

# Full Disclosure of Havex Trojans

By Erik Hjelmvik

Published: 2014-10-27 · Archived: 2026-04-05 15:08:43 UTC

Monday, 27 October 2014 11:11:00 (UTC/GMT)

I did a talk on "SCADA Network Forensics" at the [4SICS conference](#) last week, where I disclosed the results from my analysis of the Havex RAT/backdoor.

The Havex backdoor is developed and used by a hacker group called Dragonfly, who are also known as "Energetic Bear" and "Crouching Yeti". Dragonfly is an APT hacker group, who have been reported to specifically target organizations in the energy sector as well as companies in other ICS sectors such as industrial/machinery, manufacturing and pharmaceutical.

In my 4SICS talk I disclosed a previously unpublished comprehensive view of ICS software that has been trojanized with the Havex backdoor, complete with screenshots, version numbers and checksums.

Dale Petersen, founder of Digital Bond, [expressed the following request](#) regarding the lack of public information about the software trojanized with Havex:

If the names of the vendors that unwittingly spread Havex were made public, the wide coverage would likely reach most of the affected asset owners.

Following Dale's request we decided to publish the information presented at 4SICS also in this blog post, in order to reach as many affected asset owners as possible. The information published here is based on our own sandbox executions of Havex malware samples, which we have obtained via [CodeAndSec](#) and [malwr.com](#). In addition to what I presented at 4SICS, this blog post also includes new findings published by Joel "[scadahacker](#)" Langill in version 2.0 of his [Dragonfly white paper](#), which was released just a couple of hours after my talk.

In Symantec's [blog post about Havex](#) they write:

Three different ICS equipment providers were targeted and malware was inserted into the software bundles

## Trojanized MESA Imaging driver

The first vendor known to have their software trojanized by the Dragonfly group was the Swiss company MESA Imaging, who manufacture industrial grade cameras for range measurements.



Image: Screenshot of trojanized MESA Imaging driver installer from our sandbox execution

<b>Company:</b>	MESA Imaging
<b>Product:</b>	Swiss Ranger version 1.0.14.706 (libMesaSR)
<b>Filename:</b>	SwissrangerSetup1.0.14.706.exe
<b>Exposure:</b>	Six weeks in June and July 2013 (source: Symantec)
<b>Backdoor:</b>	Sysmain RAT
<b>MD5:</b>	e027d4395d9ac9cc980d6a91122d2d83
<b>SHA256:</b>	398a69b8be2ea2b4a6ed23a55459e0469f657e6c7703871f63da63fb04cefe90

### eWON / Talk2M

The second vendor to have their software trojanized was the Belgian company [eWON](#), who provide a remote maintenance service for industrial control systems called “Talk2M”.

eWON published an [incident report](#) in January 2014 and then a [follow-up report](#) in July 2014 saying:

Back in January 2014, the eWON commercial web site [www.ewon.biz](http://www.ewon.biz) had been compromised. A corrupted eCatcherSetup.exe file had been uploaded into the CMS (Content Management System) of [www.ewon.biz](http://www.ewon.biz) web site. eCatcher download hyperlinks were rerouted to this corrupted file. The

corrupted eCatcherSetup.exe contained a malware which could, under restricted conditions, compromise the Talk2M login of the infected user.



Image: Screenshot of trojanized Talk2M eCatcher installer from our sandbox execution

<b>Company:</b>	eWON
<b>Product:</b>	Talk2M eCatcher version 4.0.0.13073
<b>Filename:</b>	eCatcherSetup.exe
<b>Exposure:</b>	Ten days in January 2014, 250 copies downloaded (source: Symantec)
<b>Backdoor:</b>	Havex 038
<b>MD5:</b>	eb0dacdc8b346f44c8c370408bad4306
<b>SHA256:</b>	70103c1078d6eb28b665a89ad0b3d11c1cbca61a05a18f87f6a16c79b501dfa9

Prior to version 2.0 of Joel's Dragonfly report, eCatcher was the only product from eWON known to be infected with the Havex backdoor. However, Joel's report also listed a product called "eGrabit", which we managed to obtain a malware sample for via [malwr.com](http://malwr.com).

