Energetic Bear — Crouching Yeti

Kaspersky Lab Global Research and Analysis Team

KASPERSKY lab

1. Executive Summary

Energetic Bear/Crouching Yeti is an actor involved in several Advanced Persistent Threat (APT) campaigns that have been active since at least the end of 2010. Targeted sectors include:

- Industrial/machinery
- Manufacturing
- Pharmaceutical
- Construction
- Education
- Information Technology

Most of the victims we identified fall into the industrial / machinery building sector, indicating this is of special interest.

To infect the victims, the attackers rely on three methods:

- Spear-phishing e-mails using PDF documents embedded with an Adobe Flash exploit (CVE-2011-0611)
- Trojanized software installers
- Waterhole attacks using a variety of re-used exploits

During the attacks, the Crouching Yeti use several malware/Trojans, which exclusively infect Windows systems:

- Havex Trojan
- Sysmain Trojan
- The ClientX backdoor
- Karagany backdoor and related stealers
- Lateral movement and second stage tools

For command and control, these connect to a large network of hacked websites. These sites host malware modules, victim information and serve commands to infected systems.

The dozens of known Yeti exploit sites and their referrer sites were legitimate, compromised sites. They ran vulnerable content management systems or vulnerable web applications. None of the exploits used to compromise the servers were known to be zero-day. None of the client side exploits re-used from the open source Metasploit framework were zero-day.

Overall, we observed about 2,800 victims worldwide, the most prevalent attack tool being the Havex Trojan.

We believe this group is highly determined and focused on a very specific industrial sector of vital interest. It uses a variety of ways to infect its victims and exfiltrate strategic information. The analyzed data seems to suggest the following points:

- It is not currently possible to determine the Country of origin
- The attackers' global focus is much broader than power producers
- Their toolset has remained stable over time
- Managed, minimal, methodical approach to sustained operation
- Appropriate use of encryption (symmetric key protected with attackers public key for encrypted log file exfiltration)

This report provides technical details on how the attackers perform their operations.

Contents

1. Executive Summary 2

2. Analysis 5

2.1. Delivery 5

2.1.1. Legitimate software installers 5

2.1.2. Malicious XDP file – spear-phishing 8

2.1.3. Malicious JAR/Html files – waterholing 9

2.2. Malware 12

2.2.1 The Havex Loader 12

2.2.2 The Ddex Loader 15

2.2.3 The Sysmain backdoor 15

2.2.4 The ClientX backdoor 17

2.2.5 The Karagany Backdoor 17

2.3. C&C servers and victims 20

2.3.1. Victims 23

2.3.2. Victims-C&C relationship 33

3. Attribution 34

3.1. Non-specific Data 34

3.2. Exploit server activity 38

3.3. Victim characteristics and categories 39

4. Conclusions 40

2. Analysis

This section analyzes all the aspects we could find about how this threat actor manages its campaigns.

The Crouching Yeti actor performed a massive surveillance operation targeting strategic victims, many of them in the industrial/manufacturing sector.

There were different ways of delivering of its malware including waterholing, spearphishing and adding malware to legitimate installers. Once the victims were infected, Crouching Yeti selected different RATs for its operations. These RATs communicated with Command and Control servers on compromised servers around the world, using a simple PHP backend.

We were able to identify several victims, including high-profile ones and dozens of domains used in the campaign.

2.1. Delivery

As far as we know the group behind Crouching Yeti delivers its malware using at least three different methods.

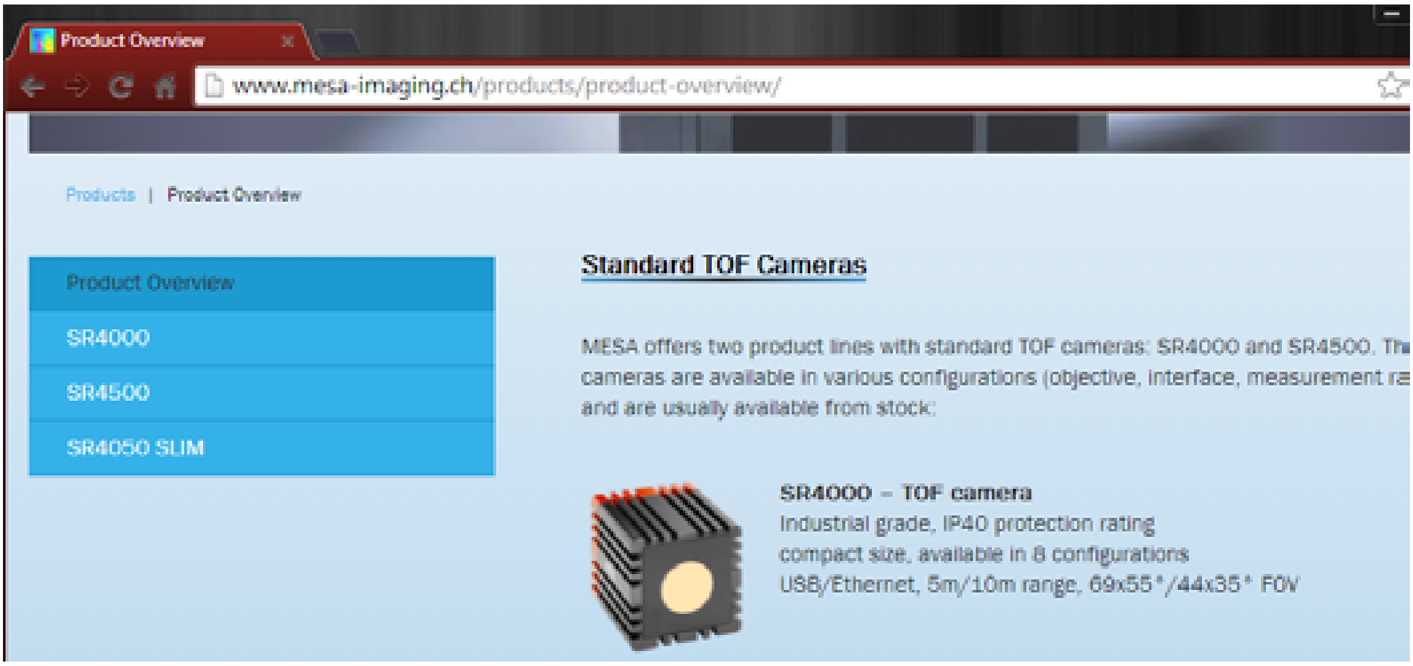
2.1.1. Legitimate software installers

The first method uses a legitimate software installer repackaged as to contain the malicious DLL. Such modified self-extracting archives could have been uploaded directly to a compromised server, replacing the original file, or sent to the victim by email.

One example of using this method was a hijacked SwissRanger camera driver (libMesaSR version 1.0.14.706) that was used to drop the **Sysmain backdoor** to:

```
%APPDATA%\sydmain.dll
```

and set the Run registry value to load malicious DLL upon next system startup.


Product Overview
www.mesa-imaging.ch/products/product-overview/
Products | Product Overview
Product Overview
SR4000
SR4500
SR4050 SLIM

Standard TOF Cameras

MESA offers two product lines with standard TOF cameras: SR4000 and SR4500. Th
cameras are available in various configurations (objective, interface, measurement ra
and are usually available from stock:

SR4000 – TOF camera
Industrial grade, IP40 protection rating
compact size, available in 8 configurations
USB/Ethernet, 5m/10m range, 69x55°/44x35° FOV

Figure 1. MESA Camera description

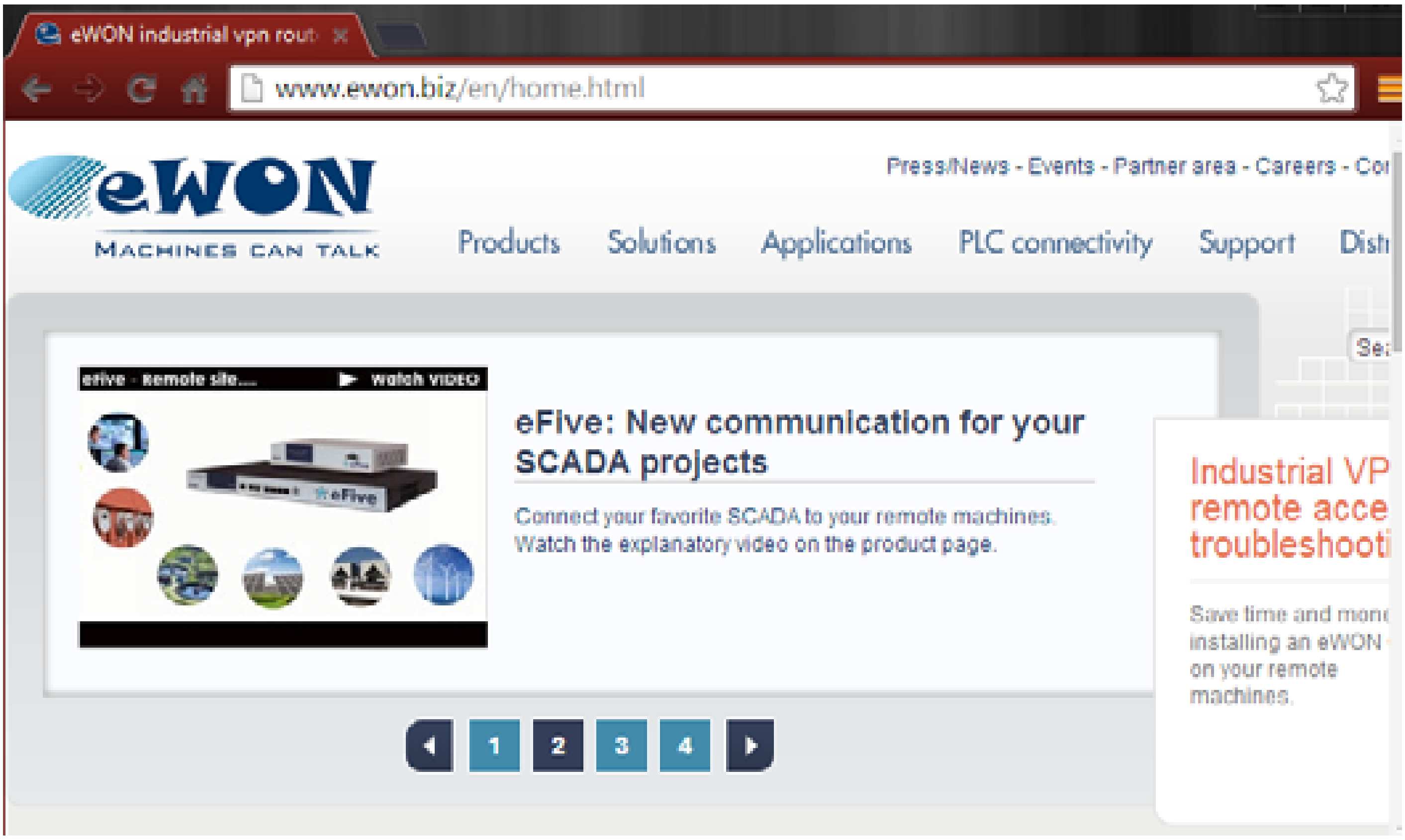
In a similar manner, as early as January 2014, Havex version 038 appears to have been dropped by a legitimate ~40MB software installer from the eWon web site:

hxxp://www.ewon.biz/software/eCatcher/eCatcherSetup.exe

“eWon” is a Belgian producer of SCADA and industrial network equipment, which helps define this attack method as a watering hole attack:

> “Breaking the barrier between industrial applications and IT standards, the mission of eWON is to connect industrial machines securely to the Internet, enabling easy remote access and gathering all types of technical data originating from industrial machines… Connecting machines across the Internet is our mission.”

