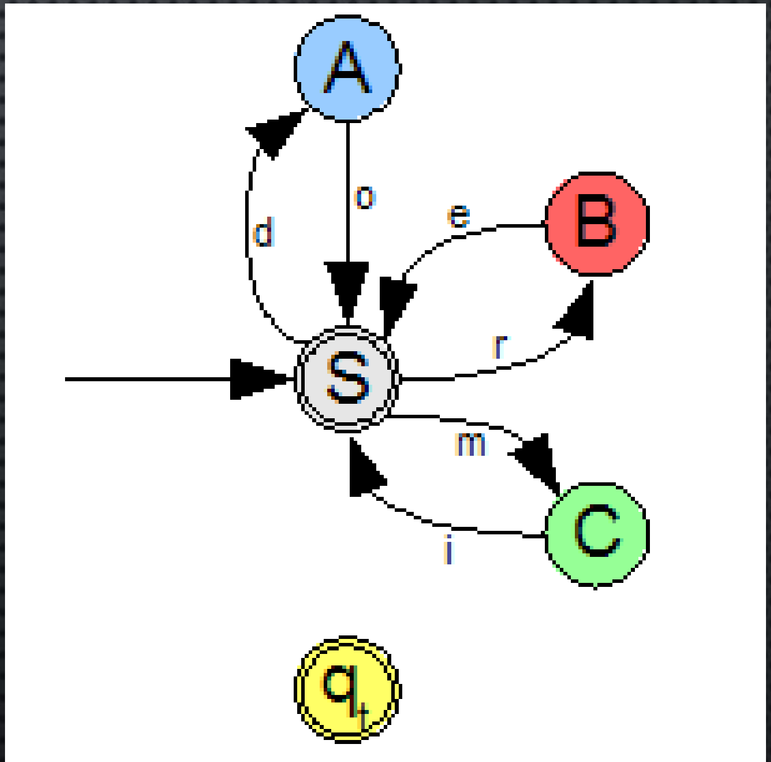
Hunting (yourself) alone is expensive and time consuming… It does get results.

Hiring someone else may be efficient, but also expensive… It does ger Results

Blueteam already knows, right? Yes, if they are looking.

Can we just automate the entire thing?

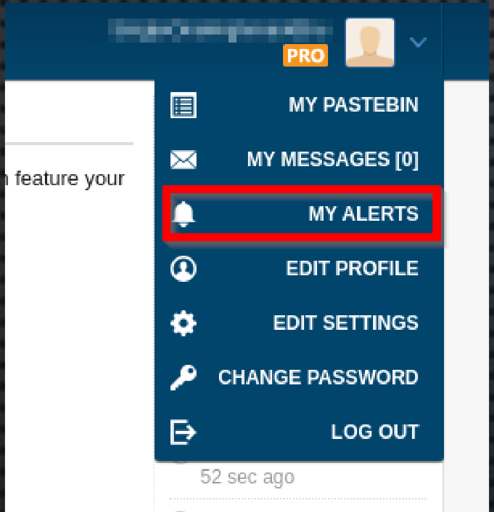
Yes.. Well.. No…. Err…



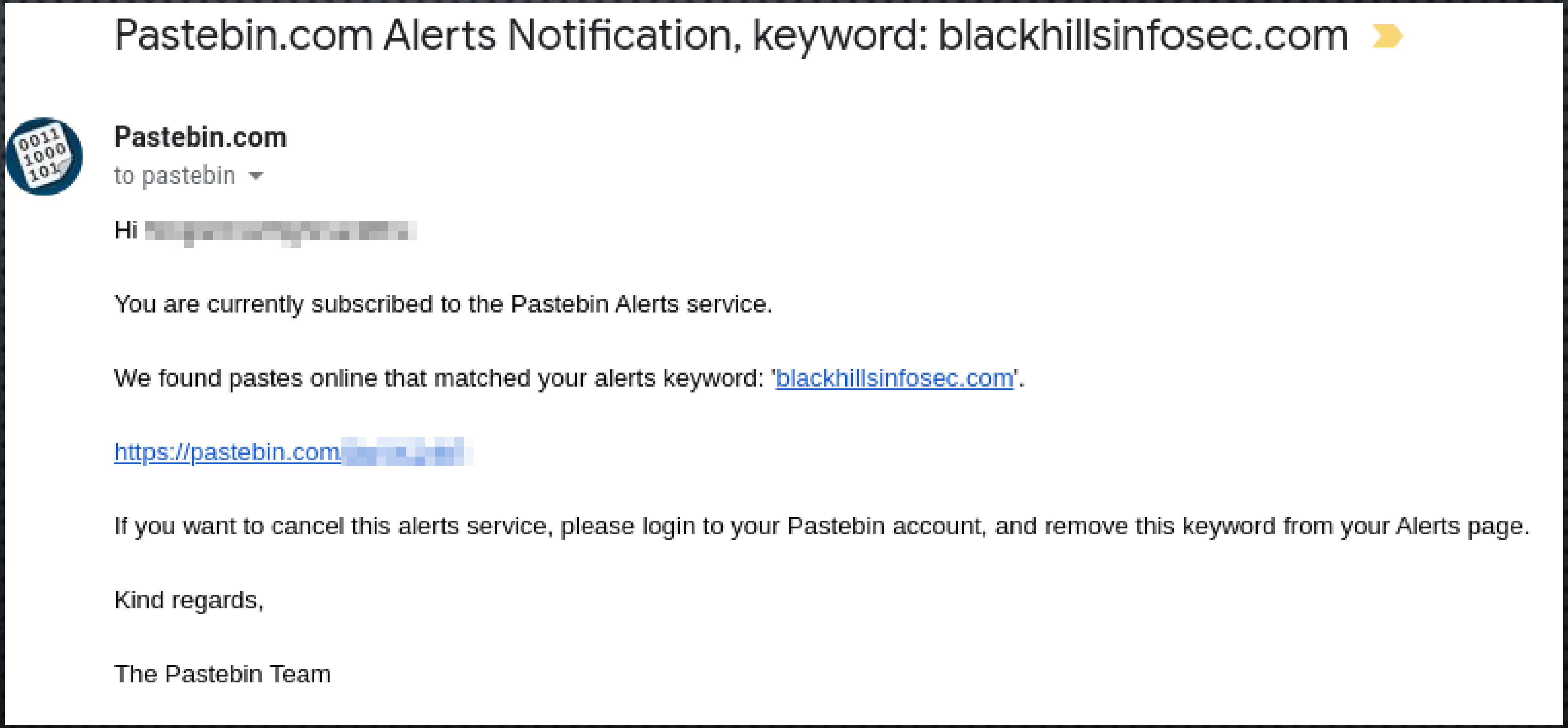
LETS TALK ABOUT THOSE SOURCES

- Pastebin – Email dumps, hash dumps, proprietary knowledge, logging, code
- Github – Typically source code, re-used code. Sometimes private keys/static passwords
- Shodan – Network Topology
- Been Verified & the likes – Too much personal info on anyone.
- Facebook, Twitter, Instagram, Reddit – Relationship Information, Projects, Vendors…
- Monster, LinkedIn – Technologies listed in Job Posting?
- Public Website and Portals – Employee names, email addresses, technologies

PASTEBIN API AND ALERTS



https://pastebin.com/alerts



Pastebin.com Alerts Notification, keyword: blackhillsinfosec.com

Pastebin.com
to pastebin

Hi [redacted]

You are currently subscribed to the Pastebin Alerts service.

We found pastes online that matched your alerts keyword: 'blackhillsinfosec.com'.

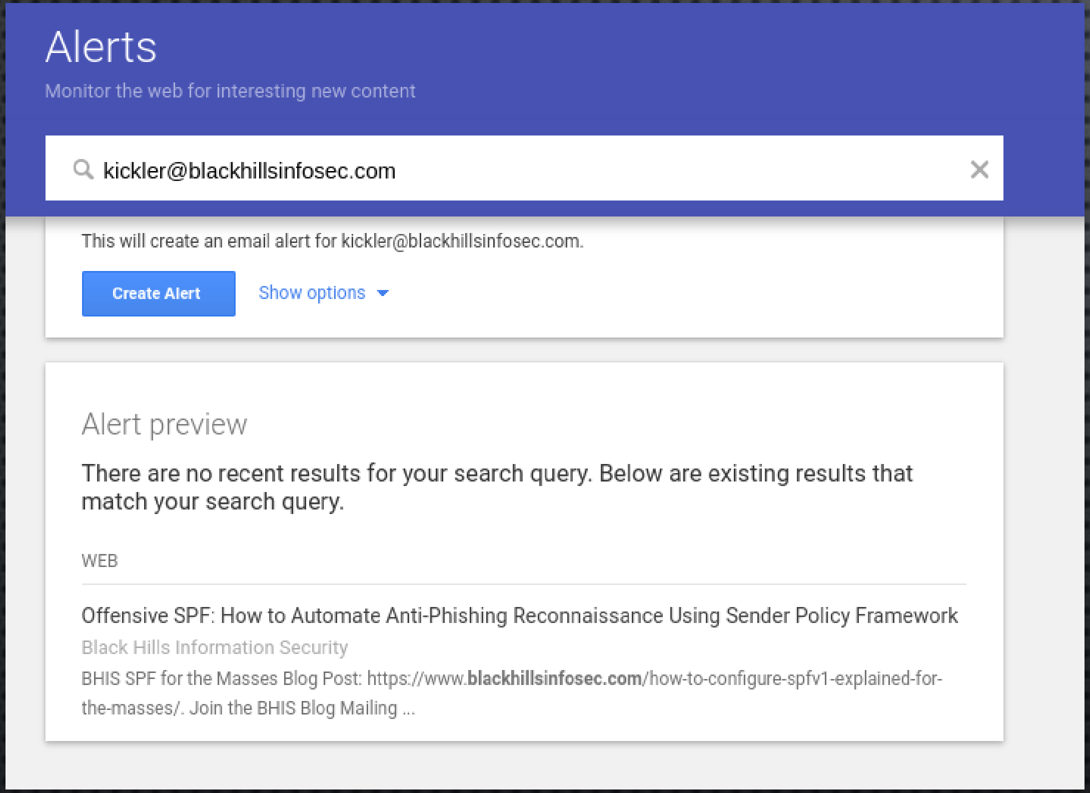
https://pastebin.com/[redacted]

If you want to cancel this alerts service, please login to your Pastebin account, and remove this keyword from your Alerts page.

Kind regards,

The Pastebin Team

GOOGLE SEARCH ALERTS



Alerts

Monitor the web for interesting new content

kickler@blackhillsinfosec.com

This will create an email alert for kickler@blackhillsinfosec.com.

Alert preview

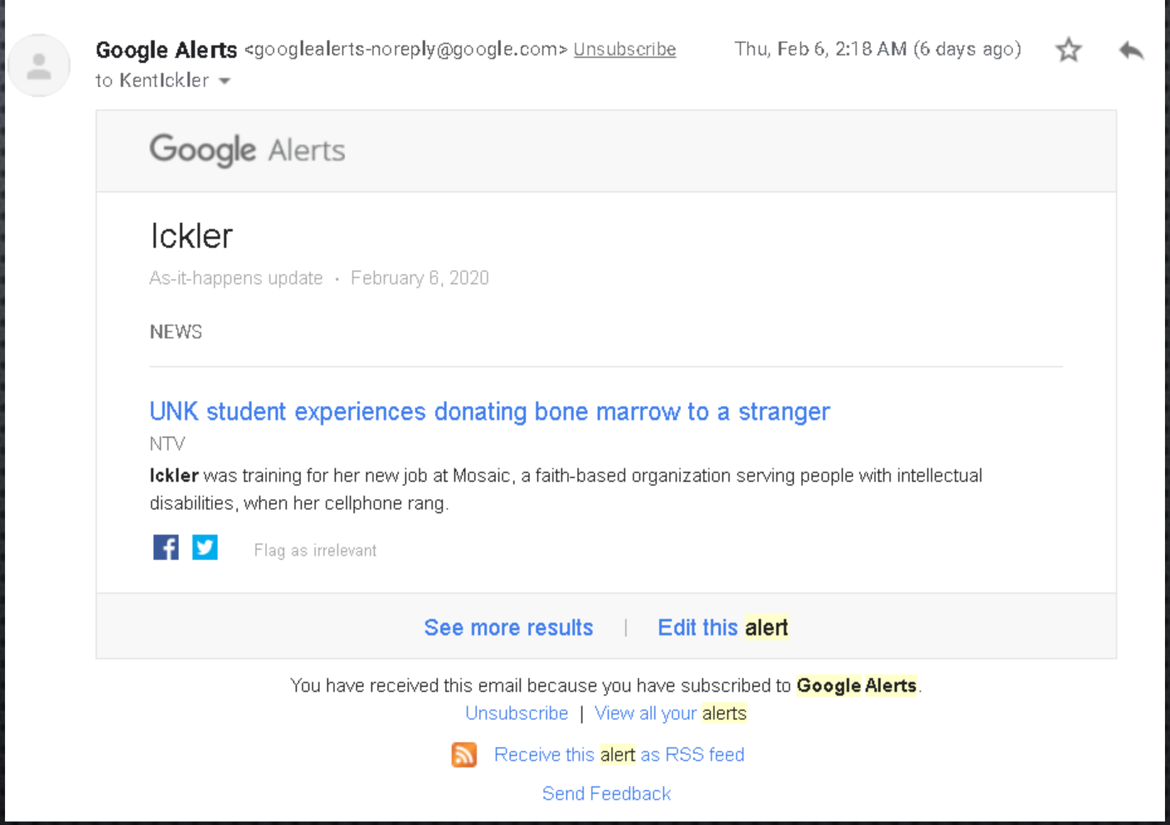
There are no recent results for your search query. Below are existing results that match your search query.

