Сцена

84ckf1r3
84ckf1r3@gmail.com

ТАЙНАЯ ЖИЗНЬ WINDOWS 10

О ЧЕМ WINDOWS 10 СТУЧИТ В MICROSOFT
И КАК ЗАСТАВИТЬ ЕЕ ПРЕКРАТИТЬ

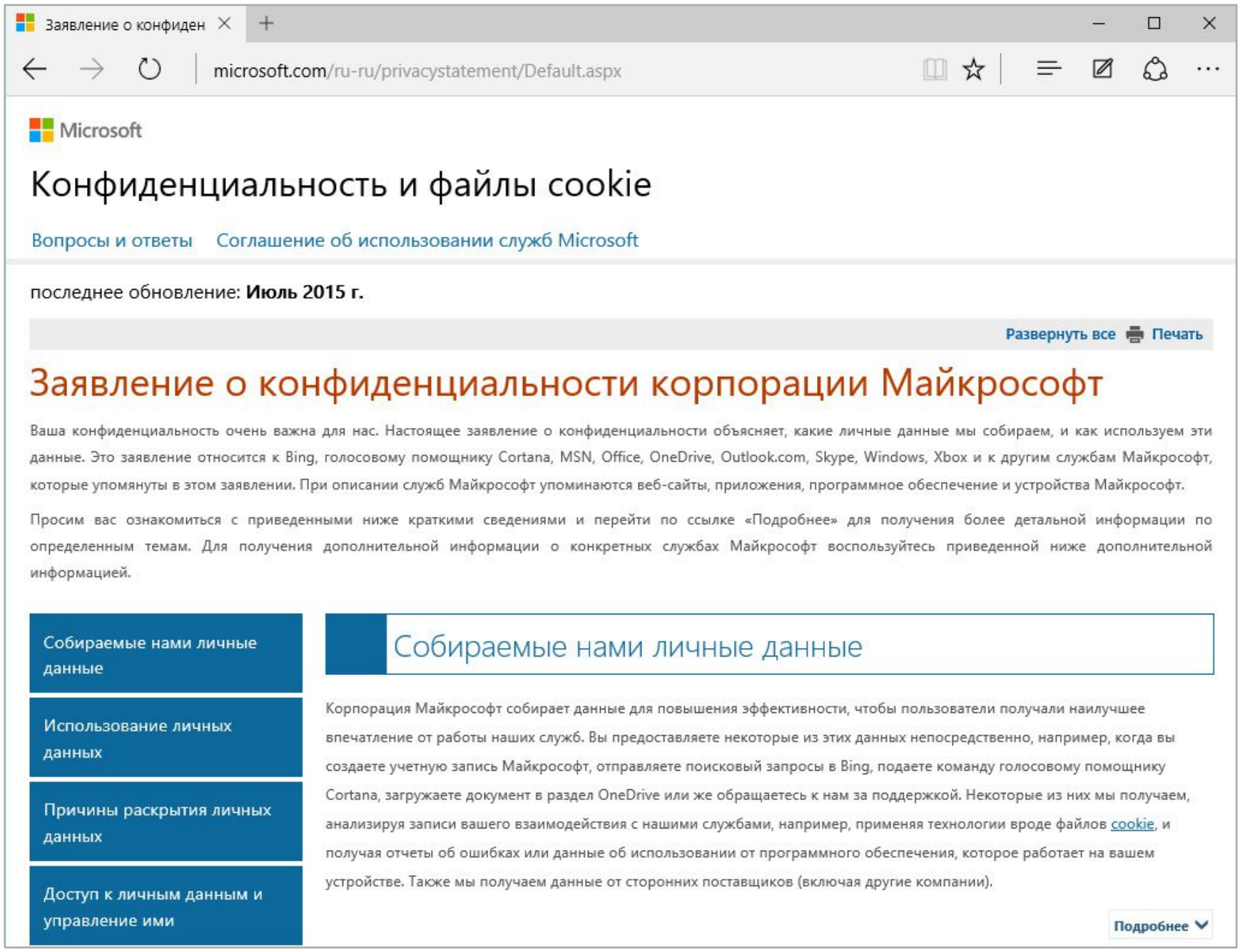
С момента своего появления Windows был естественной средой обитания зловредов всех мастей. Похоже, новая версия этой операционки сама стала одним из троянов. Сразу после установки чистая система ведет себя подозрительно. Данные рекой льются на десятки серверов Microsoft и партнерских компаний. Мы решили разобраться с жалобами на шпионские замашки «десятки» и узнали, что и куда она отправляет.

MICROSOFT > NSA

Первые сообщения о странном поведении Windows 10 появились еще на этапе знакомства с Technical Preview. Значительный трафик в ней создается постоянно — даже когда не запущено ни одно приложение для работы в сети. Тогда такое поведение списывали на сбор статистики, необходимой для отладки. В Microsoft изучали поведение нового продукта на разных конфигурациях, а пользователи играли роль бета-тестеров. Вроде бы все логично. Однако с выходом релиза ничего не изменилось и жалоб стало только больше.

«В прошлые выходные я обновил Windows 8 на лэптопе моего сына до Windows 10. Сегодня в первый рабочий день мне пришло письмо из Microsoft с темой „Еженедельный отчет об активности“. В нем были подробнейшие сведения о действиях сына за ноутбуком: когда и сколько он за ним сидел, какие приложения использовал и как долго, что искал в Сети, какие сайты посещал и многое другое. Я был крайне возмущен, поскольку не собирался следить за своим ребенком. В Microsoft мне ответили, что если я не хочу получать подобных писем, то мне следует указать это в настройках семейного аккаунта через свою учетную запись. В Windows 8 такой проблемы не было». Это отрывок из письма друга известного писателя и активиста Кори Доктороу, опубликованное в блоге Boing Boing. Многие обозреватели утверждают, что эти сведения о пользователях по-прежнему собираются — независимо от настроек аккаунта. Если что-то и можно отключить, то это отчеты, которые приходят на почту.Самое интересное, что сбор различной информации встроенными средствами Windows 10 подробно описан в «Заявлении о конфиденциальности». Конечно, большинство не станет его читать, а среди ознакомившихся будет много недоумевающих. Формулировки в объемном тексте используются хитрые и размытые. Из них трудно понять, что именно изменится в плане приватности с переходом

на Windows 10. Если кратко, то о ней можно будет забыть. Правозащитники сходятся во мнении, что система сразу начинает собирать все данные, которые только может получить.



Заявление об отсутствии конфиденциальности

Вот список их основных типов.

Биометрические:

- образец голоса и произношения определенных слов;
- образец почерка (рукописного ввода);
- образцы набираемых текстов в любом приложении.

Геолокационные:

- информация о текущем местоположении;
- история местоположений с указанием временных меток.

Технические:

- данные об оборудовании, включая идентификаторы устройств;
- сведения о подключенных сетях (проводных и беспроводных);
- сведения телеметрии;
- данные от любых встроенных датчиков.

Поведенческий анализ:

- история поисковых запросов;
- история посещенных веб-страниц;
- время старта Windows и завершения работы;
- время запуска и закрытия каждого приложения.

Покупательская активность:

- загрузки приложений из фирменного магазина;
- переход по ссылкам контекстной рекламы;
- переход по ссылкам персонализированной рекламы.

Перечень можно продолжить, но и такого набора достаточно, чтобы начать собственное исследование. Забегая вперед, отметим, что часть обвинений в адрес Windows 10 все-таки не подтвердилась. Например, чешское издание AE News предполагает, что ОС выполняет отправку изображения с веб-камеры на серверы Microsoft. В нашем тесте система отреагировала на подключение камеры лишь установкой драйверов — никаких посторонних действий с ней зарегистрировано не было ни сразу, ни потом.

НАБЛЮДЕНИЕ ЗА НАБЛЮДАТЕЛЕМ

Привычных инструментов в арсенале хакера предостаточно для изучения любого софта. Тестовый комп с чистым SSD, виртуальная машина, снифер Wireshark, HTTP-прокси и дебаггер Fiddler, монитор сетевых соединений TCPView, а также программы для создания снимков реестра и мелкие вспомогательные утилиты. Мы старались использовать версии, не требующие установки. Исключение составили только Wireshark и Fiddler из-за специфики их работы. Эти программы оставили напоследок, чтобы большая часть тестирования выполнялась на совершенно чистой системе. Сетевой трафик анализировался как в настройках Windows 10 по умолчанию, так и после поэтапного отключения всех следящих функций.

Из официальных документов следует, что за пользователем следят: сама Windows, глубоко интегрированный поиск Bing, голосовой помощник Cortana, служба MSN, пакет Office, клиент облачного хранилища OneDrive, почтовый

клиент Outlook, а также Skype, Silverlight и Xbox Live. Подробнее об этом написано на сайте Microsoft (http://www.microsoft.com/ru-ru/privacystatement/Default.aspx). Посмотрим, как именно происходит сбор данных.

