

---

---

# Assinatura de Infecção por Hancitor

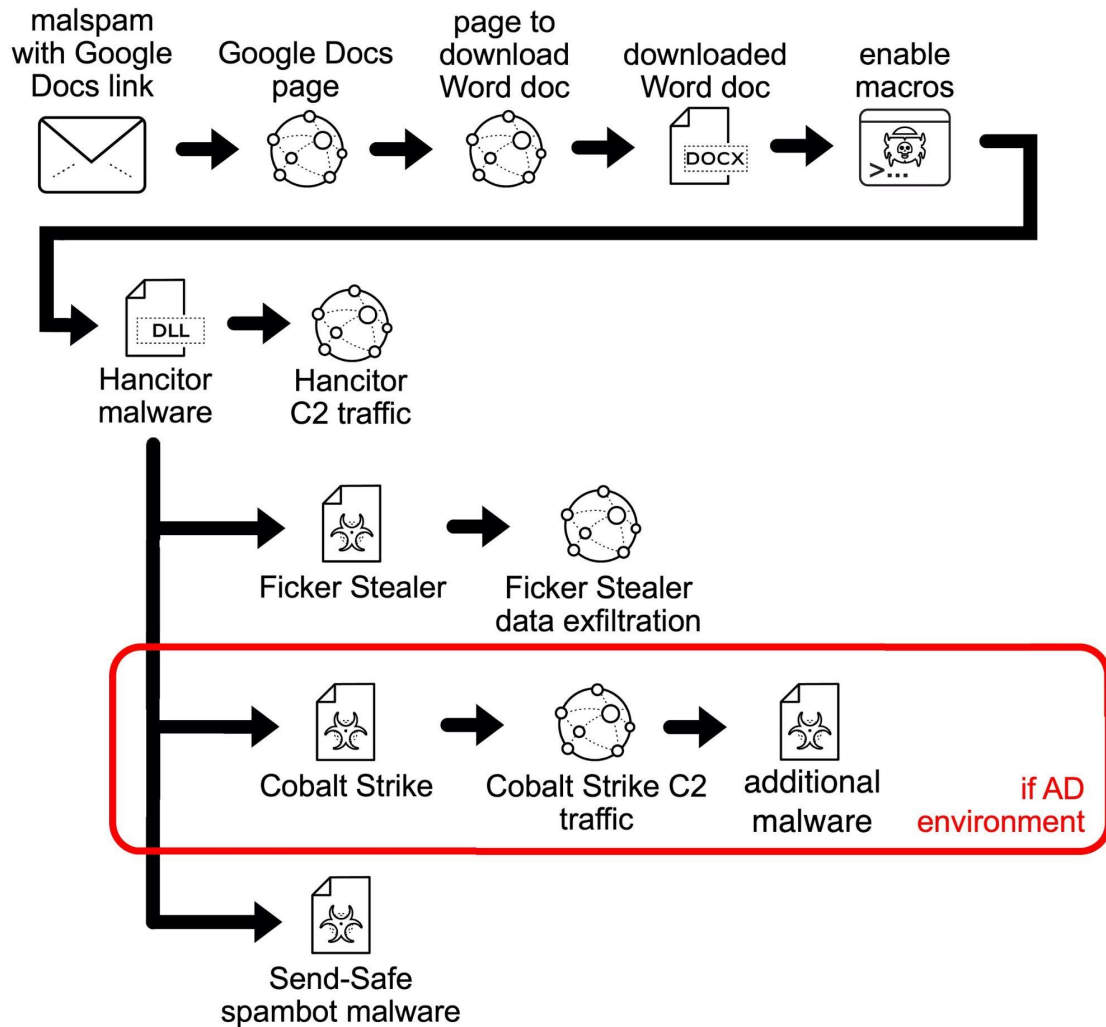
João Pedro Olimpio  
Rodrigo Cesar Barboza Rossetti

