

Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

Практическая работа №3
для слушателей программы повышения квалификации
«Основы компьютерной криминалистики
и методики реагирования на инциденты информационной
безопасности»



Брянск
БГТУ
2022

Брянский государственный технический университет
241035, Брянск, бульвар 50 лет Октября, 7.
Кафедра «Системы информационной безопасности», тел. 58-82-16.

Заполнить протокол, используя программы лекции 3
ПРОТОКОЛ № 2 от 2021 г.

Комиссия в составе:
Начала осмотр в:
Осмотр окончен:
Особенности осмотра:
Описание конфигурации устройств и программного обеспечения компьютера:
Объект осмотра:
Имя компьютера, на котором проводится осмотр:
оперативная память:
Программы участвующие в анализе сетевого дампа:

Перед комиссией поставлены следующие вопросы:

1. Является ли представленный дамп работоспособным?

Да, является

newpcap

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ...<Ctrl+>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	154.179.83.221	114.91.242.102	TCP	74	34745 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 WS=128 SACK_PERM=1 TSval=5546793 TSecr=0
2	0.000115	114.91.242.102	154.179.83.221	TCP	74	445 → 34745 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1393597 TSecr=5546793
3	0.000123	154.179.83.221	114.91.242.102	TCP	66	34745 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5546794 TSecr=1393597
4	0.001204	154.179.83.221	114.91.242.102	SNB	154	Negotiate Protocol Request
5	0.001351	114.91.242.102	154.179.83.221	SNB	275	Negotiate Protocol Response
6	0.003720	154.179.83.221	114.91.242.102	TCP	66	34745 → 445 [ACK] Seq=89 Ack=210 Win=30336 Len=0 TSval=5546794 TSecr=1393597
7	0.003721	154.179.83.221	114.91.242.102	SNB	213	Session Setup AndX Request, NTLMSSP_NEGOTIATE
8	0.003721	114.91.242.102	154.179.83.221	SNB	380	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
9	0.005721	154.179.83.221	114.91.242.102	SNB	478	Session Setup AndX Request, NTLMSSP_AUTH, User: .\
10	0.006224	114.91.242.102	154.179.83.221	SNB	105	Session Setup AndX Response, Error: STATUS_LOGON_TYPE_NOT_GRANTED
11	0.011730	154.179.83.221	114.91.242.102	SNB	169	Session Setup AndX Request, User: .\
12	0.011731	114.91.242.102	154.179.83.221	SNB	171	Session Setup AndX Response
13	0.011731	154.179.83.221	114.91.242.102	SNB	142	Tree Connect AndX Request, Path: \\114.91.242.102\IPC\$
14	0.011731	114.91.242.102	154.179.83.221	SNB	116	Tree Connect AndX Response

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: VMware_92:67:e1 (00:0c:29:92:67:e1), Dst: VMware_Id:b9:59 (00:0c:29:1d:b9:59)
> Internet Protocol Version 4, Src: 154.179.83.221, Dst: 114.91.242.102
> Transmission Control Protocol, Src Port: 34745, Dst Port: 445, Seq: 0, Len: 0

0000 00 0c 29 1d b9 59 00 0c 29 92 67 e1 08 00 45 00 --)Y-)g--E-
0010 00 3c eb 50 40 00 40 06 fc 18 9a b3 53 dd 72 5b <P@- -S-r[
0020 f2 66 87 b9 01 bd 72 d5 48 79 00 00 00 a0 02 -F...P. Hy.....
0030 72 10 1b 87 00 00 02 04 05 b4 01 03 03 07 04 02 r.....
0040 00 0a 00 54 a3 29 00 00 00 00T.)- -

