

# **Security OSINT Online Analysis Tools and Techniques**

# OSINT

Open Source Intelligence (OSINT) is a term used to refer to the data collected from publicly available sources to be used in an intelligence context.

It is not related to open-source software or public intelligence.

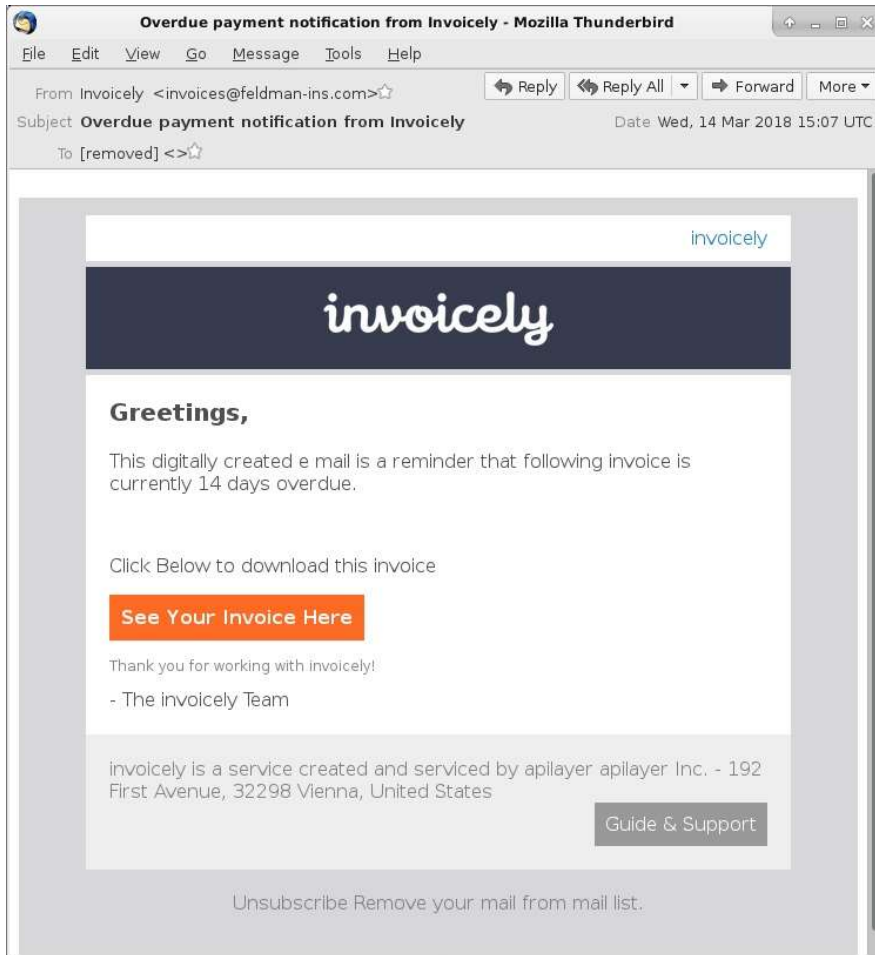
<http://osintframework.com/>

# Structure

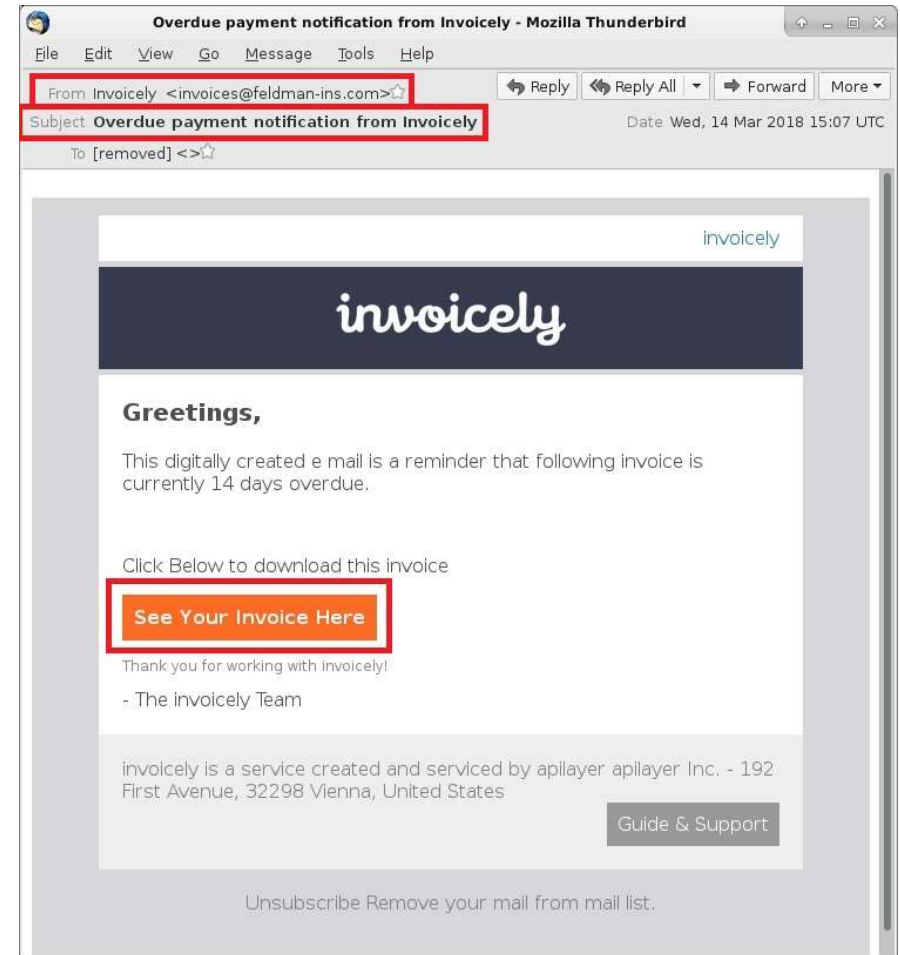
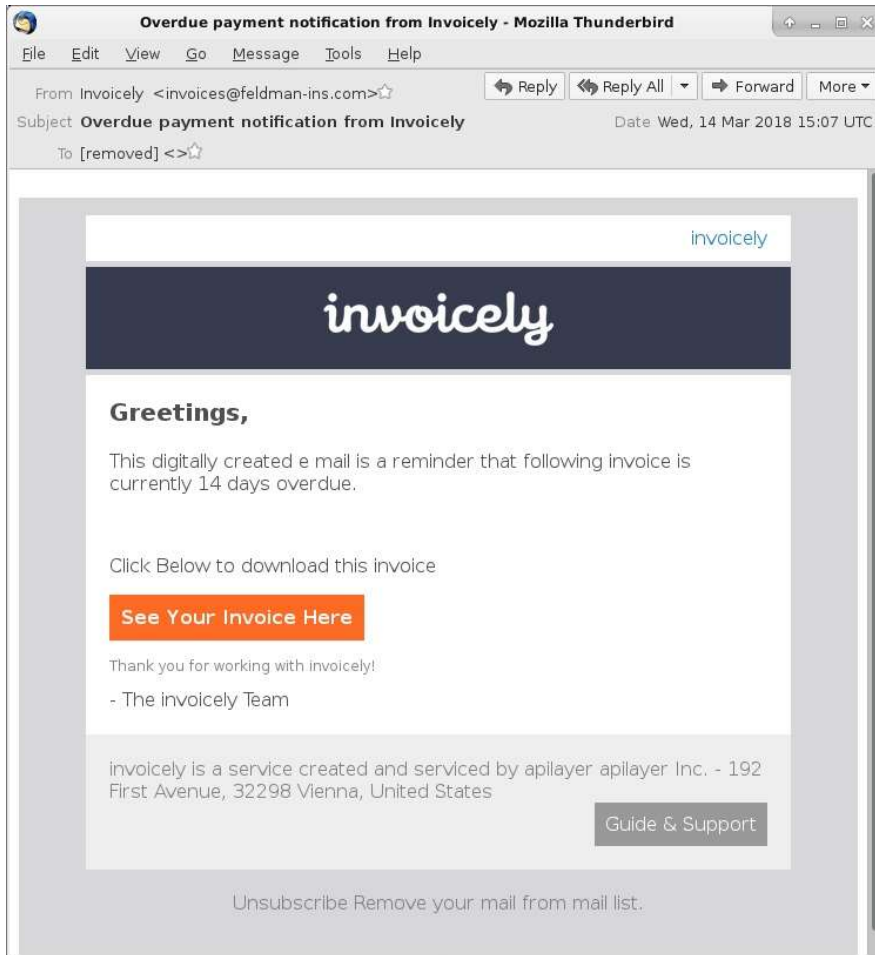
- Phishing email investigation
- Security Incident investigation

