

RECON PAPER

Executive Summary

William Raveis (<https://www.raveis.com/>) is a real estate firm in the northeastern region of the USA. This paper aims to find out interesting details that can be obtained about William Raveis using publicly available data and tools. All the findings and tools used in this paper are open source and accessible to anyone on the internet.

Spiderfoot scan which is based on the OSINT (Open Source Intelligence) framework was able to collect email addresses of employees compromised on other sites, IP addresses used by raveis, DNS records and also vulnerabilities that were found in the public domain. Shodan and Censys were used to find vulnerable products and services running on some of the raveis' internet facing machines. Google Fu was used to search for files and domains that are not shown on top of the usual google search. The Sublist3r tool was used to find various sub-domains of the organization from a lot of different sources. OSRframework tool was used to find details about the social media presence of raveis. theHarvester was used to find email addresses, hosts on less popular search engines like Bing and Web archive was used to see how the website of raveis has changed over years. More details about each of the tools and findings can be found below.

Although there weren't many vulnerabilities/weaknesses that the paper could identify, there are a few things that can be improved/changed for having a better security posture. Employees shouldnt be using their work email ids for anything other than work specific tasks. DNS records should be maintained carefully and only necessary details must be made available to anyone on the internet. Vulnerable services/products have to be updated and at least high priority vulnerabilities need to be fixed quickly. Social media profiles and presence needs to be monitored carefully and strong passwords policy and multi factor authentication can keep the accounts secure.

Introduction to Raveis

Raveis is owned and operated by the Raveis family. It was started in 1974 by William Raveis. They mainly operate in the northeastern part of the US - Mass, Connecticut, Rhode Island, New York, etc. They are ranked as one of the best real estate firms in the region. They offer listings, home valuation, agents, local market insights, mortgage, and insurance for customers.

One of the main reasons why I chose Raveis as my organization to perform recon is - as a real estate firm, most of the concentration and resources are put into the main line of business which is - buying, selling, renting houses, mortgage, insurance, etc. It's highly unlikely that they will have an extremely strong network security team to protect and safeguard their networks and websites. At the same time, I also wanted an organization to have a good online presence so that I would be getting some details about their company and network from recon. Raveis satisfies that criteria as well.

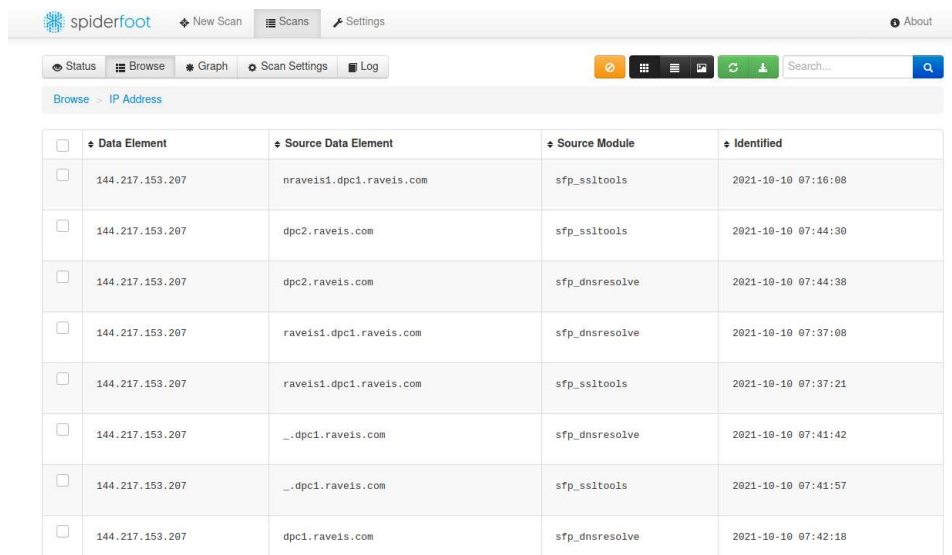
Spiderfoot Scan

Spiderfoot is a reconnaissance tool that gathers information from public data sources like - domain names, email addresses, vulnerabilities, open ports etc.

It makes use of OSINT - Open source intelligence to gather information. As the name suggests OSINT is a collection of free/open source tools that can be used to find sensitive information about your recon target.

Out of a lot of information spiderfoot gathered, there were a few which I think are interesting and can help any attacker get a better view of the organization as a whole.

