Bring Your Own Dilemma

OEM Laptops and Windows 10 Issues

Mark Loveless
@simplenomad

Contents

Introduction

With the advent of Bring Your Own Device (BYOD), corporations are allowing end users to connect countless personal, unmanaged devices to the corporate network, including smartphones, tablets and home computers.

BYOD introduces new security risks to corporations.

Most companies assume that if they allow a home laptop to connect to the corporate VPN, they are secure. In many cases, if you only allow browser access from home laptops, it's typically considered safe.

However, without knowing how secure these devices are on any network, how can you ensure your corporate network will be secure once they've connected? A laptop that is easily compromised out of the box can put corporate data at risk, especially if that laptop was used on public Wi-Fi before connecting to your corporate network.

To answer this question, Duo Labs, the security research team of Duo Security, conducted research on seven original equipment manufacturer (OEM) laptops that we had access to and were able to get packet captures from, including:

- Lenovo Flex 3
- HP Envy
- HP Stream x360 (Microsoft Signature Edition)
- HP Stream (UK version)
- Lenovo G50-80 (UK version)
- Acer Aspire F15 (UK version)
- Dell Inspiron 14 (Canada version)

Findings Summary

Things were ugly. Examining the network traffic uncovered a large amount of security and privacy issues - for both Windows 8.1 and Windows 10.

The focus of our research was on home systems accessing multiple networks, including public Wi-Fi and the corporate environment. However, this research also impacts corporate enterprises looking to improve both security and privacy settings for Windows 8.1 and Windows 10.

We found major security and privacy issues for Windows 8.1 and 10

As a reminder, the examination was done on the network traffic only. The main takeaways include:

- Many of the privacy issues found affected all of the laptops. Some were more serious than others, but all laptops had issues.
- Network protocol-related security issues affected all laptops, starting from as soon as the laptop appeared on the network during initial boot.
- After Patch Tuesday updates, many privacy settings that were adjusted were reset to their default settings - without any notification to the end user.

- The OEM Microsoft Signature Edition model, HP Stream x360, was more desirable since it contains less bolted-on and unneeded software. As a result, there was slightly less questionable traffic flowing from the Signature Edition laptop.

There were assumptions made during the analysis:

- Mixed use between a trusted home network and public Wi-Fi with the bulk of the use happening at home, so the laptops are not 100% of the time operating in a hostile public environment. In a 100% public Wi-Fi scenario, all seven laptops would fail. Just saying "bad" doesn't seem strong enough, definitely a fail. It seems that protocols such as WPAD allow for the network hijacking of communications right out of the box.
- Erosion of trust due to certificate handling created additional concerns for the integrity of the Dell. This could change if additional major flaws are found from other vendors, but as it stands at the time of this writing, this applies to Dell.
- The audience for this analysis is a typical IT admin, not the average non-technical consumer. Some of these issues are more easily mitigated than others, the amount of effort required to "fix" all of the issues is more than even your average power user might expect. Most are configuration issues that any computer pro would have no problem adjusting and correcting, but it may be more difficult for the average non-technical consumer.
- There was no examination of what exactly was being transmitted back to Microsoft or any of the OEM vendors (virtually all of this data was encrypted). All parties insist they track things so they can help improve your experience and improve future products, that they do not track personal data and only with your approval, and all say you can opt out. The main thing I was looking for was when this transmission was occurring without my consent, which did indeed happen.

Privacy settings were reset to defaults after Patch Tuesday updates — without notifying users.

In a 100% public Wi-Fi scenario, all seven laptops would fail a security test.

A Note on Methodology

The Windows operating system (OS) has evolved over the years, some traffic has been reduced (server message block (SMB) traffic is the most obvious culprit that seems to have been reined in) but there is still a lot of crap on the wire/wireless.

Within the first few packets on all seven laptops, there were issues. It took awhile to figure them out, as much of the traffic was encrypted and one had to go by server hostname or calling program name, or by reverse-engineering the calling code to find out what was going on.

That being said, there are a ton of network connections and this could make for a lot of looking at code. So the easiest route is to leverage what one can off of just the hostname, or the hostname and traffic when it is unencrypted.

However, throwing a hostname into Google to figure out what it does is not for the impatient. For example, searching the Internet for what www.msftncsi.com was (spoiler: one of many Microsoft-owned domains) turned weird rather quickly. Someone somewhere on the webs had decided that 32 Microsoft hosts were evil and tracking people, and www.msftncsi.com was one of them. This was reposted everywhere.

Additionally, in an attempt to sell questionable software to frightened consumers, many resellers of

various security cleaners, weird firewalls, and other things designed to protect you from spyware and malware used this list of 32 host names to try to drive traffic to their site and sell their wares.

In reality, Microsoft's stock ticker is MSFT, NCSI stands for Network Connectivity Status Indicator, and the www.msftncsi.com website is used to test for connectivity. You know that network connection map in Windows that shows your house and the Internet? Getting through that means the DNS lookup for www.msftncsi.com worked.

Doing the full connection to that website, accessing ncsi.txt and getting back "Microsoft NCSI" means that you are not behind a paywall or needing to register for your free Wi-Fi, and you are 100% connected to the Internet. It's all there in wonderful plaintext, nothing tracking you.

```
GET /ncsi.txt HTTP/1.1
Connection: Close
User-Agent: Microsoft NCSI
Host: www.msftncsi.com

        HTTP/1.1 200 OK
        Content-Length: 14
        Date: Wed, 18 Nov 2015 16:01:11 GMT
        Connection: close
        Content-Type: text/plain
        Cache-Control: max-age=30, must-revalidate

        Microsoft NCSI
```

Figure 1.

See?

Now I am not saying Microsoft isn't trying to track you, but this isn't one of the ways they are doing it. But look at all the work just to explain the NCSI server, which I did because someone will read this, start Googling and point to one of those 20,000 search hits and say how evil msftncsi.com is. If you are worried that Microsoft is still going to track your IP address FOR EVIL PURPOSES while testing your network connection, I could even go so far as to show you how to set up your own NCSI server, but that is complete overkill.

And the NCSI server is but one server out of DOZENS considered evil. Blocking them by hostname is not the smartest way to do things, since you are a Patch Tuesday away from a server name change and your hostname block meaning nothing. Don't expect this to turn into the world's longest explanation of boring and insufferably sad packets ever, because I am going to stick to the premise - point out the major issues, and recommendations will be made so things suck less. You've been warned.

Technical Overview

During the First Two Minutes

During the initial boot of the laptops, there is a process where the user enters in information to help configure the system, including network information. As this is entered in, the laptop starts talking on the network (Figure 2). Immediately the protocol that kicks in is Link-Local Multicast Name Resolution (LLMNR, defined in RFC 4795).

Based on DNS, the service is supposed to provide hostname resolution on the same local network. Remember link-local? Same thing except we're dealing with IPv6 here. Unfortunately it also opens up the Windows laptop to risks in environments where the local network is also a public network, like the free Wi-Fi at the coffee shop.

In addition, the Web Proxy Auto-Discovery (WPAD) protocol also kicks in. The protocol (expired in a 1999 Internet Draft) looks on the local network for a web proxy. Sending out the request, the laptop expects a reply with the information needed to proxy web requests through a proxy server.

The issue with both is that an attacker on the local network (or in the coffee shop) could reply with their own answers, telling unsuspecting victims that the attacker's computer is a specific host or the proxy server, or both. This could allow the attacker to sniff for plaintext authentication or provide fake websites modelled after the real thing to trick users into entering in sensitive information.

An attacker could sniff a target user's computer for plaintext authentication over coffeeshop Wi-Fi.

