

FREE SEMINARS: Join us in Amsterdam, Frankfurt, and London to learn the value of threat intelligence.

LEARN MORE



# Hacktivism: India vs. Pakistan

Posted by **RFSID** on February 11, 2016 in [Cyber Threat Intelligence](#)



Floodlit international border between India and Pakistan, as seen from the International Space Station.

When [India gained independence from Britain in 1947](#), a new, predominantly Muslim nation of Pakistan was created during what was called the “partition.”

During this partition, about [15 million people were displaced and a million more died](#) The “hastily drawn” border by the departing British, which separated Pakistan from the mostly Hindu India, never fully resolved all the issues.

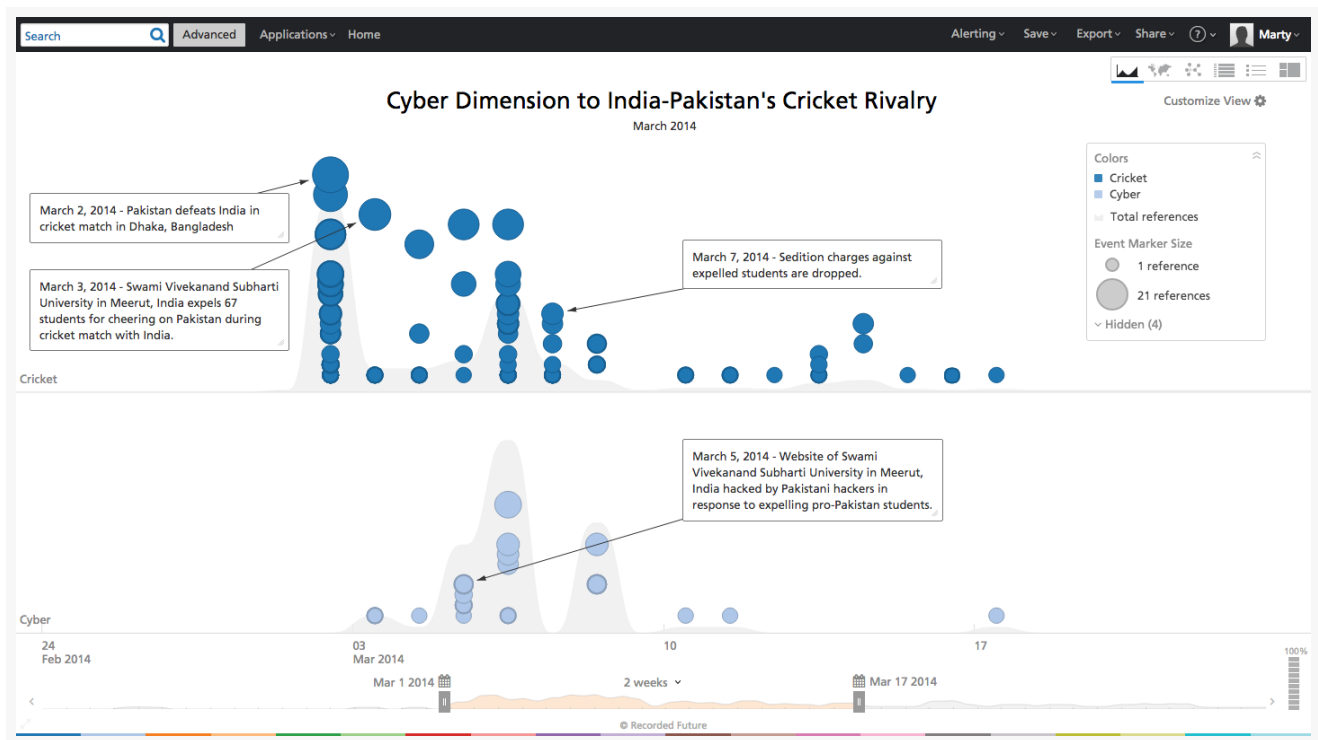
Several wars between the two nations ensued and tensions continue to this day. A floodlit,  1250-mile portion of the current international border (a.k.a. the Line of Control) is visible in a [photo taken from the International Space Station](#)



Indian soldiers (in present day Bangladesh) during the third war between India and Pakistan in December 1971.

