Spyware. HackingTeam

Table of Contents

This article is based on technical data from Kaspersky Lab experts and their analysis of the Korablin and Morcut malicious programs. A number of conclusions have been drawn by Kaspersky Lab experts based on open source data references in the conclusion of this publication. Any questions regarding the contents of this article can be posted on Kaspersky Lab's securelist.com website, or you can contact Kaspersky Lab's PR Service directly via Kaspersky.com.

Spyware for law enforcement

According to Wikipedia, "Spyware is a software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."

While most countries have laws prohibiting the creation and proliferation of malicious programs, there are currently three programs that, the developers assure us, have been designed to collect data about user operations on computers and subsequently transmit that data to law enforcement agencies.

The first widely known program of this kind is the Trojan Bundestrojaner, which has been used by German law enforcement to track suspects on the Internet. Another known spyware program is FinSpy, which was designed by Gamma International to give law enforcement agencies in different countries the ability to track suspects' computers and mobile devices. Remote Control System (RCS) is the third spyware program, and the one that will be addressed in detail in this article. This program was developed by the Italian company HackingTeam and is intended for sale to government authorities in different countries.

HackingTeam

HackingTeam first caught our attention back in 2011, when WikiLeaks released documents describing the functions of the spyware programs the company offers to government agencies in 2008.

In early 2012, Kaspersky Lab experts detected malicious programs running on Windows that were suspiciously similar to the programs described on WikiLeaks, and with Remote Control System, the description of which was published on the company's official website www.hackingteam.it. However, at the time, we had no way of knowing about the connections between the threats that were detected (Kaspersky Lab detects them as Korablin) and the HackingTeam spyware program.

Author

Sergey Golovanov

All analysis articles
All blog postings

Analysis

BitGuard: a system of forced searches
Kaspersky Security Bulletin 2013. Malware Evolution
IT Threat Evolution: Q3 2013
Kaspersky Security Bulletin 2012. Cyber Weapons
Kaspersky Security Bulletin 2012. The overall statistics for 2012

Blog

CODE BLUE in Tokyo
CVE-2014-0497 – a 0-day vulnerability
Big box LatAm hack (3rd part – infection by Office files)
Big box LatAm hack (2nd part – Email brute-force and spam)
A cross-platform java-bot

Source

Kaspersky Lab

The program's description from HackingTeam's website http://www.hackingteam.it/images/stories/RCS2012.pdf

That all changed in July 2012, when many antivirus companies received an email with an example of malicious code for Mac OS X with the same functions.

Our email address newvirus@kasperksy.com received this email on July 24, 2012 at 05:51:24 MSK. The subject line was empty, and there was no text — just an attachment called AdobeFlashPlayer.zip. The attachment had a self-signed JAR-file containing a program written for Mac OS X.

The header of the email was addressed to newvirus@kaspersky.com

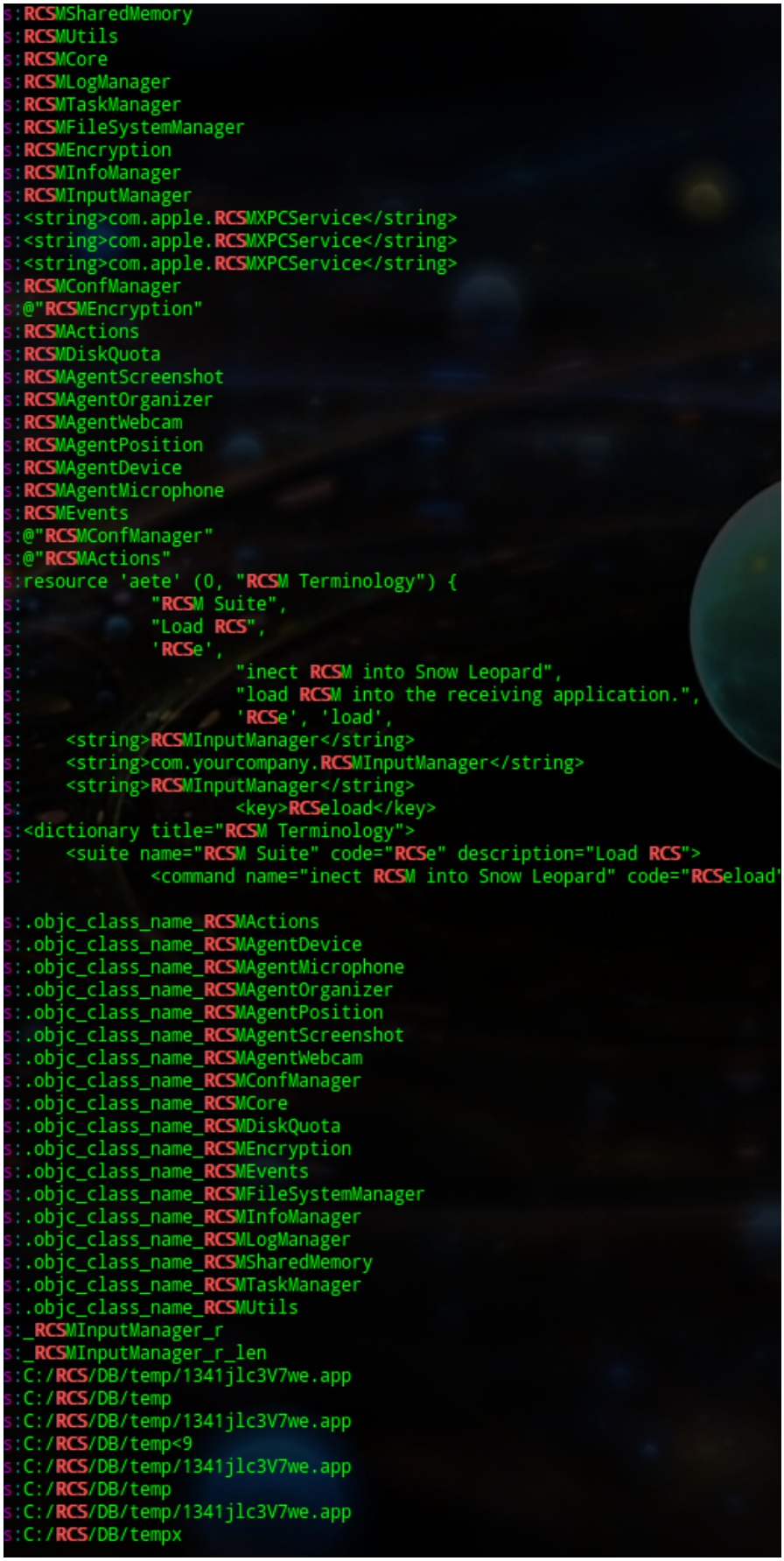
Soon, nearly all antivirus companies had added detection of this new malware, and each company named it differently (Crizis, DaVinci, Boychi, etc. — Kaspersky Lab named it 'Morcut'). Nearly all antivirus companies suspected that the program was developed by HackingTeam, which sells specialized tracking software to law enforcement agencies in a number of countries.