WEB

Offensive SPF: How to Automate Anti-Phishing Reconnaissance Using Sender Policy Framework

Black Hills Information Security

BHIS SPF for the Masses Blog Post: https://www.**blackhillsinfosec.com**/how-to-configure-spfv1-explained-for-the-masses/. Join the BHIS Blog Mailing ...



Google Alerts <googlealerts-noreply@google.com> Unsubscribe   Thu, Feb 6, 2:18 AM (6 days ago)

to KentIckler

Google Alerts

Ickler

As-it-happens update · February 6, 2020

NEWS

UNK student experiences donating bone marrow to a stranger

NTV

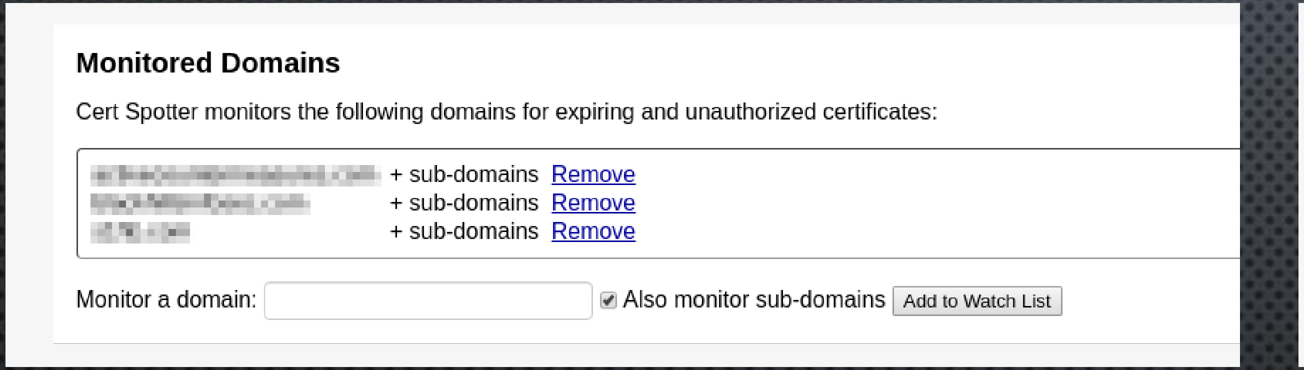
Ickler was training for her new job at Mosaic, a faith-based organization serving people with intellectual disabilities, when her cellphone rang.

You have received this email because you have subscribed to **Google Alerts**.

Unsubscribe | View all your alerts
Receive this alert as RSS feed
Send Feedback

https://www.google.com/alerts

CERTIFICATE TRANSPARENCY LOGS - SSLMATE

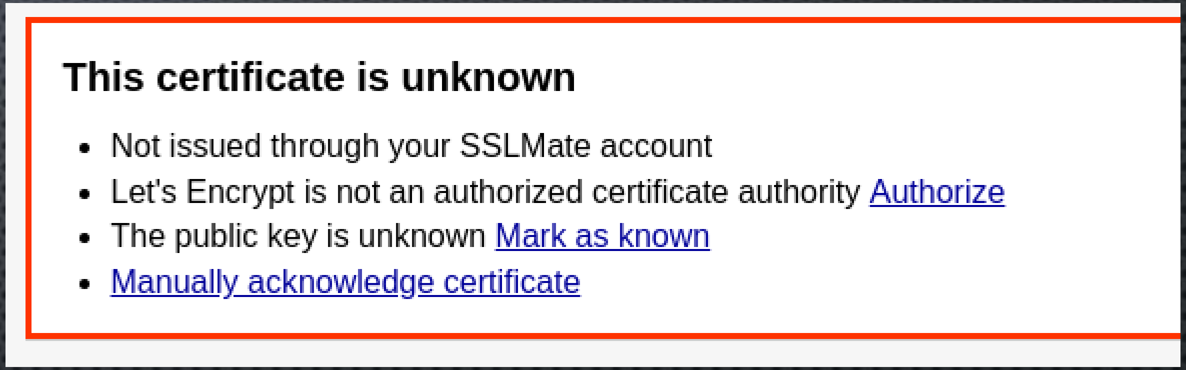


Monitored Domains

Cert Spotter monitors the following domains for expiring and unauthorized certificates:

[redacted] + sub-domains Remove
[redacted] + sub-domains Remove
[redacted] + sub-domains Remove

Monitor a domain: ☑ Also monitor sub-domains



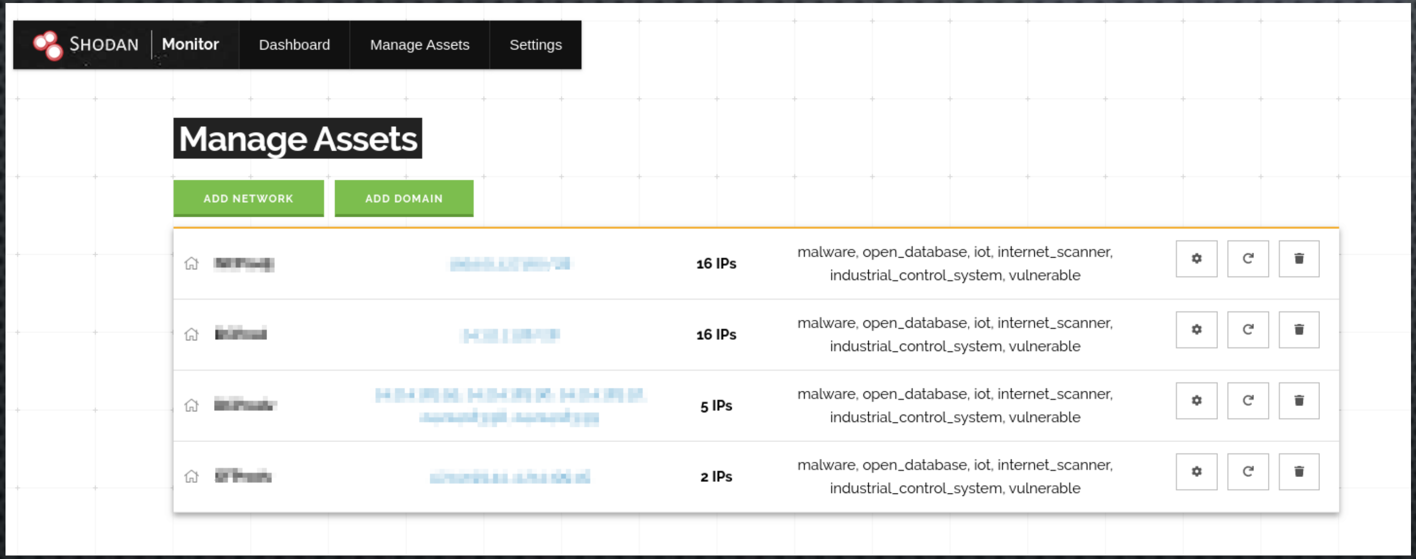
This certificate is unknown

- Not issued through your SSLMate account
- Let's Encrypt is not an authorized certificate authority Authorize
- The public key is unknown Mark as known
- Manually acknowledge certificate

SEARCHING CERTIFICATE TRANSPARENCY LOGS FOR UNAUTHORIZED CERTIFICATES

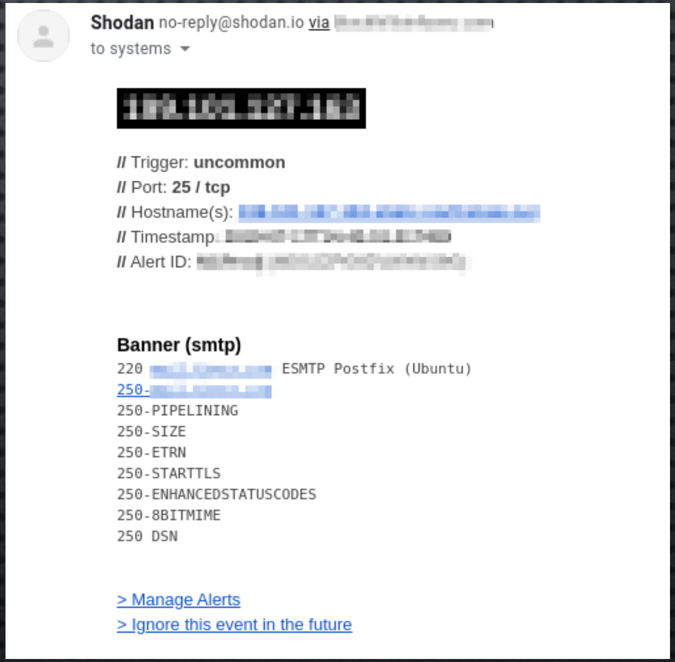
https://github.com/SSLMate/certspotter
https://sslmate.com/console/monitoring/

SHODAN MONITORING AND ALERTS



Manage Assets

[redacted]	[redacted]	16 IPs	malware, open_database, iot, internet_scanner, industrial_control_system, vulnerable
[redacted]	[redacted]	16 IPs	malware, open_database, iot, internet_scanner, industrial_control_system, vulnerable
[redacted]	[redacted]	5 IPs	malware, open_database, iot, internet_scanner, industrial_control_system, vulnerable
[redacted]	[redacted]	2 IPs	malware, open_database, iot, internet_scanner, industrial_control_system, vulnerable



Shodan no-reply@shodan.io via [redacted]
to systems

[redacted]

// Trigger: **uncommon**
// Port: **25 / tcp**
// Hostname(s): [redacted]
// Timestamp: [redacted]
// Alert ID: [redacted]