The continuing rivalry between India and Pakistan has spilled over into cyberspace, very visibly with hacktivism. This post reviews that activity and demonstrates how high-profile  events and anniversaries (e.g., Indian Independence Day on August 15, Pakistan’s Independence Day on August 14, [the Mumbai attacks on November 26](#), and even cricket matches between the two countries) often coincide with increased cyber activity.

## The Cyber Dimension to India and Pakistan’s Cricket Rivalry



An India versus Pakistan cricket match, in March 14, results in an Indian university website being hacked.

The game of cricket provides a perfect field for a great rivalry between India and Pakistan. □ Wins and losses have geopolitical, social, and cyber repercussions on both sides. Conversely, geopolitical and social tensions have led to matches being postponed or cancelled.

On March 2, 2014, Pakistan defeated India in a cricket match in the Asia Cup held in Dhaka, Bangladesh. The next day (March 3), in Meerut, India, 67 Kashmiri students at Swami Vivekanand Subharti University were suspended for having cheered for Pakistan and distributing sweets after their win.

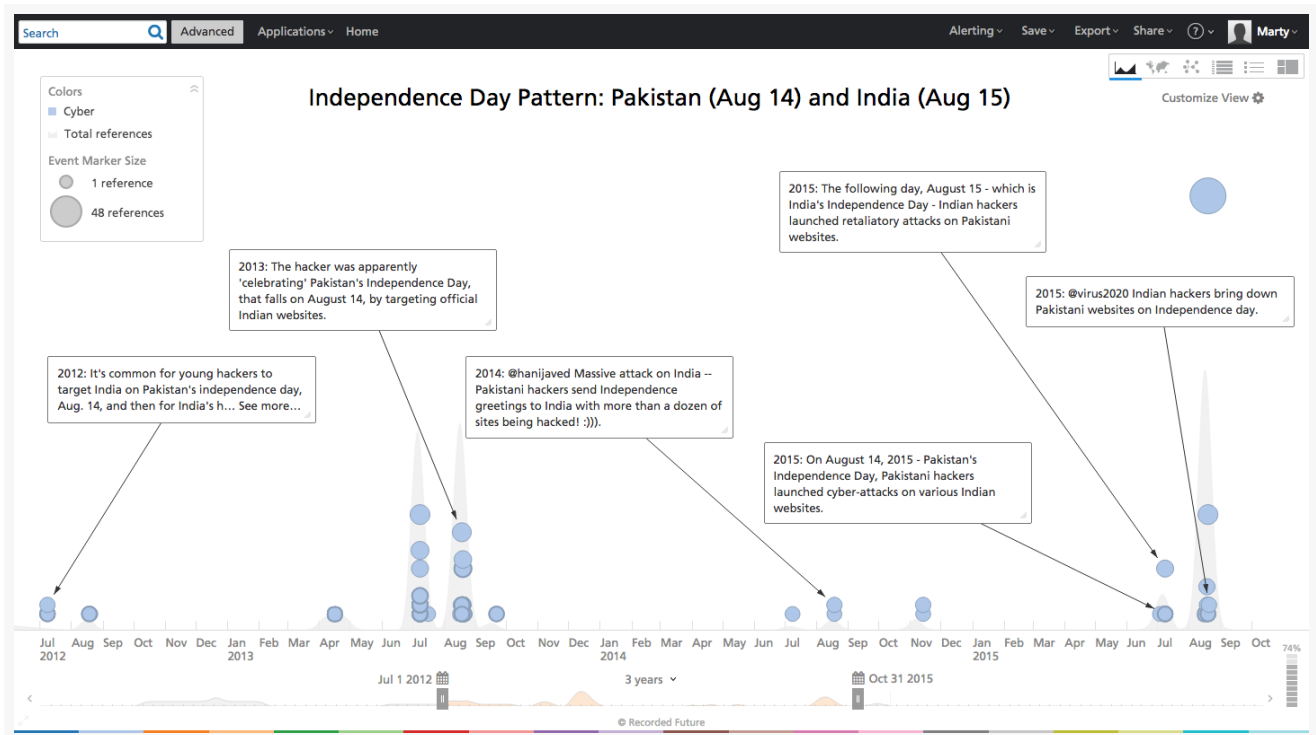
Then on March 5, 2014, the website of Swami Vivekanand Subharti University was hacked by a group claiming to be the Pakistan Cyber Army (a.k.a. Bangladesh Cyber Army) in response to expelling pro-Pakistan students.