Evidence

The fact that the functions are similar is just one of three circumstantial pieces of evidence linking HackingTeam to the files that were analyzed. Let's take a look at the other two.

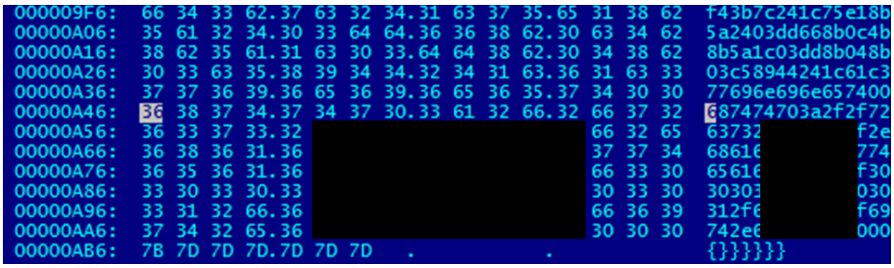
The data overhead in the Mac file contained the names of files and modules that the authors used when writing the program code. These names were also seen several times with "*RCS*", which coincides with the abbreviation of the Remote Control System name (this abbreviation is used by HackingTeam in its promotional materials and its own description of the program on their website).

RCS used in HackingTeam's description of the program
http://www.hackingteam.it/index.php/remote-control-system



Use of the RCS abbreviation in the malicious program for the Mac platform

Finally, an exploit that downloads the threat from the hackingteam.it website was detected (this exploit was uploaded to Virustotal.com on July 04, 2012).



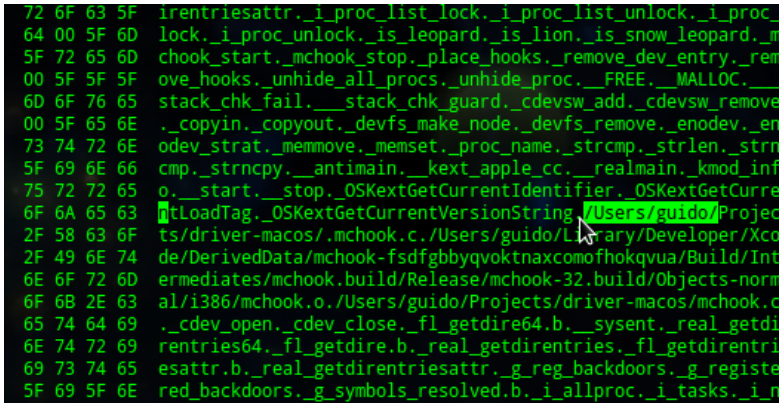
A fragment of the exploit payload that downloadsthe malicious program from the following site:
hxxp://rcs-demo.hackingteam.it/ploit.doc2***

The following was then established:

1. The functions of the malicious program matched up with the functions of HackingTeam's product.
2. The names used in the data overhead of the threats and on HackingTeam's website also matched up.
3. The threat was downloaded from the HackingTeam website.

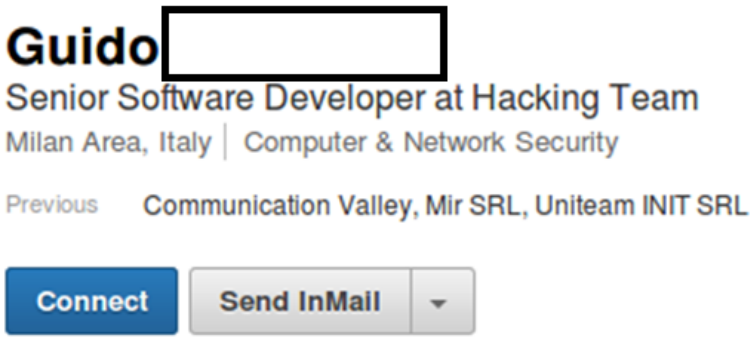
Based on the above, one can safely presume that the spyware programs that fell into the hands of the investigating IT security professionals were more than likely created by HackingTeam. For the sake of convenience, we will refer to both of these programs (both for Windows and for Mac OS X) as RCS.