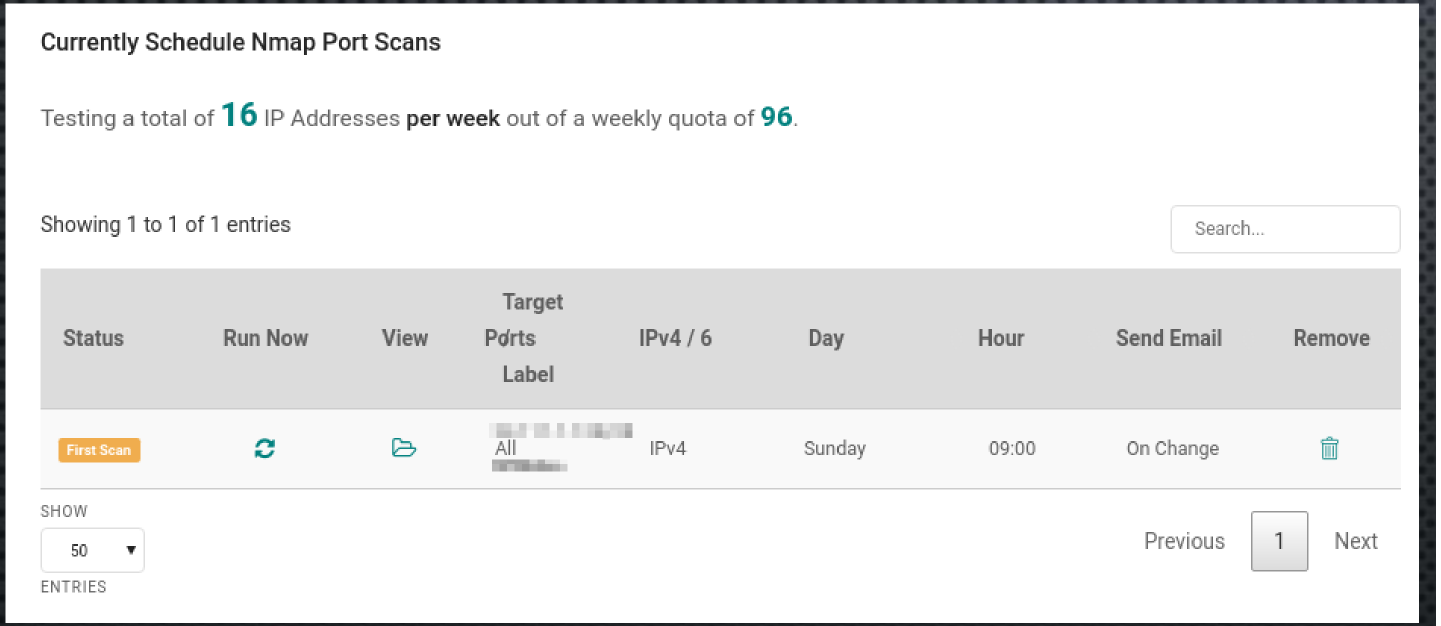
Banner (smtp)

```
220 [redacted] ESMTP Postfix (Ubuntu)
250-[redacted]
250-PIPELINING
250-SIZE
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

> Manage Alerts
> Ignore this event in the future

https://monitor.shodan.io/

HACKERTARGET.COM

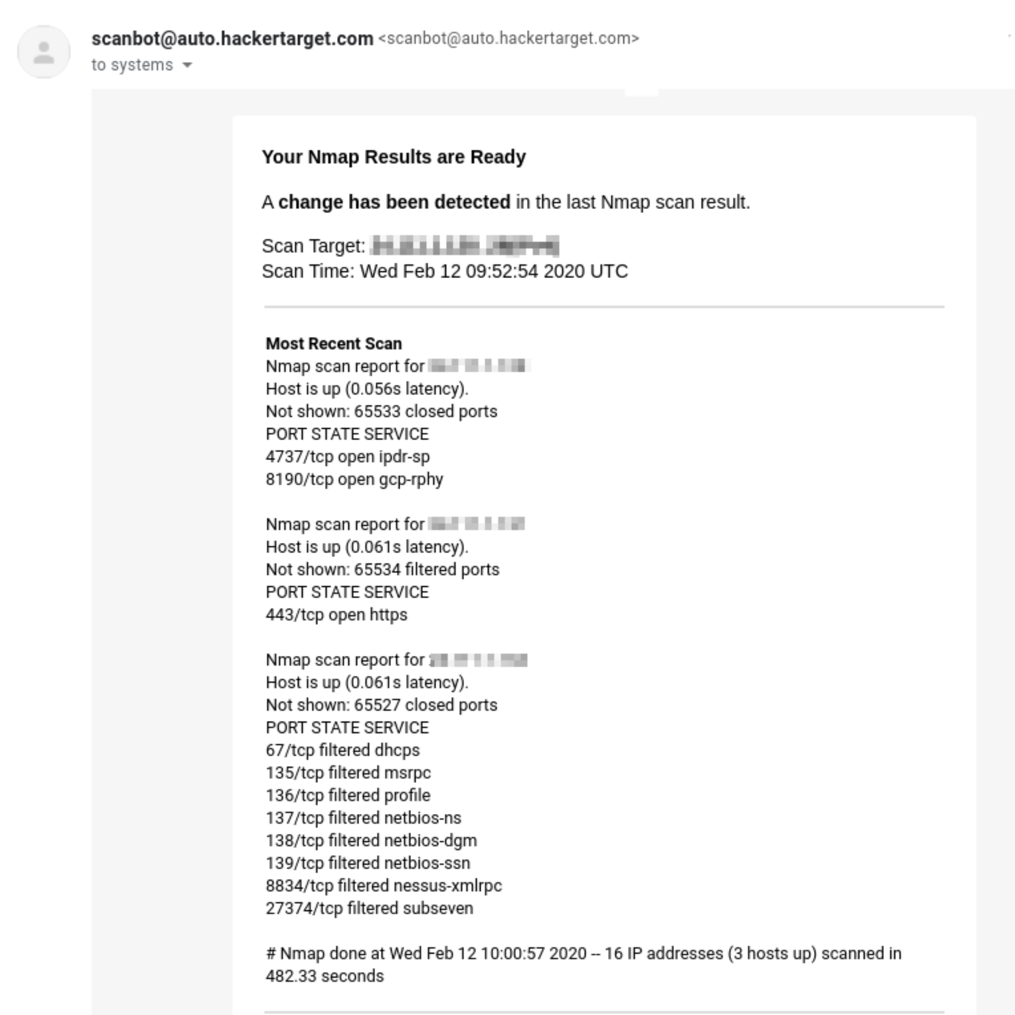


Currently Schedule Nmap Port Scans

Testing a total of **16** IP Addresses **per week** out of a weekly quota of **96**.

Showing 1 to 1 of 1 entries

Status	Run Now	View	Target Ports Label	IPv4 / 6	Day	Hour	Send Email	Remove
First Scan	↻	🗁	[redacted] All [redacted]	IPv4	Sunday	09:00	On Change	🗑



scanbot@auto.hackertarget.com <scanbot@auto.hackertarget.com>
to systems

Your Nmap Results are Ready

A **change has been detected** in the last Nmap scan result.

Scan Target: [redacted]
Scan Time: Wed Feb 12 09:52:54 2020 UTC

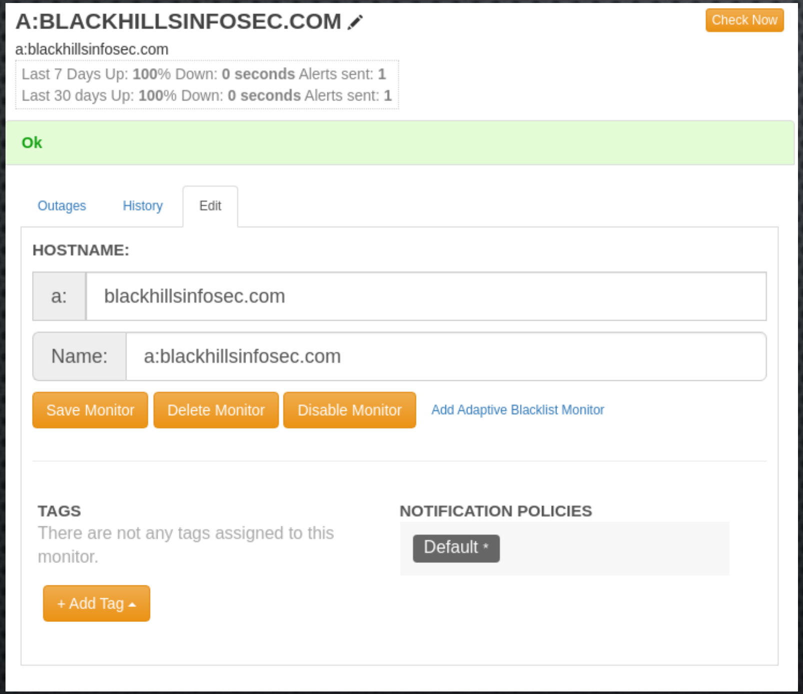
Most Recent Scan

```
Nmap scan report for [redacted]
Host is up (0.056s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE
4737/tcp open ipdr-sp
8190/tcp open gcp-rphy

Nmap scan report for [redacted]
Host is up (0.061s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE
443/tcp open https

Nmap scan report for [redacted]
Host is up (0.061s latency).
Not shown: 65527 closed ports
PORT STATE SERVICE
67/tcp filtered dhcps
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
8834/tcp filtered nessus-xmlrpc
27374/tcp filtered subseven