- Да, присутствуют. Вирусный файл ddd.exe, который запускался через powershell

```

.....".a.....V.>.r.....6v.?.].
1.....f.....V.....N.E.G.A.T.I.V.E.....W.E.B.....n.e.g.a.t.i.v.e...t.e.c.h.."W.E.B.....n.e.g.a.t.i.v.e...t.e.c.h.....n.e
.g.a.t.i.v.e...t.e.c.h.....Sy.....S.c.o.3.U.V.C.n.7.w.v.z.N.S.o.m.Windows 2000 2195.Windows 2000
5.0.....#.SMBs[.....h.....c.SMBs.....
.....@.....&.....Windows 2000 2195.Windows 2000 5.0.....e.SMBs.....e.....<.Windows 8 Enterprise
9200.Windows 8 Enterprise 6.2.NEGATIVE.....H.SMBu.....(.....\\114.91.242.102\IPC$.?????.....SMBu.....
(......IPC.....(.....\SMB.....
.netlogon.....SMB.....
(......*.....@.....
SMB.....H.....
.....<?.....P.....@......VLHpMgLSIuhR0nWmpqct0JXLDXQIqfcesZCS0SGZuLpgimyyHTqXmZcPCUknAYuYQub0wsZCrimYKUUbYlRte
BpmmVbofQzgarXvmmIagLWYNpZsmGKnfaaBdMARMvHXHCignIjGxTkSDYNstZVavQtIjTkhvLeMTfnZHIQNrvtJPGmBwZtLghTsbCdmtzgvbTXXvjhaFecMrXQWJWcqwP
ATRZmbMeauSHRFaZnmYzsanlmyghnCqKbNZMxhKcMlLWiZjsxTGPPhixQhXUioukxpoQgsBuVDxhSiHbaGKkQkJPDEnqoVLioMvfrnRWJtgrAonOZApDngeogibQspjNGH

```

[illegible]

tcp.stream eq 1									
Байты пакета		Узкий & Широкий	<input type="checkbox"/> Чувствительный к регистру букв	Строка		ddd.exe			
Time	Source	Destination	Protocol	Length	Info				
284.0.489189	114.91.242.102	179.241.18.181	TCP	66	1922 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1				
285.0.489190	179.241.18.181	114.91.242.102	TCP	66	80 → 1922 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 WS=128 SACK_PERM=1				
286.0.489190	114.91.242.102	179.241.18.181	TCP	54	1922 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0				
287.0.489191	114.91.242.102	179.241.18.181	HTTP	208	GET /ddd.exe HTTP/1.1				
288.0.489191	179.241.18.181	114.91.242.102	TCP	60	80 → 1922 [ACK] Seq=1 Ack=155 Win=30336 Len=0				
289.0.489663	179.241.18.181	114.91.242.102	TCP	71	80 → 1922 [PSH, ACK] Seq=1 Ack=155 Win=30336 Len=17 [TCP segment of a reassembled PDU]				
290.0.489664	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=18 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
291.0.489664	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=1478 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
292.0.489664	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=2938 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
293.0.489666	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=4308 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
294.0.489667	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=5858 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
295.0.489667	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=7318 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
296.0.489667	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=8778 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
297.0.489668	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=10238 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
298.0.489668	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=11698 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
299.0.489878	114.91.242.102	179.241.18.181	TCP	54	1922 → 80 [ACK] Seq=155 Ack=13158 Win=65536 Len=0				
300.0.489879	179.241.18.181	114.91.242.102	TCP	1514	80 → 1922 [ACK] Seq=13158 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]				
▼ [Expert Info (Chat/Sequence): GET /ddd.exe HTTP/1.1\r\n]									
[GET /ddd.exe HTTP/1.1\r\n]									
[Severity level: Chat]									
[Group: Sequence]									
Request Method: GET									
Request URI: /ddd.exe									
000	00 0c 29 79 fd 9e 00 0c	29 1d b9 59 08 05 40 00	-->y----	--Y--E-					
010	00 c2 02 28 40 00 80 06	cc a5 72 5b f2 66 b3 f1	---(---r[.f-						
020	12 b5 07 82 00 50 81 11	73 2c 8e 70 bb 87 50 18	-----P_s_p.-P-						
030	01 00 c1 2f 00 00 47 45	54 20 2f 64 64 64 2e 65	/-GE 1 /ddd.e						
040	78 65 20 48 54 54 50 2f	31 2e 31 0d 0a 55 73 65	xe HTTP/1.1 Use						
050	72 2d 41 67 65 6e 74 3a	20 4d 6f 7a 69 6c 6c 61	r-Agent: Mozilla						
060	2f 35 30 20 28 20 69 6b	6e 64 6f 77 73 20 4e 54	/5.0 (Windows NT						
070	3b 20 57 69 6e 64 6f 77	73 20 4e 54 20 36 2e 32	; Windows NT 6.2						
080	3b 20 65 6e 6d 55 53 29	20 57 69 6e 64 6f 77 73	; en-US; Windows						
090	50 6f 77 65 72 53 68 65	6c 6c 2f 33 2e 30 0d 0a	PowerShell/3.0.						
0a0	48 6f 73 74 3a 20 31 3f	39 2e 32 34 31 2e 31 38	Host: 17.9.241.18						

