

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н.Тихонова

Домашнее задание №4, вариант 1. Основы цифровой форензики.
По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Сорокин А. В.

Подпись _____

Выполнил:

Новиков В. С. МКБ 241

Подпись _____

Задание «Вариант 1».

1. Каков IP-адрес зараженного узла?
2. Каков MAC-адрес зараженного узла?
3. Каково доменное имя зараженного узла?
4. Какие сайты посетил пользователь зараженного устройства по своему желанию?
5. Посещение каких сайтов зафиксировано в сетевом трафике?
6. Каково доменное имя сайта, с которого произошла загрузка вредоносного программного обеспечения?
7. Каков IP-адрес узла, с которого произошла загрузка вредоносного программного обеспечения?
8. Загружались ли пользователем или системой без ведома пользователя файлы, не являющиеся вредоносными?
9. Какие сайты (доменные имена) задействованы в заражении пользователя вредоносным программным обеспечением (имеют следы вредоносной активности, участвуют во вредоносных действиях)?
10. Каков механизм переходов (перенаправлений) пользователя с посещенных сайтов на сайт, с которого было загружено вредоносное программное обеспечение?

Решение

1. Каков IP-адрес зараженного узла?

Statistics → Endpoints → IPv4 → сортировка по Packets

Абсолютный лидер среди внутренних адресов — 172.16.165.165

Wireshark · Endpoints · var1.pcap

Endpoint Settings

☐ Разрешение имён

☐ Ограничить по фильтру от

Копировать

Карта

Протокол

☐ Bluetooth

☐ BIPv7

☐ DCCP

Ethernet · 11

IPv4 · 16

IPv6 · 4

TCP · 44

UDP · 28

Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено	Стр
255.255.255.255	1	342 байты	0	0 байты	1	342 байты	
74.125.233.99	3	162 байты	0	0 байты	3	162 байты	
172.16.165.254	3	1 кБ	2	684 байты	1	350 байты	
172.16.165.255	3	276 байты	0	0 байты	3	276 байты	
224.0.0.22	5	270 байты	0	0 байты	5	270 байты	
224.0.0.252	6	416 байты	0	0 байты	6	416 байты	
131.253.61.84	7	2 кБ	4	852 байты	3	919 байты	
185.53.178.9	17	6 кБ	9	5 кБ	8	797 байты	
74.125.233.100	25	13 кБ	14	12 кБ	11	1 кБ	
172.16.165.2	43	4 кБ	11	1 кБ	32	3 кБ	
188.225.73.100	95	81 кБ	62	78 кБ	33	3 кБ	
204.79.197.200	318	26 кБ	308	23 кБ	10	3 кБ	
82.150.140.30	400	309 кБ	260	294 кБ	140	16 кБ	
74.125.233.96	555	507 кБ	382	493 кБ	173	14 кБ	
37.200.69.143	1 531	2 МБ	1 112	2 МБ	419	28 кБ	
172.16.165.165	3 012	2 МБ	848	72 кБ	2 164	2 МБ	

Рисунок 1 «сортировка IP по Packets»

2. Каков MAC-адрес зараженного узла?

У IP-адреса 172.16.165.165 число входящих пакетов 2 МБ и исходящих ≈ 848 пакетов / 72 КБ.

Это почти совпадает со строкой f0:19:af:02:9b:f1 (разница в десяток пакетов объясняется тем, что IP-и Ethernet-таблицы считаются в разное время/фильтрации).