Incidentally, all of the malicious files for Mac OS X sent by email had links to files in a folder with the name 'guido':



Use of the username "guido" in malware code

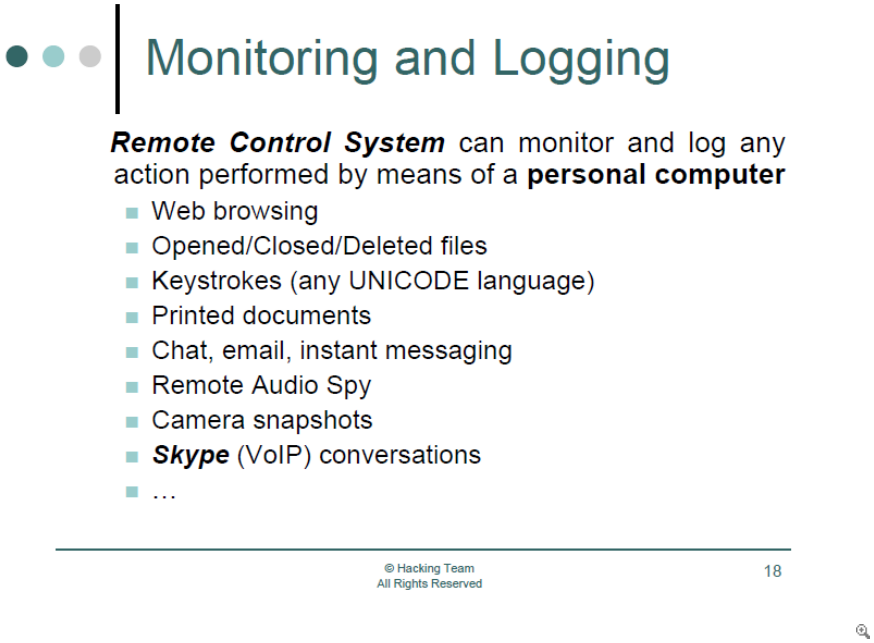
And there's a curious coincidence: one user whose linkedin.com profile states that he is a former developer for HackingTeam also goes by the name Guido.



*A certain Guido ***'s user account on LinkedIn lists HackingTeam among the user's former employers*

A rather strange spy

Today, Kaspersky Lab's malware collection includes over 100 RCS modifications, with almost identical functionality. As discussed above, the description of these samples matches that of the official Remote Control System program description on HackingTeam's official website, and the program description drafted by HackingTeam and published on WikiLeaks (pdf).



The RCS description published on WikiLeaks

RCS files for Windows are written in C++. To prevent the program from drawing the attention of antivirus products, its creators did almost nothing to protect it against analysis — a trait typical of programs used in targeted attacks.

The full set of RCS functions can be seen at the start of executable files when the threat initializes.

```
text:1000175A                           ModulesCall:                            ; CODE XREF:
text:1000175A 000 E8 01 AB 02 00                        call    init_and_apis
text:1000175F 000 68 00 A3 08 10                        push    offset CriticalSection ; lpCr
text:10001764 004 FF 15 8C D1 06 10                     call    ds:InitializeCriticalSection
text:1000176A 000 E8 E1 2E 02 00                        call    file
text:1000176F 000 E8 AC 11 02 00                        call    keylog
text:10001774 000 E8 27 14 02 00                        call    screenshot
text:10001779 000 E8 62 14 02 00                        call    position
text:1000177E 000 E8 7D 16 02 00                        call    print
text:10001783 000 E8 E8 37 02 00                        call    crisis
text:10001788 000 E8 43 19 02 00                        call    url
text:1000178D 000 E8 6E 19 02 00                        call    clipboard
text:10001792 000 E8 79 1B 02 00                        call    camera
text:10001797 000 E8 54 3F 02 00                        call    messages
text:1000179C 000 E8 DF 1D 02 00                        call    password
text:100017A1 000 E8 9A 1E 02 00                        call    chat
text:100017A6 000 E8 25 1F 02 00                        call    device
text:100017AB 000 E8 D0 20 02 00                        call    mouse
text:100017B0 000 E8 FB 20 02 00                        call    applications
text:100017B5 000 E8 86 23 02 00                        call    USB_BB_VM_Infections
text:100017BA 000 E8 B1 23 02 00                        call    addressbook
text:100017BF 000 E8 8C 1D 02 00                        call    mic
text:100017C4 000 E8 57 24 02 00                        call    social
text:100017C9 000 E8 32 18 02 00                        call    call
text:100017CE 000 B8 01 00 00 00                        mov     eax, 1
text:100017D3 000 C3                                    retn
text:100017D3                           ModulesCall_    endp
text:100017D3
```

Initialization of RCS objects

Based on the functions in the program, it follows that RCS is a self-replicating malicious program designed to steal personal data and transmit it to a remote server.

