ВЛИЯНИЕ НАСТРОЕК БРАУЗЕРА И ОПЕРАЦИОННОЙ СИСТЕМЫ, УСТАНОВЛЕННЫХ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ ПОЛЬЗОВАТЕЛЯ, НА ЕГО ИДЕНТИФИКАЦИЮ

Н.В. МИХАЛЬКОВ
Каф. Защиты информации
Факультет инфокоммуникаций
БГУИР, Минск, Беларусь

Цифровой отпечаток браузера имеет вид 32-битного числа шестнадцатеричной системы, например:

b2cf59b36581399ebf54d4ab425ac4a7

Отслеживаемые параметры

1) Заголовки браузера
2) Параметры экрана
3) Часовой пояс устройства
4) Язык используемый в ОС
5) Установленные плагины браузеров и др.

Методы для изменения отпечатка браузера

1) Изменение часового пояса устройства
2) Изменение разрешения экрана устройства
3) Обновление драйверов видеокарты
4) Изменение масштаба веб-страницы
5) Установка либо удаление плагинов браузера др.

Используемые web-приложения для идентификации

- Whoer.ru
- Ipper.ru

Методика проведения эксперимента

- 1. Получение информации о тестируемом компьютере пользователя
- 2. Оценка анонимности тестируемого компьютера пользователя
- 3. Оценка влияния параметров настройки браузера и ОС на «отпечаток браузера»

IP-адрес

Хост:	93-171-161-194.dynamic.unet.by
Обратный:	N/A
Почтовый узел:	ALT1.ASPMX.L.GOOGLE.COM
IP-диапазон:	93.171.160.0 - 93.171.161.255
Провайдер:	ALFA TELECOM s.r.o.
Организация:	ALFA TELECOM s.r.o.

Whois

Интерактивная проверка

Запустить

IP-адрес	93.171.161.194	Belarus
Flash	N/A	
WebRTC	192.168.1.45	
	93.171.161.194	Belarus
Java (TCP)	N/A	
Java (UDP)	N/A	
Java (system)	N/A	

Скрипты

JavaScript	включено
Flash	отключено
Java	отключено
ActiveX	отключено
WebRTC	включено
VBScript	отключено
AdBlock	отключено

Местоположение

Страна:	Belarus (BY) Еще
Континент:	Europe
Регион:	Minsk
Город:	Minsk
Индекс:	220002
Широта:	53.9000
Долгота:	27.5667
Карта:	Показать

DNS

Браузер	93.171.160.103	Belarus
	93.171.160.82	Belarus
Flash	N/A	
Java (request)	N/A	
Java (system)	N/A	

ОС

Заголовки:	Win7
JavaScript:	Win32 | Windows NT 6.1
Flash:	N/A
Java:	N/A
TCP/IP:	Windows 7 or 8 (PPPoE, MTU: 1492)

Порты

Открытые порты Нет

Язык

Заголовки:	us ru (ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7 | ru)
JavaScript:	ru
Flash:	N/A
Java:	N/A

Время

Часовой пояс:	Europe/Minsk
Локальное:	Tue Mar 13 2018 13:54:38 GMT+0300 (+03)
Системное:	Tue Mar 13 2018 14:01:56 GMT+0300 (Иорданское время (зима))
UTC:	Tue Mar 13 2018 10:54:38 UTC
GMT:	Tue Mar 13 2018 10:54:38 GMT
Дневное время:	Нет
Восход:	07:29:17
Закат:	19:09:10

Плагины

Chrome PDF Plugin	internal-pdf-viewer
Chrome PDF Viewer	mhjfbmdgcfjbbpaeojofohoefgiehjai
Native Client	internal-nacl-plugin
Widevine Content Decryption Module	widevinecdmadapter.dll

Навигатор

Экран

colorDepth	24
pixelDepth	24
height	768
width	1366
availHeight	728
availWidth	1366
top	N/A
left	N/A
availTop	0
availLeft	0
window size	1349x662 (1366x768)

HTTP заголовки

HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0
HTTP_ACCEPT_ENCODING	gzip
HTTP_ACCEPT_LANGUAGE	ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
HTTP_CACHE_CONTROL	max-age=0
HTTP_COOKIE	__cfduid=dff9ab05ae0e4015ae4778ca83a0622ef1
HTTP_HOST	whoer.net
HTTP_HTTPS	ON

vendorSub	
productSub	20030107
vendor	Google Inc.
maxTouchPoints	0
hardwareConcurrency	4
cookieEnabled	true
appCodeName	Mozilla
appName	Netscape
appVersion	5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36
platform	Win32
product	Gecko
userAgent	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36
language	ru
languages	ru-RU,ru,en-US,en
onLine	true
doNotTrack	null
geolocation	[object Geolocation]
mediaDevices	[object MediaDevices]
connection	[object NetworkInformation]
plugins	[object PluginArray]
mimeTypes	[object MimeTypeArray]

