

# Equation: The Death Star of Malware Galaxy

By GReAT

Published: 2015-02-16 · Archived: 2026-04-05 18:12:20 UTC

[Download “Equation group: questions and answers” PDF](#)

## “Houston, we have a problem”

One sunny day in 2009, Grzegorz Bręczyszczkiewicz<sup>1</sup> embarked on a flight to the burgeoning city of Houston to attend a prestigious international scientific conference. As a leading scientist in his field, such trips were common for Grzegorz. Over the next couple of days, Mr Bręczyszczkiewicz exchanged business cards with other researchers and talked about the kind of important issues such high level scientists would discuss (which is another way of saying “who knows?”). But, all good things must come to an end; the conference finished and Grzegorz Bręczyszczkiewicz flew back home, carrying with him many highlights from a memorable event. Sometime later, as is customary for such events, the organizers sent all the participants a CDROM carrying many beautiful pictures from the conference. As Grzegorz put the CDROM in his computer and the slideshow opened, he little suspected he had just become the victim of an almost omnipotent cyberespionage organization that had just infected his computer through the use of three exploits, two of them being zero-days.

## A rendezvous with the “God” of cyberespionage

It is not known when the Equation<sup>2</sup> group began their ascent. Some of the earliest malware samples we have seen were compiled in 2002; however, their C&C was registered in August 2001. Other C&Cs used by the Equation group appear to have been registered as early as 1996, which could indicate this group has been active for almost two decades. For many years they have interacted with other powerful groups, such as the Stuxnet and Flame groups; always from a position of superiority, as they had access to exploits earlier than the others.

The #EquationAPT group is probably one of the most sophisticated cyber attack groups in the world  
#TheSAS2015

[Tweet](#)

Since 2001, the Equation group has been busy infecting thousands, or perhaps even tens of thousands of victims throughout the world, in the following sectors:

- Government and diplomatic institutions
- Telecoms
- Aerospace
- Energy
- Nuclear research
- Oil and gas

- Military
- Nanotechnology
- Islamic activists and scholars
- Mass media
- Transportation
- Financial institutions
- Companies developing encryption technologies

To infect their victims, the Equation group uses a powerful arsenal of “implants” (as they call their Trojans), including the following we have created names for: EQUATIONLASER, EQUATIONDRUG, DOUBLEFANTASY, TRIPLEFANTASY, [FANNY](#) and GRAYFISH. No doubt other “implants” exist which we have yet to identify and name.

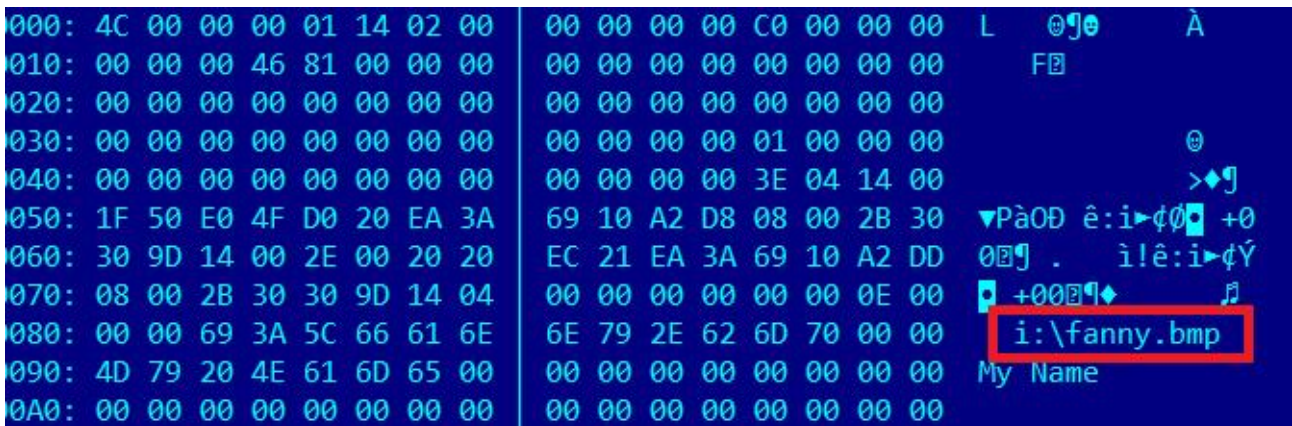
The #EquationAPT group interacted with other powerful groups, such as the #Stuxnet and #Flame groups #TheSAS2015

[Tweet](#)

The group itself has many codenames for their tools and implants, including *SKYHOOKCHOW*, *UR*, *KS*, *SF*, *STEALTHFIGHTER*, *DRINKPARSLEY*, *STRAITACID*, *LUTEUSOBSTOS*, *STRAITSHOOTER*, *DESERTWINTER* and *GROK*. Incredible as it may seem for such an elite group, one of the developers made the unforgivable mistake of leaving his username: “*RMGREE5*“, in one of the malware samples as part of his working folder: “*c:\users\rmgree5\*“.

Perhaps the **most powerful tool in the Equation group’s arsenal** is a mysterious module known only by a cryptic name: “*nls\_933w.dll*“. It allows them to **reprogram the hard drive firmware** of over a dozen different hard drive brands, including Seagate, Western Digital, Toshiba, Maxtor and IBM. This is an astonishing technical accomplishment and is testament to the group’s abilities.

Over the past years, the Equation group has performed many different attacks. One stands out: the **Fanny** worm. Presumably compiled in July 2008, it was first observed and blocked by our systems in December 2008. 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 was also used in one of the early versions of Stuxnet from 2009.