In order to perform its spyware functions, the program copies data to access user accounts and intercept messages from browsers (Firefox, Internet Explorer, Chrome, Opera), email clients (Outlook, Windows Mail, Thunderbird), and instant messaging programs (Yahoo, MS messengers, Google Talk, Skype, Paltalk, Thrillian). It also intercepts audio and video streams.

However, RCS also has some functions that, in my opinion, go beyond anything a spyware program might need. An analysis of the commands that come in from the RCS control server has helped identify the most important of these other functions. If the RCS control server issues the appropriate command, the following functions can be activated:

1. Self-replication via USB flash drive:
   a. Using a standard Autorun.inf mechanism (the same as most worms detected by Kaspersky Lab as Worm.Win32.AutoRun);
   b. Using a fake “Open folder to view files” entry (a method commonly used for self-replicating worms, especially with the Kido/Confiker worms);
   c. Exploiting the CVE-2010-2568 vulnerability (used by Stuxnet for self-replication via LNK files).
2. Infection of virtual VMware machines by copying itself into the autorun folder on the virtual drive.

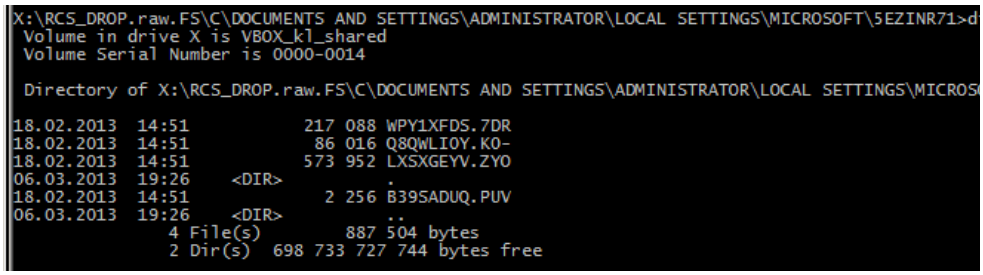
3. Infection of mobile BlackBerry and Windows CE devices.
4. Ability to self-update.
5. Use of an AES encryption algorithm to work with files and control servers.
6. Installation of drivers.

Just to be perfectly clear, RCS does not have any mechanism that allows it to accurately copy a file system's contents or copy the contents from RAM. That means that executing random code in the system (updates and driver installations) will not make it definitively clear whether or not any illegal content on a suspect's computer was downloaded there by the suspect himself, or by the RCS operator. I do not believe that this program can be used to collect information which could be used as evidence of committing unlawful actions.

Basically, the program has arather strange function: it does what it shouldn't do, and it doesn't do what a program that collects data for forensic investigations should do.

Proliferation

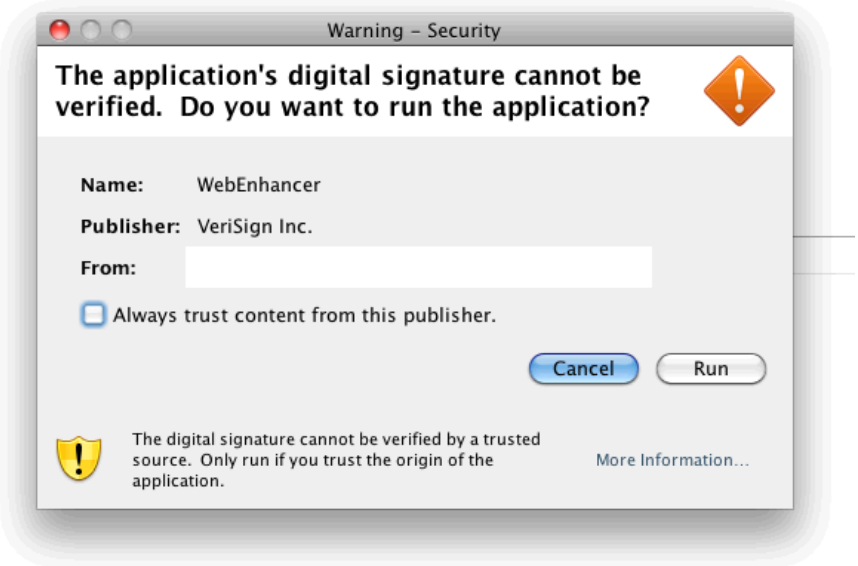
On an infected computer, RCS looks like several files with random names, and one active, dynamic registry that requires additional malicious programs before it can be installed. During our analysis, we detected droppers and downloaders being used to install RCS.



An example of the files created by the RCS installer

After the publication on WikiLeaks, I guessed that considering the abilities of law enforcement bodies in different countries, RCS is probably spread by replacing requested executable files at the Internet provider level.

However, a self-signed JAR file received by email in July 2012 showed that social engineering methods can also be used to spread RCS.



An example of the self-signed JAVA applet that installs RCS on user computers

An attack then proceeds like this: a user receives an email with a link to a file, or the file itself, as an attachment. The contents of the email are designed to entice the recipient to open the file (or click on the link).

Kaspersky Lab was also able to establish that the droppers and downloaders that install RCS can be sent by email. These malicious files have different names and may be .rar, .zip, or .exe files.

