



THE THREAT INTELLIGENCE COMPANY

脅威探知の先端企業

我が社の信念

WE BELIEVE

あらゆる組織は
脅威情報を包括的に探知することによって
リスクを大幅に低減することができる。

ORGANIZATIONS CAN
SIGNIFICANTLY LOWER RISK WITH
COMPREHENSIVE THREAT INTELLIGENCE.

RECORDED FUTUREとは

RECORDED FUTURE INTRODUCTION

- 世界のトップ企業の5社のうち4社はRecorded Futureのサービスを利用。
- 22,000名以上のセキュリティの専門家が情報配信を毎日活用。
- 世界展開
 - 本社 - マサチューセッツ州ボストン
 - ワシントンD.C.
 - スウェーデン イエーテボリ
 - 英国ロンドン
- Google, In-Q-Telをはじめとした出資者によるサポート
- 4 of the top 5 companies in the world rely on Recorded Future
- More than 22,000 security professionals receive daily
- Global offices
 - HQ - Boston, MA
 - Washington, DC
 - Göteborg, Sweden
 - London, UK
- Backed by Google, In-Q-Tel, and industry leading investors



Why Threat Intelligence?

- Global, virtual supply chains
- Global finance - SWIFT
- Everything connected to the internet (IoT)
- Criminals connected globally
- Intelligence pre-emptive defense
- Understand adversary intentions and capabilities
- Understand threat landscape

Dimon Sees Cyber-Security Spending Doubling After Hack

By Hugh Son and Madeline McMahon · Oct 10, 2014 2:21 PM ET · 2 Comments · Email · Print

JPMorgan Chase & Co. (JPM) Chief Executive Officer Jamie Dimon said the biggest U.S. bank will probably double its \$250 million annual computer-security budget within the next five years.

Dimon, whose company recently disclosed that an attack by hackers exposed contact information of 76 million households and 7 million small businesses, made the remarks today at an event sponsored by the Institute of International Finance in Washington.

"It's about firewall protection, it's about internal protection, it's about vendor protection, it's about everything that hooks up into you," said Dimon, 58. "There will be a lot of battles. Unfortunately some will be lost."



Photographer: Jason Hooten/Reuters
JPMorgan Chase & Co. Chief Executive Officer Jamie Dimon disclosed July 1 that he would... [Read More](#)

Related



脅威探知

THREAT INTELLIGENCE

包括的な脅威探知とは

DEFINING COMPREHENSIVE TI



BREADTH

オープンソース、クローズドソース、
テクニカルコレクション

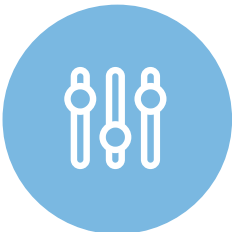
Open source, closed source and technical collections



RELEVANT

顧客のニーズに対応
リアルタイムでの提供

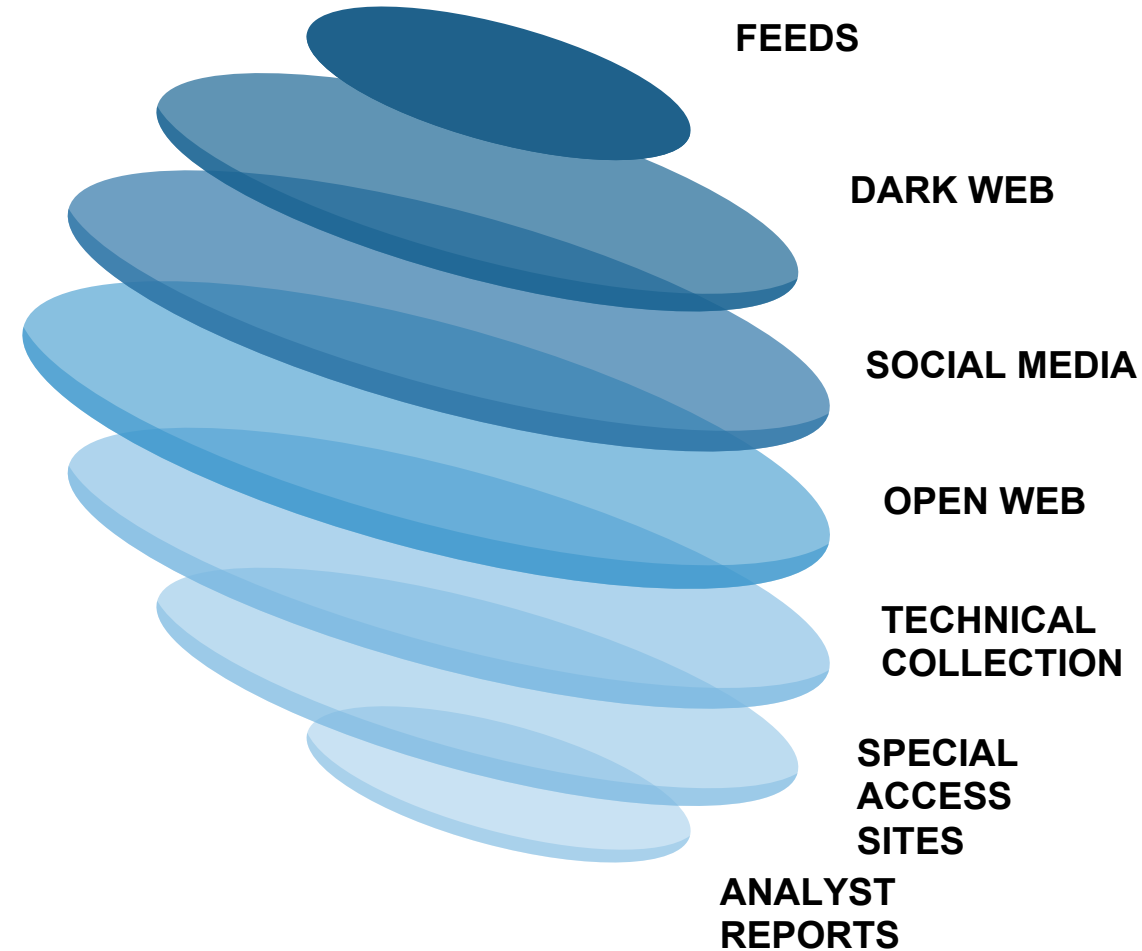
Customized to your needs Delivered in real-time