*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 that the Equation group had access to these zero-days *before* the Stuxnet group. The main purpose of Fanny was the **mapping of air-gapped networks**. For this, it used a unique USB-based command and control mechanism which allowed the attackers to pass data back and forth from air-gapped networks.

Two zero-day exploits were used by the #EquationAPT group before they were integrated into #Stuxnet #TheSAS2015

[Tweet](#)

In the coming days, we will publish more details about the Equation group malware and their attacks. The first document to be published will be a general FAQ on the group together with indicators of compromise.

By publishing this information, we hope to bring it to the attention of the ITSec community as well as independent researchers, who can extend the understanding of these attacks. The more we investigate such cyberespionage operations, the more we understand how little we actually know about them. Together, we can lift this veil and work towards a more secure (cyber-)world.

[Download “Equation group: questions and answers” PDF](#)

**Indicators of compromise (“one of each”):**

<b>Name</b>	EquationLaser
<b>MD5</b>	752af597e6d9fd70396accc0b9013dbe
<b>Type</b>	EquationLaser installer
<b>Compiled</b>	Mon Oct 18 15:24:05 2004
<b>Name</b>	Disk from Houston “autorun.exe” with EoP exploits
<b>MD5</b>	6fe6c03b938580ebf9b82f3b9cd4c4aa
<b>Type</b>	EoP package and malware launcher
<b>Compiled</b>	Wed Dec 23 15:37:33 2009
<b>Name</b>	DoubleFantasy
<b>MD5</b>	2a12630ff976ba0994143ca93feccd17f
<b>Type</b>	DoubleFantasy installer
<b>Compiled</b>	Fri Apr 30 01:03:53 2010
<b>Name</b>	EquationDrug

<b>MD5</b>	4556ce5eb007af1de5bd3b457f0b216d	
<b>Type</b>	EquationDrug installer (“LUTEUSOBSTOS”)	
<b>Compiled</b>	Tue Dec 11 20:47:12 2007	
<b>Name</b>	GrayFish	
<b>MD5</b>	9b1ca66aab784dc5f1dfe635d8f8a904	
<b>Type</b>	GrayFish installer	
<b>Compiled</b>	Compiled: Fri Feb 01 22:15:21 2008 (installer)	
<b>Name</b>	Fanny	
<b>MD5</b>	0a209ac0de4ac033f31d6ba9191a8f7a	
<b>Type</b>	Fanny worm	
<b>Compiled</b>	Mon Jul 28 11:11:35 2008	
<b>Name</b>	TripleFantasy	
<b>MD5</b>	9180d5affe1e5df0717d7385e7f54386	loader (17920 bytes .DLL)
<b>Type</b>	ba39212c5b58b97bfc9f5bc431170827	encrypted payload (.DAT)
<b>Compiled</b>	various, possibly fake	
<b>Name</b>	_SD_IP_CF.dll – unknown	
<b>MD5</b>	03718676311de33dd0b8f4f18cffd488	
<b>Type</b>	DoubleFantasy installer + LNK exploit package	
<b>Compiled</b>	Fri Feb 13 10:50:23 2009	
<b>Name</b>	nls_933w.dll	
<b>MD5</b>	11fb08b9126cdb4668b3f5135cf7a6c5	
<b>Type</b>	HDD reprogramming module	
<b>Compiled</b>	Tue Jun 15 20:23:37 2010	
<b>Name</b>	standalonegrok_2.1.1.1 / GROK	
<b>MD5</b>	24a6ec8ebf9c0867ed1c097f4a653b8d	
<b>Type</b>	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  
computertechnanalysis[.]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.moood[.]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  
rampagegrammar[.]com

rubi4edit[.]com  
rubiccrum[.]com  
rubiccrumb[.]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:**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

```
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*))  
}
```

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22

```
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="yyyyyyyyyyyyyyyyyy"  
    $a3="002"  
  condition:  
    (($mz at 0) and all of ($a*)) and filesize < 500000  
}
```

1  
2  
3

```
rule apt_equation_equationlaser_runtimeclasses {  
  meta:  
    copyright = "Kaspersky Lab"
```

```
4     description = "Rule to detect the EquationLaser malware"
5     version = "1.0"
6     last_modified = "2015-02-16"
7     reference = "https://securelist.com/blog/"
8     strings:
9         $a1="?a73957838_2@@YAXXZ"
10        $a2="?a84884@@YAXXZ"
11        $a3="?b823838_9839@@YAXXZ"
12        $a4="?e747383_94@@YAXXZ"
13        $a5="?e83834@@YAXXZ"
14        $a6="?e929348_827@@YAXXZ"
15    condition:
16        any of them
17    }
```

```
1 rule apt_equation_cryptotable {
2 meta:
3     copyright = "Kaspersky Lab"
4     description = "Rule to detect the crypto library used in Equation group malware"
5     version = "1.0"
```

```
6     last_modified = "2015-02-16"
7     reference = "https://securelist.com/blog/"
8 strings:
9     $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
10    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
11    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}
12 condition:
13     $a
14 }
15
16
17
18
19
```

<sup>1</sup> pseudonym, to protect the original victim’s identity >>

<sup>2</sup> the name “Equation group” was given because of their preference for sophisticated encryption schemes >>

**SUBSCRIBE NOW FOR KASPERSKY LAB'S APT INTELLIGENCE REPORTS**

Source: <https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/>