Wireshark · Endpoints · var1.pcap

Endpoint Settings

☐ Разрешение имён

☐ Ограничить по фильтру ото

Копировать

Карта

Ethernet · 11		IPv4 · 16		IPv6 · 4	TCP · 44	UDP · 28			
Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено	Стр		
00:0c:29:fb:9a:bf	1	60 байты	1	60 байты	0	0 байты			
00:0c:29:fe:9a:67	1	60 байты	1	60 байты	0	0 байты			
00:50:56:e9:71:c8	4	1 кБ	3	744 байты	1	350 байты			
33:33:00:00:00:16	5	450 байты	0	0 байты	5	450 байты			
01:00:5e:00:00:16	5	270 байты	0	0 байты	5	270 байты			
33:33:00:01:00:03	6	536 байты	0	0 байты	6	536 байты			
01:00:5e:00:00:fc	6	416 байты	0	0 байты	6	416 байты			
33:33:00:01:00:02	11	2 кБ	0	0 байты	11	2 кБ			
ff:ff:ff:ff:ff:ff	16	1 кБ	0	0 байты	16	1 кБ			
00:50:56:f3:ca:52	3 003	2 МБ	2 171	2 МБ	832	70 кБ			
f0:19:af:02:9b:f1	3 048	3 МБ	877	75 кБ	2 171	2 МБ			

Рисунок 2 «сортировка Ethernet по Packets»

3. Каково доменное имя зараженного узла?

Введем команду для вывода имени с учетом IP 172.16.165.165:

bootp.option.hostname && ip.addr==172.16.165.165

DHCP hostname не передавался, NBNS тоже пустой → имя не определяется («N/A»).

bootp.option.hostname && ip.addr==172.16.165.165						
No.	Time	Source	Destination	Protocol	Length	Info
2442	62.202238	172.16.165.165	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x92e7cbf7
3020	469.160328	172.16.165.165	172.16.165.254	DHCP	350	DHCP Request - Transaction ID 0xd71286ce

Wireshark · Пакет 3020 · var1.pcap

> Frame 3020: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)
✓ Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_e9:71:c8 (00:50:56:e9:71:c8)
✓ Destination: VMware_e9:71:c8 (00:50:56:e9:71:c8)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)

Рисунок 3 «bootp.option.hostname && ip.addr==172.16.165.165»

4. Какие сайты посетил пользователь зараженного устройства по своему желанию?

Введем фильтр, который выведет все HTTP-запросы и первый пакет любой HTTPS-сессии IP 172.16.165.165:

ip.src == 172.16.165.165 && (http.request || tls.handshake.type == 1)

http.request || tls.handshake.type == 1 означает, что есть начало HTTPS-сеанса со стороны клиента (поле Handshake Type = 1 (Client Hello))

var1.pcap						
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка						
ip.src == 172.16.165.165 && (http.request tls.handshake.type == 1)						
No.	Time	Source	Destination	Protocol	Length	Info
52	2.020811	172.16.165.165	204.79.197.200	HTTP/X-	1002	POST /fd/ls/lsp.aspx HTTP/1.1
109	4.237852	172.16.165.165	204.79.197.200	HTTP	861	GET /fd/ls/GLinkPing.aspx?IG=ae5908ea2d64991aa8b8996fd170a75&ID=SERP,5091.1 HTTP/1.1
161	6.073686	172.16.165.165	82.150.140.30	HTTP	621	GET / HTTP/1.1
225	7.484572	172.16.165.165	82.150.140.30	HTTP	432	GET /wp-content/themes/cini/style.css HTTP/1.1
238	7.495119	172.16.165.165	82.150.140.30	HTTP	467	GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
240	7.495288	172.16.165.165	82.150.140.30	HTTP	453	GET /wp-content/plugins/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
242	7.495489	172.16.165.165	82.150.140.30	HTTP	452	GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
243	7.495622	172.16.165.165	82.150.140.30	HTTP	438	GET /wp-content/themes/cini/js/functions.js HTTP/1.1
320	8.248504	172.16.165.165	82.150.140.30	HTTP	442	GET /wp-content/plugins/jquery/jquery.js?ver=1.10.2 HTTP/1.1
321	8.248599	172.16.165.165	82.150.140.30	HTTP	486	GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-2014.02.05 HTTP/1.1
322	8.248695	172.16.165.165	82.150.140.30	HTTP	466	GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
334	8.534284	172.16.165.165	185.53.178.9	HTTP	407	GET /new/jquery.php HTTP/1.1
342	8.720379	172.16.165.165	82.150.140.30	HTTP	432	GET /wp-content/themes/cini/reset.css HTTP/1.1
535	10.598424	172.16.165.165	82.150.140.30	HTTP	438	GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
537	10.598666	172.16.165.165	82.150.140.30	HTTP	440	GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
538	10.598797	172.16.165.165	82.150.140.30	HTTP	444	GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1
541	10.598981	172.16.165.165	82.150.140.30	HTTP	442	GET /wp-content/themes/cini/img/facebook_on.gif HTTP/1.1
543	10.599165	172.16.165.165	82.150.140.30	HTTP	441	GET /wp-content/themes/cini/img/twitter_on.gif HTTP/1.1
545	10.599362	172.16.165.165	82.150.140.30	HTTP	445	GET /wp-content/themes/cini/img/youtubelogo_on.gif HTTP/1.1