# Nmap done at Wed Feb 12 10:00:57 2020 -- 16 IP addresses (3 hosts up) scanned in 482.33 seconds
```

https://hackertarget.com/scheduled-nmap/

https://hackertarget.com/dashboard/

MX TOOLBOX – DOMAIN, WHOIS, DNS, TCP



A:BLACKHILLSINFOSEC.COM

a:blackhillsinfosec.com

Last 7 Days Up: **100%** Down: **0 seconds** Alerts sent: **1**
Last 30 days Up: **100%** Down: **0 seconds** Alerts sent: **1**

Ok

HOSTNAME:

a: blackhillsinfosec.com

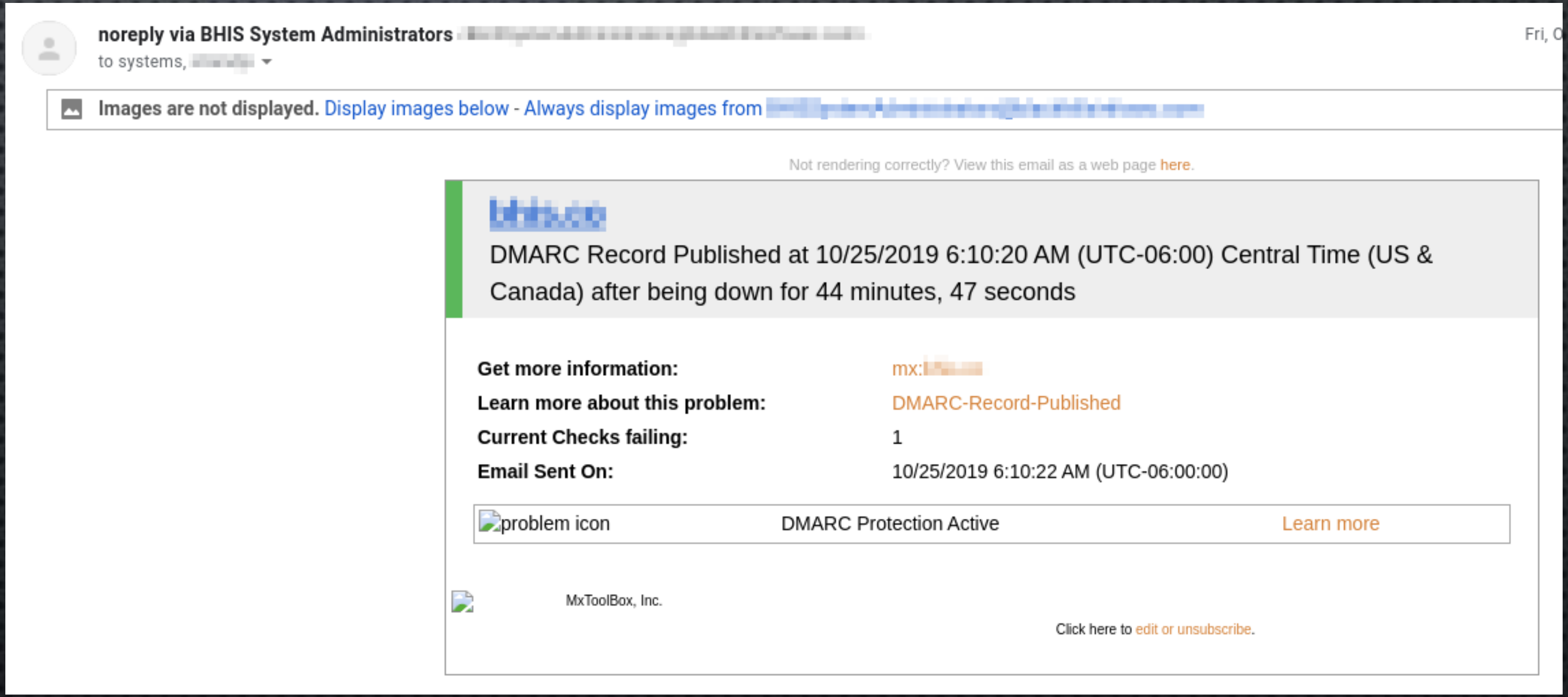
Name: a:blackhillsinfosec.com

TAGS

There are not any tags assigned to this monitor.

NOTIFICATION POLICIES

Default



noreply via BHIS System Administrators [redacted]

to systems, [redacted]

Fri, 0

Images are not displayed. Display images below - Always display images from [redacted]

Not rendering correctly? View this email as a web page here.

[redacted]

DMARC Record Published at 10/25/2019 6:10:20 AM (UTC-06:00) Central Time (US & Canada) after being down for 44 minutes, 47 seconds

Get more information:	mx:[redacted]
Learn more about this problem:	DMARC-Record-Published
Current Checks failing:	1
Email Sent On:	10/25/2019 6:10:22 AM (UTC-06:00:00)

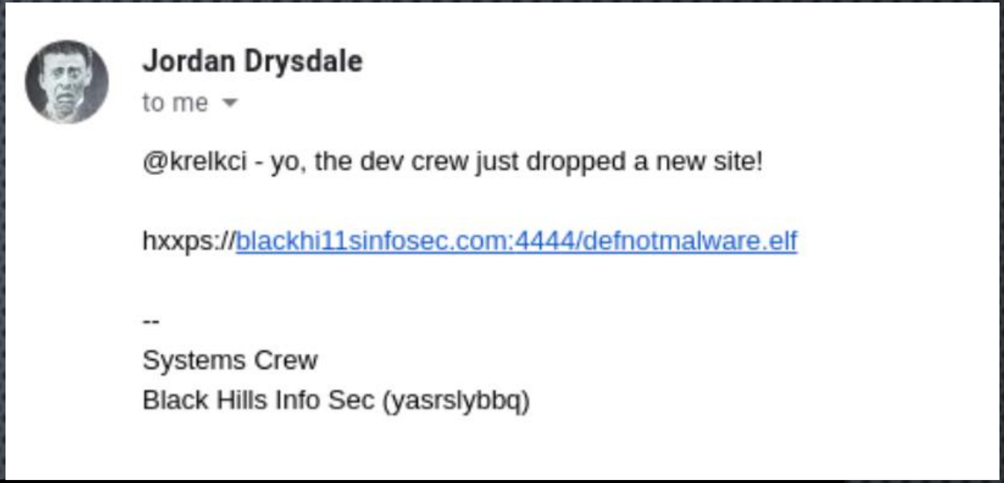
problem icon DMARC Protection Active Learn more

MxToolBox, Inc.

Click here to edit or unsubscribe.

https://mxtoolbox.com/Pro/#/monitor/

URLCRAZY – PHISHY PHISHY

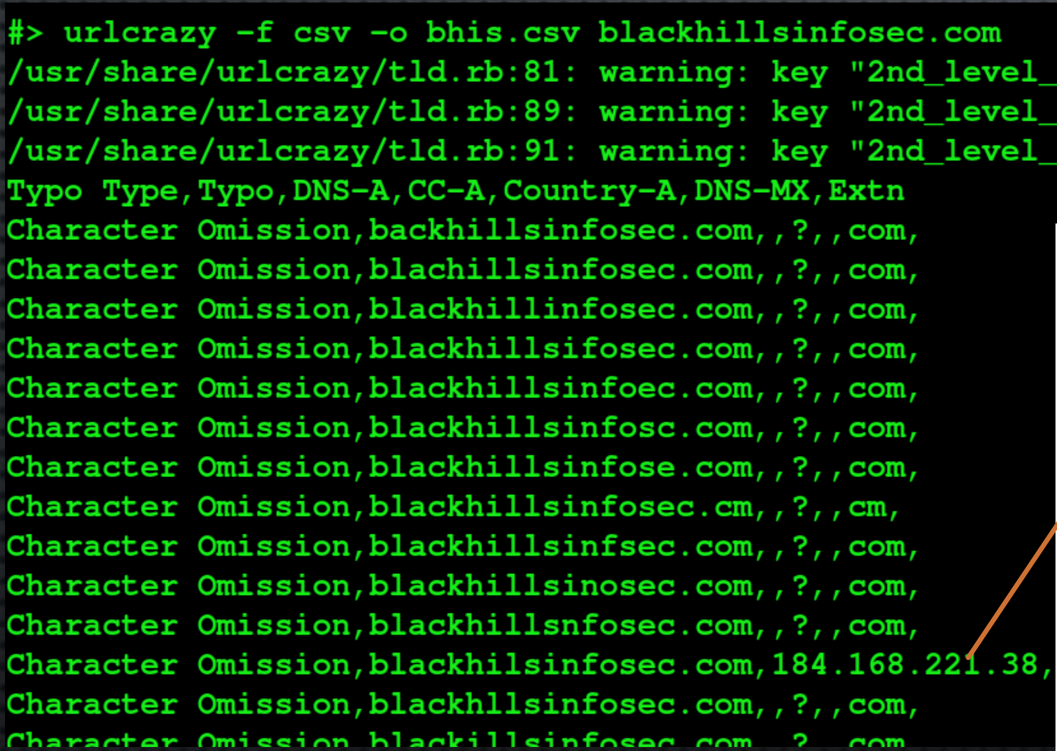


Jordan Drysdale
to me

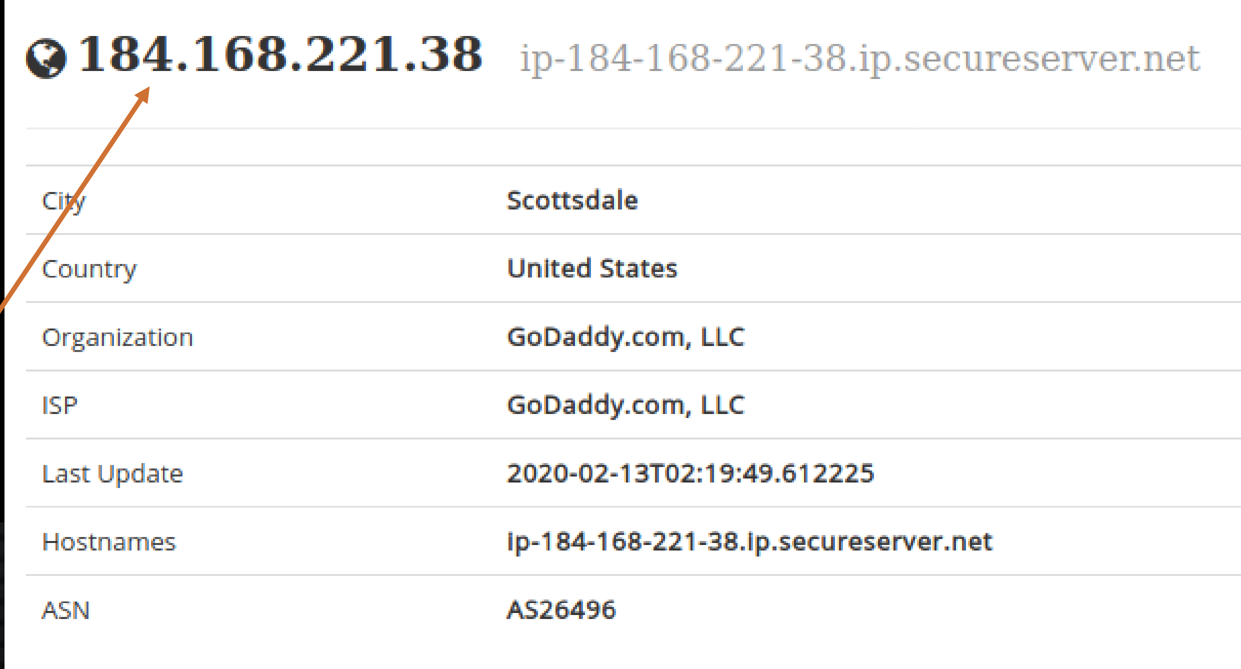
@krelkci - yo, the dev crew just dropped a new site!

hxxps://blackhi11sinfosec.com:4444/defnotmalware.elf

--
Systems Crew
Black Hills Info Sec (yasrslybbq)