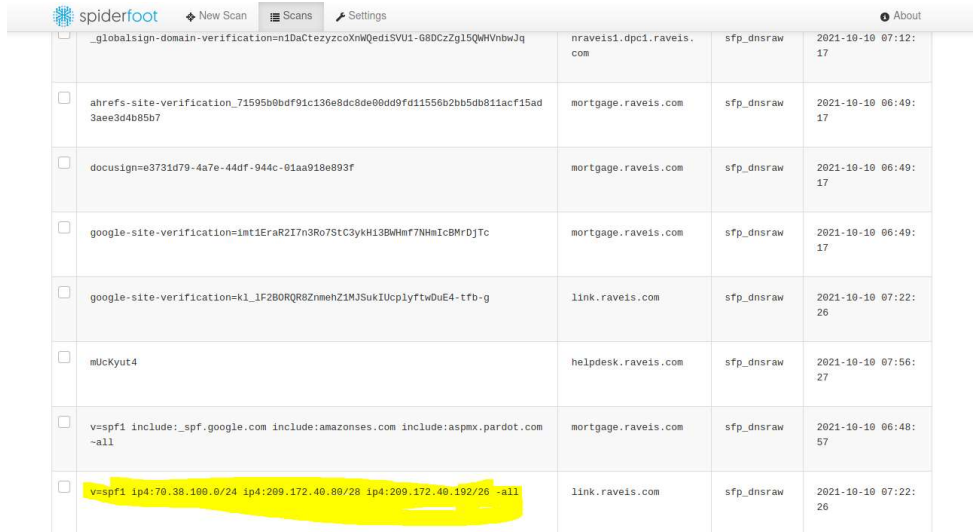
1. **Email addresses** - There were multiple email addresses identified by spiderfoot that were used or compromised in a data breach in other websites over the internet. They are - bwebb@raveis.com, david.sears@reveis.com, richh@raveis.com, marlene.fischer@raveis.com, michael.roche@raveis.com roberta.allen@raveis.com. There were also physical addresses identified for some email ids but a quick google search of the address pointed them to one of the RAVEIS offices. Social media profiles related to the email id like twitter and linkedin were also identified which can help an attacker understand more about a specific employee that can be later used for social engineering.
2. **IP addresses and netblock memberships** - Multiple IP addresses were found pointing to various domains and subdomains in raveis. Netblock memberships for contiguous IP allocations were also found using WHOIS details. Once we have the IPs, attackers can perform different scans for open ports, vulnerabilities, etc to get into the system. Please check the screenshot below.



The screenshot shows the Spiderfoot web interface. The top navigation bar includes 'New Scan', 'Scans', and 'Settings'. Below this is a secondary bar with 'Status', 'Browse', 'Graph', 'Scan Settings', and 'Log'. The main content area is titled 'Browse - IP Address' and displays a table of scan results for the IP address 144.217.153.207.

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	144.217.153.207	nraveis1.dpc1.raveis.com	sfp_ssltools	2021-10-10 07:16:08
<input type="checkbox"/>	144.217.153.207	dpc2.raveis.com	sfp_ssltools	2021-10-10 07:44:30
<input type="checkbox"/>	144.217.153.207	dpc2.raveis.com	sfp_dnsresolve	2021-10-10 07:44:38
<input type="checkbox"/>	144.217.153.207	raveis1.dpc1.raveis.com	sfp_dnsresolve	2021-10-10 07:37:08
<input type="checkbox"/>	144.217.153.207	raveis1.dpc1.raveis.com	sfp_ssltools	2021-10-10 07:37:21
<input type="checkbox"/>	144.217.153.207	__dpc1.raveis.com	sfp_dnsresolve	2021-10-10 07:41:42
<input type="checkbox"/>	144.217.153.207	__dpc1.raveis.com	sfp_ssltools	2021-10-10 07:41:57
<input type="checkbox"/>	144.217.153.207	dpc1.raveis.com	sfp_dnsresolve	2021-10-10 07:42:18

3. **DNS records** - Various types of DNS records were found in the scan - TXT, SRV, SIP, MX, NS. Some of them are useful. TXT records which are usually notes for administrators managing the servers. Some admins tend to be ignorant and may place unnecessary information here. NS records point to the authoritative name servers where the actual IP addresses are stored. MX records point to the mail servers in the domain and where the emails sent to the domain must be routed to. These details can possibly help an attacker get a good idea about the DNS servers of the organization and find any vulnerabilities in them. Please check the screenshot below.



