

1. Top 10 Entities

Total number of entities	28
Total number of links	28

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	Email Address	w3snoop.com@domainsbyproxy.com	1
2	Email Address	abuse@godaddy.com	1
3	DNS Name	apitwitter.com.w3snoop.com	1
4	Email Address	evil@unspeakable-evil.com	1
5	Email Address	vil@unspeakable-evil.com	1
6	Email Address	zen@evil.com	1
7	Domain	w3snoop.com	1
8	Email Address	hacker@evil.com	1
9	Email Address	collect@evil.com	1
10	Email Address	site@evil.com	1

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	Domain	evil.com	20
2	Domain	w3snoop.com	2
3	Website	apitwitter.com.evil.com	2
4	Website	apitwitter.com.w3snoop.com	2
5	DNS Name	apitwitter.com.w3snoop.com	1
6	DNS Name	apitwitter.com.evil.com	1
7	Email Address	w3snoop.com@domainsbyproxy.com	0
8	Email Address	abuse@godaddy.com	0
9	Email Address	evil@unspeakable-evil.com	0
10	Email Address	vil@unspeakable-evil.com	0

Ranked by Total Links

Rank	Type	Value	Total links
1	Domain	evil.com	21
2	Domain	w3snoop.com	3
3	Website	apitwitter.com.evil.com	3
4	Website	apitwitter.com.w3snoop.com	3
5	DNS Name	apitwitter.com.w3snoop.com	2
6	DNS Name	apitwitter.com.evil.com	2
7	Email Address	w3snoop.com@domainsbyproxy.com	1
8	Email Address	abuse@godaddy.com	1
9	Email Address	evil@unspeakable-evil.com	1
10	Email Address	vil@unspeakable-evil.com	1

2. Entities by Type

DNS Names (2)

apitwitter.com.evil.com

apitwitter.com.w3snoop.com

Domains (2)

evil.com

w3snoop.com

Email Addresses (22)

abuse@godaddy.com

alice@evil.com

collect@evil.com

devil@evil.com

domain.operations@web.com

hacker@evil.com

info@mid-evil.com

n69pg4637nj@networksolutionsprivateregistration.com

site@evil.com

talk2us@lesserevil.com

w3snoop.com@domainsbyproxy.com

abuse@web.com

attacker@evil.com

crart@evil.com

devilteachme@evil.com

evil@unspeakable-evil.com

info@crackevil.com

jc9aq8n264m@networksolutionsprivateregistration.com

script@evil.com

slaytanic@evil.com

vil@unspeakable-evil.com

zen@evil.com

Websites (2)

apitwitter.com.evil.com

apitwitter.com.w3snoop.com

3. Entity Details



Domain
maltego.Domain
evil.com

Weight	100
Domain Name	evil.com

WHOIS Info

Domain Name: EVIL.COM
Registry Domain ID: 1040763_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: <http://networksolutions.com>
Updated Date: 2019-12-17T16:17:59Z
Creation Date: 1995-04-10T04:00:00Z
Registry Expiry Date: 2023-04-11T04:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientDeleteProhibited
<https://icann.org/epp#clientDeleteProhibited>
Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited
<https://icann.org/epp#clientUpdateProhibited>
Name Server: NS1.VERIO.COM
Name Server: NS2.VERIO.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form:
<https://www.icann.org/wicf/>
>>> Last update of whois database: 2021-10-10T06:04:33Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain Name: EVIL.COM
Registry Domain ID: 1040763_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: <http://www.networksolutions.com>
Updated Date: 2019-12-17T16:51:42Z
Creation Date: 1995-04-10T04:00:00Z
Registrar Registration Expiration Date: 2023-04-11T04:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status:
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US

Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: n69pg4637nj@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088780
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: n69pg4637nj@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088780
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jc9aq8n264m@networksolutionsprivateregistration.com
Name Server: NS1.VERIO.COM
Name Server: NS2.VERIO.COM
DNSSEC: Unsigned
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
URL of the ICANN WHOIS Data Problem Reporting System:
<http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2021-10-11T03:47:03Z <<<

For more information on Whois status codes, please visit
<https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>

This listing is a Network Solutions Private Registration. Mail correspondence to this address must be sent via USPS Express Mail(TM) or USPS Certified Mail(R); all other mail will not be processed. Be sure to include the registrant's domain name in the address.