```
#> urlcrazy -f csv -o bhis.csv blackhillsinfosec.com
/usr/share/urlcrazy/tld.rb:81: warning: key "2nd_level_registration" is duplicated and overwritten on line 81
/usr/share/urlcrazy/tld.rb:89: warning: key "2nd_level_registration" is duplicated and overwritten on line 89
/usr/share/urlcrazy/tld.rb:91: warning: key "2nd_level_registration" is duplicated and overwritten on line 91
Typo Type,Typo,DNS-A,CC-A,Country-A,DNS-MX,Extn
Character Omission,backhillsinfosec.com,,?,,com,
Character Omission,blachillsinfosec.com,,?,,com,
Character Omission,blackhillinfosec.com,,?,,com,
Character Omission,blackhillsifosec.com,,?,,com,
Character Omission,blackhillsinfoec.com,,?,,com,
Character Omission,blackhillsinfosc.com,,?,,com,
Character Omission,blackhillsinfose.com,,?,,com,
Character Omission,blackhillsinfosec.cm,,?,,cm,
Character Omission,blackhillsinfsec.com,,?,,com,
Character Omission,blackhillsinosec.com,,?,,com,
Character Omission,blackhillsnfosec.com,,?,,com,
Character Omission,blackhilsinfosec.com,184.168.221.38,
Character Omission,blackhllsinfosec.com,,?,,com,
Character Omission,blackillsinfosec.com,,?,,com,
```



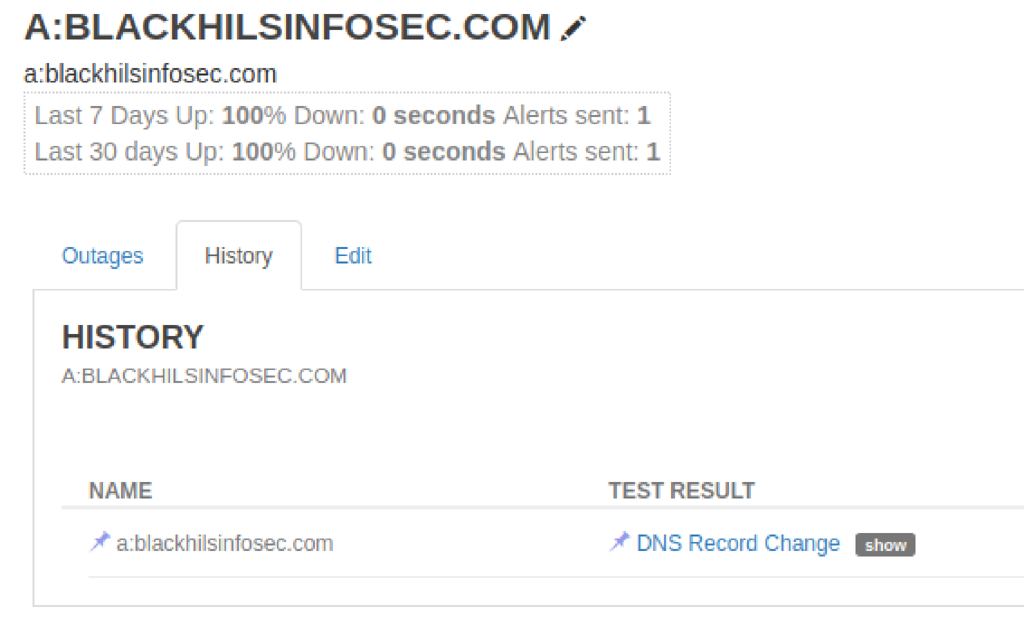
184.168.221.38 ip-184-168-221-38.ip.secureserver.net

City	Scottsdale
Country	United States
Organization	GoDaddy.com, LLC
ISP	GoDaddy.com, LLC
Last Update	2020-02-13T02:19:49.612225
Hostnames	ip-184-168-221-38.ip.secureserver.net
ASN	AS26496

URLCRAZY – PHISHY PHISHY

Why not monitor the typo squats?

Also Legal Recourse, albeit painful...



A:BLACKHILSINFOSEC.COM

a:blackhilsinfosec.com

Last 7 Days Up: **100%** Down: **0 seconds** Alerts sent: **1**
Last 30 days Up: **100%** Down: **0 seconds** Alerts sent: **1**

HISTORY

A:BLACKHILSINFOSEC.COM

NAME	TEST RESULT
a:blackhilsinfosec.com	DNS Record Change show

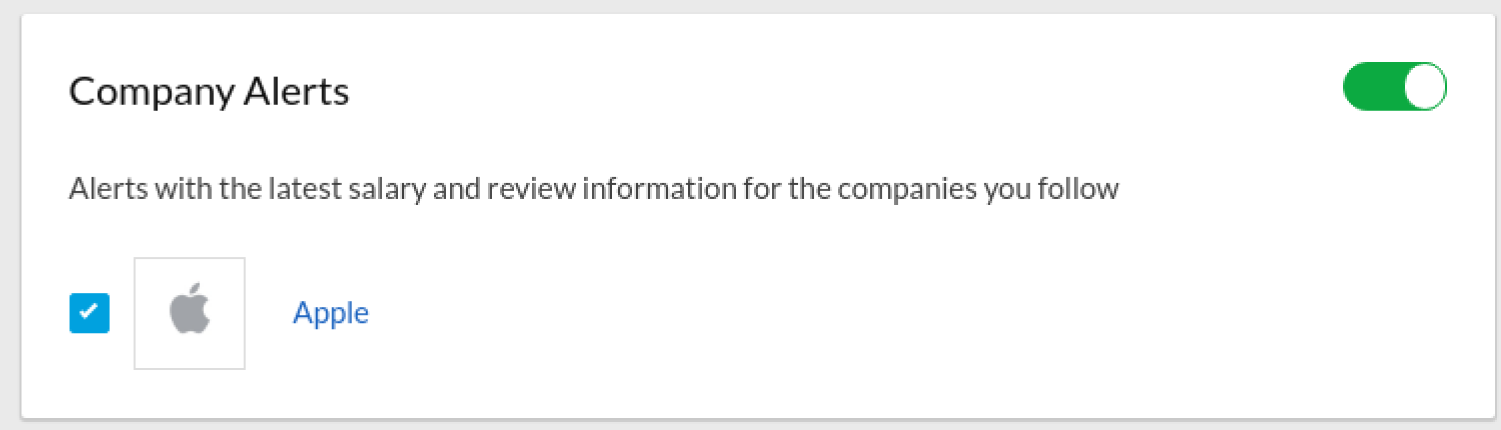
PUBLIC WEBSITE RECON

- MARKETING IS YOUR FRIEND.
- AND, WHO IS UPDATING YOUR WEBSITE?

MONSTER, GLASSDOOR, ETC

CREATE USER ACCOUNTS TO MONITOR JOB POSTINGS (BOTH EXPECTED AND UNEXPECTED)

CREATE EMPLOYER ACCOUNT TO MONITOR REVIEWS / POSTINGS ABOUT ORGANIZATION

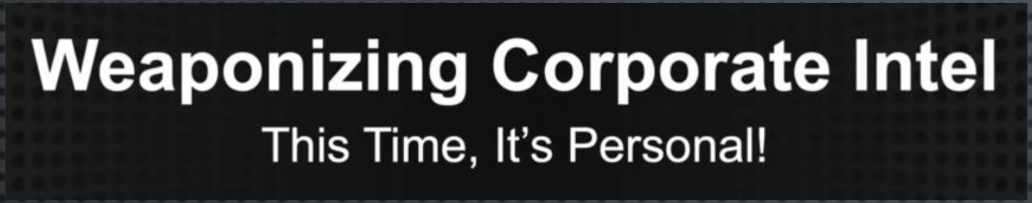


Company Alerts

Alerts with the latest salary and review information for the companies you follow

☑ Apple

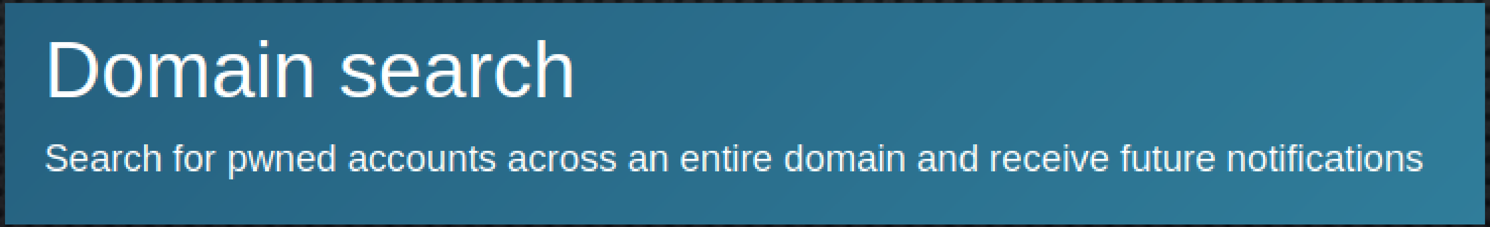
Been Verified, and the like



Weaponizing Corporate Intel

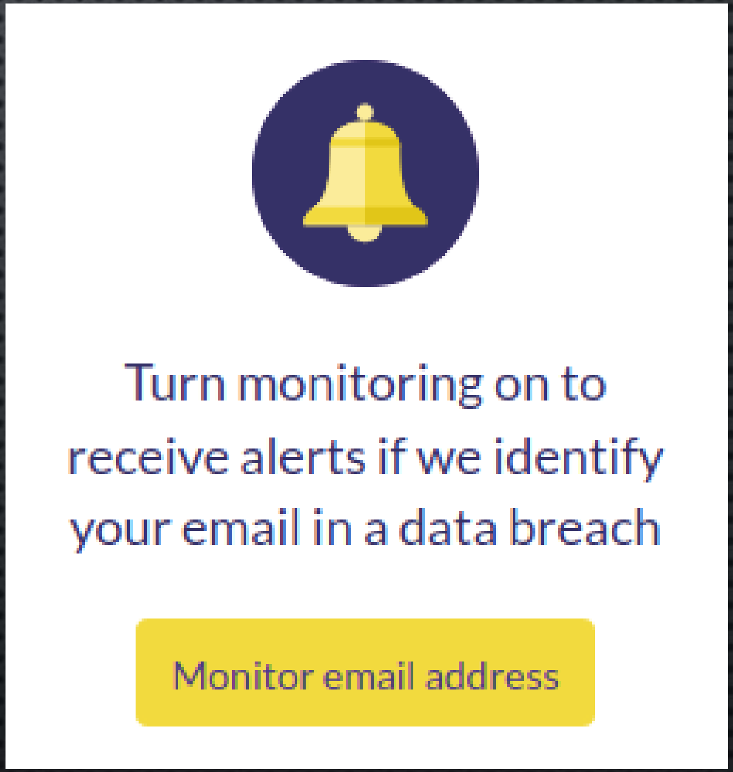
This Time, It's Personal!

- The Data brokers know just about everything
  - And can monitor things too
- Corporate Intel: This time its personal (Webcast)
- HIBP https://haveibeenpwned.com/DomainSearch



Domain search

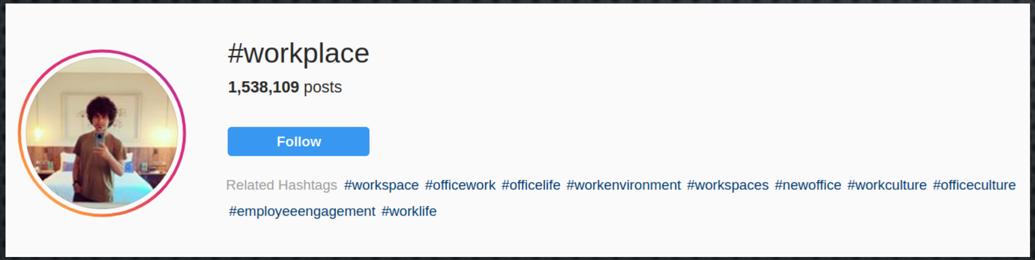
Search for pwned accounts across an entire domain and receive future notifications



Turn monitoring on to receive alerts if we identify your email in a data breach

TWITTER, FACEBOOK, INSTAGRAM, REDDIT

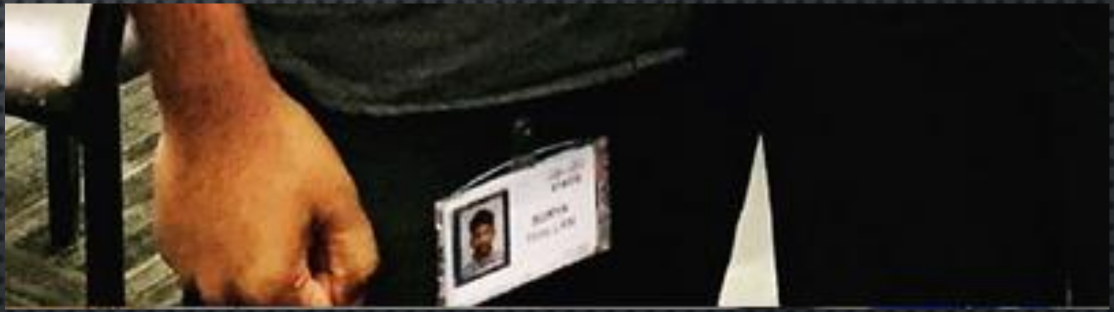
- You wouldn’t believe what people post
  - Yes, yes you would.
- #CiscoSystems
  - #NiceBadge



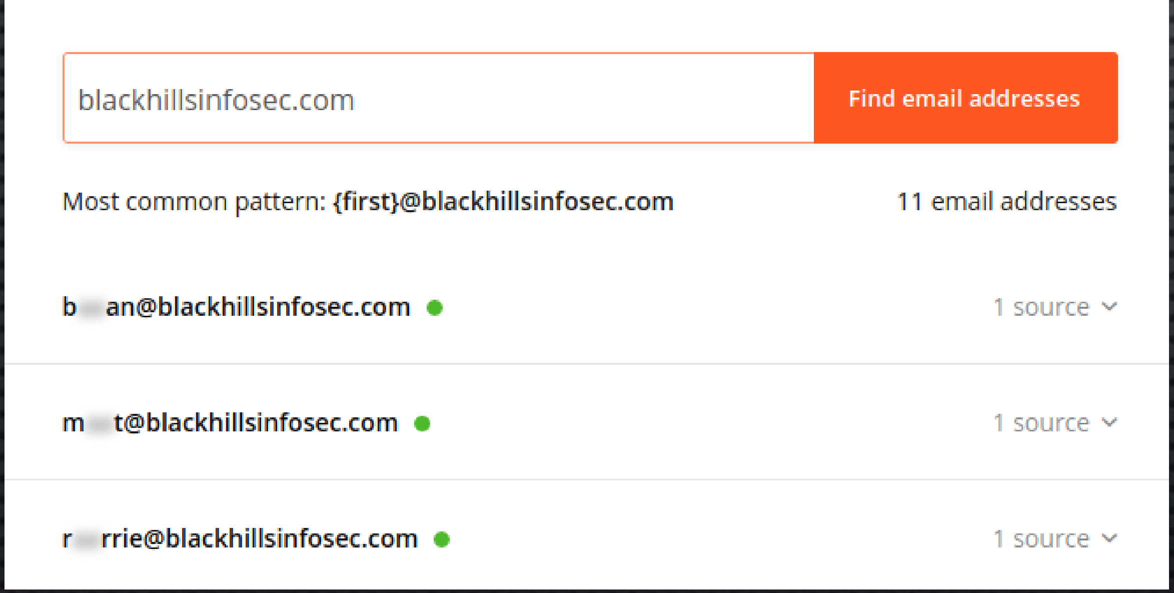
#workplace

1,538,109 posts

Related Hashtags #workspace #officework #officelife #workenvironment #workspaces #newoffice #workculture #officeculture #employeeengagement #worklife



HUNTER.IO



Most common pattern: **{first}@blackhillsinfosec.com** 11 email addresses

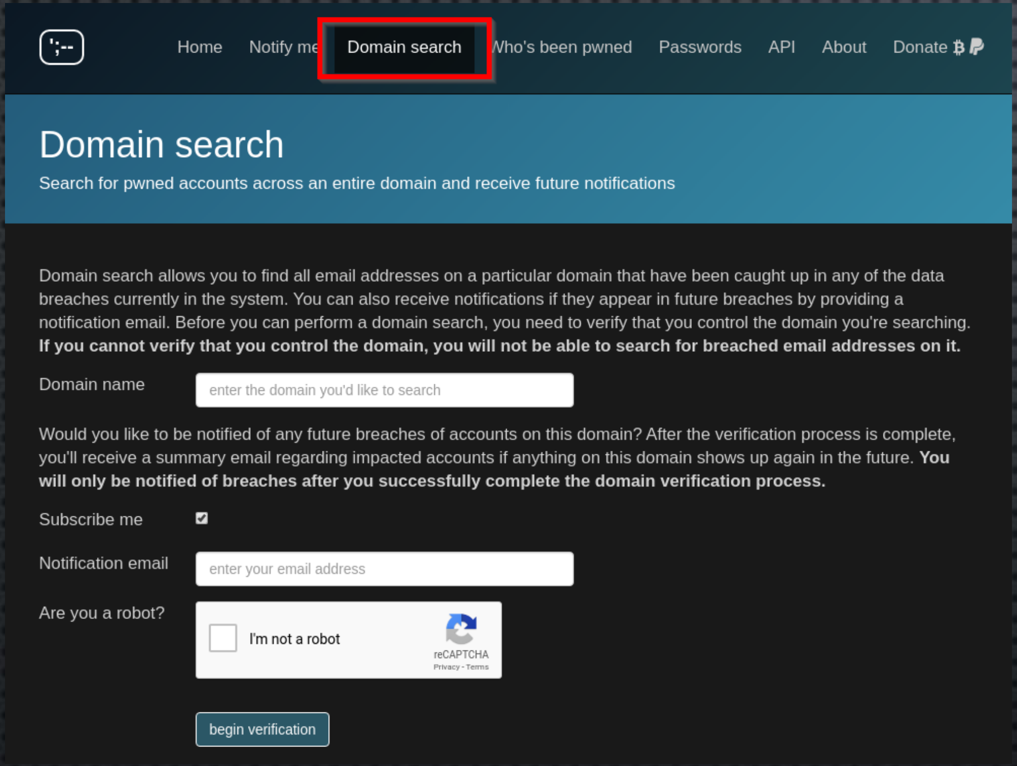
b[redacted]an@blackhillsinfosec.com ● 1 source

m[redacted]t@blackhillsinfosec.com ● 1 source

r[redacted]rrie@blackhillsinfosec.com ● 1 source

- API CALLS, BUT NO ALERTING…

HIBP? PROBABLY. [DOMAIN MONITOR]



Domain search

Search for pwned accounts across an entire domain and receive future notifications

Domain search allows you to find all email addresses on a particular domain that have been caught up in any of the data breaches currently in the system. You can also receive notifications if they appear in future breaches by providing a notification email. Before you can perform a domain search, you need to verify that you control the domain you're searching. **If you cannot verify that you control the domain, you will not be able to search for breached email addresses on it.**

Domain name: enter the domain you'd like to search

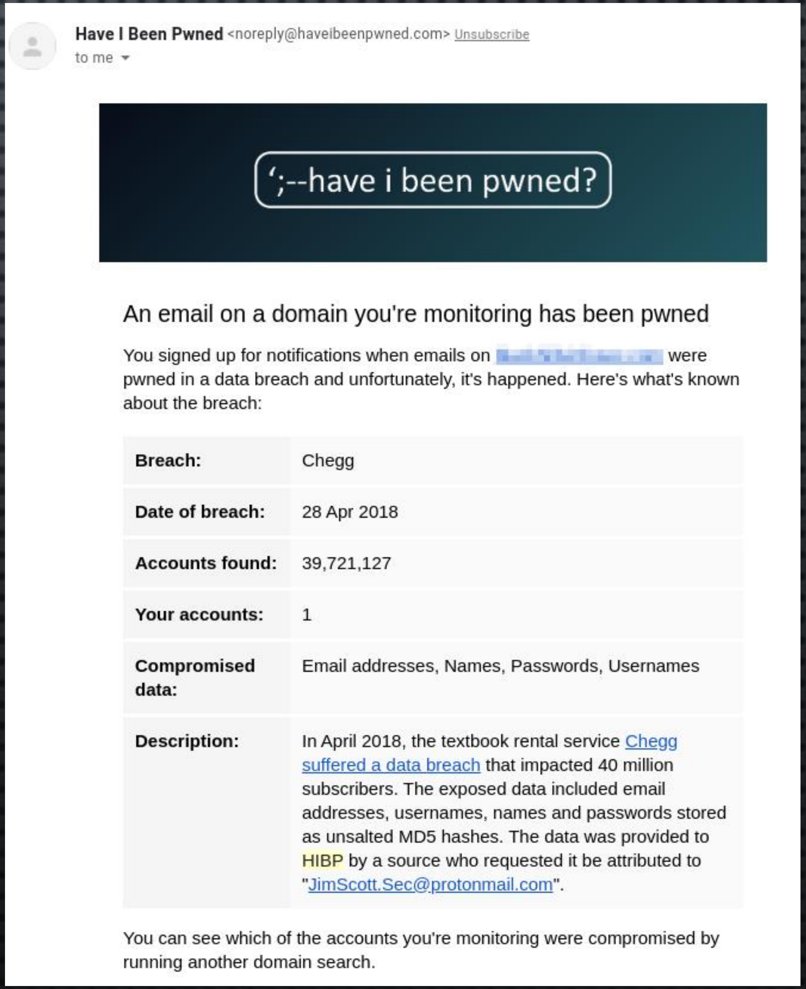
Would you like to be notified of any future breaches of accounts on this domain? After the verification process is complete, you'll receive a summary email regarding impacted accounts if anything on this domain shows up again in the future. **You will only be notified of breaches after you successfully complete the domain verification process.**

Subscribe me ☑

Notification email: enter your email address

Are you a robot? □ I'm not a robot

https://haveibeenpwned.com/DomainSearch



Have I Been Pwned <noreply@haveibeenpwned.com> Unsubscribe
to me

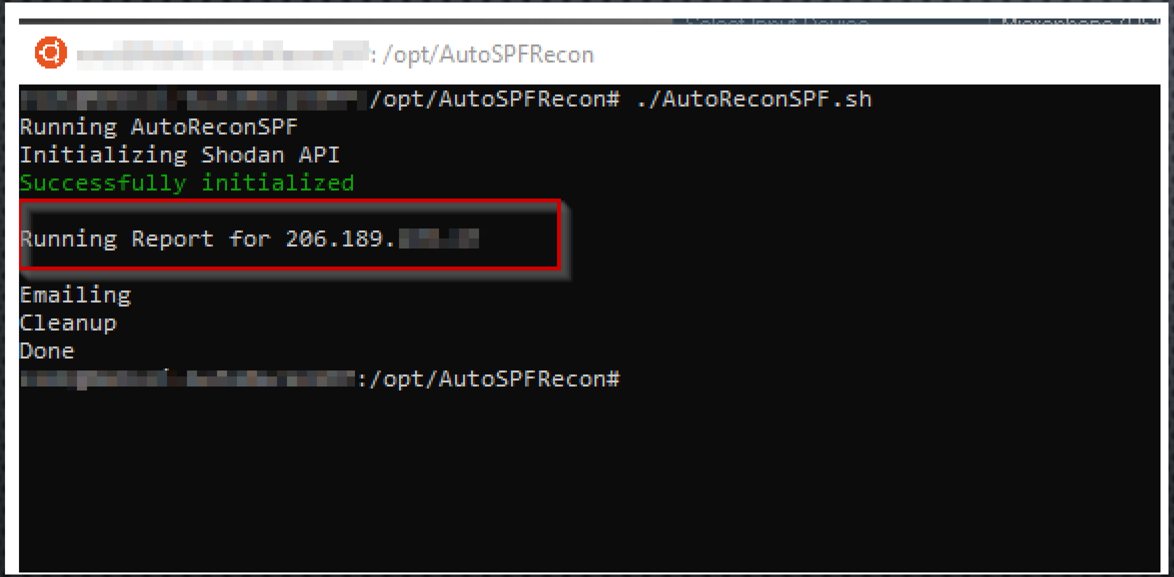
An email on a domain you're monitoring has been pwned

You signed up for notifications when emails on [redacted] were pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

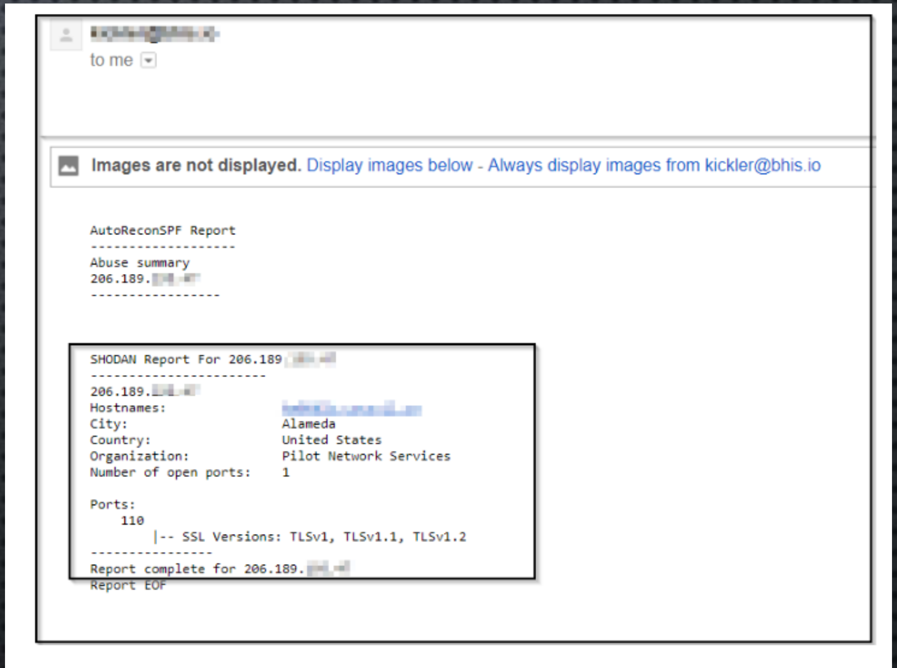
Breach:	Chegg
Date of breach:	28 Apr 2018
Accounts found:	39,721,127
Your accounts:	1
Compromised data:	Email addresses, Names, Passwords, Usernames
Description:	In April 2018, the textbook rental service Chegg suffered a data breach that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

You can see which of the accounts you're monitoring were compromised by running another domain search.

EMAIL: RE-ACTIVE SPF AUTO-RECON