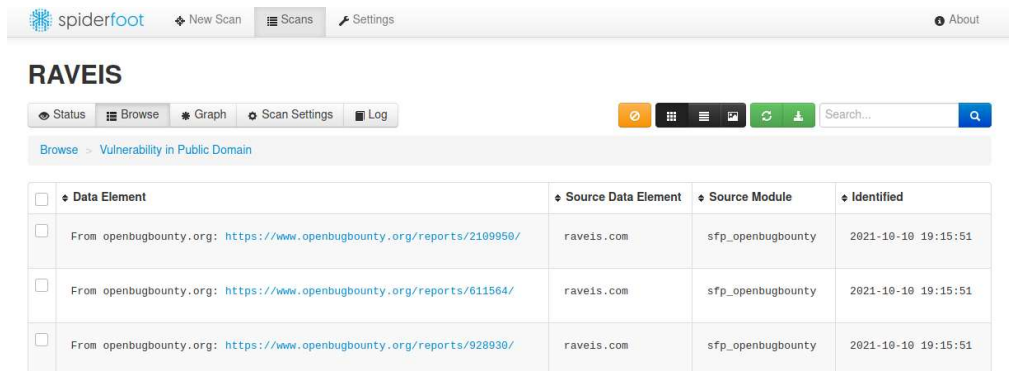
The screenshot shows the Spiderfoot application interface with a table of DNS records. The table has columns for a checkbox, a record name, a domain, a record type, and a timestamp. The records are listed as follows:

	Record Name	Domain	Type	Timestamp
<input type="checkbox"/>	_globalsign-domain-verification=n1DaCtezyzcoXnWQedi5VU1-68DCzZg15QWVnbnWJq	naveis1.dpci.raveis.com	sfp_dnsraw	2021-10-10 07:12:17
<input type="checkbox"/>	ahrefs-site-verification_71595b0bdf91c136e8dc8de08dd9fd11556b2bb5db811acf15ad3aee3d4b85b7	mortgage.raveis.com	sfp_dnsraw	2021-10-10 06:49:17
<input type="checkbox"/>	docuSign=e3731d79-4a7e-44df-944c-01aa918e893f	mortgage.raveis.com	sfp_dnsraw	2021-10-10 06:49:17
<input type="checkbox"/>	google-site-verification=imt1EraR2I7n3Ro7StC3ykH13BwHmF7NhmIcBMrDJTc	mortgage.raveis.com	sfp_dnsraw	2021-10-10 06:49:17
<input type="checkbox"/>	google-site-verification=k1_lF2B0RQ0ZmehZ1MJ5ukIucplyftwDuE4-tfb-g	link.raveis.com	sfp_dnsraw	2021-10-10 07:22:26
<input type="checkbox"/>	mUcKyut4	helpdesk.raveis.com	sfp_dnsraw	2021-10-10 07:56:27
<input type="checkbox"/>	v=spf1 include:_spf.google.com include:amazonses.com include:aspmx.pardot.com ~all	mortgage.raveis.com	sfp_dnsraw	2021-10-10 06:48:57
<input type="checkbox"/>	v=spf1 ip4:79.38.188.0/24 ip4:209.172.40.89/28 ip4:209.172.40.192/28 ~all	link.raveis.com	sfp_dnsraw	2021-10-10 07:22:26

4. **Vulnerabilities in public domain** - Sometimes the vulnerabilities found in the organization's website/devices will be reported to the customer and later archived and stored for reference. Websites like openbugbounty.org and others have such details. Raveis.com had multiple cross site scripting vulnerabilities in the last few years. Cross site scripting vulnerabilities will have attackers inject malicious scripts into benign websites. There is no way for the browser or the user using the benign website to know that there was a malicious script embedded in the website. These scripts can steal user data, cookies, session tokens and other confidential data. To prevent XSS attacks, applications must always validate all of the input data from outside your system and also sanitize other data regularly to examine and remove unwanted data. It is possible that there can be more XSS vulnerabilities that can be found on the website.

Link to the vulnerability and screenshot of others below.

<https://www.openbugbounty.org/reports/2109950/>



The screenshot shows the spiderfoot RAVEIS interface. At the top, there's a navigation bar with 'spiderfoot', 'New Scan', 'Scans', 'Settings', and 'About'. Below this, the 'RAVEIS' title is displayed. A secondary navigation bar includes 'Status', 'Browse', 'Graph', 'Scan Settings', and 'Log'. To the right of this bar are icons for various functions and a search input field. Below the navigation bar, a breadcrumb trail reads 'Browse > Vulnerability in Public Domain'. The main content area features a table with four columns: 'Data Element', 'Source Data Element', 'Source Module', and 'Identified'. The table contains three rows of data, each representing a vulnerability report from openbugbounty.org.