- PPT.rar
- FlashUpdate.exe

- Setup.exe
- Crack.exe
- Photos.zip
- GoogleUpdate.rar
- Microsoft.exe
- Install.rar
- Wrar.exe
- Important.rar

A list of files containing an RCS installer

Furthermore, after analyzing the files that download RCS, we detected a previously unknown vulnerability that was assigned the name CVE-2013-0633.This vulnerability is used in a classic targeted attack tactic: a user receives an email with a Word file as an attachment; the file contains a 0-day exploit — in this case, for Flash (this exploit has been addressed by Adobe here, for example).

The contents of a Word document that opens after running the CVE-2013-0633 exploit and installing RCS

Exploits

An active search for exploits which install RCS on user computers was launched after Citizen Lab published an article in October 2012 describing the use of exploits for the CVE-2010-3333 vulnerability to plant RCS on a UAE pro-democracy activist's computer. The list of vulnerabilities using the detected exploits currently includes the following:

- **CVE-2010-3333**
- **CVE-2012-1682**
- **CVE-2012-4167**
- **CVE-2012-5054**
- **CVE-2013-0633**

Remarkably, four of the vulnerabilities on that list remained unknown for several months; during that time, the exploits were able to use those vulnerabilities, unhindered, on any computer.

Today, there are several more vulnerabilities which we presume can be used to install RCS. However, the servers using the exploits to stealthily install executable files do not operate continuously, which makes it difficult to prove that these exploits are installing RCS.

We were able to confirm that RCS was being downloaded from the following addresses:

106.187.**.51	2.228.65.***
112.***.65.110	50.7.***.220
173.255.215.**	50.116.***.11
Update*******.info	17******.com
176.**.100.37	56****.members.linode.com
176.74.1**.119	76.***.33.13
178.**.166.117	A*****.com
178.**.176.69	A***.com
183.98.1**.152	****b.5gbfree.com
184.107.2**.78	li56*****.members.linode.com

Fira******.com	*****update.selfip.com
187.***.43.35	Clos*****.com
198.58.**.113	Fad****.com
200.67.***.2	wiki-****.com
Tmx****.com	wiki-*****.info
200.**.245.36	

Morgan Marquis-Boire, from that same Citizen Lab article, suggested that exploits developed by the French company Vupen are being used to spread HackingTeam products. This company specializes in searching out vulnerabilities in popular software programs and sells ready-made exploits to various governments. However, it is still not clear whether Vupen sells its exploits alongside HackingTeam programs, or if the clients of both companies use these two programs together to track suspects.

How it works

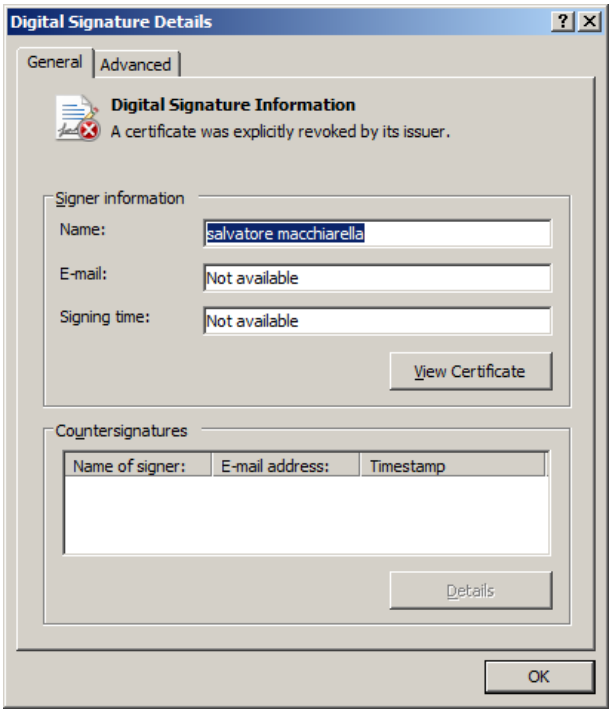
After analyzing the RCS functions, we identified a number of official criteria which help to determine whether a file belongs to HackingTeam, and to RCS in particular.

1. The use of debugging mechanisms during program execution.
   When the program is running, it can check its own PID and send messages about its performance.