[2 Reassembled TCP Segments (1768 bytes): #51(820), #52(948)]
✓ Hypertext Transfer Protocol
POST /fd/ls/lsp.aspx HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://www.bing.com/search?q=ciniholland.nl&q=ds&form=QBLH
Content-Type: text/xml
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR
Host: www.bing.com
Content-Length: 948
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: _HOP=; _EDGE_S=F=1&SID=142DA6B92026172245CA0CF93E5607F; _EDGE_V=1; MUID=3A80A34C8F5061
[Response in frame: 87]
[Full request URI: http://www.bing.com/fd/ls/lsp.aspx]
File Data: 948 bytes
eXtensible Markup Language

0000 00 50 56 f3 ca 52 f0 19 af 02 9b f1 08 00 45 00 :PV-R.....E-
0010 03 dc 14 20 40 00 80 06 ff 2d ac 10 a5 a5 cc 4f : @.....0
0020 c5 e8 c1 17 00 50 c3 e1 a5 88 e0 f0 aa 74 50 18 :....P.....TP
0030 f7 62 e8 8e 00 00 3c 43 6c 69 65 6e 74 49 6e 73 :b.....C lientIns
0040 74 52 65 71 75 65 73 74 3e 3c 45 76 65 6e 74 73 :>E><T>E vent.Cli
0050 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 6c 69 :>E><T>E vent.Cli
0060 65 6e 74 49 6e 73 74 3c 2f 54 3e 3c 49 47 3e 61 :entInst< /T><IG>a
0070 65 65 35 39 30 38 65 61 32 64 36 34 39 39 31 61 :ee5908ea 2d64991a
0080 61 38 62 38 39 39 36 66 64 31 37 30 61 37 35 3c :a8b8996f d170a75<
0090 2f 49 47 3e 3c 54 53 3e 31 34 31 36 31 30 33 39 :/IG>TS> 14161039
00a0 31 31 33 34 39 3c 2f 54 53 3e 3c 44 3e 7b 22 54 :11349</T S><D>{"T
00b0 22 3a 20 22 43 49 2e 42 6f 78 4d 6f 64 65 6c 22 : "CI.B oxModel"
00c0 2c 20 22 46 49 44 22 3a 20 22 43 49 22 2c 20 22 : "FID": "CI", "
00d0 4e 61 6d 65 22 3a 20 22 50 65 72 66 22 2c 20 22 : "Name": "Perf", "
00e0 54 65 78 74 22 3a 20 22 53 25 31 41 30 58 30 58 :Text": " S3A0X0X
00f0 36 36 30 58 32 37 38 25 33 42 42 4f 44 59 2e 25 :660X278% 3880Y.%
0100 32 30 25 33 41 30 58 30 58 39 39 30 58 34 39 39 :263A0X0 X990X499
0110 25 33 42 44 49 56 2e 62 5f 73 63 6f 70 65 62 61 :X380IV.b scopeba
0120 72 25 33 41 30 58 30 58 34 33 37 58 33 30 25 :r3A0X80 X437X30%
0130 33 42 48 31 2e 62 5f 6c 6f 67 65 25 33 41 31 37 :3BH1.b_l ogo3A17
0140 58 31 39 58 37 33 58 32 39 25 33 42 44 49 56 2e :X19X73X2 9%380IV.
0150 62 5f 73 65 61 72 63 68 62 6f 78 46 6f 72 6d 25 :b_search boxForm%
0160 33 41 31 30 30 58 31 39 58 36 34 39 58 33 30 25 :3A100X19 X649X30%

