BadTunnel:

NetBIOS Name Service spoofing over the Internet

August 2016
Yang Yu (@tombkeeper)
Tencent's Xuanwu Lab

Abstract

This article introduces a new method for cross network NetBIOS Name Service spoofing, dubbed "BadTunnel".

It does not require the attacker resides in the same network. The attack can even succeed when there are firewall and NAT devices in between.

If the attacker can convince a user to visit a webpage using Internet Explorer or Microsoft Edge Web browser, or open an Office document, the attacker can then:

- Disguise as local printer server or file server.
- Bypass sandbox of Internet Explorer, no EPM / AppContainer.
- Hijack the network traffic, including but not limited to HTTP traffics, Windows Update downloads and Certificate Revocation List updates via Microsoft Crypto API.

BadTunnel attack is effective against all versions of Windows. The attack can be performed on all versions of Internet Explorer and Microsoft Office.

In fact, it's effective on anywhere that a file URI scheme or UNC path can be embedded into. For example, if a file URI or UNC path is embedded into a shortcut link file (the Microsoft proprietary LNK / URL file) the BadTunnel attack can be triggered at the moment the user views the file in the Windows Explorer. It therefore can be exploited via webpage, email, flash drive and many other medias. It can even be effective against servers, please refer to [1] "10 Places to Stick Your UNC Path" for more information.

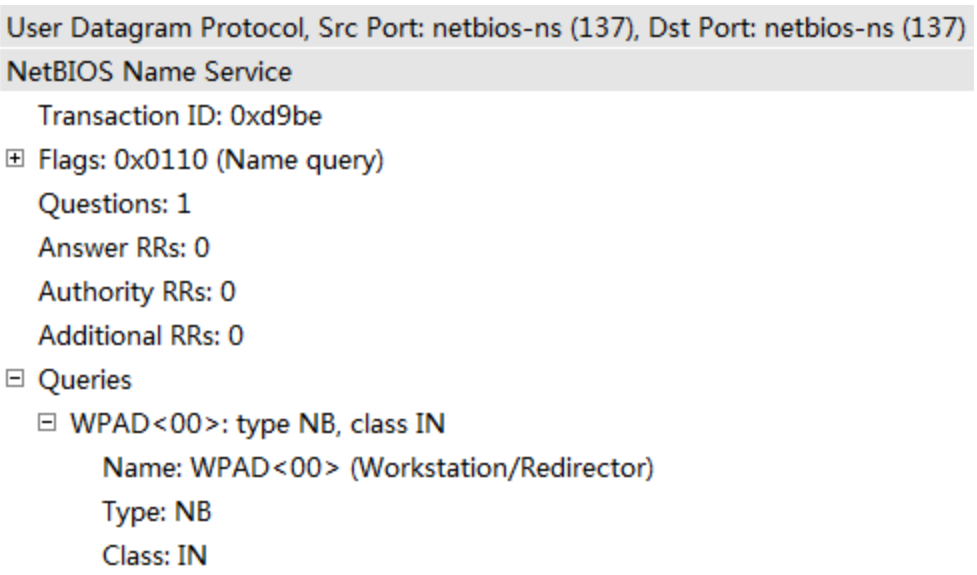
Technical Details

The BadTunnel attack is achieved by chaining a series of minor security problems:

1. When the Windows operating system is trying to resolve a name such as "WPAD" or "FileServer", it broadcasts a NBNS NB query to the local area network, but the response is accepted regardless of the origin IP address.
2. Internet Explorer and Microsoft Edge browser supports webpage with embedded resources from a file URI or UNC path. Office documents can also embed these resources by setting TargetMode="External" in those XML files.

3. When Windows is trying to access a network path via IP address and the target is unreachable (packets to target's 139, 445 port is timed out or the connection is reset), an NBNS NBSTAT query will be send to the target address.

4. Similar to the DNS protocol, NBNS NB and NBNS NBSTAT query validates the response using the transaction id. However, the NBNS transaction id is incremental. To make it even worse, NBNS NB query and NBNS NBSTAT query shares the same counter. This makes the transaction id in the NBNS NB query predictable by observing the transaction id in a NBNS NBSTAT query at the same moment.



5. The operating system sends NBNS NB query and NBNS NBSTAT query with the same 137/UDP port. That means the NBNS NB query and NBNS NBSTAT query are bidirectional 137/UDP<->137/UDP. When Alice sends a NBNS NBSTAT query to Bob, firewalls must temporarily allow Bob to send data to Alice's 137/UDP port. Even if Alice resides in a local area network, when Alice send a NBNS NBSTAT query to Bob on the Internet, the tunnel established by NAT gateway also allows NBNS NBSTAT query or response in reverse direction.

6. A quick experiment. Suppose there are two firewall-enabled systems with IP address assigned to 192.168.1.2 and 192.168.100.3 respectively. Normally, running nbtstat –A 192.168.100.3 on 192.168.1.2 will not get any response because of the firewall. But then running nbtstat -A 192.168.1.2 on 192.168.100.3 can get a response. At the same time, running nbtstat -A 192.168.100.3 on 192.168.1.2 again can also get a response.

