Days after Hacking Team breach, nobody fired, no customers lost

Eric Rabe: "The company is certainly in operation. We have a lot of work to do."

by **Cyrus Farivar** - Jul 8, 2015 10:05am CEST

Hacking Team

Not one person has been fired at Hacking Team as a result of the significant breach of its servers on Sunday, according to Eric Rabe, a company spokesman.

"I don't know, I wouldn't anticipate that happening, but maybe if somebody was found to be negligent," he told Ars by phone early Wednesday morning from the company's headquarters in Milan, Italy, where he was summoned shortly after the epic hack.

FURTHER READING

HACKING TEAM LEAK RELEASES POTENT FLASH ODAY INTO THE WILD

Windows and Android phones may be affected by other leaked exploits.

A 400GB file, distributed via BitTorrent (and published here) reportedly includes not only various employee e-mails, but also source code, financial documents, and more. In recent years, Hacking Team sold its spyware—ostensibly to combat criminal activity—to various governments globally (including American federal law enforcement). The company has even presented to Swiss and Canadian authorities.

Rabe added that Hacking Team isn't going under any time soon.

"The company is certainly in operation. We have a lot of work to do," he said.

"[The hack] was a very sophisticated operation. This wasn't a lone hacker working in an upstairs bedroom. This is a much more sophisticated attack than that. Businesses are frequently the subject of such attacks like this, and sometimes they're successful."

Shockingly, he also claimed that Hacking Team has not suffered beyond utter embarrassment for the time being.

"I don't think we've lost any clients at this point. We're obviously talking to clients and trying to reassure them," he said, underscoring that Hacking Team has asked its clients to stop using its software.

"Because if it's not discoverable now, it will be soon. I think they completely understand why that's a reasonable request, but we don't know if every single customer has."

When asked if it was appropriate for a Hacking Team "Senior System and Security Engineer" who may have been the original vector for the attack to have a list of links to a pornographic website on his work computer, Rabe said emphatically no.

A file (NSFW) attributed to Christian Pozzi's desktop, whose laughably weak plaintext passwords (including his since-changed Gmail password: "Passw0rd!81") were exposed as part of the breach and whose Twitter account was hacked, contained a list of several porn-related links.

"Do I think that employees should have pornography on their work computer? I don't, and I don't think they should have it on their home computer either."

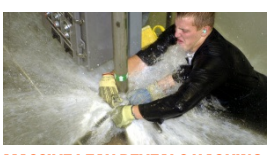
But, he added, "I have no idea what the circumstances are."

Selling to Sudan

One of the areas where Hacking Team has been roundly criticized is for selling to Sudan, a country with a notoriously poor human rights record. The African nation is also subject to a United Nations arms embargo, asset freeze, and travel ban.

"I'd like to be able to say more than I can on Sudan, but some of the reporting you've seen indicates they're no longer a customer," Rabe said.

FURTHER READING



MASSIVE LEAK REVEALS HACKING TEAM'S MOST PRIVATE MOMENTS IN MESSY DETAIL

Imagine "explaining the evilest technology on earth," company CEO joked last month.

"I came onto the company myself at the end of 2012 as the company began to mature, and there were serious public policies issues that they needed to deal with and that precipitated a review of who they were doing business with and whether they were places they felt good about."

But while Sudan may not have paid for services beyond 2012, it certainly made use of the Hacking Team Remote Control System through nearly all of 2014. Hacking Team even continued to provide training and other services, with limited success, according to The Intercept.

As that website reported on Tuesday:

> Internal records show that in 2012, Sudan's National Intelligence and Security Service in Khartoum paid 960,000 euros for Remote Control System. Emails confirm that Hacking Team cut off the account's service on November 24, 2014.
>
> During a training session for the Sudan intelligence service in January 2014, a Hacking Team engineer noted that none of the people attending the training "is enough prepared for the product usage. The main problem is the lack of basic computer usage, followed by a complete lack of English: 90% of them had problems just for typing a username on a keyboard and serious difficulties in moving the mouse."
>
> In November, Russo wrote that Sudan was "unofficially suspended, on-hold."