Первый старт Windows 10

Выполнив чистую установку сборки 10240, мы стали наблюдать за ее сетевым поведением с помощью TCPView. Никаких других действий при этом не выполнялось. Поначалу все было тихо — как в «семерке». Лишь фирменный магазин приложений показывал готовность получить данные через сеть доставки контента от Akamai Technologies.Когда уже стало надоедать сидеть в засаде, внезапно ожил системный процесс **`\Windows\System32\svchost.exe`**. Он установил подключение к удаленному узлу 191.232.139.254 и отправил на него 7,5 Кбайт.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Port	Remote Address	Remote Port	State	Sent Pa...	Sent Bytes
WinStore.Mobile.exe	2188	TCP	49465	a23-65-118-14.deploy.static.akamaitechnologies.com	https	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49466	a23-64-219-156.deploy.static.akamaitechnologies.com	https	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49467	a104-81-215-222.deploy.static.akamaitechnologies.com	http	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49468	a104-81-215-222.deploy.static.akamaitechnologies.com	http	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49469	a104-81-215-222.deploy.static.akamaitechnologies.com	http	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49470	a104-81-215-222.deploy.static.akamaitechnologies.com	http	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49471	a104-81-215-222.deploy.static.akamaitechnologies.com	http	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49472	a104-81-215-222.deploy.static.akamaitechnologies.com	http	CLOSE_WAIT		
WinStore.Mobile.exe	2188	TCP	49473	a23-64-217-191.deploy.static.akamaitechnologies.com	https	CLOSE_WAIT		
svchost.exe	828	TCP	49696	a88-221-132-41.deploy.akamaitechnologies.com	http	ESTABLISHED		

Endpoints: 10 Established: 1 Listening: 0 Time Wait: 0 Close Wait: 9

Затишье перед бурей

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Port	Remote Address	Remote Port	State	Sent Pa...	Sent Bytes	Rcvd Packe...	Rcvd Bytes
System	4	UDP	netbios-ns	*	*		9	450	3	150
svchost.exe	1692	TCP	49700	191.232.139.254	https	ESTABLISHED	5	7,465	3	1,215
svchost.exe	828	UDP	50502	*	*		4	223	3	327
System	4	UDP	netbios-dgm	*	*					
svchost.exe	916	UDP	ssdp	*	*					
svchost.exe	916	UDP	ssdp	*	*					

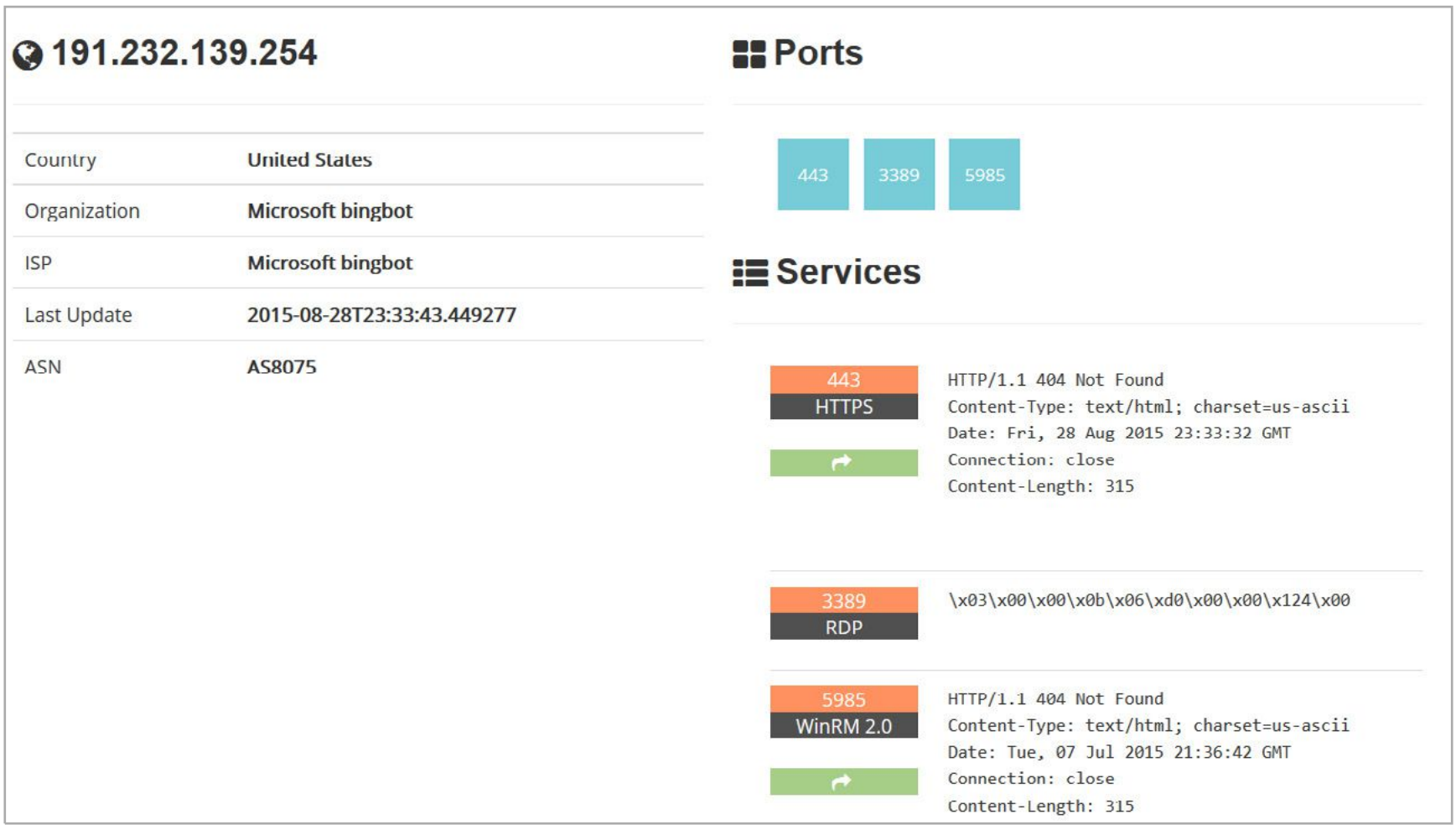
Endpoints: 65 Established: 1 Listening: 21 Time Wait: 0 Close Wait: 9

Первый буревестник

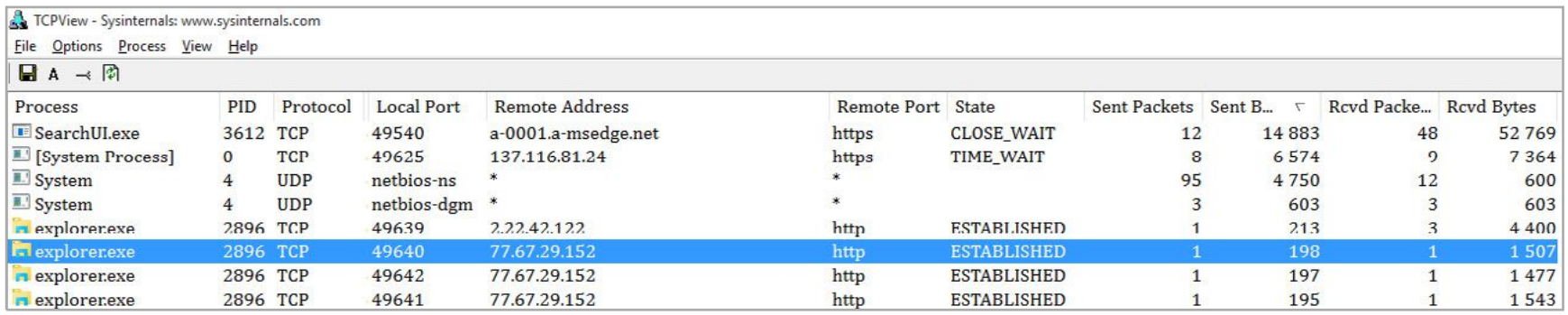
Можно было узнать принадлежность IP-адреса через сервис WHOIS, но спрашивать Shodan информативнее.Как стало ясно из описания, это робот поисковой системы Bing. Если бы в тесте был сделан хоть один поисковый запрос (даже локальный), тогда соединение не вызывало бы никаких возражений. Однако мы просто сидели и смотрели в TCPView на то, как компьютер начинает шпионить за нами.

ПОДГОТОВКА К ПАКЕТНОМУ ШТОРМУ

Спящие службы можно ждать долго. Пора пробудить их и проявить немного активности. Нажатие кнопки «Пуск» заставило ожить инфоблоки справа. Появился прогноз погоды, начали отображаться новости и реклама. TCPView показывает, что все это грузится через сеть Akamai и выглядит легитимно. Как только мы запускаем блокнот и начинаем набирать текст, картина сразу меняется.