Локация:	Belarus (BY), Minsk
DNS:	80.94.174.35, Belarus
Провайдер:	Mobile TeleSystems JLLC
Host:	prometey.bsuir.by
OS:	Windows 7
Браузер:	Mozilla Firefox 58.0

User Agent:

Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

User Agent (метод JS):

Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

Плагины:

JavaScript	включено
Flash	включено
Java	выключено
ActiveX	выключено
VBScript	выключено
AdBlock	выключено
WebRTC	включено

Угроза анонимности 99% — Мы узнали Ваш реальный IP

Угроза | Исправить

IP по WebRTC: 172.16.235.175

Угроза анонимности 50% — Обнаружено использование VPN

Угроза | Исправить

Метод определения: **Двухсторонний PING**

Угроза анонимности 30% — Время сервера и браузера не совпадают

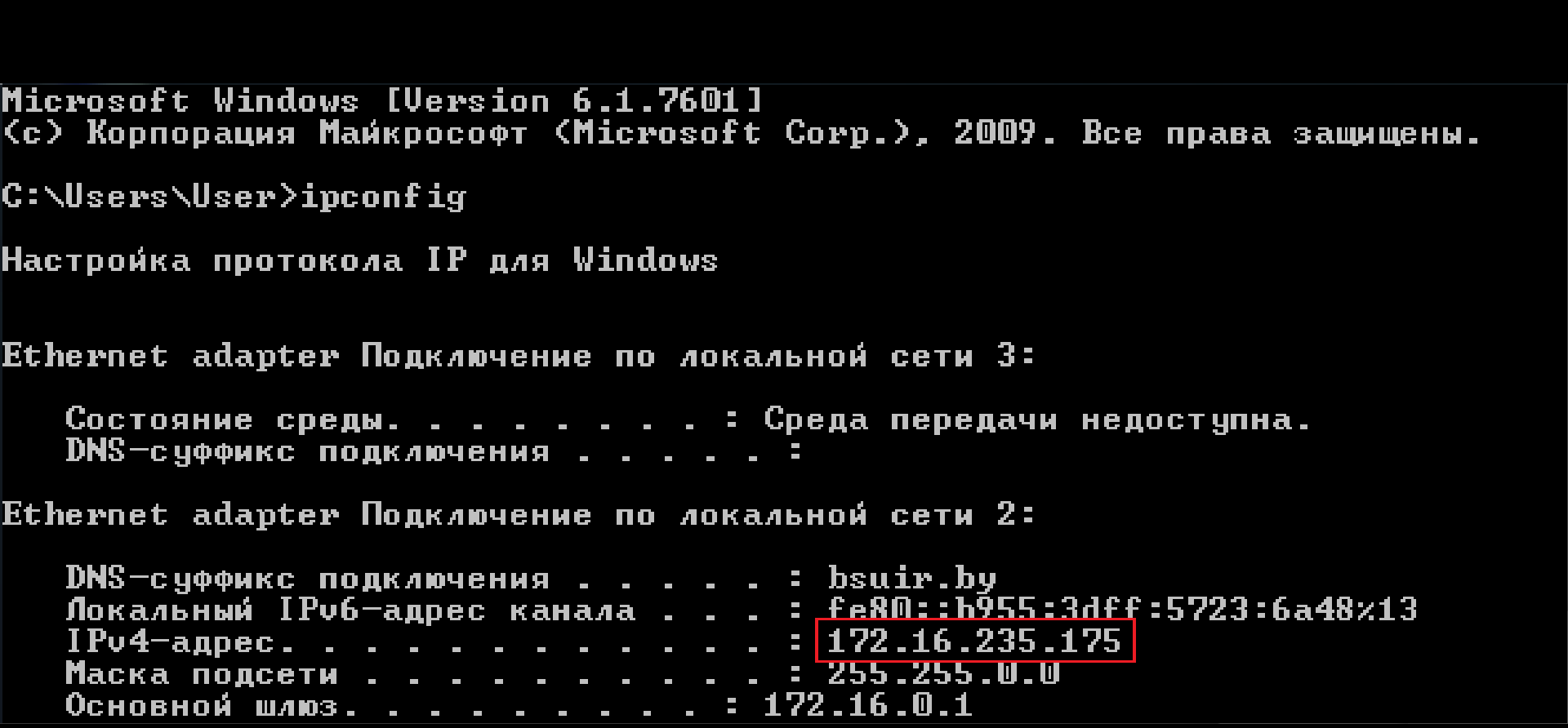
Угроза | Исправить

Временная зона сервера:	Europe/Minsk
Временная зона браузера:	Africa/Johannesburg

