UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

*Join the Global Conversation*

**The Citizen Lab**

**Research Brief**
February 2014

# *Hacking Team and the Targeting of Ethiopian Journalists*

Authors: Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton

*This post is the first in a series of posts that focus on the global proliferation and use of Hacking Team's RCS spyware, which is sold exclusively to governments.*

Read the report's coverage in the Washington Post and watch PostTV's video.

See the report on Washington Post's front page. [pdf]

Read the second report in the series, "Mapping Hacking Team's "Untraceable" Spyware".

Read the third report in the series, "Hacking Team's US Nexus."

## SUMMARY

- Ethiopian Satellite Television Service[1] (ESAT) is an independent satellite television, radio, and online news media outlet run by members of the Ethiopian diaspora. The service has operations in Alexandria, Virginia, as well as several other countries.[2] ESAT's broadcasts are frequently critical of the Ethiopian Government. Available in Ethiopia and around the world, ESAT has been subjected to jamming from within Ethiopia several times in the past few years.[3] A recent documentary shown on Ethiopian state media warned opposition parties against participating in ESAT programming.[4]

- In the space of two hours on 20 December 2013, an attacker made three separate attempts to target two ESAT employees with sophisticated computer spyware, designed to steal files and passwords, and intercept Skype calls and instant messages. The spyware communicated with an IP address belonging to Ariave Satcom, a satellite provider that services Africa, Europe, and Asia.[5] In each case, the spyware appeared to be Remote Control System (RCS), sold exclusively to governments by Milan-based Hacking Team.[6]

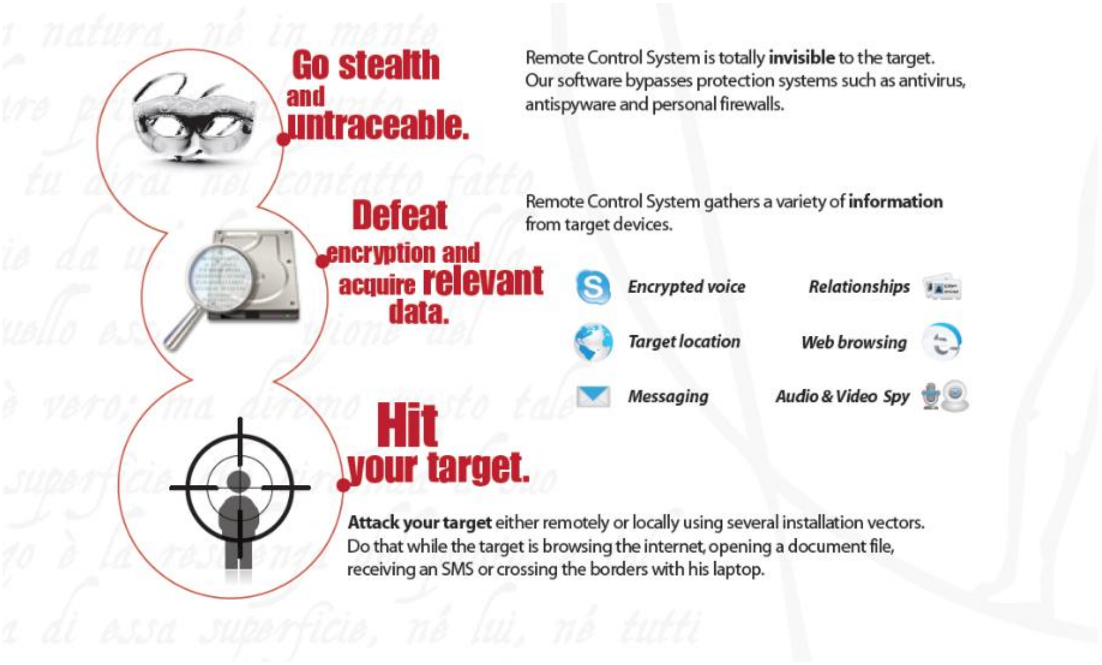
- Hacking Team states that they do not sell RCS to “repressive regimes”,[7] and that RCS is not sold through “independent agents”.[8] Hacking Team also says that all sales are reviewed by a board that includes outside engineers and lawyers. The board has veto power over any sale.[9] Before authorizing a sale, the company states that it considers “credible government or non-government reports reflecting that a potential customer could use surveillance technologies to facilitate human rights abuses,” as well as “due process requirements” for surveillance.[10]

- The Committee to Protect Journalists (CPJ) reports that Ethiopia jails more journalists than any other African country besides Eritrea, and says that the Ethiopian government has shut down more than seventy-five media outlets since 1993.[11] CPJ statistics also show that seventy-nine journalists have been forced to flee Ethiopia due to threats and intimidation over the past decade, more than any other country in the world.[12] A 2013 Human Rights Watch (HRW) report detailed ongoing torture at Ethiopia’s Maekelawi detention center, the first stop for arrested journalists and protests organizers. Former detainees described how they were “repeatedly slapped, kicked, punched, and beaten,” and hung from the ceiling by their wrists. Information extracted in confession has been used to obtain conviction at trial, and to compel former detainees to work with the government.[13] HRW also indicated abuses committed by the army, including the use of torture and rape to compel information from villagers near the site of an attack on a farm.[14] HRW noted “insufficient respect for … due process” in Ethiopia.[15]

# BACKGROUND

## Hacking Team and Remote Control System (RCS)

Hacking Team, also known as HT S.r.l., is a Milan-based purveyor of “offensive technology” to governments around the world. One of their products, known as Remote Control System (RCS), is a trojan that is sold exclusively to intelligence and law enforcement agencies worldwide. Hacking Team’s website describes the product as “the solution” to monitor targets that are increasingly using encryption, or those located outside the borders of the government that wants to monitor them.[16]



**Go stealth** and **untraceable.**

Remote Control System is totally **invisible** to the target. Our software bypasses protection systems such as antivirus, antispyware and personal firewalls.

**Defeat** encryption and acquire **relevant** data.

Remote Control System gathers a variety of **information** from target devices.

| | |
|---|---|
| *Encrypted voice* | *Relationships* |
| *Target location* | *Web browsing* |
| *Messaging* | *Audio & Video Spy* |

**Hit your target.**

**Attack your target** either remotely or locally using several installation vectors. Do that while the target is browsing the internet, opening a document file, receiving an SMS or crossing the borders with his laptop.

**Description of RCS in a 2011 official brochure.[17]**

RCS infects a target's computer or mobile phone to intercept data before it is encrypted for transmission, and can also intercept data that is never transmitted. For example, it can copy files from a computer's hard disk, and can also record Skype calls, e-mails, instant messages, and passwords typed into a Web browser.[18] Furthermore, RCS can turn on a device's webcam and microphone to spy on the user.[19]

While Hacking Team claims to potential clients that RCS can be used for mass surveillance of "hundreds of thousands of targets,"[20] public statements by Hacking Team emphasize RCS's potential use as a targeted tool for fighting crime and terrorism.[21]

Hacking Team was first thrust into the public spotlight in 2012 when RCS was used against award-winning Moroccan media outlet Mamfakinch,[22] and United Arab Emirates (UAE) human rights activist Ahmed Mansoor, who was pardoned[23] after serving seven months in prison for signing an online pro-democracy petition.[24] Mansoor was infected, his Gmail password was stolen, and his e-mails were downloaded.[25] At the same time, RCS is apparently being used by foreign governments to target individuals on US soil.[26,27]

Evidence of the use of RCS against journalists and activists led Reporters Without Borders to name Hacking Team as one of the five "Corporate Enemies of the Internet."[28] Hacking Team Senior Counsel Eric Rabe responded with a defense of his company's sales practices, in which he stated that Hacking Team does not provide its products to "repressive" regimes.[29]

*On the issue of repressive regimes, Hacking Team goes to great lengths to assure that their software is not sold to governments that are blacklisted by the EU, US, NATO, and similar international organizations, or to any "repressive" regime.*

"Repressive" is a subjective term that may be difficult to define. We instead look to a selection of publications that rank countries based on freedom and democracy using a methodology. For example, *The Economist* publishes a Democracy Index,[30] which rates governments around the world on a spectrum from "full democracies" to "authoritarian regimes." Reporters Without Borders also publishes a yearly Press Freedom Index, which ranks countries' press freedom situations from "good" to "very serious."[31]

### Ethiopia and Ethiopian Satellite Television Service (ESAT)

*The Economist* ranks Ethiopia as an "authoritarian regime," and Reporters Without Borders classifies it as a country that presents a "difficult situation" for journalists. Human Rights Watch calls Ethiopia's press law "deeply flawed," and notes that several award-winning journalists have been convicted under the law for exercising their right to freedom of expression, as part of a government crackdown on independent media.[32]

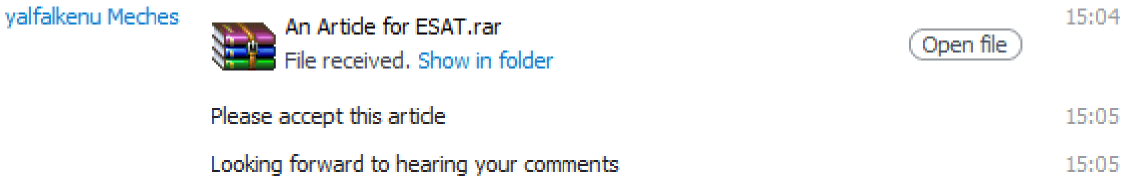
Journalists jailed under the press law includes Eskinder Nega, who was convicted of terrorism in 2012 in a case following the publication of his column that criticized the government's detention of journalists.[33] Nega won the 2012 PEN America Freedom to Write Award, and was hailed by the group as of the "bravest and most admirable of writers, one who picked up his pen to write things that he knew would surely put him at grave risk."[34] Nega is currently serving an eighteen year sentence in prison, having "[fallen] victim to exactly the measures he was highlighting."[35] In a May 2013 letter from prison, he wrote, "I will live to see the light at the end of the tunnel. It may or may not be a long wait. Whichever way events may go, I shall persevere!"[36]

ESAT describes itself as "powered by broad-based collective of exiled journalists, human rights advocates, civic society leaders and members in the Diaspora." Available in Ethiopia and around the world, ESAT's television and radio signals have been subjected to jamming from within Ethiopia several times in the past few years.[37]

Previous research by the Citizen Lab found a version of the FinFisher government spyware that used a picture of members of Ethiopian opposition group Ginbot 7 as bait, indicating politically-motivated targeting. That spyware communicated with a command-and-control server in Ethiopia.[38]

## FIRST TARGETING ATTEMPT

First, the ESATSTUDIO Skype account was targeted with spyware. This account is used by ESAT for on-air interviews. The individual operating the ESATSTUDIO account at the time was an ESAT employee in Belgium, responsible for managing ESAT's satellite broadcasts. An individual identified as "Yalfalkenu Meches" (Skype: yalfalkenu1) sent a file to ESATSTUDIO entitled "An Article for ESAT.rar." We use Skype logs provided by the targets to illustrate the attacks.



yalfalkenu Meches

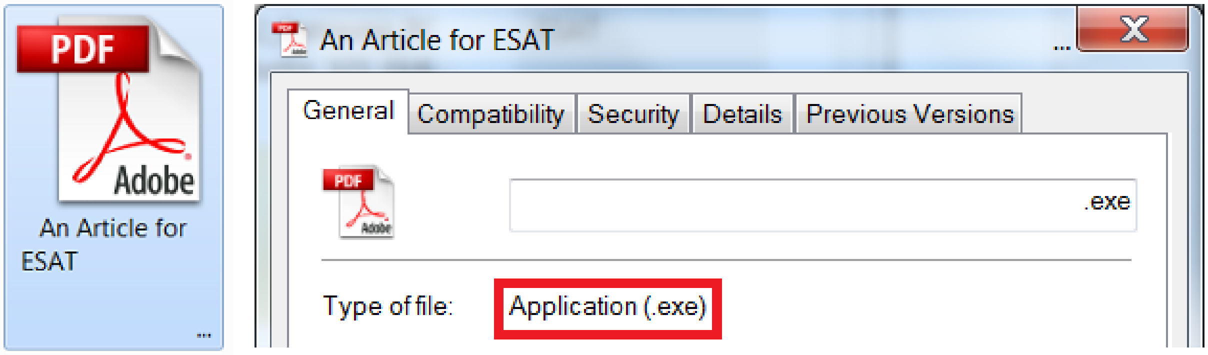
An Article for ESAT.rar
File received. Show in folder

15:04

Please accept this article 15:05

Looking forward to hearing your comments 15:05

This .rar file contained an .exe file disguised as a .pdf. The file used the Adobe PDF icon, and contained a large number of spaces between the name and extension, to prevent Windows from displaying the extension.



Type of file: Application (.exe)

**Left: How the file was rendered in Windows; Right: Windows file properties dialog**

Despite the file's name, "An Article for ESAT," the file did not display any such article, or any other content, when opened.

## ANALYSIS AND LINK TO HACKING TEAM RCS

### Summary

The file sent to ESAT appeared to be Hacking Team's RCS spyware for the following two reasons:

- The file communicated with a server that returned two SSL certificates. The second certificate was issued by "RCS Certification Authority" / "HT srl", and was similar to SSL certificates returned by two other servers apparently owned by Hacking Team. The first certificate was similar to certificates returned by two other servers that appeared to be demonstration servers for Hacking Team's RCS spyware.

- The file matched a signature that we had previously developed for RCS spyware.

### Detailed Analysis

The hash of the file was:

sha256: 4a53db7b98aa000aeaa72d6a44004ef9ed3b6c09dd04a3e6015b62d741de3437 sha1: b7438e699dd54f8b56fc779c1b8b08b1943d9892 md5: 53a9e1b59ff37cc2aeff0391cc546201

Shortly after opening the .exe file, it attempted to communicate with the server 46.4.69.25 on port 80.

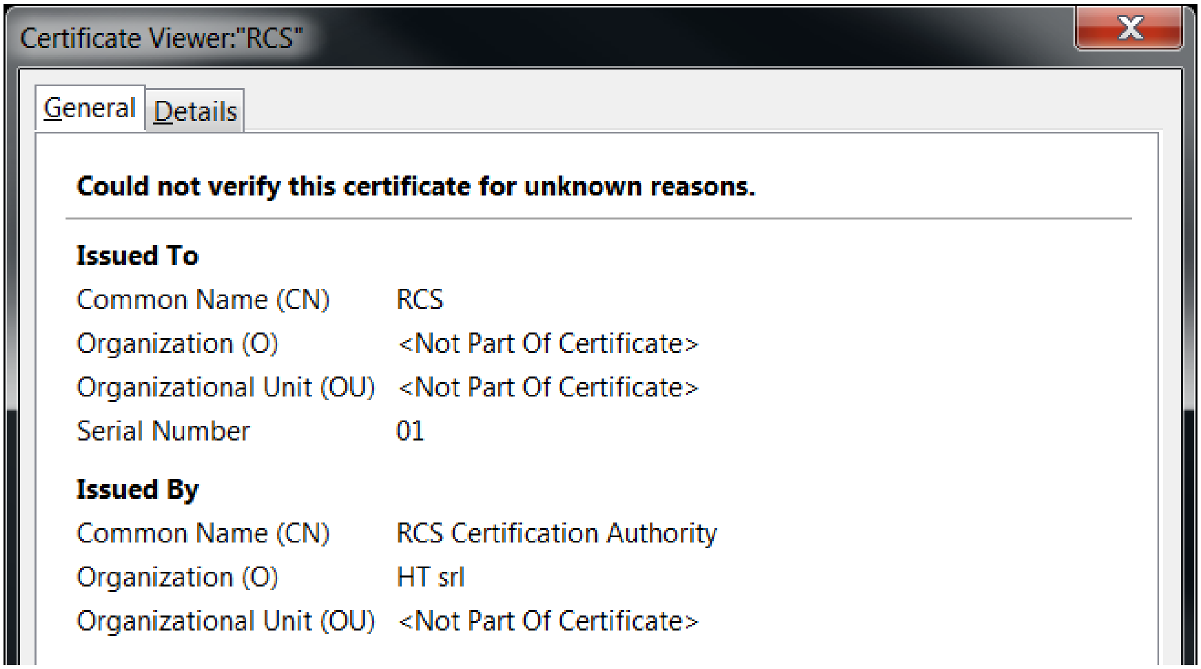
inetnum: 46.4.69.0 - 46.4.69.31 netname: HETZNER-RZ14 descr: Hetzner Online AG descr: Datacenter 14 country: DE

We probed the server and noticed that it returned two self-signed SSL certificates:[39]

| Issuer | Subject | Fingerprint |
|---|---|---|

| | | |
|---|---|---|
| /CN=default | /CN=server | a7c0eacd845a7a433eca76f7d42fc3fedf1bde3c |
| /CN=RCS Certification Authority /O=HT srl | /CN=RCS Certification Authority /O=HT srl | 6500c243015a6ecc59f1272fec38eb0065d22063 |

The second certificate is issued by "RCS Certification Authority" / "HT srl".



Certificate Viewer:"RCS"

General | Details

**Could not verify this certificate for unknown reasons.**

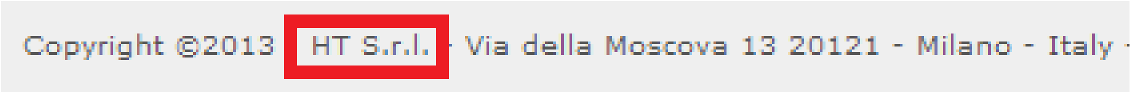
**Issued To**

Common Name (CN) RCS
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 01

**Issued By**

Common Name (CN) RCS Certification Authority
Organization (O) HT srl
Organizational Unit (OU) <Not Part Of Certificate>

Hacking Team refers to their spyware as "RCS," and identifies itself as "HT S.r.l." on its website:



Copyright ©2013 HT S.r.l. - Via della Moscova 13 20121 - Milano - Italy -

To confirm our hypothesis that these certificates were associated with Hacking Team, we searched historical SSL certificate data released by the Internet Census[40] (443-TCP_SSLSessionReq) and by the University of Michigan's zmap project.[41] We found two servers returning the "RCS Certification Authority" / "HT srl" certificate that were in the following range:

inetnum: 93.62.139.32 - 93.62.139.47 netname: FASTWEB-HT descr: HT public subnet
country: IT
person: GIANCARLO RUSSO address: VIA DELLA MOSCOVA 13 address: MILANO MI
address: IT phone: +39 0229060603

The address and phone number on the range matches those on Hacking Team's website. A Giancarlo Russo is listed as the Chief Operating Officer of Hacking Team on LinkedIn.[42] Thus, we believe that Hacking Team controls this range of IP addresses.

The two servers in this range that returned similar certificates to the server in the ESAT spyware were:

93.62.139.39 on 6/28/2012:

| Issuer | Subject | Fingerprint |
|---|---|---|
| /CN=RCS Certification Authority /O=HT srl | /CN=rcs-castore | deee895bf1f68e97cb997d929e0f991ecec6ab29 |
| /CN=RCS Certification Authority /O=HT srl | /CN=RCS Certification Authority /O=HT srl | 1e8e8806aa605544cda2bbb906b5d0cc7fb6fff7 |

93.62.139.42 on 8/12/2012:

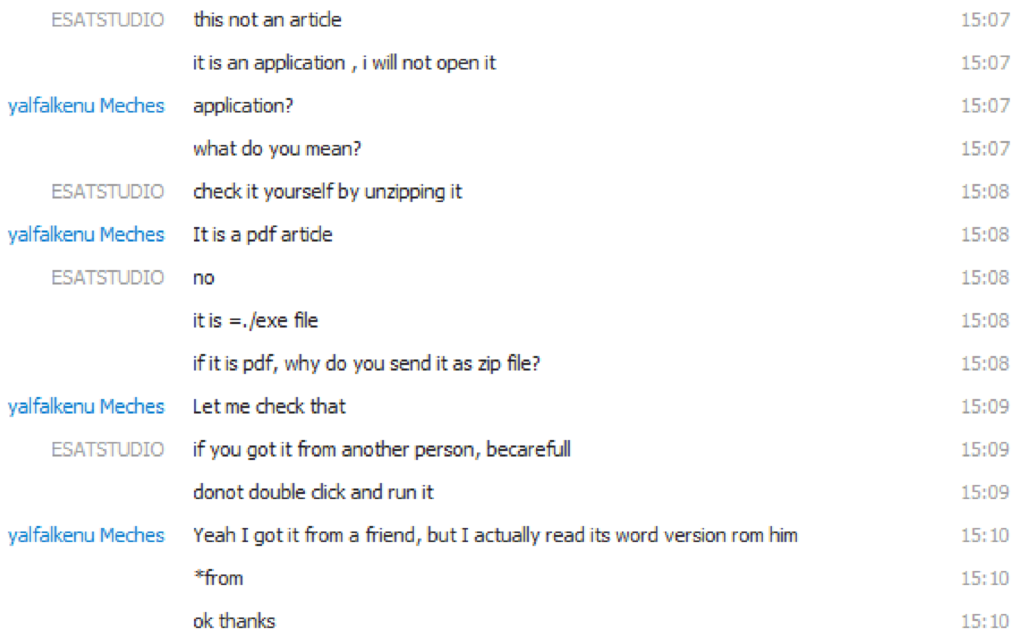
| Issuer | Subject | Fingerprint |
|---|---|---|
| /CN=RCS Certification Authority /O=HT srl | /CN=rcs-polluce | 277fdf33df7baca54ce8336982db865d9f38f514 |
| /CN=RCS Certification Authority /O=HT srl | /CN=RCS Certification Authority /O=HT srl | e8d5f17d142768abe2ed835d5a61d99602ab082b |

Because these IP addresses were registered to Hacking Team, we believe that the presence of a certificate apparently issued by “RCS Certification Authority” / “HT srl” is indicative of a server for Hacking Team’s RCS spyware. The Internet Census (443-TCP_SSLSessionReq) also recorded two instances of a server returning a certificate that matched the “default” / “server” certificate returned by the server in the ESAT spyware, along with an incomplete certificate for “rcs-demo.hackingteam.it.” This server was used by an RCS spyware sample found in VirusTotal.[43] This certificate was returned by 168.144.159.167 on 12/14/2012, and by 94.199.243.39 on 12/14/2012. This is a further indication that the server in the spyware targeting ESAT is a Hacking Team RCS server.

The file itself also matched a signature we had previously developed for RCS spyware.

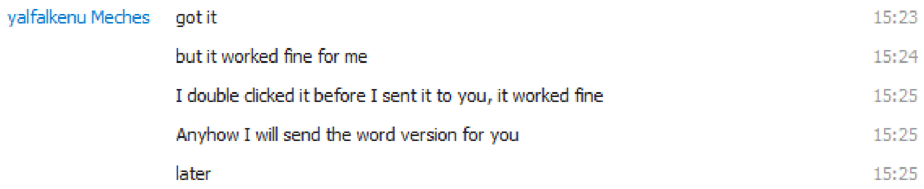
## SECOND ATTEMPT

The target did not open the first file (“An Article for ESAT.exe”), and complained to Yalfalkenu that the file was an .exe application. Yalfalkenu responded that he had received the file from a friend.



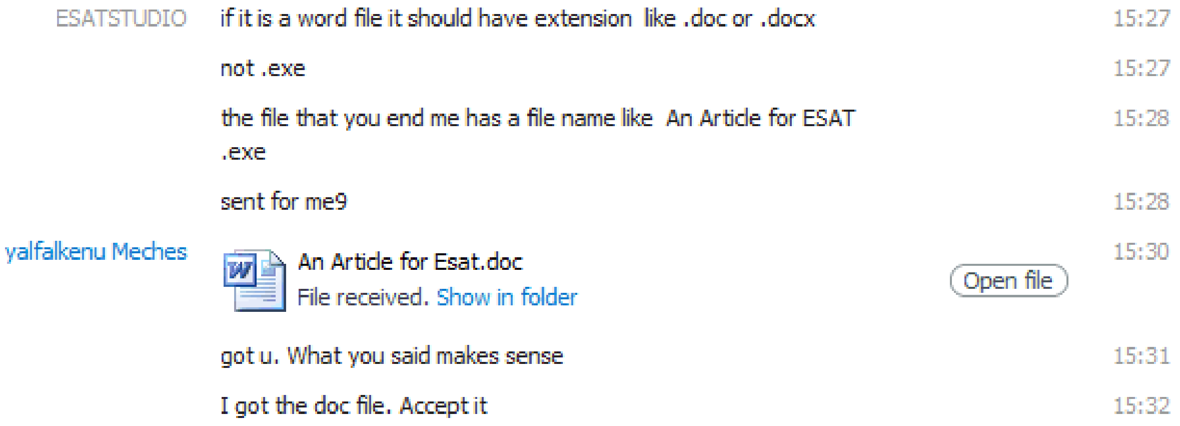
| | | |
|---|---|---|
| ESATSTUDIO | this not an article | 15:07 |
| | it is an application , i will not open it | 15:07 |
| yalfalkenu Meches | application? | 15:07 |
| | what do you mean? | 15:07 |
| ESATSTUDIO | check it yourself by unzipping it | 15:08 |
| yalfalkenu Meches | It is a pdf article | 15:08 |
| ESATSTUDIO | no | 15:08 |
| | it is =./exe file | 15:08 |
| | if it is pdf, why do you send it as zip file? | 15:08 |
| yalfalkenu Meches | Let me check that | 15:09 |
| ESATSTUDIO | if you got it from another person, becarefull | 15:09 |
| | donot double click and run it | 15:09 |
| yalfalkenu Meches | Yeah I got it from a friend, but I actually read its word version rom him | 15:10 |
| | *from | 15:10 |
| | ok thanks | 15:10 |

Yalfalkenu also said that he opened the .exe file and it "worked fine." However, despite the file's name, "An Article for ESAT," the file did not display any such article, or any other content, when opened.



| | | |
|---|---|---|
| yalfalkenu Meches | got it | 15:23 |
| | but it worked fine for me | 15:24 |
| | I double clicked it before I sent it to you, it worked fine | 15:25 |
| | Anyhow I will send the word version for you | 15:25 |
| | later | 15:25 |

Yalfalkenu followed up by sending ESATSTUDIO a Word document.



| | | |
|---|---|---|
| ESATSTUDIO | if it is a word file it should have extension like .doc or .docx | 15:27 |
| | not .exe | 15:27 |
| | the file that you end me has a file name like An Article for ESAT .exe | 15:28 |
| | sent for me9 | 15:28 |
| yalfalkenu Meches | An Article for Esat.doc<br>File received. Show in folder<br>Open file | 15:30 |
| | got u. What you said makes sense | 15:31 |
| | I got the doc file. Accept it | 15:32 |

## Analysis and Link to Hacking Team RCS

The Word document was:

sha256: 5bde4288c11f0701b54398ffeeddb4d6882d91b3e34bf76b1e250b8fc46be11d sha1: 057675f8dfda0f44a695ec18a5211ff4e68a1873 md5: 8df850088e2324d5c89615be32bd8a35

As with the previous file, opening this file did not result in any bait content being displayed. A user who opened the file saw a blank Word document, which quickly closed itself.

The document exploited a bug in Microsoft Windows (CVE-2012-0158[44]) to run a program that downloaded and executed a file: 216.118.232.254/svchst.exe. An update to Windows available since April 2012 fixes this bug.[45] The IP address 216.118.232.254 belongs to Ariave Satcom, a satellite provider that services Africa, Europe, and Asia.[46]

Private Customer VSC-ARIAVE (NET-216-118-232-0-1) 216.118.232.0 - 216.118.232.255 VSC Satellite Co.
VSC-IPOWN1 (NET-216-118-224-0-1) 216.118.224.0 - 216.118.255.255

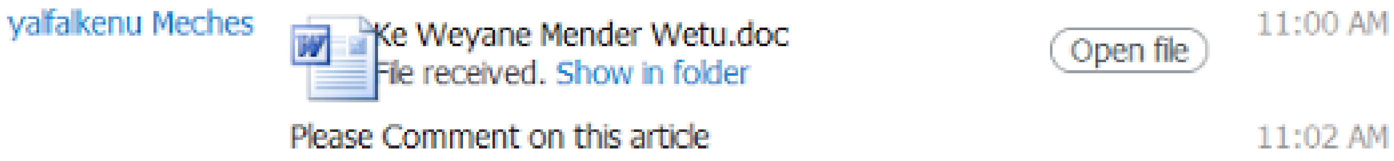
We downloaded svchst.exe:

sha256: bc68c8d86f2522fb4c58c6f482c5cacb284e5ef803d41a63142677855934d969 sha1:
b341cc1c299c07624814f35a35a4d505e65d3b67 md5: 015c238d56b8657c0946ec45b131362a

Like the first file, the file communicated with 46.4.69.25. This file also matched our signature for RCS spyware. For the same reasons as the first file, this file appears to be Hacking Team RCS spyware.

## THIRD ATTEMPT

An hour and a half later on the same day,[47] Yalfalkenu targeted another ESAT employee, this time based in their Northern Virginia offices.



yalfalkenu Meches
Ke Weyane Mender Wetu.doc
File received. Show in folder
11:00 AM
Please Comment on this article
11:02 AM

The document was:

sha256: 8f9a6ae6aa56e12596d02c864998b4373a96d3f788195db3601b6e3ec54a99fb sha1:
c384ca066fe0145455f14976c0ecf8a817a30f86 md5: daa5912d4ca0e4a143378947ef329374

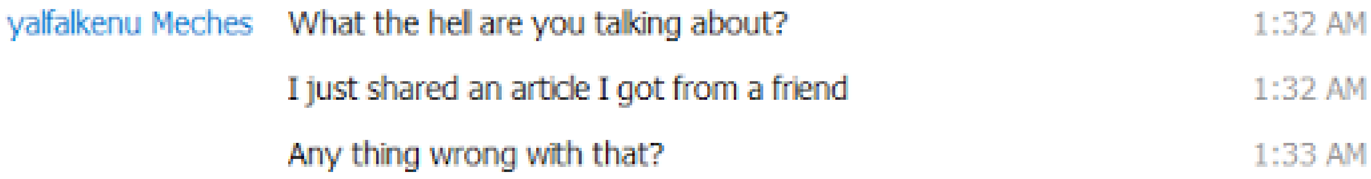
Like the second file, the document also exploited the CVE-2012-0158 bug, but had two main differences. First, the document actually displayed bait content—a copy of this article.[48] Second, instead of downloading a file from a server, the document contained an embedded file, which it copied as CyHidWin.exe. We extracted the file and analyzed it:

sha256: d30bc31d6ad75de20aa3a45d338298030dc9136ba94aee93b4843e279fa3d59c sha1:
4f8b2f1071870b9d03f3bb341cf9523b0574d8f6 md5: c5cfa1afd5d3148a0d33fc1940ea1a37

As in the previous two files, the file communicated with 46.4.69.25. This file also matched our signature for RCS spyware. For the same reasons as the first two files, this file appears to be Hacking Team RCS spyware.

## EPILOGUE

After the first two targeting attempts, we alerted ESAT that Yalfalkenu Meches was trying to target them with spyware. On the third attempt,the targeted user confronted Yalfalkenu, who again professed that he had received the file from a friend.

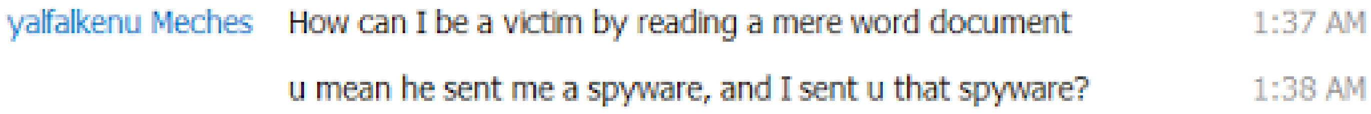


yalfalkenu Meches What the hell are you talking about? 1:32 AM

I just shared an article I got from a friend 1:32 AM

Any thing wrong with that? 1:33 AM

Yalfalkenu also expressed puzzlement about how opening a Word document could infect a computer, and said that he was a victim.



yalfalkenu Meches How can I be a victim by reading a mere word document 1:37 AM

u mean he sent me a spyware, and I sent u that spyware? 1:38 AM

We talked to employees of ESAT, who said that Yalfalkenu used to collaborate with them, but then he "disappeared for a while." It is possible that someone else is now using Yalfalkenu's account.

### Links to Other Spyware

Our scans indicated that the following other servers were likely being run by the same attacker that targeted ESAT, and were also likely Hacking Team RCS servers:

| IP | First Seen | Last Seen | Provider | Country |
|---|---|---|---|---|
| 109.200.22.160 | 7/25/2012 | 8/10/2012 | Delamere Services | UK |
| 109.200.22.161 | 7/25/2012 | 8/12/2012 | Delamere Services | UK |
| 109.200.22.162 | 10/14/2012 | 1/13/2014 | Delamere Services | UK |
| 109.200.22.163 | 10/13/2012 | 1/13/2014 | Delamere Services | UK |
| 176.74.178.45 | 10/30/2013 | 1/13/2014 | Infinite Dimension Solutions | UK |
| 176.74.178.119 | 7/25/2012 | 8/12/2012 | Infinite Dimension Solutions | UK |
| 176.74.178.120 | 7/25/2012 | 8/12/2012 | Infinite Dimension Solutions | UK |
| 176.74.178.202 | 10/13/2012 | 1/13/2014 | Infinite Dimension Solutions | UK |
| 176.74.178.203 | 10/18/2012 | 1/13/2014 | Infinite Dimension Solutions | UK |

| | | | | |
|---|---|---|---|---|
| 46.166.162.147 | 5/16/2013 | 8/11/2013 | Santrex | SC |
| 69.60.98.203 | 5/16/2013 | Active | Serverpronto | US |
| 216.118.232.245 | 11/18/2013 | Active | Ariave Satcom | ?? |

We note that the "RCS Certification Authority" / "HT srl" SSL certificates returned by these servers were issued on 5/8/2012. Based on this date, we estimate that the attacker who targeted ESAT has been using Hacking Team's RCS spyware since May 2012, or earlier.

We found the following sample in VirusTotal that matched our signature for Hacking Team RCS spyware. The sample used 46.166.162.147 as a command-and-control server. Thus, we believe the attackers were the same, though we have no indication as to who they may have targeted:

sha256: 9577aabf5e31af1409e2abe8c29ac918d7f8784dec75b4088a60fce6a45e9fc7 sha1: 0e326c39c91efeff1d045bec3c7e7c38405d0430 md5: c17e788e28d47891f94c64739ee7fffb

## CONCLUSION

In this report, we identified three instances where Ethiopian journalist group ESAT was targeted with spyware in the space of two hours by a single attacker. In each case the spyware appeared to be RCS (Remote Control System), programmed and sold exclusively to governments by Milan-based Hacking Team. While Hacking Team and other "lawful intercept" spyware vendors purport to practice effective self-regulation, this case seems to be part of a broader pattern of government abuse of such spyware. "Lawful intercept" spyware has also apparently been abused to target Bahraini activists, Moroccan journalists, critics of the Turkish Government, and Emirati human rights activists.

## ACKNOWLEDGEMENTS

Thanks to Eva Galperin, the Electronic Frontier Foundation, and ESAT.

## FOOTNOTES

[1] "About ESAT," Ethiopian Satellite Television, accessed February 13, 2014, http://ethsat.com.
[2] "About ESAT," Ethiopian Satellite Television, accessed February 13, 2014, http://ethsat.com.
[3] "ESAT Accuses China of Complicity in Jamming Signals," Ethiopian Satellite Television, June 15, 2011, accessed February 13, 2014, http://ethsat.com/2011/10/08/esat-accuses-china-of-complicity-in-jamming-signals.
[4] "UDJ Says Expressing Opinion to Media is Not 'Terror'," Ethiopian Satellite Television, January 9, 2013, accessed February 13, 2014, http://ethsat.com/2014/01/09/udj-says-expressing-opinion-to-media-is-not-terror.
[5] "Technology," Ariave Satcom, accessed February 13, 2014, https://web.archive.org/web/20130723051052/http://ariave.com/tech.htm.
[6] "Customer Policy," Hacking Team, accessed February 13, 2014, http://hackingteam.it/index.php/customer-policy.
[7] Declan McCullagh, "Meet the 'Corporate Enemies of the Internet' for 2013," CNET, March 11, 2013, accessed February 13, 2014, http://news.cnet.com/8301-13578_3-57573707-38/meet-the-corporate-enemies-of-the-internet-for-2013/.

[8] Mónica Almeida, "Firma Hacking Team Fue Contactada Por Estado Ecuatoriano," El Universo, December 11, 2013, accessed February 13, 2014, http://www.eluniverso.com/noticias/2013/12/11/nota/1901271/firma-hacking-team-fue-contactada-estado-ecuatoriano.

[9] David Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," Interntional Business Times, March 13, 2013, accessed February 13, 2014, http://www.ibtimes.co.uk/hacking-team-murky-world-state-sponsored-spying-445507.

[10] "Customer Policy," Hacking Team.

[11] "Ethiopia Arrests 2 Journalists From Independent Paper," Committee to Protect Journalists, November 5, 2013, accessed February 13, 2014, http://www.cpj.org/2013/11/ethiopia-arrests-2-journalists-from-independent-pa.php.

[12] "Ethiopia," Human Rights Watch, accessed February 13, 2014, http://www.hrw.org/world-report/2013/country-chapters/ethiopia.

[13] "They Want a Confession," Human Rights Watch, October 17, 2013, accessed February 13, 2014, http://www.hrw.org/node/119814/section/2.

[14] "Ethiopia," Human Rights Watch. http://www.hrw.org/world-report/2013/country-chapters/ethiopia?page=3.

[15] Ibid.

[16] "The Solution," Hacking Team, accessed February 13, 2014, http://hackingteam.it/index.php/remote-control-system.

[17] Hacking Team, Remote Control System: Cyber Intelligence Made Easy, accessed February 13, 2014, http://wikileaks.org/spyfiles/docs/hackingteam/147_remote-control-system.html.

[18] "Spyware. HackingTeam," Secure List, April 23, 2013, accessed February 13, 2014, https://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam.

[19] Adrianne Jeffries, "Meet Hacking Team, the Company That Helps the Police Hack You," The Verge, September 13, 2013, accessed February 13, 2014, http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers.

[20] Ibid.

[21] Pratap Chatterjee, "Turning the Table on the Trackers: Wikileaks Sniffs out Spy Salesmen," CorpWatch, September 6, 2013, accessed February 12, 2014, http://www.corpwatch.org/article.php?id=15868.

[22] Ryan Gallagher, "How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists," Slate, August 20, 2012, accessed February 14, 2014, http://slate.me/1eSTeUF.

[23] "Ahmed Mansoor and Four Other Pro-Democracy Activists Pardoned and Freed," Reporters Without Borders, November 28, 2011, accessed February 13, 2014, http://en.rsf.org/united-arab-emirates-ahmed-mansoor-and-four-other-pro-28-11-2011,41477.html.

[24] "UAE Arrests Democracy Activists," BBC, April 11, 2011, accessed February 13, 2014, http://www.bbc.co.uk/news/world-middle-east-13043270http://www.bbc.co.uk/news/world-middle-east-13043270.

[25] Morgan Marquis-Boire, "Backdoors are Forever: Hacking Team and the Targeting of Dissent?," Citizen Lab (2013), October 2012, accessed February 13, 2014, https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent.

[26] Kim Zetter, "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments," Wired, June 4, 2013, accessed February 13, 2014, http://www.wired.com/threatlevel/2013/06/spy-tool-sold-to-governments/.

[27] Christopher Soghoian, Twitter Post, February 5, 2013, 1:03 p.m., accessed February 13, 2014https://twitter.com/csoghoian/status/298899565388644352.

[28] "Corporate Enemies," Reporters Without Borders, accessed February 13, 2014, http://surveillance.rsf.org/en/category/corporate-enemies.

[29] McCullagh, "Meet the 'Corporate Enemies of the Internet' for 2013."

[30] The Economist Intelligence Unit, Democracy Index 2012 (2012), accessed February 13, 2014, https://www.eiu.com/public/topical_report.aspx?campaignid=DemocracyIndex12.

[31] "Freedom of the Press Worldwide in 2013," Reporters Without Borders, 2013, accessed February 13, 2014, https://en.rsf.org/IMG/jpg/2013_wpfi_world_press_freedom_map.jpg.
[32] "Ethiopia: Terrorism Law Decimates Media," Human Rights Watch, May 3, 2013, accessed February 13, 2014http://www.hrw.org/news/2013/05/03/ethiopia-terrorism-law-decimates-media.
[33] "Jailed Ethiopian Journalist Eskinder Nega Honoured," BBC, May 2, 2012, accessed February 13, 2014, http://www.bbc.co.uk/news/world-africa-17921950.
[34] "Top PEN Prize to Honor Eskinder Nega, Jailed Ethiopian Journalist and Blogger," PEN America, April 12, 2012, accessed February 13, 2014, http://www.pen.org/press-release/2012/04/12/top-pen-prize-honor-eskinder-nega-jailed-ethiopian-journalist-and-blogger.
[35] Ibid.
[36] "Eskinder Nega; A Journalist Behind Bars," Amnesty International, November 6, 2013, accessed February 13, 2014, https://www.amnesty.org/en/appeals-for-action/LWM2013-Ethiopia.
[37] "ESAT Accuses China of Complicity in Jamming Signals," Ethiopian Satellite Television.
[38] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab (2013), accessed February 13, 2014, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.
[39] This can be verified by consulting the Sonar SSL scans (https://scans.io/study/sonar.ssl) between 10/30/2013 and 1/13/2014.
[40] Carna Botnet, "Internet Census 2012 Port scanning /0 using insecure embedded devices," accessed February 13, 2014, http://internetcensus2012.bitbucket.org/paper.html.
[41] https://scans.io/study/umich-https
[42] http://it.linkedin.com/pub/giancarlo-russo/2/2a9/589
[43] https://www.virustotal.com/en/file/81e9647a3371568cddd0a4db597de8423179773d910d9a7b3d945cb2c3b7e1c2/analysis/
[44] "CVE-2012-0158," Mitre, accessed February 13, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158.
[45] Security TechCenter, "Microsoft Security Bulletin MS12-027 – Critical," Microsoft, April 10, 2012, accessed February 13, 2014, http://technet.microsoft.com/en-us/security/bulletin/ms12-027.
[46] "Technology," Aviave Satcom.
[47] Belgium's time zone is six hours ahead of Virginia's.
[48] The article quotes the former head of Ethiopia's Amhara region (Ayalew Gobeze) as denying that he was demoted or fired for failing to sign a border demarcation agreement between Sudan and Ethiopia. Ayalew is quoted as saying that members of the Ethiopian diaspora concocted the story, and refers to them as "taxi drivers" and "jobless."