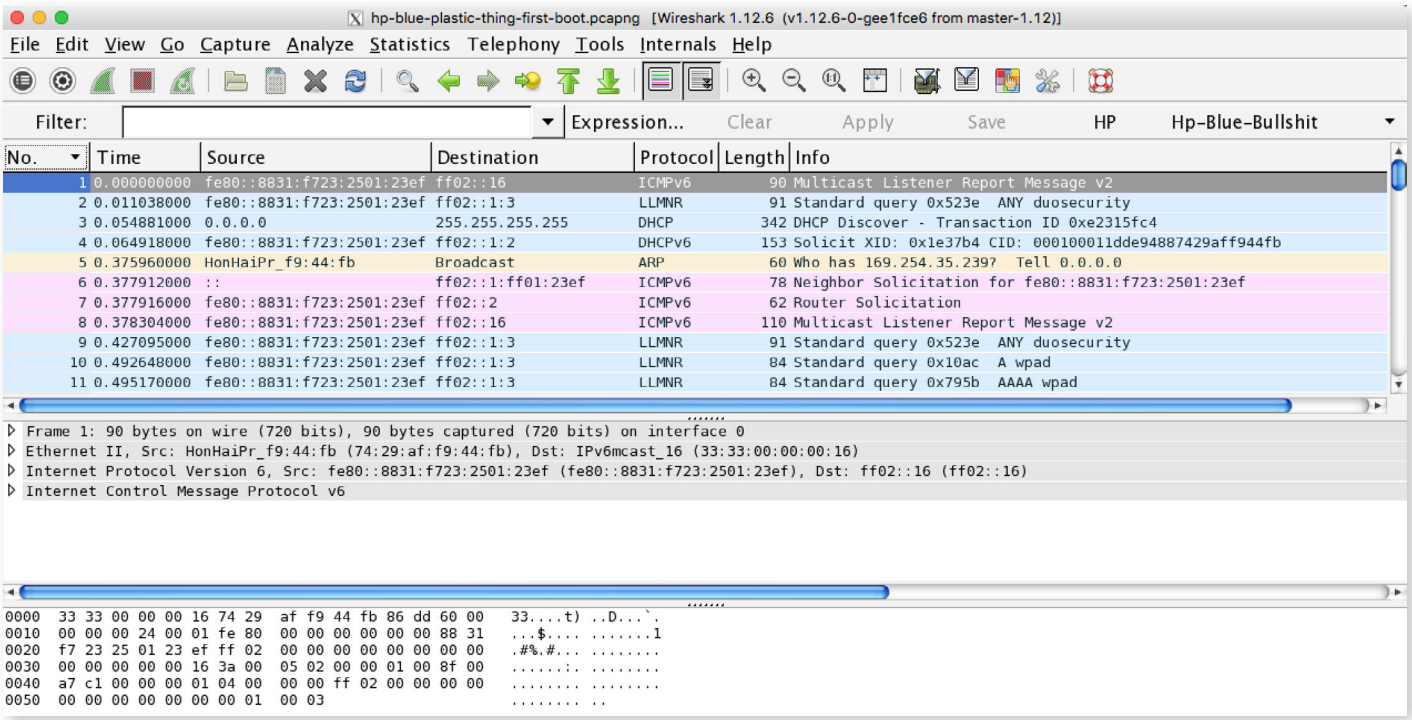


Figure 2.

LLMNR in action during initial boot.

Smart, Multi-Homed Name Resolution

The cynical part of me thinks that whenever you add the name "smart" to something, it is going to lead to something bad. Smart Multi-Homed Name Resolution seems to be one of those technologies. What is it? It is a way in which your computer tries to ensure you get the fastest DNS responses possible, by making queries on all interfaces to all DNS servers it can. This sounds fine on paper, but where things get sketchy is when you start with one DNS server and end up with another. Let me give you an example which should make things clear.

You go to the coffee shop, and you fire up your laptop. The coffee shop's router is the first DNS server you encounter on boot up. Actually it isn't really a DNS server, but it is going to forward DNS queries to the coffee shop's ISP's DNS server. It may not, but odds are the router for that coffee shop is set up like that, because the last thing the coffee shop owner wants is people bitching about the Wi-Fi. Also, this is kind of the default for most SOHO routers just for this reason - make it work as painlessly as possible.

So this becomes your first DNS server, and gets you through your boot process and onto the Internet. You launch your VPN, and work hands you a DNS server to use over your VPN connection. The issue is that with Smart Multi-Homed Name Resolution, is that every DNS query is now going to go to the first DNS server as well as the DNS server the VPN wants you to use.

ISATAP and Teredo Tunneling can allow for man-in-the-middle attacks.

IPv6 in an IPv4 World

We (the world) are running out of IPv4 addresses. With the advent of every new device coming out with an IP stack in the world of "interconnection of every single thing regardless of how stupid it sounds" - also known as the Internet of Things - IPv6 is becoming a reality. To help with the transition, there are several technologies that exist to ease the move from IPv4 to IPv6. Unfortunately, not every one of these technologies is secure.

Teredo tunneling is one of these technologies, which allows for one to use IPv6 by tunneling it over IPv4. This is in case you wish to use IPv6 on your laptop and you connect up to an IPv4 network. The same applies to Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), which does the equivalent of Link-Local for IPv6 in IPv4 environments, and is meant to handle some issues involving router discovery when using a mixed IPv6/IPv4 stack trying to talk to the Internet.

Both of these technologies, if not properly demarced at the network edge, allow for attackers to perform various man-in-the-middle (MITM) attacks against them. If you only plan on using your laptop at home, and you feel confident that your router and your ISP is adequately blocking such technologies, great.

On public Wi-Fi, attackers can easily fingerprint victim laptops, finding OS, browsers, third-party apps, and even patch levels.

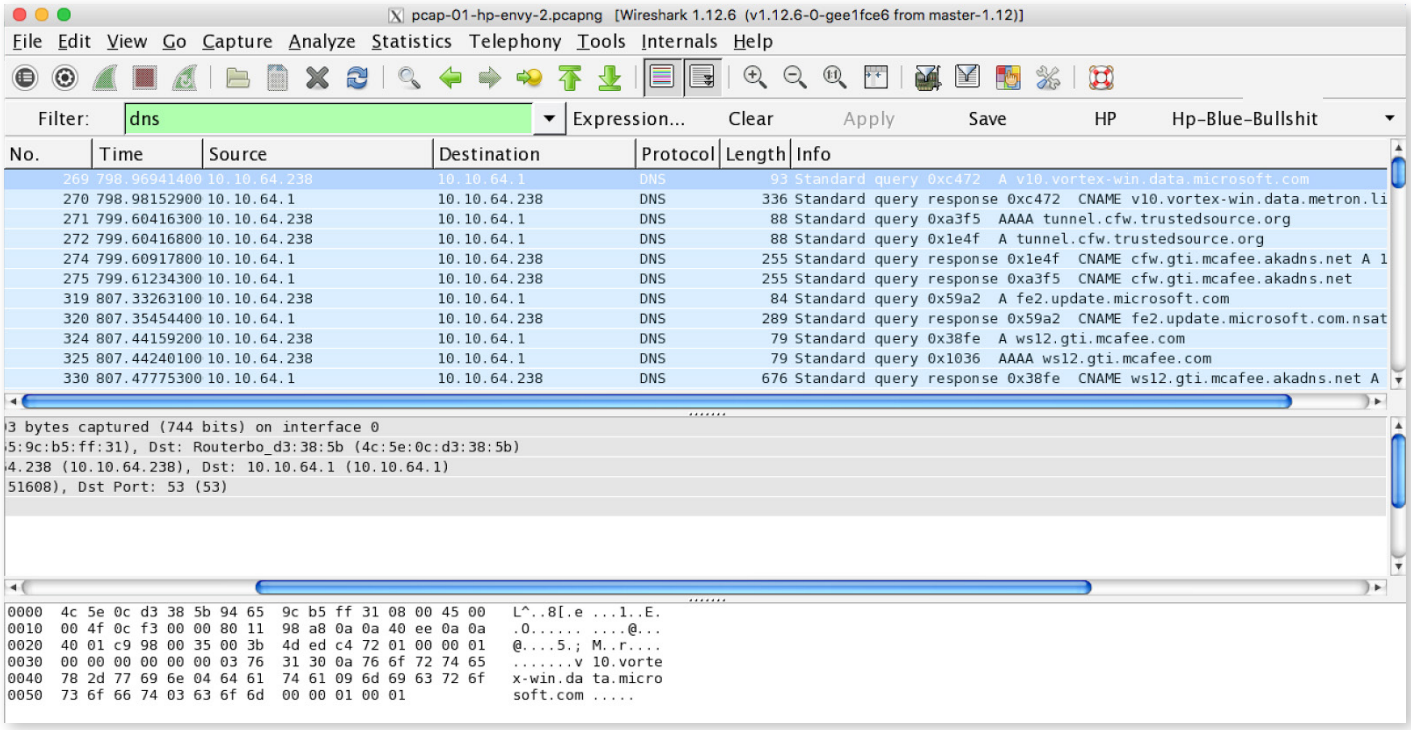
Remote OS Fingerprinting

In the old days, an attacker would have to go to great lengths to determine the OS of the remote computer, performing remote scans on the target computer to try and determine the exact attack surface before launching a specific attack - the fingerprinting of the target system is still an important part of the attack model.

But now, armed with a sniffer and a world filled with free Wi-Fi (coffee shops, hotel lobbies, restaurants, even hospital waiting rooms, the list goes on) an attacker can easily find a target and identify the OS of the potential victim computer. Aside from the OS, it is rather easy to determine information such as the browser of choice (and its patch level), third-party apps, and even the patch level of the system.

It was trivial to watch the traffic and determine the major OS version of all OEM laptops. By specifically phoning home to various Microsoft websites, including some with names that included v8 or v10 in the host names, it was obvious which systems were Windows 8 and Windows 10.

It was also trivial to determine which laptops were which. When we did our first boot packet captures, we were doing them three and four at a time, and it was easy to go back and separate things out by OEM manufacturer. HP systems talked to HP servers, Dell talked to Dell servers and so on.



This was before web surfing or even VPN connectivity occurred. Once general web surfing started, it was easy to watch User Agents and complete the picture of what browser was used, including browser version and even patch level.

Figure 3.

Various DNS requests for Microsoft and McAfee servers.

Patches and Phoning Home

Fortunately, the Windows systems are configured to go out and get operating system patches immediately, so once you get network connectivity, it doesn't take long to get the OEM laptop up to an acceptable patch level. Unfortunately, these systems also start phoning home for other reasons as well, such as to ensure that user data they've gathered about "customer experience" are uploaded.

Windows 10 has a lot of traffic heading out the door, and if Windows 8.1 didn't have enough before, one of the first downloads it retrieves from Microsoft is something to get Windows 10 onto the laptop. There have been a lot of sites reporting on Windows 10 privacy concerns, so I won't rehash that information here (however, the instructions at the end of this report do cover turning things off).