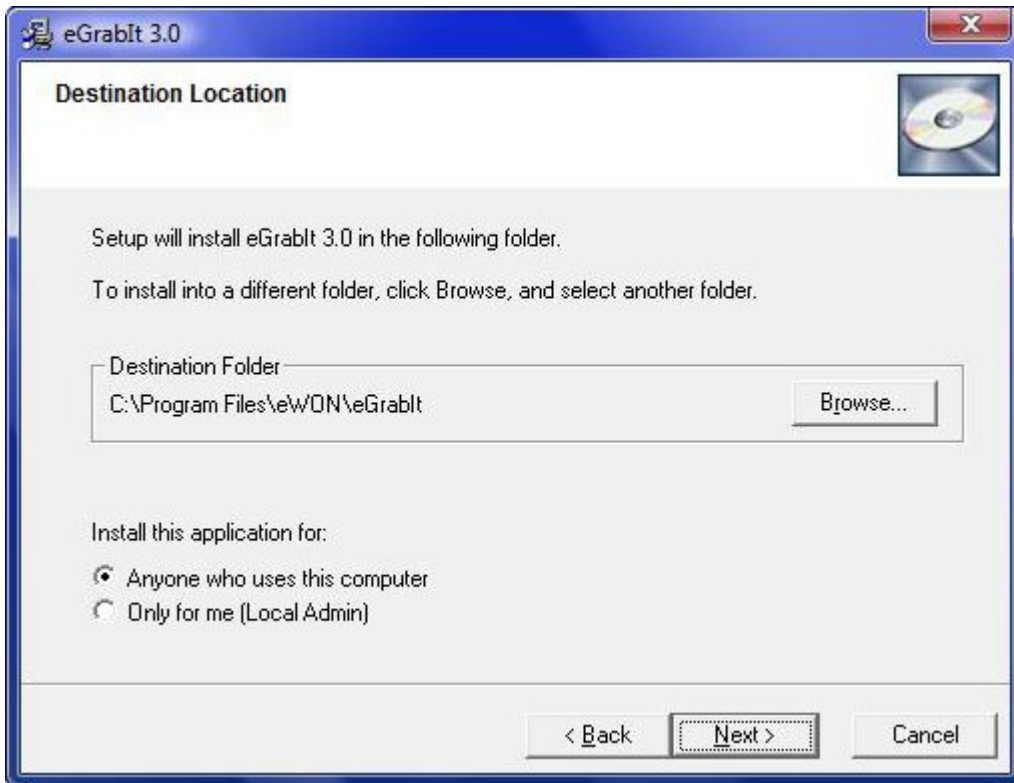


Image: Screenshot of trojanized eGrabIt installer from our sandbox execution

<b>Company:</b>	eWON
<b>Product:</b>	eGrabIt 3.0.0.82 (version 3.0 Build 82)
<b>Filename:</b>	egrabitsetup.exe
<b>Exposure:</b>	unknown
<b>Backdoor:</b>	Havex RAT 038
<b>MD5:</b>	1080e27b83c37dfeaa0daaa619bdf478
<b>SHA256:</b>	0007ccdddb12491e14c64317f314c15e0628c666b619b10aed199eefcfe09705

### MB Connect Line

The most recent company known to have their software infected with the Havex backdoor was the German company [MB Connect Line GmbH](#), who are known for their industrial router mbNET and VPN service mbCONNECT24.

MB Connect Line published a [report](#) about the Dragonfly intrusion in September 2014, where they write:

On 16th of April 2014 our website [www.mbconnectline.com](http://www.mbconnectline.com) has been attacked by hackers. The files mbCHECK (Europe), VCOM\_LAN2 and mbCONFTOOL have been replaced with infected files.

These files were available from 16th of April 2014 to 23th of April 2014 for download from our website. All of these files were infected with the known Trojan Virus Havex Rat.