RA: 191026042  
RA: 191024961

---

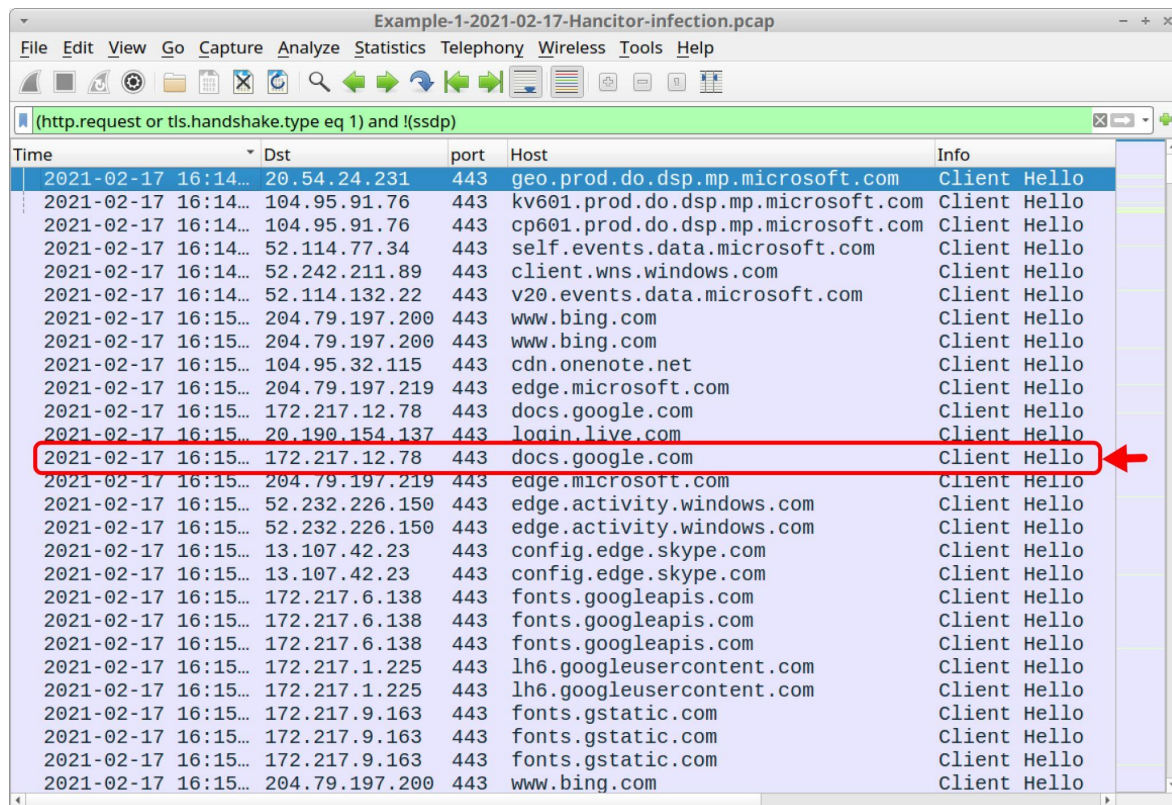
---

# O que é Hancitor?



# Processo Inicial de Infecção

(http.request or tls.handshake.type eq 1) and !(ssdp)