However, both Windows 8.1 and 10 start making contact with watson.telemetry.microsoft.com, which is a Windows Error Reporting (WER) server. The purpose of WER is to gather, handle, and process uploading of crash dump data, although there is communication from the first boot independent of any crash.

The same could be said about the Device Metadata (DMD) services. You know when you configure a new printer for the first time, it has to configure the driver? By default, it will check the local system, and then if it can't find the exact driver, it will hit the Internet and ask a Microsoft-owned server if it knows anything about the proper driver. But out of the box, there were posts to Microsoft DMD servers by all seven laptops without any hardware being added, meaning that Microsoft was learning about what was on the local system.

Some of the third-party applications, such as Lenovo's "Lenovo Customer Feedback Program" and "Lenovo Experience Improvement" gather data and upload it to Lenovo servers. Each OEM vendor uploaded some data of some sort.

Is the customer data at least secure in transit while being uploaded? Not in all cases. It seems the OEM vendor-specific apps mostly use encryption in the form of HTTPS, but Microsoft does a portion of their uploads in plaintext.

What about those updates? When those updates are being downloaded to your laptop, now those are encrypted, right? No, those are downloaded in plaintext. The reason has to do with being able to cache responses, in that the various vendors would prefer not to waste bandwidth and take advantage of the caching of plaintext HTTP.

To ensure that evil hackers did not MITM and supply their own patches with built-in badness, the updates are digitally signed. And while downloads of things like Certificate Revocation Lists from the major cert sites (and the OEM vendors themselves) all take place in plaintext HTTP (again, caching), as long as the main certificates that were pre-installed, they can update and work fairly securely. Granted, if you are a vendor and you lose your keys, you have issues.

Now one can actually download things via HTTPS if one wants, like Lenovo does here:

```
GET /pccbbs/thinkvantage_en/metroapps/Metrics/v2/Update2.xml HTTP/1.1
Host: download.lenovo.com
Cache-Control: max-age=0
Pragma: no-cache
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Server: AkamaiGHost
Content-Length: 0
Location: https://download.lenovo.com/pccbbs/thinkvantage_en/metroapps/
Metrics/v2/Update2.xml
Date: Thu, 29 Oct 2015 19:28:53 GMT
Connection: keep-alive
```

Figure 4.

Lenovo does an encrypted download via a 301 to an HTTPS server.

This doesn't address the caching issue, but Lenovo does this once after every boot-up and checks for any updates that way.

A Note on live.com

During the installation process, you are asked to create a live.com account. If you do, you will have a lot of communication with live.com, including uploads of various forms of data. We did not look into this data with any level of seriousness, specifically because you could skip the creation of your live.com account completely.

During initial boot, I did sign up the Lenovo with Len Ovo and gave Len an email account on a mail server, but there was so much communication between the laptop and the live.com servers and I really didn't want to deal with seven separate email accounts for these laptops, so as the Duo Labs team were firing up the laptops everyone was clicking on "Skip" (it is in very small letters, but it is there) during the initial boot when it came time to sign up for a live.com account.

A number of things were stopped with this - the upload of the encryption key for recovery of your laptop's encrypt data was stopped (this has recent become a thing apparently), weird plaintext MSMQ uploads and other communication, and so on. Our laziness in maintaining email and avoiding extra screens during setup made these systems more secure and most certainly improved privacy.

By the way, nothing seems to have stopped working nor is the Windows experience any less. Things work just fine without the live.com account.

Third Party Fun

With the exception of the HP Stream x360, all laptops were loaded with McAfee's antivirus program. This was apparent at boot time and the McAfee software phoned home for updates.

Port scans were done, just to see what was being offered up by the OEM laptops. All exposed high-numbered ports that were found identified to NMap as Microsoft Windows RPC, all were in the 49000 range although this varied slightly laptop to laptop. For example, the Lenovo Flex 3 had TCP ports 49408 through 49413 open, all serving up Windows RPC.

Again with the exception of the HP Stream x360, all laptops had port 6646 open on then. This was determined to be the McAfee antivirus software's network agent. This port was only open for a few minutes after boot, but definitely remained open and allowed connections during that time.

```
PORT      STATE SERVICE      REASON  VERSION
135/tcp  open  msrpc        syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack Microsoft Windows 98 netbios-ssn
445/tcp  open  microsoft-ds syn-ack (primary domain: WORKGROUP)
554/tcp  open  rtsp?        syn-ack
2869/tcp  open  http        syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6646/tcp  open  unknown      syn-ack
10243/tcp open  http        syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49156/tcp open  msrpc        syn-ack Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the follow-
ing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port445-TCP:V=6.49BETA5%I=7%D=11/19%Time=564DFB64%P=x86_64-apple-darwin
SF:13.4.0%r(SMBProgNeg,6F,"\0\0\0k\xffSMBr\0\0\0\0\x88\x01@\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0@\x06\0\0\x01\0\x11\x07\0\x03\n\0\x01\0\x04\x11\0\0\0\0\x0
SF:1\0\0\0\0\0\xfc\xe3\x01\0\x17\x1cZ\xee\xe8\"\xd1\x01h\x01\x08&\0\x18\xb
SF:5\0\xc2<\xba\x1f\nW\0O\0R\0K\0G\0R\0O\0U\0P\0\0\0D\0E\0L\0L\0\0\0");
Service Info: Host: DELL; OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:win-
dows_98
```

There are several firewall options depending on how one connects to a network, and what software you are running (such as McAfee). A network can be either "public" or "local", as in untrusted or trusted.

Figure 5.

Dell with the firewall set for a trusted network. Eww.

Normally, Windows leaves open the usual connectivity ports (TCP 135, 139, 445) to allow for basic connectivity, which for Microsoft means "file and printer connectivity." This is not actually required, and due to the fact that these ports allow for numerous probes and attacks, they should be blocked. Third-party software from the OEMs also created issues by opening up additional ports, as the Dell did above in Figure 5.

In "local" or "home" or "work" mode (the place where you have at least some level of trust in your environment) more ports are exposed for connectivity. In "public" mode, such as free Wi-Fi at the coffee shop or restaurant, or even fee-based Wi-Fi like on an airplane, less ports are exposed. Ports are still exposed, regardless.

Odd Websites

For the most part, looking at the various hosts that the OEM laptops connected to during bootup and idle time, websites fell into three categories - Microsoft-related, OEM vendor-related, and certificate-related. Anything outside of that certainly stood out. As most of the laptops had McAfee installed on them, there was, in essence, a fourth category comprised of just McAfee hosts.

While most odd websites could be explained as what I would call "tile fodder" to fill up those Windows 8/Windows 10 tiles (e.g. www.amazon.com), one that definitely stood out was a call to tags.tiqcdn.com.

This server is owned by Tealium, which is a company that does tag management. What is tag management? It is the management of tags, where tags are pieces of code placed on a web server that allow for tracking and analysis. Now normally you will encounter tags during normal surfing, and you will end up downloading tags from numerous tag vendors such as Tealium, Google and many others.

Some calls to tag servers are to download Javascript (the main implementation method of tags) for the sole purpose of serving up ads. There are plenty of examples of this happening with Windows tiles, even while idling. But the tag server accesses to Tealium's servers were different, and these were all coming from the laptops with McAfee software loaded onto them. Here's a typical GET and the reply (minus the compressed data):

```
GET /utag/mcafee/consumer-main/prod/utag.js HTTP/1.1
Accept: */*
Referer: http://home.mcafee.com/root/campaign.aspx?cid=127067&contex-
t=10&event=6&guid=d1a45e30-6fdb-4121-afdc-673b2a9e28bb&lcid=1033&ser-
vicetag=GDQCJ52&affid=105-1746&wuiv=11.0&ctst=1
Accept-Language: en-US
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; Win64;
x64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; .NET CLR
2.0.50727; .NET CLR 3.0.30729; McAfee)
Host: tags.tiqcdn.com
Connection: Keep-Alive

        HTTP/1.1 200 OK
        Content-Encoding: gzip
        Accept-Ranges: bytes
        Cache-Control: max-age=300
        Content-Type: text/javascript
        Date: Thu, 19 Nov 2015 22:16:21 GMT
        Etag: "843569594+gzip"
        Expires: Thu, 19 Nov 2015 22:21:21 GMT
        Last-Modified: Wed, 18 Nov 2015 18:41:38 GMT
        Server: ECS (mdw/13C1)
        Vary: Accept-Encoding
        X-Cache: HIT
        Content-Length: 15164
```

Figure 6.

Typical call to Tealium server, note the Referer in the request.

Tags allow for management of cookies, tracking a browser/computer/user across time and space for marketing purposes, helping a vendor comply with "Do Not Track" settings in browsers, allow for the management of content such as new product offerings based upon numerous factors including time (like the first 30 days of a trial that starts after you power on your computer for the first time).

Now take a good look at the Referer header in the GET request above. Odds are that McAfee is mainly using tags for the latter, but as I could find no documentation anywhere about how they are actually using it, I am assuming they are gathering at least some data from users. Other tag server requests simply downloaded Javascript without Referers, and actually were used to serve up ads inside tiles. Considering how Bing is used with those tiles serving up info, finding ads in your OEM laptop should pose no surprise anyway.

