Experts in network security monitoring and network forensics

NETRESEC

NETRESEC | Products | Resources | Blog | About Netresec |

NETRESEC > Blog

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

Full Disclosure of Havex Trojans

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In my 4SICS talk I disclosed a previously unpublished comprehensive view of ICS software that has been trojanized with the Havex backdoor, complete with screenshots, version numbers and checksums.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

Recent Blog Posts

» Observing the Havex RAT

» Full Disclosure of Havex Trojans

» Chinese MITM Attack on iCloud

» Verifying Chinese MITM of Yahoo

» Analysis of Chinese MITM on Google

» Running NetworkMiner on Mac OS X

» NetworkMiner 1.6 Released

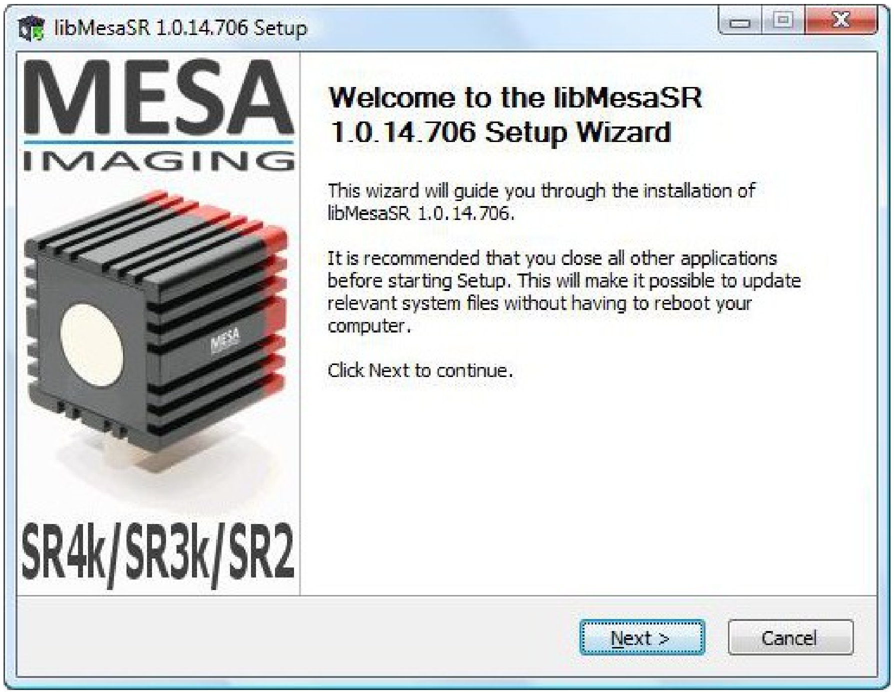
» PCAP or it didn't happen

Blog Archive

» 2014 November
» 2014 October
» 2014 September
» 2014 June
» 2014 May
» 2014 April
» 2014 March
» 2014 February
» 2013 October
» 2013 September
» 2013 August
» 2013 April
» 2013 February
» 2013 January
» 2012 December
» 2012 November
» 2012 September
» 2012 August
» 2012 July
» 2012 June
» 2012 April
» 2012 January
» 2011 December
» 2011 November
» 2011 October
» 2011 September
» 2011 August
» 2011 July
» 2011 June
» 2011 May
» 2011 April
» 2011 March
» 2011 February
» 2011 January

List all blog posts

Grab our FeedBurner or RSS feed



Welcome to the libMesaSR 1.0.14.706 Setup Wizard

This wizard will guide you through the installation of libMesaSR 1.0.14.706.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

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

Company:	MESA Imaging
Product:	Swiss Ranger version 1.0.14.706 (libMesaSR)
Filename:	SwissrangerSetup1.0.14.706.exe
Exposure:	Six weeks in June and July 2013 (source: Symantec)
Backdoor:	Sysmain RAT
MD5:	e027d4395d9ac9cc980d6a91122d2d83
SHA256:	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 had been compromised. A corrupted eCatcherSetup.exe file had been uploaded into the CMS (Content Management System) of 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.