Finally, on March 7, 2014 the sedition charges against expelled students are dropped but they could still face prosecution over the incident.

Based on this past event, it's likely that cyber activity will take place between Indian and Pakistani actors before, during, and after the next cricket match between India and Pakistan on [March 19](#) in Dharamsala, India.

## A Predictable Pattern on Independence Days

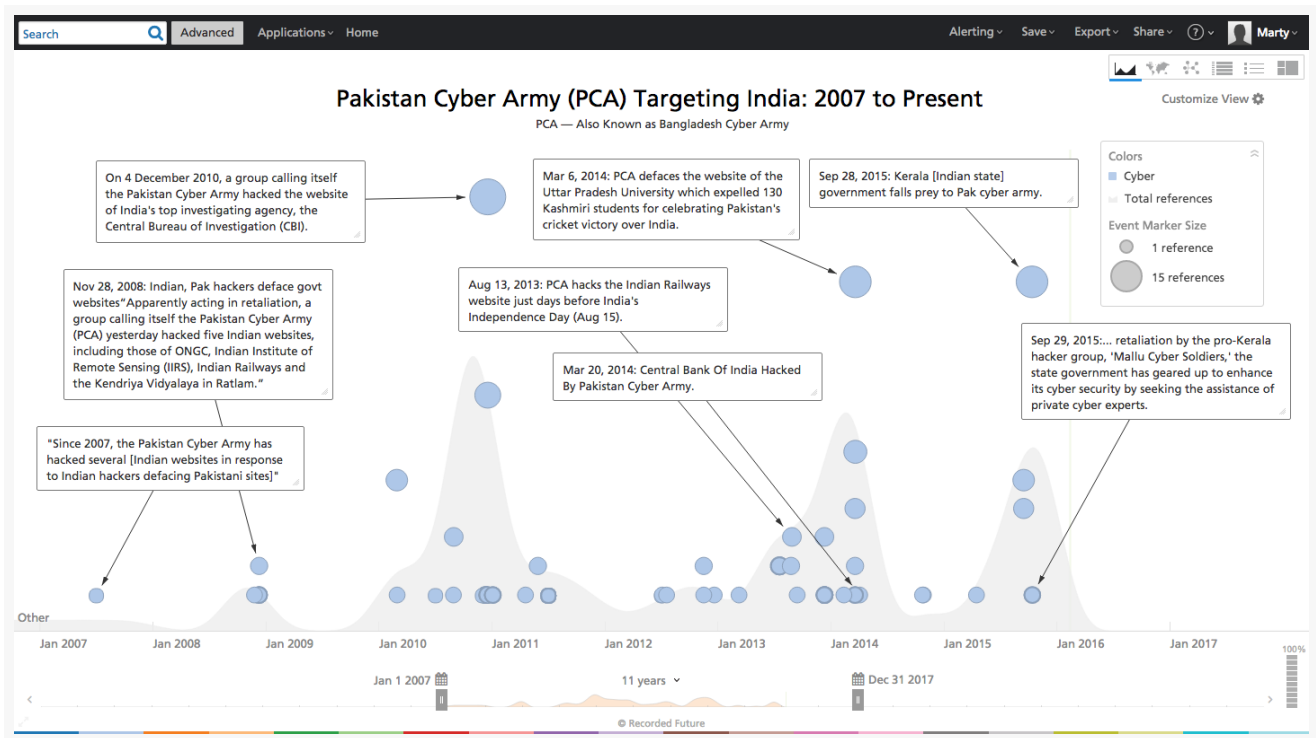
India and Pakistan's independence days, which fall on August 15 and August 14 respectively, create a predictable pattern (at least over the past three years) of attacks and retaliatory strikes by the opposing hacker groups, as shown in the timeline below. An uptick in such activity before and after this year's independence days shouldn't come as a surprise.