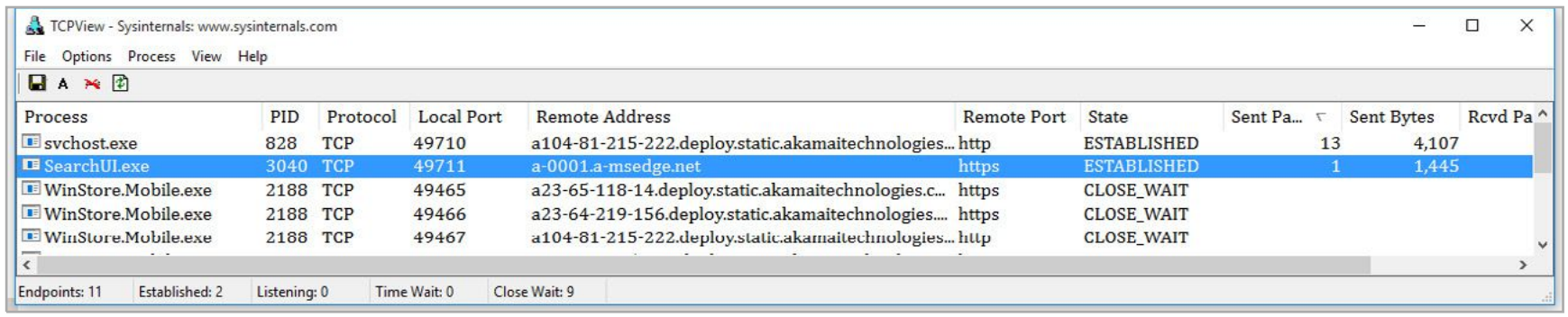


BingBot попался



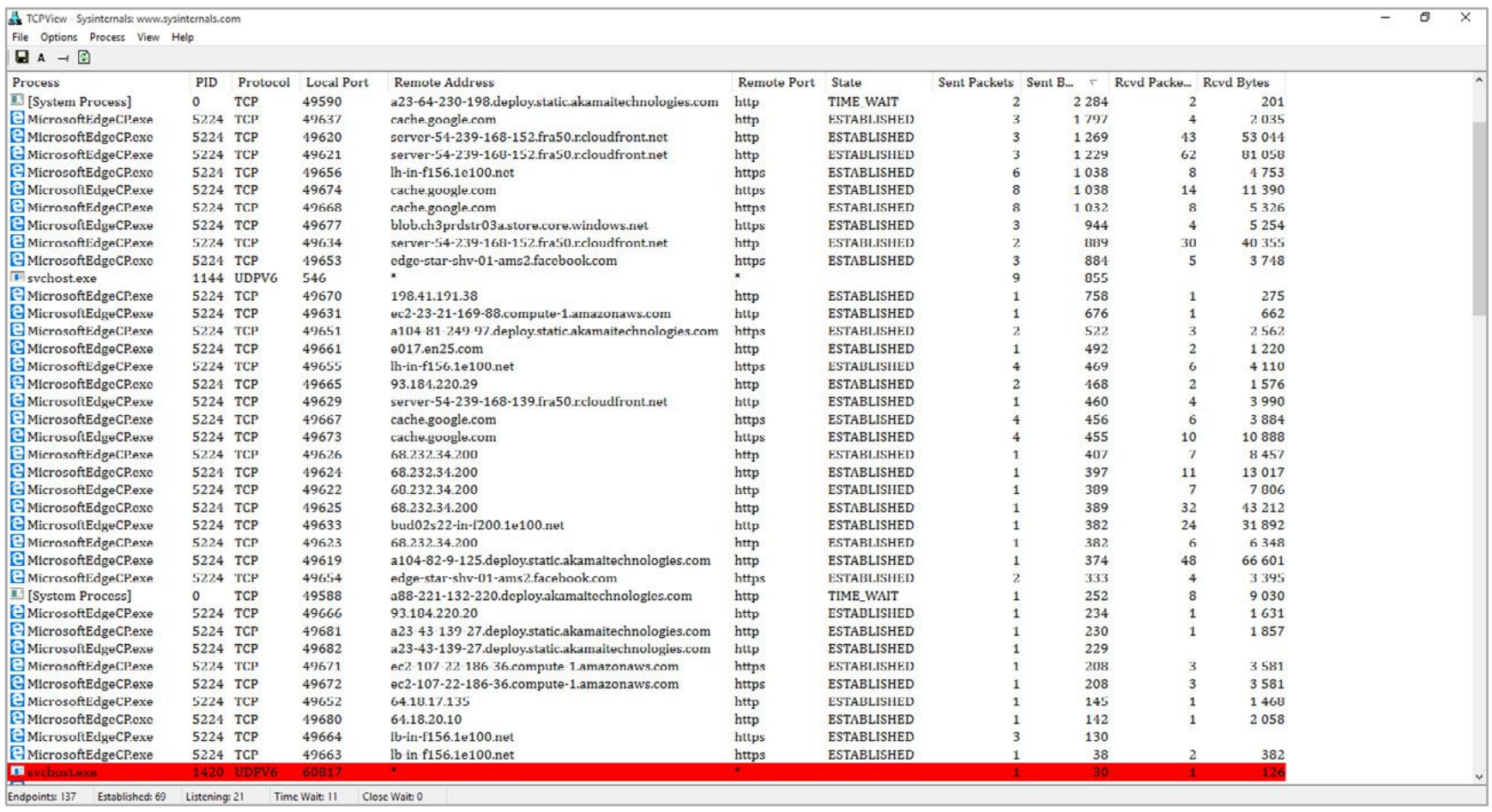
Запущен только блокнот

Возникает сразу шесть соединений, которые быстро закрываются, — в сумме уходит чуть больше сотни пакетов. Отключив функцию «искать в интернете», мы оставили только локальный поиск Windows. Снова запустили блокнот и начали набирать произвольный текст. Все равно появился процесс SearchUI и стал передавать данные в Сеть.



Поиск в интернете отключен

Наверное, мы как-то не так поняли «Заявление о конфиденциальности». Посмотрим его еще раз. Это простая текстовая страничка, которая открывается в браузере Edge. Какой она может создать трафик? Примерно такой, как на картинке.



Открыта одна страница в браузере

Перечень соединений настолько быстро обновлялся, что просто так и не уследишь. Поэтому мы приступили ко второй части исследования. Закрыли все приложения, поставили снифер Wireshark и записали активность Windows за полчаса. Чтобы сымитировать хоть какую-то деятельность, мы просто смотрели некоторые настройки в панели управления, но не меняли их.

compromat.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: eth.dst_resolved !="10.0.2.15" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
7870	2435.79116	10.0.2.15	217.69.139.202	TCP	54	[TCP ACKed unseen segment] 49626→443 [ACK] Seq=837 Ack=9431 Win=65535 Len=0
7872	2435.79289	10.0.2.15	217.69.139.202	TCP	54	[TCP ACKed unseen segment] 49626→443 [ACK] Seq=837 Ack=9432 Win=65535 Len=0
7873	2436.01667	10.0.2.15	216.218.248.203	TCP	54	49617→80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
7874	2436.01685	10.0.2.15	216.218.248.230	TCP	54	49618→80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
7882	2436.23495	10.0.2.15	216.218.248.203	TCP	54	[TCP ACKed unseen segment] 49617→80 [ACK] Seq=2 Ack=2 Win=65535 Len=0
7884	2436.23531	10.0.2.15	216.218.248.230	TCP	54	[TCP ACKed unseen segment] 49618→80 [ACK] Seq=2 Ack=2 Win=65535 Len=0
7885	2441.43786	fe80::b155:9319:75cf	ff02::1:2	DHCPv6	157	Solicit XID: 0x57ecfa CID: 000100011d70c7910800278989b3
7886	2455.25145	10.0.2.15	207.46.194.10	TCP	54	49637→443 [FIN, ACK] Seq=416 Ack=3988 Win=65535 Len=0
7887	2455.25160	10.0.2.15	207.46.194.10	TCP	54	49637→443 [RST, ACK] Seq=417 Ack=3988 Win=0 Len=0
7889	2455.25207	10.0.2.15	217.69.139.202	TCP	54	[TCP ACKed unseen segment] 49626→443 [FIN, ACK] Seq=837 Ack=9432 Win=65535 Len=0
7890	2455.25216	10.0.2.15	217.69.139.202	TCP	54	[TCP ACKed unseen segment] 49626→443 [RST, ACK] Seq=838 Ack=9432 Win=0 Len=0
7891	2455.25245	10.0.2.15	104.75.80.153	TCP	54	49629→443 [FIN, ACK] Seq=355 Ack=5050 Win=65535 Len=0
7892	2455.25253	10.0.2.15	104.75.80.153	TCP	54	49629→443 [RST, ACK] Seq=356 Ack=5050 Win=0 Len=0
7895	2455.25286	10.0.2.15	104.75.80.153	TCP	54	49631→443 [FIN, ACK] Seq=355 Ack=5050 Win=65535 Len=0
7896	2455.25298	10.0.2.15	104.75.80.153	TCP	54	49631→443 [RST, ACK] Seq=356 Ack=5050 Win=0 Len=0
7898	2455.25326	10.0.2.15	104.75.80.153	TCP	54	49630→443 [FIN, ACK] Seq=355 Ack=5050 Win=65535 Len=0
7899	2455.25335	10.0.2.15	104.75.80.153	TCP	54	49630→443 [RST, ACK] Seq=356 Ack=5050 Win=0 Len=0
7900	2455.25363	10.0.2.15	104.75.80.153	TCP	54	49632→443 [FIN, ACK] Seq=355 Ack=5050 Win=65535 Len=0
7902	2455.25372	10.0.2.15	104.75.80.153	TCP	54	49632→443 [RST, ACK] Seq=356 Ack=5050 Win=0 Len=0
7904	2455.25405	10.0.2.15	77.67.29.144	TCP	54	49636→443 [FIN, ACK] Seq=345 Ack=4575 Win=65535 Len=0
7905	2455.25415	10.0.2.15	77.67.29.144	TCP	54	49636→443 [RST, ACK] Seq=346 Ack=4575 Win=0 Len=0
7907	2455.25443	10.0.2.15	77.67.29.144	TCP	54	49634→443 [FIN, ACK] Seq=345 Ack=4575 Win=65535 Len=0
7908	2455.25453	10.0.2.15	77.67.29.144	TCP	54	49634→443 [RST, ACK] Seq=346 Ack=4575 Win=0 Len=0
7909	2455.25480	10.0.2.15	77.67.29.144	TCP	54	49635→443 [FIN, ACK] Seq=345 Ack=4575 Win=65535 Len=0
7911	2455.25489	10.0.2.15	77.67.29.144	TCP	54	49635→443 [RST, ACK] Seq=346 Ack=4575 Win=0 Len=0
7912	2455.25515	10.0.2.15	137.116.81.24	TCP	54	49625→443 [FIN, ACK] Seq=6575 Ack=7365 Win=65535 Len=0
7915	2455.25538	10.0.2.15	137.116.81.24	TCP	54	49638→443 [FIN, ACK] Seq=449 Ack=5425 Win=65535 Len=0
7916	2455.25547	10.0.2.15	137.116.81.24	TCP	54	49638→443 [RST, ACK] Seq=450 Ack=5425 Win=0 Len=0
7918	2455.25574	10.0.2.15	207.46.194.10	TCP	54	49633→443 [FIN, ACK] Seq=1300 Ack=4490 Win=65535 Len=0
7920	2455.25601	10.0.2.15	77.67.29.178	TCP	54	49628→443 [FIN, ACK] Seq=360 Ack=4591 Win=65535 Len=0
7921	2455.25612	10.0.2.15	77.67.29.178	TCP	54	49628→443 [RST, ACK] Seq=361 Ack=4591 Win=0 Len=0
7923	2455.25654	10.0.2.15	77.67.29.178	TCP	54	49627→443 [FIN, ACK] Seq=360 Ack=4591 Win=65535 Len=0
7924	2455.25665	10.0.2.15	77.67.29.178	TCP	54	49627→443 [RST, ACK] Seq=361 Ack=4591 Win=0 Len=0
7929	2455.41342	10.0.2.15	137.116.81.24	TCP	54	[TCP ACKed unseen segment] 49625→443 [ACK] Seq=6576 Ack=7366 Win=65535 Len=0
7930	2473.43781	fe80::b155:9319:75cf	ff02::1:2	DHCPv6	157	Solicit XID: 0x57ecfa CID: 000100011d70c7910800278989b3