Угроза анонимности 30% — Языковая разница в браузере

Угроза | Исправить

Языковая разница: **Язык браузера RU, Сервера BY**


Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\User>ipconfig
Настройка протокола IP для Windows
Ethernet adapter Подключение по локальной сети 3:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Ethernet adapter Подключение по локальной сети 2:
DNS-суффикс подключения . . . . . : bsuir.by
Локальный IPv6-адрес канала . . . : fe80::b955:3dff:5723:6a48%13
IPv4-адрес. . . . . : 172.16.235.175
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 172.16.0.1

Оценка функционирования плагинов для браузеров

- WebRTC Control (Google Chrome)
- NoScript (Mozilla Firefox)

Локация:	Belarus (BY), Minsk
DNS:	80.94.174.35, Belarus
Провайдер:	Mobile TeleSystems JLLC
Host:	prometey.bsuir.by
OS:	Windows 7
Браузер:	Mozilla Firefox 58.0

User Agent:

Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

User Agent (метод JS):

Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

Плагины:

JavaScript	включено
Flash	включено
Java	выключено
ActiveX	выключено
VBScript	выключено
AdBlock	выключено
WebRTC	включено

Угроза анонимности 50% — Обнаружено использование VPN

Угроза | Исправить

Метод определения	Двухсторонний PING

Угроза анонимности 30% — Время сервера и браузера не совпадают

Угроза | Исправить

Временная зона сервера:	Europe/Minsk
Временная зона браузера:	Africa/Johannesburg

Угроза анонимности 30% — Языковая разница в браузере

Угроза | Исправить

Языковая разница	Язык браузера RU, Сервера BY

Мой IP: 93.171.161.194

Whois

Скрыть IP

Местоположение:	Belarus (BY), Minsk
Провайдер:	ALFA TELECOM s.r.o.
Хост:	93-171-161-194.dynamic.unet.by
ОС:	Win7
Браузер:	Firefox 58.0

Ваша анонимность: N/A — N/A

DNS:	N/A
Прокси:	Нет
Анонимайзер:	N/A
Черный список:	Нет

Местоположение

Страна:	Belarus (BY)
Регион:	Minsk
Город:	Minsk
Индекс:	220002
Хост:	93-171-161-194.dynamic.unet.by
Обратный:	N/A
IP-диапазон:	93.171.160.0 - 93.171.161.255
Провайдер:	ALFA TELECOM s.r.o.
Организация:	ALFA TELECOM s.r.o.

Whois

Язык

us ru

Время

Часовой пояс:	Europe/Minsk
Локальное:	Tue Mar 13 2018 13:28:23 GMT+0300 (+03)
Системное:	N/A

Браузер

Заголовки:	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
JavaScript:	N/A

Javascript	отключено
Flash	отключено
Java	отключено
ActiveX	отключено
WebRTC	отключено

Результаты исследования влияния параметров настройки веб-браузера и ОС

Параметр	Отпечаток браузера	Результат
первоначальное значение	512edbd4d93e7df0e1cf00ca86e7d04b	
изменение часового пояса	0e9b0f12112d99d676e0d86115c6ef45	положительный
изменение языка ОС	0e9b0f12112d99d676e0d86115c6ef45	отрицательный
установка другого языка браузера	1c88b1b37f5342a6a6f6fdf05415975b	положительный
изменение разрешения экрана устройства	9d257079ef598af59bd68542dcdd6095	Положительный

Результаты исследования влияния параметров настройки веб-браузера и ОС

Параметр	Отпечаток браузера	Результат
изменение масштаба веб-страницы	69ed82c100dee8c6c298eec0afca3f20	положительный
установка либо удаление плагинов браузера	6fabd19b207fccc86e8c9f058221bcb5	положительный
использование режима инкогнито	131dc9ac6d6f394dc22d2d738740b948	положительный
изменение шрифта Windows	90e0d35403371ccd91372ac50bfe4617	положительный

Спасибо за внимание