Example-1-2021-02-17-Hancitor-infection.pcap

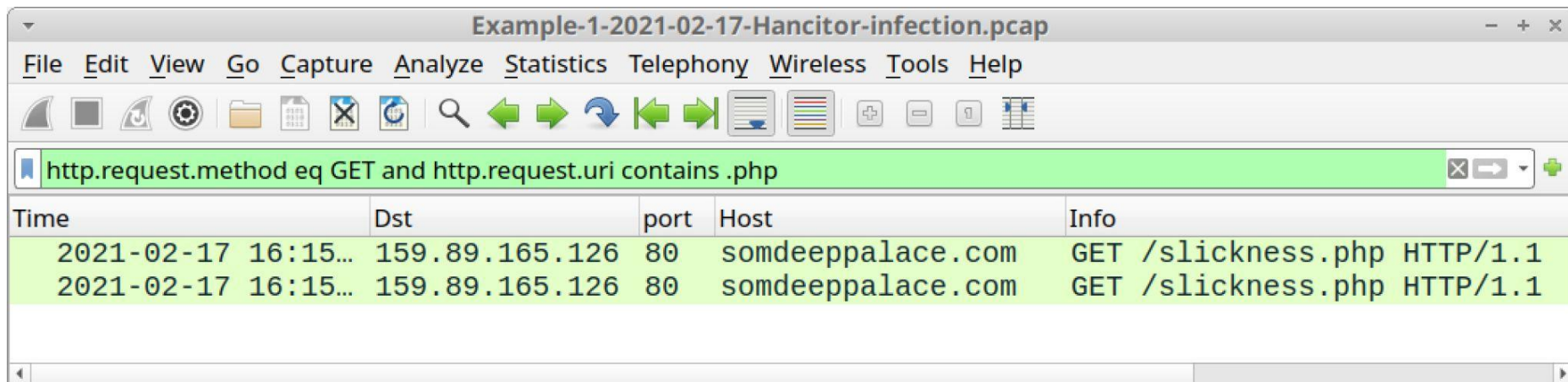
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2021-02-17 16:14...	20.54.24.231	443	geo.prod.do.dsp.mp.microsoft.com	Client Hello
2021-02-17 16:14...	104.95.91.76	443	kv601.prod.do.dsp.mp.microsoft.com	Client Hello
2021-02-17 16:14...	104.95.91.76	443	cp601.prod.do.dsp.mp.microsoft.com	Client Hello
2021-02-17 16:14...	52.114.77.34	443	self.events.data.microsoft.com	Client Hello
2021-02-17 16:14...	52.242.211.89	443	client.wns.windows.com	Client Hello
2021-02-17 16:14...	52.114.132.22	443	v20.events.data.microsoft.com	Client Hello
2021-02-17 16:15...	204.79.197.200	443	www.bing.com	Client Hello
2021-02-17 16:15...	204.79.197.200	443	www.bing.com	Client Hello
2021-02-17 16:15...	104.95.32.115	443	cdn.onenote.net	Client Hello
2021-02-17 16:15...	204.79.197.219	443	edge.microsoft.com	Client Hello
2021-02-17 16:15...	172.217.12.78	443	docs.google.com	Client Hello
2021-02-17 16:15...	20.190.154.137	443	login.live.com	Client Hello
2021-02-17 16:15...	172.217.12.78	443	docs.google.com	Client Hello
2021-02-17 16:15...	204.79.197.219	443	edge.microsoft.com	Client Hello
2021-02-17 16:15...	52.232.226.150	443	edge.activity.windows.com	Client Hello
2021-02-17 16:15...	52.232.226.150	443	edge.activity.windows.com	Client Hello
2021-02-17 16:15...	13.107.42.23	443	config.edge.skype.com	Client Hello
2021-02-17 16:15...	13.107.42.23	443	config.edge.skype.com	Client Hello
2021-02-17 16:15...	172.217.6.138	443	fonts.googleapis.com	Client Hello
2021-02-17 16:15...	172.217.6.138	443	fonts.googleapis.com	Client Hello
2021-02-17 16:15...	172.217.6.138	443	fonts.googleapis.com	Client Hello
2021-02-17 16:15...	172.217.1.225	443	lh6.googleusercontent.com	Client Hello
2021-02-17 16:15...	172.217.1.225	443	lh6.googleusercontent.com	Client Hello
2021-02-17 16:15...	172.217.9.163	443	fonts.gstatic.com	Client Hello
2021-02-17 16:15...	172.217.9.163	443	fonts.gstatic.com	Client Hello
2021-02-17 16:15...	172.217.9.163	443	fonts.gstatic.com	Client Hello
2021-02-17 16:15...	204.79.197.200	443	www.bing.com	Client Hello

# Processo Inicial de Infecção

`http.request.method eq GET and http.request.uri contains .php`



The image shows a Wireshark window titled "Example-1-2021-02-17-Hancitor-infection.pcap". The packet capture filter is set to "http.request.method eq GET and http.request.uri contains .php". The packet list shows two filtered packets, both GET requests to /slickness.php on somdeeppalace.com.

Time	Dst	port	Host	Info
2021-02-17 16:15...	159.89.165.126	80	somdeeppalace.com	GET /slickness.php HTTP/1.1
2021-02-17 16:15...	159.89.165.126	80	somdeeppalace.com	GET /slickness.php HTTP/1.1