Image: Screenshot of trojanized mbCONFTOOL installer from our sandbox execution

<b>Company:</b>	MB Connect Line GmbH
<b>Product:</b>	mbCONFTOOL V 1.0.1
<b>Filename:</b>	setup_1.0.1.exe
<b>Exposure:</b>	April 16 to April 23, 2014 (source: MB Connect Line)
<b>Backdoor:</b>	Havex RAT 043
<b>MD5:</b>	0a9ae7fdcd9a9fe0d8c5c106e8940701
<b>SHA256:</b>	c32277fba70c82b237a86e9b542eb11b2b49e4995817b7c2da3ef67f6a971d4a

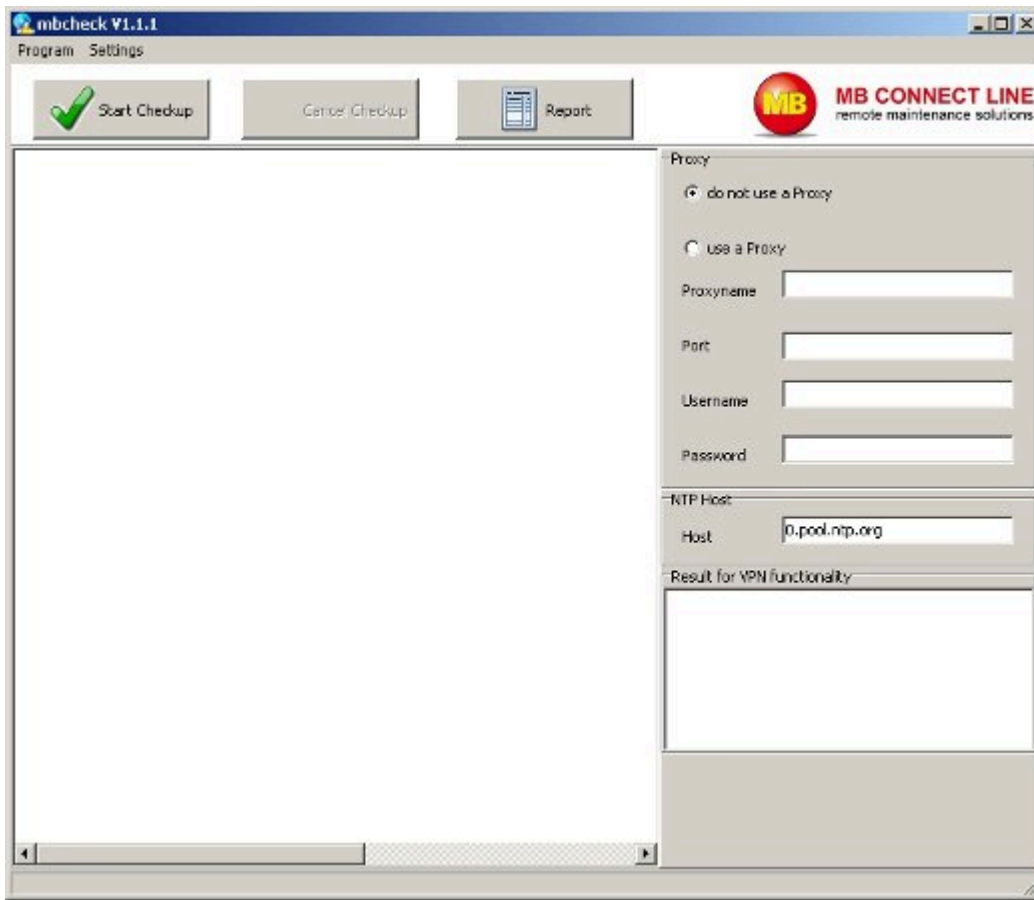


Image: Screenshot of trojanized mbCHECK application from our sandbox execution

<b>Company:</b>	MB Connect Line GmbH
<b>Product:</b>	mbCHECK (EUROPE) V 1.1.1
<b>Filename:</b>	mbCHECK.exe
<b>Exposure:</b>	April 16 to April 23, 2014 (source: MB Connect Line)
<b>Backdoor:</b>	Havex RAT 043
<b>MD5:</b>	1d6b11f85debdda27e873662e721289e
<b>SHA256:</b>	0b74282d9c03affb25bbe28d5155c582e246f0ce21be27b75504f1779707f5

Notice how only mbCHECK for users in Europe was trojanized, there has been no report of the USA/CAN version of mbCHECK being infected with Havex.