The data in Networksolutions.com's WHOIS database is provided to you by Networksolutions.com for information purposes only, that is, to assist you in obtaining information about or related to a domain name registration record. Networksolutions.com makes this information available "as is," and does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; or (2) enable high volume, automated, electronic processes that apply to Networksolutions.com (or its systems). The compilation, repackaging, dissemination or other use of this data is expressly prohibited without the prior written consent of Networksolutions.com. Networksolutions.com reserves the right to modify these terms at any time. By submitting this query, you agree to abide by these terms.

For more information on Whois status codes, please visit
<https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>.

Incoming (1)



Website

apitwitter.com.evill.com

Outgoing (20)

@	Email Address	abuse@web.com
@	Email Address	alice@evil.com
@	Email Address	attacker@evil.com
@	Email Address	collect@evil.com
@	Email Address	crart@evil.com
@	Email Address	devil@evil.com
@	Email Address	deviltachme@evil.com
@	Email Address	domain.operations@web.com
@	Email Address	evil@unspeakable-evil.com
@	Email Address	hacker@evil.com
@	Email Address	info@crackevil.com
@	Email Address	info@mid-evil.com
@	Email Address	jc9aq8n264m@networksolutionsprivateregistration.com
@	Email Address	n69pg4637nj@networksolutionsprivateregistration.com
@	Email Address	script@evil.com
@	Email Address	site@evil.com
@	Email Address	slaytanic@evil.com
@	Email Address	talk2us@lesserevil.com
@	Email Address	vil@unspeakable-evil.com
@	Email Address	zen@evil.com



Domain

maltego.Domain

w3snoop.com

Weight	100
Domain Name	w3snoop.com

WHOIS Info

Domain Name: W3SNOOP.COM
Registry Domain ID: 1660071767_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: <http://www.godaddy.com>
Updated Date: 2020-02-10T04:49:41Z
Creation Date: 2011-06-06T02:04:22Z
Registry Expiry Date: 2023-06-06T02:04:22Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited
<https://icann.org/epp#clientDeleteProhibited>
Domain Status: clientRenewProhibited
<https://icann.org/epp#clientRenewProhibited>
Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited
<https://icann.org/epp#clientUpdateProhibited>
Name Server: INDRI.EZOICNS.COM
Name Server: SAOLA.EZOICNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form:
<https://www.icann.org/wicf/>
>>> Last update of whois database: 2021-10-10T06:04:33Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.


Domain Name: W3SNOOP.COM
Registry Domain ID: 1660071767_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: <http://www.godaddy.com>
Updated Date: 2019-05-16T00:10:25Z
Creation Date: 2011-06-05T21:04:22Z
Registrar Registration Expiration Date: 2023-06-05T21:04:22Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited
<https://icann.org/epp#clientUpdateProhibited>
Domain Status: clientRenewProhibited
<https://icann.org/epp#clientRenewProhibited>

<https://icann.org/epp#clientRenewProhibited>
Domain Status: clientDeleteProhibited
<https://icann.org/epp#clientDeleteProhibited>
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: W3SNOOP.COM@domainsbyproxy.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: W3SNOOP.COM@domainsbyproxy.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: W3SNOOP.COM@domainsbyproxy.com
Name Server: INDRI.EZOICNS.COM
Name Server: SAOLA.EZOICNS.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
<http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2021-10-11T03:47:03Z <<<
For more information on Whois status codes, please visit <https://icann.org/epp>



TERMS OF USE: The data contained in this registrar's Whois database, while believed by the registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its accuracy. This information is provided for the sole purpose of assisting you in obtaining information about domain name registration records. Any use of this data for any other purpose is expressly forbidden without the prior written permission of this registrar. By submitting an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not to use this data to allow, enable, or otherwise support the dissemination or collection of this data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations of any kind, including spam. You further agree not to use this data to enable high volume, automated or robotic electronic processes designed to collect or compile this data for any purpose, including mining this data for your own personal or commercial purposes. Failure to comply with these terms may result in termination of access to the Whois database. These terms may

may result in termination of access to the Whois database. These terms may be subject to modification at any time without notice.