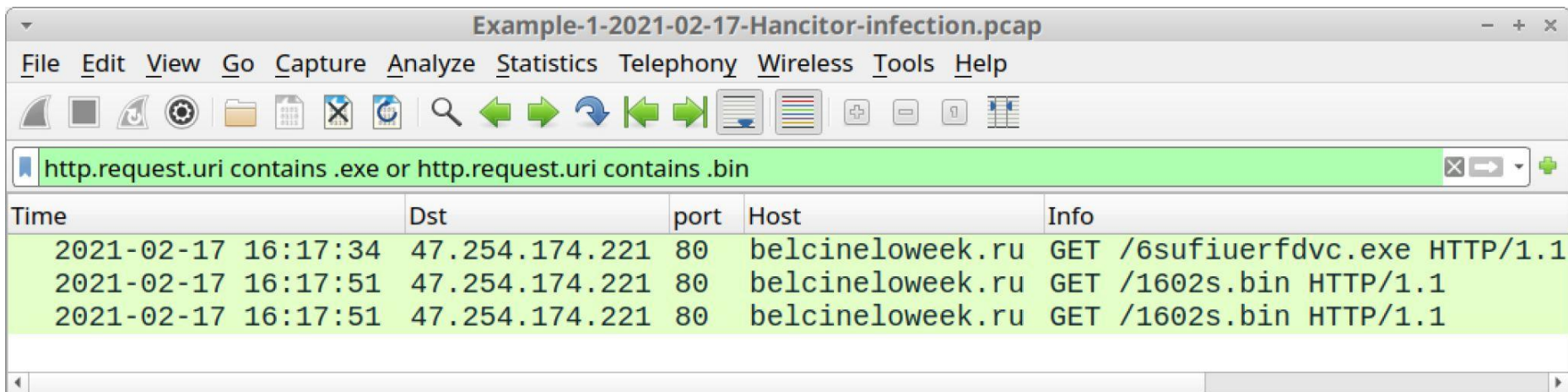
# Tráfego Hancitor C2

http.request.uri contains "/8/forum.php" or http.host contains api.ipify.org

Example-1-2021-02-17-Hancitor-infection.pcap					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
http.request.uri contains "/8/forum.php" or http.host contains api.ipify.org					
Time	Dst	port	Host	Info	
2021-02-17 16:17:20	54.225.129.141	80	api.ipify.org	GET / HTTP/1.1	
2021-02-17 16:17:32	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:17:51	54.225.129.141	80	api.ipify.org	GET /?format=xml HTTP/1.1	
2021-02-17 16:19:52	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:21:53	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:23:55	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:25:57	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:27:58	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:30:20	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:32:22	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:34:43	88.218.248.74	80	zinsubtal.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:36:44	88.218.248.74	80	zinsubtal.ru	POST /8/forum.php HTTP/1.1 (	
2021-02-17 16:38:44	88.218.248.74	80	zinsubtal.ru	POST /8/forum.php HTTP/1.1 (	

# Tráfego Hancitor C2

http.request.uri contains .exe or http.request.uri  
contains .bin



The image shows a Wireshark window titled "Example-1-2021-02-17-Hancitor-infection.pcap". The packet capture filter is set to "http.request.uri contains .exe or http.request.uri contains .bin". The packet list shows three HTTP GET requests to belcineloweeek.ru. The first request is for /6sufiuerfdvc.exe, and the next two are for /1602s.bin.

Time	Dst	port	Host	Info
2021-02-17 16:17:34	47.254.174.221	80	belcineloweeek.ru	GET /6sufiuerfdvc.exe HTTP/1.1
2021-02-17 16:17:51	47.254.174.221	80	belcineloweeek.ru	GET /1602s.bin HTTP/1.1
2021-02-17 16:17:51	47.254.174.221	80	belcineloweeek.ru	GET /1602s.bin HTTP/1.1



# Tráfego Ficker Stealer

dns.qry.name contains sveyblidian

Example-1-2021-02-17-Hancitor-infection.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains sveyblidian

Time	Dst	port	Info
2021-02-17 16:17:52	10.2.17.2	53	Standard query 0x237e A sveyblidian.com
2021-02-17 16:17:53	10.2.17.2	53	Standard query 0x237e A sveyblidian.com
2021-02-17 16:17:53	10.2.17.101	61402	Standard query response 0x237e A sveyblidian.com

Frame 4355: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)

Ethernet II, Src: Dell\_c2:09:6a (a4:1f:72:c2:09:6a), Dst: HewlettP\_1c:47:ae (00:08:02:1c:47:ae)

Internet Protocol Version 4, Src: 10.2.17.2, Dst: 10.2.17.101

User Datagram Protocol, Src Port: 53, Dst Port: 61402

Domain Name System (response)

Transaction ID: 0x237e

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

Answers

sveyblidian.com: type A, class IN, addr 185.100.65.29

[Request In: 4343]

[Time: 1.067081000 seconds]

