

HACKINGTEAM AND GAMMA INTERNATIONAL IN “BUSINESS-TO-GOVERNMENT MALWARE”

Sergey @k1k Golovanov, Malware Expert

Kaspersky Lab

MAIL_TO:v3sos@ahnlab.com, virus@arcabit.com,
samples@superantispyware.com, virus@avast.com,
virus@grisoft.cz, ANALYSIS@NORMAN.NO,
virus@avira.com, newvirus@kaspersky.com,
virus_submission@bitdefender.com, virus@ca.com,
vms@drweb.com, submit@emsisoft.com,
esafe.virus@eAladdin.com, samples@eset.com,
samples@nod32.com, submit@ewido.net,
submitvirus@fortinet.com, viruslab@f-prot.com,
samples@f-secure.com, analyse@ikarus.at ...

DATE_TIME: 24.07.2012 5:52:00

ATTCH: **AbodeFlashPlayer.zip** (~1M)

TEXT:

From: Kev

How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists

By Ryan Gallagher



http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html



<http://www.bloomberg.com/photo/security-researcher-morgan-marquis-boire-/214749.html>

HOW WE CAN BE SURE THAT IT IS HACKINGTEAM?

]HackingTeam[

About us

The Solution

Careers

Contacts

Home > The Solution

The Solution

In modern digital communications, encryption is widely employed to protect users from eavesdropping. Unfortunately, encryption also prevents law enforcement and intelligence agencies from being able to monitor and prevent crimes and threats to the country security.

Remote Control System (RCS) is a solution designed to evade encryption by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable. For Governmental LEAs and Agencies ONLY.

Remote Control System (RCS)

<http://www.hackingteam.it/index.php/remote-control-system>

```
s: .objc_class_name_RCSMActions
s: .objc_class_name_RCSMAgentDevice
s: .objc_class_name_RCSMAgentMicrophone
s: .objc_class_name_RCSMAgentOrganizer
s: .objc_class_name_RCSMAgentPosition
s: .objc_class_name_RCSMAgentScreenshot
s: .objc_class_name_RCSMAgentWebcam
s: .objc_class_name_RCSMConfManager
s: .objc_class_name_RCSMCore
```

HOW WE CAN BE SURE THAT IT IS HACKINGTEAM?

```
000009F6: 66 34 33 62.37 63 32 34.31 63 37 35.65 31 38 62 f43b7c241c75e18b
00000A06: 35 61 32 34.30 33 64 64.36 36 38 62.30 63 34 62 5a2403dd668b0c4b
00000A16: 38 62 35 61.31 63 30 33.64 64 38 62.30 34 38 62 8b5a1c03dd8b048b
00000A26: 30 33 63 35.38 39 34 34.32 34 31 63.36 31 63 33 03c58944241c61c3
00000A36: 37 37 36 39.36 65 36 39.36 65 36 35.37 34 30 30 77696e696e657400
00000A46: 36 38 37 34.37 34 37 30.33 61 32 66.32 66 37 32 687474703a2f2f72
00000A56: 36 33 37 33.32 [REDACTED] 66 32 65 63732 [REDACTED] f2e
00000A66: 36 38 36 31.36 [REDACTED] 37 37 34 68616 [REDACTED] 774
00000A76: 36 35 36 31.36 [REDACTED] 66 33 30 65616 [REDACTED] f30
00000A86: 33 30 33 30.33 [REDACTED] 30 33 30 30303 [REDACTED] 030
00000A96: 33 31 32 66.36 [REDACTED] 66 36 39 312f6 [REDACTED] f69
00000AA6: 37 34 32 65.36 [REDACTED] 30 30 30 742e6 [REDACTED] 000
00000AB6: 7B 7D 7D 7D.7D 7D 7D . . {}}}}}}}
```