Incoming (1)

 Website	apitwitter.com.w3snoop.com
---	----------------------------

Outgoing (2)

 Email Address	abuse@godaddy.com
 Email Address	w3snoop.com@domainsbyproxy.com



Website

maltego.Website


apitwitter.com.evil.com

Weight	100
Website	apitwitter.com.evil.com
SSL Enabled	false
Ports	[80]
SSL Ports	443



Info

[View Website](#)

Incoming (1)

 DNS Name	apitwitter.com.evil.com
--	-------------------------

Outgoing (2)

 DNS Name	apitwitter.com.evil.com
 Domain	evil.com



Website

maltego.Website


apitwitter.com.w3snoop.com

Weight	100
Website	apitwitter.com.w3snoop.com
SSL Enabled	false
Ports	[80]
SSL Ports	443



Info

[View Website](#)

Incoming (1)

 DNS Name	apitwitter.com.w3snoop.com
--	----------------------------

Outgoing (2)

 DNS Name	apitwitter.com.w3snoop.com
 Domain	w3snoop.com



DNS Name

maltego.DNSName

apitwitter.com.w3snoop.com

Weight	10
DNS Name	apitwitter.com.w3snoop.com
DNSDB JSON Output	{"count": 3, "time_first": 1520301970, "time_last": 1520301971, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "CNAME", "bailiwick": "w3snoop.com.", "rdata": "w3snoop.com."}

DNSDB JSON Output

```
{"count": 2, "time_first": 1555029159, "time_last": 1555029159, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "A", "bailiwick": "w3snoop.com.", "rdata": "18.195.122.112"}
```

DNSDB JSON Output

```
{"count": 2, "time_first": 1558494374, "time_last": 1558494374, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "A", "bailiwick": "w3snoop.com.", "rdata": "18.197.0.7"}
```

DNSDB JSON Output

```
{"count": 18, "time_first": 1454605804, "time_last": 1512134580, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "A", "bailiwick": "w3snoop.com.", "rdata": "173.199.149.76"}
```

DNSDB JSON Output

```
{"count": 3, "time_first": 1520301970, "time_last": 1520301971, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "CNAME", "bailiwick": "w3snoop.com.", "rdata": "w3snoop.com."}
```

Incoming (1)



Website

apitwitter.com.w3snoop.com

Outgoing (1)



Website

apitwitter.com.w3snoop.com



DNS Name

maltego.DNSName

apitwitter.com.evil.com

Weight	3
DNS Name	apitwitter.com.evil.com
DNSDB JSON Output	{"count": 3, "time_first": 1614290179, "time_last": 1622789802, "rrname": "apitwitter.com.evil.com.", "rrtype": "A", "bailiwick": "evil.com.", "rdata": "66.96.146.129"}

DNSDB JSON Output

```
{"count": 3, "time_first": 1614290179, "time_last": 1622789802, "rrname": "apitwitter.com.evil.com.", "rrtype": "A", "bailiwick": "evil.com.", "rdata": "66.96.146.129"}
```

Incoming (1)



Website

apitwitter.com.evil.com

Outgoing (1)



Website

apitwitter.com.evil.com





Email Address


maltego.EmailAddress

w3snoop.com@domainsbyproxy.com

Weight	100
Email Address	w3snoop.com@domainsbyproxy.com
Incoming (1)	
 Domain	w3snoop.com

	Email Address maltego.EmailAddress abuse@godaddy.com
Weight	100
Email Address	abuse@godaddy.com
Incoming (1)	
 Domain	w3snoop.com

	Email Address maltego.EmailAddress evil@unspeakable-evil.com
Weight	9
Email Address	evil@unspeakable-evil.com
Urls	https://www.unspeakable-evil.com/ Unspeakable Evil
Snippets	
From Bing Search: ["evil.com" contact; Page 7]	
Unspeakable Evil	
[https://www.unspeakable-evil.com]	
Unspeakable Evil All-Hand-Made / All-Natural / Pure-Evil. Evil is here. Shop - Unspeakable Evil on Etsy. Evil is nice. Contact us: E vil@Unspeakable-Evil.com. contact: evil@unspeakable-evil.com est. 2020, Brooklyn, NY . Page updated. Google Sites. Report abuse ...	
2021-10-03T15:13:00.0000000Z	
Incoming (1)	
 Domain	evil.com