Real-World Security Implications

Link-Local

Link-local is an older protocol. In basic terms, it allows for a network interface to "self-configure" an IP address when other methods are absent (such as DHCP) or have simply failed (unable to read a config file). The protocol's packets are not passed by routers, so link-local packets and the addressing scheme stays on the local network segment. Since the protocol was introduced in 1999 before the advent of wireless, having link-local on your home network was fine.

However, when a wireless network interface is introduced, the local network segment is now confined by how powerful the wireless network interface actually is. This means that an attacker could conceivably start manipulating the wireless "local network" as they see fit - introduce a rogue DHCP and DNS server, and convince the victim's computer that they are the victim's mail server, bank, or anything else in an attempt to trick the victim into revealing credentials.

An attacker could manipulate a local network and convince a victim to reveal their credentials.

What is Bad About WPAD and LLMNR?

WPAD is really trying to make things easier for the end user. One common thing for the computer to ask is "where is the web proxy so web browsing will work?" WPAD is the one that asks the question and fields the answer. The issue - much more prevalent for wireless - is that anyone nearby could provide that answer, even when no proxy is required.

The attacker could tell the victim that they are the web proxy, so that all web requests from the victim are routed to the attacker first, subject to reading of plaintext, downgrading encryption, insertion of HTML on the fly, and any number of additional attacks. LLMNR is the IPv6 version of link-local, and as we mentioned previously an attacker could answer some of those important questions the victim computer is asking, allowing for the manipulation of traffic to the attacker's advantage.

An attacker could route web requests from the victim to the attacker, allowing them to read personal info in plaintext.

What's Wrong With Smart Multi-Homed Name Resolution?

When it comes to DNS servers, obviously the fastest server is desirable as this ever so slightly improves things like web browsing performance. Smart Multi-Homed Name Resolution remembers what DNS server is the quickest. You connect up to the Wi-Fi at the coffee shop, the DNS for the coffee shop is deemed the fastest (probably by default), and then you connect up to the VPN at work. Sure, your DNS requests are now going over the VPN, but a copy of the requests are still being sent to that coffee shop DNS, leaking DNS queries to the coffee shop's ISP, or to anyone else in the coffee shop sniffing the Wi-Fi.

This means an attacker could have the names of your company's internal hosts at the bare minimum — heaven forbid the attacker starts forging replies. If dual-homing is not enforced or if the VPN software doesn't know how to handle this, this becomes a massive security risk.

What's the Deal With Teredo Tunneling and ISATAP?

Teredo Tunneling and ISATAP are both technologies that build upon the same territory laid down by our friend link-local. Both are intended to help the computer operate IPv6 in IPv4-only and IPv4/IPv6 mixed environments respectively. However, if you plan on taking your new laptop to the coffee shop (or any other place with free Wi-Fi), there is an inherent danger of MITM attacks - with the same consequences as the ones associated with LLMNR and WPAD we previously discussed.

If you're not using something, you should disable or uninstall it.

The technologies ask questions about the environment around them, and in a wireless environment any attacker within physical range can provide crafted answers that allow the attacker to route and manipulate the traffic to their advantage. In basic computer security terms, if you are not using something, you should disable or uninstall it. If you are not using IPv6, or if you are exclusively using IPv6, you do not need these transitional networking technologies which are considered temporary anyway.

What Can These Issues Lead To?

As previously stated, most of these scenarios involve some service asking a question and trusting the answer - regardless of where the answer comes from. Some of these issues taken individually are not 100% guaranteed to lead to instant compromise, but these can be combined with each other and additional techniques to compromise victim operating systems or steal credentials. Coupled with simple sniffing just to see what the victim's computer is putting out there on the wireless, a coffee shop attacker could get a fairly clear picture about what the user is generally looking at, even when traffic is encrypted.

Attackers may target hotels or coffee shops near conference venues to find potential victims.

While a coffee shop attack might seem far-fetched, an attacker who targets specific companies could be hanging out at coffee shops, restaurants, or hotel lobbies near the target in the hopes of finding employees. For the convention attendee for a specific industry, hanging out at hotels or coffee shops near the convention also may be an easy way for the determined attacker to find victims.

Implications and Mitigations

Any of these issues alone are not serious - concerning yes, but not serious. The reason these network issues become serious is when you start compounding things by combining issues. The MITM issues with WPAD, LLMNR, Teredo, and ISATAP give attackers a choice in how to MITM, and when you consider how well people like Dell are handling certificates you start realizing that those uploads, and more importantly the downloads of patches, updates, and revisions that require absolute trust are hanging in the balance, security concerns become security seriousness very quickly.

The combination of multiple network issues results in serious security concerns.

If we were grading on annoyance only, every system with McAfee on it would be deemed as a complete fail. Numerous times the software reminds you that your free trial is coming to an end, you will be subject to an unsafe world with massively bad things ready to happen, so sign up NOW. It has its pluses and minuses, being that given the option of antivirus versus no antivirus I'd pick antivirus (especially if I was gifting an OEM laptop running Windows to a relative), but one could just as easily uninstall McAfee and rely on Windows Defender and call it a day. In fact, I am advocating just that.

If grading on annoyance only, every system with McAfee would be deemed a complete fail.

And speaking of making changes, here is what you can do to improve things and make the laptops a little safer:

- During installation, bypass/skip the signups for a live.com account. They are not required.
- LLMNR, Smart Multi-Homed Name Resolution, WPAD, Teredo tunneling, and ISATAP need to be disabled.
- Microsoft Windows systems settings need to be adjusted to prevent customer experience data from being reported back to Microsoft.
- A number of OEM applications - especially those whose sole purpose is to upload customer stats and other telemetry data - need to be reconfigured or completely uninstalled.
- If you have a McAfee trial version of their antivirus software, just uninstall it and rely upon Windows Defender. This may horrify many security professionals, but consider that by most estimates Windows Defender will catch 95% of the common stuff and 85% of the zero day, (McAfee gets near 100% in both categories), and depending on how you use your new laptop, that may be an acceptable risk. Windows Defender is also included with Windows 10, so it is free. McAfee's use of Tealium's tag technology brings into question what information McAfee is tracking on its users - certainly enough to try and get you to purchase their products and services.
- Adjustments to the firewall to ensure no services are exposed to the network.

This is a lot of effort, so we've included the various steps in a little more detail in the Detailed Mitigation Instructions section below. This is still far from perfect, but a significant improvement for most of the laptops anyway. Even with these steps I would not give any of these laptops an A+ on the network.

If you are a computer guy handing out laptop gifts, I'd advise just doing all this yourself (and patch things up of course) before wrapping it up and handing it to that non-technical friend or loved one on your list. Just make sure they change the password you created for them!

Conclusion

These laptops out of the box from a networking standpoint are not ready for prime time. With the exception of the HP Stream x360 that is "classic" non-OEM software Windows being OK, everything else is bad. None of them are ready for the rough world of a public network. With some deletion of certain software and reconfiguration they will fair much better than your average laptop, although this is still no guarantee of absolute laptop safety. You still have to keep up your patches, and after every patch cycle it might not hurt to at least recheck Privacy settings.

Out of the box, these laptops are not ready for prime time.

The Microsoft Signature Edition laptops are definitely a step up. Less OEM bloat means less annoyance and a reduced attack surface, although straight out of the box they are still less than ideal.

Detailed Mitigation Instructions

These instructions assume a working knowledge of Windows, in that you will be editing things in the Registry, mucking about with Services, and so on. These instructions are for both Windows 8 and Windows 10, with the differences noted. As stated before, one could block those 32 hosts or whatever the number is now, and then just hope Microsoft never changes or renames anything. Or you could turn off the service or feature that is talking to those servers, and just stop the behavior completely. These instructions do that.

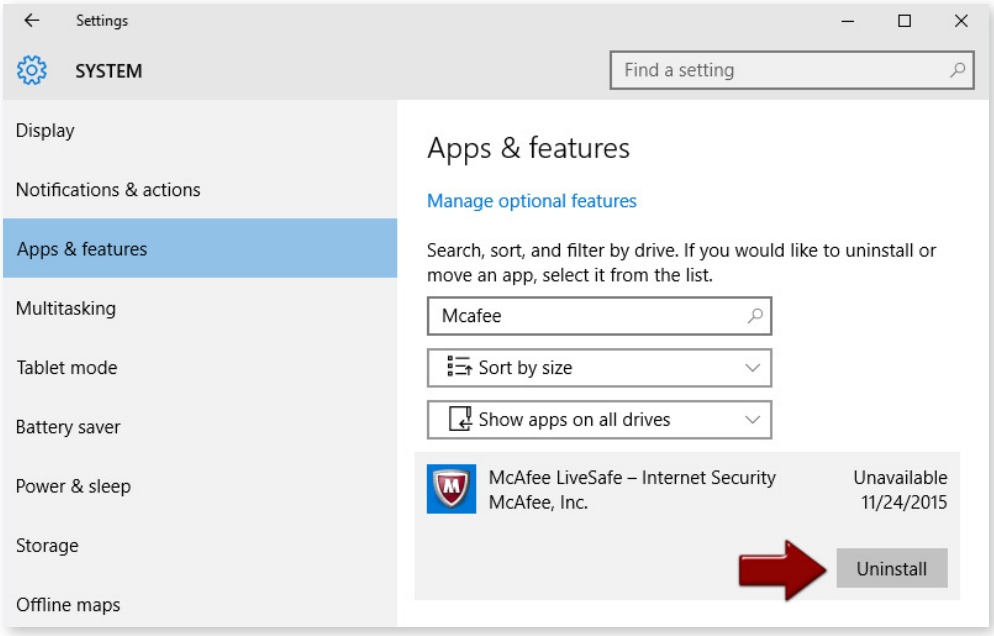
NOTE: A few times a year Microsoft releases a cumulative update. These will typically include security patches, new features being added to existing apps, and so on. After one of these updates, recheck your settings.

