CERIAS

The Center for Education and Research in Information Assurance and Security

Windows 10 data leakage: A digital forensics project

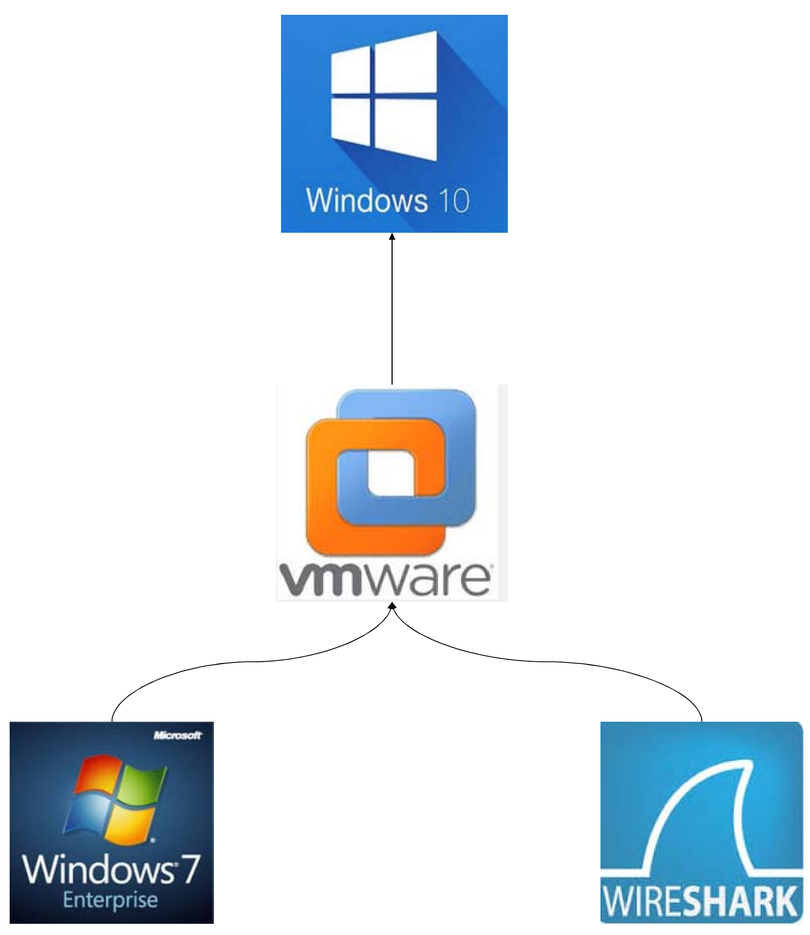
Nicholas Hughes, Cliff Blizzard, Aaron Oles, Dr. Connie Justice

Abstract

The problem reported was even when there are numerous ways to disable Windows 10 tracking, it is believed that Windows 10 still talks to Microsoft several times a day. It is reported that Windows 10 sends information to Microsoft via unsecure channels and makes your data easy to obtain by hackers. When using the Windows 10 Enterprise Edition which has the most controls, data tracking still continues.

The purpose of this project is to either prove or disprove Windows 10 data leakage by investigating seven various scenarios of Windows 10 with diverse security settings.

The methods used for this testing are Wireshark, to monitor all outgoing IP addresses and capture the packets for several hours on each load of Windows 10; and various Windows 10 installations on virtual machines.



Investigation configuration

Findings

After 7 clean installs we have discovered:

1. Microsoft encrypts the telemetry data with the TLSv1.2 protocol
2. To date no one has decrypted the encrypted data
3. Of the collected packets with no restrictions: 236, 107 packets were collected, 50,079 going to Microsoft equaling 21.2% of all packets.
4. Of the collected packets with most restrictions we collected 16,775 and 1,054 went to Microsoft, which is 6.3% of all packets.
5. Of the other five different settings, we have determined that the average packet size going to Microsoft is 1MB.
6. We have concluded that the only way one can stop Microsoft from capturing packets completely is to put the Enterprise edition on a domain and have the organization unit manage what telemetry data can or can't go back to Microsoft.

Wireshark output: Telemetry data

Source	Destination	Protocol	Length
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	66
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	54
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TLSv1.2	254
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	54
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TLSv1.2	268
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TLSv1.2	267
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	1514
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	1514
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TLSv1.2	179
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TLSv1.2	267
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	1514
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TLSv1.2	1463
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	54
192.168.134.128	sqm.telemetry.microsoft.com.nsatc.net	TCP	54

Open. Express Settings. Nothing Changed

192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP

General and location options off.

192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TLSv1.2
192.168.134.128	cy2.vortex.data.microsoft.com.akadns.net	TCP

Location settings on, rest off.

Telemetry data: Microsoft's terminology for collecting individual's data

http://thehackernews.com/2016/02/microsoft-windows10-privacy.html

CERIAS

PURDUE UNIVERSITY