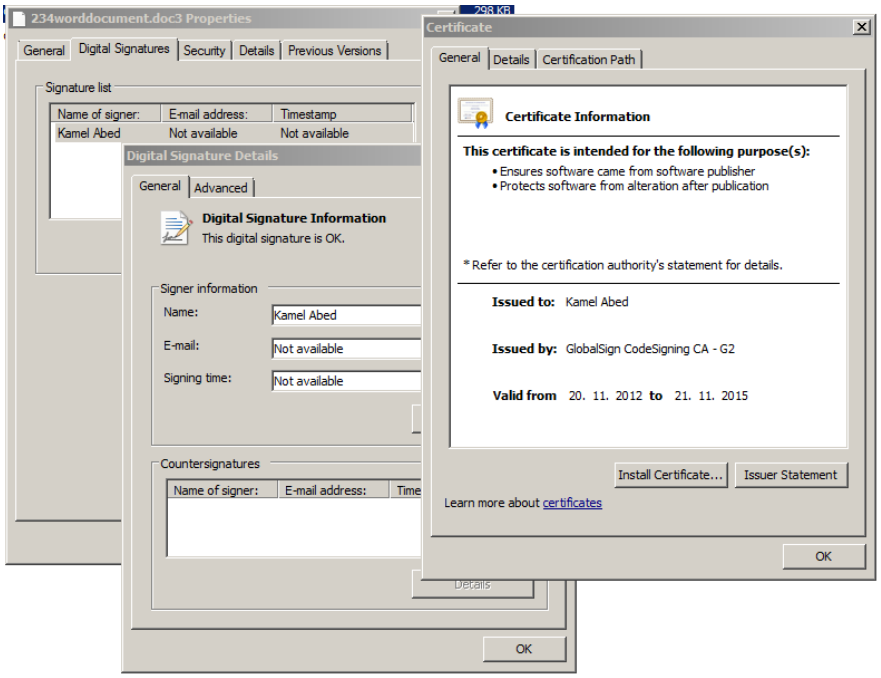
```
.text:00401030
.text:00401030                          ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
.text:00401030                          _WinMain@16     proc near               ; CODE XREF: ___tmainCRTStartup+115↓p
.text:00401030
.text:00401030                          NumberOfBytesRead= dword ptr -4
.text:00401030                          hInstance       = dword ptr  8
.text:00401030                          hPrevInstance   = dword ptr  0Ch
.text:00401030                          lpCmdLine       = dword ptr  10h
.text:00401030                          nShowCmd        = dword ptr  14h
.text:00401030
.text:00401030 000 55                                   push    ebp
.text:00401031 004 8B EC                                mov     ebp, esp
.text:00401033 004 51                                   push    ecx
.text:00401034 008 53                                   push    ebx
.text:00401035 00C 56                                   push    esi
.text:00401036 010 57                                   push    edi
.text:00401037 014 68 00 80 00 00                       push    8000h           ; size_t
.text:0040103C 018 E8 8F 15 00 00                       call    _malloc
.text:00401041 018 83 C4 04                             add     esp, 4
.text:00401044 014 68 00 80 00 00                       push    8000h           ; nSize
.text:00401049 018 8B F0                                mov     esi, eax
.text:0040104B 018 56                                   push    esi             ; lpFilename
.text:0040104C 01C 6A 00                                push    0               ; hModule
.text:0040104E 020 FF 15 14 70 40 00                    call    ds:GetModuleFileNameW
.text:00401054 014 FF 15 10 70 40 00                    call    ds:GetCurrentProcessId
.text:0040105A 014 83 F8 04                             cmp     eax, 4
.text:0040105D 014 75 14                                jnz     short loc_401073
.text:0040105F 014 6A 00                                push    0               ; uType
.text:00401061 018 68 50 71 40 00                       push    offset Caption  ; "Program is loading"
.text:00401066 01C 68 78 71 40 00                       push    offset Text     ; "Program is loading"
.text:0040106B 020 6A 00                                push    0               ; hWnd
.text:0040106D 024 FF 15 14 71 40 00                    call    ds:MessageBoxW
.text:00401073
.text:00401073                          loc_401073:                             ; CODE XREF: WinMain(x,x,x,x)+2D↑j
.text:00401073 014 6A 00                                push    0               ; hTemplateFile
.text:00401075 018 68 80 00 00 00                       push    80h             ; dwFlagsAndAttributes
.text:0040107A 01C 6A 03                                push    3               ; dwCreationDisposition
.text:0040107C 020 6A 00                                push    0               ; lpSecurityAttributes
.text:0040107E 024 6A 03                                push    3               ; dwShareMode
.text:00401080 028 68 00 00 00 80                       push    80000000h       ; dwDesiredAccess
.text:00401085 02C 56                                   push    esi             ; lpFileName
.text:00401086 030 FF 15 0C 70 40 00                    call    ds:CreateFileW
.text:0040108C 014 8B F8                                mov     edi, eax
.text:0040108E 014 6A 00                                push    0               ; lpFileSizeHigh
.text:00401090 018 57                                   push    edi             ; hFile
.text:00401091 01C FF 15 08 70 40 00                    call    ds:GetFileSize
```

An example of PID verification during initial RCS installation

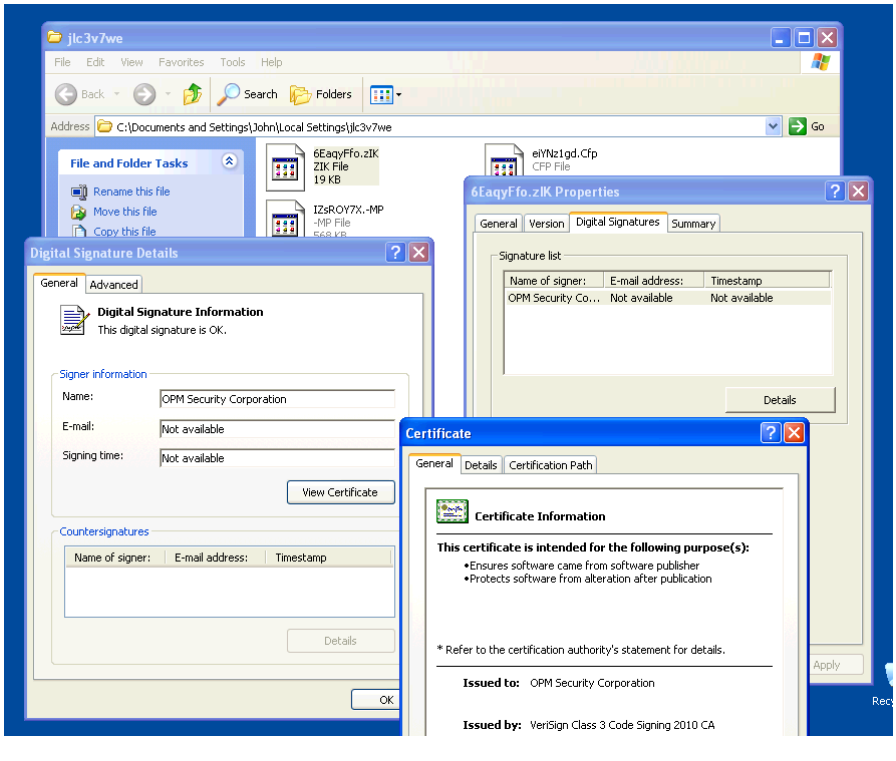
2. The use of encrypted AES POST requests and logging by the Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0) user agent.
3. The use of executable file signatures to get around security systems installed on user computers.