For example, after KB 3116900 a few privacy settings involving Mail and Calendar, as well as "Sync with devices" was turned back on. A few other things, such as WPAD and some of the Diagnostics Tracking were turned back on as well. Basically after major patches from Microsoft, you will want to revisit the steps below. And certainly if you upgrade to Windows 10 from Windows 8, you will definitely want to go over things.

Basic Settings

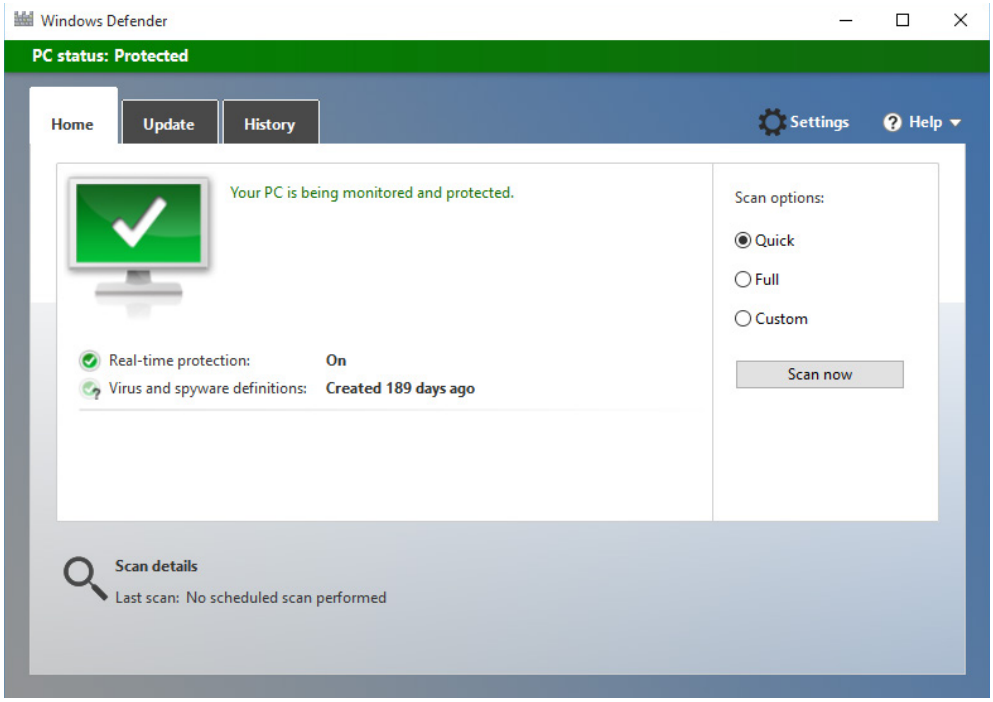
1. Remove McAfee and set up Windows Defender

First things first, for those non-Microsoft Signature Edition computers, delete McAfee. On the search bar type in Settings, launch the desktop app, click on System, and click on Apps & features. In the "Type an app name..." start typing McAfee until you see the app appear. Click on it and click on Uninstall.

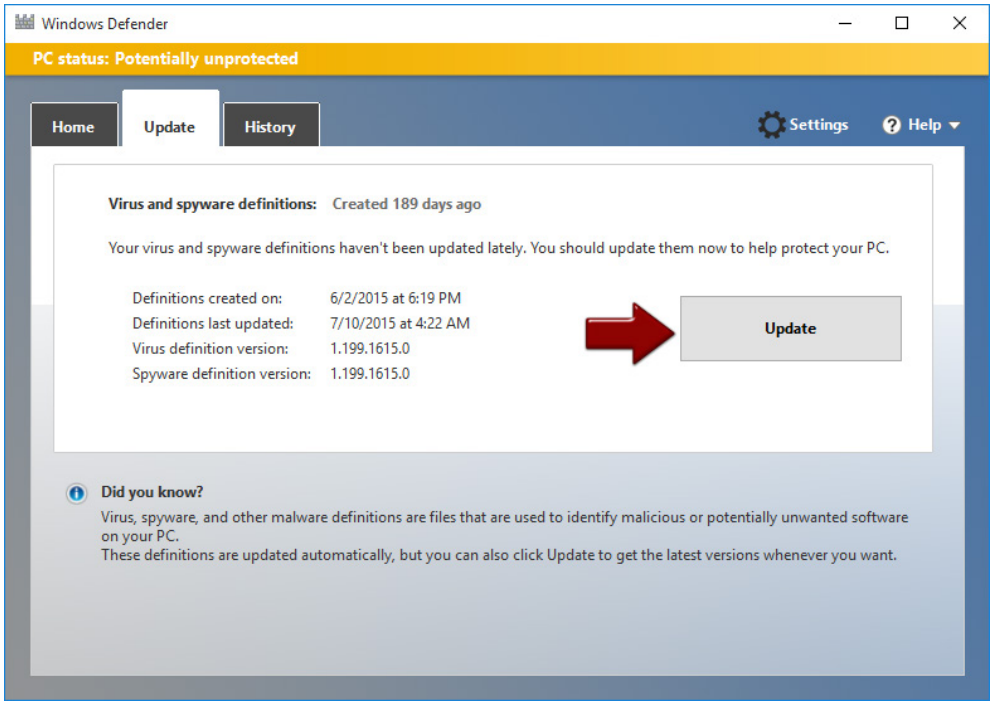


You will get a window asking if you wish to proceed. You want to make sure you uninstall all files, this should get the registry settings as well. We need those registry settings freed up so we can work on other things later on.

After installation, there will be a little warning window that appears at the bottom of the screen and says you are without antivirus and you need to use Windows Defender. Click on it, and Windows Defender will come up and fairly quickly turn green.



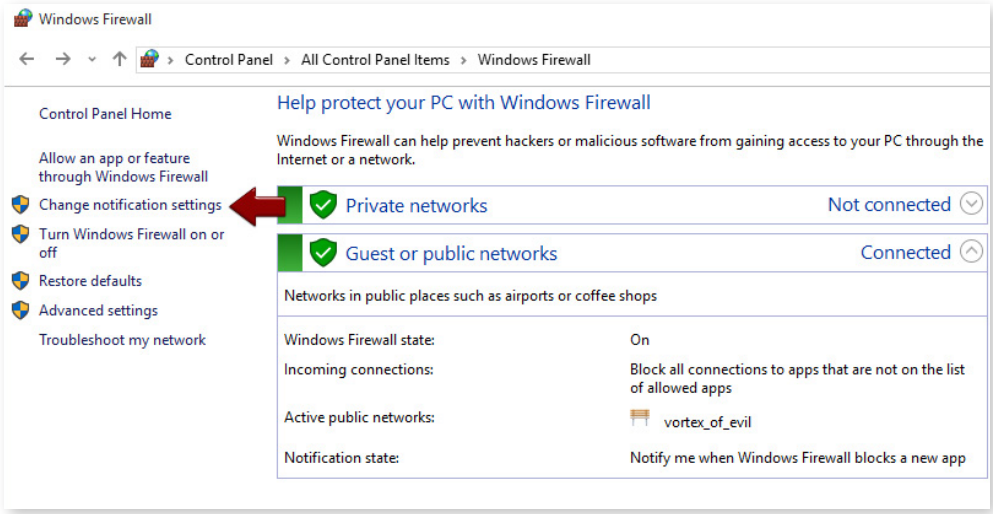
It may turn Yellow and state you have not run a scan on your PC for a while. Before you run a scan though, click on the Update tab then click on the Update button.



