Abusing TCP/IP name resolution in Windows to carry out phishing attacks.

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

The NetBIOS b-node broacasts can be abused to carry out phishing attacks. Thus, if someone types "gmail.ocm" instead of "gmail.com" , than 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)

URL: 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	**Local Subnet + Attacker running fakenbns**
Ping 'gmail.ocm'----------→	Broadcast request for gmail.ocm[nbns query]
←----------	Attacker responds for gmail.ocm[nbns response]
Ping 'attacker's ip 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
```

Here is a good article from Microsoft which discusses this process in detail.

Drawbacks: Here are a few drawbacks of this attack:

1. This attack will only work for domain names that are less than 16 characters.

2. Routers typically do not forward broadcasts, so only *NetBIOS name* on the local network can be resolved and the attacker thus has to be on the same local network.

3. The victim has to enable NetBios Over TCP/IP to send out broadcast request.

Workaround: I could not locate any settings to disable windows from broadcasting requests to the network. Disable NetBios Over TCP/IP if they are not required. Use a third party firewall which disallows all outbound broadcast for name query or *just don't use Windows☺.*

References:

1. Fake NetBiosNS
   http://honeynet.rstack.org/tools.php
2. Netbios Node Types
   http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/cnet/cnbb_tcp_ejis.mspx?mfr=true
3. Name Resolution Article
   http://www.comptechdoc.org/os/windows/wintcp/wtcpname.html
4. Microsoft Article on Name resolution in windows
   http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/prork/prcc_tcp_gclb.mspx?mfr=true

Contacts:

Sumit Siddharth Sid@notsosecure.com