Sometimes, the Havex loader was dropped from “eCatcherSetup_v4.exe”, so it seems that the site operators may have removed a previous file and the attackers replaced it with their Trojanized installer. It is also likely that the attackers gained access to eWon’s FTP site and replaced the legitimate file with one that is bound with the Havex dropper several times.



eFive: New communication for your SCADA projects

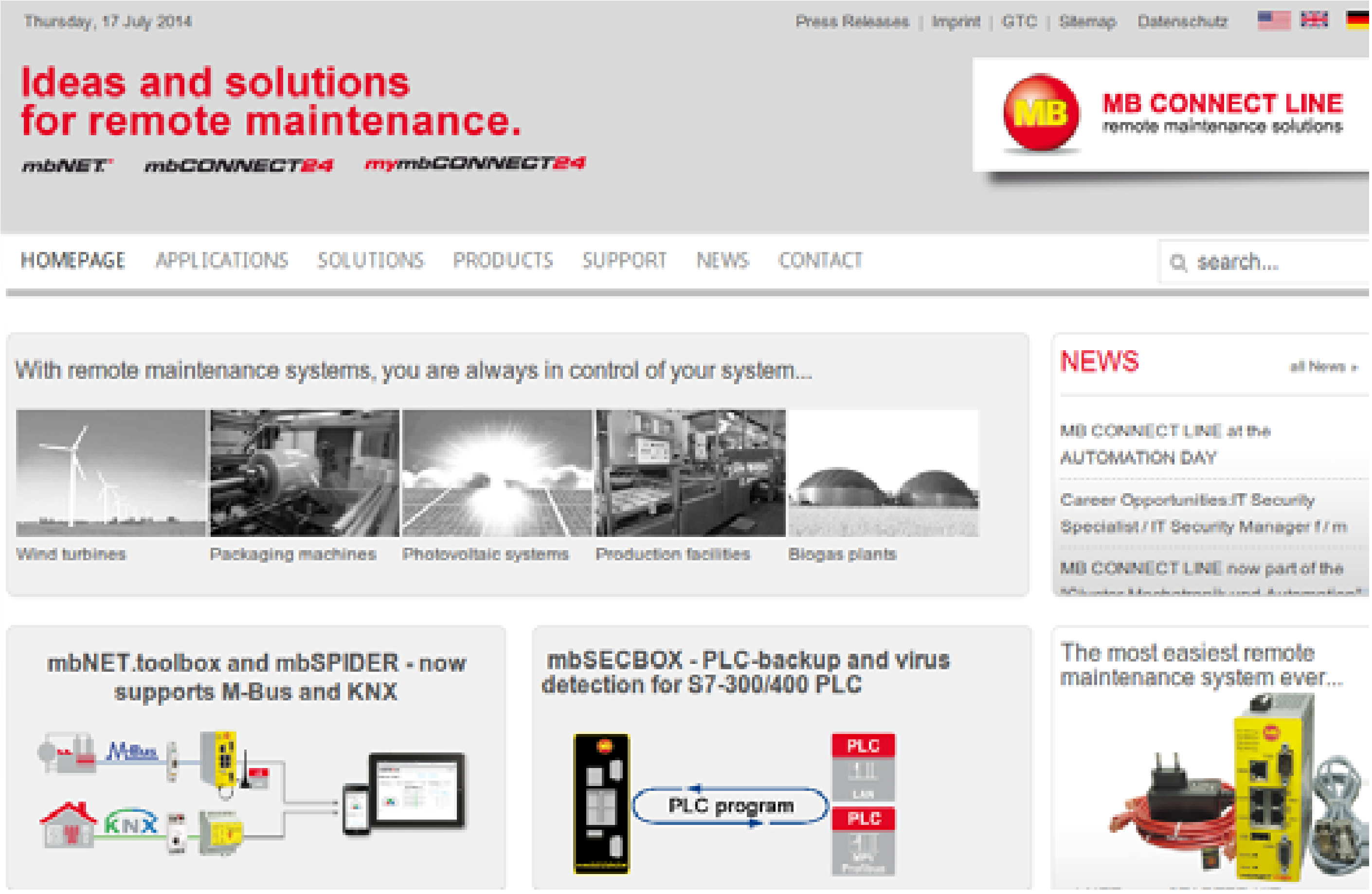
Connect your favorite SCADA to your remote machines. Watch the explanatory video on the product page.

Industrial VP remote acce troubleshooti

Save time and mone installing an eWON on your remote machines.

Figure 2. MESA Camera description

Another example that involves a hijacked application from a PLC-related vendor is a Trojanized mbCHECK installer which replaced the original legitimate version freely downloadable from the vendor's website. The vendor - MB Connect Line - is a company which specializes in software for remote maintenance of PLC systems: MB Connect Line GmbH (hxxp://www.mbconnectline.com/index.php/en/).


Thursday, 17 July 2014

Ideas and solutions for remote maintenance.

With remote maintenance systems, you are always in control of your system...

MB CONNECT LINE at the AUTOMATION DAY

Career Opportunities:IT Security Specialist / IT Security Manager f / m

MB CONNECT LINE now part of the

mbNET.toolbox and mbSPIDER - now supports M-Bus and KNX

mbSECBOX - PLC-backup and virus detection for S7-300/400 PLC

The most easiest remote maintenance system ever...

Figure 3. MB Connect Line website

In this case, the dropped DLL was Havex version 043.

2.1.2. Malicious XDP file – spear-phishing

The second method relies on a malicious XDP file containing the PDF/SWF exploit (CVE-2011-0611) and was most likely used in spear-phishing attacks. This exploit drops the **Havex loader** DLL, which is stored in an encrypted form in the XDP file.

The exploit is delivered as an XDP (XML Data Package) file which is actually a PDF file packaged within an XML container. This is a known the PDF obfuscation method and serves as an additional anti-detection layer.

The XDP file contains a SWF exploit and two files (encrypted with XOR) stored in the invalid section of the PDF file. One of the files is Havex DLL (version 038), the other is a small JAR file, which is used to copy and run the DLL by executing the following command:

```
cmd /c copy <fname_passed_as_param> %TEMP%\\explore.dll /y & rundll32.exe
%TEMP%\\explore.dll,RunDllEntry
```

The SWF executes the action script, which contains another SWF file which in turn uses the CVE-2011-0611 vulnerability to run the shellcode.

The shellcode then looks for a specific signature in the memory (which signs the start of the encrypted DLL), decrypts and loads it.

2.1.3. Malicious JAR/Html files – waterholing

Finally, this actor actively compromises legitimate websites for watering hole attacks. These hacked websites in turn redirect victims to malicious JAR or HTML files hosted on other sites maintained by the group (exploiting CVE-2013-2465, CVE-2013-1347, and CVE-2012-1723 in Java 6, Java 7, IE 7 and IE 8). These then drop the **Havex loader, the Karagany backdoor and helper tools**. These sites run an exploit kit known as “LightsOut”. It appears that the “LightsOut” exploit kit is exclusively used by the Energetic Bear/Crouching Yeti actor.

From the dozens of Yeti exploit sites we reviewed, the malicious code was nothing more than slightly modified metasploit java exploits delivering the Havex loader. Some sort of internal review must have pushed them towards the LightsOut EK. KSN data records help provide a list of Crouching Yeti related exploit delivery from dozens of these sites.

In earlier cases (July 2013), successful Java exploitation served from nahoonservices.com would cascade into more Yeti components planted on victim systems. The Java exploit downloaded Karagany backdoors, which in turn downloaded stealers from 91.203.6.71:

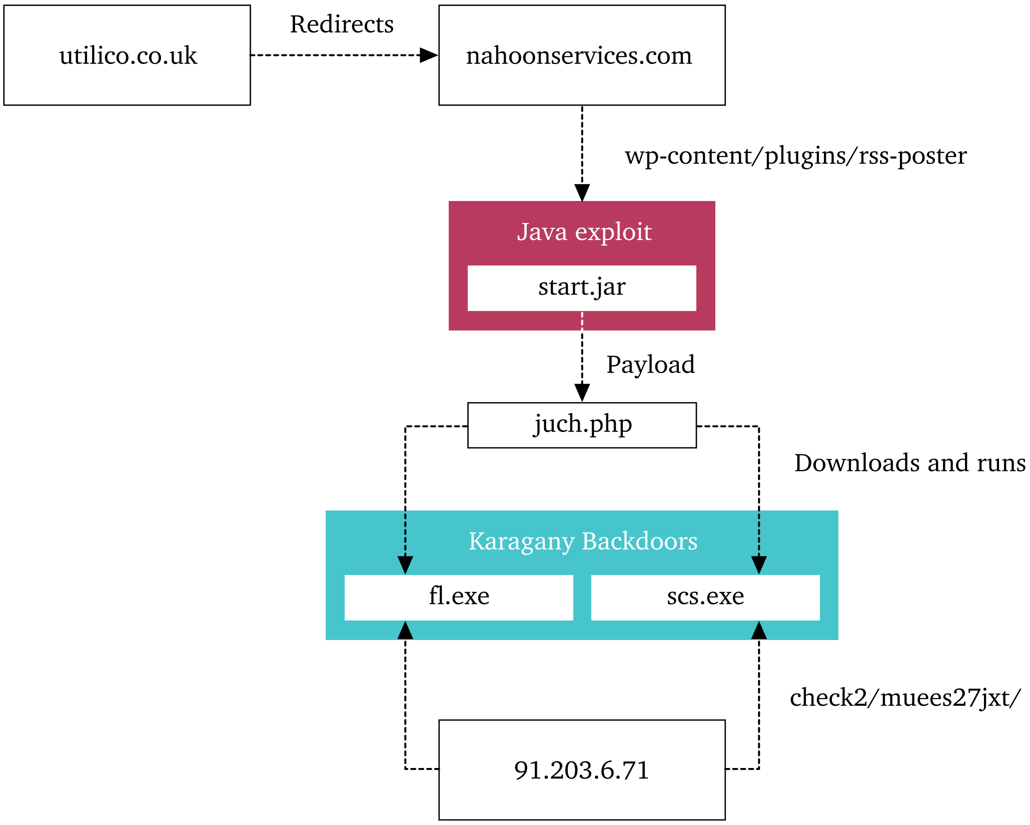
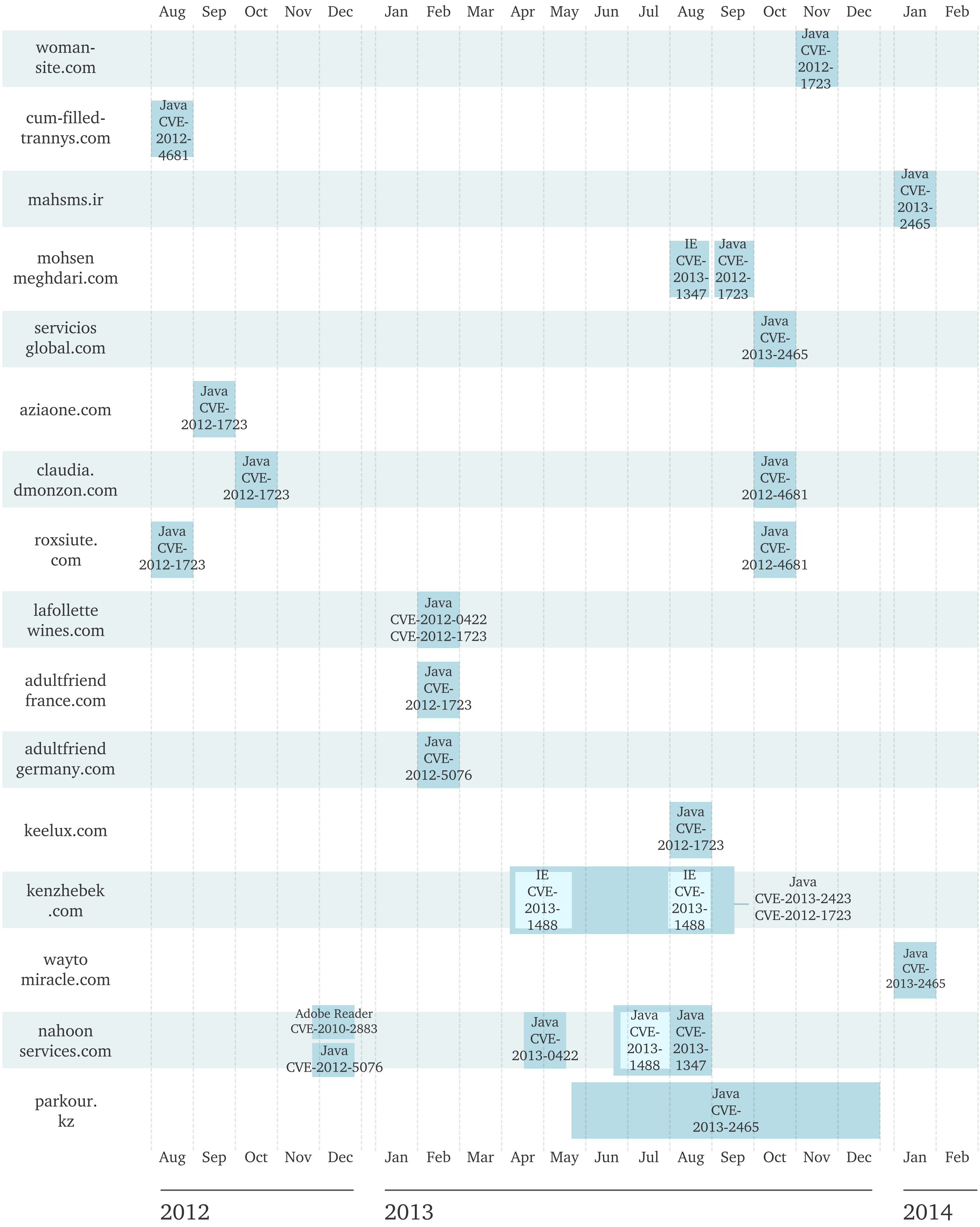


Figure 4. Infection diagram

KSN data recorded at least 20 victim sites that were compromised and injected with Yeti iFrames, redirecting hundreds of visitors to compromised Yeti exploit sites. Most of these redirector sites were owned by Western and Eastern European industrial power players, investors, legal advisors and advocates, and European and US industrial IT equipment makers. The compromised sites hosting the Lights Out exploit kit were fairly well trafficked, legitimate sites. Their content widely varies from California winemakers to Cuban travel agencies and Iranian general interest/religious inspiration sites.