```
[redacted] /opt/AutoSPFRecon# ./AutoReconSPF.sh
Running AutoReconSPF
Initializing Shodan API
Successfully initialized

Running Report for 206.189.[redacted]

Emailing
Cleanup
Done
[redacted]:/opt/AutoSPFRecon#
```



[redacted]
to me

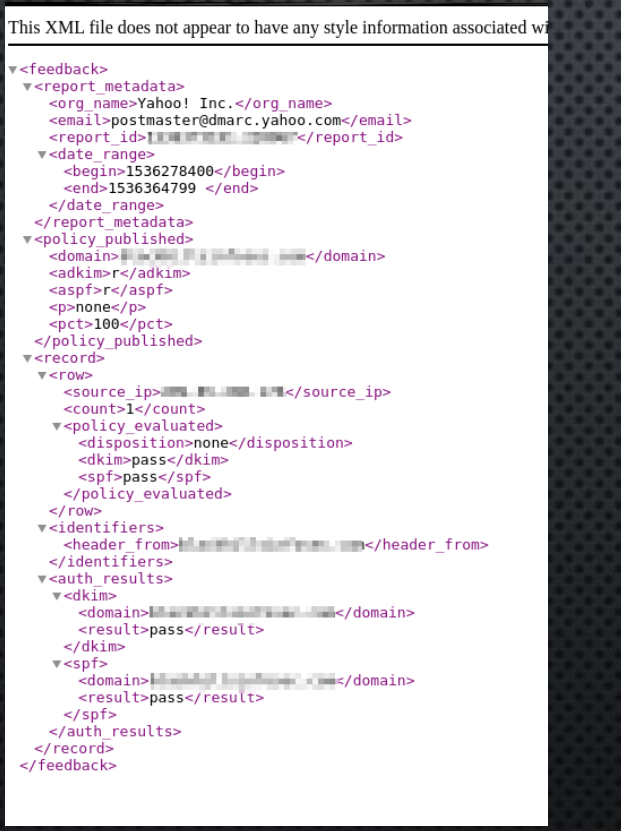
Images are not displayed. Display images below - Always display images from kickler@bhis.io

```
AutoReconSPF Report
-------------------
Abuse summary
206.189.[redacted]
-----------------