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	From openbugbounty.org: https://www.openbugbounty.org/reports/2109950/	raveis.com	sfp_openbugbounty	2021-10-10 19:15:51
<input type="checkbox"/>	From openbugbounty.org: https://www.openbugbounty.org/reports/611564/	raveis.com	sfp_openbugbounty	2021-10-10 19:15:51
<input type="checkbox"/>	From openbugbounty.org: https://www.openbugbounty.org/reports/928930/	raveis.com	sfp_openbugbounty	2021-10-10 19:15:51

More screenshots in the appendix section at the end of the paper.

Shodan and Censys

Shodan and Censys are the search engines for finding devices connected to the internet. While Google helps us find websites, these tools help us find devices and the products, services running on these devices. They have a lot of other options of filtering the data based on ports, protocols, locations etc.

There are multiple advantages of using these tools:

1. They perform active recon for us and have the results stored and the users can access, filter them according to their needs.
2. Their powerful search queries help us find devices in which there are vulnerable products or service versions. They support regex, ranges and many other options to filter the products/services that you are specifically looking for.

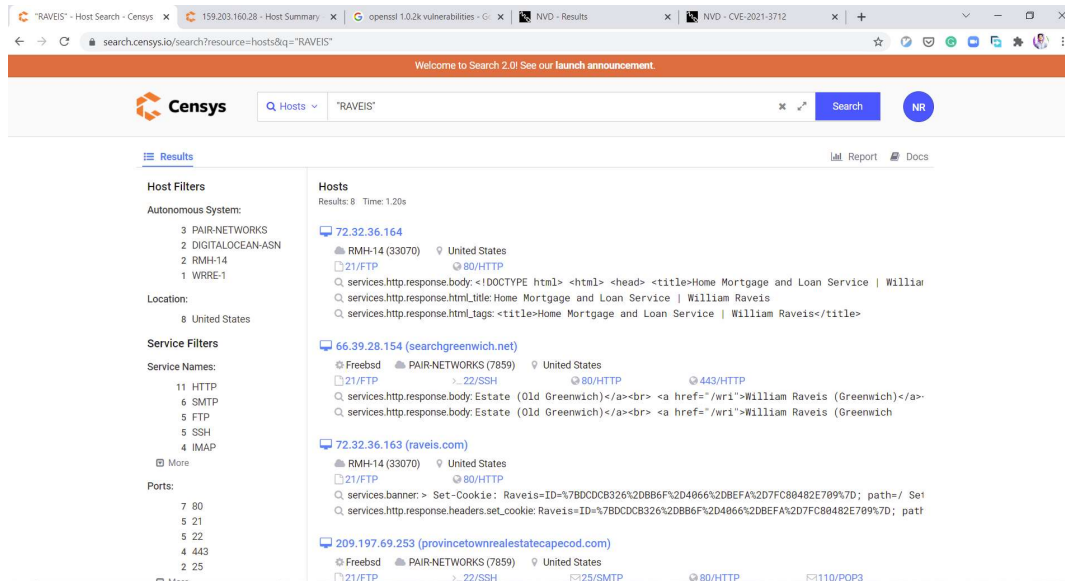
Although I didn't expect RAVEIS, which is primarily a real estate firm, to have a lot of devices connected to the internet. There were still some interesting details that I could find from searching for devices connected to the internet. Few observations that I could make and an attacker can possibly make use of to exploit a vulnerability in these services and versions:

1. Most of the devices were still using the HTTP version and port 80 even though it's not recommended anymore. Communication done on HTTP is not encrypted and it's possible for someone to intercept and read the traffic.
2. One of the devices was running an OpenSSH service version 7.4. There was a vulnerability that was discovered recently that will allow privilege escalations in OpenSSH versions from 6.2 to 8.8 - <https://nvd.nist.gov/vuln/detail/CVE-2021-41617>
3. OpenSSL 1.0.2k is being used in some of the devices which had some vulnerabilities discovered in it. This vulnerability made use of a design flaw in how NULL characters are added at the end of strings in C programming language. When exploited it can cause a buffer overrun which may lead to crashes and eventually Denial of Service

attacks-

https://nvd.nist.gov/vuln/search/results?adv_search=true&cves=on&cpe_version=cpe:/a:openssl:openssl:1.0.2k

4. One of the devices still used MD-5 hash which is not considered to be safe anymore and can be easily broken with modern GPUs.



Censys screenshot of various devices belonging to Shodan



Shodan screenshot of one of the device still using MD-5 hashing

Although having vulnerable versions of products and services doesn't necessarily mean that they can be exploited, there are other factors that should also be taken into account to make the exploit working. However, it's a good place to start and maybe narrow the process of trying to break into the system as a whole and not concentrating our efforts and resources on specific targets. I have also tried to list the vulnerability with high CVSS score as they are more likely and easier to be exploited by the attackers.