Attack Scenario

1. Alice and Bob can be located anywhere on their network, and have firewall and NAT devices in-between, as long as Bob's 137/UDP port is reachable by Alice.

2. Bob closes 139 and 445 port, but listen on 137/UDP port.

3. Alice is convinced to access a file URI or UNC path that points to Bob, and another hostname based URI such as "http://WPAD/x.jpg" or "http://FileServer/x.jpg". Alice will send a NBNS NBSTAT query to Bob, and also send a NBNS NB query to the LAN broadcast address.

4. If Bob blocks access to 139 and 445 port using a firewall, Alice will send a NBNS NBSTAT query after approximately 22 seconds. If Bob instead closed 139 and 445 port by disabling Server Windows service and NetBIOS over TCP/IP protocol, Alice do not need to wait for connection to time out before send the query.

5. When Bob received NBNS NBSTAT query sent by Alice, Bob forge a NBNS NB response by predicting the transaction id, and send to Alice. If a heartbeat packet is sent every few second, most firewall and NAT devices will keep the 137/UDP<->137/UDP tunnel open.

6. Alice will now add the resolved address sent by Bob to the NBT cache. The default TTL for NBT cache entry is 600 seconds.

The attack is now completed. Bob can now hijack Alice's network traffic by disguising as WPAD or ISATAP server. WPAD tricks can be traced back to at least CVE-1999-0858. HD Moore & Valsmith first presented technique to disguise as WPAD server in LAN by faking hostname in their Black Hat 2007 talk "Tactical Exploitation". The Flame worm uncovered in 2012 also borrowed this technique.

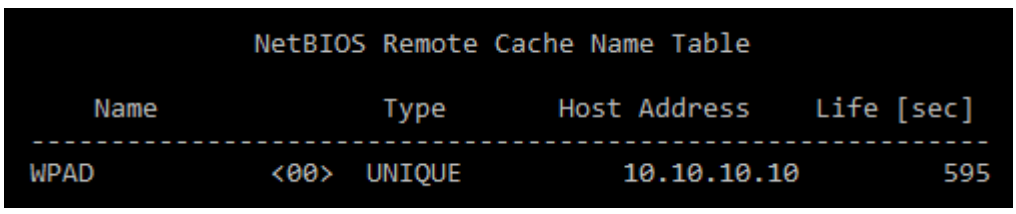
If the WPAD script returns "DIRECT" for a site, or we just spoof an IP to a periods-less hostname, the browser will runs at Medium IL, outside of EPM/AppContainer.

When hijacking Alice's network traffic, Bob can periodically redirect some HTTP request to file URI or UNC path points to Bob. In this way the attack can be persisted regardless of NBT cache TTL.

HTTP/1.1 302 Found
Content-Type: text/html
Location: file://[IP of Bob]/BadTunnel
Content-Length: 0

Bob can also insert attack vectors in webpages visited by Alice. These webpages will be cached by Web browser, and can retrigger attacks even if the tunnel between Alice and Bob is somehow disconnected.

Also, because Bob can keep the tunnel open by sending packet in every few seconds, even if Alice never visits Bob's file URI or UNC path again, Bob can still send forged NBNS NB response to Alice. In this scenario, although the transaction id cannot be precisely predicted, it will not increase much than 600 seconds earlier, usually within 100. Bob knows if the hijack is successful by observing if Alice accessed the hijacked IP address, Bob can therefore constantly probe the current range of Alice's transaction id, and the predicting difficulty will not increase over time.