Windows передает непрерывно — неважно, делаешь что-то или нет

IPNetInfo

File Edit View Options Help

IP Address	Country	Network Name	Owner Name	Contact Name	Address	Resolved Name
2.20.254.89	European Union	AKAMAI-PA	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, Cambridge, MA 02142	
2.22.42.122	European Union	AKAMAI-PA	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, Cambridge, MA 02142	
2.23.143.150	European Union	AKAMAI-PA	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, Cambridge, MA 02142	
23.43.139.27	Netherlands	AIBV	Akamai International, BV	Akamai International, BV	Prins Bernhardplein 200, Amsterdam	a23-43-139-27.deploy.static.akamaitechnologies.com
23.78.117.155	Netherlands	AIBV	Akamai International, BV	Akamai International, BV	Prins Bernhardplein 200, Amsterdam	a23-78-117-155.deploy.static.akamaitechnologies.com
23.99.116.116	USA - Washington	MSFT	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	
31.13.64.1	Netherlands	AMS2	Facebook	RIPE DBM	1601 Willow Rd., Menlo Park, CA, 94025	edge-star-shv-01-ams2.facebook.com
64.4.54.254	USA - Washington	MICROSOFT	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	
64.18.20.10	USA - Maryland	CYBERTRUSTCIDR	Verizon Business Global, LLC	Verizon Business Global, LLC	13100 Columbia Pk, Silver Spring	
65.52.108.33	USA - Washington	MICROSOFT-1BLK	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	msnbot-65-52-108-33.search.msn.com
65.55.44.54	USA - Washington	MICROSOFT-1BLK	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	
65.207.25.151	USA - Virginia	UU-65-207-25	INTERNAL/MCI7468		18155 Technology Drive Extend to Terremark MPR3 room, Culpeper	
68.232.34.200	USA - California	EDGECAST-NETBLK-04	EdgeCast Networks, Inc.	EdgeCast Networks, Inc.	2850 Ocean Park Blvd., Suite 110, Santa Monica	
77.67.29.144	United States	AKAMAI-TINET	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, Cambridge, MA 02142	
88.221.132.128	European Union	AKAMAI-PA	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, Cambridge, MA 02142	a88-221-132-128.deploy.akamaitechnologies.com
93.184.220.20	European Union	EDGECAST-NETBLK-03	NETBLK-03-EU-93-184-220-0-22	Derrick Sawyer	2850 Ocean Park Blvd., Suite 200, Santa Monica CA 90405 USA	
104.47.153.35	USA - Washington	MSFT	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	
104.75.53.17	USA - Massachusetts	AIBV	Akamai International, BV	Akamai International, BV	Prins Bernhardplein 200, Amsterdam	a104-75-53-17.deploy.static.akamaitechnologies.com
104.82.10.129	USA - Massachusetts	AIBV	Akamai International, BV	Akamai International, BV	Prins Bernhardplein 200, Amsterdam	a104-82-10-129.deploy.static.akamaitechnologies.com
108.162.232.199	USA - California	CLOUDFLARENET	CloudFlare, Inc.	CloudFlare, Inc.	665 Third Street #207, San Francisco	
131.253.61.66	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
134.170.185.125	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
137.116.81.24	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
137.117.235.16	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
138.91.246.237	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
157.55.231.252	USA - Washington	MSFT-GFS	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	
162.159.241.165	USA - California	CLOUDFLARENET	CloudFlare, Inc.	CloudFlare, Inc.	665 Third Street #207, San Francisco	
191.232.139.253	Brazil	060.316.817/0001-03	Microsoft Informatica Ltda	Benjamin Orndorff		
195.12.232.155	Netherlands	AKAMAI	Akamai international V B	Cristian Galve	Akamai International BV, Parkring 29, 85748 Garching bei Munich....	195-12-232-155.customer.teliacarrier.com
207.46.194.10	USA - Washington	MICROSOFT-GLOBAL-NET	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	msnbot-207-46-194-10.search.msn.com
208.67.222.222	USA - California	OPENDNS-NET-1	OpenDNS, LLC	OpenDNS, LLC	145 Bluxome st., San Francisco	resolver1.opendns.com
216.218.248.203	USA - California	HURRICANE-CE0065-2827	Soylent	Soylent	PO Box 4436, Mountain View	
137.135.8.42	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	aka.ms

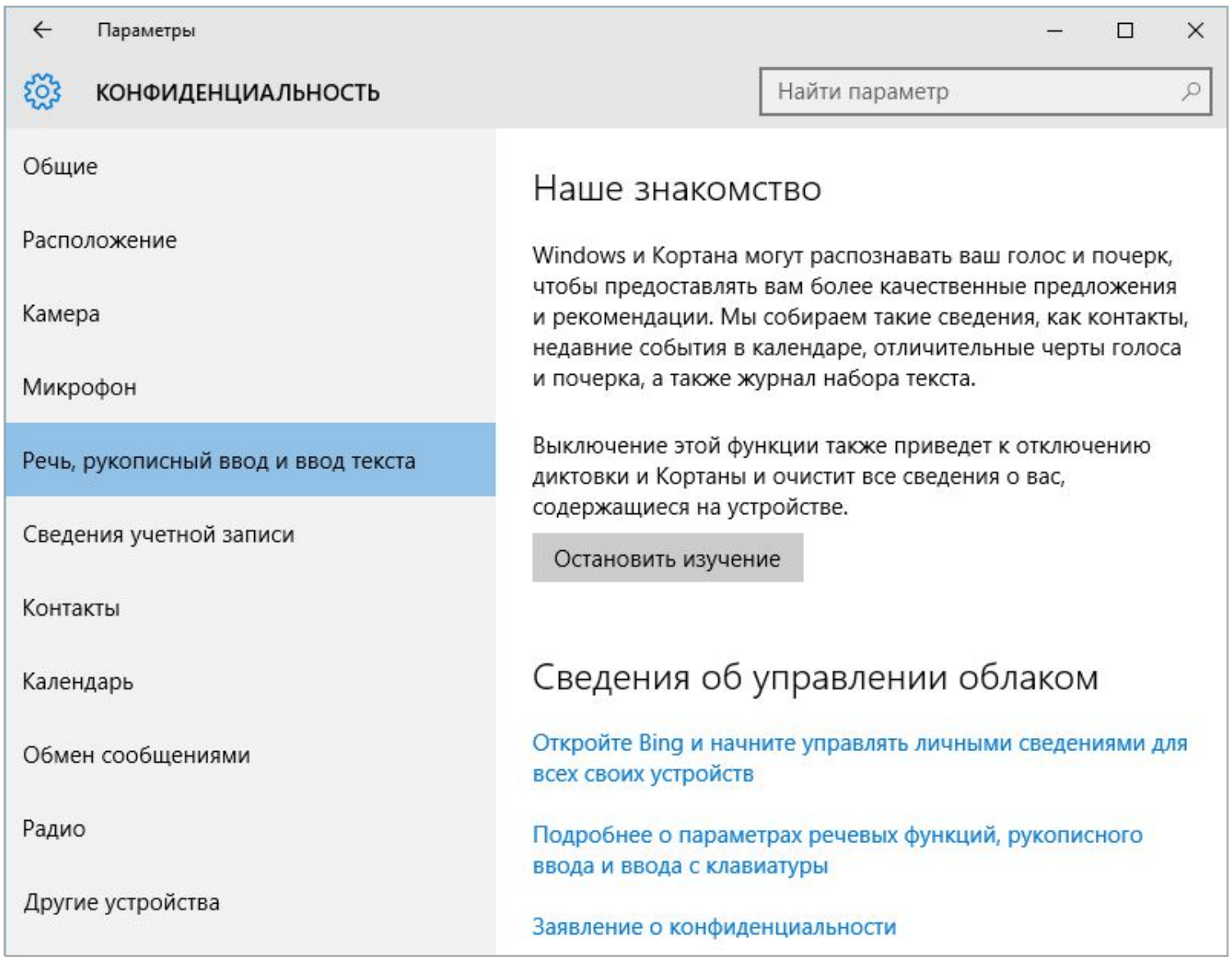
За полчаса нашего бездействия Windows успела разослать отчеты по всему свету