Finally, other second stage tools were simply retrieved by the downloaders over http from various servers. Some of these Yeti sites, like kinoporno.org, served both Havex and these tools. KSN events recorded the sites serving Windows Credential Editor and custom credential and document stealing tools.

2.2. Malware

The Crouching Yeti group has different tools of choice for their operations. This section describes them from a technical perspective.

2.2.1 The Havex Loader

1. Description

The main functionality of this component is to download and load additional DLL modules into the memory. These are stored on compromised websites that act as C&C servers. In order to do that, the malware injects itself into the `EXPLORER.EXE` process, sends a GET/POST request to the PHP script on the compromised website, then reads the HTML document returned by the script, looking for a base64 encrypted data between the two "havex" strings in the comment tag `<!--havexhavex-->` and writes this data to a `%TEMP%\<tmp>.xmd` file (the filename is generated by GetTempFilename function).

In the meantime, another routine is constantly checking the `%TEMP%` folder for all `*.xmd` files. For each file it finds, it decompresses the content, decrypts (if encrypted) and loads into the memory as the DLL.

In order to run on each system boot, malware copies itself to: `<path>\TMPprovider0XX.dll` and creates the autorun registry key.

All samples of this component contain statically linked bzip2 library. Versions >= 01B contain also a RSAeuro library, used for encryption of log files and decryption of downloadable modules. Public keys for encryption are hardcoded in the binary and/or stored in the configuration section. In some cases, these keys are written to the registry values.

In total, we identified 124 different samples of Havex loader, belonging to 27 different versions. As of June 2014, the latest version number we know of is 044.

2. C&C communication

The URL addresses of the C&C servers (which are indeed compromised websites) are either hardcoded in the binary, or - in versions => 038 - specified in the configuration section inside the ICT resource. This resource is compressed with bzip2 and encrypted with XOR.

There are usually 2-4 URLs per binary, different for each malware version and sometimes also different between samples of the same version.

Malware sends a GET request (versions < 017) or POST request to the first available URL. The request contents depends on the malware version and it may include such information as unique bot id, malware version number, OS version number, and some other data from configuration, as well as the harvested information logged into the `*.yls` file (if any). Then the malware searches the HTML code of each returned page for havex markers and saves the data between the markers into a temporary file.

3. Downloadable modules - common characteristics

These modules are hosted between the havex markers in the HTML code of compromised websites. The module code are usually XORed with "1312312" then compressed with BZIP2 and finally base64 encoded. Once downloaded into the `%TEMP%\*.xmd` file by the main Havex DLL, the code gets decoded, decompressed, saved into the temporary DLL file and loaded into the memory.

The modules perform variety of different actions, including collecting information about the victim's system and other machines in the local network, harvesting passwords, listing documents, etc. In order to do that, some of the modules make use of additional 3rd stage, third-party executables.

Each module contains the configuration information stored in an encrypted and compressed form inside a resource. Configuration data includes 29-byte UID (unique ID), a 1024 bit RSA Public key (base64 encoded) and other necessary info (like file paths, etc.). All harvested data is compressed, encrypted and written into the `%TEMP%\*.yls` files, which are then sent to the C&C by the main Havex/Sysmain module.

The "yls" files are encrypted with the 3DES crypto algorithm using a random 192-bit key (168 bit effective). The 3DES key is encrypted using the public RSA 1024 key and therefore never transferred in plain text to attackers.

In-depth analysis of the cryptography used by log files is presented in the Appendix 2

4. List of known modules

<u>OPC scanner</u>

This module is designed to collect the detailed data about the OPC servers running in the local network and save them to to %TEMP%\{rand}.yls file. To query the OPC servers, it uses the following interfaces:

- `IID_IOPCEnumGUID`
- `IID_IOPCServerList`
- `IID_IOPCServerList2`

- IID_IOPCServer
- IID_IOPCBrowsr
- IID_IOPCBrowseServerAddressSpace
- IID_IOPCItemProperties
- CATID_OPCDAServer10
- CATID_OPCDAServer20
- CATID_OPCDAServer30

Sysinfo module

This module collects basic information about the system it's running on, and saves it to the %TEMP%\{rand}.yls file. Harvested data includes:

- Unique system ID
- OS version
- Username
- Computer name
- Country
- Language
- Current IP
- List of drives
- Default Browser
- Running Processes
- Proxy Setting
- User Agent
- Email Name
- BIOS version and date
- Lists of files and folders (non-recursive) from Desktop, My Documents and Program Files folders and root directories on all drives.

Contacts stealer module

This module collects contact details stored in all outlook.nk2 files and writes them to the %TEMP%\{rand}.yls file.
Outlook.nk2 file is the file where Outlook (version greater or equal to 2007) keeps contacts details in order to use them for AutoComplete feature.

Password stealer module

This module uses the embedded **BrowserPasswordDecryptor 2.0** tool (hxxp://securityxploded.

com/browser-password-decryptor.php) to dump login credentials stored by the password managers of various browsers. Decrypted passwords are saved into the `%TEMP%\~tmp1237.txt` file, which is then copied by the parent module into an encrypted `*.tmp.yls` file.

List of browsers supported by the tool (from the product's website):

- Firefox
- Internet Explorer
- Google Chrome
- Google Chrome Canary/SXS
- CoolNovo Browser
- Opera Browser
- Apple Safari
- Comodo Dragon Browser
- SeaMonkey Browser
- SRWare Iron Browser
- Flock Browser

Network scanner module

This module is designed to scan the local network and look for all hosts listening on ports related to OPC/SCADA software. Information about these hosts is then saved to the `%TEMP%\~tracedscn.yls` file.

Port number	Software that uses this port
port 44818	Rslinx
port 502	Modbus
port 102	Siemens PLC
port 11234	Measuresoft ScadaPro
port 12401	7-Technologies IGSS SCADA

In-depth analysis of Havex loader and the related modules is presented in the Appendix 2.

2.2.2 The Ddex Loader

1. Description

This component is a simple downloader with the functionality similar to the Havex component.

It sends the request to PHP script at the C&C (compromised website) and looks for specific data in the returned HTML code.

It writes the data (some ASCII string) from between `<I6></I6>` tags to the file in `%TEMP%\Low\~task.tmp` and the data (binary data XORed with 0x0A) from between `<B6></B6>` tags into the `%TEMP%\Low\~ldXXXX.TMP` file.

Then it decrypts the `ldXXXX.TMP` file and loads it into memory.

Based on the compilation times, we may assume that this loader was used to download and run modules before it got replaced by Havex.

The Ddex loader is analyzed in more details in Appendix 4.

2.2.3 The Sysmain backdoor

1. Description

This malware can be described as a classical RAT (Remote Access Trojan), since it gives the attacker a wide range of opportunities to control and to interact with the victims' machine.

The autonomous part of *Sysmain* installs and registers itself to be persistent in the system.

Then it gathers general information about the victims system, like

- User- and computer names
- Locale information
- Network- and drive status
- Default browsers
- Running processes
- File listing of the users profile directory.

When ready, this data is submitted to one of the C&C-servers. After that, it checks periodically for new commands from C&C (pulling via HTTP).

With a set of 11 commands, the malware is able to:

- Execute shell-commands
- Launch additional executables or libraries (sent by the attacker)
- Collect arbitrary files for later exfiltration
- Examine the victim's filesystem.

There are also commands used for maintenance purposes. Among others, there are commands to change the pubkey for C&C-communication or delete its traces in the registry.

2. C&C communication

It receives its commands from one of four static command-and-control servers. Every variant of this malware has its own set of servers.

As usual, the attackers are using most likely compromised webservers as part of their C&C-infrastructure. To communicate with the C&C-server, the Trojan makes use of asymmetric encryption with a hardcoded pair of private and public keys.

Another public key is used to encrypt files, which are collected in a local dropzone on the victim's file system. The files in that dropzone will be submitted to the attacker later, all in one go.

Appendix 3 provides in-depth analysis of the Sysmain backdoor.

2.2.4 The ClientX backdoor

1. Description

This component is written in .NET and is very similar to The Sysmain backdoor.
The settings of the RAT are stored in the registry as BASE64 encoded values.

The RAT gets its commands by sending a request to a PHP script on the C&C (compromised server) as usual, and looks for specific data in the returned HTML code. The data in this case is stored between the havexhavex tags, it is then decrypted and decoded (base64).

The RAT supports 13 commands including:

- Screen capture
- Trojan Update
- Loading DLLs

- Starting executables
- Running shell commands
- Listing directories

Each time a command (task) is executed, the result of that command is stored in the registry under a subkey named “done” or “doneEXT”. The result (which are called “answers” by the authors) is then posted to the C&C server.

The ClientX backdoor is analyzed in depth in the Appendix 5.

2.2.5 The Karagany Backdoor

1. Description

Karagany is a simple backdoor that connects to the C&C and waits for commands. It can download and run additional executables, load/delete modules, read file content, reboot the computer, update itself and remove all components.

Besides backdoor functionality, it also extract credentials from Internet Explorer’s password manager to the prx.jpg file and injects a small DLL into the processes of web browsers. This DLL keeps listening on the outgoing network traffic and looking for the basic access authentication details sent over unencrypted HTTP. Affected browsers include: Internet Explorer, Firefox, Mozilla and Opera.

When executed, it copies itself to the folder under `%APPDATA%` and create a `.lnk` file in the `%STARTUP%` directory. Folder name and filename are chosen from the list of strings hardcoded in the binary:

Folder name	File name
Microsoft WCF services	SearchIndexer
Broker services	ImeBroker
Flash Utilities	fsutil
Media Center Programs;	PnPutil
Policy Definitions	BdeUISrv
Microsoft Web Tools	WinSAT
Reference Assemblies	pwNative
Analysis Services	SnippingTool

Folder name	File name
InstallShield Information	DFDWizard
IIS SQL Server	PrintBrmEngine
Diagnostics;	WbemMonitor
NTAPI Perfomance	dxpserver
WPF Platform	PowerMng

It also creates `C:\ProgramData\Mail\MailAg\ folder`, where the information harvested by downloaded modules will be stored.

After checking if the connection to the Internet is up, it sends the initial POST request to the C&C server. Known parameters used in C&C communication are:

- `&identifiant=<victim_uid>`, which is calculated based on system version, system install date, username and system metrics
- `&version=<bot_version_nr>`
- `&fichier=<file_content>`

2. List of known modules:

Screenshot module

This module is used to drop and run the DuckLink CmdCapture tool - a 3rd party freeware AutoIt application for capturing the screenshots (hxxp://www.ducklink.com/).

A screenshot of the desktop is saved into the `C:\ProgramData\Mail\MailAg\scs.jpg` file. Additionally, other system system information - such as day and time of capture, computer name, username, cpu architecture, os version, IP address, logon domain and logon server, desktop details (height, width, depth, refresh rate) and environmental variables - are logged in `C:\ProgramData\Mail\MailAg\scs.txt` file.