## Pakistan Cyber Army Targeting India: A Snapshot 2007 Onward

Let's take a closer look at the activities of the Pakistan Cyber Army (PCA), which was involved in the cricket incident described earlier.

The timeline below shows that the PCA has been consistently active at least since the 2007 hacking, defacing and shutting down high-profile Indian websites. Government and private sites have been targeted including Indian Oil and Natural Gas Corporation (a [Fortune 500 company](#)), Indian Railways, the Central Bureau of Investigation, Central Bank of India, and the State Government of Kerala.



The PCA's "public announcement" of its operations against India and the PCA's motives are described in a document on Pastebin as shown in the image below, conveniently cached in Recorded Future. This particular message is related to PCA's attacks to commemorate Pakistan's independence day (August 14).



## Cached Document





Title Untitled

Downloaded Jul 21, 2013, 07:11

Original URL <http://pastebin.com/Xc8wCgSf>

```
1. PUFFFF hahaha pakisthan skids :P LOL LOL ~team indishell
2. -----#####PAKISTAN ZINDABAD#####-----
3. #opindia
4. this is first public announcement for largest pakistan independence day operation. We are
5. legion of Pakistani and international independence warriors. we want the
6. hacker world, especially in ████████ India to know that warriors are
7. planning special Independence day (PAKISTAN ZINDABAD) party on india and
8. indian hackers.
9. this party will be for pakistan and kashmir independence. this will be largest pakistani cyber
   attack on indian hackers and industrys.
```

When we investigate the PCA's TTPs (tactics, techniques, and procedures) to learn how they operate, we find examples like tutorials on how to set up phishing attacks as shown in  this Facebook post. Though of course it's hard to establish, this is indeed a PCA actor who posted this:

 **pass.php mentioned**  
1 reference • 1 source • United States

---

**Hack Facebook With Phising**  
“So for this copy and paste this code in a notepad and save the file as pass.php.”

May 16, 2013, 16:06 • Facebook • Pakistan Cyber Army  
🚩 Flag for review • Save this reference to...  
<http://www.facebook.com/132973833534524/posts/173797306118843> • Show all events from this document



**Pakistan Cyber Army Official** published a note.  
May 16, 2013 · 🌟

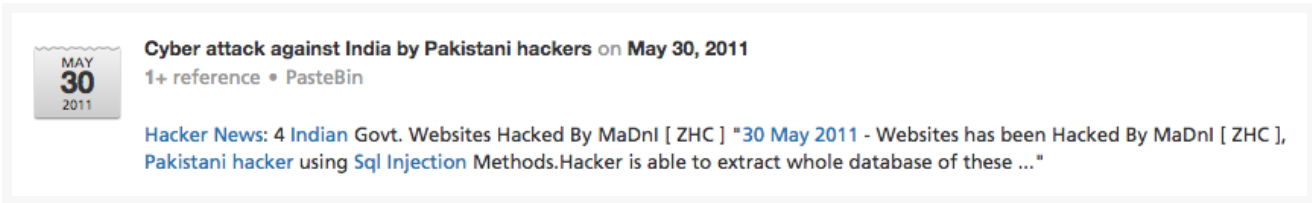
### Hack Facebook With Phising

// msf-armitage is here to guide u how to hack facebook on requests of fanzzz.....

Note :The trick/tutorial that I'm gonna show you today is just for educational purpose and I don't mean it to be used for illegal purposes.

How to hack a Facebook account?For facebook hacking,the most simple and easiest method is phishing and it works every time as long as your victim is not aware of it.So what is phishing? In simple words, Phishing is

Below is another example where SQL injection attacks are allegedly used by Pakistani hackers to compromise Indian websites.

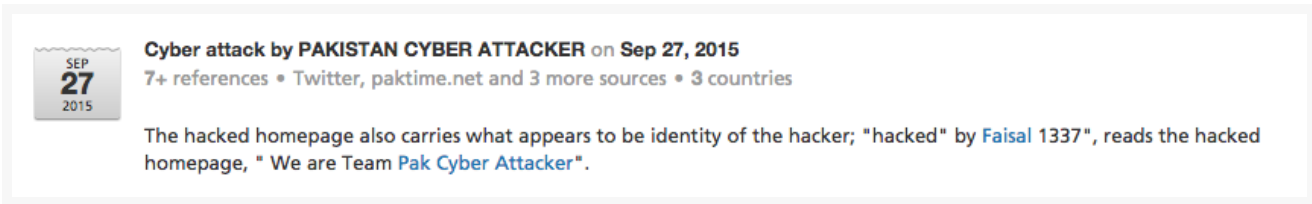


**Cyber attack against India by Pakistani hackers** on **May 30, 2011**  
1+ reference • PasteBin

**Hacker News:** 4 Indian Govt. Websites Hacked By MaDnI [ ZHC ] "30 May 2011 - Websites has been Hacked By MaDnI [ ZHC ], Pakistani hacker using Sql Injection Methods.Hacker is able to extract whole database of these ..."

In their research into PCA’s activities, [ThreatConnect](#) and [FireEye](#) also reported finding possible links to personas with skills in exploiting Web applications and services, identifying zero-day vulnerabilities, SQL injection, WEP cracking, and spear phishing.