Frame (1002 bytes) Reassembled TCP (1768 bytes) Decoded UTF-8 text (948 bytes)
Пакеты: 3053 · Отображено: 39 (1.3%)

Рисунок 4 «ip.src == 172.16.165.165 && (http.request || tls.handshake.type == 1)»

Ответ (пользователь зараженного устройства посетил по своему желанию):

- www.bing.com поиск
- www.ciniholland.nl клик по выдаче

5. Посещение каких сайтов зафиксировано в сетевом трафике?

В Wireshark перейти по Statistics → HTTP → Requests.

Вывод:

www.bing.com - страница поиска

www.ciniholland.nl - «ручной» переход

stand.trustandprobaterealty.com - конечный malware-хост, отдаёт JAR/SWF/MP3

adultbiz.in - промежуточный зловердный скрипт (`/new/jquery.php`)

24corp-shop.com - redirect-вставка (+ gif «notfound»)

www.youtube.com - встраиваемый плеер (`/embed/...`)

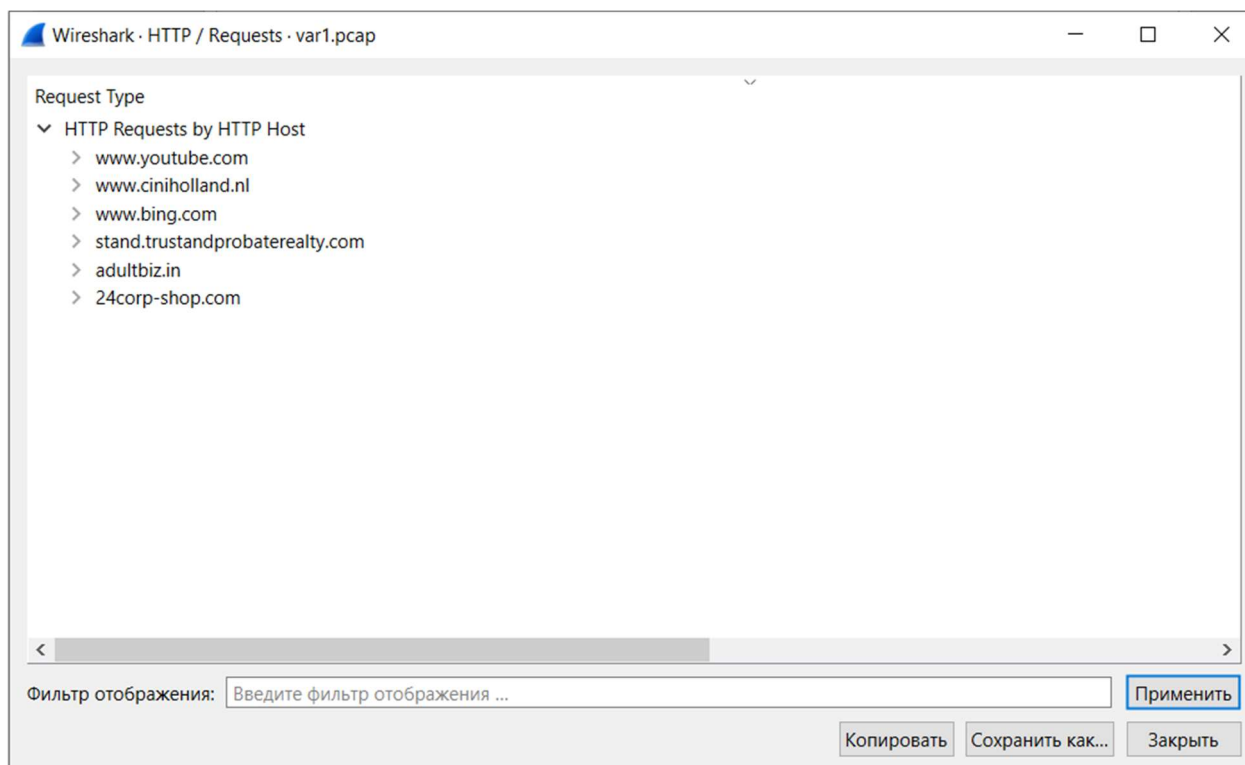


Рисунок 5 «Statistics → HTTP → Requests»

6. Каково доменное имя сайта, с которого произошла загрузка вредоносного программного обеспечения?

Ответ: stand.trustandprobaterealty.com

В Wireshark откроем File → Export Objects → HTTP. Сортировка по Типу содержимого:

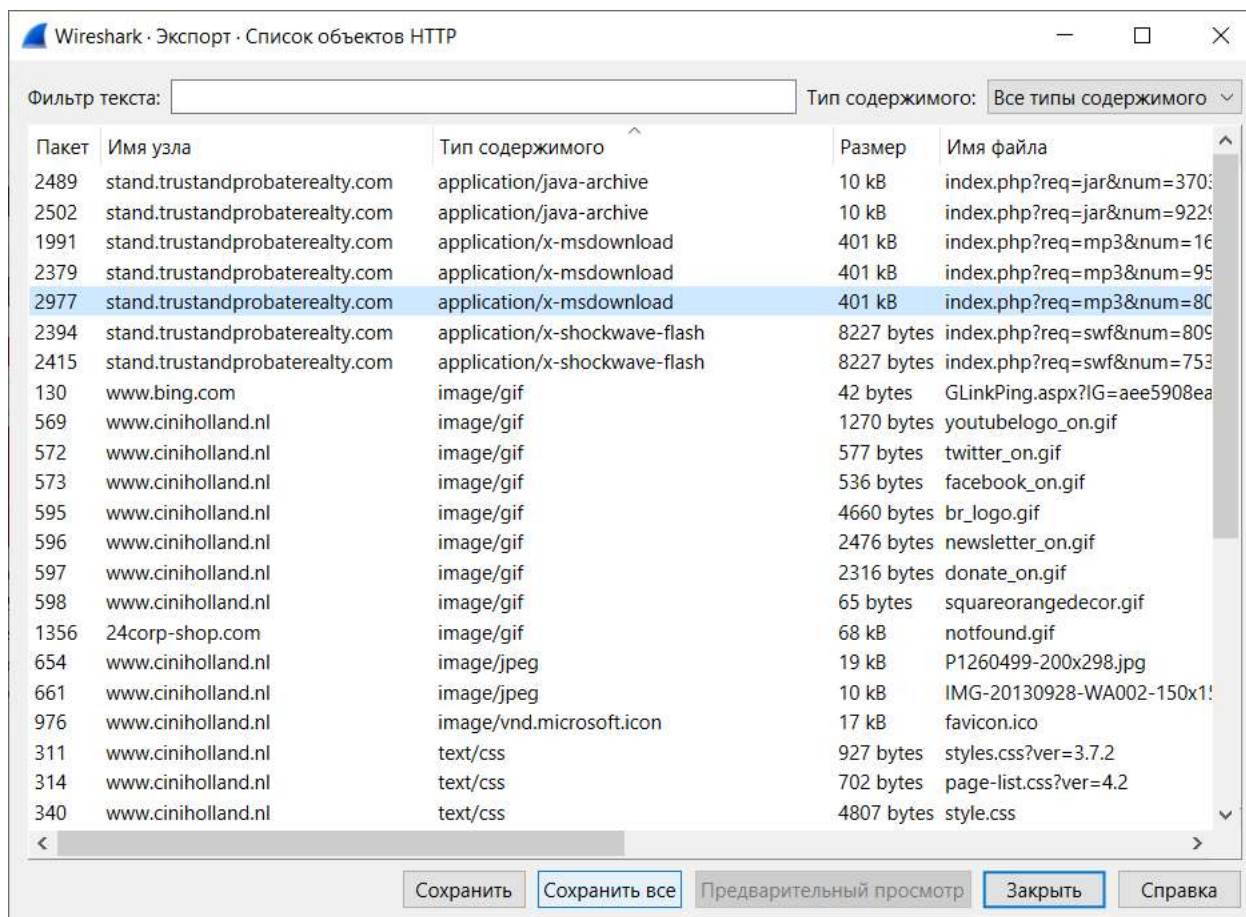


Рисунок 6 «File → Export Objects → HTTP»

7. Каков IP-адрес узла, с которого произошла загрузка вредоносного программного обеспечения?

В Wireshark откроем File → Export Objects → HTTP. Сортировка по Типу содержимого и выбираем загрузки. В Wireshark отобразиться IP адрес с которого произошла загрузка вредоносного программного обеспечения - **37.200.69.143**

Host = stand.trustandprobaterealty.com

IP.dst = 37.200.69.143

2968	84.341168	37.200.69.143	172.16.165.165	TCP	1409 80 → 49456 [PSH,	Wireshark - Экспорт - Список объектов HTTP
2969	84.341199	172.16.165.165	37.200.69.143	TCP	54 49456 → 80 [ACK]	
2970	84.341958	37.200.69.143	172.16.165.165	TCP	1409 80 → 49456 [PSH,	
2971	84.342058	37.200.69.143	172.16.165.165	TCP	1514 80 → 49456 [ACK]	
2972	84.342059	37.200.69.143	172.16.165.165	TCP	1304 80 → 49456 [PSH,	
2973	84.342068	172.16.165.165	37.200.69.143	TCP	54 49456 → 80 [ACK]	
2974	84.342691	37.200.69.143	172.16.165.165	TCP	1409 80 → 49456 [PSH,	
2975	84.442860	37.200.69.143	172.16.165.165	TCP	1409 [TCP Retransmiss	
2976	84.442878	172.16.165.165	37.200.69.143	TCP	54 49456 → 80 [ACK]	
2977	84.464154	37.200.69.143	172.16.165.165	HTTP	941 HTTP/1.1 200 OK	
2978	84.565718	37.200.69.143	172.16.165.165	TCP	941 [TCP Retransmiss	
2979	84.565738	172.16.165.165	37.200.69.143	TCP	54 49456 → 80 [ACK]	
2980	84.638665	172.16.165.165	37.200.69.143	TCP	54 49456 → 80 [RST,	
2981	86.766872	82.150.140.30	172.16.165.165	TCP	60 80 → 49438 [FIN,	
2982	86.766894	172.16.165.165	82.150.140.30	TCP	54 49438 → 80 [ACK]	
2983	88.612146	172.16.165.165	74.125.233.96	TCP	54 49447 → 443 [RST	
2984	88.612273	172.16.165.165	74.125.233.96	TCP	54 49446 → 443 [RST	
2985	88.612345	172.16.165.165	82.150.140.30	TCP	54 49438 → 80 [RST,	
2986	88.612471	172.16.165.165	74.125.233.100	TCP	54 49448 → 443 [RST	

Пакет	Имя узла	Тип содержимого
2489	stand.trustandprobateerale.com	application/java-archive
2502	stand.trustandprobateerale.com	application/java-archive
1991	stand.trustandprobateerale.com	application/x-msdownload
2379	stand.trustandprobateerale.com	application/x-msdownload
2977	stand.trustandprobateerale.com	application/x-msdownload
2394	stand.trustandprobateerale.com	application/x-shockwave-flash
2415	stand.trustandprobateerale.com	application/x-shockwave-flash
130	www.bing.com	image/gif
569	www.ciniholland.nl	image/gif
572	www.ciniholland.nl	image/gif
573	www.ciniholland.nl	image/gif
595	www.ciniholland.nl	image/gif
596	www.ciniholland.nl	image/gif
597	www.ciniholland.nl	image/gif
598	www.ciniholland.nl	image/gif
1356	24corp-shop.com	image/gif
654	www.ciniholland.nl	image/jpeg
661	www.ciniholland.nl	image/jpeg
976	www.ciniholland.nl	image/vnd.microsoft.icon

Рисунок 7 «File → Export Objects → HTTP и вывод в Wireshark IP адреса»

8. Загружались ли пользователем или системой без ведома пользователя файлы, не являющиеся вредоносными?

Да, загружались «мирные» файлы фоном (не вредоносные)

В Wireshark откроем File → Export Objects → HTTP.

- IMG-20130928-WA002-150x150.jpg
- newsletter_on.gif
- P1260499-200x298.jpg
- squareorangedecor.gif
- twitter_on.gif
- youtubelogo_on.gif
- и скрипты JS

Эти объекты загружались **автоматически** для отображения страницы и сбора аналитики; пользователь о них не заботился, и они не несут вредоносного кода

52	www.bing.com	text/xml	948 bytes	lsp.aspx
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b899
533	www.ciniholland.nl	text/javascript	93 kB	jquery.js?ver=1.10.2
318	www.ciniholland.nl	text/html	61 kB	\
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
445	www.ciniholland.nl	text/javascript	16 kB	jquery.form.min.js?ver=3.50.0-2014.02.05
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
432	www.ciniholland.nl	text/javascript	8913 bytes	scripts.js?ver=3.7.2
341	www.ciniholland.nl	text/javascript	7200 bytes	jquery-migrate.min.js?ver=1.2.1
340	www.ciniholland.nl	text/css	4807 bytes	style.css
595	www.ciniholland.nl	image/gif	4660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2316 bytes	donate_on.gif
569	www.ciniholland.nl	image/gif	1270 bytes	youtubelogo_on.gif
401	www.ciniholland.nl	text/css	1092 bytes	reset.css
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3.7.2
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ver=4.2
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
313	www.ciniholland.nl	text/javascript	237 bytes	functions.js
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif

Рисунок 8 «File → Export Objects → HTTP»

9. Какие сайты (доменные имена) задействованы в заражении пользователя вредоносным программным обеспечением (имеют следы вредоносной активности, участвуют во вредоносных действиях)?

Собираем цепочку по полю Referer:

www.ciniholland.nl

24corp-shop.com

stand.trustandprobaterealty.com

adultbiz.in есть в DNS, но HTTP-трафика не было, значит не задействован.

10. Каков механизм переходов (перенаправлений) пользователя с посещенных сайтов на сайт, с которого было загружено вредоносное программное обеспечение?

Пользователь открыл www.ciniholland.nl из поиска Bing. Страница незаметно вставила iframe на 24corp-shop.com, который вернул HTTP 302 на stand.trustandprobaterealty.com. Последний отдал несколько файлов, среди которых находилось вредоносное ПО ([Exploit:JS/Meadgive.P](#), [Trojan:Win32/Ceevee](#), [Exploit:Java/CVE-2012-0507](#)).

Переход	Техника	Как видно в пакете
<i>ciniholland</i> → 24corp	Iframe	в HTML ответа www.ciniholland.nl - строка <iframe src="http://24corp-shop.com/">
24corp → stand.trustandprobaterealty	HTTP 302	ответ HTTP/1.1 302 Found с Location: http://stand.trustandprobaterealty.com/...
stand.trustandprobaterealty → payload	многократные GET (...req=jar, ...req=swf, ...req=mp3)	обычные HTTP 200 и скачивание бинарей