Module listing documents and other files

This module is used to list all files and documents with specified extensions, or which names contain specified strings, in the `C:\ProgramData\Mail\MailAg\fls.txt` file.
Saved information include path, size and modification time. File matching patterns:

pass.*	*.rtf	*.xls	*.pdf
secret.*	*.pst	*.doc	*.vmdk
*.pgp	*.p12	*.mdb	*.tc

2.3. C&C servers and victims

The Command and Control servers are compromised legitimate websites, like blogs, from different countries.

In total we have identified **219** unique domain names for these C&C servers hosted in 21 different countries.
We found most hosted C&Cs in the United States (81 servers), Germany (33 servers), the Russian Federation (19 servers) and the United Kingdom (7 servers).

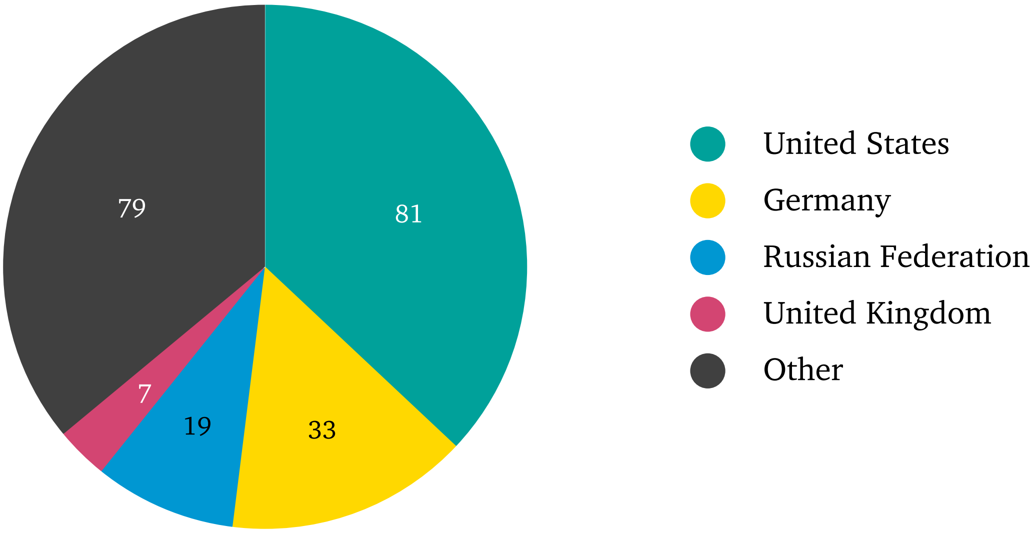
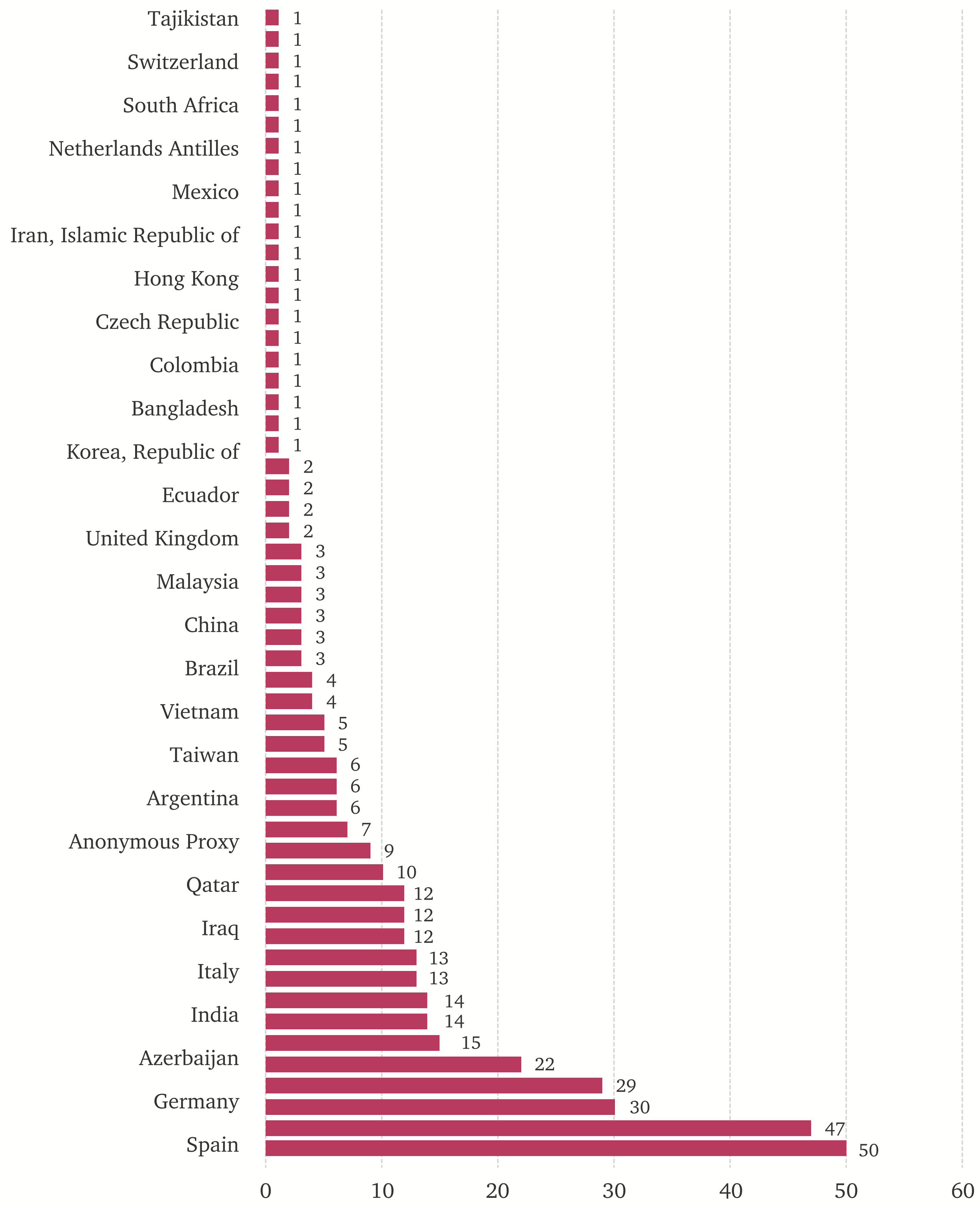


Figure 5. C&C country distribution

The table below shows the distribution of victims affected by the samples identified according to our KSN data. Victims infected with samples from any of the Crouching Yeti group's malware were found in:



65 of these C&C servers, in the following countries, were monitored during our investigation.

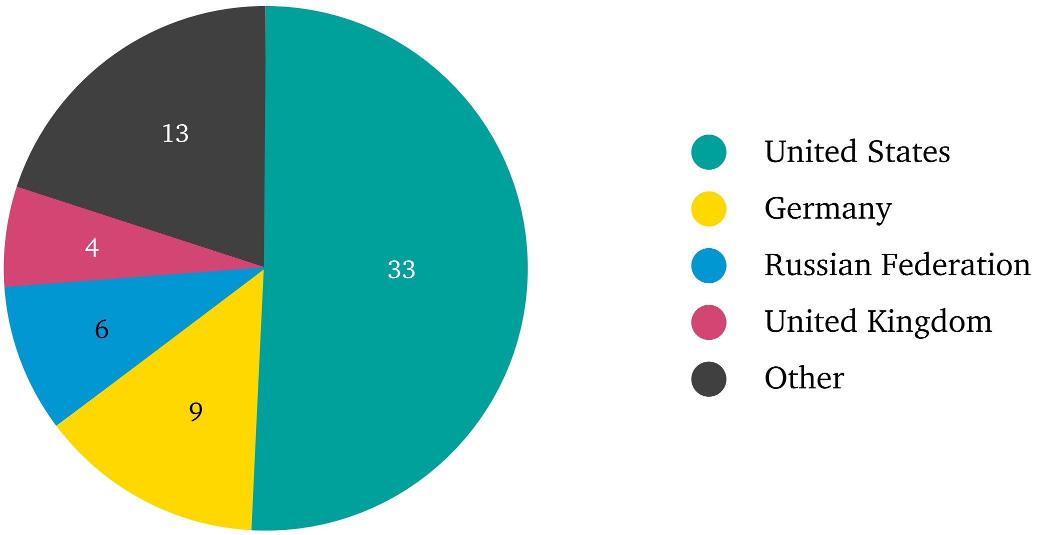


Figure 6. Monitored C&C servers country distribution

This monitoring enabled us to get a list of the victims connected to them.

1. C&C backend

The C&C Backend is written in PHP, consisting of 3 files:

- **"log.php"** is a Web-Shell, used for file level operations.
- **"testlog.php"** is not a PHP-script but it contains the C&C Server logfile of backdoor-connections. Please see **"source.php"** below for further information.
- **"source.php"**

The Backdoors interact with *"source.php"*, which is the control script. These are its functions on execution:

1. Collects the following information:

Information	Syntax/content	Used (written to log)
Timestamp	day-month-year hour:minute-second	Yes
IP-address	checks and return valid IP-address from HTTP-Request (`"HTTP_CLIENT_IP"`, `"HTTP_X_FORWARDED"`, `"HTTP_X_iFORWARDED_FOR"`, `"REMOTE_ADDR"`)	Yes
Host	reverse lookup of IP-address (gethostbyaddr)	No

Information	Syntax/content	Used (written to log)
Proxy	Proxy-IP-address if Bot connected through Proxy	No
UserAgent	UserAgent from HTTP-Request	Yes
Request-URI	string of URI requested by Bot	Yes
BotID	BotID transferred with HTTP-request	Yes

2. Writes above information to "testlog.php", separated by "Tabulator" and base64-encoded, with following syntax:

   <timestamp>\t<victim ip-address>\t<proxy>\t<botID>\t<request-uri>\t<useragent>

3. Writes all transferred HTTP-GET Variables to "*<botID>.log*", separated by "Tabulator" and base64-encoded.

4. If the bot executes an HTTP-POST-request, the transferred data is written to the file "*<botID>.ans*", enclosed in "xdata"-Tag with timestamp. ("ans" is the acronym for "Answer").

5. Checks for any file "*<botID>_*.txt*"

   a. If found the first step is to append the timestamp, filename and a "sent" Status indicated to "<botID>.log". Then the file content is transferred to the bot, embedded into HTML with HTML-Body *"No data!"* and HTML-Comment "havex" containing the data to be transferred. Finally the file on the server is removed. If this removal fails it is logged to "<botID>.log".

   b. If no matching file is found, a HTML-Response is sent with an empty "havex" HTML-Comment and HTML-Body text *"Sorry, no data corresponding your request."*

2.3.1. Victims

The term "victim" in this section refers to a botID (unique String of the Backdoor), connecting to one or more C&C Servers. Based on the 45 C&C Servers we monitored, a total of **2,811** unique Victims were discovered.

