Domain name holders hit with personalized, malware-laden suspension notices

Ilan Meller, 2015-01-11

This according to Zeljka Zorz, HNS Managing Editor from Help Net Security.

In his article, Zeljka mention that new email spam campaign has been spotted targeting domain name holders, trying to trick them into downloading malware on their systems. The email is likely to fool some recipients, as it contains the valid domain registration and the recipient's full name, which the attackers must have harvested online, via the “whois” query. The sender's email address is also spoofed to make it look like the sender is the domain registrar. Those who get fooled and download and execute the file linked in the email will get saddled with malware - most likely a Trojan downloader, which will then proceed to download additional malware.

Below is the spam e-mail that was sent:

Subject: [Domain name] Suspension Notice

Dear Sir/Madam,

The following domain names have been suspended for violation of the Melbourne IT Ltd Abuse Policy:

Domain Name: [domain name]
Registrar: Melbourne IT Ltd
Registrant Name: [Registrant name matching whois]

Multiple warnings were sent by Melbourne IT Ltd Spam and Abuse Department to give you an opportunity to address the complaints we have received.

We did not receive a reply from you to these email warnings so we then attempted to contact you via telephone.

We had no choice but to suspend your domain name when you did not respond to our attempts to contact you.

Click here [LINK] and download a copy of complaints we have received.

Please contact us by email at mailto:abuse@melbourneit.com.au for additional information regarding this notification.

Sincerely,
Melbourne IT Ltd
Spam and Abuse Department
Abuse Department Hotline: 480-124-0101

According to the article, the most targeted registrars are Melbourne IT and Dynadot that already notified their clients of this campaign. In their official notification Dynadot states that “We have recently become aware of fake abuse notifications being sent out to our customers. The abuse messages look like they are being sent from our abuse@dynadot.com email; however, these messages are NOT being sent from us and should be disregarded. If you receive one of these emails or an email that you think may not be from us, do not click on any links, reply directly to the email, or call the number listed in the email".

To read Melbourne IT public announcement click here.

F5 SOC is familiar with this spam campaign as well with many others that come and go almost every day. This attack vector is very common in the hacktivists communities that using Social Engineering to lure victims into opening links and/or attachments in e-mail messages in order to broader their botnet pools and inititate DDoS attacks, money transfer, identity theft and more.

On a day to day basis, F5 mitigates online identity theft by preventing phishing, malware, and pharming attacks in real time with advanced encryption and identification mechanisms enabling financial organizations working online to gain control over areas that were once virtually unreachable and indefensible, and to neutralize local threats found on customers' personal computers, without requiring the installation of software on the end user side.

If you would like to learn more about F5 fraud protection, read the WebSafe datasheet as well as the MobileSafe datasheet.

To learn more about F5 Security Operation Centers, read the F5 SOC datasheet.

Click here to read the original article by Help Net Security.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com