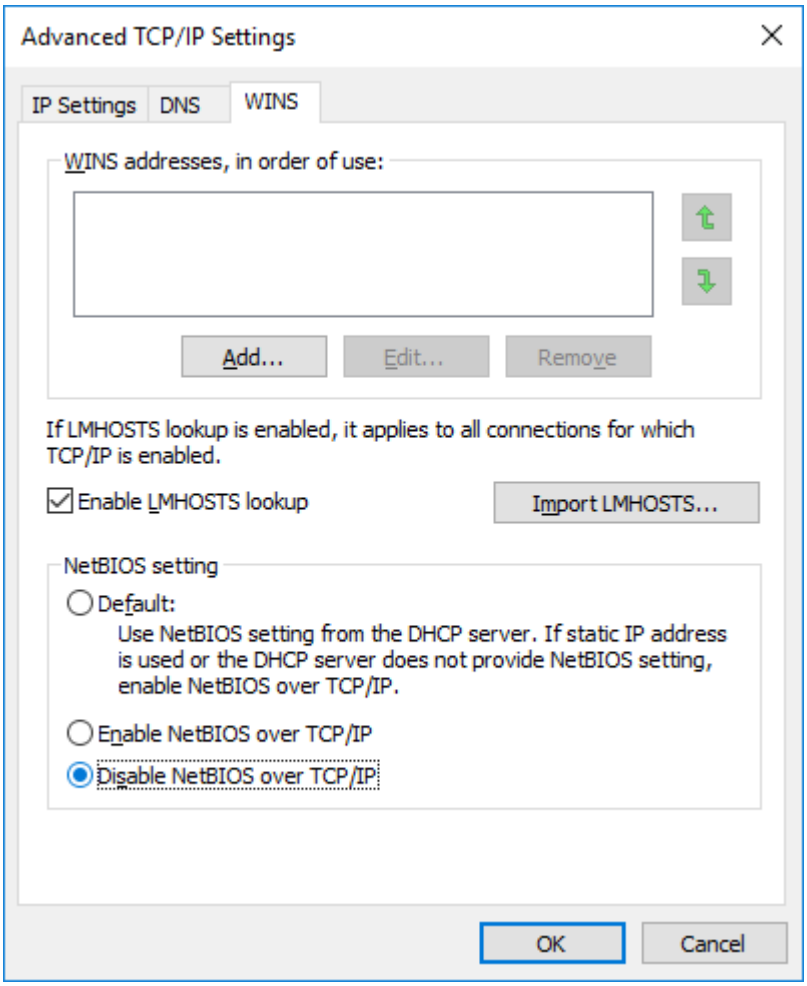


Mitigation Recommendations

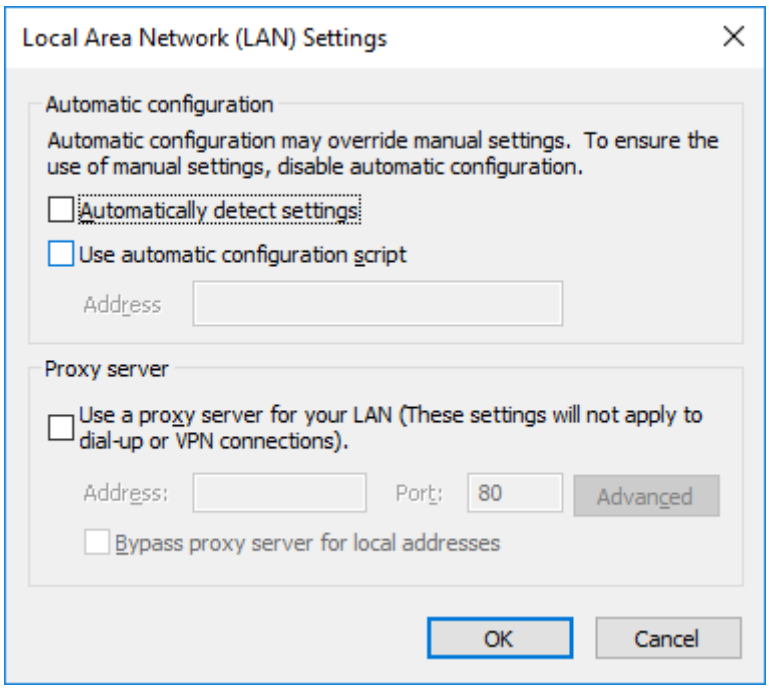
Even if the MS16-063 and MS16-077 patch cannot be installed immediately, there are workarounds that can stop the BadTunnel attack.

For enterprises, they can drop the 137/UDP packets on perimeter firewalls.

For end users that do not need to access Windows network sharing services, NetBIOS over TCP/IP can be disabled:



For minimal compatibility impact, WPAD address can be pinned to 127.0.0.1 in %SystemRoot%\System32\drivers\etc\hosts, or the automatic proxy discovery can be disabled to prevent hijacking:



However, BadTunnel is not limited to WPAD, and this does not stop hijacking of other names.

References

[1] 10 Places to Stick Your UNC Path
https://blog.netspi.com/10-places-to-stick-your-unc-path/

[2] Tactical Exploitation
https://www.blackhat.com/presentations/bh-usa-07/Moore_and_Valsmith/Whitepaper/bh-usa-07-moore_and_valsmith-WP.pdf

[3] Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployment
http://research.microsoft.com/pubs/79323/PBP-oakland-public.ppt

[4] Web Proxy Auto-Discovery Protocol
http://tools.ietf.org/html/draft-ietf-wrec-wpad-01

[5] NetBIOS Over TCP/IP
https://technet.microsoft.com/en-us/library/cc940063.aspx

[6] Disable WINS/NetBT name resolution
https://technet.microsoft.com/en-us/library/cc782733(v=ws.10).aspx

[7] MS99-054, CVE-1999-0858
https://technet.microsoft.com/en-us/library/security/ms99-054.aspx

[8] MS09-008, CVE-2009-0093, CVE-2009-0094
https://technet.microsoft.com/en-us/library/security/ms09-008.aspx

[9] MS12-074, CVE-2012-4776
https://technet.microsoft.com/en-us/library/security/ms12-074.aspx