The average number of victims per C&C is 70:

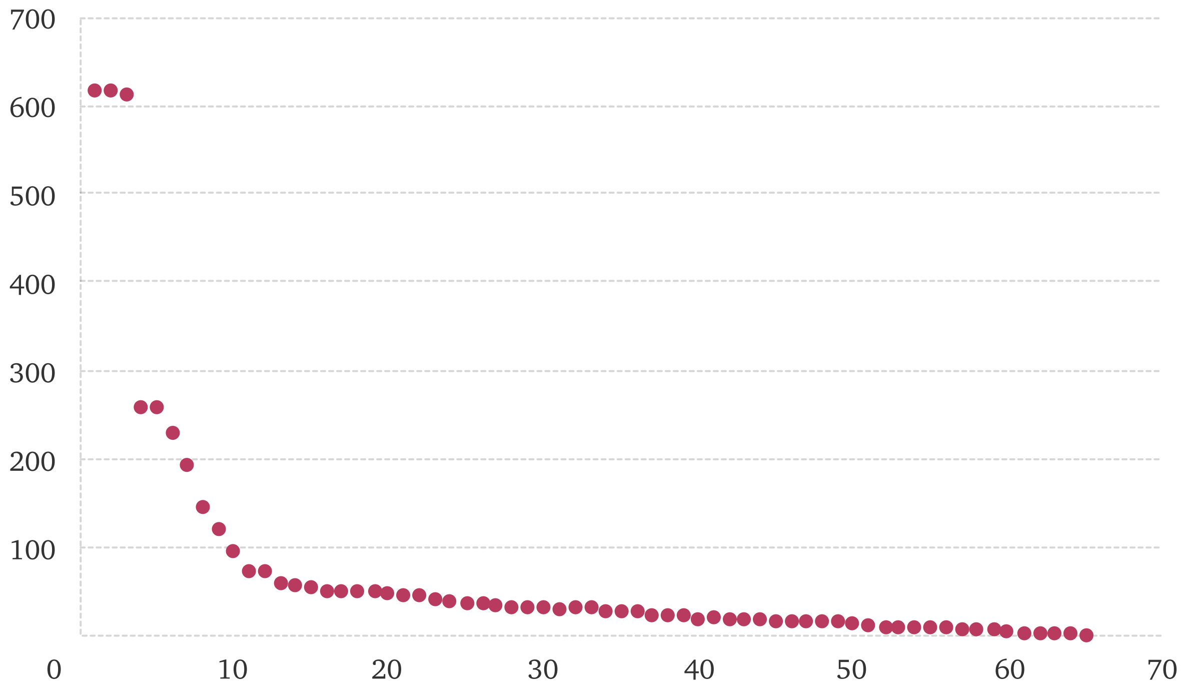


Figure 7. Number of victims (Y) per C&C server instance (X)

The following chart depicts the first (red line) and last (blue line) appearance of each victim on the C&C.

The “FirstHit” shows how the rate of accumulating new victims has accelerated over the course of 2014. “LastHit” shows how the last connection of victims to C&C servers also increases over time. This could mean victims are disinfecting their computers, or it may be that they simply report to a different C&C server that we do not monitor.

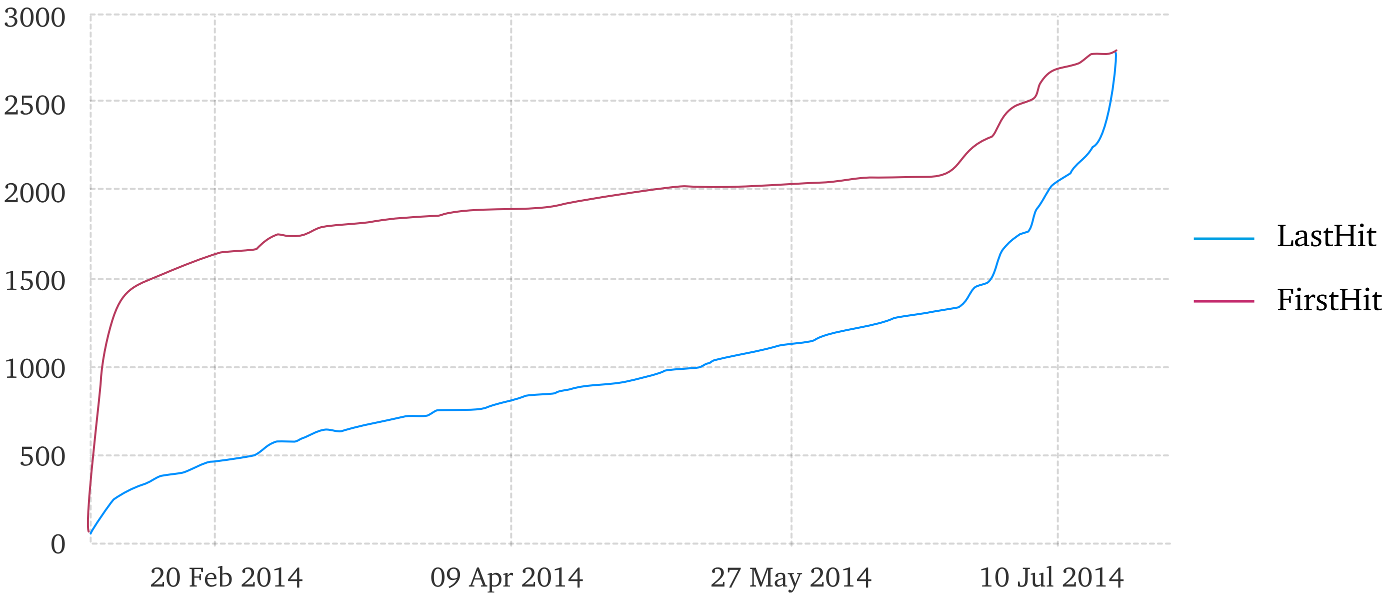


Figure 8. Evolution of “FirstSeen“ and “LastSeen“ victims

Mapping unique hits of victims per day also indicates a decrease of “active” infections. The following chart clearly shows a difference between weekdays (groups of five higher bars) and weekends (two lower bars). The daily unique hit-rate fell by about half from around 800 connections at the beginning of 2014 to around 400 connections per week-day by the middle of the year:

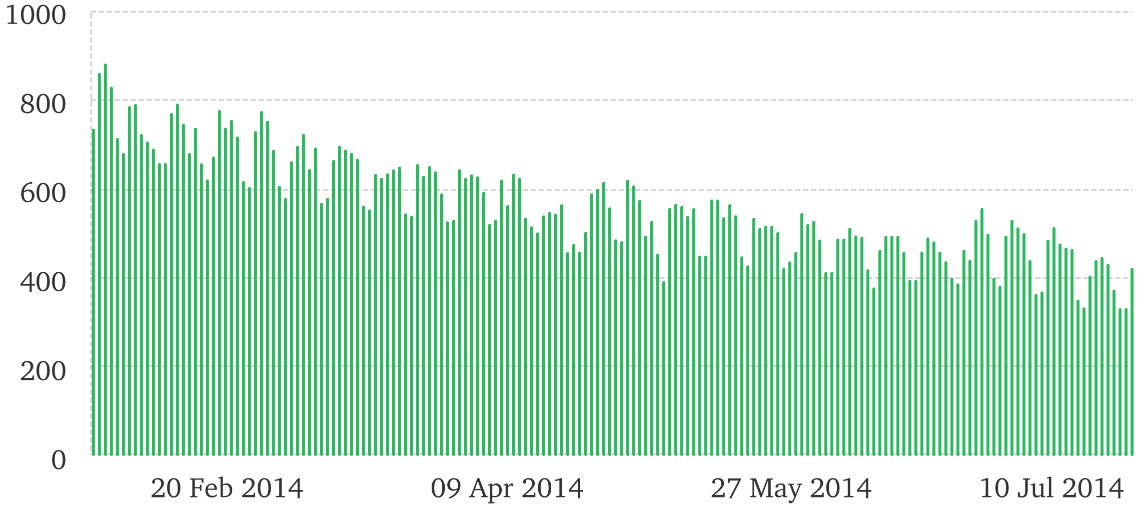


Figure 9. Unique victims per day reporting to C&Cs

More than half of the victims always connect from the same IP address. Less than half of the victims connect from two or more different IP addresses as the following graph shows.

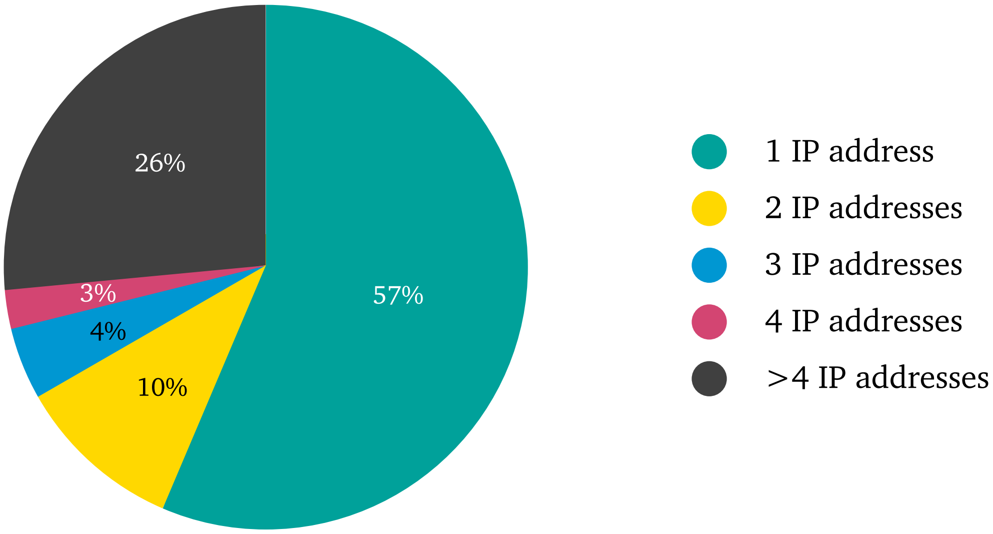


Figure 10. Number of different IPs per victim

This might indicate that some of the victims are behind proxies, which makes sense for corporate environments. Victims using many different IP addresses may indicate the use of laptops computers.

The following chart visualizes all the unique victims connecting to C&C servers. The main C&C Servers can be clearly seen in Russia and the USA. The victims are distributed across **99** different countries.

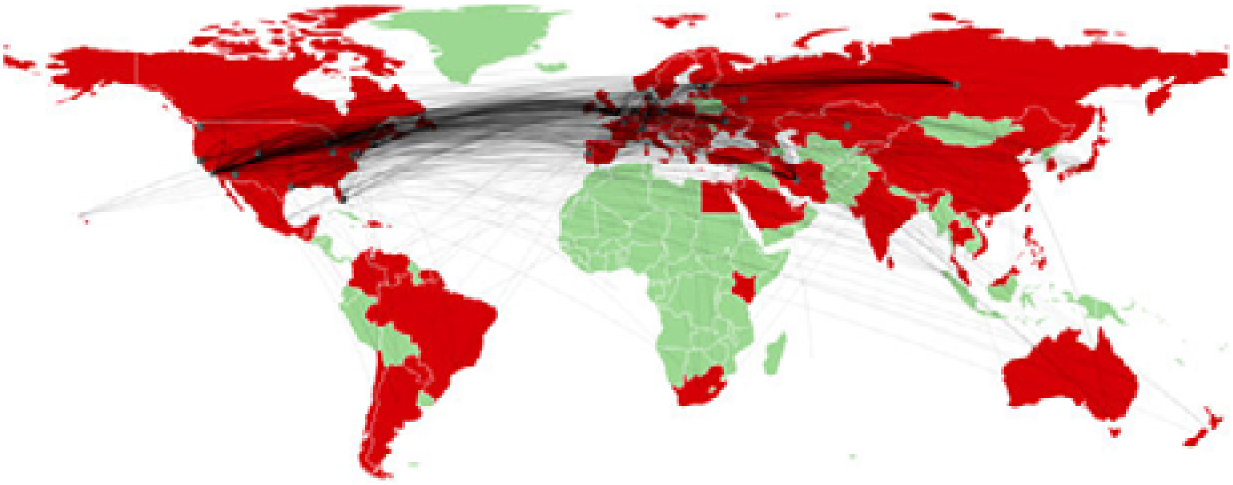


Figure 11. Connection between victims and C&C

From the total of **2,811** victims, it was possible to accurately identify **106** of them. Appendix 8 contains a brief description about the sector/company on which these victims operate.

The table below shows a summarizes the distribution of the identified victims per sector.

Sector	Number of victim organizations
Educational	32
Research	14
Mechanical Engineering	10
Information Technology	10
Construction	9
Government	8
Health	5
Network Infrastructure	3
Pharmaceutical	2
Electrical Engineering	2
Packaging	2
Financial	2
Energy	2
Cleaning	1
Automotive	1
Structural Engineering	1
Transportation	1
Chemical	1

1. Havex Victims

Based on our monitoring, the most widespread Backdoor is Havex with a total of **2,470** infected systems, mostly based in USA and Spain.