NETRESEC on Twitter

Follow @netresec on twitter:
» twitter.com/netresec

Recommended Books

» The Practice of Network Security Monitoring, Richard Bejtlich (2013)

» Applied Network Security Monitoring, Chris Sanders and Jason Smith (2013)

» Network Forensics, Sherri Davidoff and Jonathan Ham (2012)

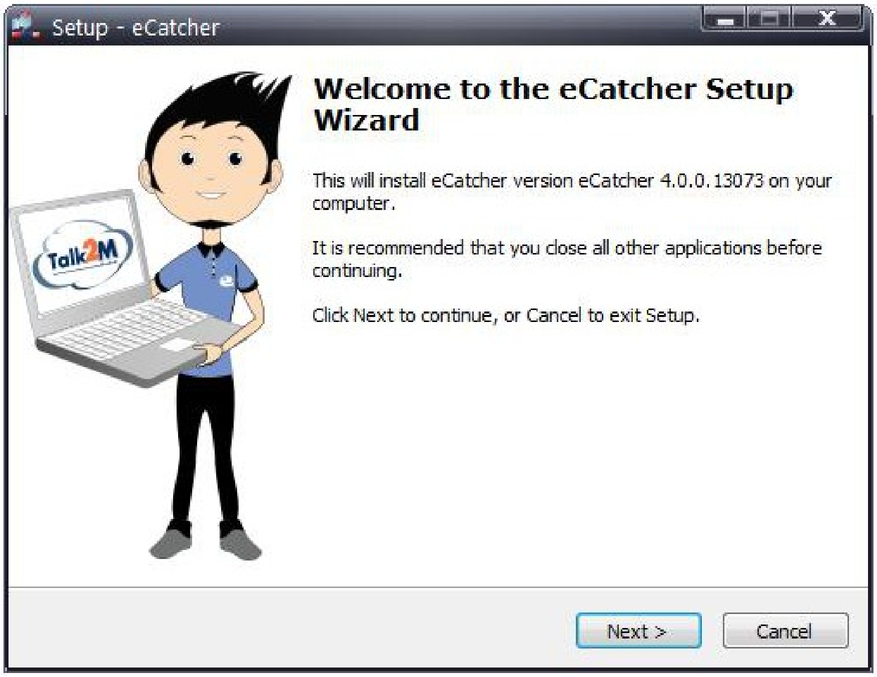
» The Tao of Network Security Monitoring, Richard Bejtlich (2004)

» Practical Packet Analysis, Chris Sanders (2011)

» Windows Forensic Analysis, Harlan Carvey (2009)

» TCP/IP Illustrated, Volume 1, Kevin Fall and Richard Stevens (2011)

» Industrial Network Security, Eric D. Knapp and Joel Langill (2014)



Setup - eCatcher

Welcome to the eCatcher Setup Wizard

This will install eCatcher version eCatcher 4.0.0.13073 on your computer.

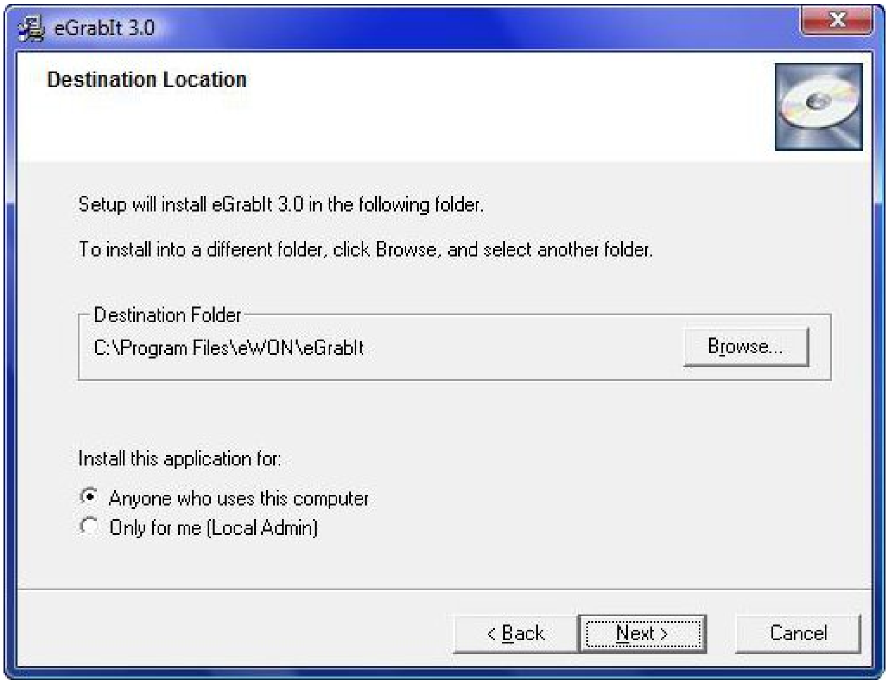
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

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

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



Setup will install eGrabIt 3.0 in the following folder.

