Star of Malware Galaxy

By GReAT on February 16, 2015. 6:55 pm

Download "Equation group: questions and answers" PDF

"Houston, we have a problem"

One sunny day in 2009, Grzegorz Brzęczyszczykiewicz[1] 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 Brzęczyszczykiewicz 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 Brzęczyszczykiewicz 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 became 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[2] 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

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

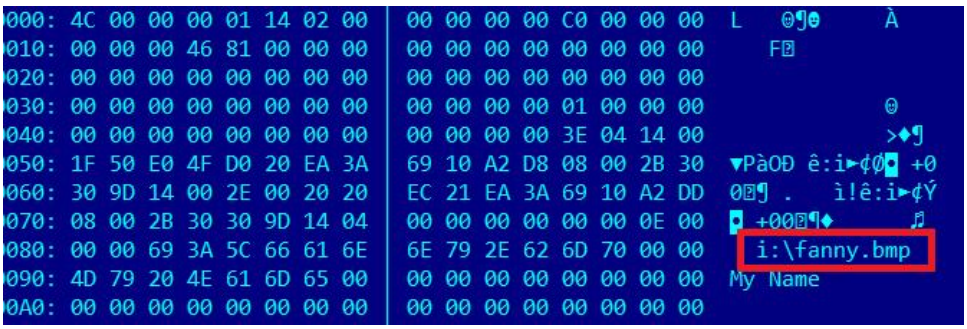
To infect their victims, the Equation group uses a powerful arsenal of "implants" (as they call their Trojans), including the following we have created names for: EQUATIONLASER, EQUATIONDRUG, DOUBLEFANTASY, TRIPLEFANTASY, FANNY and GRAYFISH. No doubt other "implants" exist which we have yet to identify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

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

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.

Tweet

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

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, we 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”):

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)
Type	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 Exploitati
    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 confi
    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=“yyyyyyyyyyyyyyyy”
    $a3=“002”
```

```
18
19
20  condition:
21
22  (($mz at 0) and all of ($a*))  and filesize &lt; 500000
    }
```

```
1
2   rule apt_equation_equationlaser_runtimeclasses {
3
4   meta:
5
6       copyright = “Kaspersky Lab”
7       description = “Rule to detect the EquationLaser malware”
8       version = “1.0”
9       last_modified = “2015-02-16”
10      reference = “https://securelist.com/blog/”
11
12  strings:
13
14      $a1=“?a73957838_2@@YAXXZ”
15      $a2=“?a84884@@YAXXZ”
16      $a3=“?b823838_9839@@YAXXZ”
17      $a4=“?e747383_94@@YAXXZ”
18      $a5=“?e83834@@YAXXZ”
19      $a6=“?e929348_827@@YAXXZ”
20
21  condition:
22
23      any of them
    }
```