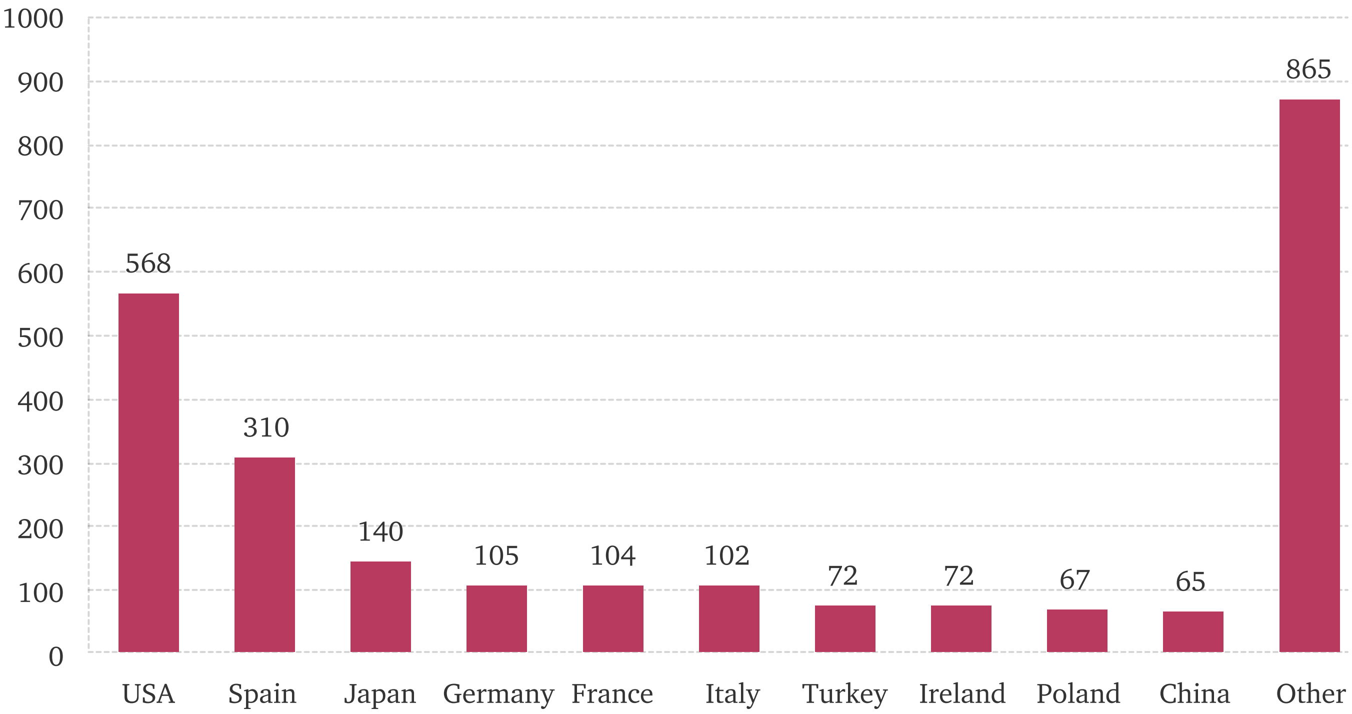


Figure 12. Havex victims per country

There are 32 different versions of Havex being used among all victims, with 51 victims left without identifiable Havex-Version. Havex Version 024, compiled in the end of 2012, is the most widespread.

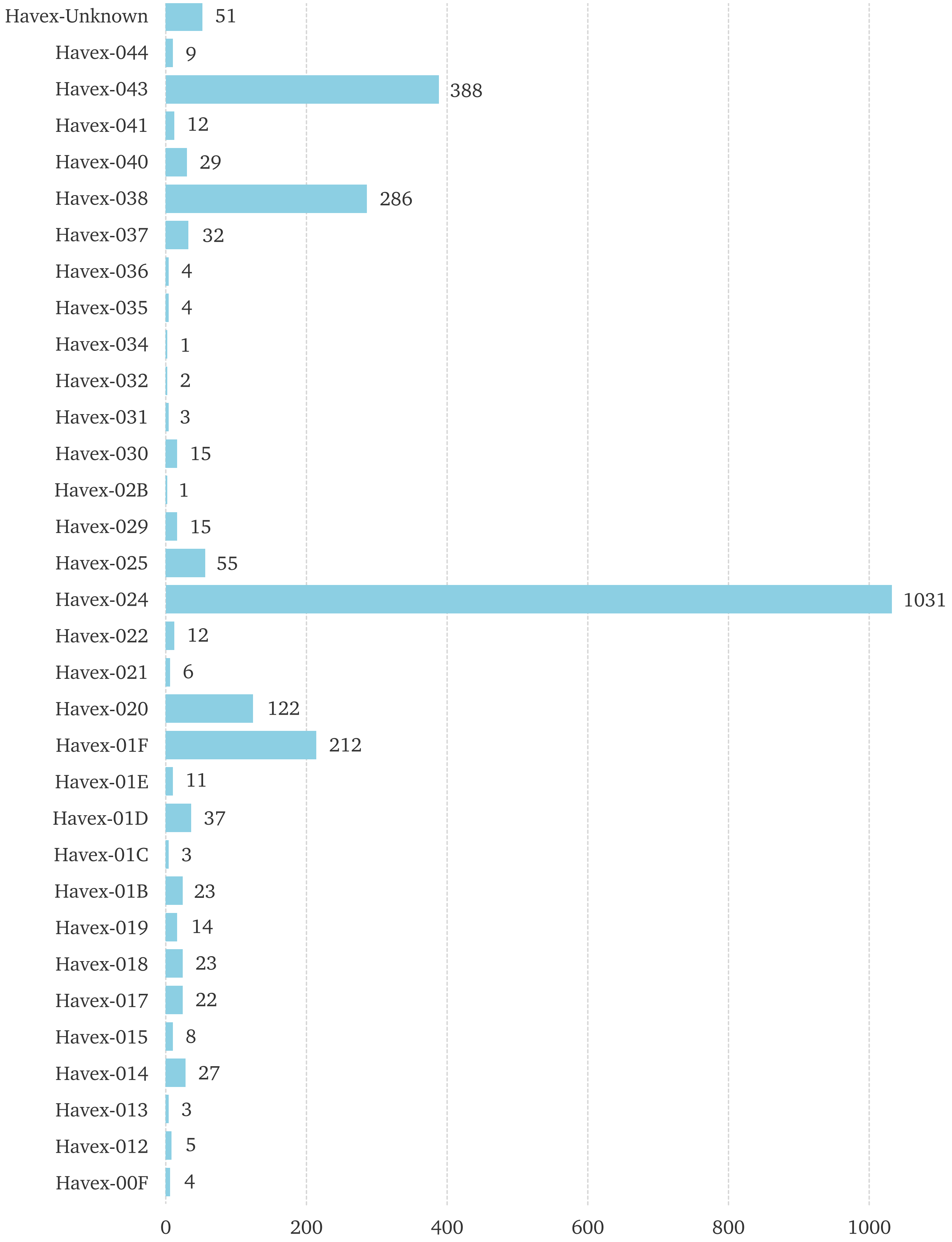


Figure 13. Havex version distribution

Besides the Havex version, also the OS-Version of the victim computer is also communicated to the C&C server. The most common Operating System among victims is Windows XP, but Windows 8.1 is also in the list.

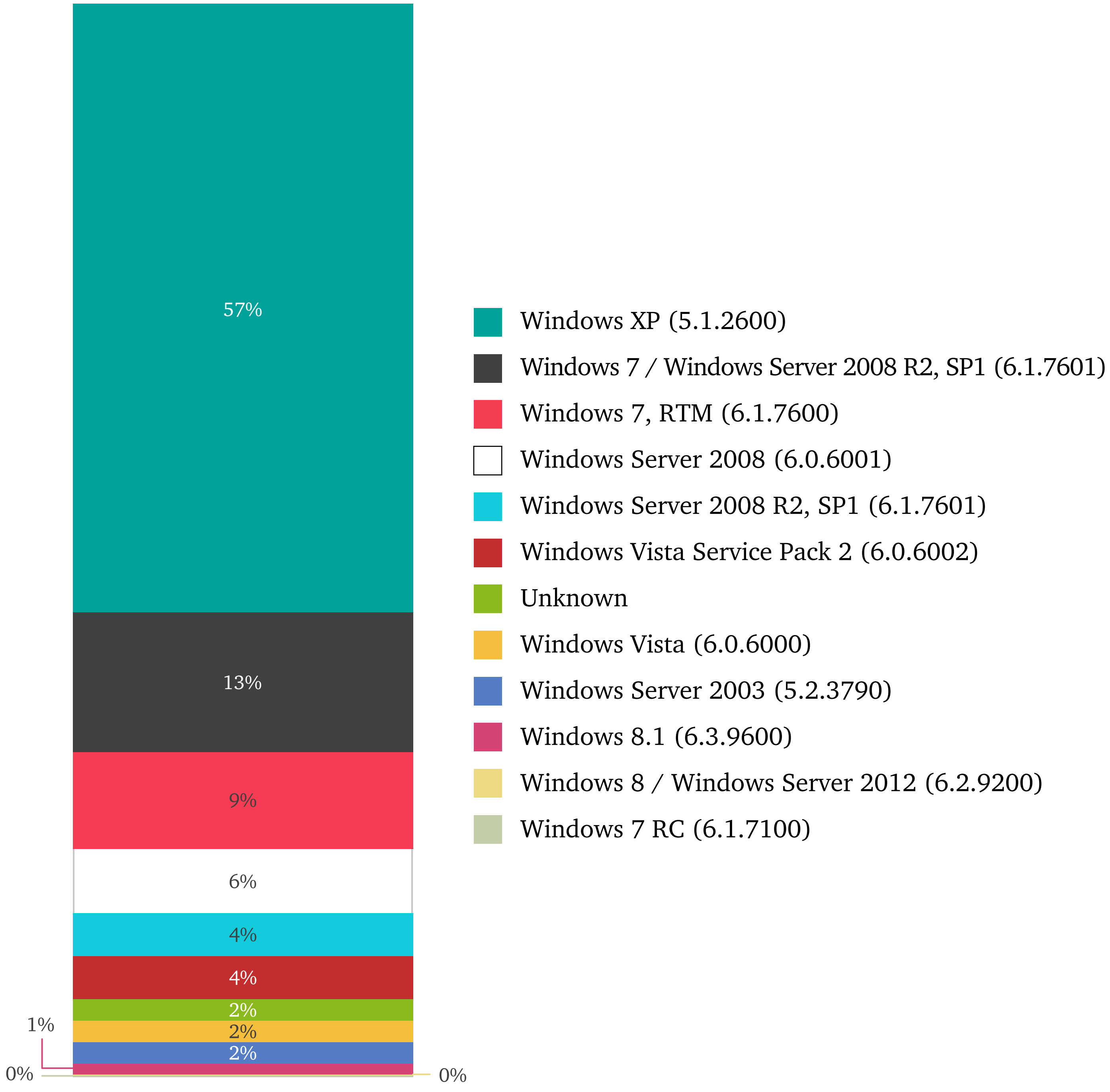


Figure 14. OS distribution among victims

2. Sysmain Victims

The Sysmain victims connect to six of the monitored C&C servers, where **261** unique victims were counted, located in **38** different countries.

