Security awareness for the security

and don’tCry any more

Kir Ermakov

Jet Security Conference, 2017

#:whoami

- Known as ‘**isox**’
- **vulners.com** founder
- QIWI Group CTO (prev. – CISO)
- Web penetration tester
- Member of “hall-of-fames” (Yandex, Mail.ru, Apple and so on)
- JBFC community participant
- Security skeptic

Information security awareness is an evolving part of information security that focuses on raising consciousness regarding potential risks of the rapidly evolving forms of information and the rapidly evolving threats to that information which target human behavior.

© Wiki

Service for the regular employees

- All kind of trainings for non-security guys
- Speeches of security preachers
- Mandatory part of many standards and laws (PCI, SOX, ISO27k, US)
- The challenge of measurement in pentest practice

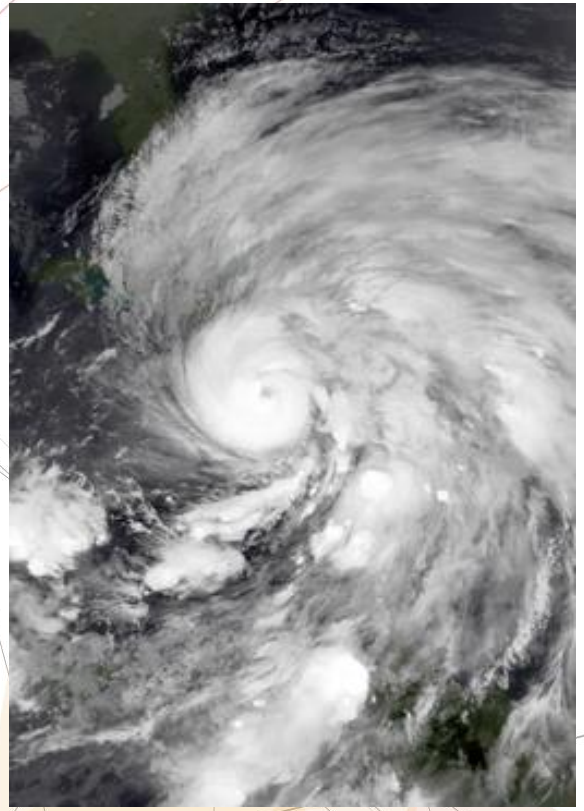
You are a human too!

- Lack of information is **unforgivable**
- But who will support **you**?!
- How not to **skip** the threat?
- Unawareness is also a **human error**!

Threats drag race

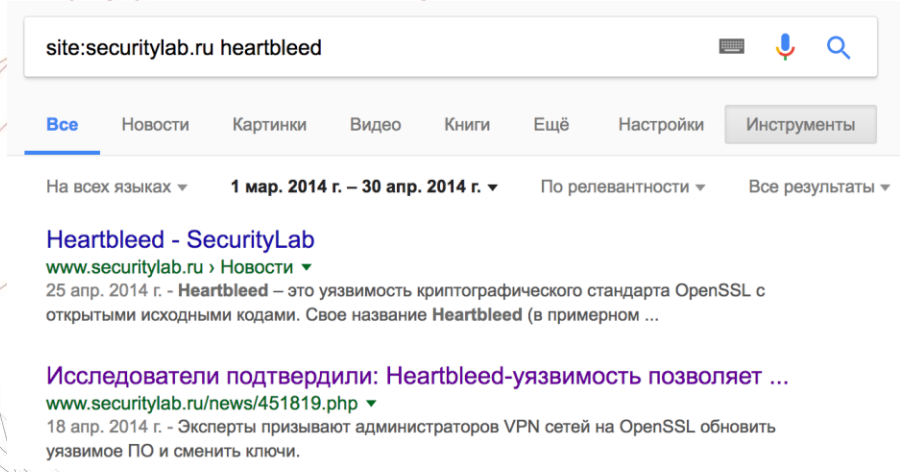
- Modern threat is like a race car
- The one who slows will die
- Information is the main treasure
- The reaction rate will determine the winner