387 0.491433	179.241.18.181	114.91.242.102	TCP	1514 80 → 1922 [ACK] Seq=132878 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
388 0.491434	179.241.18.181	114.91.242.102	TCP	1458 [TCP Window Full] 80 → 1922 [ACK] Seq=134338 Ack=155 Win=30336 Len=1484 [TCP segment of a reassembled PDU]
389 0.491434	114.91.242.102	179.241.18.181	TCP	54 [TCP ZeroWindow] 1922 → 80 [ACK] Seq=155 Ack=135742 Win=0 Len=0
390 0.496213	114.91.242.102	179.241.18.181	TCP	54 [TCP Window Update] 1922 → 80 [ACK] Seq=155 Ack=135742 Win=65536 Len=0

networkminer 1.1.2										
File Tools Help										
Select a network adapter in the list --										
Hosts (63) Files (26) Images (1) Messages (2) Credentials (63) Sessions (733) DNS (1073) Parameters (1108) Keywords Anomalies										
Filter keyword										
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed file
287	ddd[1].exe	exe	718 336 B	179.241.18.181 [179.241.18.181]	TCP 80	114.91.242.102 (Windows)	TCP 1922	HttpGetNormal	2018-02-19 17:32:06 UTC	D:\Kypc KK\Pass

+файлы удалены антивирусом при запуске networkminer

Полный журнал

Здесь показан список элементов, которые антивирусная программа "Защитника Windows" определила как угрозы на вашем устройстве.

Очистить журнал

TrojanDropper:PowerShell/Ploty.C
04.04.2022 22:05 (Удалено)

Критический
^

Trojan:Script/Wacatac.B!ml
04.04.2022 22:05 (Удалено)

Критический
v

Exploit:O97M/DDEDownloader.R
04.04.2022 22:05 (Удалено)

Критический
v

Backdoor:Win32/Fynloski.A
04.04.2022 22:05 (Удалено)

Критический
v

3. Содержат ли какие-то процессы подозрительные расположения файлов?

Да, во всех этих процессах антивирус находит зараженные файлы:

53068	2018_0178[1].png	png	746 784 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2097	HttpGetNormal	2018-02-19 17:32:06 UTC
57466	favicon.ico[3].html	html	101 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2098	HttpGetNormal	2018-02-19 17:32:06 UTC
59207	Report_20180206_122018[1].xlsx	xlsx	30 472 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 445	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2122	SMB2	2018-02-19 17:32:06 UTC
71939	financial_report[1].rtf	rtf	583 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 51101	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 25	SMTP	2018-02-19 17:32:06 UTC
71939	Simeport[1].eml	eml	1 854 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 51101	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 25	SMTP	2018-02-19 17:32:06 UTC
72643	financial_report[1].rtf	rtf	583 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 110	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50125	POP3	2018-02-19 17:32:06 UTC
72643	Simeport[1].eml	eml	2 008 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 110	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50125	POP3	2018-02-19 17:32:06 UTC
72747	gpt[3].ini	ini	22 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 445	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 49408	SMB2	2018-02-19 17:32:06 UTC
72817	3Aabol.sct[1].txt	txt	340 B	154.179.83.221 [SCo3UVCh7wvzNSom] [154.179.83.221:...	TCP 8080	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50083	HttpGetNormal	2018-02-19 17:32:06 UTC
72824	3Aabol[1].octet-stream	octet-stream	2 042 B	154.179.83.221 [SCo3UVCh7wvzNSom] [154.179.83.221:...	TCP 8080	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50084	HttpGetNormal	2018-02-19 17:32:06 UTC
72985	dnscat2.ps[1].octet-stream	octet-stream	1 218 B	179.241.18.181 [179.241.18.181]	TCP 80	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 49502	HttpGetNormal	2018-02-19 17:32:06 UTC

Например, dnscat2.ps – бэкдор для dns-туннеля

4. Возможно ли установить хронологию событий до утечки информации, возможно ли ее описать?