APPLIED

顧客が必要とする機会
統合された脅威探知システム

Context where you need it
Integrated machine readable TI



HOW IT WORKS

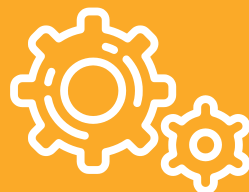
人工知能が点と点をつなげる

ARTIFICIAL INTELLIGENCE CONNECTS THE DOTS



7年以上の実績のある
リアルタイムの
情報収集プラットフォーム

**REAL-TIME
COLLECTION PLATFORM
+ 7 YEAR HISTORY**



特許化された
リスク分析・予測
定量化

**PATENTED ANALYTICS
& PREDICTIVE RISK SCORES**

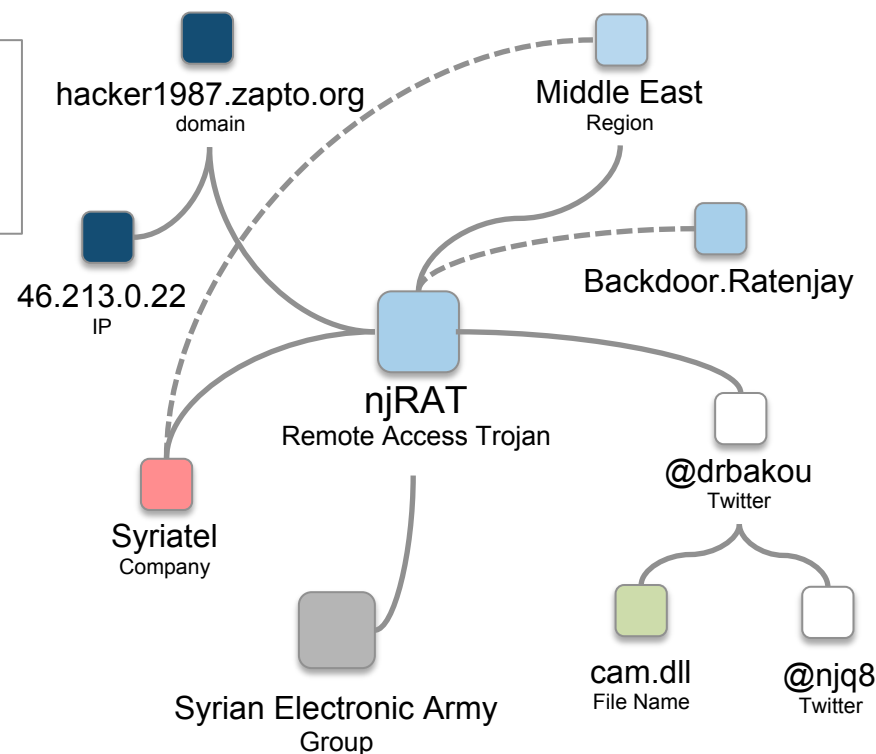
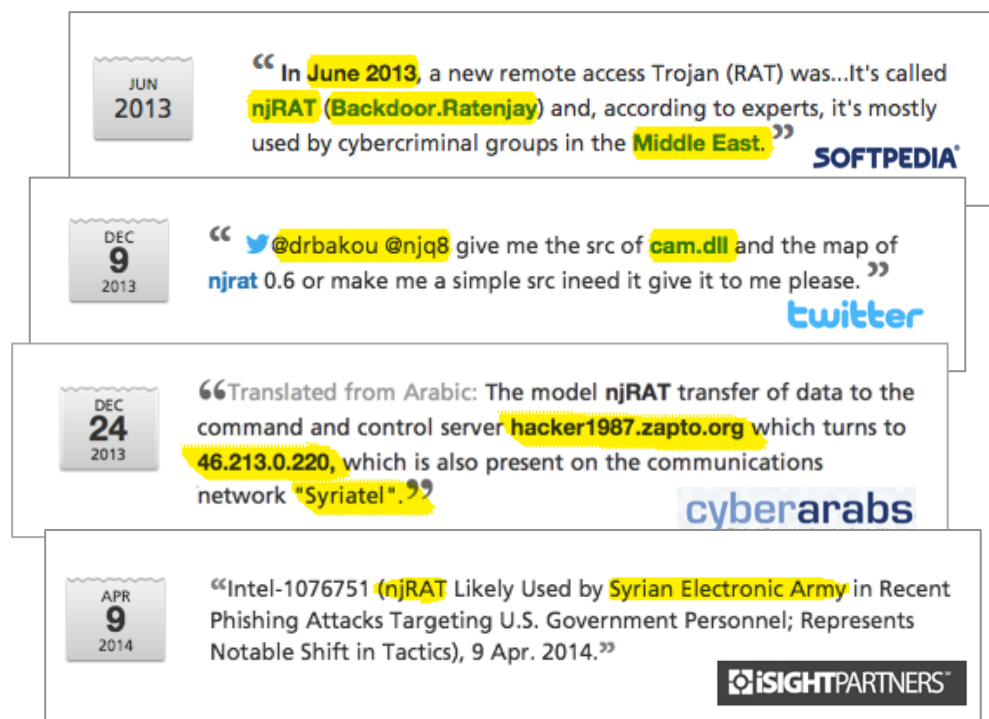


包括的
分析専門家による
サポート

**COMPREHENSIVE INTEL
& EXPERT ANALYST SUPPORT**

特許化された Web探知

PATENTED WEB INTELLIGENCE



COLLECTION

WORLD'S LARGEST SAAS PLATFORM



あらゆる言語において
750,000以上の情報源

750,000+ targeted sources,
in every language



1,200+ FORUMS

Hacker, criminal, extremist,
and researchers



40+ THREAT FEEDS

Every high-value feed
available on the web



30+ PASTE SITES

Leak posts, credential
breaches, corp IP



DARK WEB COLLECTION

100s of new TOR pages
daily, 400+ IRC channels



BLOGS & SOCIAL MEDIA

Security community, public
Tweets, Facebook, and more



CODE REPOSITORIES

Code sharing, malware,
POCs, app stores, vuln DBs



REAL-TIME ALERTS

Monitor TTP changes,
breached creds in real time



TECHNICAL COLLECTION

Shodan RAT controllers,
Google dorking, GEO IP

100s of NEW SOURCES

Every week, with direct links to sites

Very Critical
Risk Score 99
4 of 14 Risk Rules Triggered

Print

Request D

Add to List

EXPORT

100+ References to This Entity
First Seen Oct 9, 2016
Last Seen Oct 21, 2016

Show all events involving CVE-2016-3298 in Table | ▾

Risk Score Evidence

- Recently Linked to Ransomware** • 4 sightings on 1 source
HackDig Posts. Most recent link (Oct 19, 2016): <http://www.hackdig.com/10/hack-40248.htm>
- Recently Linked to Exploit Kit** • 119 sightings on 83 sources including @saidelike, @Fox0x01, @malwaregroup, @insecur1tea, @malwareforme. Most recent tweet: RT @proofpoint: Peas in a pod:#MSFT patches CVE-2016-3298, a 2nd info disclosure #0Day used in #malvertising campaigns & Neutrino EK https:.... Most recent link 17, 2016): https://twitter.com/ayanopapa_0612/statuses/787855955501289472
- Linked to Recent Cyber Exploit** • 162 sightings on 100 sources including @saidelike, @Fox0x01, CodeSec.net, @malwaregroup, @insecur1tea. Most recent tweet: RT @proofpoint: Peas in a pod:#MSFT patches CVE-2016-3298, a 2nd info disclosure #0Day used in #malvertising campaigns & Neutrino EK https:.... Most recent link 17, 2016): https://twitter.com/ayanopapa_0612/statuses/787855955501289472
- NIST Severity: Low** • 1 sighting on 1 source
National Common Vulnerabilities and Exposures (CVE) Database.

NVD Summary

Microsoft Internet Explorer 9 through 11 and the Internet Messaging API in Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to determine the existence of arbitrary files via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."

CWE ID 200
Published Oct 13, 2016
Updated Oct 17, 2016

Affected Products 6 of 7

Microsoft Internet Explorer 10	Microsoft Internet Explorer 11
Microsoft Internet Explorer 9	Microsoft Windows 7 sp1
Microsoft Windows Server 2008 R2 Service Pack 1	Microsoft Windows Server 2008 sp2

[Show All](#)

CVSS V2 Score 2.6 of 10 (Low)

Access Vector Network
Authentication Not Required

Confidentiality Partial

Access Complexity High
Integrity None
Availability None

INTEL CARDS UPDATE IN REAL TIME



IPs



DOMAINS



HASHES



VULNERABILITIES



THREAT ACTORS



MALWARE

統合された、リアルタイムの対策

他のプログラムと連携可能な脅威分析

INTEGRATED, REAL-TIME MACHINE READABLE INTELLIGENCE

LogRhythm splunk



THREAT INTEL

Real-time alerts to direct threats, data leaks
Eliminate manual research and collection
Identify emerging TTPs most likely to impact your business

SOC

10x faster at dismissing false alerts
Enrich events with risk scores and context

VMT

Prioritize CVE based on real-time intel and risk scores
Alerts on CVE's exploits in the wild

IR

Rapidly link actors/vectors/targets
Ticketing: intelligence and context for IT support

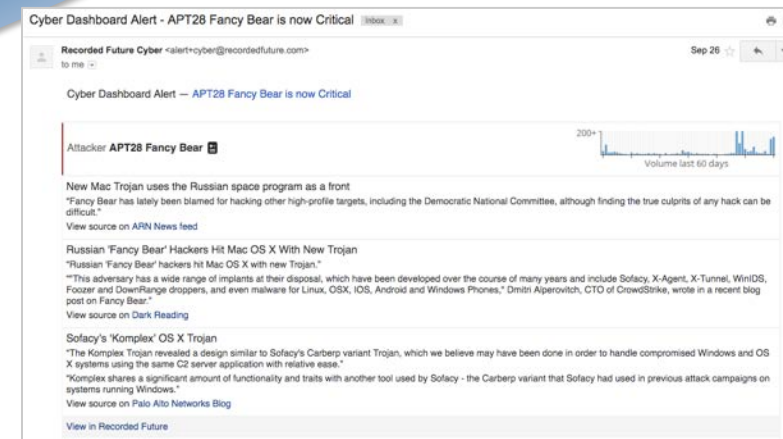
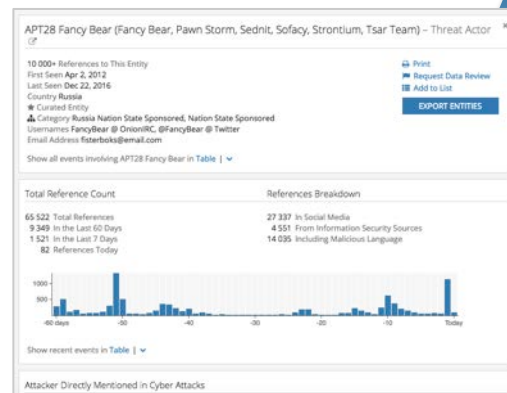
RISK

Early warning on emerging threats
Global, industry, cohort/peer trends
On-the-fly risk assessments

ケース 1：状況に応じた注意喚起とアラート

CASE A: SITUATIONAL AWARENESS & ALERTING

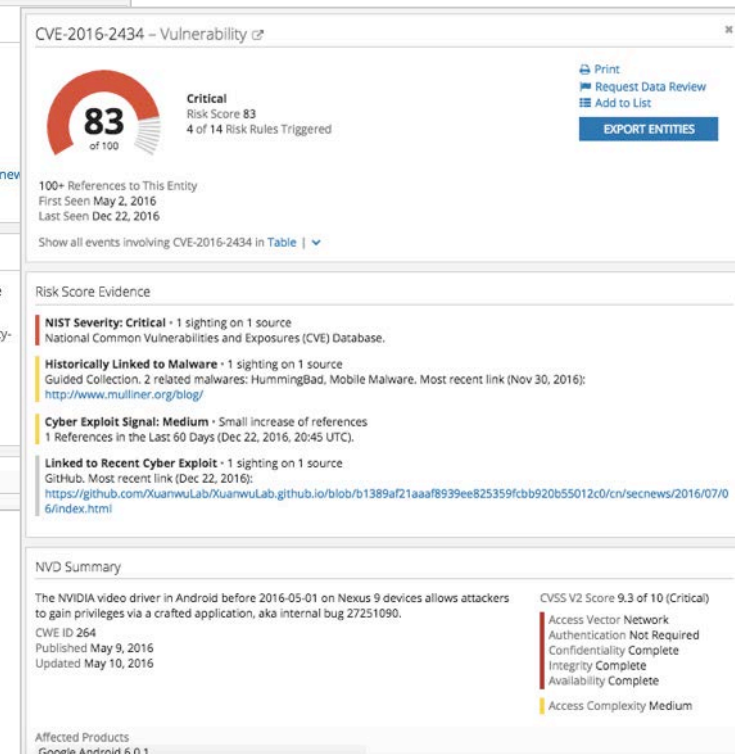
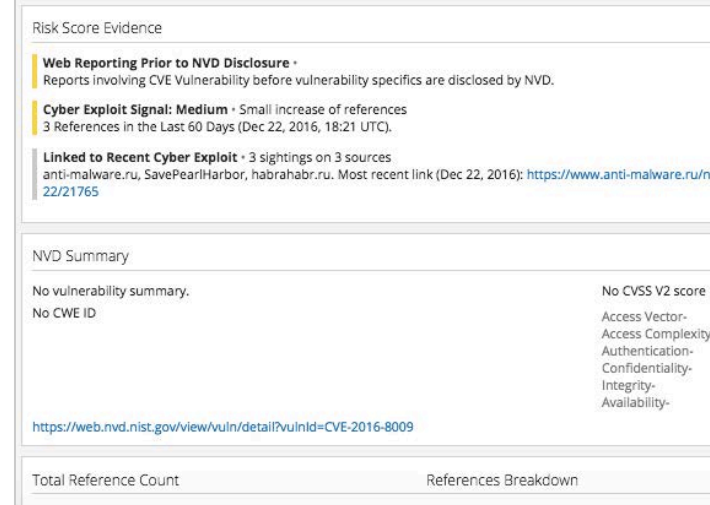
- 世界的な注意喚起
- 関係者・手法・ターゲット・行動・脅威の痕跡のモニタリング
- 特定のアラートの発信
- 重要な情報を精査
- Splunk, Qradar, ArcSightといった他のセキュリティ関係サービスと連携
- Global awareness
- Monitor actors, methods, targets, operations, IOCs
- Targeted alerts
- Drill into items of interest
- Correlate with perimeter security
- Splunk, Qradar, ArcSight



ケース 2: 脆弱性とTTP分析

CASE B: VULNERABILITY AND TTP ANALYSIS

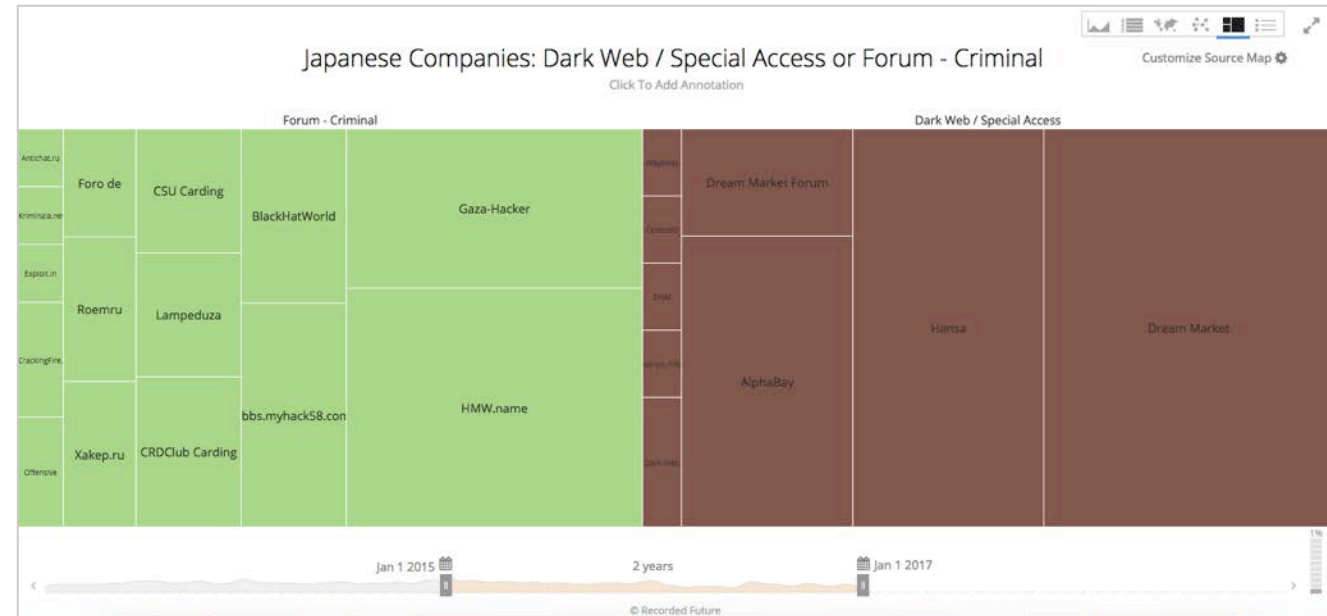
- 脆弱性とTTPの分析
- 関係する脅威情報を一箇所に集約
- 事前の脆弱性の検知
- エクスプロイト、エクスプロイトキット、マルウェアの早期検知
- Tenable, Qualysといった脆弱性マネジメントシステムとの統合
- Analyze vulnerabilities and TTPs
- All relevant intelligence in one place
- Intelligence on vulns before official sources
- Early intel on exploits, exploit kits, malware
- Integrate with vuln mngmt systems – Tenable, Qualys



ケース 3: ダークウェブのモニタリング

CASE C: DARK WEB MONITORING

- Web上からダークウェブの情報を収集
- クレジットカード、振り込み情報、社会保障番号
- 知的財産
- Technical surface area
- Monitor dark web sources
- Credit cards, SWIFT addresses, SSNs
- Intellectual property
- Technical surface area



530230, Sumitomo Corp and MasterCard Inc. mentioned

Static Bins

DEC 8 2016

Translated from English: "530230** | **MASTERCARD** | **SUMITOMO MITSUI CARD COMPANY, LTD.**" [Cached](#)

Show original

Source CSU Carding Forum on Dec 8, 2016, 16:57

<http://csu.su/showthread.php?p=580758> • Reference Actions • 1+ reference

456678, Japan and Mitsubishi UFJ Financial Group, Inc. mentioned

Partage de CC Gratuites par des membres

JUL 24 2016

"456678 [**MITSUBISHI UFJ FINANCIAL GROUP, INC.** VISA CREDIT GOLD PREMIUM **JAPAN**]" [Cached](#)

Source French Deep Web by par on Jul 24, 2016, 11:29

<http://fdwocbsnity6vzwd.onion/viewtopic.php?pid=518465#p518465> • Reference Actions • 1+ reference

PlayStation Network mentioned

JUST CAUSE 3 - PS4 ACCOUNT

APR 1 2016

"In **PlayStation@Network**, click Register" [Cached](#)

Source Hansa by wakawaka on Apr 1, 2016, 08:57

<http://hansamkt2rr6nfg3.onion/listing/14160/> • Reference Actions • 2+ references

Macquarie, Mizuho Financial Group, Inc., ICICI Bank Ltd and 2 more mentioned in Oceania

Over \$10,000 balance HSBC Login with email:pass and answers to security questions United Kingdom

AUG 9 2016

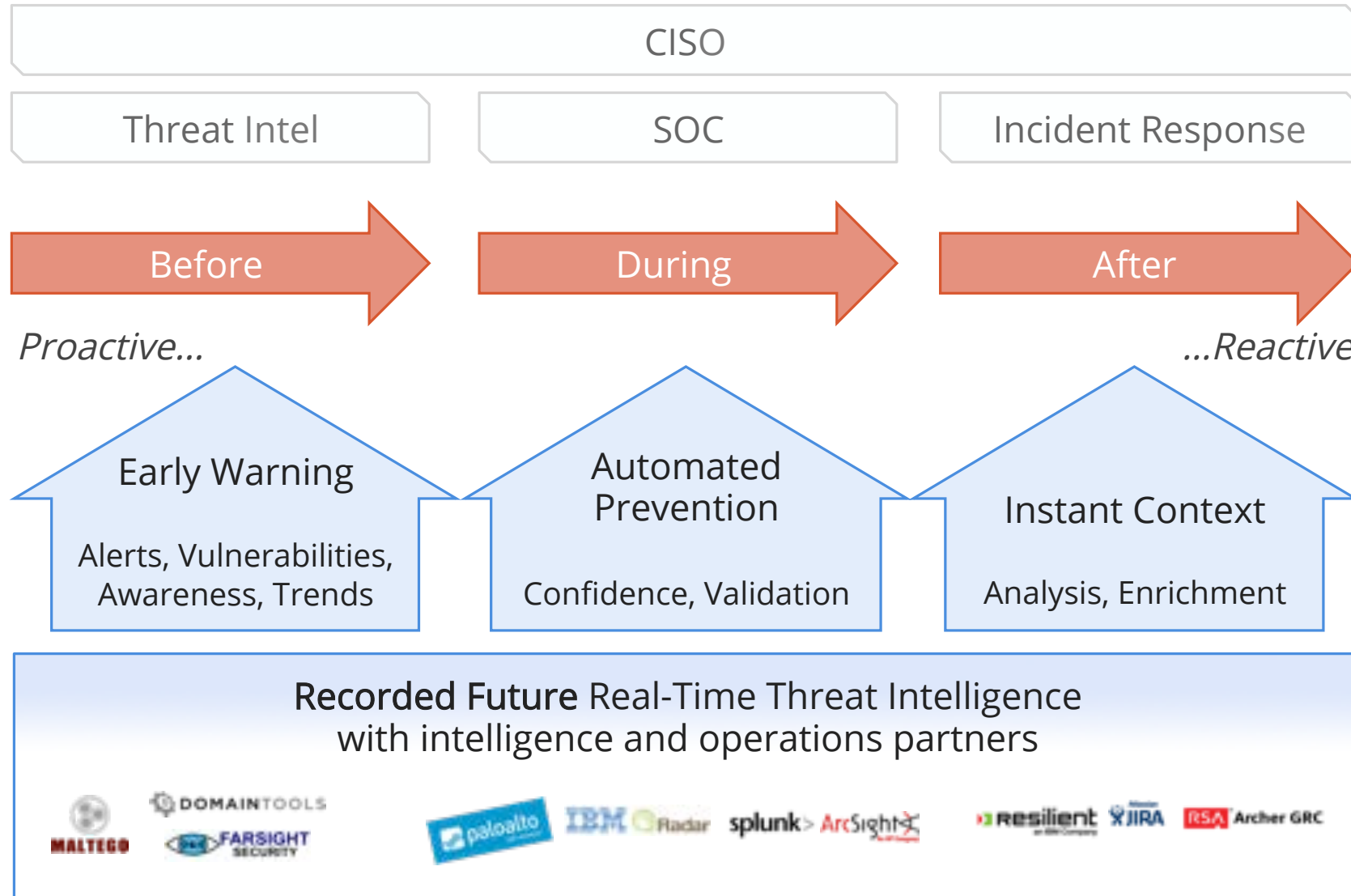
"**Societe Generale, Mizuho Financial Group, ICICI Bank, Akbank, Macquarie,**" [Cached](#)

Source Hansa by European_American on Aug 9, 2016, 11:55

<http://hansamkt2rr6nfg3.onion/listing/34138/> • Reference Actions • 1+ reference