Hurricane Sandy

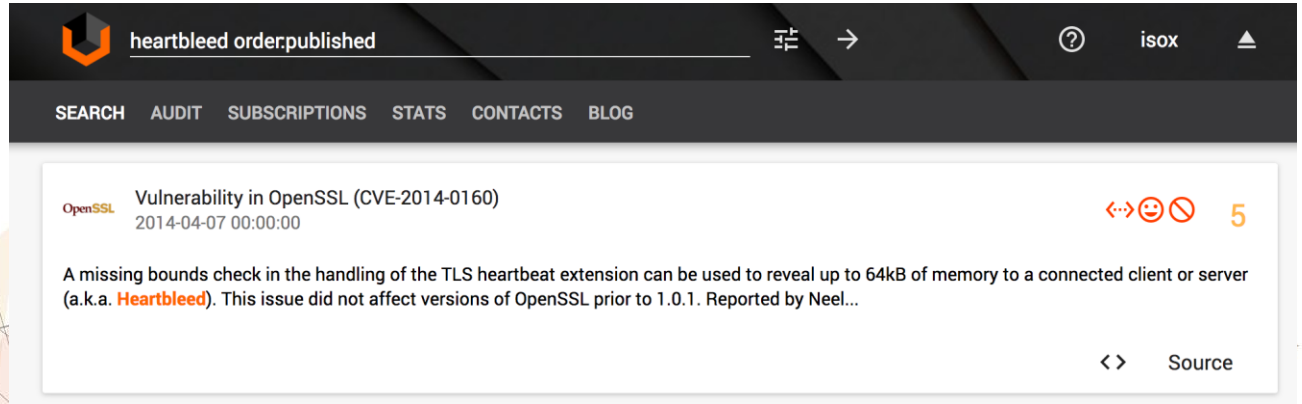


- Disaster as we know it
- Immediate news resources reaction
- High-speed information dissemination
- Remediation and recovery plans

Heartbleed



11 days delay vs the most popular Russian infosec news resource



20:35, 12 мая 2017

Вирус-вымогатель заразил компьютеры по всему миру и добрался до МВД России

Добавить в «Мою Ленту»

Фото: @dabazdyrev

wannaCry

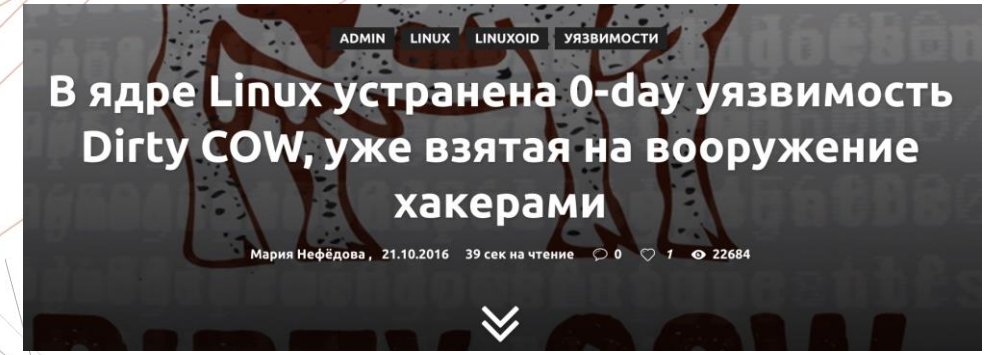
12 hours delay vs Lenta.ru, a major news portal

THN WannaCry Ransomware That's Hitting World Right Now Uses NSA Windows Exploit
2017-05-12 08:22:00

ID THN:388894CFE5A1D90889BA3B0B12225427
Type thn
Reporter Swati Khandelwal
Modified 2017-05-16 08:25:59

Description

Dirty COW



1 day delay vs xakep.ru, a Russian security magazine and news resource

THN

Dirty COW — Critical Linux Kernel Flaw Being Exploited in the Wild
2016-10-20 23:02:00

7.2

ID THN:CE61C12EE00ABEC1457F5F03F53AE6AD
Type thn
Reporter Swati Khandelwal
Modified 2016-10-25 15:07:13

Threats are new disasters

- React them as if it is an earthquake
- Be informed!
- Keep your eyes on the security news
- This is the dark side of the security awareness

Gathering information

- **Vendor critical advisories subscriptions**
- **Sec Lists** [http://seclists.org/]
- **The Hacker News** [http://thehackernews.com/]
- **Netsec Reddit** [https://www.reddit.com/r/netsec/]
- …

Automate it with Vulners database!