<https://www.virustotal.com/en/file/81e9647a3371568cddd0a4db597de8423179773d910d9a7b3d945cb2c3b7e1c2/analysis/>

hxxp://rcs-demo.hackingteam.it//ploit.doc2***

HOW WE CAN BE SURE THAT IT IS HACKINGTEAM?

```
72 6F 63 5F irentriesattr.i_proc_list_lock.i_proc_list_unlock.i_proc
64 0
5F 7 /Users/guido/Projects/driver-macos/
00 5
6D 6F 76 65 stack_chk_fail.__stack_chk_guard.cdevsw_add.cdevsw_remove
00 5F 65
73 74 72
5F 69 6E
75 72 72
6F 6A 65
2F 58 63
2F 49 6E
6E 6F 72
6F 6B 2E
65 74 64
6E 74 72
69 73 74
5F 69 5F be red_backdoors.g_symbols_resolved.b.i_allproc.i_tasks.i_n
```

/Users/guido/Projects/driver-macos/

Guido



Senior Software Developer at Hacking Team

Milan Area, Italy | Computer & Network Security

Previous Communication Valley, Mir SRL, Uniteam INIT SRL

[Connect](#)

[Send InMail](#)



Call:

; CODE XREF:

```
call    init_and_apis
push    offset CriticalSection ; lpCr
call    ds:InitializeCriticalSection
call    file
call    keylog
call    screenshot
call    position
call    print
call    crisis
call    url
call    clipboard
call    camera
call    messages
call    password
call    chat
call    device
call    mouse
```

11

1: 00401000

WHAT CAN IT DO?

1. **Self-replication** via USB flash drive (**3** methods)
2. Infection of virtual **VMware** machines by copying itself into the autorun folder on the virtual drive
3. Infection of mobile **BlackBerry** and **Windows CE** devices
4. Ability to **self-update**
5. Installation of **drivers**
6. **Signed**



Local (physical) installation

- Local infection vectors
 - (Bootable) CD-ROM
 - (Bootable/Autorun) USB pen drive
 - Direct hard disk infection by means of tampering with computer case
 - Firewire Port/PCMCIA attacks
 - HT consultancy: anonymous attack scenario analysis, attack cookbook
 - ▶ E.g., Internet Café using DeepFreeze

HOW IT IS PROPAGATING?

1. Social engineering:

Self-signed **JAR** files

Filenames like **FlashUpdate.exe**

2. Exploits:

CVE-2010-3333

CVE-2012-1682 (**0-day** by Security Explorations.
~2 months ITW before publishing.)

CVE-2012-4167 (**0-day** by Vupen. ~3 months ITW
before publishing.)

CVE-2012-5054 (**0-day** by Vupen. ~3months ITW.)

CVE-2013-0633 (**0-day** by me. Do not ask for how
long.)

IS IT RCS OR FSB_SPY?