攻撃のあらゆるフェイズで検知が可能

INTEL FOR ALL PHASES OF ATTACK CYCLE



脅威探知の先端企業

THE THREAT INTELLIGENCE COMPANY

サイバー攻撃対策のリーディングカンパニー

LEADING DEDICATED CTI PROVIDER



- 2009年に設立、社員120名
- Google、In-Q-Tel、Basis Technologyをはじめとした出資者による支援
- 拠点：ボストン、ワシントンDC、ロンドン、スウェーデン
- 22,000名以上のサイバーセキュリティ専門家が利用
- Founded in 2009, 120 employees
- Backed by Google, In-Q-Tel, Basis Technology & industry leading investors
- Offices: Boston, DC, London, Sweden
- Used by more than 22,000 security professionals worldwide



86% のFORTUNE 100企業が利用
OF FORTUNE 100



104% の顧客が契約更新
CUSTOMER RENEWALS



63% の悪意のある通信をブロック
DECREASE IN MALICIOUS TRAFFIC

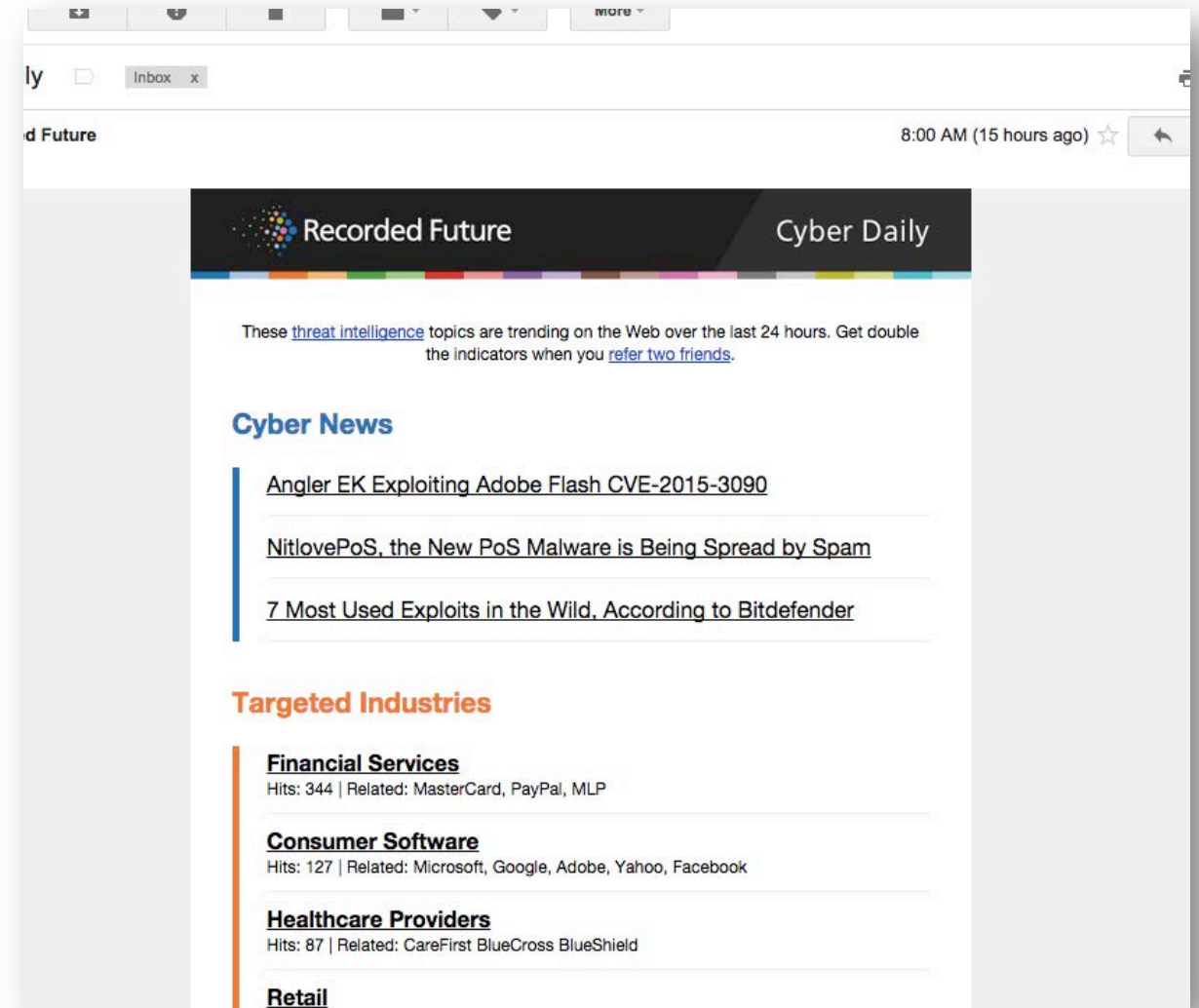
Follow-up

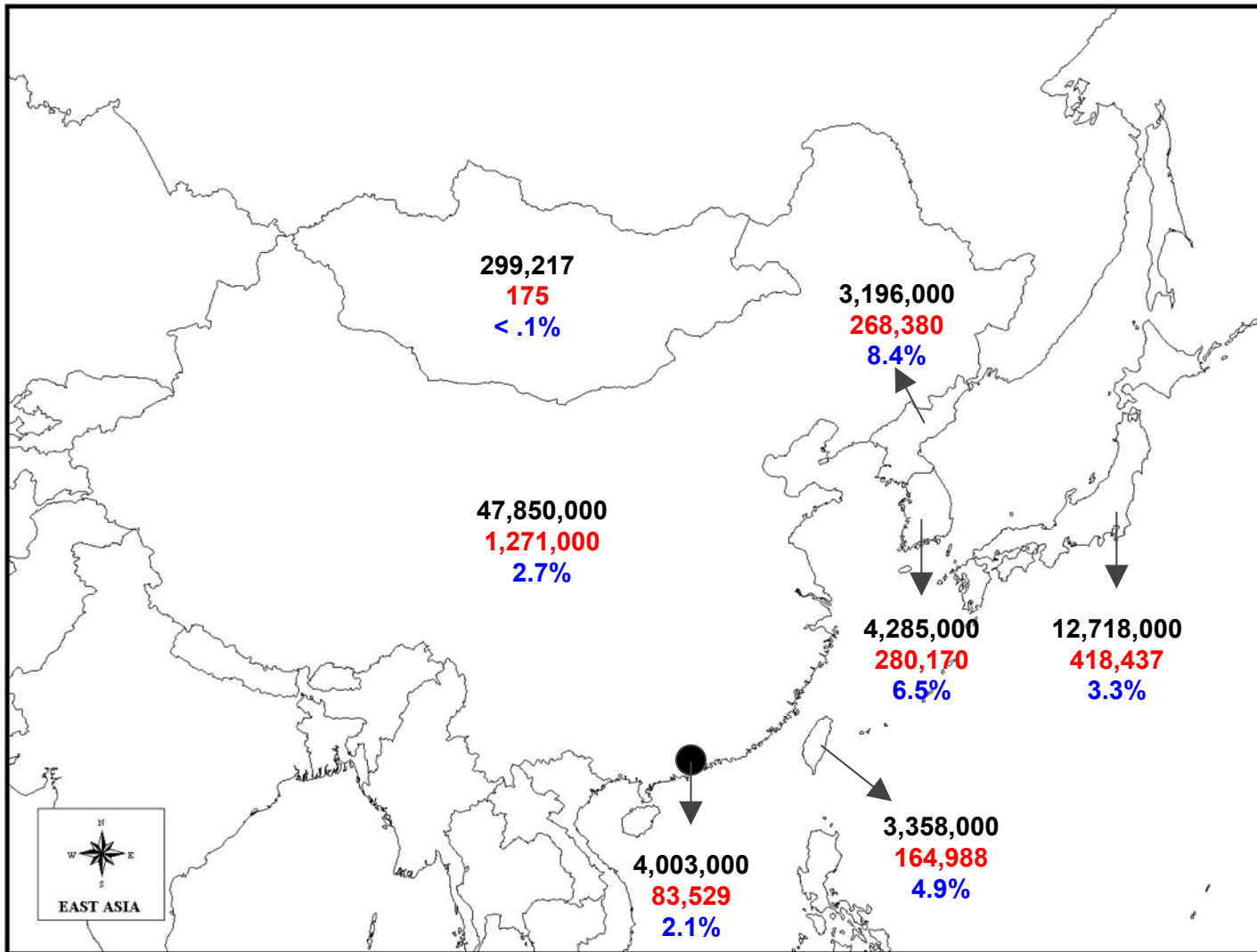
Contact me: c@recordedfuture.com

Visit: www.recordedfuture.com

Sign up for Cyber Daily

Follow me on Twitter: [@cahlberg](https://twitter.com/cahlberg)





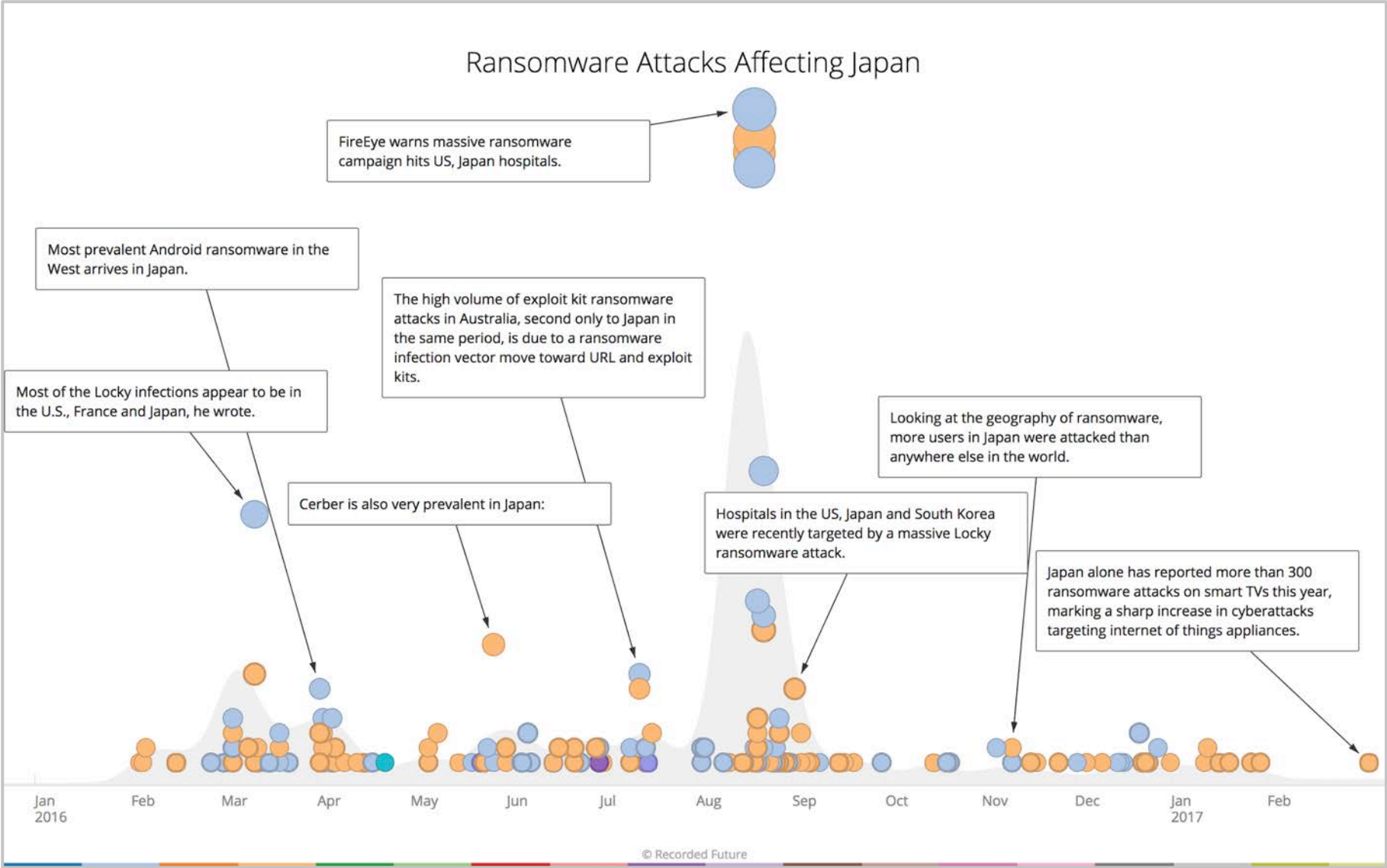
Total References -

Cyber References -

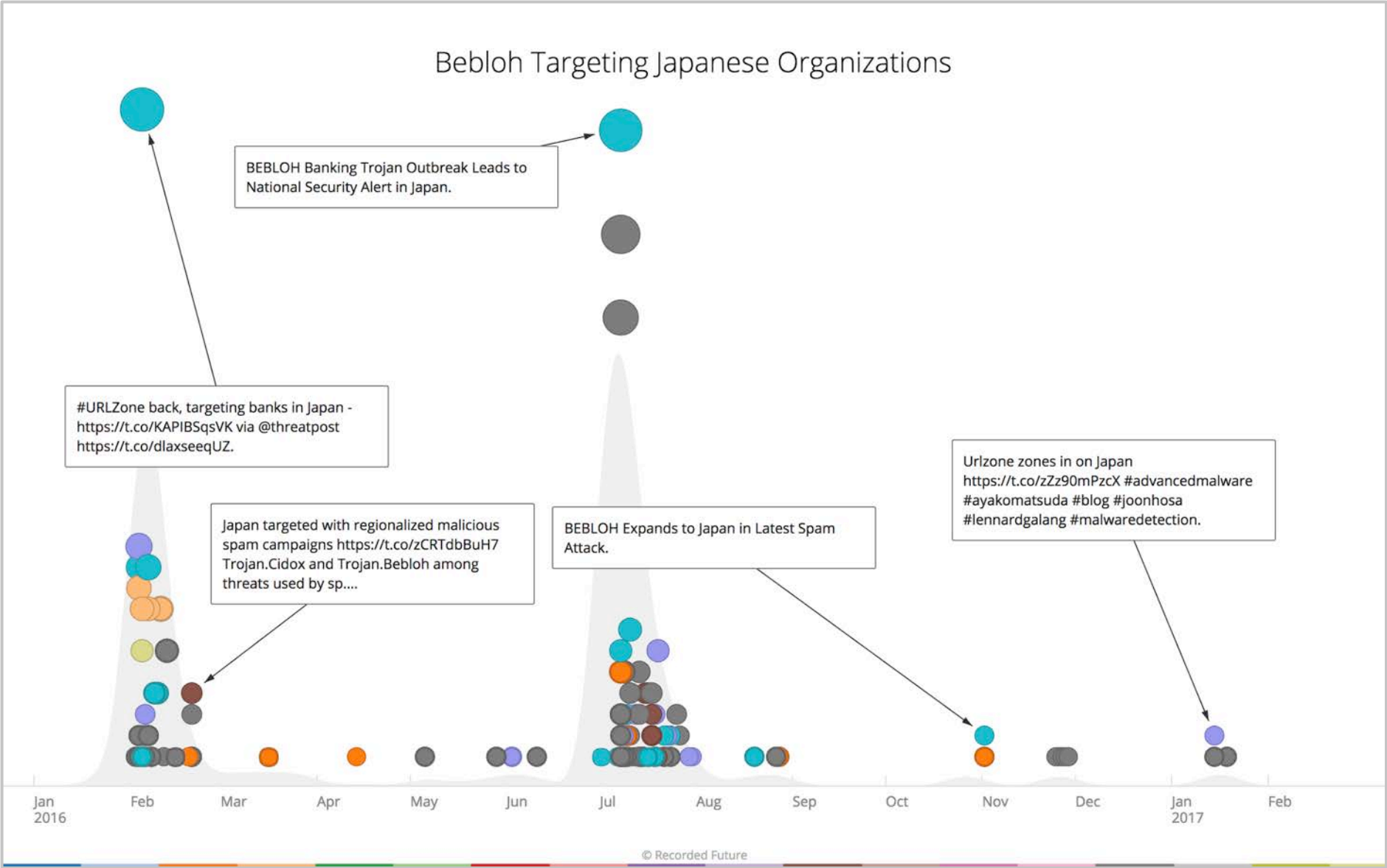
Percentage -



Malware Category	Instances
Ransomware	1259
Trojan	417
Banking Trojan	315
Adware	213
Botnet	192
Remote Access Trojan (RAT)	103
Computer virus	97
Exploit Kit	44
Rootkit	9



Malware	Instances
Bebloh	548
Stuxnet	547
Locky	406
VAWTRAK	240
Elirks	182
Mirai	129
NetTraveler	93
Rovnix	75
Shifu	64





▼ Events

Involving **Bebloh (Shiotob, URLZone) x**

AND

"snort" x

OR "yara" x

OR "yara rule" x

Event Type Any event type

Event Time Anytime x

Publish Time Anytime

► Sources Nothing selected

► Exclude Nothing selected

Clear All Options

DONE



Gootkit, Bebloh, SNORT and 2 more mentioned

OCT
15
2016

Rig Exploit Kit via EiTest delivers malicious payload from 185.141.26.12 – BroadAnalysis

"Today I captured traffic from the **Rig Exploit Kit (EK)**...**Snort**, using the Emerging Threats open ruleset generated alerts for likely Shylock/**URLZone/Gootkit/Zeus Panda C2.**"

Source BroadAnalysis on Oct 15, 2016, 00:00

<http://www.broadanalysis.com/2016/10/15/rig-exploit-kit-via-eitest-delivers-malicious-payload-f...> • Reference Actions • 1+ reference

There are the Emerging Threats.net Open rulesets.

More information available at <http://www.emergingthreats.net>.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
blockrules/	2017-01-27 00:30	-	
changelogs/	2017-01-27 16:27	-	
fwrules/	2014-08-11 13:22	-	
open-nogpl/	2016-10-06 12:51	-	
open/	2016-10-06 12:51	-	
projects/	2011-01-17 13:34	-	
research/	2016-02-12 13:55	-	
sidmap/	2012-07-12 12:18	-	
version.txt	2017-01-27 16:27	5	

Apache/2.4.7 (Ubuntu) Server at rules.emergingthreats.net Port 443

Search

AdvancedApplicationsHome

▼ Events

Involving

Bebloh (Shiotob, URLZone) ✕

Add | ▼

AND

Any AS Number ✕

OR Any Email Address ✕

OR Any Filename ✕

OR Any Hash ✕

OR Any IP Address ✕

OR Any Registry Key ✕

Add

Event Type

Any event type

Event Time

-4y to +1y

Publish Time

Anytime

► Sources

Nothing selected

► Exclude

Nothing selected

Clear All

Options

DONE

Search

AdvancedApplicationsHome

AlertingSaveExportShare?

Zach Flom

Bebloh IOCs

Domain (16)

File Type (2)

Binary executable files

Archive files

Filename (27)

9e416802a31ee6a610...

explorer.exe

cmd.exe

winupdt.exe

1f40feff1bb01d296b26...

278f0db31e420152ba...

Show all items

Filename Extension (3)

Hash (160)

c3b2ff6ddf403dcf502a...

010e4b5f90a78542c68...

15896a44319d18f8486...

36e553dc6ea092af7d8...

88f12cf66117c119a0d...

Time

Event Information

JAN 15 2017

Bebloh and d862bbfaf39a69f55a394a7bdc08921009e86d25ef357caf5faf95487f1370...

Antivirus scan for d862bbfaf39a69f55a394a7bdc08921009e86d25ef357caf5faf95487f1370...

VirusTotal

"Shiotob.235008[h] d862bbfaf39a69f55a394a7bdc08921009e86d25ef357caf5faf95487f13705."

Source VirusTotal on Jan 15, 2017, 00:55

https://www.virustotal.com/file/d862bbfaf39a69f55a394a7bdc08921009e86d25ef357caf5faf95487f1370... • Reference Actions • 1+ reference

JAN 6 2017

Bebloh, Sophos Group Plc and bfff911f7c2d17012562ed23b214756bfc49f339e53f13c71116baa693ff8b50 mentioned

Antivirus scan for bfff911f7c2d17012562ed23b214756bfc49f339e53f13c71116baa693ff8b50 at 2017-01-06 07:30:22 UTC -

VirusTotal

"scans Sophos result Trojan/Shiotob-Bj bfff911f7c2d17012562ed23b214756bfc49f339e53f13c71116baa693ff8b50."

Source VirusTotal on Jan 6, 2017, 07:30

https://www.virustotal.com/file/bfff911f7c2d17012562ed23b214756bfc49f339e53f13c71116baa693ff8b50... • Reference Actions • 1+ reference

W32/Bebloh.Kltr.spy, 32c7cabfe8365ea00b12a82ebd7fcb88, trojan.win32.dorv.a and 12 more mentioned

Antivirus scan for bfff911f7c2d17012562ed23b214756bfc49f339e53f13c71116baa693ff8b50 at 2017-01-06 07:30:22 UTC -

Entities in result

Indicators and Observables (233)

AS Number (1)

Domain (21)

File Type (2)

Filename (27)

Filename Extension (3)

☒ Hash (160)

☒ IP Address (3)

CIDR (1)

URL (15)


Location (4)

Person (7)