# Tráfego Ficker Stealer

`ip.addr eq 185.100.65.29 and tcp.flags eq 0x0002`

Example-1-2021-02-17-Hancitor-infection.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

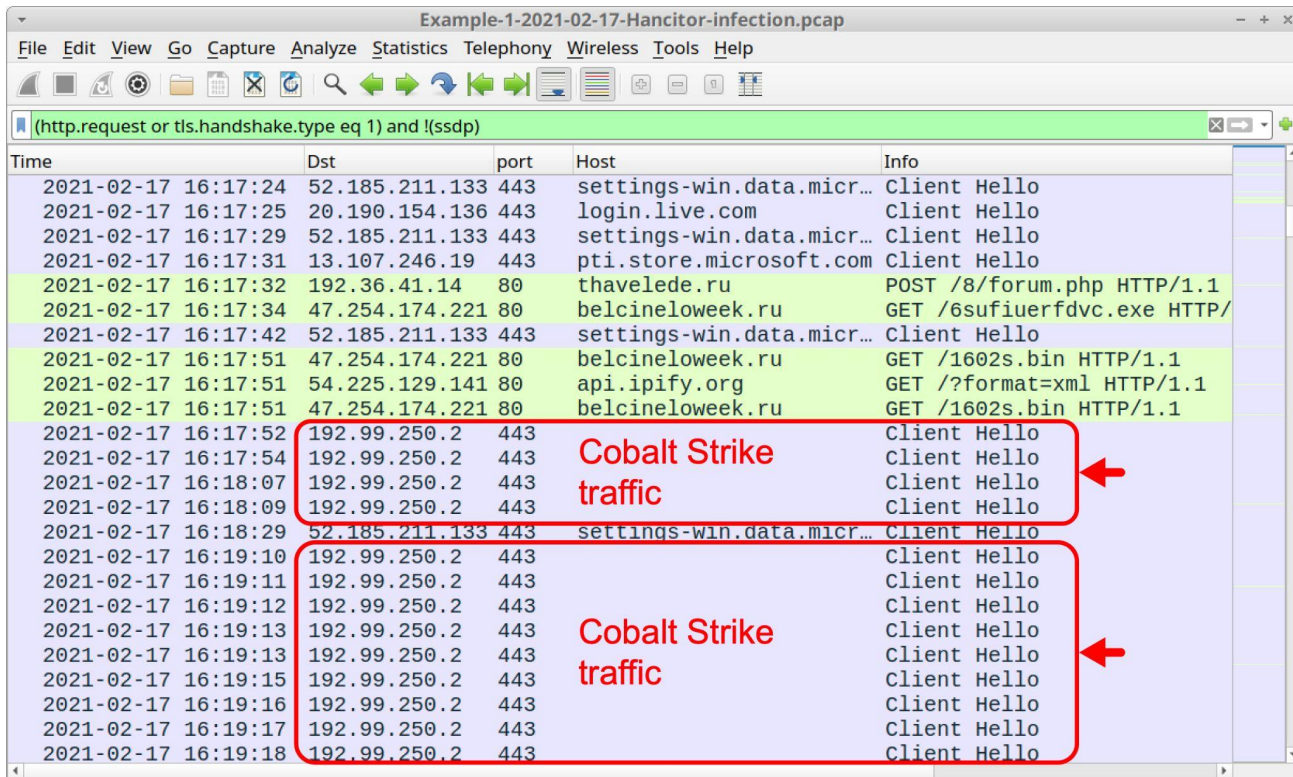
ip.addr eq 185.100.65.29 and tcp.flags eq 0x0002

Time	Src	port	Dst	port	Info
2021-02-17 16:17:53	10.2.17.101	49807	185.100.65.29	80	49807 → 80 [SYN] Seq=
2021-02-17 16:17:54	10.2.17.101	49807	185.100.65.29	80	[TCP Retransmission]
2021-02-17 16:20:24	10.2.17.101	49857	185.100.65.29	80	49857 → 80 [SYN] Seq=



# Tráfego Cobalt Strike

(http.request or tls.handshake.type eq 1) and !(ssdp)