```
1
2   rule apt_equation_cryptotable {
3
4   meta:
5
6       copyright = “Kaspersky Lab”
7       description = “Rule to detect the crypto library used in
8       version = “1.0”
9       last_modified = “2015-02-16”
10      reference = “https://securelist.com/blog/”
11
12  strings:
13
14
15      $a={37 DF E8 B6 C7 9C 0B AE 91 EF F0 3B 90 C6 80 85 5D 19
16
17  condition:
18
19      $a
    }
```

[1] pseudonym, to protect the original victim’s identity >>

[2] the name “Equation group” was given because of their preference for sophisticated encryption schemes >>

APT CYBER ESPIONAGE EQUATION FLAME
GAUSS SPYWARE STUXNET TARGETED ATTACKS

Share post on:

Related Posts

Happy IR in the New Year!

Kaspersky Security Bulletin: Review of the Year 2017

Android commercial spyware

THERE ARE 28 COMMENTS

lynx
Posted on February 17, 2015. 4:58 am

Ok, reading through NSA files that Der Spiegel released i found this:

http://www.spiegel.de/media/media-35661.pdf

This is a file that shows the job postings for NSA interns, you can find a NSA wiki link in the last page. And this is very interesting:

(TS//SI//REL) Create a covert storage product that is enabled from a hard drive firmware modification. The ideia would be to modify the firmware of a particular hard drive so that it normally only recognizes half of its available space. It would report this size back to the operating system and not provide any way to access the additional space.

This is a 2006 document, it took 8 years to finish this product, which is what kaspersky found.

So maybe you guys would easily find the malware if you revert the firmware to a state prior of this date.

REPLY

Bildos
Posted on February 17, 2015. 6:43 am

Firmware – definitely it's something what AV should start to scan / check.
Yes it's not easy task but absolutely needed to provide protection.
What's required to check? Firmware modifications- to verify if we have version in 100% confirmed by vendor.

REPLY

pj

Posted on February 17, 2015. 9:13 am

I've read that most hard drive firmware is write-only

REPLY

Nigel Tolley

Posted on February 17, 2015. 1:14 pm

I think you may have got that backward. But it's wrong either way.

The whole point of this is that they (NSA) have worked out how to re-write the HDD firmware, which is usually just about impossible. Then it is read every time the disk is used, if they want. Your AV can't see it, & it wouldn't shock me if they had figured out a secondary way to send the data out.

In fact, if they've secretly halved the disc capacity they could just store the unencrypted data on the half you can't delete!

REPLY

MegaByte

Posted on September 24, 2016. 8:51 am

We can use the whole HD. There is a percentage of the HD that is not usable. Perhaps the NSA hides out (Or could hide out) in that unusable space?

REPLY

Costin Raiu

Posted on February 19, 2015. 12:57 pm

The problem comes from the fact there's a standardized API to write the firmware but no API to read it. This means we can't easily check if a HDD has been compromised. Several suggested solutions from our side include: firmware signing and checking on the disk side, firmware write-protect switch on the HDD and the ability to read the firmware easily and check for alterations.

REPLY

Roger Jollie

Posted on February 17, 2015. 3:42 pm

I'm surprised someone like OnTrack or other companies that recover hard drives have not found items on this "empty space".

REPLY

Mike Smitheee

Posted on February 17, 2015. 7:57 pm

Not really surprising when you think about it. If the world-wide infection rate is in the 10's of thousands, then lets assume that 10,000 of those are in the US, where data recovery is most prevalent. If that's the case, then there would still only be about a 0.004% chance of a particular machine being infected. Now, if you take that and extrapolate out the likelihood of the particular infected machine requiring a DRS, which is extremely expensive and would only be used in those cases where critical data was unrecoverable, had not been backed up in some other fashion, and/or was not otherwise replicate-able by the user.

If we roll that to oh say 1 in 100 which is EXTREMELY low, then you're now looking at a 0.00004% chance or about a 1 in 2.5million, that a DRS service would even lay their hands on an infected device. Then... they have to actually notice it.

REPLY

Ryan

Posted on February 17, 2015. 7:40 pm

Can Kaspersky give a timeline of discoveries? Where you aided by the discovery of BadUSB?

REPLY

GSK

Posted on February 17, 2015. 7:56 pm

If Kroll OnTrack ever did run across this, they probably wouldn't report it. They are a DoD cleared contractor and are used to recover data from damaged classified hard drives.

REPLY

Gordon

Posted on February 17, 2015. 9:33 pm

Maybe you never heard about Rakshasa malware: http://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-that-china-could-embed-in-every-computer

It can hide himself also in your graphic card bios and, most important, it CANNOT BE REMOVED.

REPLY

dave

Posted on February 17, 2015. 10:32 pm

I wonder what the situation on Linux is. Obviously the new firmware will only be controlled by a windows only stack of exploits even in a dual boot situation , but is Kaspersky aware of any possible tampering of binary distributed packages in linux major distributions, so that an equivalent infection can act on a linux system ? what is the probability of that ?

REPLY

wondering

Posted on March 4, 2015. 2:59 pm

I've thought that perhaps Linux's main backdoor now is called "systemd" – since it's VERY odd to see such rapid adoption of an unknown package(s) curated/written/compiled by only a few people whose goals are not clear. And with only approx. 3 major Linux bases (Fedora, Debian, etc) the NSA etc only had to convince one of them to get a back door(s) included as a "dependency" and now, poof, you have the same problem as Windows in loading components you can't completely check, an enlarged attack surface, and partially closed code.