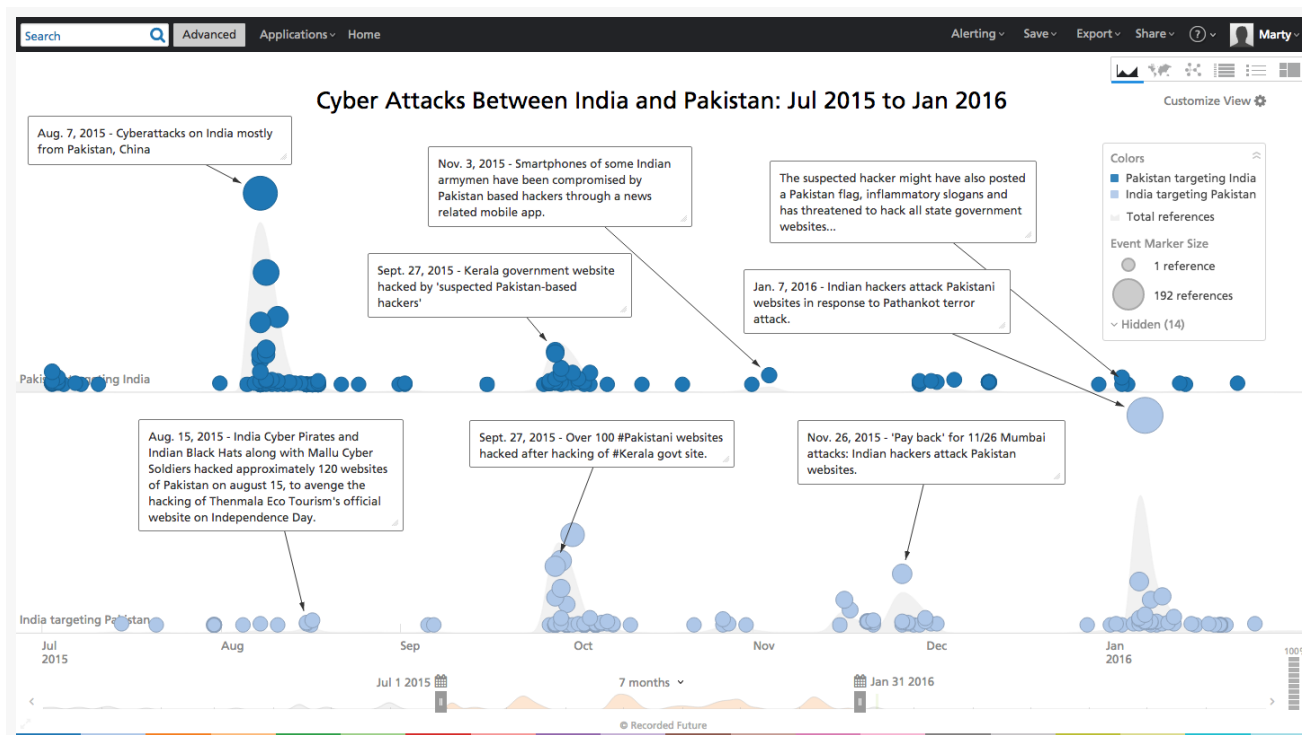
In some instances the hackers chose to identify themselves — for example, the hacker behind India’s Kerala state website defacement in September 2015 identified himself as “Faisal 1337” as shown in the image below.



**Cyber attack by PAKISTAN CYBER ATTACKER** on **Sep 27, 2015**  
7+ references • Twitter, paktime.net and 3 more sources • 3 countries

The hacked homepage also carries what appears to be identity of the hacker; "hacked" by [Faisal 1337](#)", reads the hacked homepage, " We are Team [Pak Cyber Attacker](#)".

If we widen our view again and look at hackers from Pakistan and India targeting each other over the last seven months, we can see an interesting retaliatory pattern of attacks; the latest major response being Indian hackers avenging the deadly [January 2, 2016 attack](#) on the Indian Air Force base in Pathankot.



There are a number of hacker groups in India including the Indian Black Hats who reportedly claimed responsibility for the January 7 (timeline image above) revenge for the attack on Pathankot, and the Mallu Cyber Soldiers who were said to avenge the attacks on the Kerala state government website.

When looking at hacking methods used by these groups, given that they go after weakly secured websites or those with unpatched vulnerabilities, one can expect to find generally applicable instructions and techniques used and shared by various groups, especially when they self-identify themselves under the broad umbrella of "India hackers." The methods used by these groups include SQL injection and PHP Web application hacks as shown by the mentions below.

JUL  
**17**  
2015

**Indian hackers, IMH, SQL and 1 more mentioned on Jul 17, 2015**  
 1+ reference • PasteBin

| Thanks : Darkc0de (SQL) , IHC , IMH ,and All INDIAN HACKERS |





```
10.
11. D3LT4 is a mutation of smartd0rk3r and can search for 10,446 google dorks and scans for SQL
    injection vulnerabilities.
12.
13.
14. #!/usr/bin/python
15.
16. import string, sys, time, urllib2, cookielib, re, random, threading,
17. socket, os, subprocess
18. from random import choice
19.
```


The Pastebin references mentions a tool “D3LT4” to scan websites for SQL injection vulnerabilities, and further references to PHP scripts which can be used to hack Web applications.

## Conclusion

The glimpses above hint at the many possible motivations and objectives of the cyber activities between India and Pakistan.

These could range all the way from loosely affiliated hacktivist groups avenging attacks by defacing symbols and institutions to more coordinated state-sponsored attacks, which will be covered in a future piece. The Line of Control (a.k.a. international border) between the two only serves as a symbol of adversarial tension and certainly not a barrier in the cyber realm.





**FREE**

TRENDING CYBER  
VULNERABILITIES  
**DELIVERED TO  
YOUR INBOX DAILY**

Sign up for the  
Recorded Future **Cyber Daily**  
and receive trending threat  
insights every day by email.

- Top Hackers**
- Top Exploits**
- Top Vulnerabilities**

**SUBSCRIBE**

OVER **7,000** SUBSCRIBERS

## Related Articles

---



Analyzing the Patch Timeline for Zero-Day Exploits



POS Malware Overview for the 2014 Holiday Shopping Season



The Russia-Ukraine Cyber Front Takes Shape



Mazar Android Bot: Threat or Not? Quick Threat Identification and Assessment Example□

**FREE**

**TRENDING  
CYBER VULNERABILITIES  
DELIVERED TO  
YOUR INBOX DAILY**

▼

**SUBSCRIBE**

OVER 7,000 SUBSCRIBERS

## Recent Blog Posts

---



### [Hactivism: India vs. Pakistan](#)

*By RFSID on February 11, 2016*



### [Threat Intelligence and SIEM \(Part 2\) — Understanding Threat Intelligence](#)

*By Guillaume Dupont on February 9, 2016*



### [Improve Your Threat Intelligence Strategy With These Ideas](#)

*By Pete Hugh on February 2, 2016*



### [How to Avoid the Common Pitfalls While Browsing the Web](#)

*By Amanda on January 28, 2016*



### [7 Habits of Smart Threat Intelligence Analysts](#)

*By Amanda on January 26, 2016*

Search our blog...



## SUBSCRIBE TO OUR BLOG

Join over 14,000 intelligence analysts and security professionals who receive free Recorded Future content as soon as it's published.



GET EMAIL UPDATES



# See Recorded Future's threat intelligence in action.

REQUEST DEMO >

## R E C E N T B L O G P O S T S

Hactivism: India vs. Pakistan

---

Threat Intelligence and SIEM (Part 2) — Understanding Threat Intelligence

---

Improve Your Threat Intelligence Strategy With These Ideas

---

How to Avoid the Common Pitfalls While Browsing the Web

## @ R E C O R D E D F U T U R E

Nice example of how threat intelligence from Recorded Future can help you proactively identify new malware: <https://t.co/pVGevO6hSp> #DarkWeb

---

RT @peterkruse: @RecordedFuture this is what you mentioned on your blog in November being deployed in live attacks! <https://t.co/AMD7lrEauq>

---

Does your #threatintel team fit your enterprise needs? Watch our webinar featuring [@levigundert](#) to find out: <https://t.co/CELGBs2b6A>

## R E C E N T P R E S S

Big Data Firm Says It Can Link Snowden Data To Changed Terrorist Behavior

---

Snowden Is The Kind of Guy I Used to Recruit — in Russia

---

Report: Al Qaeda Tries New Encryption Post-Snowden Leaks

---

Intel Firm Links Ukraine Energy Debt With Potential Cyber Assault

C O M P A N Y

- [About](#) >
- [Contact](#) >
- [Press](#) >
- [Events](#) >
- [Services](#) >

P R O D U C T S

- [Cyber Threat Intelligence](#) >
- [Corporate Security](#) >
- [Competitive Intelligence](#) >
- [Defense Intelligence](#) >
- [Web Intelligence Platform](#) >

C U S T O M E R S

- [Login](#) >
- [Support Center](#) >
- [Software Status](#) >
- [Source Suggestion](#) >
- [Developer Code](#) >

Copyright © 2016 Recorded Future, Inc.

[Privacy Policy](#) [Terms of Use](#) [API Terms of Use](#) [Jobs](#)