Злоумышленник проводил сканирование портов

Ethernet · 27		IPv4 · 25		IPv6 · 4		TCP · 787		UDP · 1123						
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
192.168.183.103	1994	192.168.183.101	139	24	3490	13	1681	11	1809	003.45621	12.0393	1117		
192.168.183.103	57627	192.168.183.108	587	2	118	1	58	1	60	016.36920	0.0000	—		
192.168.183.102	49488	192.168.183.100	445	28	7257	16	4835	12	2422	026.31669	12.0249	3216		
192.168.183.103	40634	192.168.183.101	80	2	112	1	58	1	54	107.94075	0.0000	—		
192.168.183.103	40634	192.168.183.102	80	2	112	1	58	1	54	107.94075	0.0000	—		
192.168.183.103	40634	192.168.183.108	80	3	172	2	112	1	60	107.94075	0.0000	—		
192.168.183.103	40634	192.168.183.254	80	1	58	1	58	0	0	107.94075	0.0000	—		
192.168.183.103	40634	192.168.183.100	80	2	112	1	58	1	54	107.94075	0.0000	—		
192.168.183.103	40634	192.168.183.101	1723	2	112	1	58	1	54	107.94078	0.0000	—		
192.168.183.103	40634	192.168.183.102	1723	2	112	1	58	1	54	107.94078	0.0000	—		
192.168.183.103	40634	192.168.183.108	1723	2	118	1	58	1	60	107.94078	0.0000	—		
192.168.183.103	40634	192.168.183.254	1723	1	58	1	58	0	0	107.94078	0.0000	—		
192.168.183.103	40634	192.168.183.100	1723	2	112	1	58	1	54	107.94079	0.0000	—		
192.168.183.103	40634	192.168.183.108	995	2	118	1	58	1	60	107.95735	0.0000	—		
192.168.183.103	40634	192.168.183.254	995	1	58	1	58	0	0	107.95735	0.0000	—		
192.168.183.103	40634	192.168.183.100	995	2	112	1	58	1	54	107.95735	0.0000	—		
192.168.183.103	40634	192.168.183.101	995	2	112	1	58	1	54	107.95735	0.0000	—		
192.168.183.103	40634	192.168.183.102	995	2	112	1	58	1	54	107.95735	0.0005	—		
192.168.183.103	40634	192.168.183.108	445	3	172	2	112	1	60	107.95735	0.0006	—		
192.168.183.103	40634	192.168.183.254	445	1	58	1	58	0	0	107.95735	0.0000	—		
192.168.183.103	40634	192.168.183.100	445	3	170	2	112	1	58	107.95792	0.0000	—		
192.168.183.103	40634	192.168.183.101	445	3	170	2	112	1	58	107.95792	0.0000	—		
192.168.183.103	40634	192.168.183.102	445	3	170	2	112	1	58	107.95792	0.0000	—		
192.168.183.103	40634	192.168.183.108	587	2	118	1	58	1	60	107.95792	0.0000	—		
192.168.183.103	40634	192.168.183.254	587	1	58	1	58	0	0	107.95794	0.0000	—		

Злоумышленник начиная с 19.02.2018 17:52:19 проводит подбор пароля на компьютере с linux 192.168.183.108

32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	root	root	Unknown	2018-02-19 17:52:19 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	admin	admin	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	administrator	administrator	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	webadmin	webadmin	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	sysadmin	sysadmin	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	netadmin	netadmin	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	guest	guest	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	user	user	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	web	web	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	test	test	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	root		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	admin		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	administrator		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	webadmin		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	sysadmin		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	netadmin		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	guest		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	user		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	web		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	test		Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	root	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	admin	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	administrator	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	webadmin	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	sysadmin	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	netadmin	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	guest	123456	Unknown	2018-02-19 17:53:41 UTC
32.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	user	123456	Unknown	2018-02-19 17:53:41 UTC

Далее 19.02.2018 17:54:45 с 192.168.183.108 был загружен файл – картинка, формат .png

52593	favicon.ico[2].html	html	101 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2096	HttpGetNormal	2018-0
53068	2018_0178[1].png	png	706 784 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2097	HttpGetNormal	2018-0
57466	favicon.ico[3].html	html	101 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2098	HttpGetNormal	2018-0
69207	Report_20180206_122018[1].xlsx	xlsx	30 472 B	192.168.183.101 [ACC] [ACC<20>] [ACC negative.tech] [A...	TCP 445	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2122	SMB2	2018-0

В картинке был сохранен пароль от системы авторизации-аутентификации,

FileToolsHelp

Select a network adapter in the list

Hosts (63)Files (26)Images (1)Messages (2)Credentials (63)Sessions (733)DNS (1073)Parameters (1108)KeywordsAnomalies

2018_0178[1].png

3024x3024, 706 784 B

Так как далее злоумышленник 19.02.2018 17:55:54 взаимодействует с Kerberos, получая доступы к компьютерам 192.168.183.100, 192.168.183.101, 192.168.183.103

