Settings

Post

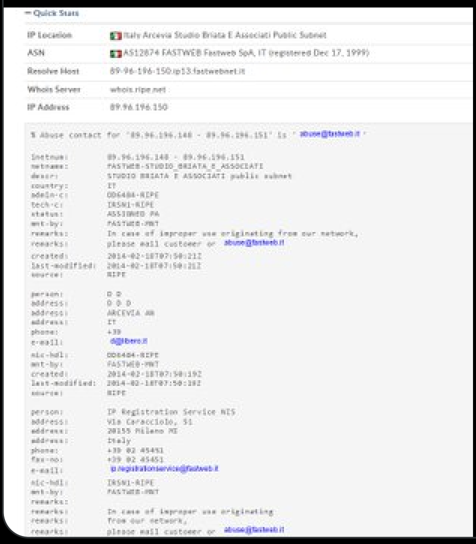
The Haag™ @M_haggis

Uncovered a fascinating yet potentially risky technique that is worthy of an #AtomicRedTeam test. The script manipulates the Windows Registry to reconfigure the default Internet Zone settings for both HTTP and HTTPS, aligning them with the "My Computer" zone. The implications? Websites, regardless of their intent, would be granted the same level of trust as files and applications locally stored on your machine. This could pave the way for malicious actors to exploit this elevated trust level. It's a clever approach.

Test it out:

Set-ItemProperty -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults' -Name 'http' -Value 0; Set-ItemProperty -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults' -Name 'https' -Value 0

> **JAMESWT** @JAMESWT_MHT · Sep 5, 2023
>
> http://89.96.196.]150:8080/
> Sample
> bazaar.abuse.ch/sample/339ff72...
> cc @csirt_it @AgidCert @FASTWEBHelp



— Quick Stats

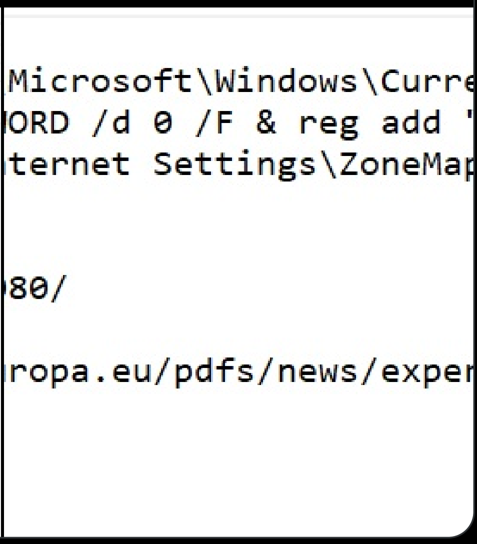
IP Location	Italy Arcevia Studio Briata E Associati Public Subnet
ASN	AS12874 FASTWEB Fastweb SpA, IT (registered Dec 17, 1999)
Resolve Host	89-96-196-150.ip13.fastwebnet.it
Whois Server	whois.ripe.net
IP Address	89.96.196.150

```
% Abuse contact for '89.96.196.148 - 89.96.196.151' is 'abuse@fastweb.it'

inetnum:        89.96.196.148 - 89.96.196.151
netname:        FASTWEB-STUDIO_BRIATA_E_ASSOCIATI
descr:          STUDIO BRIATA E ASSOCIATI public subnet
country:        IT
admin-c:        DD6404-RIPE
tech-c:         IRSN1-RIPE
status:         ASSIGNED PA
mnt-by:         FASTWEB-MNT
remarks:        In case of improper use originating from our network,
remarks:        please mail customer or  abuse@fastweb.it
created:        2014-02-18T07:50:21Z
last-modified:  2014-02-18T07:50:21Z
source:         RIPE

person:         D D
address:        D D D
address:        ARCEVIA AN
address:        IT
phone:          +39
e-mail:         d@libero.it
nic-hdl:        DD6404-RIPE
mnt-by:         FASTWEB-MNT
created:        2014-02-18T07:50:19Z
last-modified:  2014-02-18T07:50:19Z
source:         RIPE

person:         IP Registration Service NIS
address:        Via Caracciolo, 51
address:        20155 Milano MI
address:        Italy
phone:          +39 02 45451
fax-no:         +39 02 45451
e-mail:         ip.registrationservice@fastweb.it
nic-hdl:        IRSN1-RIPE
mnt-by:         FASTWEB-MNT
remarks:
remarks:        In case of improper use originating
remarks:        from our network,
remarks:        please mail customer or  abuse@fastweb.it
```



```
Microsoft\Windows\Curre
ORD /d 0 /F & reg add '
ternet Settings\ZoneMap

80/

ropa.eu/pdfs/news/exper
```

3:48 PM · Sep 5, 2023 · **20.4K** Views

30 Reposts **1** Quote **92** Likes **41** Bookmarks

41

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Something went wrong. Try reloading.

Retry

Terms of Service Privacy Policy Cookie Policy Accessibility Ads info More ··· © 2024 X Corp.

Don't miss what's happening

People on X are the first to know.

Log in Sign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: https://x.com/en/privacy

Did someone say … cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. Show more about your choices.

Accept all cookies

Refuse non-essential cookies