За полчаса в Сеть ушло около восьми тысяч пакетов. Как показало изучение логов, большинство соединений устанавливалось по адресам в пределах одной из крупных подсетей. У принадлежащих им айпишников часто менялись два-три последних октета. Это говорит о том, что Microsoft развернула огромную сеть для обработки всей стекающейся от пользователей Windows информации. Если отсеять однотипные адреса, то в сухом остатке получится подборка, как на картинке.

В глаза бросается бразильский сервер, это очередной BingBot (возможно, какой-то особо специализированный), но вопросы вызывает далеко не только он. Например, какого черта выполнялось соединение с сервером Facebook в Нидерландах? Кто просил подключаться к облачному хранилищу CloudFlare? Ни одного файла еще не создано. Даже учетная запись Microsoft не была активирована.

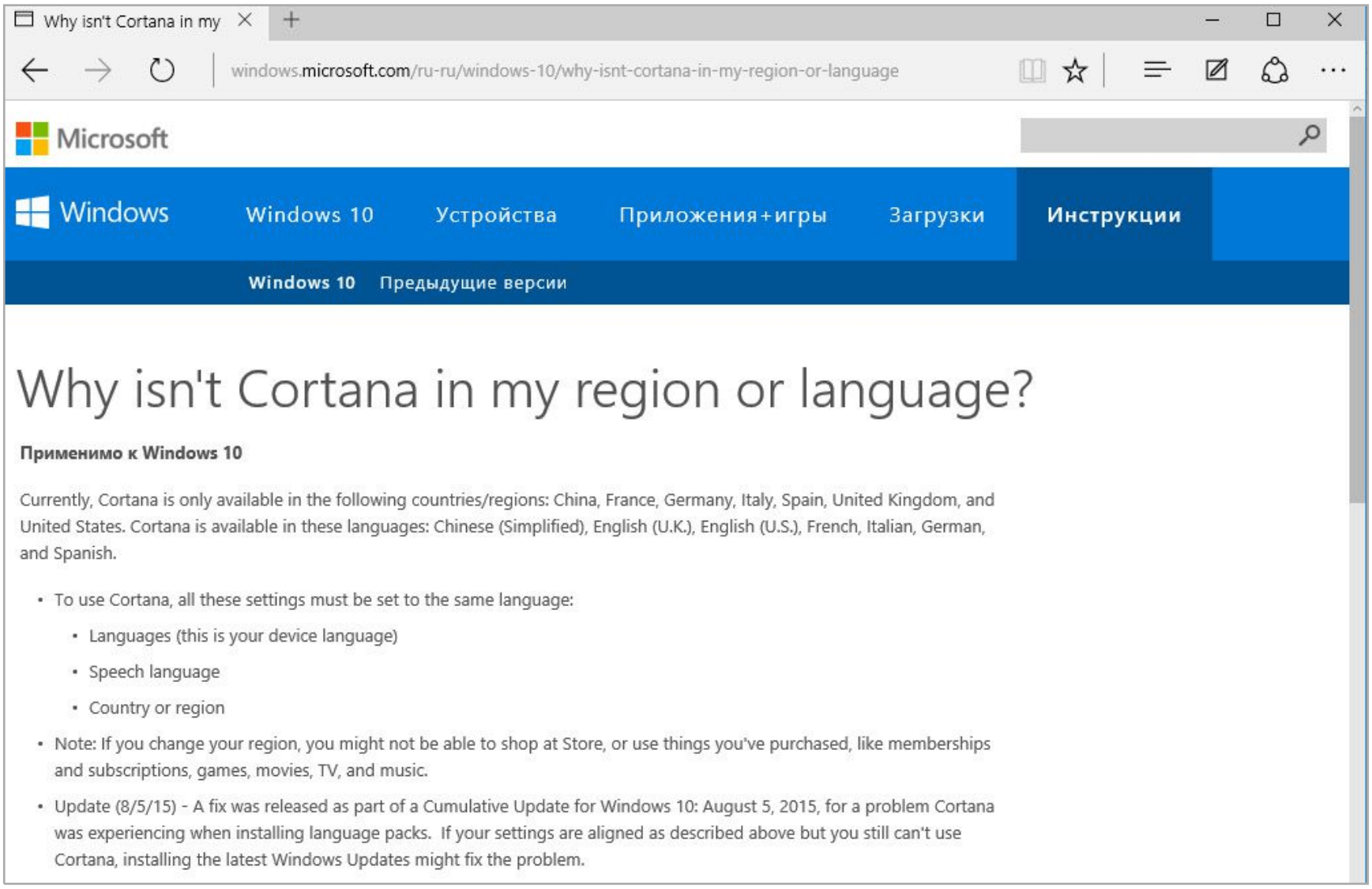
ВСКРЫВАЕМ ШПИОНСКУЮ СЕТЬ

После поиска Bing главная шпионка в Windows — Кортана. С ней как-то сразу сложились натянутые отношения. Сперва она сама настояла на знакомстве, а затем вдруг заявила, что не понимает русскую речь и даже учиться этому не собирается.



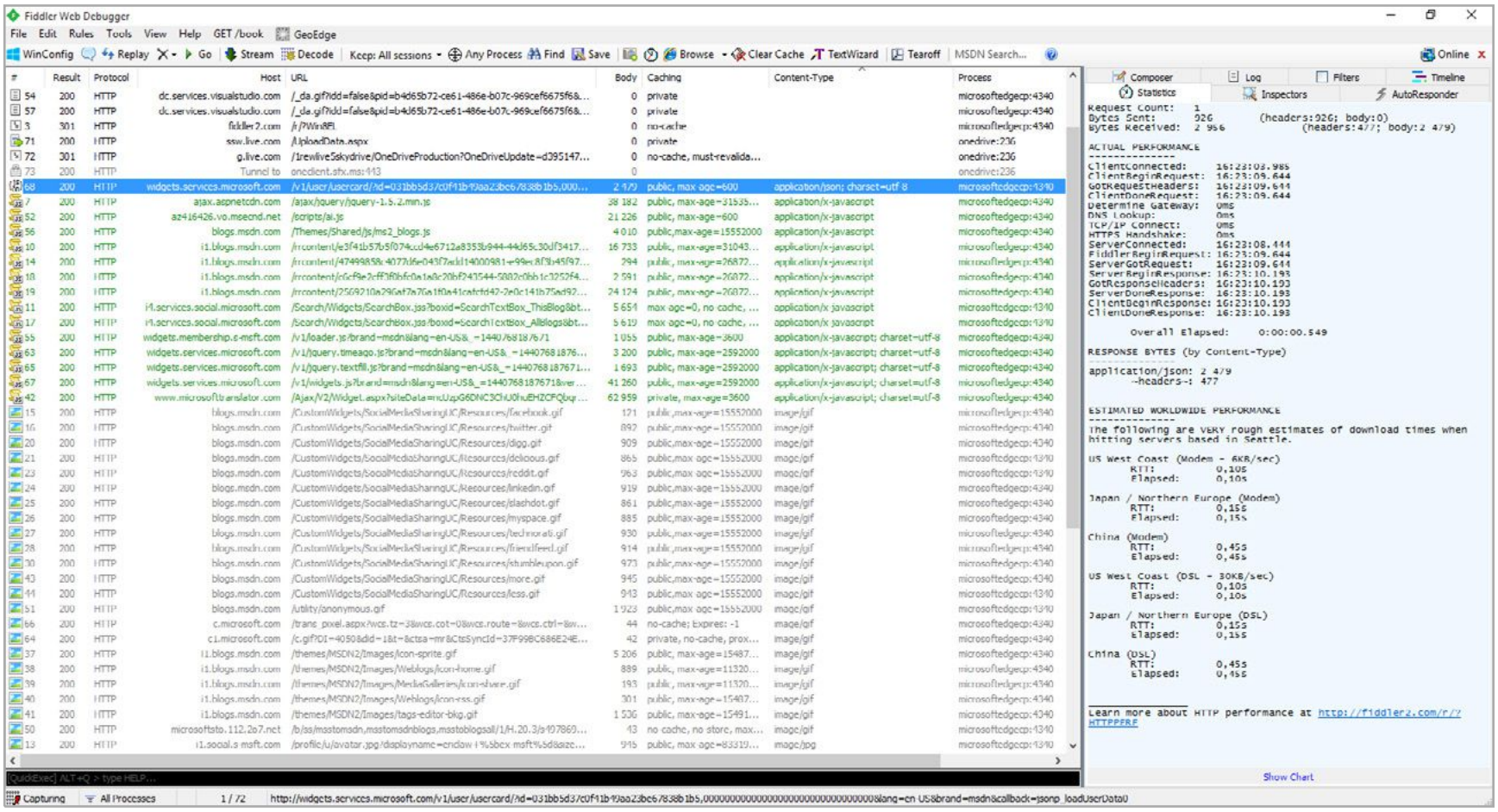
Кортана привыкла знакомиться первой

Даже сменив язык на английский, а регион на США, мы так и не добились ее расположения. В базе знаний Microsoft об этом говорится просто: установите соответствующее исправление через службу обновлений. Жаль только, что пользователь теперь лишен возможности ставить апдейты по своему усмотрению. Они скачиваются и устанавливаются Windows автоматически. Юзер может выбрать лишь отмену перезагрузки и задать отложенную инсталляцию.