SHODAN Report For 206.189[redacted]
-----------------------
206.189.[redacted]
Hostnames:                [redacted]
City:                     Alameda
Country:                  United States
Organization:             Pilot Network Services
Number of open ports:     1

Ports:
    110
        |-- SSL Versions: TLSv1, TLSv1.1, TLSv1.2
----------------
Report complete for 206.189.[redacted]
Report EOF
```

https://github.com/Relkci/AutoSPFRecon

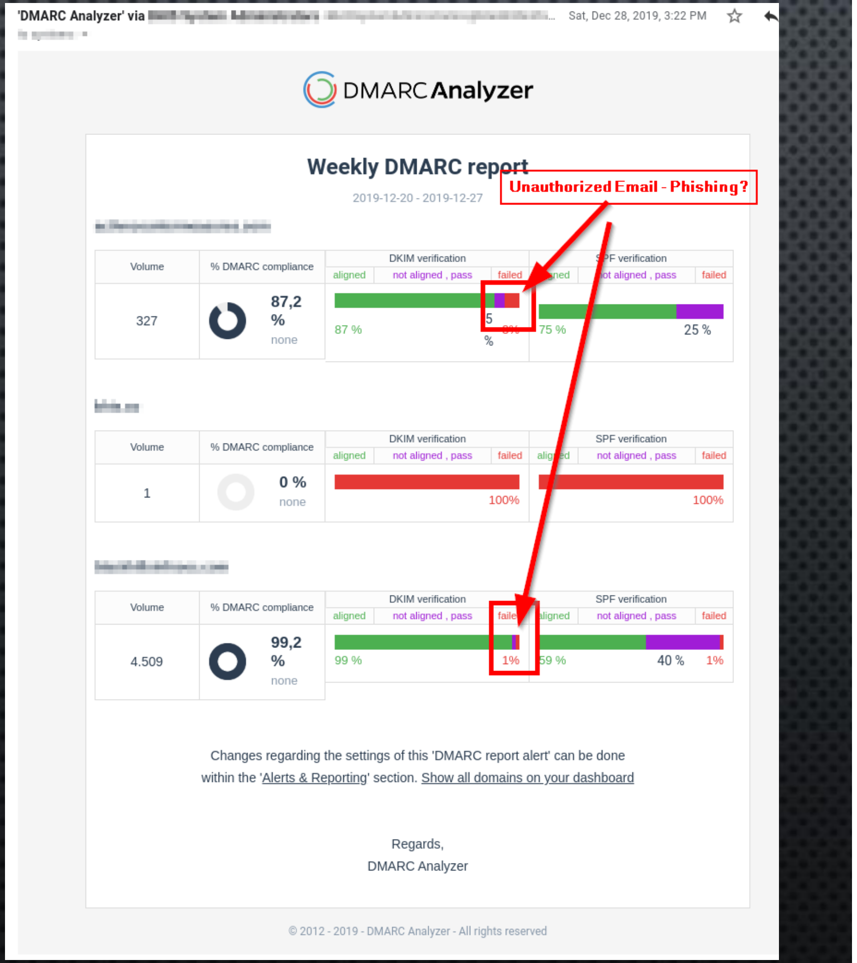
https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework/

DMARC REPORTS AND AGGREGATE DATA



This XML file does not appear to have any style information associated wi

```
▼<feedback>
  ▼<report_metadata>
     <org_name>Yahoo! Inc.</org_name>
     <email>postmaster@dmarc.yahoo.com</email>
     <report_id>[redacted]</report_id>
   ▼<date_range>
       <begin>1536278400</begin>
       <end>1536364799 </end>
     </date_range>
   </report_metadata>
  ▼<policy_published>
     <domain>[redacted]</domain>
     <adkim>r</adkim>
     <aspf>r</aspf>
     <p>none</p>
     <pct>100</pct>
   </policy_published>
  ▼<record>
    ▼<row>
       <source_ip>[redacted]</source_ip>
       <count>1</count>
      ▼<policy_evaluated>
         <disposition>none</disposition>
         <dkim>pass</dkim>
         <spf>pass</spf>
       </policy_evaluated>
     </row>
    ▼<identifiers>
       <header_from>[redacted]</header_from>
     </identifiers>
    ▼<auth_results>
      ▼<dkim>
         <domain>[redacted]</domain>
         <result>pass</result>
       </dkim>
      ▼<spf>
         <domain>[redacted]</domain>
         <result>pass</result>
       </spf>
     </auth_results>
   </record>
</feedback>
```



'DMARC Analyzer' via [redacted] Sat, Dec 28, 2019, 3:22 PM

DMARC Analyzer

Weekly DMARC report

2019-12-20 - 2019-12-27

Unauthorized Email - Phishing?

[redacted]

Volume	% DMARC compliance	DKIM verification			SPF verification		
		aligned	not aligned , pass	failed	aligned	not aligned , pass	failed
327	87,2 % none	87 %	5 %	8%	75 %	25 %	

[redacted]

Volume	% DMARC compliance	DKIM verification			SPF verification		
		aligned	not aligned , pass	failed	aligned	not aligned , pass	failed
1	0 % none			100%			100%

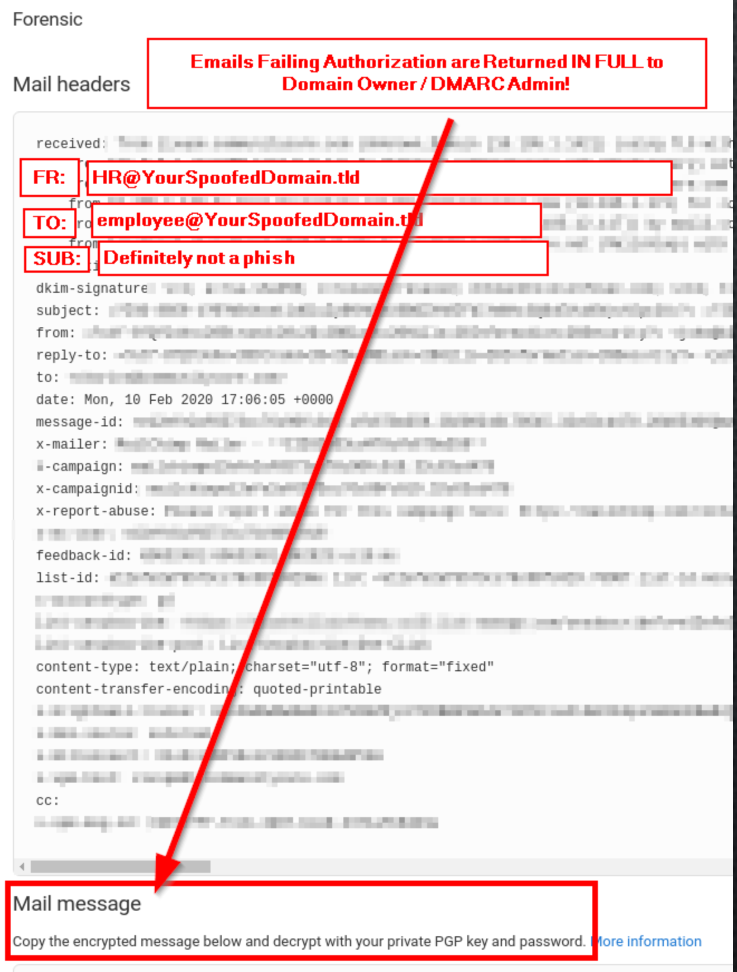
[redacted]

Volume	% DMARC compliance	DKIM verification			SPF verification		
		aligned	not aligned , pass	failed	aligned	not aligned , pass	failed
4.509	99,2 % none	99 %		1%	59 %	40 %	1%

Changes regarding the settings of this 'DMARC report alert' can be done within the 'Alerts & Reporting' section. Show all domains on your dashboard

Regards,
DMARC Analyzer

© 2012 - 2019 - DMARC Analyzer - All rights reserved



Forensic

Mail headers

Emails Failing Authorization are Returned IN FULL to Domain Owner / DMARC Admin!

FR: HR@YourSpoofedDomain.tld

TO: employee@YourSpoofedDomain.tld

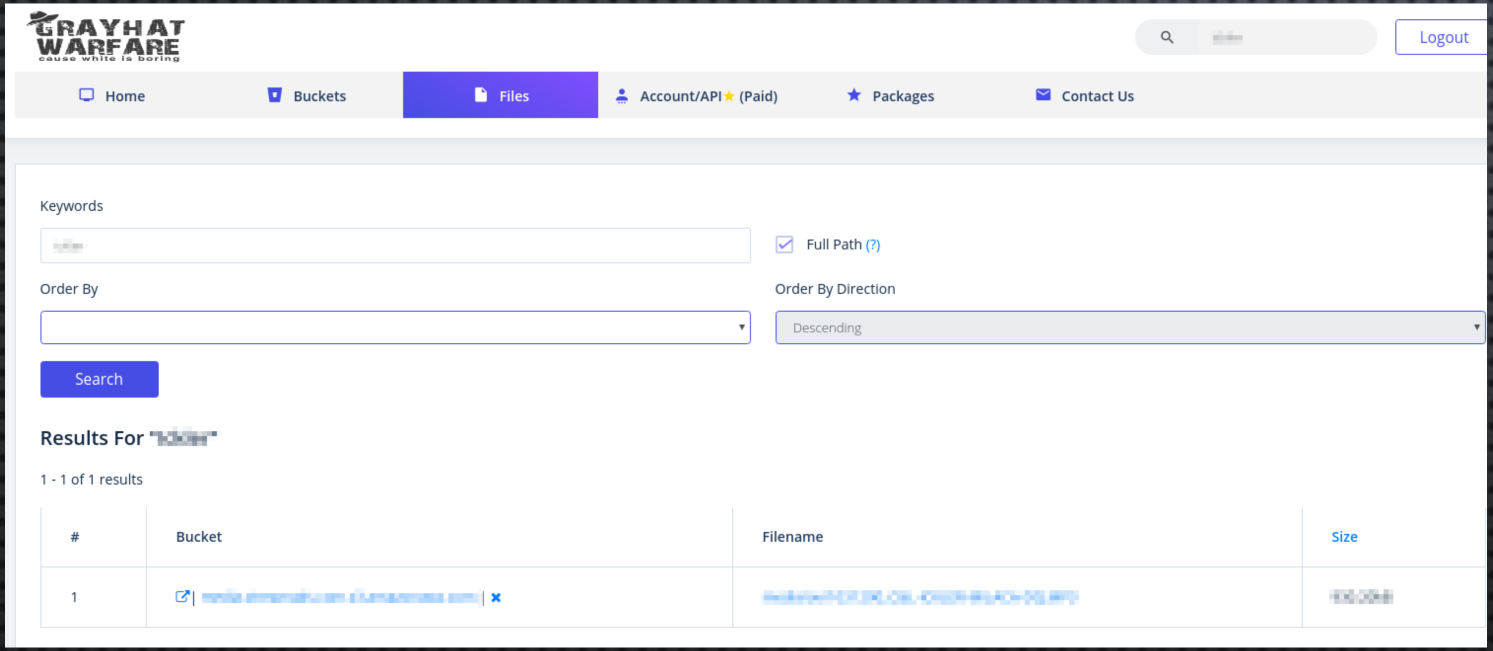
SUB: Definitely not a phish

