

[NT] Abusing TCP/IP Name Resolution in Windows To Carry Out Phishing Attacks

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00037.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Mar 2007 13:15:01 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Abusing TCP/IP Name Resolution in Windows To Carry Out Phishing Attacks

SUMMARY

A vulnerability in the way Window tries to resolves FQDN allows attackers present on the local network to redirect them to a third-party server without needing to take over the DNS server.

DETAILS

Name resolution takes place in the following order on *nix boxes:

- * Local name
- * Look up into /etc/hosts file
- * Query the DNS server.

In Windows the name resolution follows:

- * Local name
- * Hosts file
- * DNS
- * WINS
- * NetBIOS b-node broadcasts
- * lmhosts file

[NT] Abusing TCP/IP Name Resolution in Windows To Carry Out Phishing Attacks

The NetBIOS b-node broadcasts can be abused to carry out phishing attacks. Thus, if someone types "gmail.ocm" instead of "gmail.com", then DNS and the WINS query will fail for this hostname and the victim's O.S will send the broadcast request on UDP 137 looking for the name gmail.ocm. This can then be responded by the attacker and a phishing attack can be done against him.

Victim -> DNS -> WINS -> (Local subnet + Attacker)
gmail.ocm -> failed -> failed -> broadcast request
<----- Attacker's response to victim for name
gmail.ocm

Tool Used:

FakeNetbiosNS (NetBIOS Name Service) available from URL:

<<http://honeynet.rstack.org/tools.php>>

<http://honeynet.rstack.org/tools.php>

Demonstration:

Case-1 Normal Scenario

Victim -> Local Subnet + Attacker

Ping gmail.ocm -----> Broadcast request for gmail.ocm [nbns query]

Time out (no response for NBNS query)

Case-2 Attacker Emulating hostnames

Victim fakenbns -> Local Subnet + Attacker running

Ping gmail.ocm -----> Broadcast request for gmail.ocm[nbns query]

<----- Attacker responds for gmail.ocm[nbns response]

Ping attacker's IP address as in NBNS response) <--> ping response

Attacker runs fakenetbios-ns script with these parameters:

/fakenbns -f ../FakeNetbiosDGM.conf.ini

Entries in FakeNetbiosDGM.conf.ini

MYDOMAIN HOST01 192.168.1.101 1 Windows XP Workstation

MYDOMAIN gmail.ocm 192.168.1.101 1 Windows XP Workstation

MYDOMAIN hotmail.ocm 192.168.1.101 1 Windows XP Workstation

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sid@xxxxxxxxxxxxxxxx>> Sumit Siddharth.

The original article can be found at:

<<http://www.ntsossecure.com/folder2/wp-content/uploads/2007/03/microsoft-word-abusing-nbns.pdf>>

<http://www.ntsossecure.com/folder2/wp-content/uploads/2007/03/microsoft-word-abusing-nbns.pdf>

=====

[NT] Abusing TCP/IP Name Resolution in Windows To Carry Out Phishing Attacks

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.