Rabe did not immediately respond to Ars' e-mailed followup questions regarding Sudan.

Trust us

Ars also asked about Hacking Team selling products and services to private companies, and not just law enforcement or government agencies—such as banks.

"I think that's a misunderstanding of the documents," Rabe said. "Years ago Hacking Team provided other services like security audits, and in those days some of those were provided to non-governmental organizations, but the surveillance tool was never sold to non-governmental organizations, and that remains the case."

FURTHER READING

DEA, US ARMY BOUGHT $1.2M WORTH OF HACKING TOOLS IN RECENT YEARS

Remote access malware either already has or will soon turn up in local cops' kits.

He explained that the company had a "panel that reviewed sales and looked at the human rights records and had veto power over the sale if they didn't think it was appropriate."

While Rabe did say this had happened, he would not say how many times.

"Obviously I'm not going to tell you that," he responded. "It's certainly within our right of who we want to do business with. When the Wassenaar Protocols took effect we felt that replaced the need for the panel. I'm not going to discuss it further. You're just going to have to take my word for it, I'm afraid."

Rabe argued that just as the United States and other Western countries routinely sell arms to allied countries like Saudi Arabia, so too should Hacking Team be able to sell its wares as well. After all, he pointed out, more than a dozen of the September 11 hijackers were from that country.

"Do you want Saudi Arabia to be able to track that sort of thing or would you rather have them be able to operate behind contemporary secrecy and the Internet?" he said.

"My point is not really to argue the various dangers of different kinds of equipment but just to say that if you're going to sell weaponry to a country, it's a little disingenuous to say that a crime-fighting tool is off-limits."

Rabe ended the call with a forceful defense of the company's entire business model, saying that there should be a controlled, appropriate way for governments and law enforcement to breach digital security.

"[CEO David Vincenzetti] started life in what we would call defensive security, to keep people out, and then he realized as more and more of the communications became inaccessible, that there was a need for a tool that gave investigators the opportunity to do surveillance. I don't think that's really that hard to understand, frankly. I don't think any of us are against cryptography, but what we're against is police being able to catch criminals and prevent crime, that's what we're worried about."

READER COMMENTS 20

Cyrus Farivar / Cyrus is the Senior Business Editor at Ars Technica, and is also a radio producer and author. His first book, *The Internet of Elsewhere*, was published in April 2011.
@cfarivar on Twitter

← OLDER STORY

LATEST FROM ARS TECHNICA/UK

MO' MONEY MO' PROBLEMS
PewDiePie responds to "haters" over £4.5 million YouTube earnings


BBC Micro:bit—a free single-board PC for every Year 7 kid in the UK


Europe's top tech news, June 2015


The UK National Videogame Arcade is the inspirational mecca that gaming needs


Police raid programmer who reported flaw in Argentinian e-voting system [Updated]

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)
Terminator-vision and the complex questions behind "augmented reality"
With info overlaid on our vision, "cool" doesn't equal "useful" or even "safe."

WATCH ARS VIDEO

Turn 10 Gets Technical with Ars
A world exclusive look at what's under the hood of Turn 10's new racing sim.

STAY IN THE KNOW WITH

LATEST NEWS

SUCH IS LIFE IN MOSCOW
In Russia, selfie takes you, prompts official "safety selfie" warning


Indonesian mud volcano probably human-triggered

BONE THROW
AT&T will give poor people 1.5Mbps DSL for $10 if US allows DirecTV merger

THE TRUTH IS IN HERE
New X-Files teaser trailer heralds 201 days to the new series

EVERYTHING IS AWESOME
Cloudy with a chance of Jedi: Han Solo movie set for May 2018

"SUPER AMERICAN"
American and Japanese mechs set to duel for supremacy

YOU MAY ALSO LIKE