To install into a different folder, click Browse, and select another folder.

Destination Folder
C:\Program Files\eWON\eGrabIt

Install this application for:

● Anyone who uses this computer
○ Only for me (Local Admin)

Image: Screenshot of trojanized eGrabIt installer from our sandbox execution

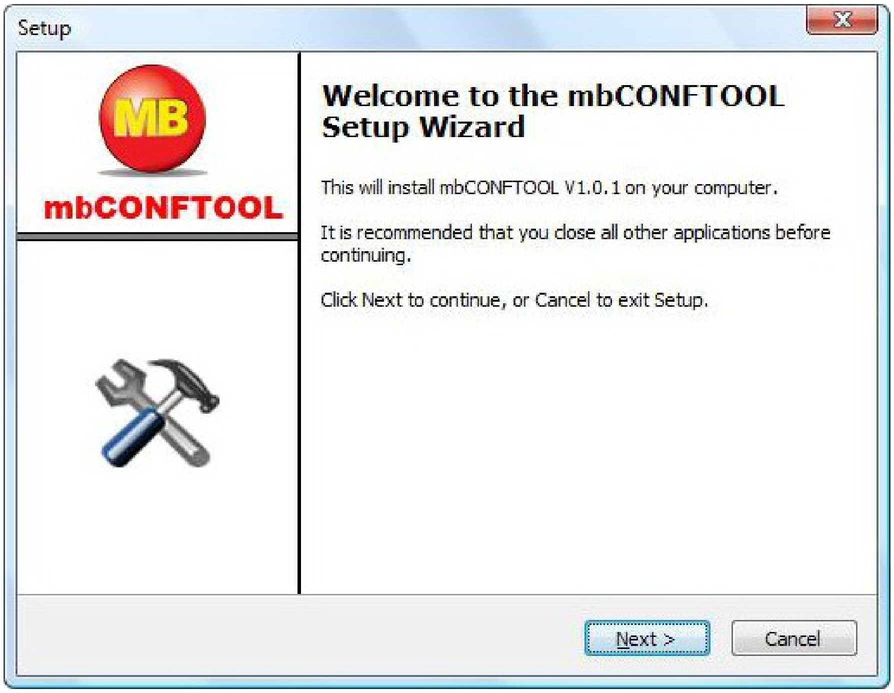
Company:	eWON
Product:	eGrabIt 3.0.0.82 (version 3.0 Build 82)
Filename:	egrabitsetup.exe
Exposure:	unknown
Backdoor:	Havex RAT 038
MD5:	1080e27b83c37dfeaa0daaa619bdf478
SHA256:	0007ccdddb12491e14c64317f314c15e0628c666b619b10aed199eefcfe09705

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 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.