# Phishing email investigation

# Phishing email investigation – First Glance



# Phishing email investigation – First Glance



# Phishing email investigation

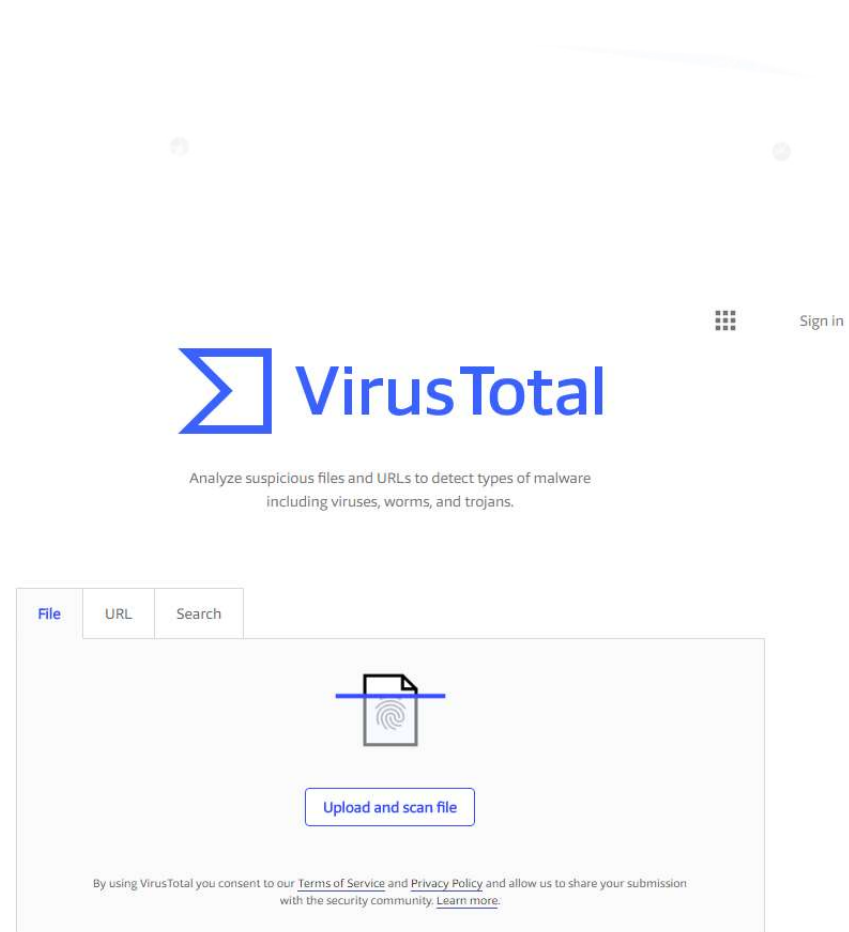
## IOCs

- Sender: [invoices@feldman-ins.com](mailto:invoices@feldman-ins.com)
- Header:
  - Source Domain/IP - **feldman-ins.com/12.169.83.217/205.182.135.63**
- Subject: **Overdue payment notice from Invoicely**
- Delivered file:
  - Hashes: **af290434ffa9a677133952b2d2622eabd7b274f545fc662f31dcfa0164d9f9de**
  - File: **invoice\_353492.doc**
  - URL: **hxxp://argentstrim.com?[string of characters]=[encoded string representing recipient's email address]**

# Phishing email investigation

<https://www.virustotal.com/>

- VirusTotal inspects items with over 60 antivirus scanners and URL/domain blacklisting services
- Able to investigate and correlate details about:
  - URLs/Domains,
  - IP Addresses;
  - Hashes;
  - Filenames,
- Provides behavioral information
- Alternatives: Malware, Metadefender, Cymon, Threat Miner etc.

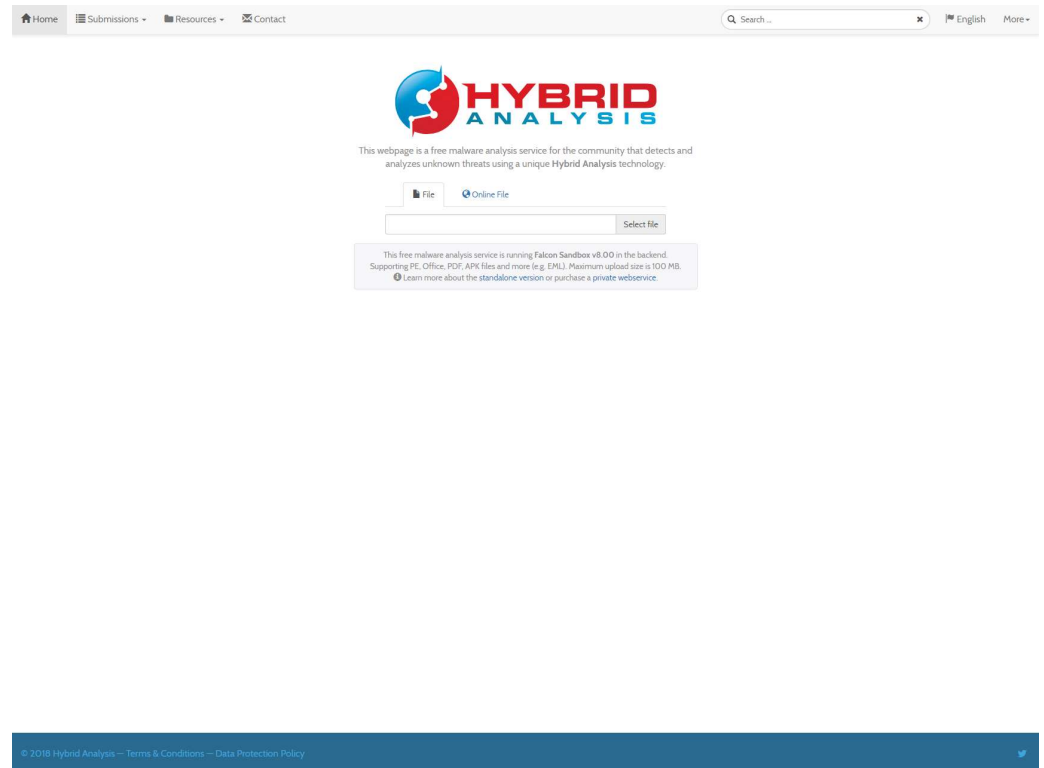




# Phishing email investigation

<https://www.hybrid-analysis.com/>

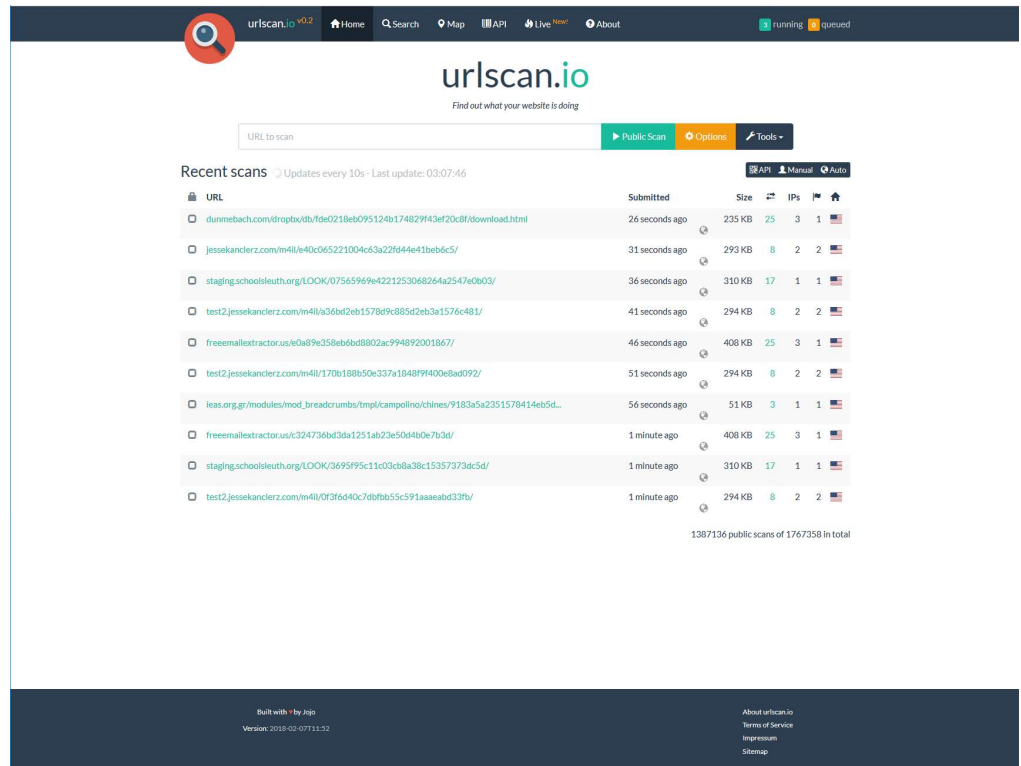
- Based on Falcon Sandbox v8.00
- Can display the report for previously analyzed file by searching for hash
- Extracts the following details:
  - Indicators
  - File details
  - Screenshots
  - Network data
  - Extracted strings/files
- Performs hybrid analysis displaying all loaded modules and shows VT AV hits
- Alternatives: Malwr, Any.Run etc.



# Phishing email investigation

<https://urlscan.io/>

- Displays a screenshot of the website
- Provides reports on IP, ASN, Domain, Subdomains, Links, Certificates
- Records and displays HTTP requests and responses with the possibility to highlight scripts
- Summarizes a behavior of the scanned website
- Provides a list of “IoCs” containing the domains, IPs and hashes for loaded resources



The screenshot displays the urlscan.io web application. At the top, there is a navigation bar with a search icon, the urlscan.io logo, and links for Home, Search, Map, API, Live, and About. Below the navigation bar, the main header features the urlscan.io logo and the tagline "Find out what your website is doing". A search bar labeled "URL to scan" is positioned next to buttons for "Public Scan", "Options", and "Tools".

The "Recent scans" section shows a list of scans with columns for URL, Submitted, Size, and IPs. The list includes various URLs such as durmebach.com, jessekancierz.com, staging.schoolsleuth.org, and freemallextractor.us. Each entry shows the time since it was submitted and the size of the scan. At the bottom of the page, there is a footer with the text "Built with 1by1" and "Version: 2018-02-07T11:32".

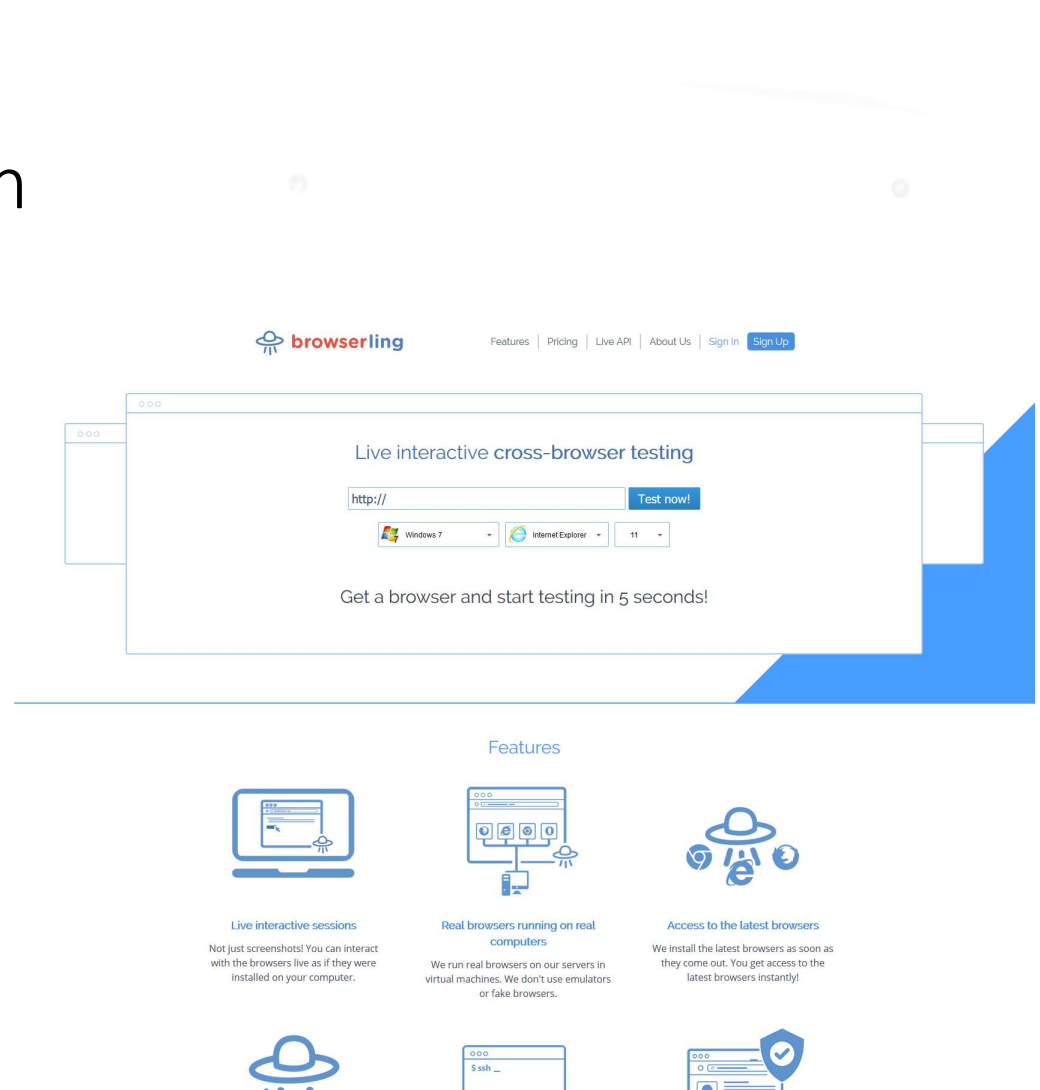
URL	Submitted	Size	IPs
<a href="#">durmebach.com/tropbox/fde0218eb095124b174829f43ef20c8f/download.html</a>	26 seconds ago	235 KB	25
<a href="#">jessekancierz.com/m4il/e40c065221004c63a22644e41beb6c5/</a>	31 seconds ago	293 KB	8
<a href="#">staging.schoolsleuth.org/LOOK/07545969e4221253068264a2547ec0b03/</a>	36 seconds ago	310 KB	17
<a href="#">test2.jessekancierz.com/m4il/a36bd2eb1578d9c885d2eb3a1576c481/</a>	41 seconds ago	294 KB	8
<a href="#">freemallextractor.us/e0a89e358eb6bd8802ac994892001867/</a>	46 seconds ago	408 KB	25
<a href="#">test2.jessekancierz.com/m4il/170b188b50c337a1848f9f400e8ad092/</a>	51 seconds ago	294 KB	8
<a href="#">leas.org.gr/modules/mod_breadcrumbs/tmpl/campolino/chines/9183a5a2351578414eb5d...</a>	56 seconds ago	51 KB	3
<a href="#">freemallextractor.us/c324736bd3da1251ab23e50d4b0e7b3d/</a>	1 minute ago	408 KB	25
<a href="#">staging.schoolsleuth.org/LOOK/3695f95c11e03cbda38c15357373dc5d/</a>	1 minute ago	310 KB	17
<a href="#">test2.jessekancierz.com/m4il/Qf3f6d40c7dbfba55c591aaeabd33fb/</a>	1 minute ago	294 KB	8

1387136 public scans of 1767358 in total

# Phishing email investigation

## Browserling

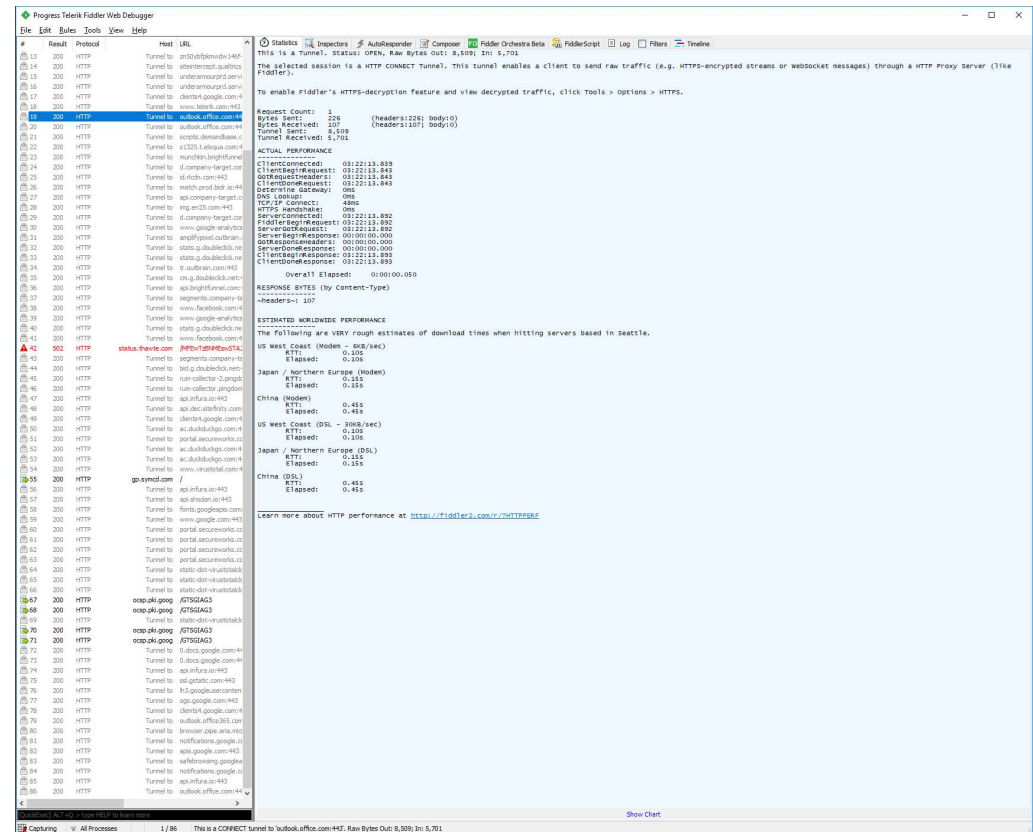
- Simple, interactive website sandbox
- Very useful to verify a website that requires multiple steps to reach malicious payload
- Great alternative to a local investigation VM



# Phishing email investigation

## Fiddler

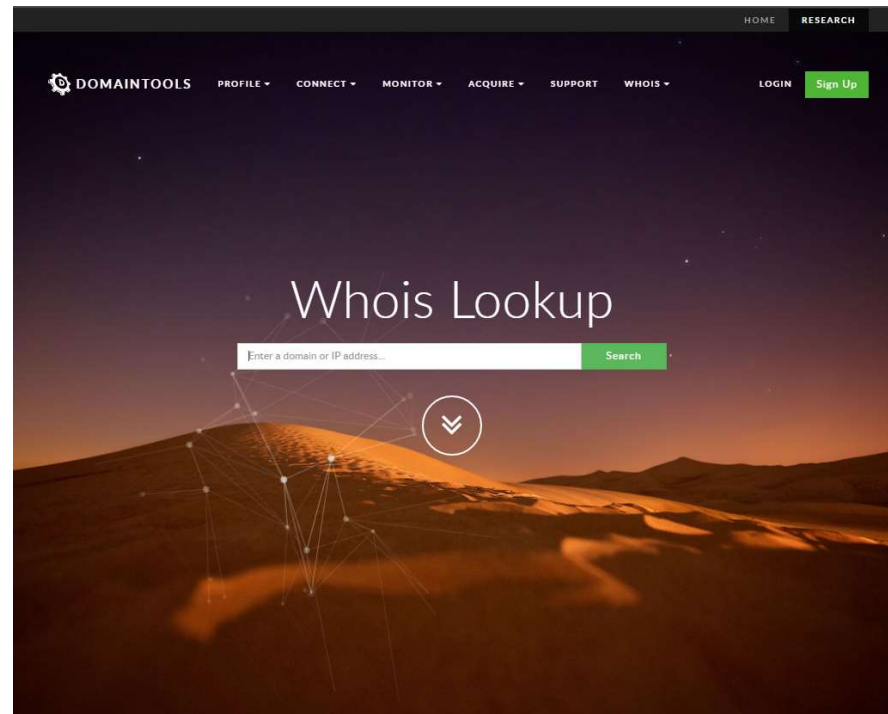
- The free web debugging proxy for any browser, system or platform
- Web session manipulation tool
- HTTPS inspection can be set up
- Amazing tool to log “behind the scenes” activities



# Phishing email investigation

<https://whois.domaintools.com/> or <https://centralops.net/co/>

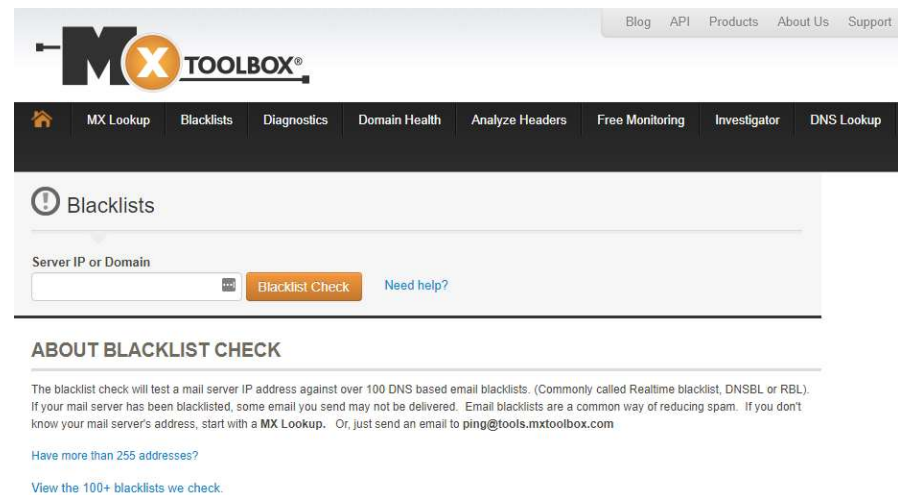
- It provides website details like website title, server type, registered date, SEO score, nameservers, geolocation etc
- Whois record and registrar data



# Phishing email investigation

<https://mxtoolbox.com/blacklists.aspx>

- The blacklist check will test a mail server IP address or domain against over 100 DNS based email blacklists commonly called Realtime blacklist, DNSBL or RBL



The screenshot shows the MXToolbox website's 'Blacklists' page. At the top, there's a navigation bar with links for Blog, API, Products, About Us, and Support. Below this is a dark navigation bar with icons and labels for MX Lookup, Blacklists (active), Diagnostics, Domain Health, Analyze Headers, Free Monitoring, Investigator, and DNS Lookup. The main content area is titled 'Blacklists' with a warning icon. It features a form with a label 'Server IP or Domain', a text input field, a 'Blacklist Check' button, and a 'Need help?' link. Below the form, there's a section titled 'ABOUT BLACKLIST CHECK' which explains that the tool tests against over 100 DNS-based email blacklists (Realtime, DNSBL, or RBL) and provides instructions on how to use the tool and where to find more information.