Perhaps I am wrong, or slightly off as to where these backdoors are in Linux, but if I were a betting man then systemd is to me Linux's downfall.

REPLY

Paul Williams

Posted on February 18, 2015. 1:07 am

Roger, the kinds of targets tat Equation are aiming to infect (high-value data) are probably not the sorts of targets who will happily give up a hard drive containing high value data to companies such as OnTrack. With only a few tens of thousands of infected targets globally, I'm not surprised that this has been secret until recently.

REPLY

Low Value Target (but a target nonetheless)

Posted on March 16, 2015. 5:53 pm

Paul, I found out recently from a security professional – a very reliable source, who has examined samples from my systems directly on several occasions – that the malware complex about which I have been fighting and collecting forensic evidence (in my own amateurish but tenacious fashion) for the better part of a decade...it strongly resembles this type of coordinated "omnipotent" attack.

Everyone thought I was crazy until last month (which I am, but it has become clear from evidence and analysis of trusted advisers that my problems are not imagined) – everyone kept telling me it was physically impossible that a boot/rootkit could and would flash firmware (definitely many HDD's, definitely router firmware & a customized install of a new router microOS, definitely some/all of a motherboard's firemware, and – for certain – at least one AIO printer's firmware) and deny me access to my own BIOS's with the use of fake bios's... starting when I first started documenting my digital woes back in 2009-2010 or so. Symptoms of`infection in my situation include infected image files, infected .lnk's/.ico's (despite disabled autorun), ghost drives, computers booting from ramdisks (when no storage media was connected, or booting from ramdisk OS despite boot menu instructions to boot from a live rescue disk instead), HDD's refusing to wipe (DBAN failures, among other methods tried) and so on...

I just wish I knew how to reach reputable/trustworthy (verifiably so) security researchers in the Pacific Northwest, to give copies of all the hard (literally – paper printouts of camera images and dump files) evidence I have of my own situation, to maybe give myself hope I will eventually be able to "pwn" MY OWN DEVICES back under my own control someday. I'm tired of running only zombies in this house. Or at least help others avoid my own fate in the future. Who can someone turn to, when you can't even trust a search engine, e-mail provider, cell phone service, or the postal service anymore?

REPLY

blackwater

Posted on February 18, 2015. 6:24 am

http://spritesmods.com/?art=hddhack
nsa isnt the only one capable of doing this sort of thing

what im wondering is
why you make claims that this malware would be so hard to remove when you can simply use publically accessible tools to re-flash clean working firmware to the hdd microcontroller, have you seriously not done research on this or are you just trying to spread propaganda by making users believe there is nothing that can be done

REPLY

Costin Raiu
Posted on February 19, 2015. 1:02 pm

Thanks for your comment. Based on our experience, re-flashing the firmware doesn't seem to always help. There are certain areas in the firmware which do not get updated. In another case, the firmware update didn't work because it was "already the latest version". Yet another problem is that it's not so healthy to keep reflashing the firmware every day and leave under a constant fear that it has been infected since the last re-flash. I think we need reliable means to check if the firmware was compromised and better defense against such attacks instead of wearing down the ROM of your HDD.

REPLY

Moritz Kroll
Posted on February 18, 2015. 1:06 pm

You forgot moretimeads.com in the list of DoubleFantasy CnCs, although you sinkholed it yourself 😉
SHA256:
a2a9e948fb829685d0a9161cac845fd0dfa943d023a6b2faab205fa8664b7c26

REPLY

Joey
Posted on February 19, 2015. 3:59 am

So if it's based on Israel and the US's prior malware, and it's not directed against Israel but Islam, and nanotechnology, with all due respect, this is another Israel/US joint. Who stands to gain? And who invented it? Therefore who is ultimately responsible?

REPLY

cpuvirtual

Posted on February 19, 2015. 5:40 pm

Great Job!

Will the german people come back to the paper, pencil and rubber ?

Only time will tell !

halt

REPLY

Russel Future

Posted on February 19, 2015. 5:56 pm

Thx to K. Group for this research and result. Flashed HDD firmware cannot typically be read. Its a one-way action, so it is an obvious good place to hide malware. I am interested in “Joey”‘s questions. Who invented this suite, and as my old legal friends say, cui bono? If this is another USA-Israel joint venture, it would be useful and helpful to have proof, or at least some direct evidence. We will be having an election soon in my country, and this sort of risk factor to our economy will be an election issue. Most folks don’t care about security and spycraft issues until they are on the wrong side of a bad scenario. But for folks who do care, they care deeply. There is suspicion by some folks that our financial markets have been compromised by modern methods. Information about this exploit makes it very clear that this concern is not idle fear.

REPLY

Shane

Posted on March 16, 2015. 5:19 pm

I am skeptical of the idea that this comes from any government in particular.

For one, the coding is simply too smooth. DoD, CIA, and NSA cyber-anything has lagged behind the civilian world since the 90s. The coding was almost certainly a private entity operating under contract or from a private group of benefactors (the targeting of Iran despite the fickle nature of DC politics suggests another principle is at play).