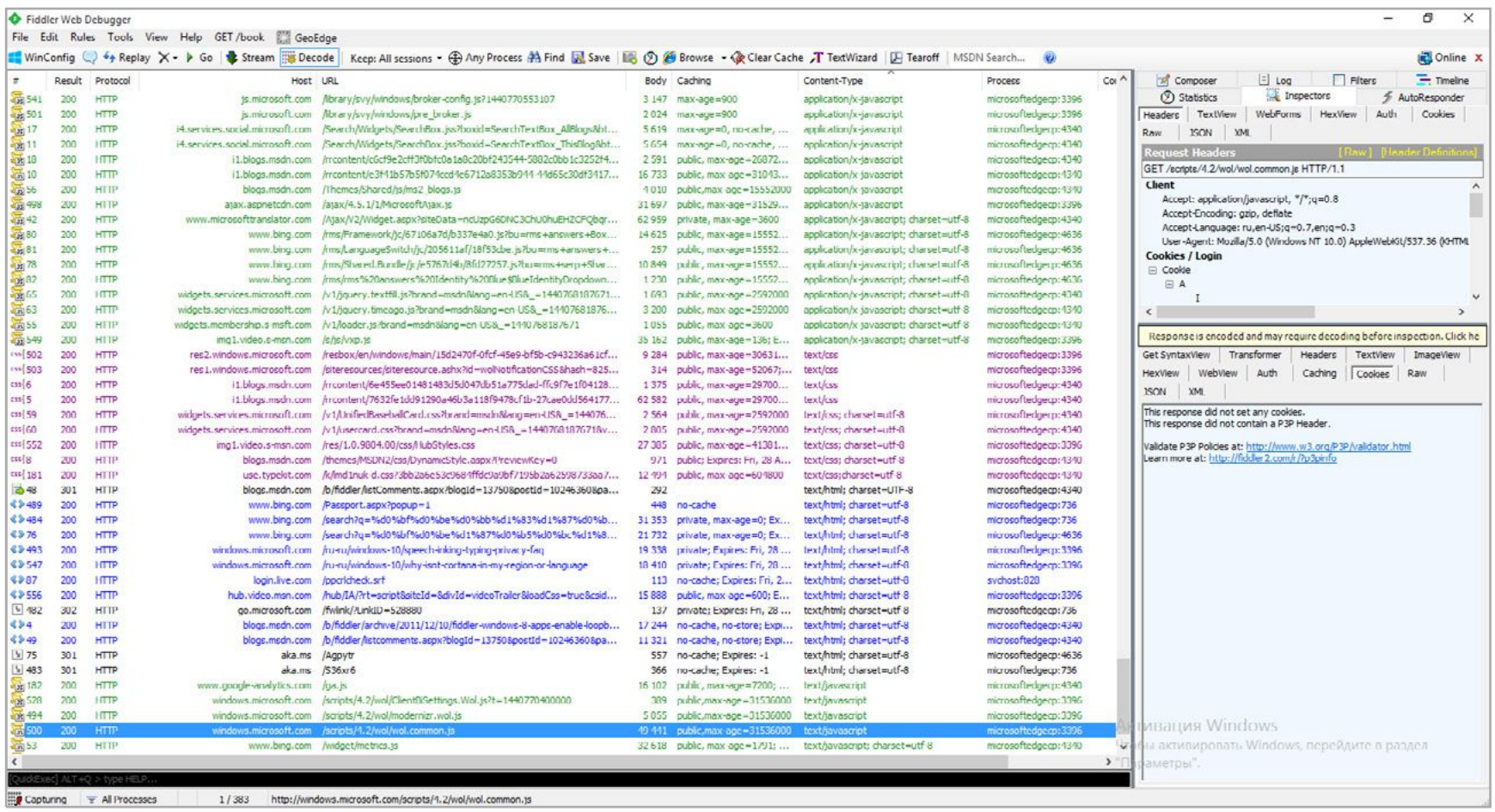
BingBot попался

Большая часть скрытого трафика Windows идет через сеть доставки контента Akamai, поэтому не отображается в логах HTTP-прокси. Однако это не значит, что смотреть их бесполезно. Запустив Fiddler, можно обнаружить интересные вещи. Например, выяснить, что идентификация пользователя происходит еще до активации установленной копии Windows.



Фрагмент лога HTTP-прокси

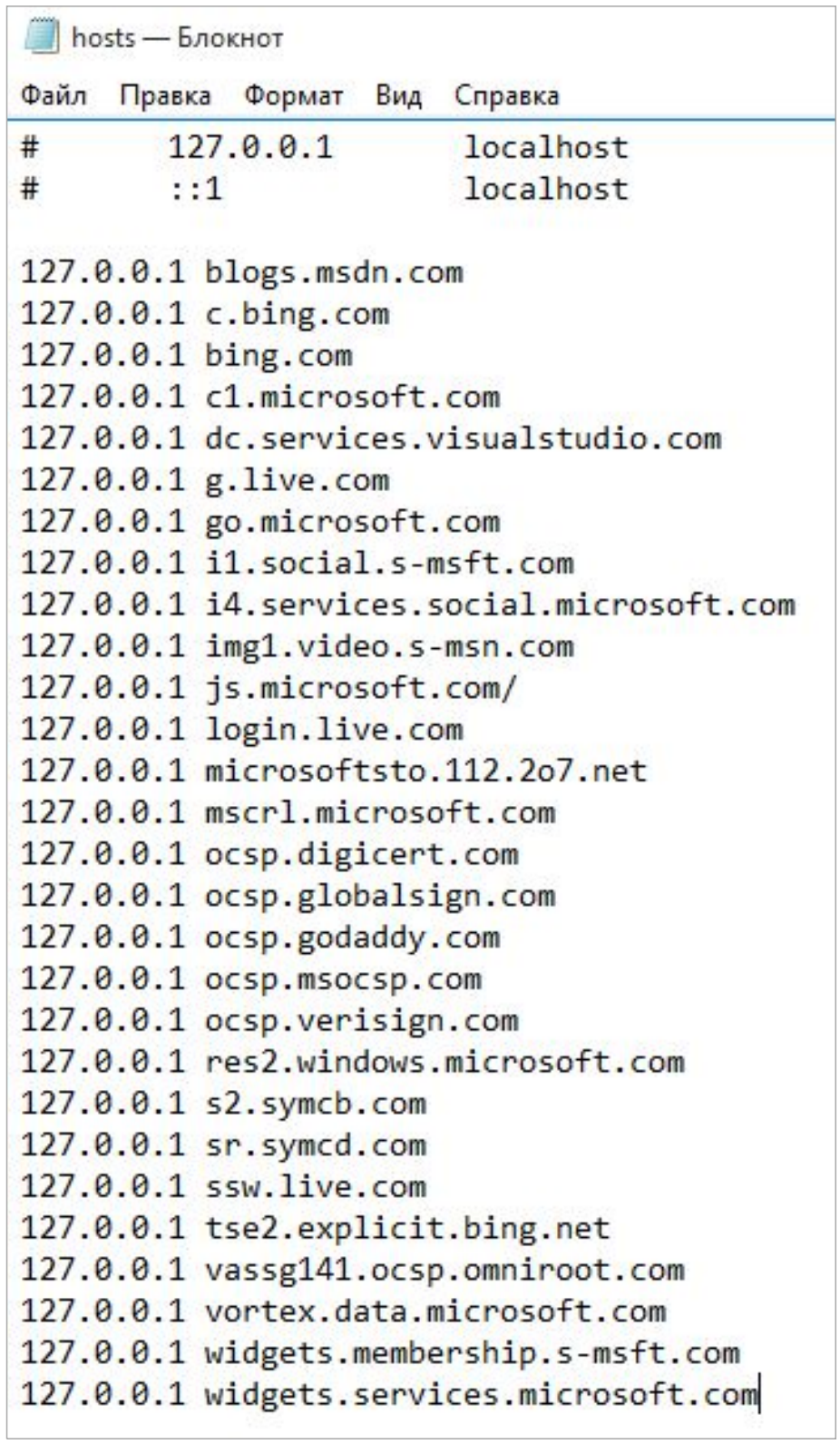
При взгляде на окно Fiddler видно характерную форму **/usercard/?id=**, обращения к учетной записи через службу Microsoft Live и многое другое. Откуда взялись запросы к visualstudio.com и социальным сервисам Microsoft — загадка.



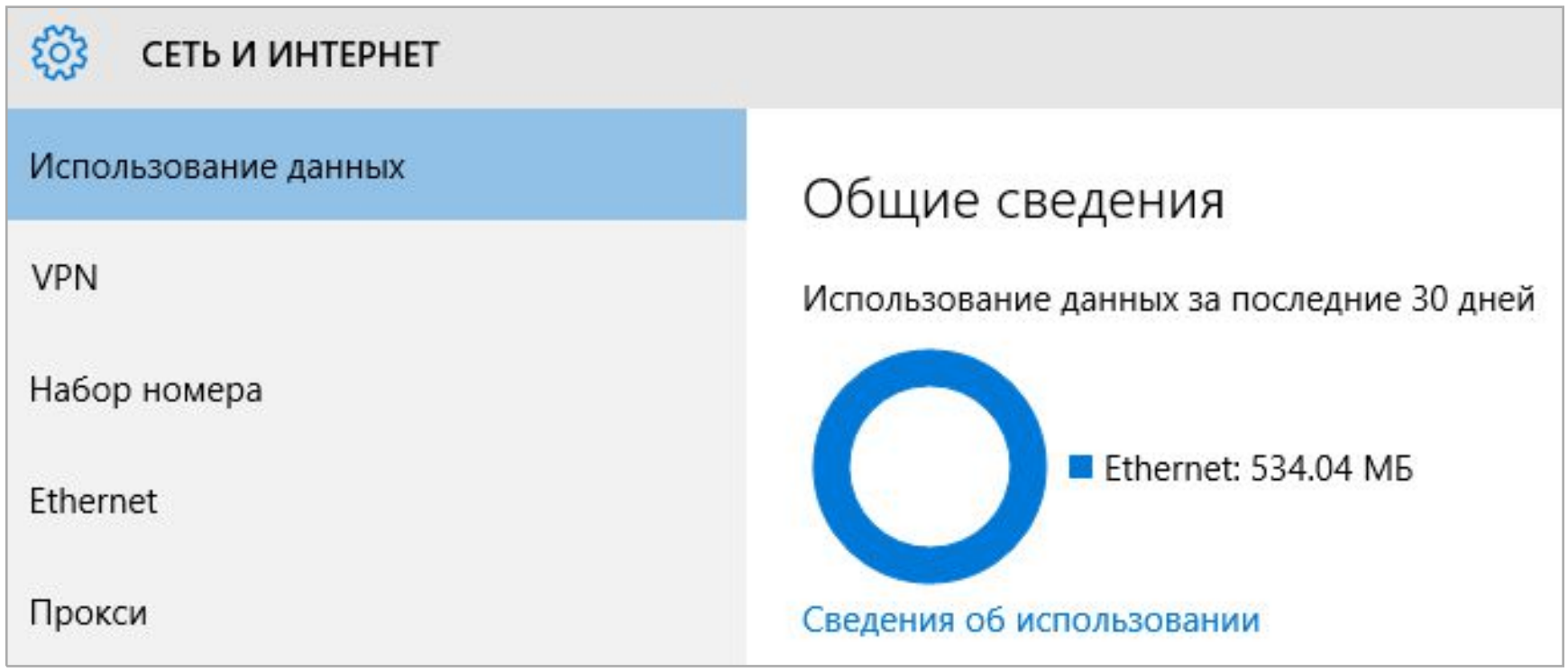
Fiddler собрал 29 веб-адресов

Трафик по HTTP за полчаса бездействия оказался настолько большим, что стало проблемой наглядно отобразить его на экране. Мы сделали пару скриншотов, а затем составили список засветившихся хостов. Можно бы сразу занести их в файл hosts, но мы пока отложим это, чтобы не нарушать ход эксперимента.

Из этого списка ожидаемым выглядит только URL windowsupdate.com, который мы не стали включать в список блокировки. Согласно журналу установки, за все время эксперимента автоматически было инсталлировано 21 обновление общим объемом около 150 Мбайт. В ходе теста, кроме блокнота, мы запускали только калькулятор и свои утилиты для анализа активности Windows, в которых было отключено автообновление. При этом общий сетевой трафик превысил полгигабайта. Многовато для «служебных данных, собираемых в целях улучшения впечатления от работы программ»!



Улов Fiddler кормит localhost



Полгига данных утекли в Сеть

Впечатление оказалось сильно испорченным. Следящих функций в Windows 10 действительно чересчур много. Отключение интегрированного поиска и увольнение Кортаны помогает лишь отчасти. «Защитник Windows» отправляет в Microsoft образы файлов, которые сочтет подозрительными или вредоносными. Фильтр SmartScreen не только проверяет веб-контент, но и формирует список посещенных страниц. Журнал местоположений протоколирует все физические перемещения (особенно актуально, если Windows 10 установлена на мобильном устройстве). Отчет о взаимодействии с пользователем отсылают и многие приложения в новом стиле, а в разделе «данные диагностики и использования» вообще нельзя запретить отправку отчета — можно лишь выбрать менее подробный вариант.

INFO

В последнее время Microsoft пытается научить прежние версии ОС Windows шпионить так же, как это делает «десятка». В частности, следящие функции добавятся с обновлениями KB3075249 и KB3080149.

УХОД В ОФЛАЙН

Мы решили полностью отключить все узаконенные средства шпионажа штатными средствами Windows. В основном настройки меняются через вкладки «Конфиденциальность», «Поиск» и «Обновление и безопасность» в панели управления. Переключателей там с полсотни, вот только будет ли от них толк?

Мы отключили все, что только можно, и запустили Wireshark снова. На этот раз не пользовались никакими встроенными приложениями и даже не трогали мышку. Вернувшись через час, видим в логах снифера до боли знакомые IP.

ds.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
714	3702.64925	10.0.2.15	104.82.19.2	TCP	54	49479→443 [ACK] Seq=206 Ack=2841 Win=64240 Len=0
717	3702.64937	10.0.2.15	104.82.19.2	TCP	54	49479→443 [ACK] Seq=206 Ack=4359 Win=64240 Len=0
720	3702.65594	10.0.2.15	104.82.19.2	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
724	3702.66071	10.0.2.15	104.82.19.2	TCP	54	49482→443 [ACK] Seq=206 Ack=2841 Win=64240 Len=0
727	3702.66084	10.0.2.15	104.82.19.2	TCP	54	49482→443 [ACK] Seq=206 Ack=4359 Win=64240 Len=0
728	3702.66191	10.0.2.15	104.82.19.2	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
749	3702.74851	10.0.2.15	104.82.19.2	TLSv1.2	187	Application Data
755	3702.76352	10.0.2.15	104.82.19.2	TLSv1.2	187	Application Data
783	3702.97773	10.0.2.15	104.82.19.2	TLSv1.2	235	Application Data
785	3702.97926	10.0.2.15	104.82.19.2	TLSv1.2	235	Application Data
822	3703.21624	10.0.2.15	104.82.19.2	TCP	54	49479→443 [ACK] Seq=862 Ack=5707 Win=62892 Len=0
823	3703.23166	10.0.2.15	104.82.19.2	TCP	54	49482→443 [ACK] Seq=862 Ack=5707 Win=62892 Len=0
840	3722.50455	10.0.2.15	104.82.19.2	TCP	54	49482→443 [RST, ACK] Seq=862 Ack=5707 Win=0 Len=0
846	3722.50585	10.0.2.15	104.82.19.2	TCP	54	49479→443 [RST, ACK] Seq=862 Ack=5707 Win=0 Len=0
602	3702.38538	10.0.2.15	131.253.14.8	TCP	66	49478→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
666	3702.60623	10.0.2.15	131.253.14.8	TCP	54	49478→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
667	3702.60799	10.0.2.15	131.253.14.8	TLSv1.2	247	Client Hello
764	3702.83111	10.0.2.15	131.253.14.8	TCP	54	49478→443 [ACK] Seq=194 Ack=2841 Win=64240 Len=0
767	3702.83141	10.0.2.15	131.253.14.8	TCP	54	49478→443 [ACK] Seq=194 Ack=5336 Win=64240 Len=0
769	3702.84720	10.0.2.15	131.253.14.8	TLSv1.2	268	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
790	3703.07357	10.0.2.15	131.253.14.8	TLSv1.2	363	Application Data
832	3703.30318	10.0.2.15	131.253.14.8	TCP	54	49478→443 [ACK] Seq=717 Ack=6669 Win=62907 Len=0
842	3722.50478	10.0.2.15	131.253.14.8	TCP	54	49478→443 [RST, ACK] Seq=717 Ack=6669 Win=0 Len=0
500	3119.42320	10.0.2.15	134.170.58.118	TCP	66	49475→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
502	3119.61978	10.0.2.15	134.170.58.118	TCP	54	49475→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
503	3119.62063	10.0.2.15	134.170.58.118	TLSv1.2	251	Client Hello
507	3119.81418	10.0.2.15	134.170.58.118	TCP	54	49475→443 [ACK] Seq=198 Ack=2841 Win=64240 Len=0
509	3119.86885	10.0.2.15	134.170.58.118	TLSv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
512	3120.06521	10.0.2.15	134.170.58.118	TLSv1.2	555	Application Data
514	3120.06543	10.0.2.15	134.170.58.118	TLSv1.2	891	Application Data
517	3120.27292	10.0.2.15	134.170.58.118	TCP	54	49475→443 [FIN, ACK] Seq=1894 Ack=4263 Win=62818 Len=0
520	3120.46584	10.0.2.15	134.170.58.118	TCP	54	49475→443 [ACK] Seq=1895 Ack=4264 Win=62818 Len=0
851	3781.87651	10.0.2.15	134.170.58.118	TCP	66	49490→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
853	3782.06643	10.0.2.15	134.170.58.118	TCP	54	49490→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
854	3782.06725	10.0.2.15	134.170.58.118	TLSv1.2	251	Client Hello

Змея меняет кожу, но не меняет нрава

Прогресс есть. Общее число запросов уменьшилось на порядок. Примерно втрое сократилось и число удаленных узлов, к которым выполняется подключение без ведома пользователя. Однако среди них появились новые. Если в первом логе Wireshark внезапно нашелся сервер Facebook, то теперь засветился дата-центр Amazon из Ирландии.