Vulnerability Assessment Subscriptions

Receive daily news

Scenarios of 0-day vulnerabilities repeat day by day, year from year.
Some of them appear so fast that users can't patch them before hackers come with fresh exploits

Knowleges is a power! Be first who receives news about new vulnerability as soon as it appears!

Heart Bleed
CVE-2014-0160

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets...

Shell Shock
CVE-2014-6271

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables which allows remote...

Dirty COW
CVE-2016-5195

Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows users to gain privileges by leveraging incorrect handling...

Security awareness for security guys

- Be the first to know about
- Inspired by Google Search subscriptions
- Get only content that you need
- Query based subscription
- Any delivery method:
  - RSS
  - Email
  - Telegram
  - API

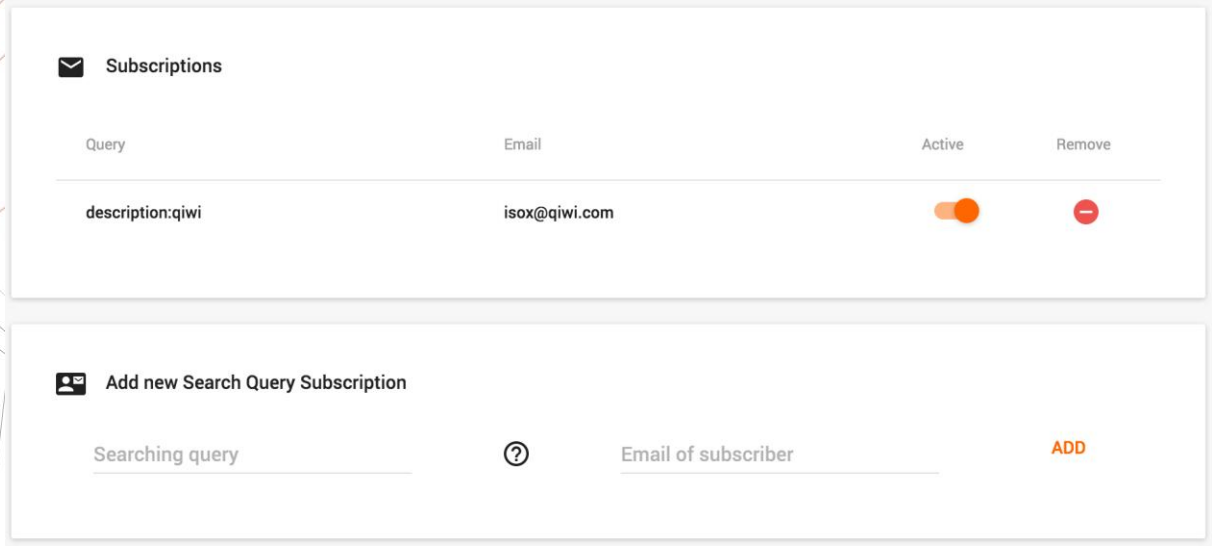
Advanced queries

- Any complex query
  - *title:**httpd** type:**centos** order:**published** last 15 days*
- Sortable by any field (type, CVSS, dates, reporter, etc)
- Apache Lucene syntax (AND, OR and so on)
- Exploit search by sources and CVE’s
  - *cvelist:CVE-2014-0160 type:exploitdb*
  - *sourceData:**.bash_profile***
  - *sourceData:"magic bytes”*