Raveis being a real estate firm, we can't necessarily expect them to have the latest and greatest versions of all the products and services they are using. But it's important to at least have high CVSS score vulnerabilities patched either by updating to the fixed versions or taking the necessary steps/workarounds in the same version so that they are not exploited.

It's also important to use the tools that attackers might use to get a view of how the attacker might see the organization's network and possible weaknesses that they can exploit.

Google-Fu

Any attacker doing recon on an organization makes use of google to get details about the website, usernames, emails and so much more. Google bots crawl the websites and index the pages for users to search for. But the hard part is searching for information the right way and this is where google advanced operators come handy both for good and bad. Google has its own search language which uses operators to filter and show the data that the user is looking for, from billions of indexed webpages. Some of the advanced operators include - filetype, inurl, site, cache and more. These advanced operators can be combined smartly to make a google dork that can be used on the target website and extract information that usually doesn't show on top of the usual google search results.

Some of the interesting links that I found for raveis are their intranet links that were accessible to anyone on the internet without any authentication. I found some documents that were meant for the agents of the company. Intranet in any organization is usually meant for employees of that organization only. But in this case I was able to access resources in the Intranet pages of raveis.com. What made it easier to access other intranet resources is the pattern followed by URLs in accessing the resources. All the resources had a number to them at the end of the URL which can be easily modified and a different resource can be accessed. Although all the numbers didn't have a resource attached to it, it was still pretty easy to play around to find what all internal resources were accessible to anyone on the internet.

Internal resources are sensitive and shouldn't be accessible to anyone on the internet. Some of them are more critical than others but if they are under internal resources they should be kept that way. If the attackers can get critical/sensitive information about the company that can lead to huge losses that are both tangible in terms of profits and revenue and also general opinion of the company in the public.

Whoever is maintaining the websites and devices connected to the internet must always know what is accessible to the outside world and what is not. Google bots crawl all the websites on the internet and sufficient controls need to be used effectively to show what you only want to show to the world and not sensitive or critical information. Robots.txt can be used to tell what part of the website needs to be indexed and what not. You also need to hide the robot.txt from the attacker so that they don't know what is hidden from the internet. One effective strategy is always to think in terms of the attacker's mindset and the security team of the organization should do the recon before the attacker and fix any glaring high priority vulnerabilities immediately. Use authentication or sometimes 2FA for highly critical information access so that it doesn't fall into the wrong hands. Encrypt your sensitive information like - PII, passwords, emails, credit card numbers etc.

<https://intranet.raveis.com/resources/5578.pdf>

<https://intranet.raveis.com/resources/2860.pdf>

<https://intranet.raveis.com/resources/7145.pdf>

Sublist3r

Sublist3r (sublister) is a handy tool that comes pre-installed in Kali that can be used for passive recon. It is designed to enumerate subdomains of websites using OSINT. It uses all the popular search engines like - Google, Yahoo, Bing, Baidu and Ask. It also uses Virustotal, DNSDumpster and more OSINT tools to get details about sub domains. You can even configure how it should be run using various flags like -t for number of threads, -e search engines, -v for verbose output, -o to write into a file and many more.

Sublist3r was able to find 35 unique sub-domains for raveis -

raveis.com	ldaps.raveis.com
ask.raveis.com	legacy.raveis.com
autodiscover.raveis.com	link.raveis.com
blog.raveis.com	login.raveis.com
bma.raveis.com	mail.raveis.com
dpc1.raveis.com	mail4.raveis.com
dpc2.raveis.com	mailgun.raveis.com
elainefalkenberg.raveis.com	marcyrichardson.raveis.com
email.raveis.com	mortgage.raveis.com
forward.raveis.com	myagent.raveis.com
helpdesk.raveis.com	mysearch.raveis.com
homeplus.raveis.com	nataliegrant.raveis.com
images.raveis.com	neagleandcaffreyteam.raveis.com
imap.raveis.com	photos.raveis.com
ingapuzikov.raveis.com	relay.raveis.com
intranet.raveis.com	stats.raveis.com
kristenrice.raveis.com	webmail.raveis.com
	wrmal.raveis.com

Many of them maynot be directly accessible through the browser directly and some of them may even need credentials to login. But a simple tool like sublist3r can give us all the different subdomains for raveis and attackers can narrow down their target space to the subdomains that they might be interested in. There are links to the mail servers, login or authentication servers and even some of the legacy subdomains.