Example 1: the signature of an RCS component



Example 2: the signature of an RCS component



Example 3: the signature of an RCS component

The RCS component signatures in examples 1 and 2 were issued to private individuals. In the last example, unlike the first two, the certificate was issued to an organization. The name of that organization is OPM Security Corporation.

OPM Security

OPM Security is a company registered in Panama. Its website (www.opmsecurity.com) states that among other things, it offers a software product called Power Spy. The description of Power Spy is more or less the same as HackingTeam's description of RCS.

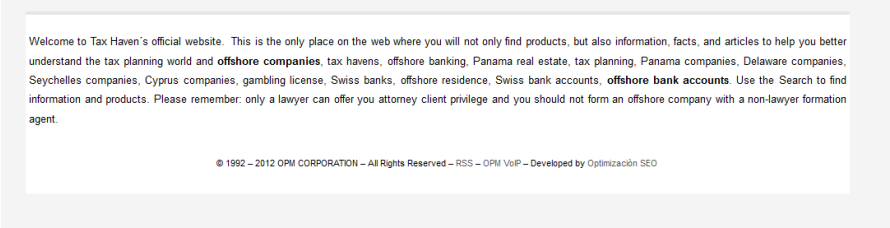
Spying on Computers:
Interception of Computer Activity

Power Spy lets you know what others have been doing on your computer while you were out. Secretly tape all keys that have been hit, chat-rooms and instant messages on MSN Messenger, Windows Live Messenger, ICQ, AOL Messenger, AIM, Yahoo! Messenger, Windows Messenger and Skype. Records websites that have been visited, e-mails that have been read, file activities, passwords, opened documents, opened windows and applications that have been used. Power Spy software includes instant recognition of screen options such as a surveillance camera. Describes activities precisely, such as MySpace, Facebook, computer games, Internet searches, on-line buying, archive transfers, e-mails from websites such as Hotmail, AOL email, Gmail, Yahoo mail and hundreds of others.

OPM Security's description of Power Spy on the company's website
http://www.opmsecurity.com/security-tools/spying-on-on-your-husband-wife-children-or-employees.html

This gives one grounds to presume that OPM Security is possibly selling either an older or pirated version of RCS. Furthermore, it will sell it to any interested party for just EUR 200, even though the average price at HackingTeam, according to some sources, is an average of EUR 600 000.

It's worth noting that OPM Security is part of OPM Corporation, which offers offshore company registration and dual citizenship passport services among other things.



The description of OPM Corporation's business on the website www.taxhavens.us

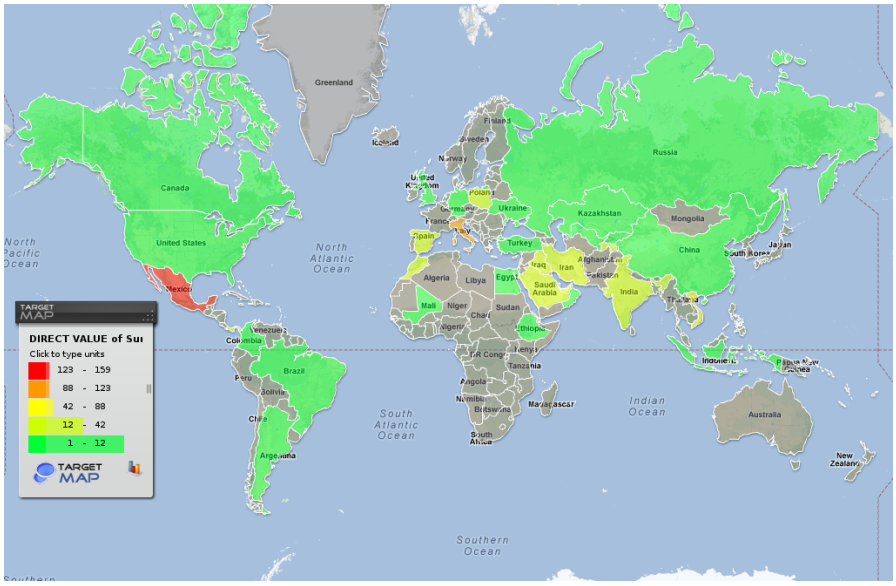
Infection stats

The map below was put together using data from KSN about the number of attempts made to install RCS components on computers around the world in 2012.

Since RCS has a multi-modular structure, data on the detection of the following malicious programs were included (using Kaspersky Lab's classification names).