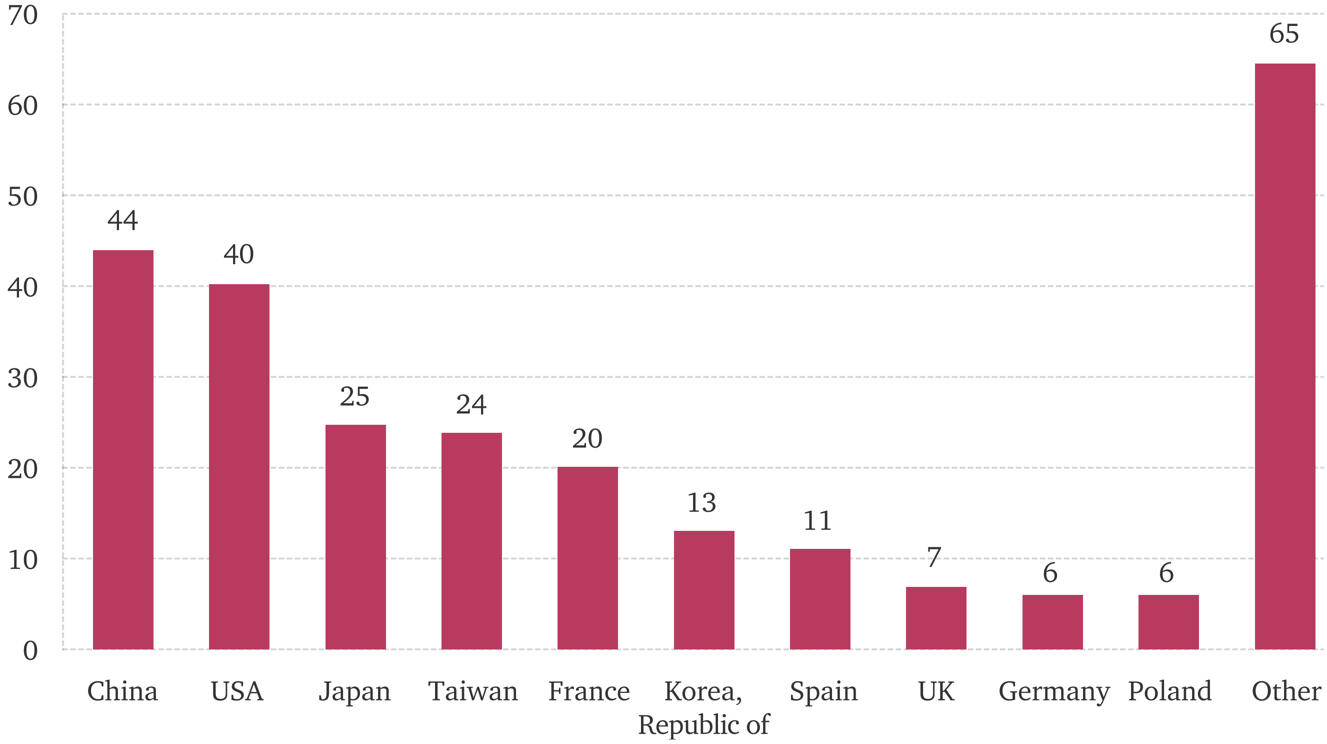


Figure 15. Sysmain victims per country

3. ClientX Victims

Victims of the Clientx backdoor connect to 2 of the monitored C&C Servers, where 10 unique Victims were counted in **5** different countries.

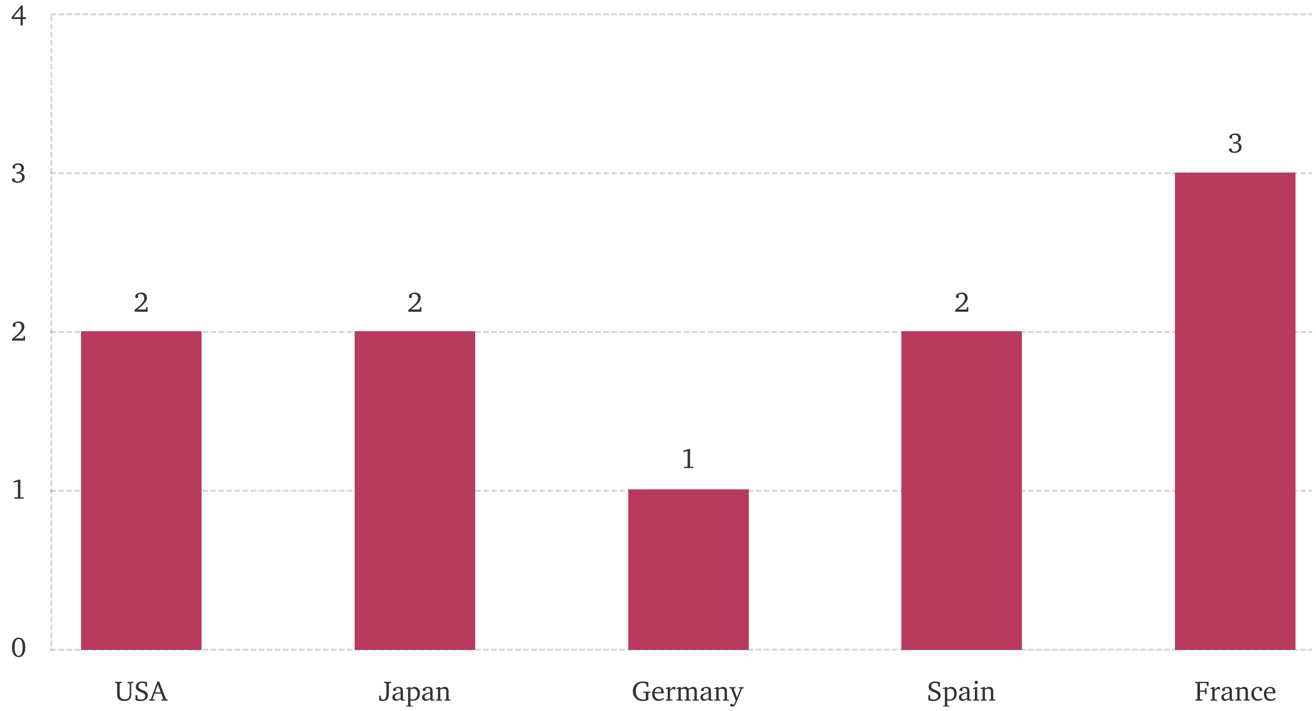


Figure 16. ClientX victims per country

2.3.2. Victims-C&C relationship

Based on the analysis of the monitored C&C servers we identify some clusters depending on malware versions and the victims.

This graph visualizes these relations. Every dot represents a victim, different backdoors and versions are colored differently. The C&C servers are also represented as dot where several clients connect. Grey lines are connections from a victim to its C&C Server.

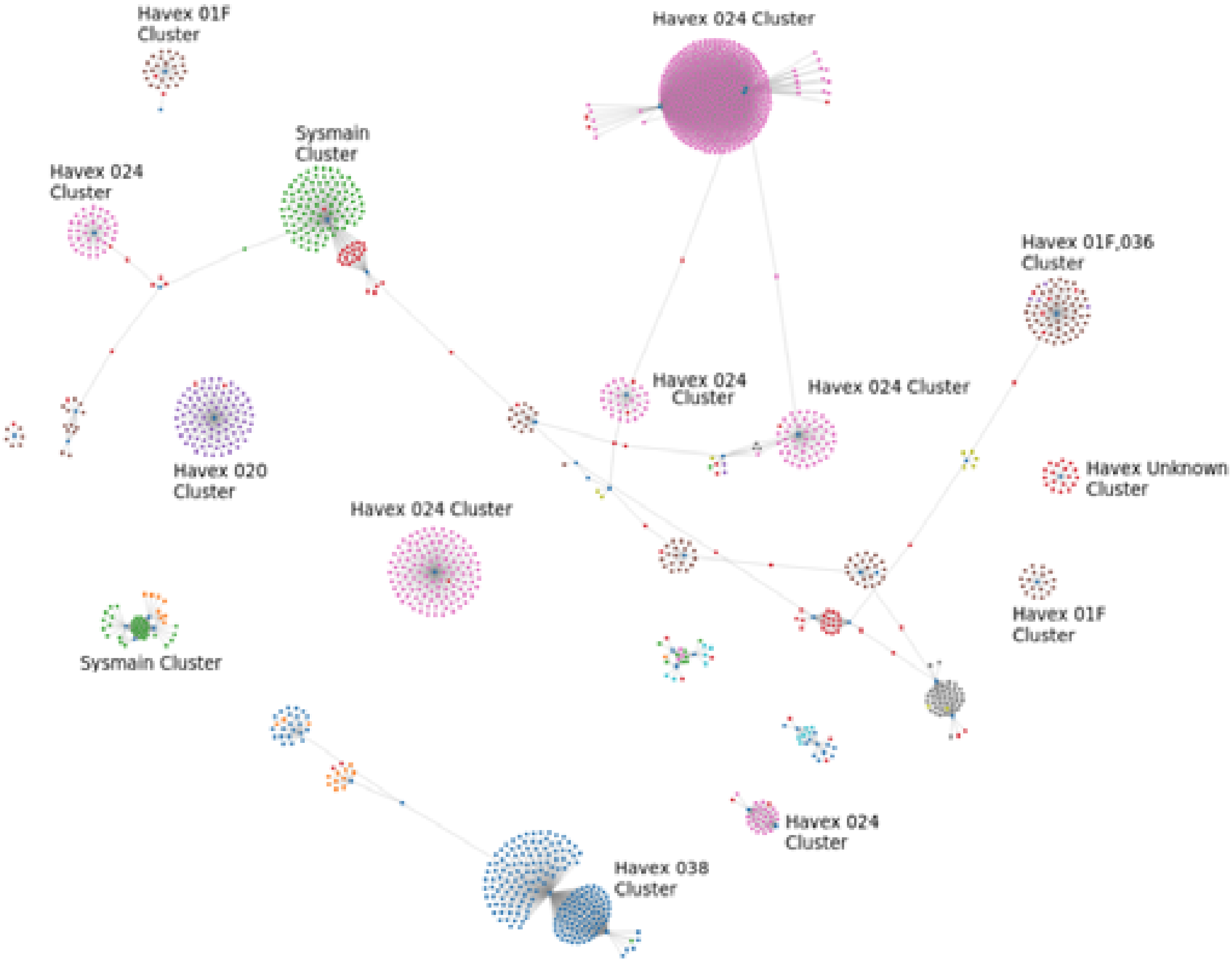


Figure 17. Clusters of victim-C&C relationships

Some C&C servers are dedicated to a given version of a backdoor (big Cluster). Others share connections with different backdoor versions and different backdoors.

Breaking this down to the sectors of the identified victims, we cannot see any correlation between C&Cs and victims. The same sectors are targeted with different backdoor versions.

3. Attribution

3.1. Non-specific Data

Compared to our other APT research the available data is more non-specific than usual. There simply is no one piece or set of data that would lead to the conclusion that the threat actor is Bear, Kitten, Panda, Salmon, or otherwise. Significant data points below.

File timestamp analysis and unique strings

It is rare to see file timestamps used as a precise, primary source of information when it comes to threat actor attribution. In previous reports, these timestamps are used as supporting, or secondary pieces of data. They may help to suggest or support a time range of attacker activity, but they are very easily modified. So it is not very helpful to focus on this data set.

The strings present in the backdoors, web components, and exploits are English. Almost 200 malicious binaries and the related operational content all present a complete lack of Cyrillic content, the opposite of our documented findings from researching Red October, Miniduke, Cosmicduke, Snake, and TeamSpy.

The OPC module strings include typos and bad grammar. Some are so bad they are almost silly, and there doesn't seem to be a consistent pattern here:

```
Programm was started at %02i:%02i:%02i
Start finging of LAN hosts...
Finding was fault. Unexpective error
Was found %i hosts in LAN:
Hosts was't found.
```

There are also three interesting strings inside the Karagany backdoor:

`identifiant` (which is French for *identifier*)`,` `fichier` (French for *file*) `and` `liteliteliteskot` (*lite scot* is Swedish for *little sheet*)

Timestamp details

Timestamp analysis is based on the total number of 154 collected binaries:

- 124 samples of Havex loader (versions 01 - 044) + 7 downloaded modules
- 7 samples of Sysmain backdoor
- 4 samples of Ddex loader
- 1 sample of ClientX backdoor
- 4 samples of Karagany Trojan + 2 downloaded modules
- 3 samples of Trojanized installers

Highlights:

- The earliest samples related to this campaign are the Ddex loader binaries with compilation timestamps between **October and November 2010**.
- The first Havex loader samples are the version 01 and version 02 samples with compilation timestamps from **28th September 2011**.
- The latest known samples are Havex loader version 044, compiled on 7th May 2014 and all OPC modules compiled in **April and May 2014**.
- Most of samples were compiled during the weekdays, although there is a couple of samples with the compilation timestamp indicating Saturday
- Most of samples were compiled between **6:00 and 16:00 UTC** with the peak between **6:00 and 8:00 UTC**.
    - Earliest compilation hour: 02:15:23 UTC (Wed, 28 Sep 2011)
    - Latest hour: 23:39:34 UTC (Thu, 02 Jun 2011)

Activity / Year (all samples):