The NSA also lacks the human intelligence resources to plant a virus on a commercial printing of CDs. I contend that private entities have supplanted even the CIA in developing human intelligence and operator networks. Such networks would also be easily capable of accessing government archives of source code samples. The government rarely understands the market value of the things it so poorly secures after forcing them from companies.

The callback servers are easily operated and maintained by small private entities whose admins don't even need to know what it is for.

The data retrieved is valuable to many different private entities. Northrop would be interested. Boeing, Sukhoi, Mikoyan-Greivich… any large defense contractor would be willing to pay for information related to the topography of a network or some of the data they are working on.

Remember when Lockheed suffered from the massive data breech related to the F-35? Then the new super-sized F-35 China started playing with?

The recent ruling by the FCC is typical government intrusion – but the sudden nature of it, I would argue, is an attempt to get a hold on the call-back servers for these types of threats. Though it may not be effective – it is classic government logic that I would argue indicates they are -not- in control of these groups and honestly have no idea how it is they are accomplishing what they are.

Further evidence can be supplied by a war-games trial run between the Active Duty Navy ITs and the Reserve-side ITs – who were civilian IT security, as well.

The Active duty didn't even know what hit them – had no idea how they were compromised.

Obviously – it is mostly conjecture…

But if you look at the platform, it is a virtual "Sword of Damocles" – it can sit quietly on systems for years – giving information that is marketable while also giving the operator the ability to carry out "hits" for no additional cost. If a customer is willing to pay to embed a virus – or someone else has a virus they wish for you to embed – then you have the perfect delivery platform.

A state tends to have a more results-driven approach – using operators to physically infect a system with a single objective. Ten years is a -long- time in politics, and a project with a pay-off 8 years down the line gets the seating official 3 terms behind yours the cookie.

The more I look at it – the more this looks to be a business model.

"But only in Iran?"

Iran has no choice but to turn to outside IT sources like Kaspersky. Boeing could be rife with this thing and we would never know it unless news of major data breaches get out (F-35 for Lockheed). Business is equal

opportunity. The Chinese are just as willing to pay to play as the U.S. is – or as Blackwater/XE is regarding a planned operation.

There is a lot more money to be made in cyber-espionage than the government has to waste on it.

Not to say that the government wouldn't be interested in being a customer of such a business....

REPLY

Marki

Posted on February 19, 2015. 7:26 pm

Very interesting thing to silently flash parts of a HDD firmware – I had a short peek into the circulating samples of EquationDrug and GrayFish. I couldn't find a place where stands "SAMSUNG" or "WDC" in any of these samples.

To be sure that I grabbed valid files I also looked for the string "GROK" in another sample and found it – so the collection seems valid ...

So – what part of what sample is shown in the report on page 17 ??

appreciate any feedback

REPLY

Costin Raiu

Posted on March 4, 2015. 8:45 am

Hi Marki,

Thanks for your comment! Unlike the "GROK" string, the strings from NLS_933W are encrypted, so you'd have to decrypt them first. We provide an MD5 for NLS_933W in the blog.

Good luck!

REPLY

Theodis Butler

Posted on February 21, 2015. 5:51 am

Holy Shit

REPLY

A. Nolen

Posted on March 23, 2015. 4:04 pm

This report and the work you detail in the post are awesome achievements Costin; congrats to you and the team at Kaspersky. Have you or Kaspersky Labs received any blowback from either the US government, or any organization, for making these revelations?

REPLY

Arturo Spinoza

Posted on March 23, 2015. 6:58 pm

'Holy Shit' doesn't begin to describe it. Kaspersky is right, we need to band together to fight this.

REPLY

alexander

Posted on April 12, 2015. 5:58 pm

Having read this and further articles about Equation group, I made a conclusion that the user computer security should be considered complexly from from the computer turning on to standard user actions in the operating system.
That is why I want to know answers on these 10 questions:
1. Can usual antivirus check find all the harmful software of Equation Group family, if the check has tough options?
2. Can Equation group software patch system drivers, hard drive firmware and make other changes in OS booting when Secure boot is on and Kaspersky Internet Security with ELAM support is used?
3. If they can, are these changes fixed under question 2 conditions?
4. If the software acts successfully and no changes fixed by Secure boot or KIS, can TPM module fix them?
5. Do the components of Equation Group interact in the Oeration system environment or within internal family structure (directly between each other)?
6. Will new publications about the Grayfish and its main differences from the Equationdrug be?
7. Please give the list of hard drives models with changed firmware.
8. Can the core and components of the Equation Group mask themselves and other components to become unvulnerable for proactive defence and behavioral analysis? This is about all the components and any antivirus or antispyware. First of all I mean software control function of Kis or HIPS in the Comodo Internet Security.
9. What signs can be used to define the patching of the drive firmware exactly or with high possibility? Can it be some files in the system or virtual file system?
10. Can the such software as 7datarecovery or other like it find such a virtual system?
11. Does Kaspersky Laboratory know about the development and

implementation of the technologies complicating the firmware patching by hard drives producers?

REPLY