Example-1-2021-02-17-Hancitor-infection.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2021-02-17 16:17:24	52.185.211.133	443	settings-win.data.micr...	Client Hello
2021-02-17 16:17:25	20.190.154.136	443	login.live.com	Client Hello
2021-02-17 16:17:29	52.185.211.133	443	settings-win.data.micr...	Client Hello
2021-02-17 16:17:31	13.107.246.19	443	pti.store.microsoft.com	Client Hello
2021-02-17 16:17:32	192.36.41.14	80	thavelede.ru	POST /8/forum.php HTTP/1.1
2021-02-17 16:17:34	47.254.174.221	80	belcineloweeek.ru	GET /6sufiuerfdvc.exe HTTP/
2021-02-17 16:17:42	52.185.211.133	443	settings-win.data.micr...	Client Hello
2021-02-17 16:17:51	47.254.174.221	80	belcineloweeek.ru	GET /1602s.bin HTTP/1.1
2021-02-17 16:17:51	54.225.129.141	80	api.ipify.org	GET /?format=xml HTTP/1.1
2021-02-17 16:17:51	47.254.174.221	80	belcineloweeek.ru	GET /1602s.bin HTTP/1.1
2021-02-17 16:17:52	192.99.250.2	443		Client Hello
2021-02-17 16:17:54	192.99.250.2	443		Client Hello
2021-02-17 16:18:07	192.99.250.2	443		Client Hello
2021-02-17 16:18:09	192.99.250.2	443		Client Hello
2021-02-17 16:18:29	52.185.211.133	443	settings-win.data.micr...	Client Hello
2021-02-17 16:19:10	192.99.250.2	443		Client Hello
2021-02-17 16:19:11	192.99.250.2	443		Client Hello
2021-02-17 16:19:12	192.99.250.2	443		Client Hello
2021-02-17 16:19:13	192.99.250.2	443		Client Hello
2021-02-17 16:19:13	192.99.250.2	443		Client Hello
2021-02-17 16:19:15	192.99.250.2	443		Client Hello
2021-02-17 16:19:16	192.99.250.2	443		Client Hello
2021-02-17 16:19:17	192.99.250.2	443		Client Hello
2021-02-17 16:19:18	192.99.250.2	443		Client Hello

# Tráfego Cobalt Strike

`tls.handshake.type eq 11 and ip.addr eq 192.99.250.2`

The image shows a Wireshark packet capture window titled "Example-1-2021-02-17-Hancitor-infection.pcap". The filter bar at the top displays the filter `tls.handshake.type eq 11 and ip.addr eq 192.99.250.2`. The packet list shows two packets at 2021-02-17 16:17:53 and 16:17:55, both from 192.99.250.2 to 10.2.17.101 on ports 443 and 49806, identified as "Certificate, Server Key Exchange, Serv".

The packet details pane for the selected packet (Frame 4357) shows the following structure:

- Frame 4357: 1190 bytes on wire (9520 bits), 1190 bytes captured (9520 bits)
- Ethernet II, Src: Netgear\_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP\_1c:47:ae (00:08:02:1c:47:ae)
- Internet Protocol Version 4, Src: 192.99.250.2, Dst: 10.2.17.101
- Transmission Control Protocol, Src Port: 443, Dst Port: 49806, Seq: 91, Ack: 150, Len: 1136
- Transport Layer Security
  - TLSv1.2 Record Layer: Handshake Protocol: Certificate
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 817
    - Handshake Protocol: Certificate
      - Handshake Type: Certificate (11)
      - Length: 813
      - Certificates Length: 810
      - Certificates (810 bytes)
        - Certificate Length: 807
        - Certificate: 308203233082020ba003020102020408bb00ee300d06092a... (id-at-commonName=, id-at-org...
        - signedCertificate
          - version: v3 (2)
          - serialNumber: 146473198
          - signature (sha256WithRSAEncryption)
          - issuer: rdnSequence (0)
            - rdnSequence: 6 items (id-at-commonName=, id-at-organizationalUnitName=, id-at-organizationalUnitName=, id-at-organizationalUnitName=, id-at-organizationalUnitName=, id-at-organizationalUnitName=)
            - RDNSequence item: 1 item (id-at-countryName=)
            - RDNSequence item: 1 item (id-at-stateOrProvinceName=)
            - RDNSequence item: 1 item (id-at-localityName=)
            - RDNSequence item: 1 item (id-at-organizationName=)
            - RDNSequence item: 1 item (id-at-organizationalUnitName=)
            - RDNSequence item: 1 item (id-at-commonName=)

certificate issuer  
data for Cobalt  
Strike HTTPS  
traffic