	Email Address maltego.EmailAddress vil@unspeakable-evil.com
Weight	18
Email Address	vil@unspeakable-evil.com
Urls	https://www.unspeakable-evil.com/ Unspeakable Evil

Snippets

From Bing Search: ["evil.com" contact; Page 7]

Unspeakable Evil

[\[https://www.unspeakable-evil.com\]](https://www.unspeakable-evil.com)

Unspeakable Evil All-Hand-Made / All-Natural / Pure-Evil. Evil is here. Shop - Unspeakable Evil on Etsy. Evil is nice. Contact us: E vil@Unspeakable-Evil.com. contact: evil@unspeakable-evil.com est. 2020, Brooklyn, NY . Page updated. Google Sites. Report abuse ...

2021-10-03T15:13:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

zen@evil.com

Weight	59
Email Address	zen@evil.com
Urls	https://sites.google.com/a/devitto.com/dom/Dom-De-Vitto-DeVitto-Brain-Sprinkles/Dom-De-Vitto-DeVitto-Brain-Sprinkles-Security Security - Dom De Vitto's Home Page - Google Search

Snippets

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

hacker@evil.com

Weight	68
Email Address	hacker@evil.com
Urls	https://inst.eecs.berkeley.edu/~cs161/sp14/slides/2.10.Webinject.pdf Server-side Web Security and Injection Attacks

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

Server-side Web Security and Injection Attacks

[\[https://inst.eecs.berkeley.edu/~cs161/sp14/slides/2.10.Webinject.pdf\]](https://inst.eecs.berkeley.edu/~cs161/sp14/slides/2.10.Webinject.pdf)

"grep 'foo\\'; mail -s hacker@evil.com

2021-08-28T11:52:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

collect@evil.com

Weight	77
Email Address	collect@evil.com
Urls	https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/ New cracks in Google mail • The Register https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/ New cracks in Google mail • The Register

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

New cracks in Google mail • The Register

[\[https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/\]](https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/)

The naughty site uses a sleight of hand known as a multipart/form-data POST, which writes a filter to Gmail that causes all email with attachments to be forwarded to collect@evil.com. Petkov didn't provide a proof of concept or detailed documentation, but Ryan Naraine of the Zero Day blog writes here that the exploit was demonstrated for him.

2021-07-17T06:24:00.0000000Z

New cracks in Google mail • The Register

[\[https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/\]](https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/)

The naughty site uses a sleight of hand known as a multipart/form-data POST, which writes a filter to Gmail that causes all email with attachments to be forwarded to collect@evil.com. Petkov didn't provide a proof of concept or detailed documentation, but Ryan Naraine of the Zero Day blog writes here that the exploit was demonstrated for him.

2021-07-17T06:24:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

site@evil.com

Weight	84
Email Address	site@evil.com
Urls	https://softwareengineering.stackexchange.com/questions/216605/how-do-web-servers-enforce-the-same-origin-policy web development - How do web servers enforce the same ...

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

web development - How do web servers enforce the same ...

[\[https://softwareengineering.stackexchange.com/questions/216605\]](https://softwareengineering.stackexchange.com/questions/216605)

If the SOP were not in place, and I was signed into Gmail, the script at evil.com could see my inbox. If the site at evil.com wants to load mail.google.com without my cookies, it can just use a proxy server; the public contents of mail.google.com are not a secret (but the contents of mail.google.com when accessed with my cookies are a secret).

2021-09-16T17:33:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

talk2us@lesserevil.com

Weight	26
Email Address	talk2us@lesserevil.com
Urls	https://lesserevil.com/pages/contact Contact LesserEvil Contact Lesser Evil Healthy Snacks

Snippets

From Bing Search: ["evil.com" contact; Page 7]

Contact LesserEvil | Contact Lesser Evil | Healthy Snacks

[\[https://lesserevil.com/pages/contact\]](https://lesserevil.com/pages/contact)

Contact. NAME EMAIL SUBJECT. MESSAGE. Reach Us (203) 529-3551 x 100 talk2us@lesserevil.com. Office Hours Monday - Friday 8:30am - 5:00pm EST Snail Mail 41 Eagle Rd Danbury, CT 06810 YOUR CART. CONTINUE SHOPPING \$ Subtotal. Checkout. temp. Shop All; Shop Wholesale ...