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VID

THREAT LEVEL

surveillance

hacks and cracks

cybersecurity

American Gets Targeted by Digital Spy Tool Sold to Foreign Governments


BY KIM ZETTER 06.04.13 6:30 AM

 Follow @KimZetter

 Share 710

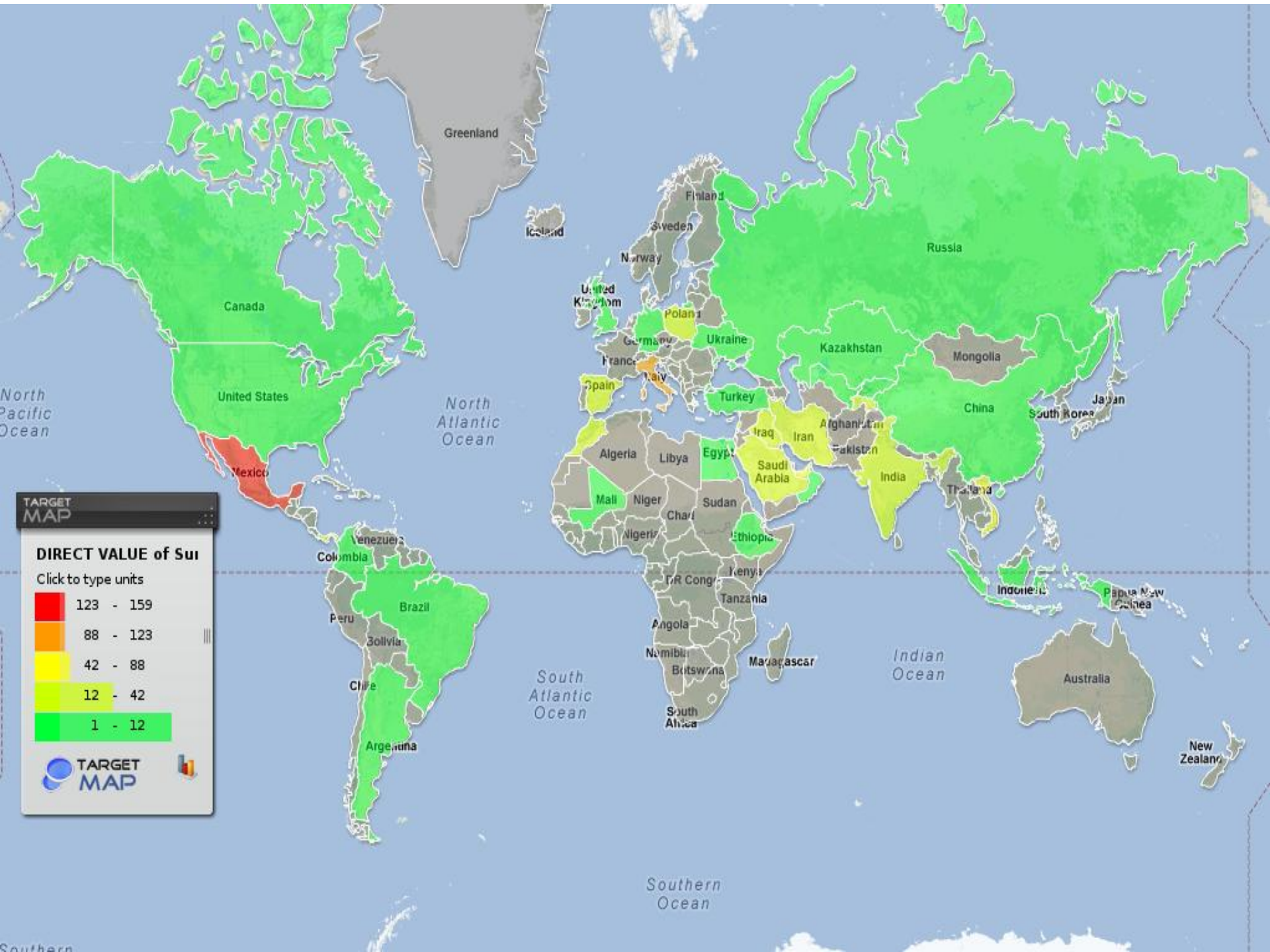
 Tweet 842

 +1 50

 Share 63

 Pin it

www.wired.com/threatlevel/2013/06/spy-tool-sold-to-governments/



TARGET MAP

DIRECT VALUE of Sui

Click to type units

Red	123 - 159
Orange	88 - 123
Yellow	42 - 88
Light Green	12 - 42
Dark Green	1 - 12

TARGET MAP

C2 FINGERPRINT

> GET /con/trust/ HTTP/1.1

User-Agent: curl/7.22.0 (x86_64-pc-linux-gnu)

libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23

librtmp/2.3

Host: ***

Accept: */*

< HTTP/1.1 500 InternalServerError < Connection: close

< Content-Type: text/html < Content-length: 88 < *

Closing connection #0 undefined method

`prepare_response' for

#<RCS::Collector::CollectorController:0x38ac540

FINFISHER™

IT INTRUSION



[Home](#)

[Portfolio](#)

[News](#)

[Contact Us](#)

English



FINFISHER™: GOVERNMENTAL IT INTRUSION
AND REMOTE MONITORING SOLUTIONS

HOW IS IT PROPAGATING?