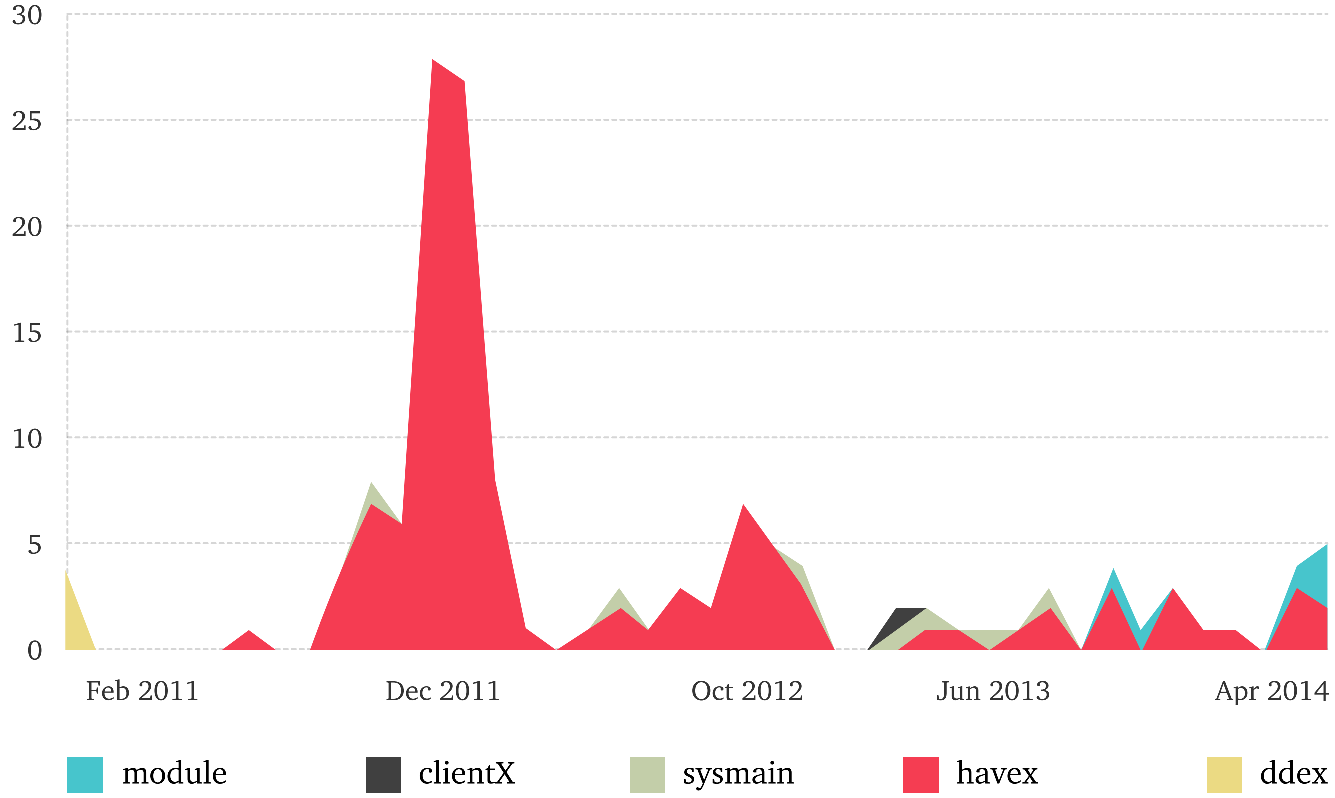


Figure 18. Activity per year on different components

Activity / Weekdays based on compilation time:

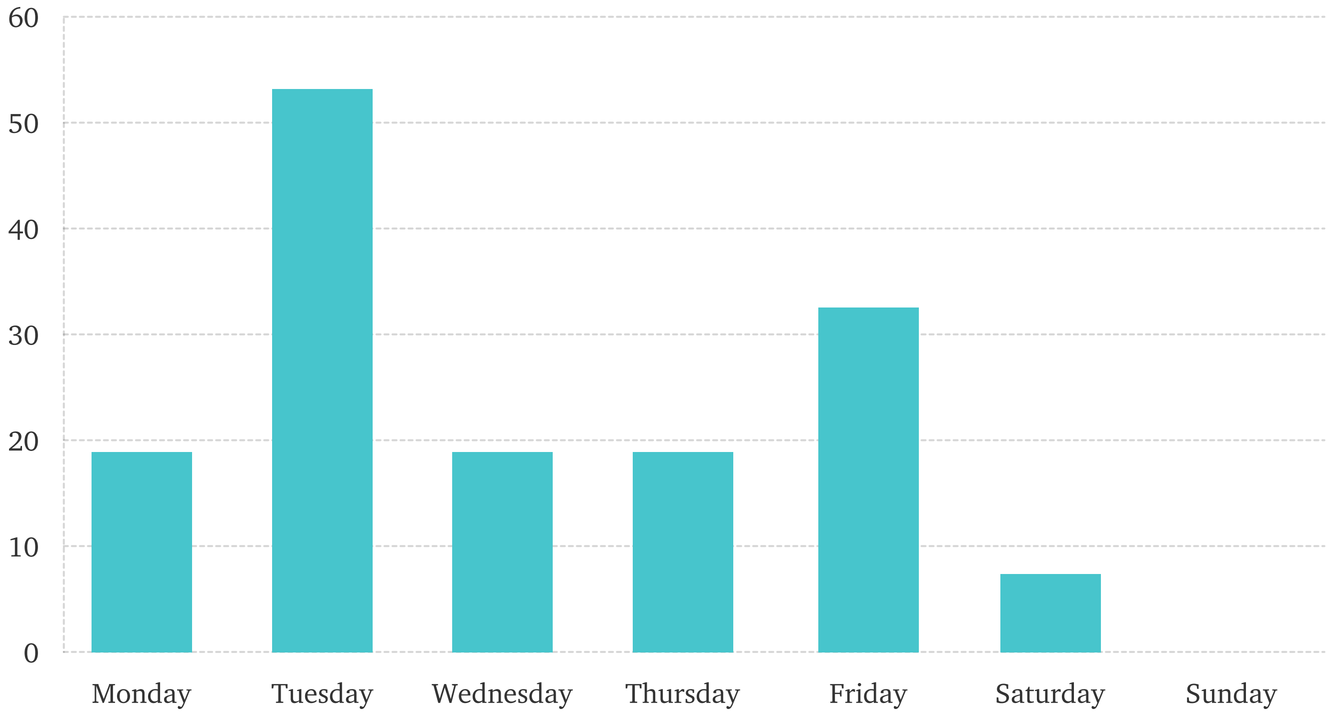


Figure 19. Activity per weekday distribution

Activity / Hours (UTC) based on compilation time:

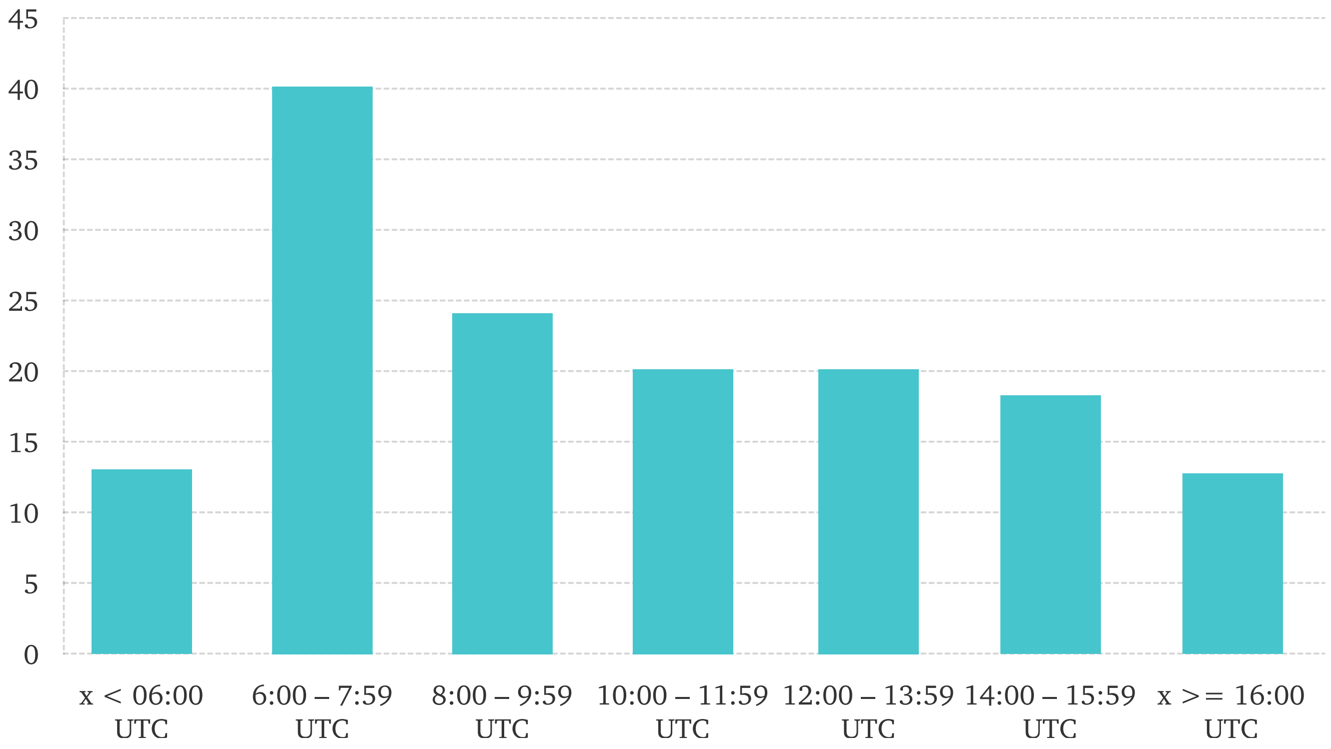


Figure 20. Activity per hour distribution

3.2. Exploit server activity

All the exploit servers delivered slightly modified ripped content from open source repositories. All the servers appear to be hacked servers. According to the available data, no zero-day exploits were used in any of these attacks, either to compromise the servers in the first place, or delivered as client side attack exploits by the Lights Out Exploit Kit.

While this purely malicious re-use of metasploit PoC highlights the danger that these attack tools pose, it is also unusual to see an exclusively metasploit attack toolset effectively used in this way, delivered from what appear to be a chain of higher value compromised sites.

All of these compromised web applications were vulnerable to freely available offensive security tools. We acknowledge that many of the compromised referrer servers were related to industrial power producers in some way. However, these targets almost seem an afterthought, as the exploit servers themselves were compromised web servers from Cuban travel agency sites, a Californian winery site, a US based women's fashion site, an Iranian general interest/religious inspiration site, a number of dating and adult content websites, and a variety of others. Although, we note that the known Trojanized software packages were ICS/SCADA related as well, possibly because those victim sets or environments required special attention. So, while there was a strong set of offensive activities on power producers during the campaigns, it was by no means the full focus of them.

3.3. Victim characteristics and categories

While it may be “shocking” to observe industrial power producers around the world targeted by any one threat actor, this actor’s attack activity does not appear to be constrained to this sector. The related industries of interest show a much broader global scope than previously discussed, and the geographic regions of interest have gone completely undiscussed. For example, Spain had the highest number of victims. However, it appears that there was no significant correlation between the victim location and the C&C geolocation. According to our data, the list rounds out with the victim organizations fitting the following additional categories:

- Pharmaceuticals
- Health
- Cleaning
- Education
- Automotive
- Transportation
- Packaging
- Network Infrastructure
- Information Technology
- Structural Engineering
- Mechanical Engineering

4. Conclusions

The Crouching Yeti actor has been performing massive surveillance campaigns over the last few years, at least since 2010. Their targets included thousands of victims of which we were able to identify a few, confirming Crouching Yeti's interest in several strategic sectors.

The distribution strategy of the group focuses on methods following this targeted philosophy, including spear-phishing and waterholing. Noticeably, they also compromised legitimate software packages from strategic actors in the SCADA sector in order to infect their final victims. The victim list confirms that the tactic proved successful.

There is nothing especially sophisticated in the exploits used, or in the malware used to infect victims. The RATs are flexible enough to perform surveillance and data exfiltration efficiently. The attackers used dozens of compromised servers as C&C domains with a simple, but effective, PHP backend.

However, there is an interesting connection with this group and the LightsOut exploit kit for the distribution of its malware in some waterholing attacks. We believe they are likely its only operators as of June 2014.

Thanks to the monitoring of several of the C&C domains used by the group, we were able to identify several victims. This victim list reinforces the interests shown by the Crouching Yeti actor in strategic targets, but also shows the interest of the group in many other not-so-obvious institutions. We believe they might be collateral victims, but it might also be fair to redefine the Crouching Yeti actor not only as a highly targeted one in a very specific area of interest, but a broad surveillance campaign with interests in different sectors.

We will continue to monitor this threat actor.