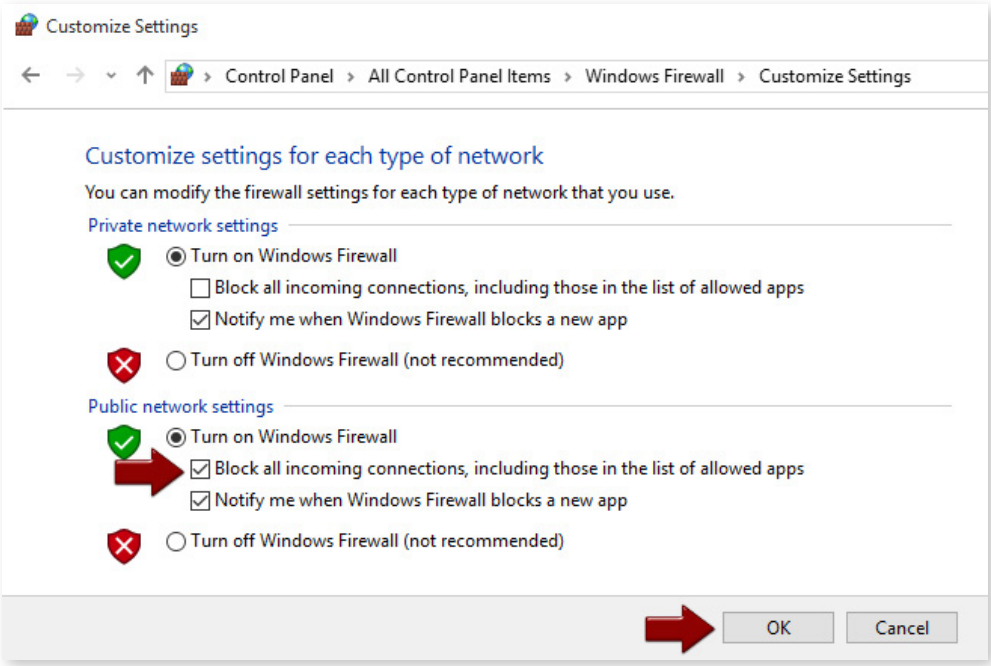
Now you can run a scan if you wish, but it will happen automatically going forward. At the end of the uninstall process, you will need to restart your computer. Do so.

2. Adjust the firewall

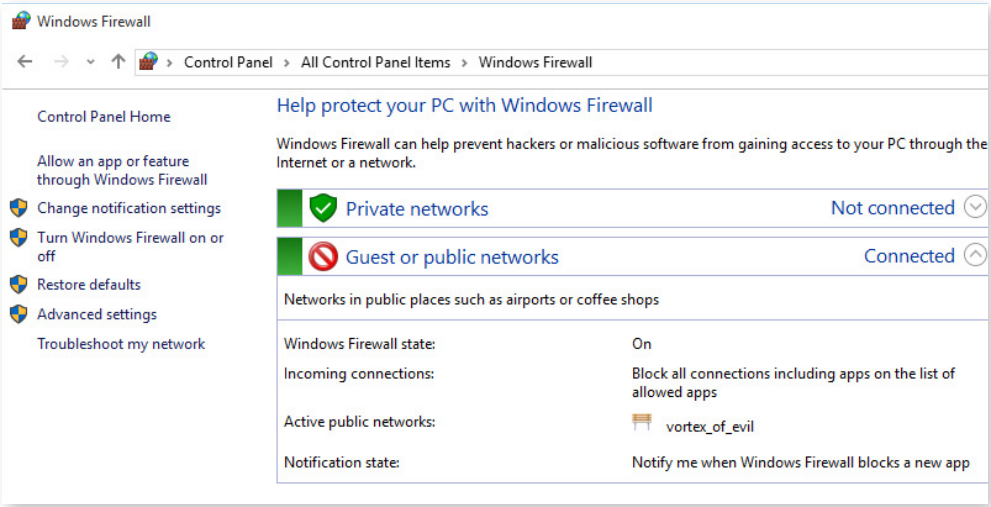
I am assuming you have already uninstalled McAfee, which, if still installed, will inhibit you from performing these tasks, so don't skip it. To access the firewall, right-click on the Start icon and select Control Panel. The Windows Firewall will be near the bottom. Double-click on it and you are in:



On the left side, you will see “Change notification settings.” Click on it. Under Public network settings, check the box next to “Block all incoming connections, including those in the list of allowed app” then click OK:



Now the firewall screen has changed with a nice big red circle with a line through it next to Guest or public networks:



That’s it! Reboot and enjoy how many 1’s and 0’s you are no longer transmitting.

3. Adjust privacy settings

The steps here are simple but tedious. In Windows 8, right click on the Start button, click on search and type in "PC Settings" in the search bar, and launch PC Settings. In Windows 10, go to Settings. Click on Privacy. In Windows 8, there will be five screens to go through.

In Windows 10, there will be a total of thirteen screens. As you go through each screen, turn everything off that bothers you. If there's any doubt turn it off. Personally, I'd just turn everything off or set it to disabled, then open things back up as you use your apps and decide you need certain things.

4. Disable and delete OEM apps that gather data

This is going to vary per OEM vendor, you should be able to search the OEM's website and find instructions for opting out of data gathering. Lenovo has a web page that details the steps for disabling and deleting their to prevent products.

On the plus side, Lenovo were the only ones at the time of this writing that offered up anything on their website that was easy to find. I spent less than five minutes using the OEM vendor's website and Google to find vendor-provided info, and Lenovo's instructions were on the first page of Google search results.

I could find nothing for HP, Dell, and Acer except non-comforting statements about cookies and web bugs (PR firms call them "Web Beacons" because that sounds less evil). All admitted they gather data, only Lenovo provided some level of opting out. On the minus side, the Lenovo stuff on the website was out of date, and not all of the various Lenovo apps from this document were actually installed. Names were slightly changed as well, but usually something close.

The best advice I can give you is to look through the various OEM apps, clicking on every button and turning off every feature that remotely suggests it will phone home or gather data. The more advanced user may want to poke around in Task Scheduler and Services, similar to what is in the more advanced steps below.

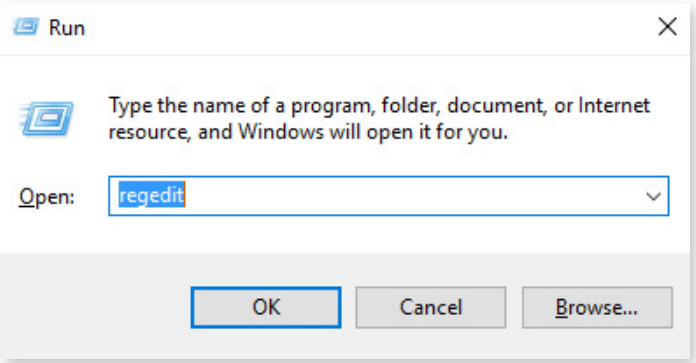
If you are sufficiently skilled at sniffing and looking at the data, fire up a sniffer to check your work. Google searches are a mixed bag at being helpful as they are often outdated, inaccurate, and laden with the opinions of many that point in every direction - but it is possible to find out information about some of these OEM apps via searches. Kind of like all of the Windows stuff.

Advanced Settings

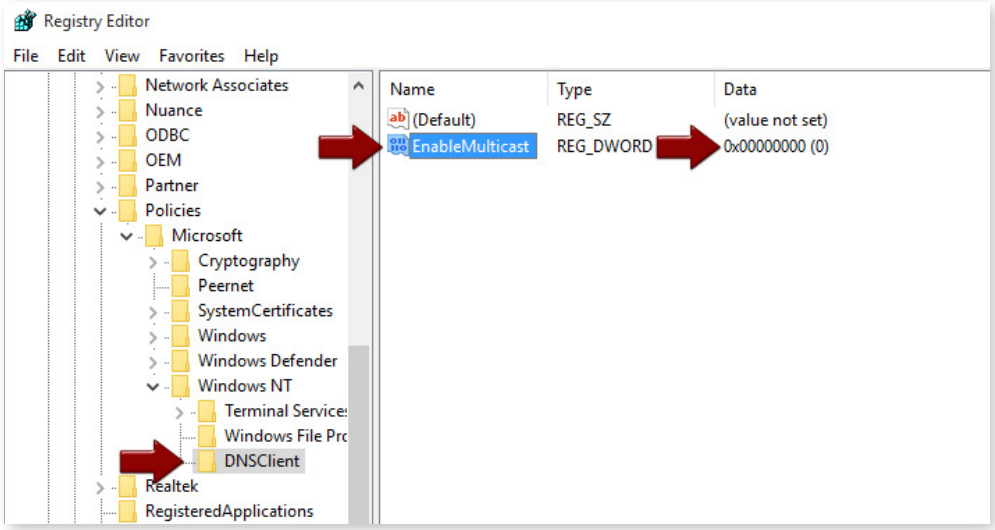
Ok, time to plow ahead and get your hands dirty.