**MX TOOLBOX®**

Blog API Products About Us Support

Home MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Monitoring Investigator DNS Lookup

**Blacklists**

Server IP or Domain  **Blacklist Check** [Need help?](#)

**ABOUT BLACKLIST CHECK**

The blacklist check will test a mail server IP address against over 100 DNS based email blacklists. (Commonly called Realtime blacklist, DNSBL or RBL). If your mail server has been blacklisted, some email you send may not be delivered. Email blacklists are a common way of reducing spam. If you don't know your mail server's address, start with a **MX Lookup**. Or, just send an email to [ping@tools.mxtoolbox.com](mailto:ping@tools.mxtoolbox.com)

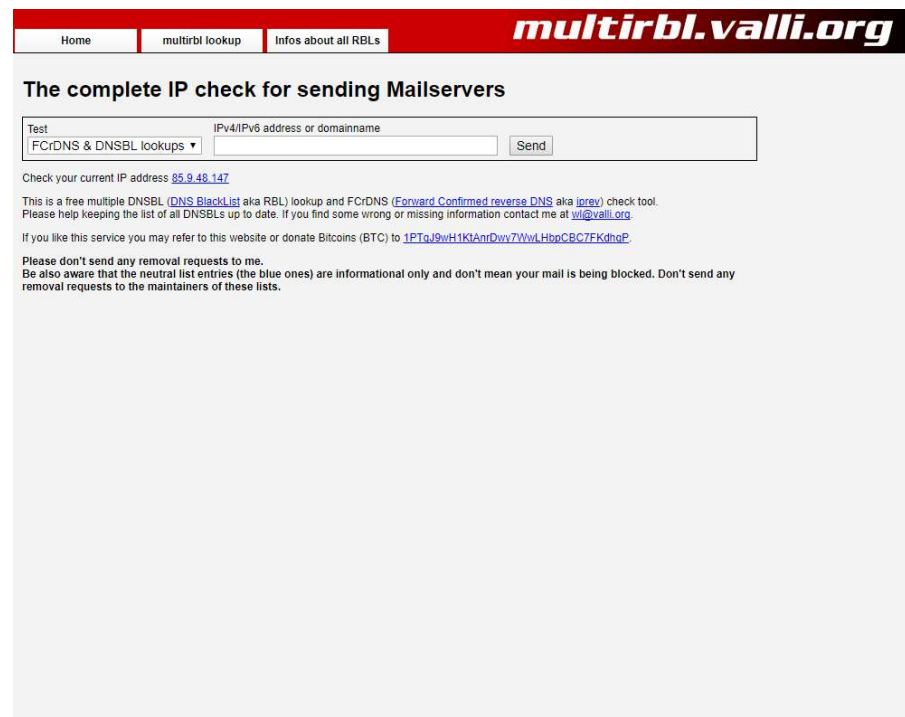
[Have more than 255 addresses?](#)

[View the 100+ blacklists we check.](#)

# Phishing email investigation

<http://multirbl.valli.org/>

- Checks an IP against 183 blacklist databases from the email relay behavior perspective
- Has the possibility to open a report to any of the sources already checked
- Displays 2 sections:
  - Summary list
  - Detailed list

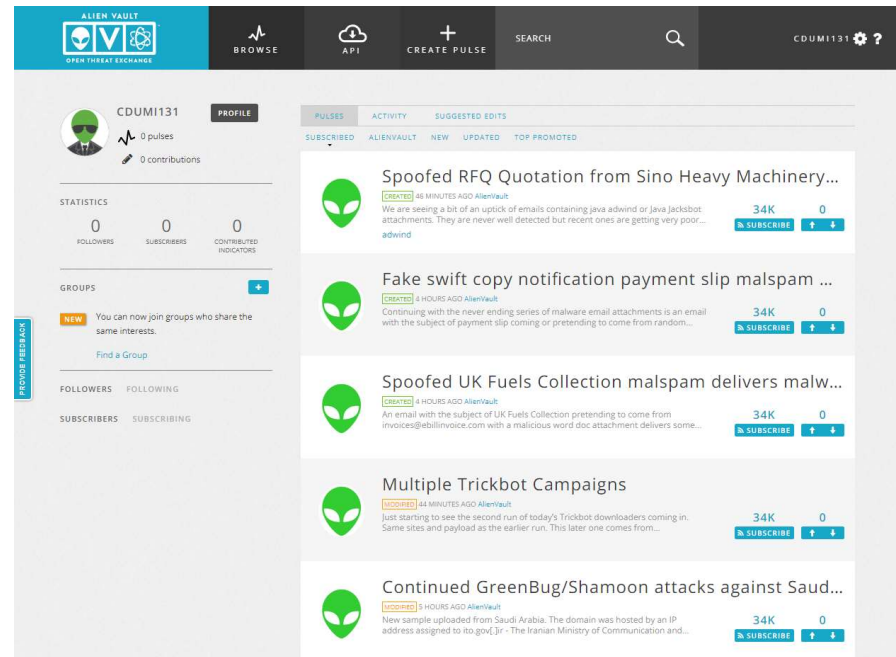


The screenshot shows the website **multirbl.valli.org** with a red header bar containing navigation links: Home, multirbl lookup, and Infos about all RBLs. The main heading is "The complete IP check for sending Mailservers". Below this is a form with a "Test" dropdown menu set to "FCrDNS & DNSBL lookups", a text input field for "IPv4/IPv6 address or domainname", and a "Send" button. Under the form, it says "Check your current IP address [85.9.48.147](#)". A paragraph of text explains the service is free and provides contact information. A Bitcoin address is also listed for donations. A final disclaimer states that the service does not handle removal requests and that blue entries in the results are informational only.