- **Backdoor.OSX.Morcut**
- **Rootkit.OSX.Morcut**
- **Trojan.OSX.Morcut**
- **Backdoor.Win32.Korablin**
- **Backdoor.Win64.Korablin**
- **Rootkit.Win32.Korablin**
- **Rootkit.Win64.Korablin**
- **Trojan.Multi.Korablin**
- **Trojan-Dropper.Win32.Korablin**
- **Trojan-PSW.Win32.Agent.acnn**

If a user is subjected to an attack several times, the detection data is aggregated.



The total number of recorded attempts to install RCS on computers running Kaspersky Lab products around the world, January 2012 – February 2013

Remember, we only have data on attempts to infect computers running Kaspersky Lab products, and only those where users agreed to participate in KSN. Considering the specifics and the highly targeted nature of RCS attacks, their number can't be very large.

It is possible to assess the motives of the attackers by comparing the number of infection attempts made against a single computer in each country. Tajikistan and India are both leaders for this indicator; incidentally, in both of these countries, just one computer was attacked, and RCS installation attempts were persistent, at 21 and 20 attempts, respectively.

RCS is very prevalent in Mexico, where each of the 11 targeted computers were attacked an average of 14.5 times. Users in Italy were attacked the most, with a total of 19 computers targeted an average of 6.5 times each.

Country	Number of unique user	Number of attacks	Number of attacks per user

Mexico	11	159	14.5
Italy	19	123	6.5
Vietnam	10	88	8.8
UAE	9	77	8.6
Iraq	5	42	8.4
Lebanon	2	29	14.5
Morocco	4	27	6.8
Panama	4	23	5.8
Tajikistan	1	21	21.0
India	1	20	20
Iran	2	19	9.5
Saudi Arabia	3	19	6.3
South Korea	5	18	3.6
Spain	4	18	4.5
Poland	6	16	2.7
Turkey	5	12	2.4
Argentina	2	12	6.0
Canada	1	8	8.0
Mali	1	8	8.0
Oman	1	8	8.0
China	3	8	2.7
the US	4	6	1.5
Kazakhstan	2	5	2.5
Egypt	1	5	5.0
Ukraine	1	5	5.0
Uzbekistan	1	5	5.0
Colombia	1	4	4.0
Taiwan	3	4	1.3
Brazil	2	4	2.0
Russia	2	4	2.0
Kyrgyzstan	2	3	1.5
Great Britain	1	3	3.0
Bahrain	1	2	2.0
Ethiopia	1	1	1.0
Indonesia	1	1	1.0
Germany	1	1	1.0
Libya	1	1	1.0

RCS installation attempts against user computers running Kaspersky Lab products around the world, January 2012 – February 2013

Furthermore, just under 10 incidents were logged at workstations in government agencies, industrial companies, legal firms, and media outlets.

Conclusion

In recent years, the world has seen some major changes that computer users have only just found out about: software programs used as cyberweapons and for cyberespionage.

We have also seen the emergence of privately owned companies that, according to the information on their official websites, develop and offer software to law enforcement agencies to facilitate the collection of data from user computers. Countries that do not have the requisite technical capabilities are thus able

to purchase software with similar functions from private companies. In spite of the fact that most countries have laws prohibiting the creation and distribution of malicious programs, this spyware is offered with almost no attempt to conceal its functions.

So far, there aren't very many of these companies and almost no competition in this particular market. These conditions are highly attractive to new players and have planted the seeds for a technologies race among them. At the same time, according to Kaspersky Lab's data, these companies are not held accountable for how their tracking software is used, be it in international espionage or traditional cybercrime used by small-time scammers to make money.

The situation is further complicated by the possibility of these types of programs hitting the shelves on the open market, where fictitious companies, for example, could resell them however they wish.

References

1. The RCS advertising pamphlet http://www.hackingteam.it/images/stories/RCS2012.pdf
2. Citizen Lab's article on its RCS investigation https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/
3. Vupen's company description http://www.vupen.com/english/company.php
4. An entry on Adobe's blog on the detection of an unknown vulnerability http://blogs.adobe.com/psirt/2013/02/security-updates-available-for-adobe-flash-player-apsb13-04.html
5. HackingTeam documents published on WikiLeaks http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf
6. OPM Security's description of Power Spy software http://www.opmsecurity.com/security-tools/spying-on-on-your-husband-wife-children-or-employees.html

2 comments

Oldest first Newest first Table view Threaded view

Sahil KAV
2013 May 30, 16:37

1

KAV 2012

KASPERSKY ANTI-VIRUS IS BEST

Reply

Michael Haephrati, TargetEye
2013 Aug 20, 15:22

0

The Target Eye Monitoring System

I would like to bring another aspect which is legitimate spyware, mostly used by law enforcement agencies to fight crime and terror, and can be used for self monitoring and parental control as well.

http://www.codeproject.com/Articles/310530/Target-Eye-Revealed-part-1-Target-Eyes-Unique-Auto

http://www.codeproject.com/Articles/460498/Target-Eye-Revealed-part-2-Target-Eyes-Screen-Capt

http://www.codeproject.com/Articles/461344/Target-Eye-Revealed-part-3-The-Shopping-List-Mecha

http://www.codeproject.com/Articles/635134/Target-Eye-Revealed-part-4-Keyboard-Capturing

Reply

If you would like to comment on this article you must first login

Descriptions
Glossary
RSS feeds
Contacts
Search

Downloads
Support
Partners
About Us
Search