```
received: [redacted]
dkim-signature [redacted]
subject: [redacted]
from: [redacted]
reply-to: [redacted]
to: [redacted]
date: Mon, 10 Feb 2020 17:06:05 +0000
message-id: [redacted]
x-mailer: [redacted]
[redacted]-campaign: [redacted]
x-campaignid: [redacted]
x-report-abuse: [redacted]
feedback-id: [redacted]
list-id: [redacted]
content-type: text/plain; charset="utf-8"; format="fixed"
content-transfer-encoding: quoted-printable
[redacted]
cc:
[redacted]
```

Mail message

Copy the encrypted message below and decrypt with your private PGP key and password. More information

AMAZON S3? GRAYHATWAREFARE



Search: [redacted]

Keywords: [redacted]

☑ Full Path (?)

Order By:

Order By Direction: Descending

Search

Results For "[redacted]"

1 - 1 of 1 results

#	Bucket	Filename	Size
1	[redacted]	[redacted]	[redacted]

https://buckets.grayhatwarfare.com/

"https://buckets.grayhatwarfare.com/api/v1/files[/keywords[/start[/limit]]]?access_token=api-key[&order=size&direction=asc|desc]"

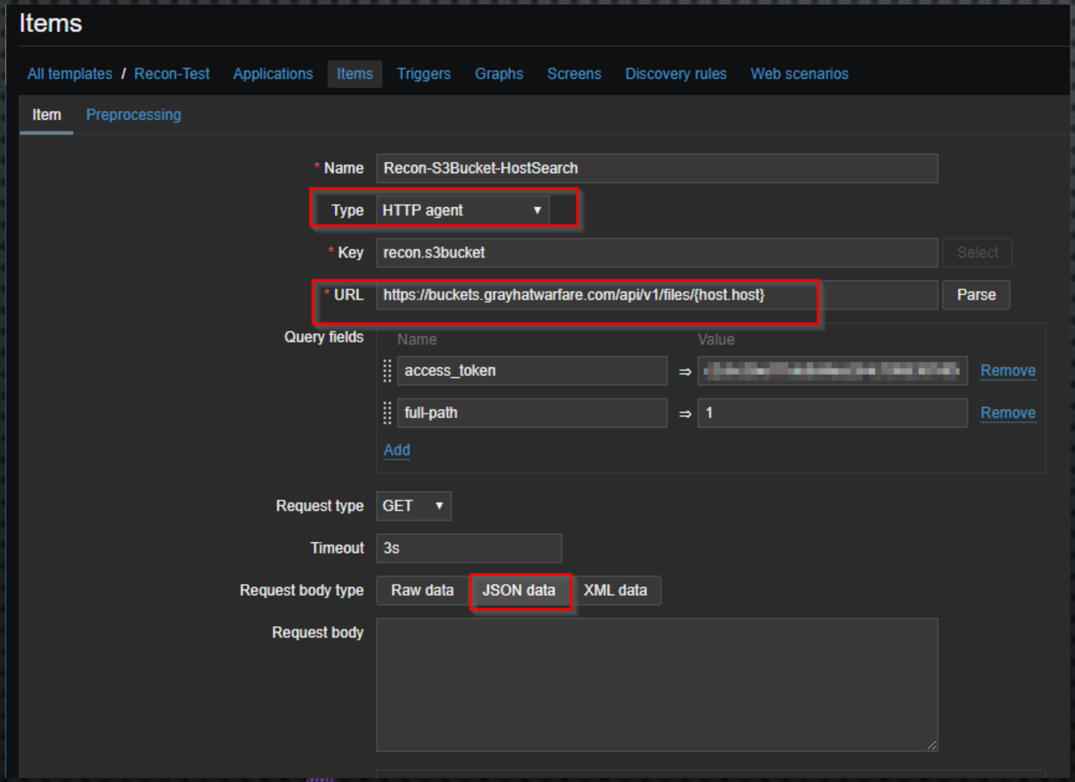
https://github.com/toniblyx/my-arsenal-of-aws-security-tools

TIE ALL THOSE APIS …. WHAT IF…

- Almost all these services offered API access to the data instead of email alerts.
- Is there a platform that can manage all this OSINT and only alert on changes?

- AUTOMATE ALL THE THINGS

ZABBIX TEMPLATES, ITEMS, DISCOVERY, TRIGGERS…



Items

* Name	Recon-S3Bucket-HostSearch
Type	HTTP agent
* Key	recon.s3bucket
* URL	https://buckets.grayhatwarfare.com/api/v1/files/{host.host}

Query fields

Name		Value	
access_token	⇒	[redacted]	Remove
full-path	⇒	1	Remove

Request type	GET
Timeout	3s
Request body type	Raw data / JSON data / XML data
Request body	

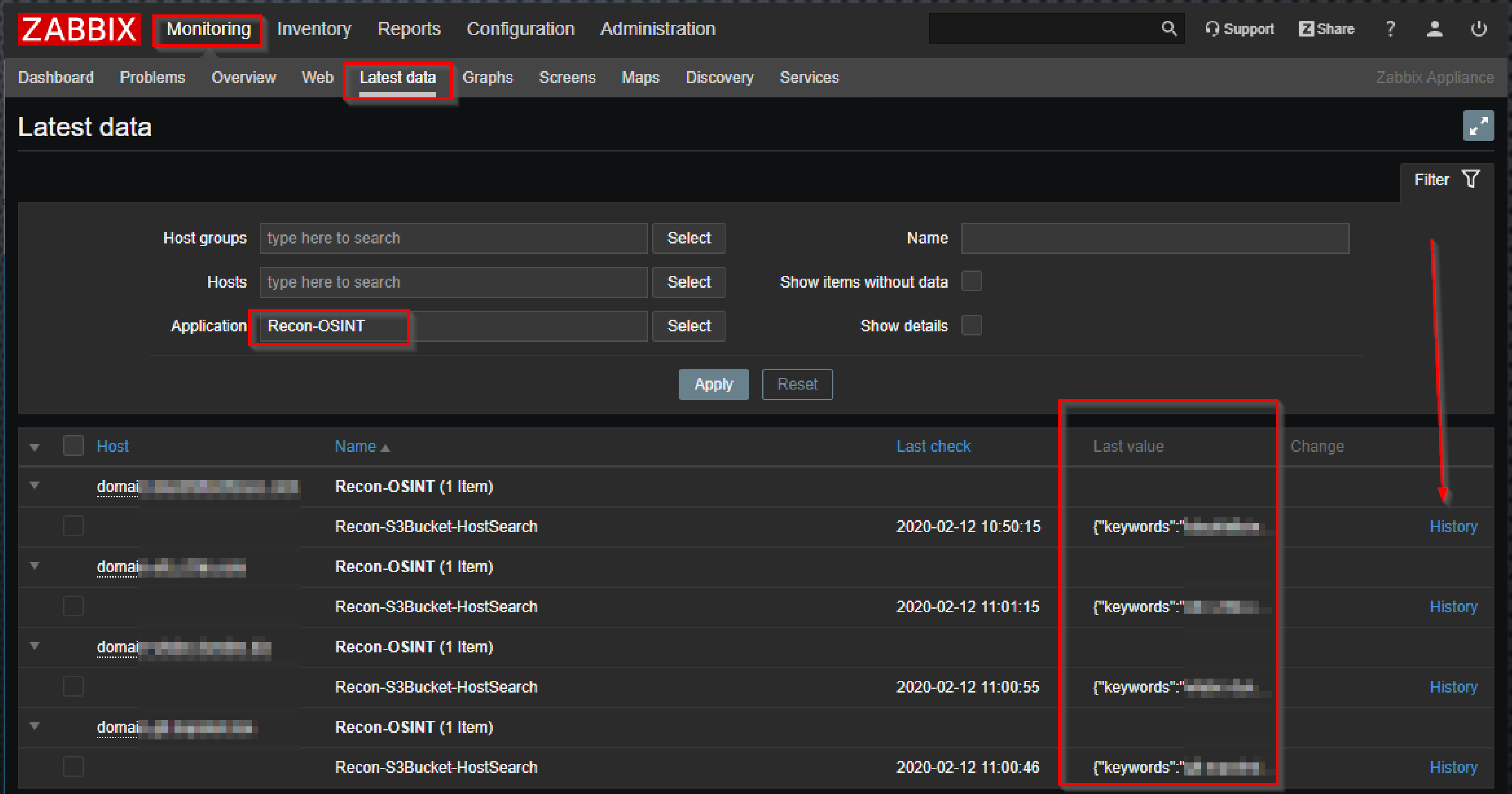
Zabbix Items Tied to Zabbix Templates.

Example: Search GrayHatWarfare for all buckets with the Host's hostname.

ZABBIX RESULT

Creates historical record of each API call and its contents. Can be broken out into more objects, can download the S3 files…

Alert any time a new file is discovered…



Latest data

Host groups	type here to search	Name	
Hosts	type here to search	Show items without data	□
Application	Recon-OSINT	Show details	□

Host	Name ▲	Last check	Last value	Change	
domai[redacted]	Recon-OSINT (1 Item)				
	Recon-S3Bucket-HostSearch	2020-02-12 10:50:15	{"keywords":"[redacted]		History
domai[redacted]	Recon-OSINT (1 Item)				
	Recon-S3Bucket-HostSearch	2020-02-12 11:01:15	{"keywords":"[redacted]		History
domai[redacted]	Recon-OSINT (1 Item)				
	Recon-S3Bucket-HostSearch	2020-02-12 11:00:55	{"keywords":"[redacted]		History
domai[redacted]	Recon-OSINT (1 Item)				
	Recon-S3Bucket-HostSearch	2020-02-12 11:00:46	{"keywords":"[redacted]		History

A BIGGER PICTURE ABOUT AUTOMATION

Re-iterative Recon could look like:

Zabbix gets email addresses from API call. Creates a new Item for each email address.

Each email address record then gets searched for OSINT, S3 buckets, HIBP…

Everything stored historical. OSINT Profiles checked daily, hourly… etc

Alerts are sent when changes are seen.

WILD WEST HACKIN' FEST

www.wildwesthackinfest.com

Watch Past WWHF Talks on

YouTube

Backdoors & Breaches INJECTS

Backdoors & Breaches PERSISTENCE

Backdoors & Breaches INITIAL COMPROMISE

Backdoors & Breaches PROCEDURES

DNS as a C2

This is another protocol that is often ignored. Why? Because it is variable in content and length. This makes it very tough to monitor.

DETECTION

Internal Password Spray

The attackers start a password spray against the rest of the organization from a compromised system.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis

TOOLS

Domain

DLL Attacks

The attackers hijack the order in which DLLs are loaded. This is usually done through insecure directory/file permissions.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

vulnerable-

Insider Threat

An internal disgruntled user exfiltrates information from your network.

DETECTION

User and Entity Behavior Analytics
DLP (Ha! Ha! Kidding. DLP never works.)
Working with HR

TOOLS

Being considered a Full Time Expenditure (FTE)
Long Hours
Addiction

https://americanaddictioncenters.org

Data Loaded on Pastebin

Bummer, the attacker has posted internal sensitive data on Pastebin. Your customers are now informed of the attack via the media.

NOTES

We have no idea why we added this in. It happens...a lot, but it is just pure evil. Tim bring in upper management and the legal

Social Engineering

Attackers use social engineering to trick a user into running malware.

DETECTION

Endpoint Security Protection Analysis
User Awareness Training

TOOLS

Phone
A goal and a dream of evil
People trusting people

https://youtu.be/mmcRTnTNC8
https://youtu.be/FvhkKwHjUVg

It Was A Pentest

Ha! Ha! Just kidding, you were never attacked. The CEO hired an external firm (BHIS?) to run an unannounced Red Team.

NOTES

This is almost always a bittersweet moment for companies. On one hand they are glad it was not the real thing. On the other - well, they were compromised. It is time to start working through how to prevent this from happening again.

Malicious Driver

Attacker loads a malicious driver into the operating system.

DETECTION

Endpoint Security Protection
Endpoint Analysis

TOOLS

Pasam
Wingbird
SeaDuke
ROCKR
Alure

Token Pa

Detecting weak relationships between accounts in Acti

SIEM
UBEA
Internal Segmentation

BloodHound
DeathStar

Firewall Log Review

Can your organization analyze firewall logs? Do you regular scenarios and verify that you

SOF-ELK

Internal Segmentation

Turn on your host base

HTTPS as an Exfil

HTTPS. Lots and lots Meterpreter time. It can be tego techniques.

BLACK HILLS
Information Security

Backdoors & Breaches

BLACK HILLS

Information Security

• 2008 •

PENETRATION TESTING

RED TEAMING

THREAT HUNTING

WEBCASTS

OPEN-SOURCE TOOLS

BLOGS

bhis.co

AI HUNTER™

Network Threat Hunting Solution

ANALYZE
Network Traffic

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

- BEACONS MODULE
- LONG CONNECTIONS MODULE
- DEEP DIVE MODULE
- ALERTING

acm.re

HUNT
TEAM
OPERATIONS
CENTER

BLACK HILLS | Information Security

Powered By AI HUNTER™

WILD WEST
HACKIN' FEST

Two-Day Training

NETWORK THREAT HUNTING WITH SECURITY ONION

Instructor: Chris Brenton

WILD WEST
HACKIN' FEST

Two-Day Training

AN INTRODUCTION TO DEVELOPING PHISHING MALWARE

Instructors: Christopher Truncer & Matt Grandy