RSS

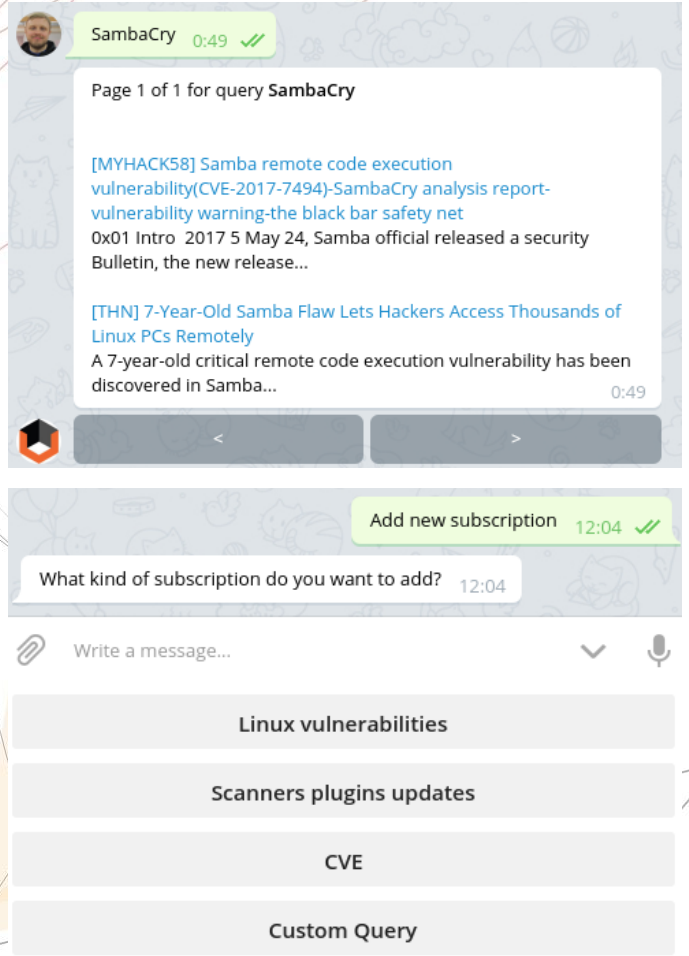
- Fully customizable news feed in RSS format
- Powered by Apache Lucene query
  - *https://vulners.com/rss.xml?query=type:debian*
- Updates-on-demand. No cache, it builds right when you ask it to.
- Atom, Webfeeds, mrss compatible

Email subscriptions



- Awareness service
- Absolutely customizable

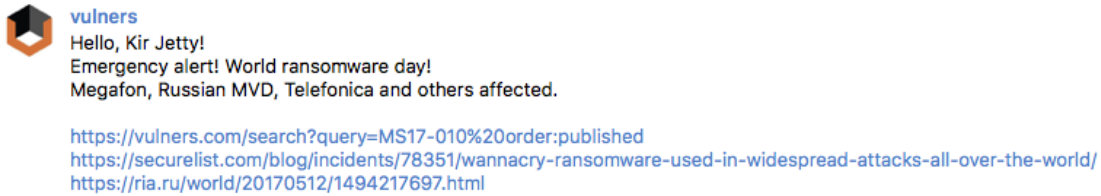
Telegram - @vulnersBot

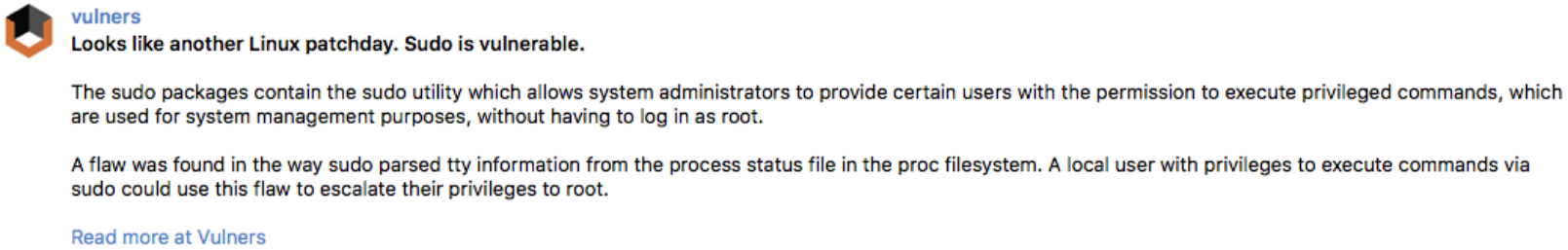


- Unlimited subscriptions for a user
- Rapid news and digests
- In-app search
- Broadcasts for emergency news

QIWI Emergency News

- Security disaster broadcast
- Choice of analysts
- Prepared for you by QIWI team





Thanks

- isox@vulners.com
- https://github.com/videns/vulners-scanner/
- We are really trying to make this world better
- **Stop paying for features, that are available for free**