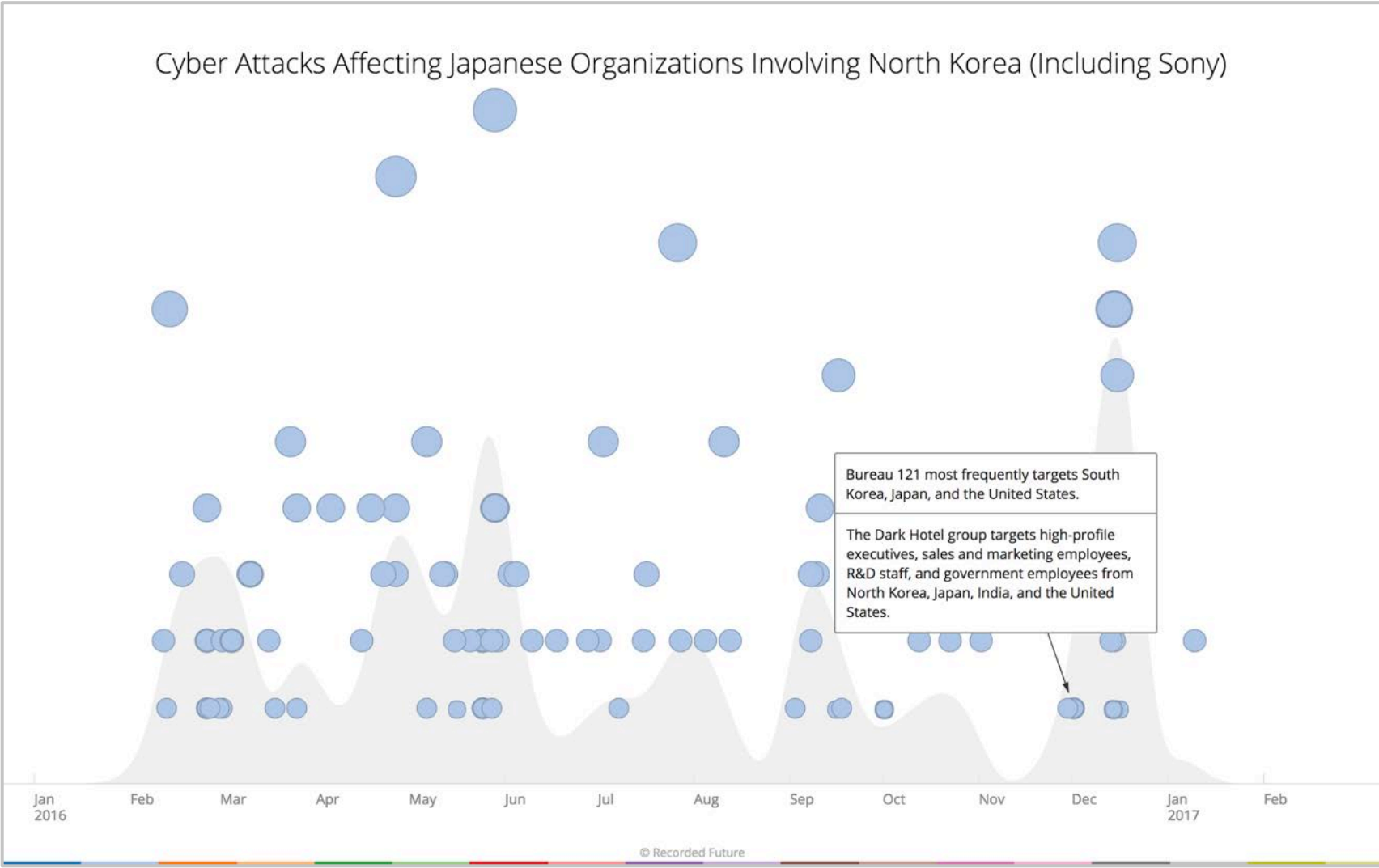
ea5086484064ce239232cd...	Hash(SHA-256)	VirusTotal	https://www.virustotal.com...
f162181fba271ed5ca95987...	Hash(SHA-256)	VirusTotal	https://www.virustotal.com...
fe9b87d98cb1e708ea6df40...	Hash(SHA-256)	VirusTotal	https://www.virustotal.com...
ffa3cb58b11b59c63462c15...	Hash(SHA-256)	VirusTotal	https://www.virustotal.com...
5.187.2.19	IP Address	Proofpoint	http://proofpoint.com/us/t... insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-japan
5.45.179.179	IP Address	Proofpoint	http://proofpoint.com/us/t... insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-japan
91.242.163.74	IP Address	Proofpoint	http://proofpoint.com/us/t... insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-japan

GET CSV

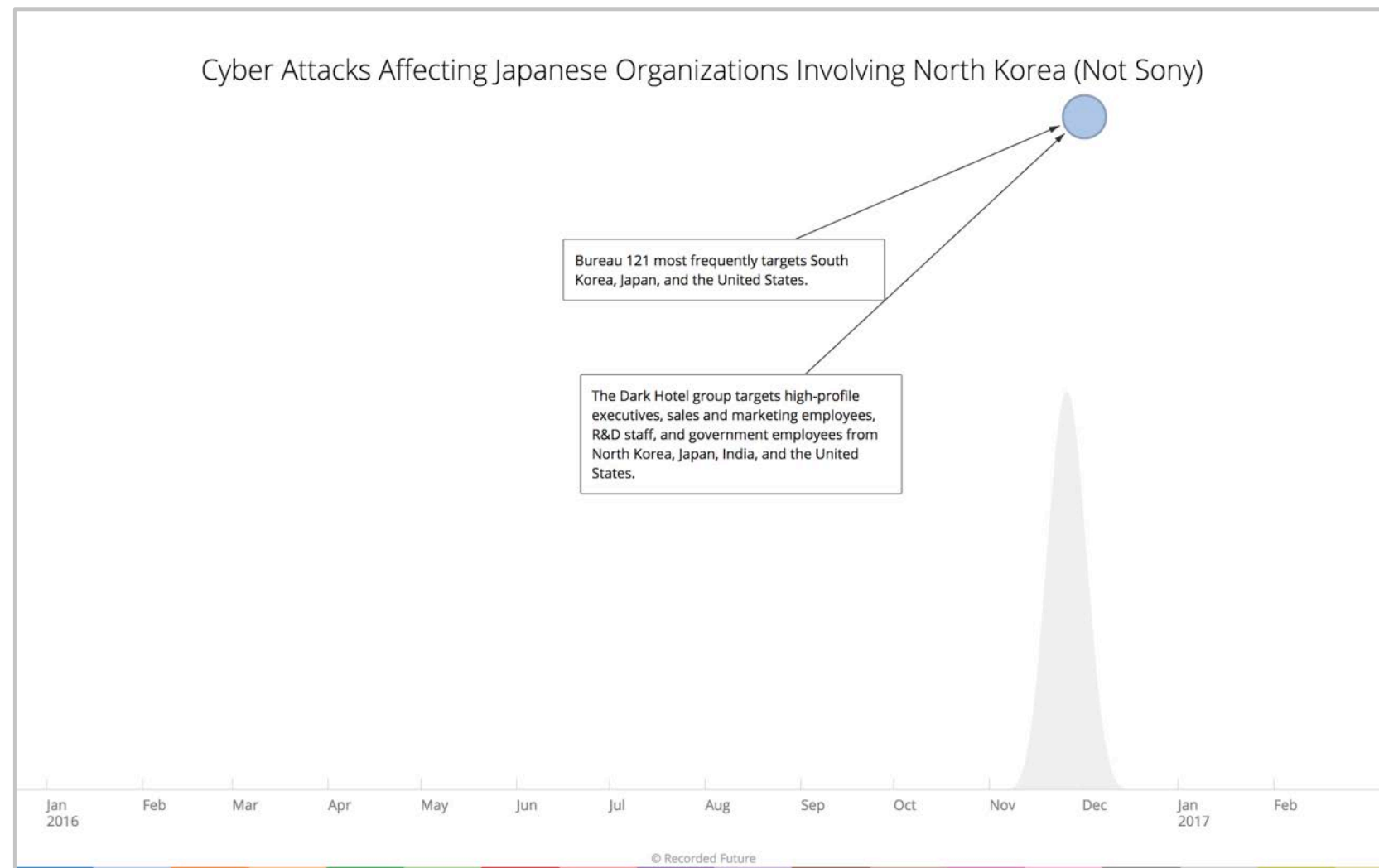
CANCEL

 Recorded Future

Countries (Not Japan/U.S.)	Instances
North Korea	417
Bangladesh	51
China	50
South Korea	41
Russia	39
United Kingdom	37
Taiwan	16
Iran	15
Australia	14



Countries (Not Japan/U.S.)	Instances
North Korea	417
Bangladesh	51
China	50
South Korea	41
Russia	39
United Kingdom	37
Taiwan	16
Iran	15
Australia	14



Countries (Not Japan/U.S.)	Instances
North Korea	417
Bangladesh	51
China	50
South Korea	41
Russia	39
United Kingdom	37
Taiwan	16
Iran	15
Australia	14