We have not been able to get hold of a malware sample for the trojanized version of VCOM\_LAN2. The screenshot below is therefore from a clean version of this software.

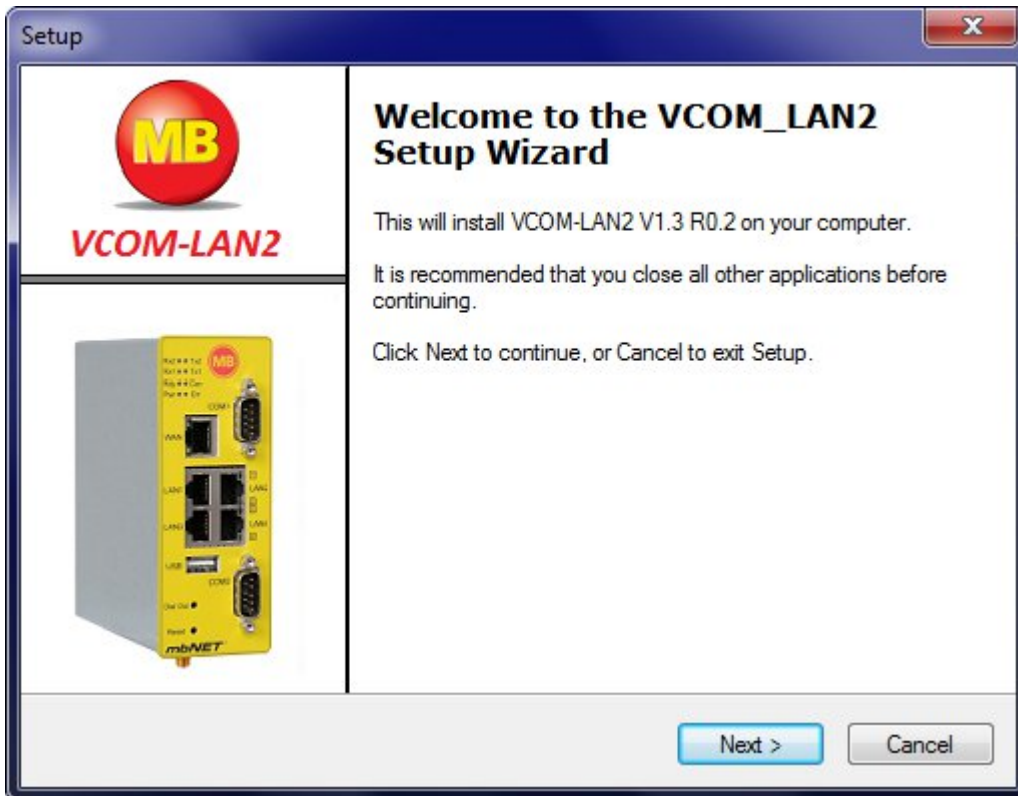


Image: Screenshot VCOM\_LAN2 installer

<b>Company:</b>	MB Connect Line GmbH
<b>Product:</b>	VCOM_LAN2
<b>Filename:</b>	setupvcom_lan2.exe
<b>Exposure:</b>	April 16 to April 23, 2014 (source: MB Connect Line)
<b>Backdoor:</b>	unknown
<b>MD5:</b>	unknown
<b>SHA256:</b>	unknown

### Conclusions on Havex Trojans

The vendors who have gotten their software trojanized by Dragonfly are all European ICS companies (Switzerland, Belgium and Germany). Additionally, only the mbCHECK version for users in Europe was infected with Havex, but not the one for US / Canada. These facts indicate that the Dragonfly / Energetic Bear threat actor seems to primarily target ICS companies in Europe.

### Next: Detecting Havex with NSM

Read our follow-up blog post [Observing the Havex RAT](#), which shows how to detect and analyze network traffic from ICS networks infected with Havex.

Posted by Erik Hjelmvik on Monday, 27 October 2014 11:11:00 (UTC/GMT)

Tags: [#Havex](#)[#ICS](#)[#SCADA](#)[#Trojan](#)[#4SICS](#)

---

Source: <http://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans>