UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
March 2014

Hacking Team's US Nexus

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

This post is the third 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*.

Read the first report in the series, "Hacking Team and the Targeting of Ethiopian Journalists."

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

SUMMARY

- Remote Control System (RCS) is sophisticated computer spyware marketed and sold exclusively to governments by Milan-based Hacking Team.[1] RCS can record Skype calls, copy passwords, e-mails, files and instant messages,[2] and turn on a computer or phone's webcam and microphone to spy on nearby activity.[3] An earlier Citizen Lab report showed how one RCS user believed to be the Ethiopian Government—targeted journalists in the Washington DC area with the spyware. Previously, governments have used RCS to target journalists in Morocco,[4] activists in the UAE,[5] and a US-based critic of Turkish charter schools.[6]

- Two weeks ago, the present authors released a report Mapping Hacking Team's "Untraceable" Spyware, which identifies 21 governments that we suspect are current or former users of RCS. The report showed that computers infected with RCS send surveillance data back to the government operator through a series of servers in multiple third countries, called a proxy chain or circuit. This is to prevent someone who discovers a copy of the spyware or an infected computer from tracing it back to the government. For example, an infected target may discover that his computer is sending

information to a server in Fremont, California, but would not be able to trace the ultimate destination of this information to Uzbekistan.

- In this post, we delve deeper into these proxy chains, and find that in at least **12 cases, US-based data centers are part of this dedicated foreign espionage infrastructure**. Our analysis traces these proxy chains, and finds that US-based servers appear to assist the governments of **Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and the United Arab Emirates** in their espionage and/or law enforcement operations. Azerbaijan, Ethiopia, and Uzbekistan receive the lowest ranking, "authoritarian," in *The Economist's* 2012 Democracy Index.[7]

- The extensive and deliberate use of dedicated US hosting companies by foreign countries' wiretapping activities raises a number of pressing legal and policy concerns. These include whether RCS client countries violate US law and longstanding international legal principles on sovereignty and nonintervention through use of this spyware. Moreover, RCS client countries, by exposing wiretap data to US and other jurisdictions, may have violated internal laws governing the safeguarding of wiretapped material.

- We also identify several cases where US-based spyware servers were disguised as the websites of US companies, including a small New York-based financial services firm related to an SEC investigation, a small Oregon newspaper, and ABC News. We believe that the disguises were designed to mislead targets if they discovered that their systems were communicating with these servers. Thus, we believe that the targets of the the spyware in these instances had some familiarity with these companies.

FOREIGN ESPIONAGE USING US SERVERS

RCS's use of third-country proxy servers[8] to launder data from infected computers back to the government operator of the spyware raises a number of questions. First, how are the third-country proxies selected? Are the proxy locations selected by Hacking Team itself, or its government clients? If Hacking Team selects the locations, does it inform its clients of these? How does Hacking Team represent itself when engaging with a hosting company to procure servers for use as proxies? Does Hacking Team evaluate the laws of the countries in which it employs servers to determine the legality of their use for surveillance? The answers to these questions have important legal and policy implications, discussed below.

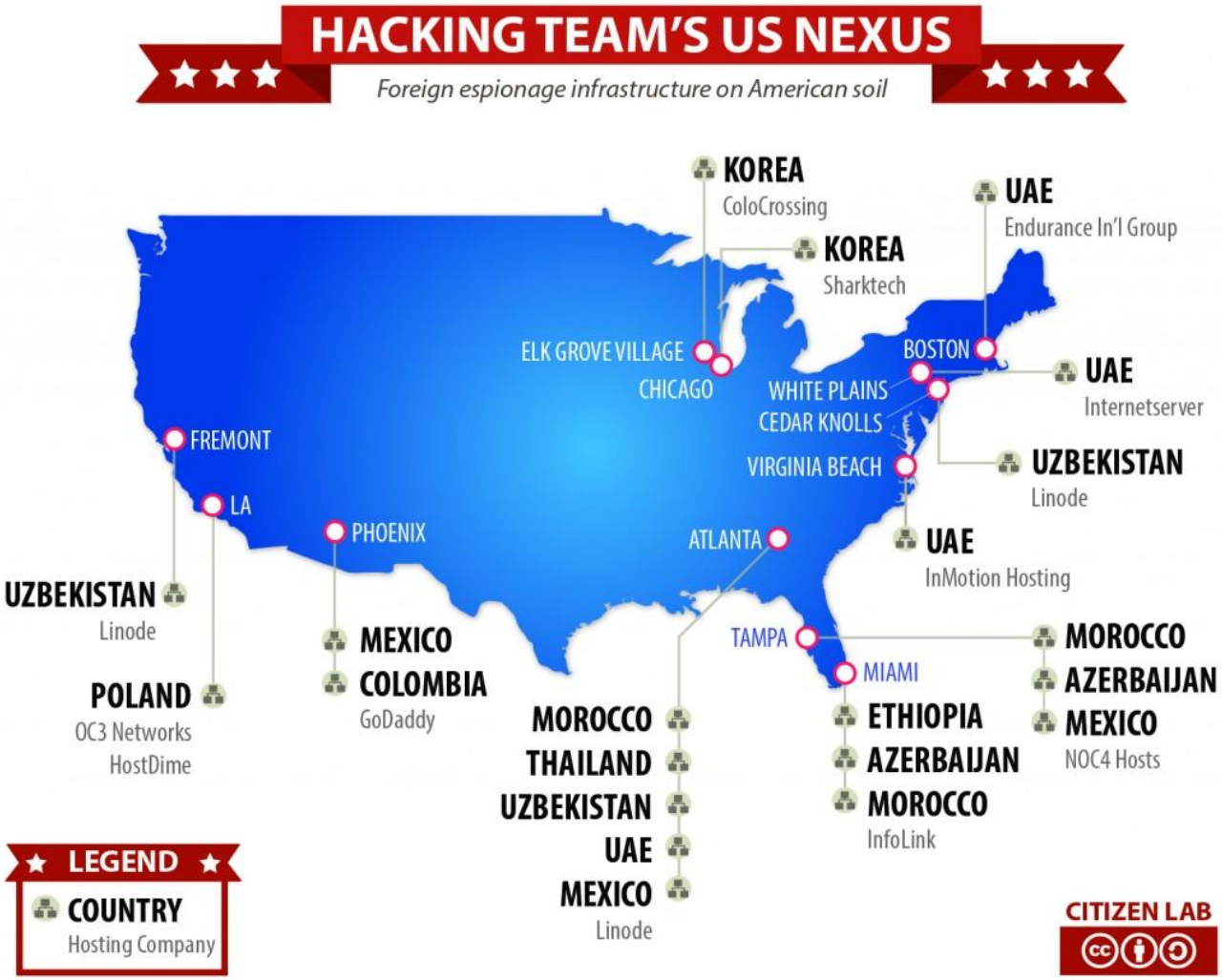

Figure 1: US Nexus of Hacking Team Circuits

We found 10 foreign governments using RCS proxy chains with a US nexus:

Number of Hacking Team RCS servers	555
Number of Hacking Team RCS servers in the US	114
Number of identified RCS proxy chains	103
Number of identified RCS proxy chains with US nexus	22
RCS proxy chains with US nexus attributed to foreign governments	14
Number of foreign governments using RCS proxy chains with a US nexus	10

We found 10 foreign governments using RCS proxy chains with a US nexus:

Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and UAE

Click here For Appendix A and a full list of all circuits with a US Nexus.

LINODE

Atlanta, GA

A facility ringed with razor wire in an industrial part of Atlanta run by Linode hosts Hacking Team command and Control circuits for **Moroco**, **Thailand**, **Uzbekistan**, **Mexico** and the **UAE**. A server directly registered to Hacking Team is also operated from this facility.

INMOTION HOSTING

Virginia Beach, VA

Tucked into a suburban office park next to a Wawa Gas Station and Four Seasons Chinese, Inmotion's data center handles traffic from a Hacking Team circuit traced to the United Arab Emirates.

Other Transit Countries

Beyond the US, a number of other countries are also large hosters of Hacking Team servers. We list the top 5 countries and top 5 providers below:

Provider	Number of Servers
Linode	80
Telecom Italia	32
Santrex	26
Rackspace	19
NOC4Hosts	16

Country	Number of Servers
United States	114

Italy	48
United Kingdom	43
Seychelles	26
Japan	17

A DELIBERATE AND EXPANSIVE US NEXUS: LEGAL AND POLICY IMPLICATIONS

The US is a major provider of internet service, meaning that a great deal of global internet traffic passes through US servers. However, this case poses novel challenges that deserve heightened legal and policy scrutiny.

- The passage of RCS traffic through the US is not normal routing incident to benign electronic communications, but the purposeful use of US servers for the surreptitious transmission of wiretapped data to foreign governments. Whether moving such information through US-based communications facilities violates US law, including the Computer Fraud and Abuse Act and the Wiretap Act, deserves immediate attention.

- We doubt foreign governments using Hacking Team's RCS spyware seek permission from the US government to engage in surveillance of US-based targets, or to transmit surveilled data obtained elsewhere through US-based services. Without that consent, foreign governments using the RCS spyware in this manner wilfully flout the international legal principles of sovereignty and nonintervention. These principles provide the basis for the formal rules and procedures states have developed for law enforcement cooperation and assistance concerning investigation of crimes with transnational dimensions. Moreover, unauthorized interception of electronic communications within the US by a foreign government is contrary to US law.

- We question whether Hacking Team has informed its government clients of the potential legal liabilities raised by the design and operation of its RCS spyware. We also question whether Hacking Team tells its government clients that information obtained through domestically-initiated wiretaps passes by design through servers located in the US or other countries – routing that might violate that government's own laws on electronic surveillance.

- Hacking Team's use of US-based services as part of its spyware also creates liabilities for the companies providing such service. As a matter of corporate social responsibility, these companies certainly would want to ensure that their services are not used for purposes potentially in violation of US and international law and inimical to the enjoyment of basic human rights. We suspect Hacking Team does not inform its US-based service providers of the nature of the data it transmits, and question what representations Hacking Team has in fact made to these companies.

- In addition, the Hacking Team spyware appears to violate terms of service that internet service providers typically include in their contracts with customers. For example, under its terms of service,

> Linode can terminate a contract if a customer attempts unauthorized and / or illegal access to computers, networks or accounts not belonging to the party seeking access. Similarly, any act involving circumvention of security measures is forbidden.

Excerpt from Linode's Terms of Service[9]

You agree that any of the below activities are considered prohibited usage and will result in immediate account suspension or cancellation without a refund and the possibility that Linode.com will impose fees; and/or pursue civil remedies without providing advance notice. . . .

Access to Other Computers or Networks without Authorization: Attempting unauthorized and/or illegal access of computers, networks and/or accounts not belonging to party seeking access. Any act which interferes with the services of another user or network. Any act relating to the circumvention of security measures.

The operation of Hacking Team's spyware in many situations involves knowing violation of such contractual terms, and companies used to facilitate the spyware's functioning are well within their rights to terminate the service and pursue other legal remedies.

As our research peels back the layers of obfuscation that are inherent to the spyware market, it is becoming clear that this market takes advantage of opaque or non-existent laws, rules, and procedures—in effect, slipping through the cracks of the international system. Remedying the adverse consequences of this market will require filling those gaps.

A PERPLEXING CASE: REDIRECTIONS TO US SERVERS

Separate from foreign use of US infrastructure to launder data from infected computers back to government operators, we identified the possible use of US servers to target US-based targets. We are unable to speculate as to the government operators in this case.

In 2012 and early 2013, most Hacking Team servers, when viewed in a web browser, were disguised as http://www.google.com, i.e., they loaded a page that immediately redirected to Google. This redirection is never invoked by the spyware itself, and seems designed to make a Hacking Team RCS server appear to be another website to an individual who loads the server address into their web browser.[10] However, we found a group of 20 highly distinctive Hacking Team servers hosted by Linode and Rackspace that were, in some cases, disguised as the websites of US-based corporations. This was only one of two cases where we identified redirections to sites other than Google. We briefly summarize the redirects we found in this group:

C2 Server	Redirected to Website	Dates of Redirect
198.101.232.81	http://www.blackberry.com/btsc/kb18327	8/10/2012 – 8/30/2012
198.101.232.37	http://www.blackberry.com/btsc/kb18327	8/10/2012 – 8/30/2012
50.56.182.189	http://www.blackberry.com/security	10/26/2012

50.56.182.189	http://www.apple.com	12/14/2012 – 12/15/2012
184.106.244.36	http://www.apple.com	3/31/2013 – 5/9/2013
66.228.61.26	http://www.apple.com	12/13/2012 – 5/7/2013
184.106.196.42	http://www.mailtribune.com	12/14/2012 – 12/15/2012
108.171.173.171	http://www.davidlerner.com/default.aspx	12/14/2012 – 5/2/2013
166.78.143.145	http://www.fidelity.com	3/7/2013 – 4/18/2013
50.57.153.182	http://www.publix.com	4/22/2013 – 5/5/2013
173.230.142.200	http://www.abcnews.com	7/25/2012
173.255.234.29	http://www.abcnews.com	7/25/2012 – 12/15/2012

We cannot conclusively say what purpose the disguises serve. It is possible that the servers employed these specific disguises in order to appear benign to a target who noticed their computer communicating with one of these servers. For example, a target might discover one of these server IP addresses in their connection logs, and put the address into their web browser to investigate. Or a target might receive bait content containing spyware hosted at one of these IP addresses,[11] and then put the IP into their browser to see if it appeared associated with the bait content.

The most interesting redirects seem to be http://www.davidlerner.com/default.aspx (David Lerner Associates; a New York-based financial firm), and http://www.mailtribune.com (Mail Tribune; a small local newspaper in Oregon). We observed the redirect to David Lerner between 12/14/2012 and 5/2/2013. David Lerner was sanctioned by self-regulatory agency FINRA on 22 October 2012.[12] On 13 March 2013, Apple REIT revealed that its REITs Six, Seven, Eight, and Nine, were under SEC investigation, which the SEC refused to confirm or deny;[13] David Lerner Associates was the sole underwriter and distributor for Apple REITs One through Ten.[14] We emphasize that we do not know who the targets of the spyware were in any of these cases, and are including this information only for the purpose of spurring further investigation.

In the case of http://www.abcnews.com/, the redirect was highly unusual in that it used JavaScript rather than a META redirect as in the aforementioned cases. We observed 173.230.142.200 return the following response:

```
<!DOCTYPE HTML>
<html>
<head>
<script type=”text/javascript”>
<!–
var iprequest = windows.location.hostname;
if( iprequest == “173.255.234.29”)
{
window.location = “http://www.abcnews.com”;
```

```
}
else
{
window.location = “http://www.google.com”;
}
//–>
</script>
</head>
<body>
</body>
</html>
```

The purpose of the script is to redirect a user who has typed the IP “173.255.234.29” into their web browser address bar to the website “http://www.abcnews.com”. A user who has reached this page by typing in any other address will instead be redirected to “http://www.google.com”. Note that there is a typo—“windows.location.hostname” should be “window.location.hostname”. The typo causes the script to be inoperative—i.e., the user sees a blank webpage in their browser. Interestingly, 173.255.234.29 returned a response identical to the above, except without the typo. Thus, a user who typed 173.255.234.29 into their browser was indeed correctly redirected to http://www.abcnews.com.

Click here for Appendix B: An interesting Rackspace-based server group.

ACKNOWLEDGEMENTS

The authors would like to thank David Fidler, Indiana University for helpful feedback.

FOOTNOTES

[1] http://hackingteam.it/index.php/customer-policy.
[2] https://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam.
[3] http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers.
[4] http://slate.me/1eSTeUF.
[5] https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/.
[6] “http://www.wired.com/threatlevel/2013/06/spy-tool-sold-to-governments/.
[7] https://www.eiu.com/public/topical_report.aspx?campaignid=DemocracyIndex12.
[8] https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.
[9] https://www.linode.com/tos.cfm .
[10] In all cases, the redirects were META redirects, or JavaScript redirects; both would only be evident in a web browser.
[11] e.g., in the Panama case mentioned in https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[12] http://www.finra.org/Newsroom/NewsReleases/2012/P191729.
[13] http://www.richmondbizsense.com/2013/03/13/local-reits-funds-under-sec-scrutiny/.
[14] http://www.finra.org/web/groups/industry/@ip/@enf/@ad/documents/industry/p123739.