It is important to be aware of all the subdomains on the internet and what is their role and significance for the company. If something is not needed anymore it's better to remove it from the internet even though it's working fine for now. In that way, organizations can reduce the attack surface for the bad guys.

OSRFramework

OSRframework is another popular OSINT tool that can help gather information from various sources on the internet. It has various modes like - usufy, searchfy, phonefy, mailfy and others which can gather various kinds of data such as social media profiles, phone numbers, email ids from usernames and more. I was interested in finding the social media profiles of raveis. Social media plays a big role in companies' success these days. Most of the companies have active social media presence on various platforms like - twitter, facebook, instagram, youtube and more. Organizations take their social media outlook very seriously because that's how they retain or grow their customer base. All it takes is one bad incident that can ruin the organization's reputation forever.

Usufy mode of OSRframework was able to identify the username - "**williamraveis**" in 52 different websites, including all the popular social media sites like - facebook, twitter, instagram and youtube. The complete list of all the profiles is listed in the miscellaneous section at the end of the paper. Other modes can also be used to identify phone numbers, email ids of the organization and employees within the organization.

_id	com.i3visio.URI	com.i3visio.Alias	com.i3visio.Platform
17	https://www.facebook.com/williamraveis	williamraveis	Facebook
26	http://www.instagram.com/williamraveis	williamraveis	Instagram
46	http://twitter.com/williamraveis	williamraveis	Twitter
51	https://www.youtube.com/user/williamraveis/about	williamraveis	Youtube

Usually there will just be one individual maintaining the social media presence unless it's a huge organization and there is a social media team specifically for it. Compromising one social media account most probably means compromising all or atleast, most social media profiles. One possible attack scenario is when employees leave organizations their credentials are sometimes still present in the accounts unless its regularly monitored and cleanup is performed. Cybersecurity firm McAfee's twitter profile was hacked in the same way. If the users who are maintaining the company's profile have their passwords compromised in a different website, it's very likely that they would have reused passwords in other sites and sometimes organization's profiles.

It's very important to have a strong password policy for all social media accounts and regularly monitor who has admin access, who is not part of the organization anymore and what needs to be cleaned up.

theHarvester

Harvester is another OSINT tool that can help the attacker get usernames, email ids, ip addresses of hosts and other details that can help with understanding the organization better and obtained details can be used in the later part of recon maybe for password cracking or social engineering and so on. What stood out in this tool was the ability to use different search engines like bing or yahoo. I was able to get some of the email addresses and ip addresses of the hosts on bing using this tool.

```
(kali㉿kali)-[~]
$ theHarvester -d raveis.com -l 500 -b bing

*****
*
* theHarvester
*
* theHarvester 3.2.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: raveis.com
    Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] Emails found: 2
jackie.davis@raveis.com
wilcoxteam@raveis.com
[*] Hosts found: 6
ask.raveis.com:72.32.182.219
blog.raveis.com:35.208.142.252
homeplus.raveis.com:72.32.65.175
openhouse.raveis.com:72.32.36.163
stats.raveis.com:52.225.220.23
www.raveis.com:72.32.36.163
```

Web archiving

Web archiving is an interesting tool that can tell us how the website of the organization we are performing recon has changed over the years. There are snapshots that are created in different time periods in the last twenty to thirty years. We will be able to access the links from the past sometimes, check how the website has changed and possibly make use of links and resources from the earlier version of websites to gather information about the organization. I couldn't specifically get any meaningful information for this org, that can be helpful with recon, from the way back feature in the web archives website, but it's a good tool to have in your passive recon arsenal. Please find a screenshot of the website that has changed from 2011 to 2021.

2011:

NY
DUTCHESS
PUTNAM
WESTCHESTER
MANHATTAN

VT
NH
MA
RI

CT

CAPE COD
NANTUCKET
MARtha's VINEYARD

Find A Home

Need Help?
Click here for on-line assistance or call 1.888.699.8876

Local Housing Data

Unit Sales

Unit Sales - 12 Month

Market Time for Sold

Mortgage Rate Watch

Loan Type	Rate	APR
15 YR Fixed Conforming	4.000%	4.139%
15 YR Fixed Jumbo	4.375%	4.470%

Open Houses

Mapping

Housing Data

Home Evaluation

Sold Homes

Mortgage

Insurance

Featured Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont Homes

Fairfield, CT \$2,000,000

Farmington, CT \$799,000

Simsbury, CT \$999,900

Barnstable, MA \$10,900,000

Little Compton, RI \$2,950,000

2021:

WILLIAM RAVEIS
REAL ESTATE • MORTGAGE • INSURANCE

Search Open Houses Home Valuation Agents/Offices Local Market Insights Mortgage Insurance

Search

Town, Agent, Address, Zip, MLS#, Bldg

GO

Min Price

Click or Type

Bedrooms

Any

Open House

Max Price

Click or Type

Bathrooms

Any

For Rent

Quick Search

State

Connecticut

Massachusetts

New York

Rhode Island

Vermont

Maine

Florida

New Hampshire

Destination

Boston

New York City

Cape Cod

Nantucket

Martha's Vineyard

Long Island

New Jersey

National & Global

My Raveis Login

f t i p in

PHN

How Much Is Your Home Worth?