192.168.183.103 [WEB] [WEB<20>] [WEB<20>] (Windows)	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	Kerberos	accountant	Skrb5pa\$18\$accountant\$NEGATIVE\$NEGATIVE	Unknown	2018-02-19 17:55:54
192.168.183.103 [WEB] [WEB<20>] [WEB<20>] (Windows)	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	Kerberos	accountant	Skrb5asrep\$18\$NEGATIVE.TECHaccountant\$#7b...	Unknown	2018-02-19 17:55:54

И после к компьютеру бухгалтера

192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [AC...	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	SMTP	accountant@negative.tech	L_Löve_P33a	Unknown	2018-02-19 18:05:03 UTC
192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [AC...	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	SMTP	accountant		Unknown	2018-02-19 18:05:03 UTC

5. Как злоумышленник проник на компьютер директора?

С компьютера бухг был отправлен зараженный email на компьютер директора 192.168.183.102

71939	financial_report[1].rtf	rtf	583 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 51101	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 25	SMTP	2018-02-19 18:05:03 UTC	D:
71939	Simeport[1].eml	eml	1 854 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 51101	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 25	SMTP	2018-02-19 18:05:03 UTC	D:
72643	financial_report[1].rtf	rtf	583 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 110	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50125	POP3	2018-02-19 18:05:44 UTC	D:
72643	Simeport[1].eml	eml	2 008 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 110	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50125	POP3	2018-02-19 18:05:44 UTC	D:

72817	3Abol[1].txt	txt	340 B	154.179.83.221 [SCo3UVGn7wvzNSon] [154.179.83.221...	TCP 8080	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50083	HttpGetNormal	2018-02-19 18:07:28 UTC	D:\Крпс КК\Passa
72824	3Abol[1].octet-stream	octet-stream	2 042 B	154.179.83.221 [SCo3UVGn7wvzNSon] [154.179.83.221...	TCP 8080	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50084	HttpGetNormal	2018-02-19 18:07:29 UTC	D:\Крпс КК\Passa
72985	dnscat2.ps[1].octet-stream	octet-stream	411 218 B	179.241.18.181 [179.241.18.181]	TCP 80	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 49502	HttpGetNormal	2018-02-19 18:09:27 UTC	D:\Крпс КК\Passa

File	Tools	Help
— Select a network adapter in the list —		
Hosts (63) Files (26) Images (1) Messages (2) Credentials (63) Sessions (733) DNS (1073) Parameters (1108) Keywords Anomalies		
Filter keyword: <input type="text"/> <input type="checkbox"/> Case sensitive ExactPhrase <input type="text"/> Any column <input type="text"/> Clear Apply		
Source host	Destination host	From
192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	accountant <accountant@negative.tech>
192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	192.168.183.102 [DIR] [DIR<20>] (Windows)	accountant <accountant@negative.tech>
To Subject Protocol		
director@negative.tech Sir, report is ready SmtP		
director@negative.tech Sir, report is ready Pop3		

Были переданы зараженные файлы псевдо-отчета:

File	Tools	Help
Select a network adapter in the list —		
Hosts (63) Files (26) Images (1) Messages (2) Credentials (63) Sessions (733) DNS (1073) Parameters (1108) Keywords Anomalies		
Filter keyword: <input type="text"/> <input type="checkbox"/> Case sensitive ExactPhrase <input type="text"/> Any column <input type="text"/> Clear Apply		
Filename	Extension	Size
ddd[1].exe	exe	718 336 B
lsarp[3]		160 B
samr[4]		160 B
wirreg[3]		1 750 B
lsarp[4]		160 B
lsarp[5]		160 B
wirreg[4]		1 750 B
lsarp[5]		160 B
samr[6]		160 B
wirreg[5]		1 750 B
gpt[2].ini	ini	22 B
samr[7]		160 B
index[2].html	html	101 B
index[3].html	html	101 B
favicon.ico[2].html	html	101 B
2018_0178[1].png	png	706 784 B
favicon.ico[3].html	html	101 B
Report_20180206_122018[1].xlsx	xlsx	30 472 B
financial_report[1].rtf	rtf	583 B
Simeport[1].eml	eml	1 854 B
financial_report[1].rtf	rtf	583 B
Simeport[1].eml	eml	2 008 B
gpt[3].ini	ini	22 B
3Abol[1].txt	txt	340 B
3Abol[1].octet-stream	octet-stream	2 042 B
dnscat2.ps[1].octet-stream	octet-stream	411 218 B

Через зараженный отчет был получен доступ к компьютеру директора

В момент осмотра установлены:

Результаты осмотра:

Комиссия постановила:

Подписи членов комиссии:

