
10:25 AM


10:25 AM

Hacking Team 2.0

株式会社カスペルスキー
情報セキュリティラボ
前田 典彦 | Norihiko Maeda

KASPERSKY lab

JAPAN SMARTPHONE SECURITY ASSOCIATION

日本スマートフォンセキュリティ協会（JSSEC）技術部会 マルウェア対策WG
2014年8月1日

SECURELIST

HackingTeam 2.0: The Story Goes Mobile

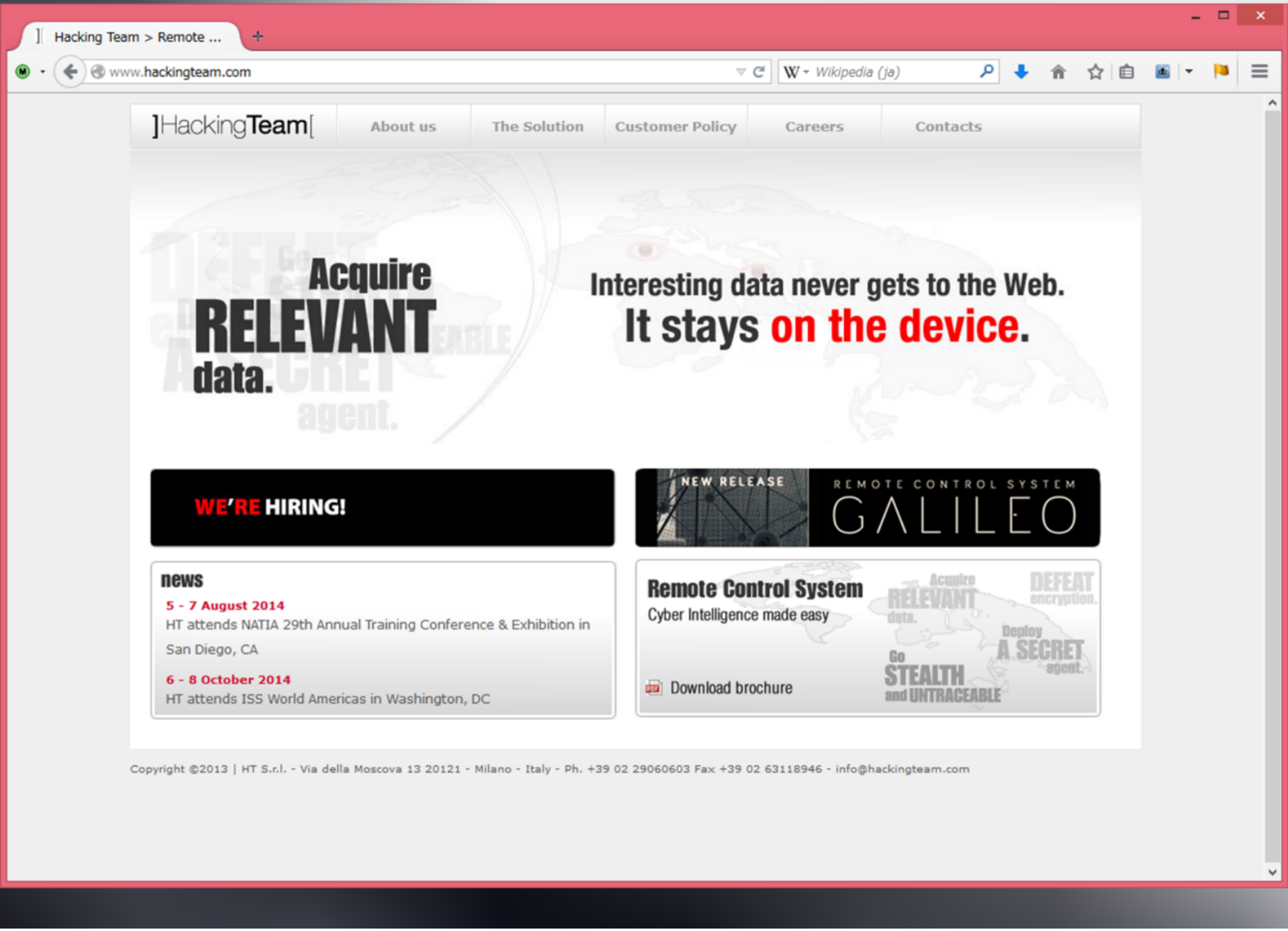
http://securelist.com/blog/mobile/63693/hackingteam-2-0-the-story-goes-mobile/

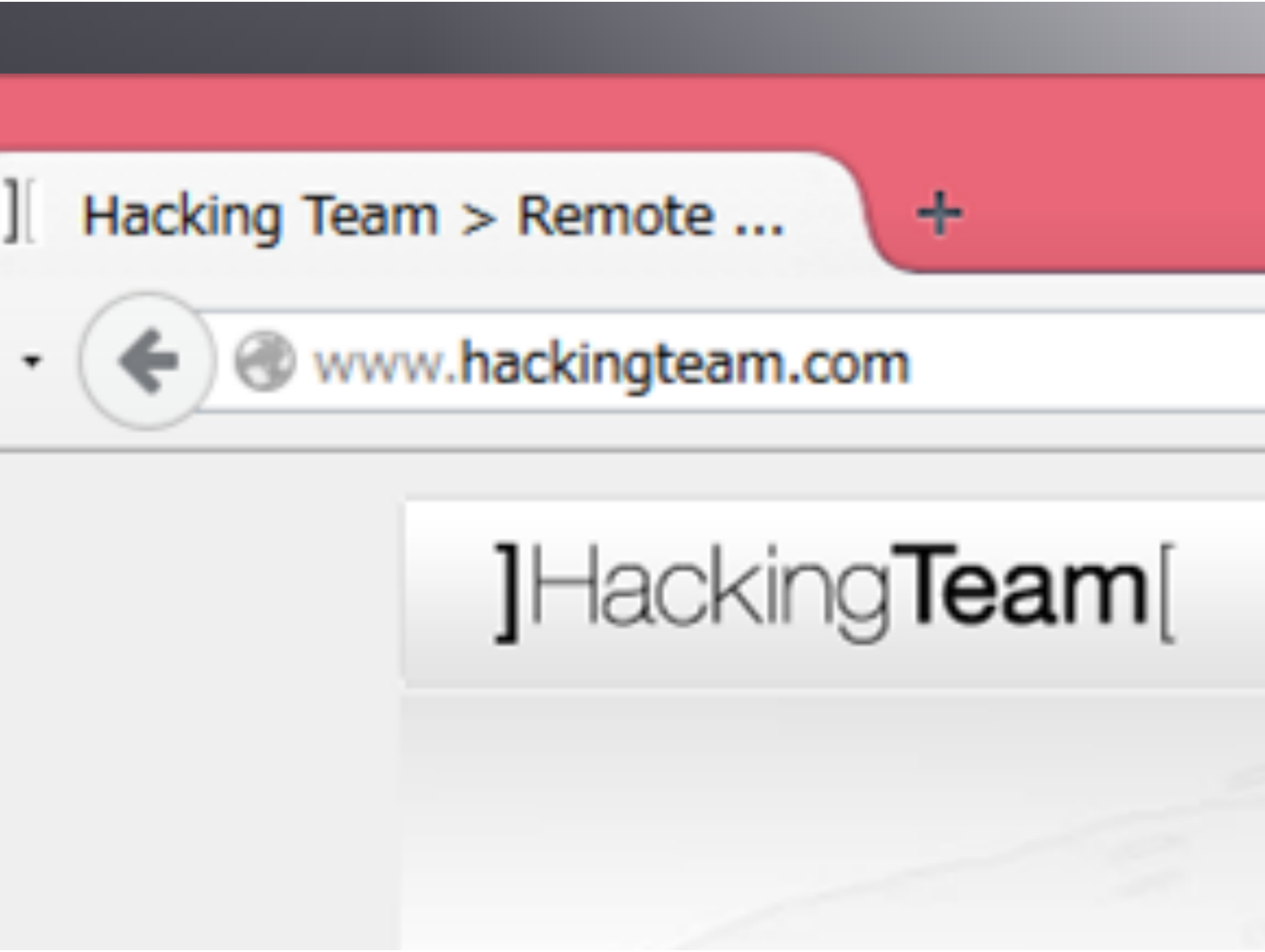
謝辞

Mr. Morgan Marquis-Boire from Citizen Lab,
Munk School of Global Affairs,
University of Toronto

MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO


Hacking Team > Remote ...
www.hackingteam.com
Wikipedia (ja)
]HackingTeam[
About us
The Solution
Customer Policy
Careers
Contacts
Acquire
RELEVANT
data.
Interesting data never gets to the Web.
It stays on the device.
WE'RE HIRING!
NEW RELEASE
REMOTE CONTROL SYSTEM
GALILEO
news
5 - 7 August 2014
HT attends NATIA 29th Annual Training Conference & Exhibition in San Diego, CA
6 - 8 October 2014
HT attends ISS World Americas in Washington, DC
Remote Control System
Cyber Intelligence made easy
Download brochure
Copyright ©2013 | HT S.r.l. - Via della Moscova 13 20121 - Milano - Italy - Ph. +39 02 29060603 Fax +39 02 63118946 - info@hackingteam.com


Hacking Team > Remote ...
www.hackingteam.com
]HackingTeam[

It stays on the device.

Remote Control System

Cyber Intelligence made easy

Acquire RELEVANT data.

DEFEAT encryption.

Deploy A SECRET agent.

Go STEALTH

Download brochure

Remote Control System Version9


REMOTE CONTROL SYSTEM
GALILEO
THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

Sergey k1k Golovanov
@k1k_

フォロー

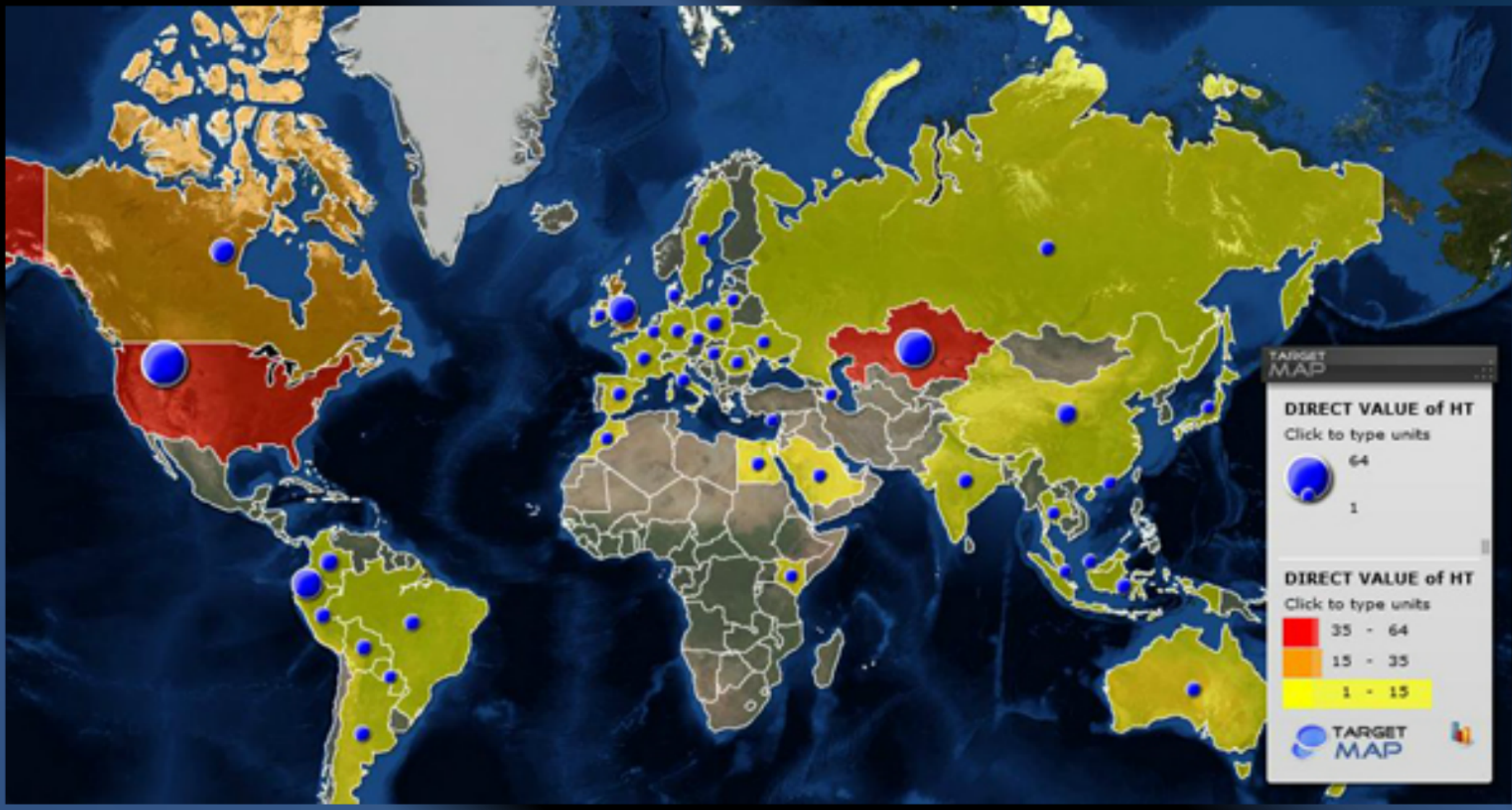
Updated #HackingTeam #RCS C2 #Map for today. Grand total: 326 C2s. pic.twitter.com/jKLOmpxvdn

返信 リツイート お気に入りに登録 その他

リツイート	お気に入り
10	4

12:29 - 2014年3月19日

画像/動画を報告する



http://securelist.com/blog/mobile/63693/hackingteam-2-0-the-story-goes-mobile/

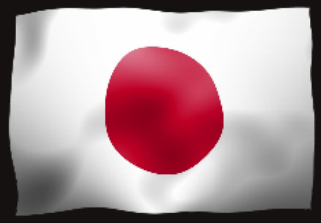
64	アメリカ合衆国
49	カザフスタン
35	エクアドル
32	イギリス
24	カナダ
15	中華人民共和国
12	コロンビア

7	ポーランド、ニュージーランド
6	ペルー、インドネシア、ブラジル、 アルゼンチン、ボリビア
5	ロシア連邦、インド
4	香港、オーストラリア
3	スペイン
2	サウジアラビア、マレーシア、イタリア、 ドイツ、フランス、エジプト

ウクライナ、タイ王国、スウェーデン、シンガポール、ルーマニア、パラグアイ、モロッコ、リトアニア、ケニア、日本、アイルランド、ハンガリー、デンマーク、チェコ、キプロス、ベルギー、アゼルバイジャン
(各1)

日本、

106.186.17.60



li528-60.members.linode.com

AS2516 KDDI CORPORATION

出典：Police Story: Hacking Team’s Government Surveillance Malware
https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/

誰が狙われたか？

RCS9の機能は？

- 通話記録
- メール
- 電話帳
- 保存データ・ファイル
- 位置情報
- IMの内容
- 録音

- 写真を撮る(フロントカメラ)
- クリップボードのデータ
- 訪問サイト履歴とcookie
- カレンダー
- 新しいSIM

マルウェアなの？

- Backdoor.Win32.Korablin
- Backdoor.Win64.Korablin
- Backdoor.Multi.Korablin
- Backdoor.AndroidOS.Criag

- Trojan.OSX.Morcut
- Trojan.Multi.Korablin
- Trojan.Win32.Agent

- Rootkit.Win32.Korablin
- Rootkit.Win64.Korablin
- Rootkit.OSX.Morcut

- Trojan-Spy.AndroidOS.Mekir

- Trojan-PSW.Win32.Agent

- Trojan-Dropper.Win32.Korablin

いつ？

どこで？

誰が？

感染に気付いたら？

JAPAN SMARTPHONE SECURITY ASSOCIATION

ありがとうございました。

株式会社カスペルスキー
前田 典彦
maeda@kaspersky.co.jp

KASPERSKY lab