Welcome to the mbCONFTOOL Setup Wizard

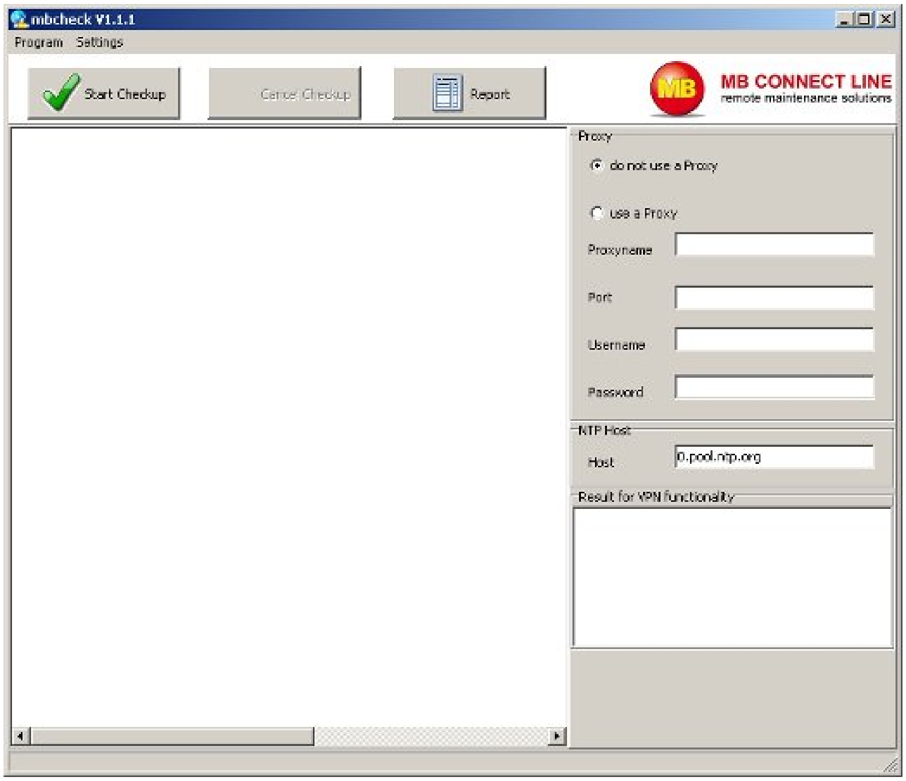
This will install mbCONFTOOL V1.0.1 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Image: Screenshot of trojanized mbCONFTOOL installer from our sandbox execution

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



● do not use a Proxy

○ use a Proxy

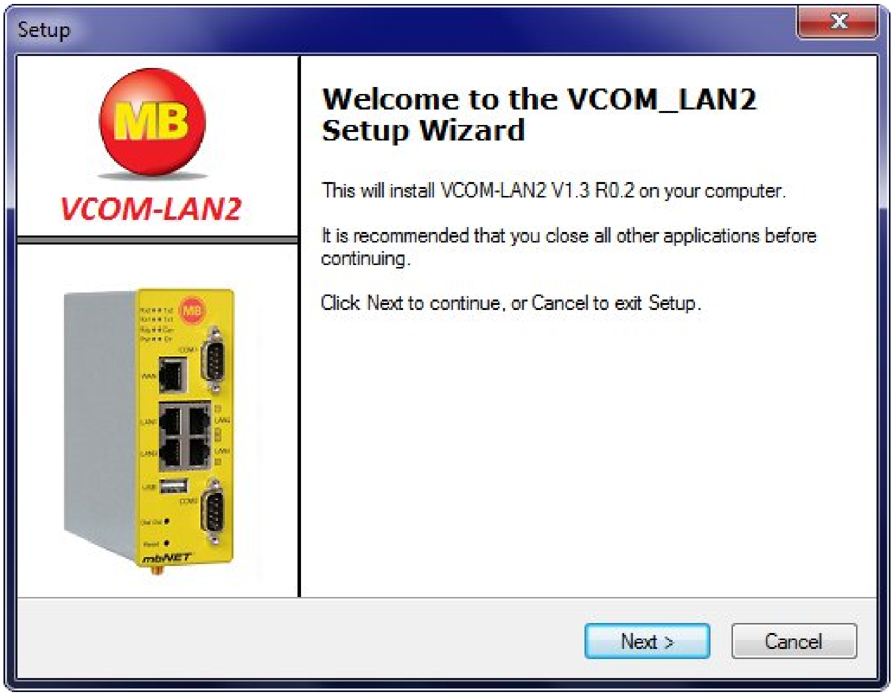
Host 0.pool.ntp.org

Image: Screenshot of trojanized mbCHECK application from our sandbox execution

Company:	MB Connect Line GmbH
Product:	mbCHECK (EUROPE) V 1.1.1
Filename:	mbCHECK.exe
Exposure:	April 16 to April 23, 2014 (source: MB Connect Line)
Backdoor:	Havex RAT 043
MD5:	1d6b11f85debdda27e873662e721289e
SHA256:	0b74282d9c03affb25bbecf28d5155c582e246f0ce21be27b75504f1779707f5

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.



Welcome to the VCOM_LAN2 Setup Wizard

This will install VCOM-LAN2 V1.3 R0.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Image: Screenshot VCOM_LAN2 installer

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

Share | Short URL: http://netresec.com/?b=14ABDA4

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