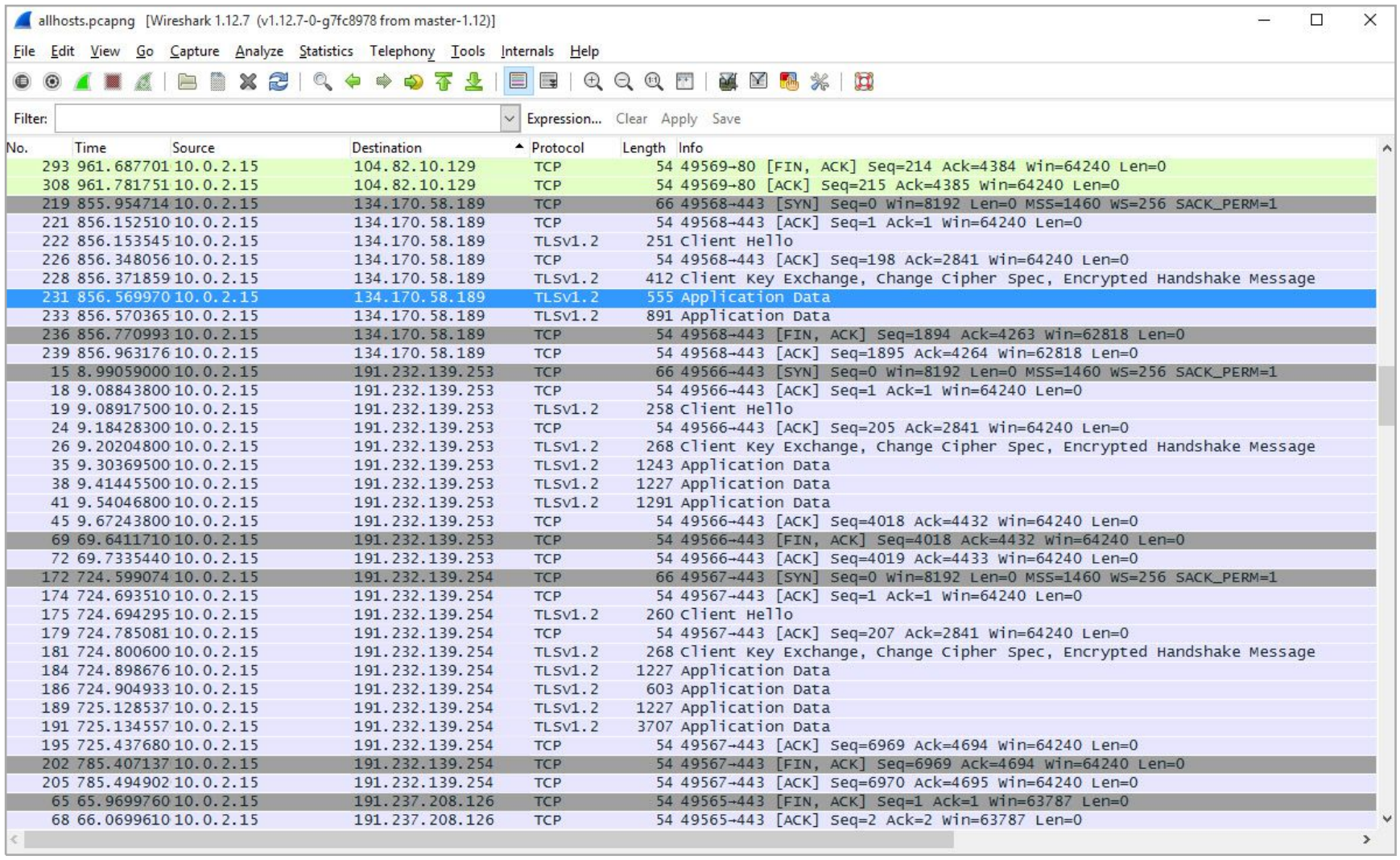
IPNetInfo

File Edit View Options Help

IP Address	Country	Network Name	Owner Name	Contact Name	Address	Resolved Name
2.20.255.38	European Union	AKAMAI-PA	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, C...	
64.4.54.254	USA - Washington	MICROSOFT	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	
88.221.132.17	European Union	AKAMAI-PA	Akamai Technologies	Network Architecture Role Account	Akamai Technologies, 8 Cambridge Center, C...	a88-221-132-17.deploy.akamaitechnologies.com
104.82.19.2	USA - Massachusetts	AIBV	Akamai International, BV	Akamai International, BV	Prins Bernhardplein 200, Amsterdam	a104-82-19-2.deploy.static.akamaitechnologies.com
131.253.14.8	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
134.170.58.118	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
137.117.235.16	USA - Washington	MICROSOFT	Microsoft Corp	Microsoft Corp	One Microsoft Way, Redmond	
176.34.116.125	Ireland	IE-AMAZON-20110523	Amazon Data Services Ireland Ltd	Amazon Data Services Ireland Technical Role Account	Amazon Data Services Ireland, Digital Depot, ...	ec2-176-34-116-125.eu-west-1.compute.amazonaws.com
191.232.139.253	Brazil	060.316.817/0001-03	Microsoft Informatica Ltda	Benjamin Orndorff		
204.79.197.200	USA - Washington	ECN-NETWORK	Microsoft Corporation	Microsoft Corporation	One Microsoft Way, Redmond	a-0001.a-msedge.net
208.67.222.222	USA - California	OPENDNS-NET-1	OpenDNS, LLC	OpenDNS, LLC	145 Bluxome st., San Francisco	resolver1.opendns.com

Ряды шпионов поредели

Раз уж Fiddler помог добыть список IP, то их массовое добавление в файл hosts должно помочь прекратить слежку. Проверим, создав список блокировки, и снова запустим Wireshark.



Скромный улов Wireshark

По сравнению с первым логом этот выглядит скучно. На экране не уместился только один айпишник, а их общий список состоит всего из четырех. Два из них относятся к сети доставки контента и не могут эффективно блокироваться в hosts — слишком много подсетей принадлежит Akamai. Третий IP-адрес принадлежит службе Windows Update, которую не блокировали. Самым стойким шпионом оказался BingBot. Его связь с бразильской Microsoft Informatica не знает преград. Видимо, процесс содержит встроенные средства обхода ограничений.

ДОБИВАЕМ АГЕНТОВ МАТРИЦЫ

Справиться с оставшимися агентами Microsoft помогает ряд дополнительных мер. Нужно задать в брандмауэре блокировку подключений ко всем IP-адресам, выявленным Wireshark. У нас их получилось 47, но наверняка при более длительном мониторинге список увеличится. Еще есть шанс, что при очередном автоматическом обновлении в системных файлах пропишутся новые айпишники, но пока вместе с модификацией файла hosts это обеспечивает большую часть защиты от слежки.

Отключить «неотключаемые» функции можно через реестр.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection
```

Задав нулевое значение этому параметру, запретим отправку «технических» данных.

Желательно удалить файл сервиса DiagTrack с уже собранными данными. Вот путь к нему.

```
C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\ ↵
    AutoLogger-Diagtrack-Listener.etl
```

Отключить сами сервисы DiagTrack и dmwappushsvc можно через управление службами или ветку реестра.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
```

В планировщике заданий стоит посмотреть очередь задач и отключить все регулярные отправки данных, если они еще остались.

Рекомендуется деинсталлировать облачный клиент OneDrive, если ты все равно не собирался им пользоваться.

Все эти действия можно выполнить вручную, но сэкономить время сильно помогает утилита DisableWinTracking. В отличие от многих аналогов, она распространяется с открытым исходным кодом и хорошо документирована.

После выполнения всех описанных действий Windows 10 лишилась шпионских привычек. Вместе с ними, правда, исчезли почти все новые фишки, которые призваны повысить удобство работы и обеспечить безопасность. Впрочем, как говорил Франклин: «Те, кто готовы пожертвовать насущной свободой ради малой толики временной безопасности, не достойны ни свободы, ни безопасности».

WWW

Статья чешского обозревателя со списком следящих подключений

Бесплатная утилита IPNetInfo

Снифер Wireshark для Windows