# Phishing email investigation

<https://otx.alienvault.com/>

- Can be searched for IP, domain, email address, hash
- Based on IOCs, campaigns can be identified, which are named “pulses”
- Great structure which can be organized by Industry
- Offers information about Malicious parties and identifies associated pulses
- Grants the possibility to create and join specific groups
- API Integration, amongst which Carbon Black feeds integration





# Security Incident investigation

# Security Incident investigation

## CTP Incident

- Timestamp: Mar 15 04:27:09
- Hostname: LPT-PC12877
- Local: 192.168.1.103
- Local Port 51737
- Remote: 46.173.213.228
- Remote Port 80
- TCPIntrusion ID: 0
- Begin: 2018-03-13 11:27:38
- End: 2018-03-13 11:27:38
- Occurrences: 1
- Application:  
C:/WINDOWS/SYSWOW64/SVCHOST.EXE
- User: jsmith
- Domain: EXAMPLE.com
- CIDS Signature ID: 29714
- CIDS Signature string: System Infected:  
Trojan.Snifula Activity 9CIDS
- Signature SubID: 74394
- Intrusion URL:  
sumohimbe.com/ls5/forum.php

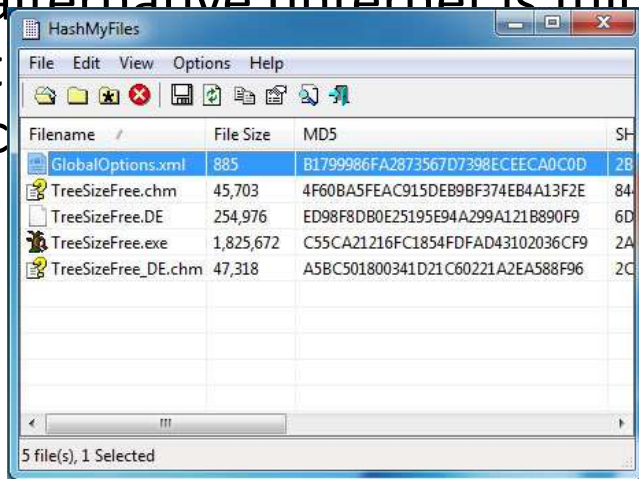
# CTP Incident

## Hashing a file

- **Nirsoft HashMyFiles**

[www.nirsoft.net/utils/hash\\_my\\_files.html](http://www.nirsoft.net/utils/hash_my_files.html)

- A tool like Nirsoft or any other alternative (internet is full of



- **Microsoft File Checksum Integrity Verifier utility**

[support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u](http://support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u)

- A tool like this can be installed and can be used from CLI to generate hashes for multiple files at once

# Google Dorking

## Google Dorking

- Incredibly useful to narrow down the search results and make them easier to surf
- Also used to gather juicy information
- Searching for publicly available information that should not be indexed:
  - Email addresses
  - Documents: pdf, ppt, doc, xls etc.
  - Personal Identifiable Information
- Reference: <https://www.sans.org/security-resources/GoogleCheatSheet.pdf>
- Tons of searches: <https://www.exploit-db.com/google-hacking-database/>

# Category Checkers

# Category Checkers

- Forcepoint (Websense) CSI <https://csi.forcepoint.com/>
- McAfee Trusted Source <http://www.trustedsource.org/>
- Fortinet Web Filter Lookup <http://fortiguard.com/iprep>
- Webroot URL/IP Lookup <http://www.brightcloud.com/tools/url-ip-lookup.php>
- Checkpoint URL categories <https://www.checkpoint.com/urlcat/main.htm>
- Palo Alto - Test a site <https://urlfiltering.paloaltonetworks.com/>
- AVG Threat Lab <http://www.avgthreatlabs.com/en-ww/website-safety-reports>
- Norton Safe Web <https://safeweb.norton.com/>
- Bluecoat WebPulse <https://sitereview.bluecoat.com/sitereview.jsp>
- Trend Micro Site Safety <https://global.sitesafety.trendmicro.com/>
- Google Safebrowsing <https://transparencyreport.google.com/safe-browsing/search>

Other useful tools

# Online - Useful tools or add-ons

- Check Short URL - <http://www.checkshorturl.com/>
- ASCII to Hex - <http://www.asciitohex.com/>
- JS Beautifier - <http://jsbeautifier.org/>
- Threat Analytics Search - <http://www.criticalstart.com/threat-analytics-chrome-plugin/>
- Project Naptha - <http://projectnaptha.com/>
- Export Tabs - <https://chrome.google.com/webstore/detail/export-tabs/odafagokkafdbbeojliiojjmimakacil>
- Postman - <https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdgggehcdcbncdddomop>
- Malware Traffic Analysis - <http://www.malware-traffic-analysis.net/index.html>



# Offline - Useful tools

- Nirsoft HashMyFiles - [http://www.nirsoft.net/utils/hash\\_my\\_files.html](http://www.nirsoft.net/utils/hash_my_files.html)
- Notepad++ - <https://notepad-plus-plus.org/download>
- Sublime Text - <https://www.sublimetext.com/>
- Wireshark - <https://www.wireshark.org/#download>
- Fiddler - <https://www.telerik.com/download/fiddler>
- Gary Kessler's list: [https://www.garykessler.net/library/file\\_sigs.html](https://www.garykessler.net/library/file_sigs.html)

Q&A