Product Components

**NO EXPLOITS!
(I COULD NOT FIND IT)**



The screenshot shows the homepage of arrahmah.com, a website with the tagline "filter your mind, get the truth". The page features a navigation menu with categories like Home, News, Islamic World, Jihad Zone, Kajian Islam, Muslimah, Rubrik, Kontribusi, and Ramadhan. A search bar is located in the top right corner. The main content area displays a large image of a destroyed building and a list of news items. A prominent yellow box with a black border is overlaid on the page, containing the text "NO EXPLOITS! (I COULD NOT FIND IT)". Below this box, a "Download now" button is visible, accompanied by a disclaimer: "By clicking the Download now button, you acknowledge that you have read and agree to the Adobe Software Licensing Agreement." and "Please note, depending on your settings, you may have to temporarily disable your antivirus software." The page also includes a "Terbaru" (Latest) section with a list of news items and a "Terpopuler" (Most Popular) section. At the bottom, there is a "IndonesiaToday" section with a date of "Sabtu, 28/07/2012 20:40:04" and several news headlines, including "PBNU desak Pemerintah RI menolong Muslim Rohingya bukan JAKARTA (Arrahmah.com)" and "Bentrok Brimob-warga di PTPN VII Cinta Manis, satu tewas lima luka PALEMBANG (Arrahmah.com)".

http://wikileaks.org/spyfiles/files/0/289_GAMM

<http://www.domaintools.com/research/screenshot-history/arrahmah.info#0>

MAIN FUNCTIONALITY

1. New files monitoring
2. Printed files recording
3. Deleted files recording
4. Forensics recording
5. VoIP files recording
6. Changed files recording
7. Skype file transfer recording
8. Skype text conversations recording
9. Skype audio conversations recording
10. File system recording
11. Command line recording
12. Scheduler recording
13. Audio recording
14. Screenshots
15. Webcam recording
16. Keylogging

Browsers: Mozilla Firefox, Internet Explorer, **Opera**, Chrome

Messengers: **ICQ**, AIM, Skype, Yahoo Messenger, Pidgin, Trillian, Google Talk

E-mail: Microsoft Outlook, Outlook Express, Mozilla Thunderbird,

Windows Mail, **The Bat**

File sharing: BitTorrent, uTorrent, eMule, eDonkoy (typo?), Kazaa, FrostWire, LimeWire

VoIP: CGStarter, X-Lite, Gizmo,

Mercuro, **TeamSpeak** 3, Zfone

During his mission, the sailors had precise details of the narco boss using wiretapping equipment and tracking software, called **Finfisher/Finspy...**



To capture Miguel Angel Trevino Morales, El Z-40, leader of Los Zetas, the elements of the Navy (Semar) had support from a avión no tripulado (better known as a drone), owned by U.S. agencies operating these flying objects since 2004 on the border with Mexico.

During his mission, the sailors had precise details of the narco boss using wiretapping equipment and tracking software, called Finfisher/Finspy, and Hunter Punta Tracking/Locksys, revealed officials involved in national security cabinet.

WHAT CAN IT DO?

```
integer545 = new Integer(0x801c40);
hashtable545.put("TlvTypeRemoveTgLicenseInfo", integer545);
integer546 = TLVPAYLOADTYPES;
integer546 = new Integer(0x801d90);
hashtable546.put("TlvTypeTgAllConfigurations", integer546);
integer547 = TLVPAYLOADTYPES;
integer547 = new Integer(0x8020a0);
hashtable547.put("TlvTypeTgError", integer547);
integer548 = TLVPAYLOADTYPES;
integer548 = new Integer(0x8030a0);
hashtable548.put("TlvTypeGetTgConfigRequest", integer548);
integer549 = TLVPAYLOADTYPES;
integer549 = new Integer(0x8031a0);
hashtable549.put("TlvTypeTgConfigReply", integer549);
integer550 = TLVPAYLOADTYPES;
integer550 = new Integer(0x8032a0);
hashtable550.put("TlvTypeSetTgConfigRequest", integer550);
integer551 = TLVPAYLOADTYPES;
integer551 = new Integer(0x803580);
hashtable551.put("TlvTypeConfigTgID", integer551);
integer552 = TLVPAYLOADTYPES;
integer552 = new Integer(0x803640);
hashtable552.put("TlvTypeConfigTgHeartbeatInterval", integer552);
integer553 = TLVPAYLOADTYPES;
integer553 = new Integer(0x803770);
```

return "E";

SUMMARY

1. Sophisticated **malware**
2. Trying very hard to **avoid** detection
3. Physical access/Exploits/Social engineering **installations**
4. Several **hundred** detections around the world via KSN
- 5. What should we do?**

IMHO

Original: Tim Minchin - The Song For Phil Daoust

THANK YOU!

Sergey @k1k Golovanov, Malware Expert

Kaspersky Lab