5. Disable LLMNR

Normally, if you were going to disable LLMNR, you would do it with the Group Policy Editor, however the OEM laptops are running the Home Edition and that isn't an option, so we'll have to edit the appropriate registry settings to make this work. Hold down the Windows key and press R (for Run). Type in regedit and hit enter:

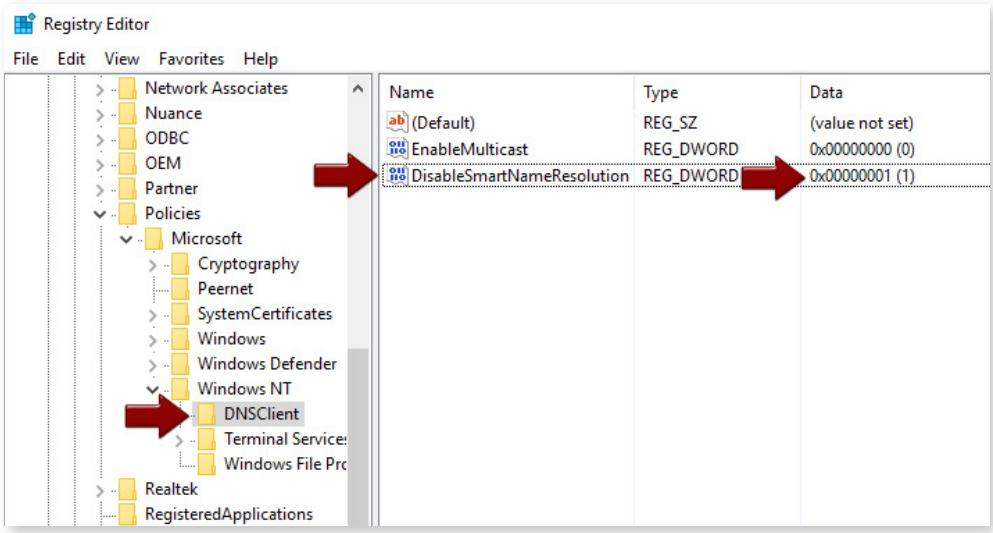


You will need to navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT. Create a new key named DNSClient (assuming it is not there), and inside this new key create a new DWORD called EnableMulticast. The default value for this will be zero, so leave it that way:

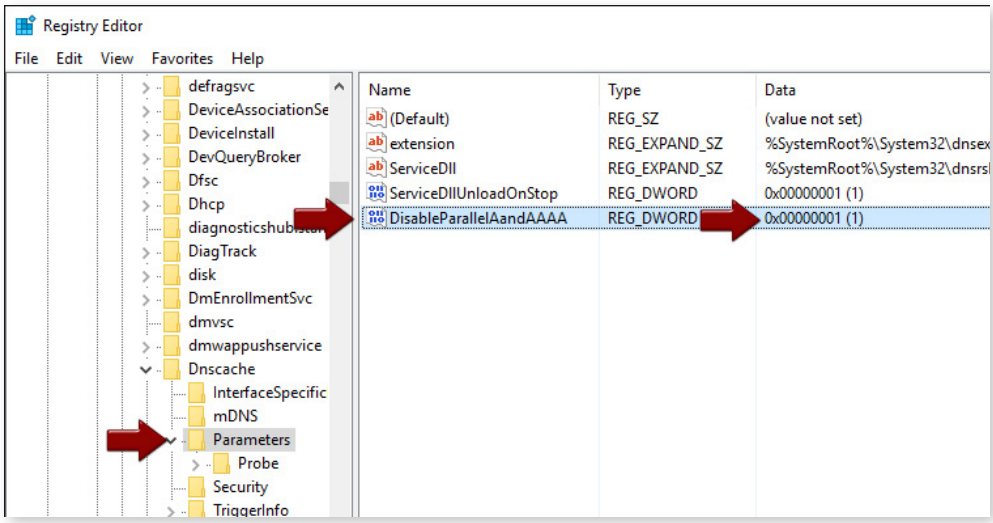


6. Disable Smart Multi-Homed Name Resolution

This is done via a registry entry. Launch regedit (hold down the Windows key, press R, type regedit and then enter), navigate to HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient and create a DWORD called DisableSmartNameResolution. Give it a value of one:



With Windows 10, you need to do one additional entry (Smart Multi-Homed Name Resolution was heavily rewritten for Windows 10). Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters and create a DWORD called DisableParallelAandAAAA. Give it a value of one:

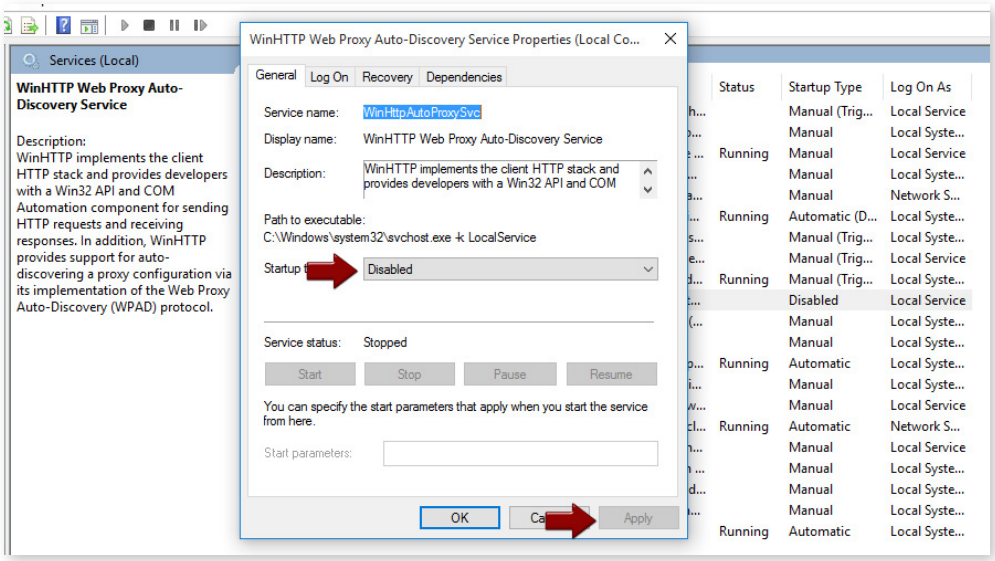


7. Disable WPAD

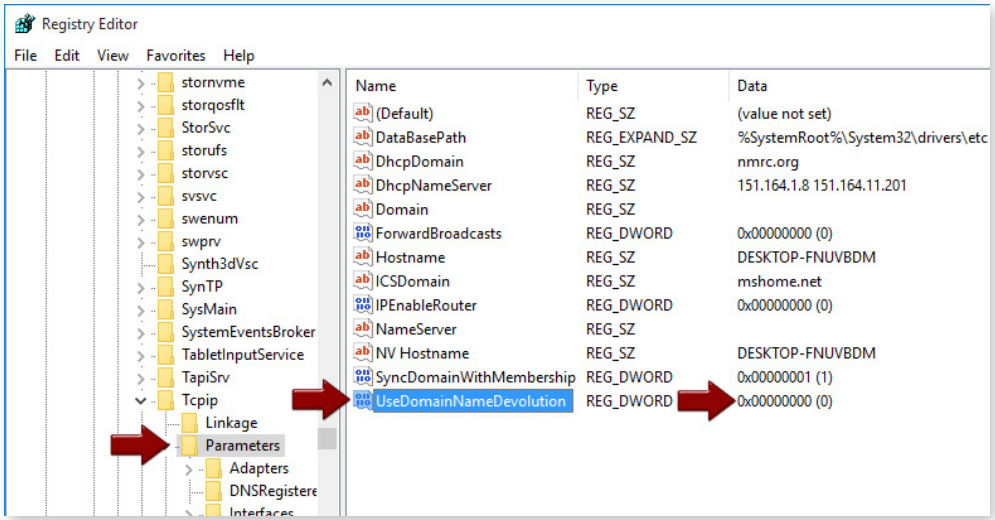
Hold down the Windows key and press X. Select “Command Prompt (Admin).” Issue the following command on a command line:

```
netsh winhttp reset proxy
```

Type in Services in the search bar and launch the Services desktop app. Find WinHTTP Web Proxy Auto-Discovery Service and stop it. Now right-click on it and select Properties. Halfway down on the General tab, set the Startup type to “Disabled.” Click on Apply at the bottom, then click OK.



More Regedit fun. Open regedit (you probably have this shortcut memorized now from above) and navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, and create a DWORD under the Parameters key called UseDomainNameDevolution. Leave it at zero:



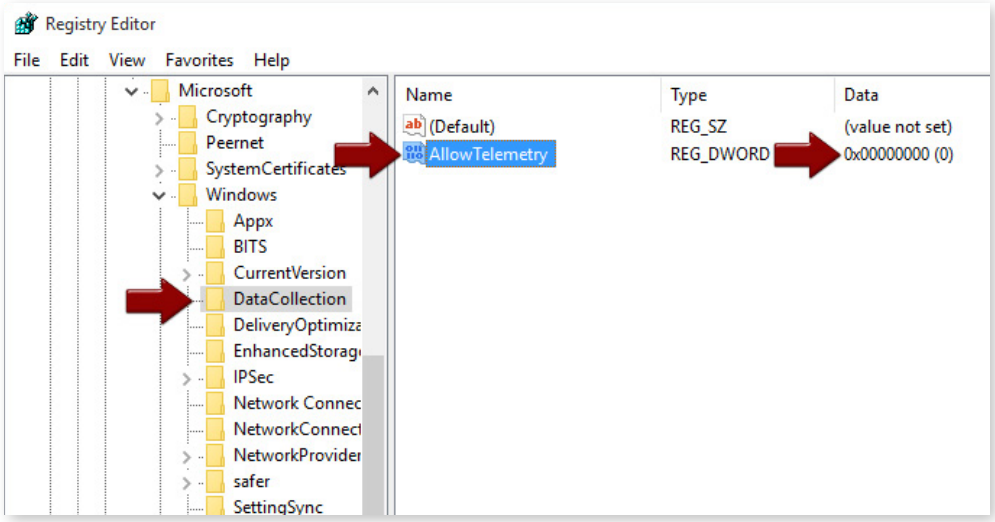
8. Disable Teredo tunneling and ISATAP

Hold down the Windows key and press X. Select "Command Prompt (Admin)." Issue the following command on a command line:

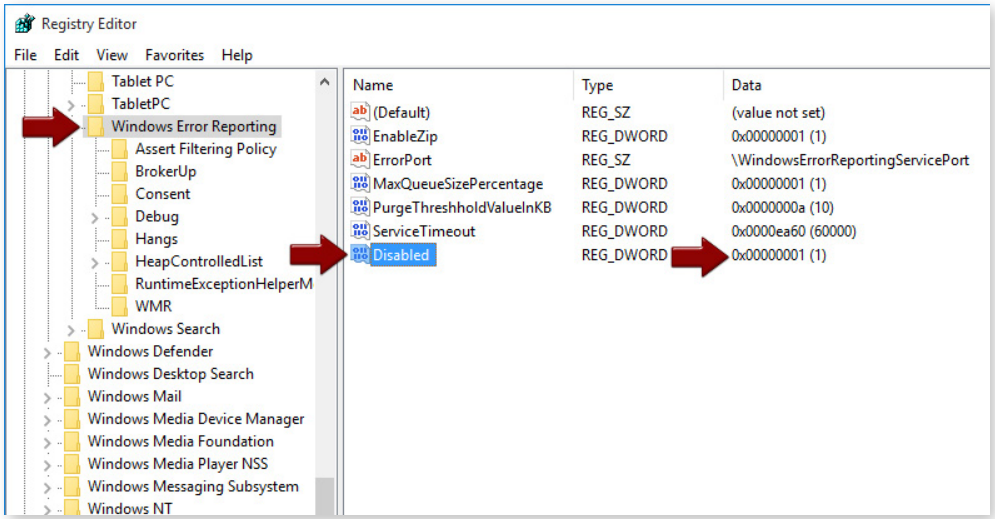
```
netsh interface teredo set state disabled
netsh interface isatap set state disabled
```

9. A Few More Privacy Settings

You'll still need to do some low-level adjustments. For Windows 10 launch regedit, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection, and create a DWORD called AllowTelemetry. Leave it at zero:

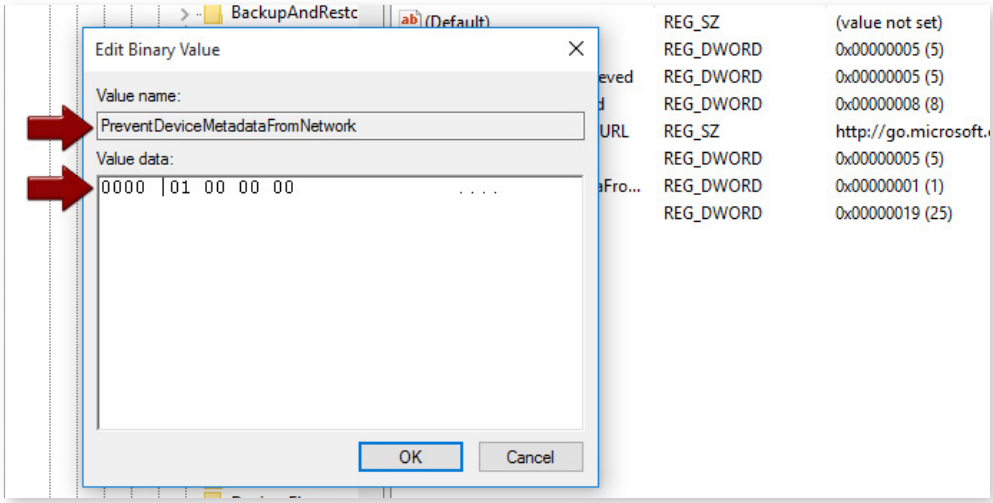


While in the registry, to disable Windows Error Reporting, you will also need to navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting. If there is a DWORD called Disabled, make sure it is set to one. If it isn't there, create it, and of course set it to one:



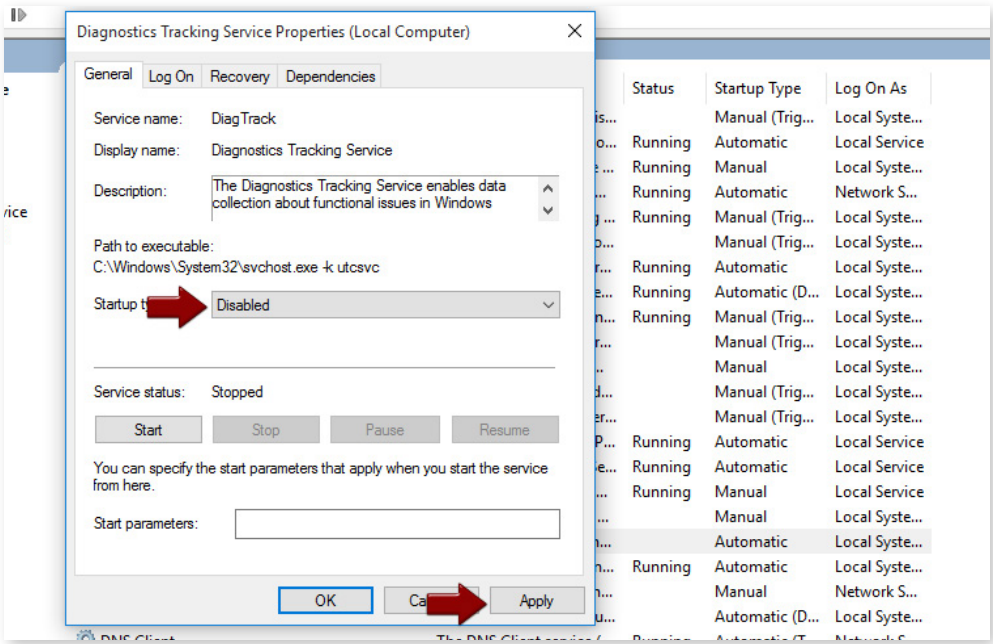
This one is kind of optional. If you are paranoid about Microsoft learning what is in your machine as far as hardware and its configuration, you may wish to disable DMD. If you attach something odd to your new laptop, you may have to go the extra mile to locate a driver yourself instead of pulling the information directly from a Microsoft server.

However, to disable it you have to be in the registry. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Device Metadata, and edit the DWORD called PreventDeviceMetadataFromNetwork. Set it to one:

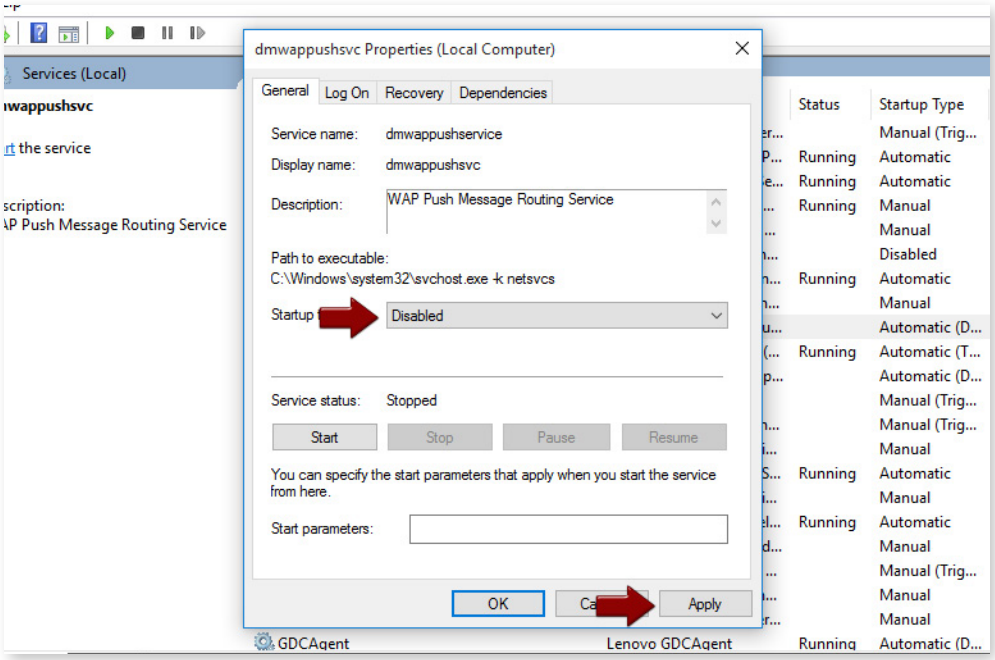


You can exit the registry. Type Services into the search bar and launch the Services desktop app. Find Diagnostics Tracking Service and stop it (after KB 3116900 this will be called the Connected User Experiences and Telemetry).

Now right-click on it and select Properties. Halfway down on the General tab, set the Startup type to "Disabled". Click on Apply at the bottom, then click OK:



If you are using Windows 10, while still in Services, find the intuitively-named dmwappushsvc and disable it as well. Click Apply, then OK:



Reboot. Fun stuff, eh? As a bonus you can try uninstalling some of the various Windows apps you won't be needing, many of which will phone home and be annoying, but we won't cover that in great detail here.

Mark Loveless

Senior Security Researcher

Mark Loveless is a Duo Labs researcher who also goes by the name Simple Nomad on the interwebs. He is not overly paranoid in spite of the fact that evil alien robots are stealing his luggage when he travels.