Enter Your Property Address

Get My Estimate

Appendix

Netblock membership details of RAVEIS

RAVEIS

StatusBrowseGraphScan SettingsLog

🔍

📄

☰

📧

🔄

👤

Search...

🔍

Browse → Netblock Membership

<input type="checkbox"/>	↕ Data Element	↕ Source Data Element	↕ Source Module	↕ Identified
<input type="checkbox"/>	144.217.0.0/16	144.217.158.30	sfp_bgpview	2021-10-10 07:13:30
<input type="checkbox"/>	144.217.0.0/16	144.217.158.30	sfp_ripe	2021-10-10 07:14:09
<input type="checkbox"/>	144.217.0.0/16	144.217.153.207	sfp_bgpview	2021-10-10 07:16:21
<input type="checkbox"/>	144.217.0.0/16	144.217.153.207	sfp_ripe	2021-10-10 07:16:52
<input type="checkbox"/>	148.76.0.0/17	148.76.73.204	sfp_bgpview	2021-10-10 07:10:08
<input type="checkbox"/>	148.76.0.0/17	148.76.73.207	sfp_bgpview	2021-10-10 18:33:41
<input type="checkbox"/>	148.76.0.0/17	148.76.73.209	sfp_bgpview	2021-10-10 07:56:51

HTTP and vulnerable version of OpenSSL being used

80/HTTP

TCP

2021-10-25

Software

CentOS Linux

CPE cpe:2.3:o:centos:centos:*:*:*:*:*

OpenSSL

Version 1.0.2k-fips

CPE cpe:2.3:a:*:openssl:1.0.2k-fips:*:*:*:*

Apache HTTPD

Version 2.4.6

CPE cpe:2.3:a:apache:http_server:2.4.6:*:*:*:*

Components cpe:2.3:a:*:openssl:1.0.2k-fips:*:*:*:*
cpe:2.3:a:*:php:7.4.19:*:*:*:*

PHP

Version 7.4.19

CPE cpe:2.3:a:*:php:7.4.19:*:*:*:*

Vulnerable version of OpenSSH being used

22 / SSH

TCP

Software

linux

CPE cpe:2.3:o:linux:*****

Ubuntu Linux

Version 14.04

CPE cpe:2.3:o:canonical:ubuntu_linux:14.04:*****

OpenBSD OpenSSH

Version 6.6.1p1

CPE cpe:2.3:a:openbsd:openssh:6.6.1p1:*****

Shodan devices found for raveis

org:"raveis" - Shodan Search

Search Query Fundamentals - Shodan

Shodan

Explore

Downloads

Pricing

org:"raveis"

Account

TOTAL RESULTS

7

TOP PORTS

443 5

554 1

8008 1

TOP ORGANIZATIONS

WILLIAM RAVEIS REAL ESTATE, INCORPORATED 5

William Raveis Real Estate 2

View Report

View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

216.238.166.26

216-238-166-26.sbaic-testing.tl.net

William Raveis Real Estate

United States, Stewartstown

SSL Certificate

HTTP/1.1 200 OK

Issued By: Common Name: fortinet-subca2001

Organization: Fortinet

Issued To: Common Name: FG166FYK2605513

Organization: Fortinet

Supported SSL Versions: TLSv1.1, TLSv1.2, TLSv1.3

Diffie-Hellman Fingerprint: RFC3526/Oakley Group 14

2021-10-27T04:26:24.971106

148.76.73.211

944c9d5.cslightpath.net

WILLIAM RAVEIS REAL ESTATE, INCORPORATED

United States, New York City

SSL Certificate

HTTP/1.1 302 Object Moved

Location: /vpn/index.html

Strict-Transport-Security: max-age=157680000

Set-Cookie: NSC_Auth=eyJzPathw/;expires=Wednesday, 09-Nov-1999 13:12:40 GMT;Secure

Set-Cookie: NSC_EPAC=eyJzPathw/;expires=Wednesday, 09-Nov-1999 13:12:40 GMT;Secure

