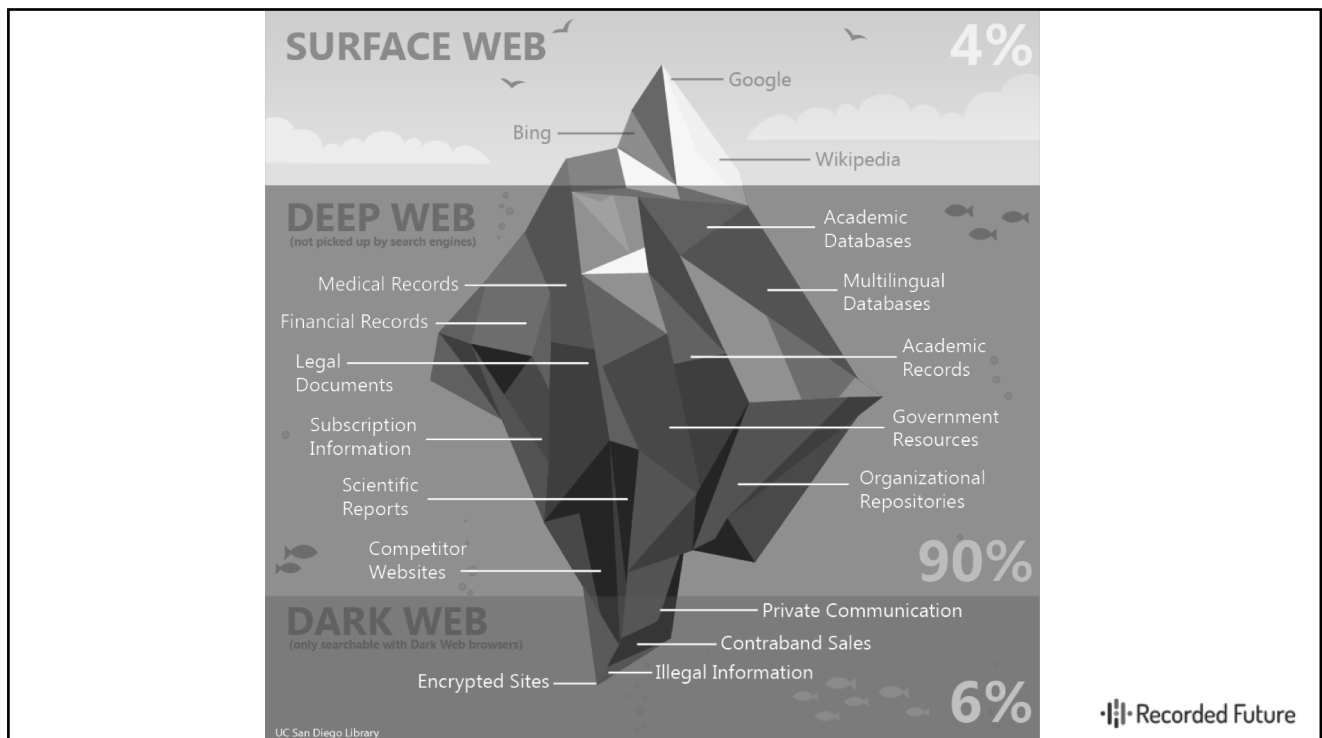
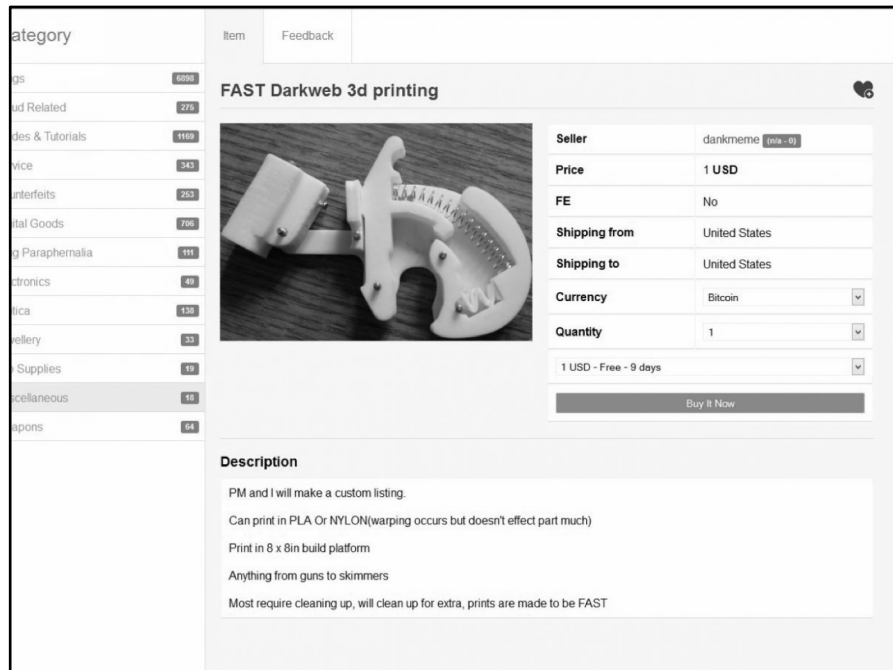
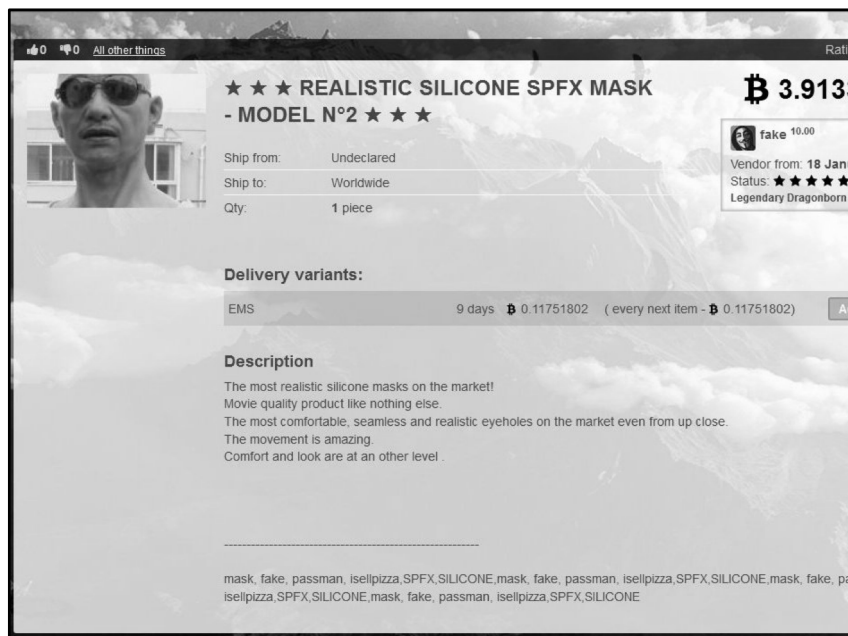


# The Dark Web's Deep Threat Intelligence Secrets

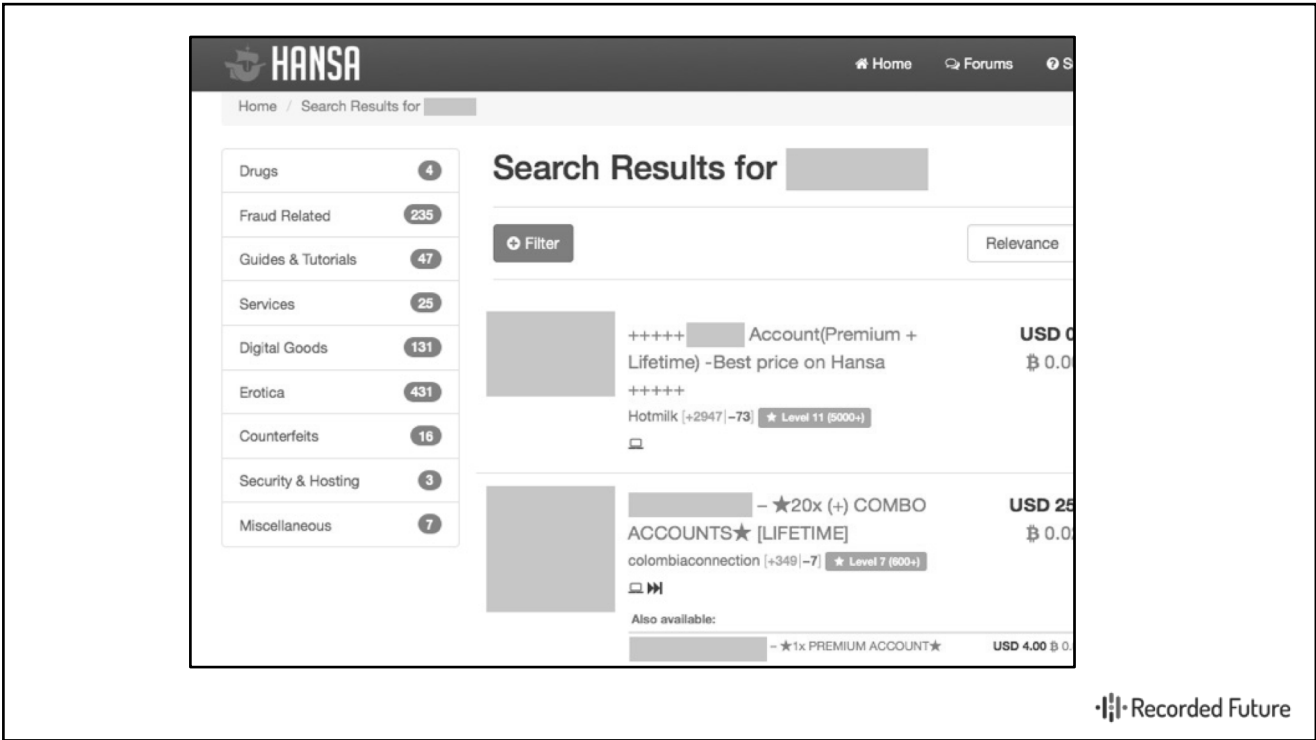








Recorded Future



Recorded Future



HOME ABOUT SHIPPING/PRICES CONTACT/ORDER FEEDBACK


We are offering top quality cards:


All our cards come with PINs and instructions. You can use them at any ATM worldwide.  
Our cards are equiped with magnetic strip and chip.  
Once you purchase, we will email you a Full Guide on how to safely cash out.


Us cards - available balance \$2,500( minimum) and up to \$5,000.  
usage:  
✓ ATM  
✓ Stores  
✓ Online

Eu cards - available balance 2,500 Euro(minimum) and up to 4,500 Euro.  
usage:  
✓ ATM  
✓ Stores

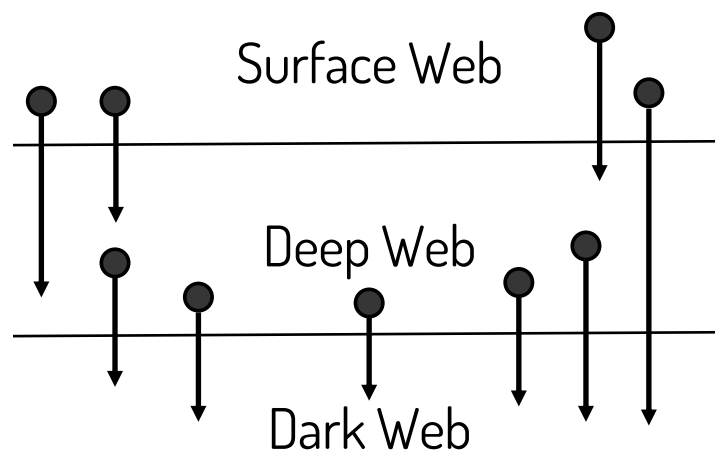
Payment methods we accept:



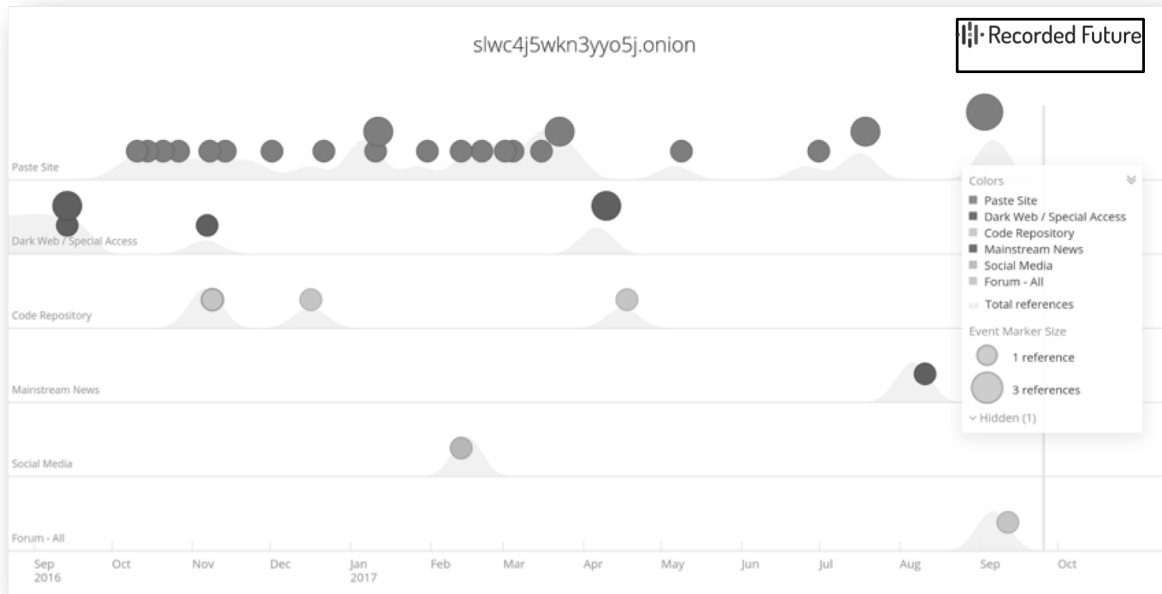




Recorded Future



Recorded Future



Recorded Future

Cached Document

Title onion links  
 Author Ramanusasango  
 Downloaded Jan 10, 2017, 11:18  
 Original URL <https://nopaste.me/view/f8d81b23>

```

25. Mobile Store: http://mob11/rab6nui/vx.onion/
26. PC Shop: http://matrixtxri745dfw.onion
27. Creditcards: http://tgssx32xnahbto7b.onion
28. UK Passports: http://vfqnd6mieccgyiit.onion/
29. US Fake ID Store: http://en35tuzqmn4lofbk.onion/
30. USA Citizenship: http://xfnwyig7olypdq5r.onion/
31. Onion Identity Services: http://abbujjh5vqtq77wg.onion/
32. EuroGuns: http://2kka4f23pcxgqkpv.onion/
33. :::Drugs:::
34. Drug Market: http://4yjes6zfucnh7vcj.onion/
35. Kamagra for BitCoins: http://k4btcoezc5tlxyaf.onion/
36. EuCanna: http://rso4hutlefirefgp.onion/
37. Peoples Drug Store: http://newpdsuslmzqazvr.onion
38. Smokeables: http://smoker32pk4qt3mx.onion/
39. CannabisUK: http://fzqnrlcvhkgbdwx5.onion/
40. DeDope: http://kbvvh4kdddiha2ht.onion/
41. BitPharma: http://s5q54hfw56ov2xc.onion/
42. Brainmagic: http://1l61ardicrvrljvq.onion/
43. NLGrowers: http://25ffhnaechrbzwf3.onion/
44. :::Hosting:::
  
```

Recorded Future

## USE CASE 1

Are you being talked  
about on Dark Web?



Only amateurs attack machines;  
professionals target people

Bruce Schneier



## TMOBILE INSIDER mentioned

FEB  
18  
2019

TMOBILE INSIDER

"HAVE TMOBILE INSIDER ONLY WANTS TO DEAL WITH EXISTING ACCOUNTS SOMEONE POINT" Forum Thread

Source Omerta Carder Forum New Posts by the\_professor on Feb 18, 2019, 15:09

[https://Omerta%20Carder%20Forum%20New%20Posts%20\(Obfuscated\)/showpost.php?p=356486&postcount=2](https://Omerta%20Carder%20Forum%20New%20Posts%20(Obfuscated)/showpost.php?p=356486&postcount=2) • Reference Actions • 2+ references

## Amazon Refund Methods + Insider Knowledge [HUGE] mentioned

FEB  
10  
2019

Amazon Refund Methods + Insider Knowledge [HUGE]

"Amazon refund methods + insider knowledge [HUGE]" Forum Thread

Source Sinisterly Forum by theult on Feb 10, 2019, 15:53

[https://Sinisterly%20Forum%20\(Obfuscated\)/Thread-Amazon-Refund-Methods-Insider-Knowledge-HUGE?pid=859662#pid859662](https://Sinisterly%20Forum%20(Obfuscated)/Thread-Amazon-Refund-Methods-Insider-Knowledge-HUGE?pid=859662#pid859662) • Reference Actions • 1+ reference

## Any interests in identity swaps? and Department of Motor Vehicles mentioned

FEB  
6  
2019

Any interests in identity swaps?

"&gt;&gt; brother by any chance do you have any DMV insider/plugin?" Forum Thread

Source Empire Market Forum by GotFraud on Feb 6, 2019, 18:24

<http://empforumgftfqng.onion/index.php?threads/any-interests-in-identity-swaps.4365/#post-26555> • Reference Actions • 1+ reference

DR4NK

Posted in 0day Forum

Posts in thread 1

First posting Feb 08 2019, 17:28

Most recent posting Feb 08 2019, 17:28

[Previous 50](#) [Next 50](#)

[malware] I'll share here some hacked Accounts with money. Cracked Software Crypters/Silent Crypto Miners. RATTED Users. SQL Dumps. Your knowledge and skills? I worked before as a Software Engineer, today I'm a Cyber Security Expert working for companies to secure them. My knowledge: C++ (great) Python (great) NET (great) JAVA (good)

Post 1 of 1 by DR4NK on Feb 08 2019, 17:28

Online anonymous crypting service, C/Assembly, \$20/crypt

Posted in 0day Forum

Posts in thread 27

First posting Mar 13 2017, 21:38

Most recent posting Feb 25 2019, 20:37

[Previous 50](#) [Next 50](#)

ture as a cross russian-english forum and all the

Post 24 of 27 by bl00d on Feb 17 2019, 00:00

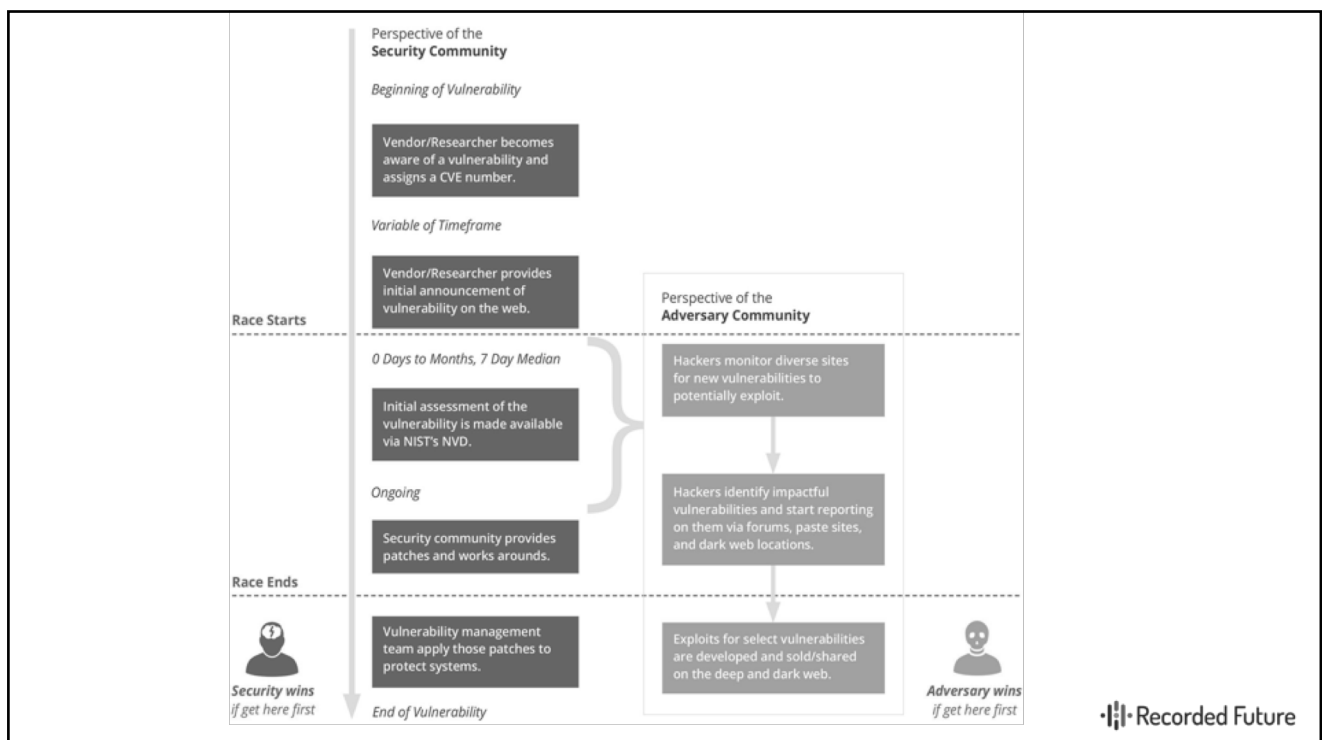
Hello everyone. Looking for serious hackers to hack a bank. I have an inside man for any onsite malware injection. Serious money to be made. Trust will have to be established to ensure everyone gets his cut. Hit me up at [popeak47@jabber.at](mailto:popeak47@jabber.at)

Post 25 of 27 by popeak47 on Feb 17 2019, 00:00

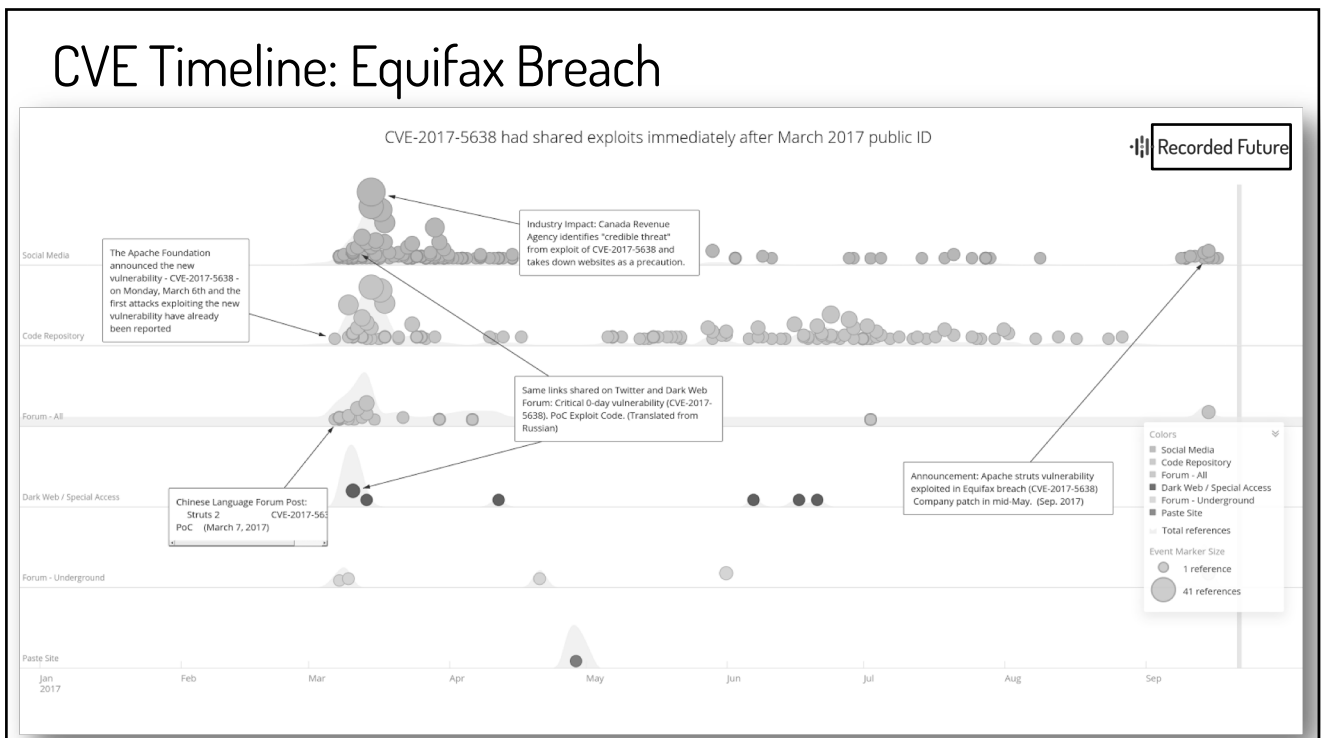
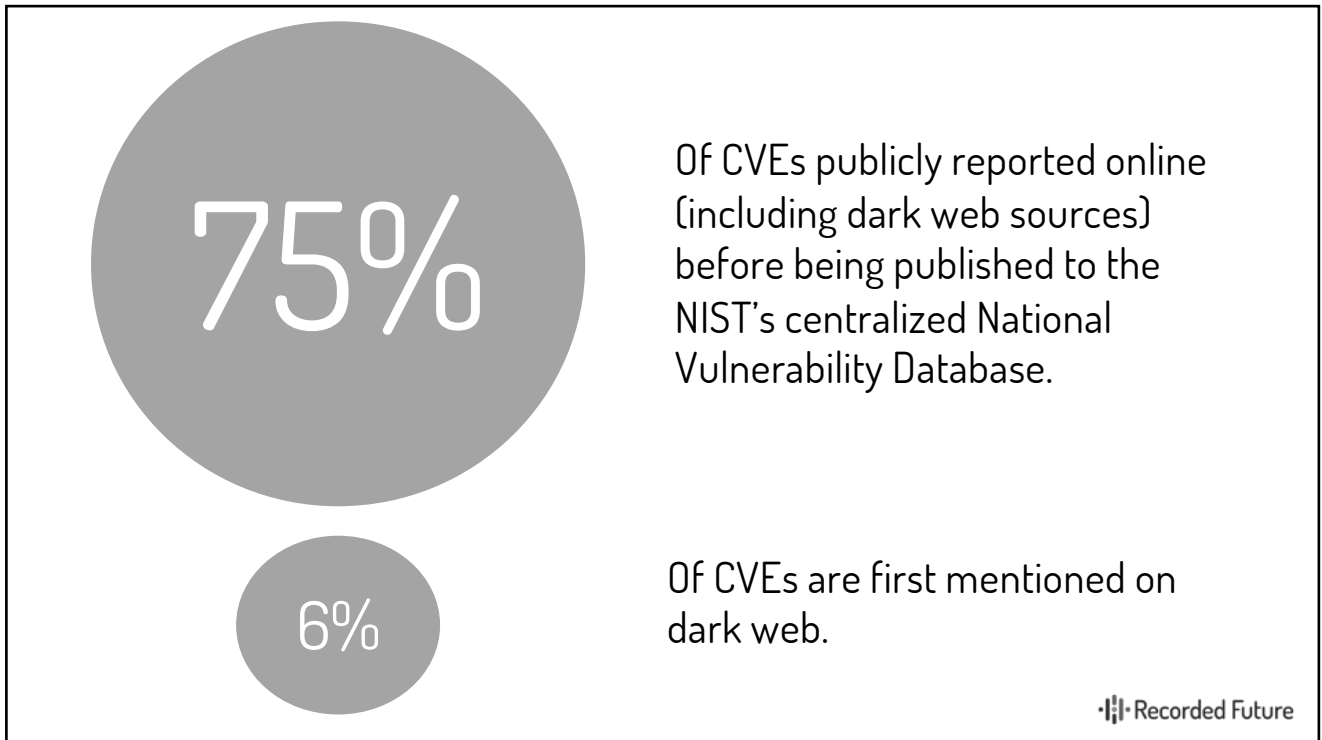


## USE CASE 2

What vulnerabilities should you patch?







## CVE-2017-5638 – Vulnerability in CVE

## 3 Threat Research Notes

1 000+ References to This Entity

First Reference Collected on Mar 7, 2017

Latest Reference Collected on Oct 16, 2017

★ Curated Entity

Show recent cyber events involving CVE-2017-5638 in Table | v

Show all events involving CVE-2017-5638 in Table | v

89  
of 100

Critical

Risk Score 89

12 of 18 Risk Rules Triggered

Recorded Future

Recorded Future

## Triggered Risk Rules

**NIST Severity: Critical** • 1 sighting on 1 source  
National Common Vulnerabilities and Exposures (CVE) Database.

**Historically Linked to Exploit Kit** • 9 sightings on 6 sources including  
Facebook, @NWsecure, @jddf, Vulners Vulnerability Database, @Nue\_Dev. 1 related malware: JexBoss. Most recent tweet: 例のアレ関連のwiki見てたら引っかけたし調べたらCVE-2017-5638使ってる臭い Jexboss+metasploitの組み合わせ。Most recent link (Jun 12, 2017): [https://twitter.com/alice\\_r1pper/statuses/874118155571937281](https://twitter.com/alice_r1pper/statuses/874118155571937281)

**Historically Linked to Ransomware** • 107 sightings on 74 sources including  
@stevemcgregory, @ccasel, blog\_trendmicro\_co\_jp, @DrOzdag, Threat Intelligence on Medium. 1 related malware: Cerber. Most recent tweet: Delivering #ransomware via Apache Struts CVE-2017-5638 <https://t.co/W4Jl9kofIS> #ixiacom @ixia\_ATI #Cerber <https://t.co/0CX4EbT3Go>. Most recent link (Apr 17, 2017): <https://twitter.com/GabeLuis/statuses/854045567525289984>

**Historically Linked to Remote Access Trojan** • 2 sightings on 2 sources  
Trend Micro, Hackbusters. 2 related malwares: Adwind, Proton RAT. Most recent link (Jul 11, 2017): <http://blog.trendmicro.com/trendlabs-security-intelligence/spam-remote-access-trojan-adwind-jrat/>

**Recently Linked to Malware** • 4 sightings on 4 sources  
@TheM4rksman, @PaladionN, @FLCyberSec, Netsparker, Web Application Security Scanner. 2 related malwares: Ransomware, OGNL Expression Injection. Most recent tweet: Apache Struts OGNL Expression Injection (CVE-2017-5638) posted by FrontlineCyberSec on @AlienVault OTX: <https://t.co/QF1zPU0iPp>. Most recent link (Oct 16, 2017): <https://twitter.com/FLCyberSec/statuses/919851295250448385>

**Historically Linked to Malware** • 140 sightings on 115 sources including  
@securityinsight, @garynewe, @knoknokcom, KitPloit - PenTest Tools for your Security Arsenal, Facebook. 18 related malwares including Infostealer, Ransomware, Backdoor, Banking Trojan, OGNL Expression Injection. Most recent tweet: Delivering

Recorded Future

## WebShell Cyber attack

白帽说：一句话就让你流产

AUG  
16  
2017

“通常网站会使用http协议与浏览器进行交互，客户端通过发送GET或者POST请求向服务器提交数据，webshell正是基于http协议的这两种数据请求方式，向服务器发送我们需要执行的shell指令，进而达到我们的目的。” Forum Thread

Translate

Source Ichunqiu Forum by 屌丝绅士 on Aug 16, 2017, 21:11

[https://bbs.ichunqiu.com/forum.php?](https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=260688&fromuid=227825)[mod=viewthread&tid=260688&fromuid=227825](https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=260688&fromuid=227825) • 8+ references

See references

Add as Annotation

Add Reference to List...

Share Event

Request Data Review

Hide This Event

Retry Translation

Who is reported together with WebShell?

What attackers are using WebShell?

Who is targeted using WebShell?

What operations are reported with WebShell?

What technical indicators are related to WebShell?

Which authors are reporting about WebShell?

Recorded Future

SEP  
7  
2018

إختراق الأجهزة وسحب باسوردات الفيسبوك و جيميل SpyGate-RAT v 3.3 النسخة الألمانية  
"إختراق الأجهزة وسحب باسوردات الفيسبوك و جيميل SpyGate-RAT v 3.3 النسخة الألمانية" Forum Thread  
Translate

Source Aljyyosh by zazloz on Sep 7, 2018, 18:10

[http://www.aljyyosh.com/vb/showthread.php?](http://www.aljyyosh.com/vb/showthread.php?t=55874&s=ba37924a46f7453d47f43bb0f0d70f6e&p=568867&viewfull=1#post568867)

[t=55874&s=ba37924a46f7453d47f43bb0f0d70f6e&p=568867&viewfull=1#post568867](http://www.aljyyosh.com/vb/showthread.php?t=55874&s=ba37924a46f7453d47f43bb0f0d70f6e&p=568867&viewfull=1#post568867) • Reference Actions • 6+ references

Recorded Future



Educate yourself and your stakeholders on what the dark web is (and isn't!).

Swathes of what you will find down there will not relate directly to your security at all. Find efficient ways to monitor for what does.

Recorded Future

# Free Cyber Daily

Trending Threat Insights Delivered Daily

[www.recordedfuture.com/intel](http://www.recordedfuture.com/intel)



# Recorded Future