2021-09-30T19:34:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

attacker@evil.com

Weight	34
Email Address	attacker@evil.com
Urls	https://blog.sucuri.net/2019/10/an-indirect-way-to-change-cpanel-passwords.html An Indirect Way to Change cPanel Passwords

Snippets

From Bing Search: [inbody:"evil.com" contact; Page 6]

An Indirect Way to Change cPanel Passwords

[\[https://blog.sucuri.net/2019/10/an-indirect-way-to-change-cpanel-passwords.html\]](https://blog.sucuri.net/2019/10/an-indirect-way-to-change-cpanel-passwords.html)

Secondary contact email addresses configured in this manner can also be silently removed during this modification process for the primary contact email address. "email": 'attacker@evil.com' "notify_contact_address_change": 0

2021-09-29T04:45:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

info@mid-evil.com

Weight

45

Email Address

info@mid-evil.com

Urls

<https://www.mid-evil.com/contact/> Contact | Mid-Evil Industries
<https://www.mid-evil.com/products/> Products | Mid-Evil Industries
<https://www.mid-evil.com/contact/> Contact | Mid-Evil Industries

Snippets

From Bing Search: [inbody:"evil.com" contact; Page 6]

Contact | Mid-Evil Industries

[\[https://www.mid-evil.com/contact\]](https://www.mid-evil.com/contact)

Phone: (844) 556-GRIP (4747) PO Box 7735 San Diego, CA 92167, USA Email: info@mid-evil.com Hours: Mon-Fri 9am-5pm PST

2021-10-08T17:27:00.0000000Z

Products | Mid-Evil Industries

[\[https://www.mid-evil.com/products\]](https://www.mid-evil.com/products)

Contact. Phone: (844) 556-GRIP (4747) PO Box 7735 San Diego, CA 92167, USA Email: info@mid-evil.com Hours: Mon-Fri 9am-5pm PST . Newsletter Sign-up. Sign-up for our newsletter to stay in-the-know on news, new product releases and special deals! Name * Email * Website. Sign Me Up! Search by Keyword. Search for: ...

2021-10-05T15:11:00.0000000Z

Contact | Mid-Evil Industries

[\[https://www.mid-evil.com/contact\]](https://www.mid-evil.com/contact)

Phone: (844) 556-GRIP (4747) PO Box 7735 San Diego, CA 92167, USA Email: info@mid-evil.com Hours: Mon-Fri 9am-5pm PST

2021-10-08T17:27:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

info@crackevil.com

Weight	52
Email Address	info@crackevil.com
Urls	https://crackevil.com/crackevil/wordpress-16-9-apk WordPress 16.9 APK - FREE DOWNLOAD - crackevil.com https://crackevil.com/wordpress-themes/newspaper-9-1-wordpress-news-theme Newspaper V9.1 – WordPress News Theme - FREE DOWNLOAD

Snippets

From Bing Search: ["evil.com" mail; Page 4]

WordPress 16.9 APK - FREE DOWNLOAD - crackevil.com

[\[https://crackevil.com/crackevil/wordpress-16-9-apk\]](https://crackevil.com/crackevil/wordpress-16-9-apk)

Crack Evil is the best platform to get the Premium Themes and Templates for free. Enjoy! ... And if the developers feel bad about sharing their templates, please kindly mail us at info@crackevil.com, we will remove your templates immediately. Mission News Theme by Compete Themes.

2021-08-29T19:43:00.0000000Z

Newspaper V9.1 – WordPress News Theme - FREE DOWNLOAD

[\[https://crackevil.com/wordpress-themes/newspaper-9-1-wordpress-news-theme\]](https://crackevil.com/wordpress-themes/newspaper-9-1-wordpress-news-theme)

Crack Evil is the best platform to get the Premium Themes and Templates for free. Enjoy! ... And if the developers feel bad about sharing their templates, please kindly mail us at info@crackevil.com, we will remove your templates immediately. Mission News Theme by Compete Themes.

2021-09-15T07:13:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

script@evil.com

Weight

93

Email Address

script@evil.com

Urls

<https://softwareengineering.stackexchange.com/questions/216605/how-do-web-servers-enforce-the-same-origin-policy> web development - How do web servers enforce the same ...

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

web development - How do web servers enforce the same ...

[\[https://softwareengineering.stackexchange.com/questions/216605\]](https://softwareengineering.stackexchange.com/questions/216605)

If the SOP were not in place, and I was signed into Gmail, the script at evil.com could see my inbox. If the site at evil.com wants to load mail.google.com without my cookies, it can just use a proxy server; the public contents of mail.google.com are not a secret (but the contents of mail.google.com when accessed with my cookies are a secret).

2021-09-16T17:33:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

alice@evil.com

Weight	102
Email Address	alice@evil.com
Urls	https://security.stackexchange.com/questions/214925/mail-interception-fraud email - Mail interception fraud - Information Security ... https://security.stackexchange.com/questions/214925/mail-interception-fraud email - Mail interception fraud - Information Security ...

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

email - Mail interception fraud - Information Security ...

[\[https://security.stackexchange.com/questions/214925/mail-interception-fraud\]](https://security.stackexchange.com/questions/214925/mail-interception-fraud)

Shortly after alice@evil.com also sends a reminder mail to the customer. In this reminder there is also a pdf attachment that's nearly identical to the one Alice send, only the payment information has been altered. The customer also has a conversation with Alice about the change of bank account and always receives answers. My boss is cc'ed in ...

2021-10-04T19:21:00.0000000Z

email - Mail interception fraud - Information Security ...

[\[https://security.stackexchange.com/questions/214925/mail-interception-fraud\]](https://security.stackexchange.com/questions/214925/mail-interception-fraud)

Shortly after alice@evil.com also sends a reminder mail to the customer. In this reminder there is also a pdf attachment that's nearly identical to the one Alice send, only the payment information has been altered. The customer also has a conversation with Alice about the change of bank account and always receives answers. My boss is cc'ed in ...

2021-10-04T19:21:00.0000000Z

Incoming (1)



Domain

evil.com



Email Address

maltego.EmailAddress

devilteachme@evil.com

Weight	0
Email Address	devilteachme@evil.com

Info


View PGP Public Keys


1. [bed745bffe9d4930](#)

Signatures

SN	Key ID	Created	Expiry	View URL
1	bed745bffe9d4930	2015-03-19T14:06:24Z	2124-06-11T19:30:40Z	[selfsig]

Incoming (1)

 Domain evil.com



Email Address
 maltego.EmailAddress
slaytanic@evil.com

Weight0


Email Addressslaytanic@evil.com


Info

View PGP Public Keys
 1. [e1d2d93ec60ea033](#)
Signatures

SN	Key ID	Created	Expiry	View URL
1	e1d2d93ec60ea033	2016-06-29T15:16:56Z		[selfsig]

Incoming (1)

 Domain evil.com



Email Address
 maltego.EmailAddress
devil@evil.com

Weight0


Email Addressdevil@evil.com


Info

View PGP Public Keys
 1. [a82acf8c1ac73b64](#)
Signatures

SN	Key ID	Created	Expiry	View URL
1	a82acf8c1ac73b64	2015-03-27T19:44Z		[selfsig]

Incoming (1)

 Domain evil.com



Email Address
 maltego.EmailAddress
crart@evil.com

Weight0

Email Addresscrart@evil.com

Info


View PGP Public Keys


1. [1c96279827864f22](#)

Signatures

SN	Key ID	Created	Expiry	View URL
1	1c96279827864f22	2017-07-01T22:06:26Z		[selfsig]


Incoming (1)


 Domain	evil.com
--	----------

 Email Address
maltego.EmailAddress
domain.operations@web.com

Weight	100
Email Address	domain.operations@web.com


Incoming (1)


 Domain	evil.com
--	----------

 Email Address
maltego.EmailAddress
jc9aq8n264m@networksolutionsprivateregistration.com

Weight	100
Email Address	jc9aq8n264m@networksolutionsprivateregistration.com


Incoming (1)


 Domain	evil.com
--	----------


 Email Address
maltego.EmailAddress
n69pg4637nj@networksolutionsprivateregistration.com

Weight	100
Email Address	n69pg4637nj@networksolutionsprivateregistration.com

Incoming (1)

 Domain	evil.com
--	----------

 Email Address
maltego.EmailAddress
abuse@web.com

Weight	100
Email Address	abuse@web.com
Incoming (1)	
 Domain	evil.com