Set-Cookie: NSC_USER=eyJzPathw/

Issued To: Common Name: www.sbaic-testing.com

2021-10-25T23:14:58.340398

URLs identified by OSRframework from many different websites

_id	com.i3visio.URI	com.i3visio.Alias	com.i3visio.Platform
1	https://www.canva.com/williamraveis	williamraveis	Canva
2	http://www.betblog.com/tipster/williamraveis	williamraveis	Betblog

3	http://www.bucketlistly.com/users/williamraveis	williamraveis	Bucketlistly
4	https://www.causes.com/williamraveis	williamraveis	Causes
5	http://williamraveis.carbonmade.com	williamraveis	Carbonmade
6	http://williamraveis.blogspot.com.es/	williamraveis	Blogspot
7	http://www.chess.com/members/view/williamraveis	williamraveis	Chess
8	http://forum.arduino.cc/index.php?action=profile;user=williamraveis	williamraveis	Arduino
9	http://www.burbuja.info/inmobiliaria/member-williamraveis.html	williamraveis	Burbuja.info
10	https://forums.digitalspy.com/profile/discussions/williamraveis	williamraveis	Digitalspy
11	https://es.dreamstime.com/williamraveis_info	williamraveis	Dreamstime
12	https://www.drupal.org/u/williamraveis	williamraveis	Drupal
13	https://www.eyeem.com/u/williamraveis	williamraveis	Eyeem
14	https://site.douban.com/williamraveis	williamraveis	Douban
15	https://forum.fiverr.com/u/williamraveis/summary	williamraveis	Fiverr
16	http://foursquare.com/williamraveis	williamraveis	Foursquare
17	https://www.facebook.com/williamraveis	williamraveis	Facebook
18	https://getsatisfaction.com/people/williamraveis	williamraveis	GetSatisfaction
19	https://www.freelancer.com/u/williamraveis	williamraveis	Freelancer
20	https://bitbacker.io/user/williamraveis	williamraveis	bitbacker
21	https://forum.ethereum.org/profile/williamraveis	williamraveis	Ethereum
22	https://ifunny.co/williamraveis	williamraveis	IFunny
23	https://www.issuu.com/williamraveis	williamraveis	Issuu
24	http://kupika.com/williamraveis	williamraveis	Kupika
25	https://medium.com/@williamraveis	williamraveis	Medium
26	http://www.instagram.com/williamraveis	williamraveis	Instagram

27	https://mastodon.xyz/@williamraveis	williamraveis	MastodonXyz
28	https://developer.mozilla.org/es/docs/user:williamraveis	williamraveis	Mozilla
29	http://www.metacafe.com/channels/williamraveis	williamraveis	Metacafe
30	https://www.openbugbounty.org/researchers/williamraveis/	williamraveis	OpenBugBounty
31	https://www.okcupid.com/profile/williamraveis	williamraveis	Okcupid
32	http://www.meneame.net/user/williamraveis	williamraveis	Meneame
33	https://www.patreon.com/williamraveis	williamraveis	Patreon
34	http://pastebin.com/u/williamraveis	williamraveis	Pastebin
35	http://photobucket.com/user/williamraveis/library/?sort=3&page=1	williamraveis	Photobucket
36	http://pixinsight.com/forum/index.php?action=profile;user=williamraveis	williamraveis	Pixinsight
37	http://500px.com/williamraveis	williamraveis	500px
38	http://www.researchgate.net/profile/williamraveis	williamraveis	Researchgate
39	http://www.sidereel.com/profile/williamraveis	williamraveis	Sidereel
40	https://onename.com/williamraveis	williamraveis	Onename
41	http://www.slideshare.net/williamraveis	williamraveis	Slideshare
42	https://williamraveis.soup.io	williamraveis	Soup
43	http://www.thiscrush.com/~williamraveis	williamraveis	Thiscrush
44	https://trakt.tv/people/williamraveis	williamraveis	Trakt
45	https://unsplash.com/@williamraveis	williamraveis	Unsplash
46	http://twitter.com/williamraveis	williamraveis	Twitter
47	http://www.steinberg.net/forums/memberlist.php?username=williamraveis	williamraveis	Steinberg
48	https://www.virustotal.com/en/user/williamraveis	williamraveis	Virustotal

49	http://community.wikia.com/wiki/User:williamraveis	williamraveis	Wikia
50	http://www.xtube.com/profile/williamraveis	williamraveis	Xtube
51	https://www.youtube.com/user/williamraveis/about	williamraveis	Youtube
52	http://www.ebay.com/usr/williamraveis	williamraveis	Ebay