.conf18

splunk>

Battling Online Bank Attacks with Detection Methods Using Splunk

Kaz Ozawa | Japan Net Bank

Rie Tokita | Macnica Networks, Splunk Architect

Takashi Komatsubara | Splunk Senior Partner Sales Engineer

October 2018 | Version 1.0

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

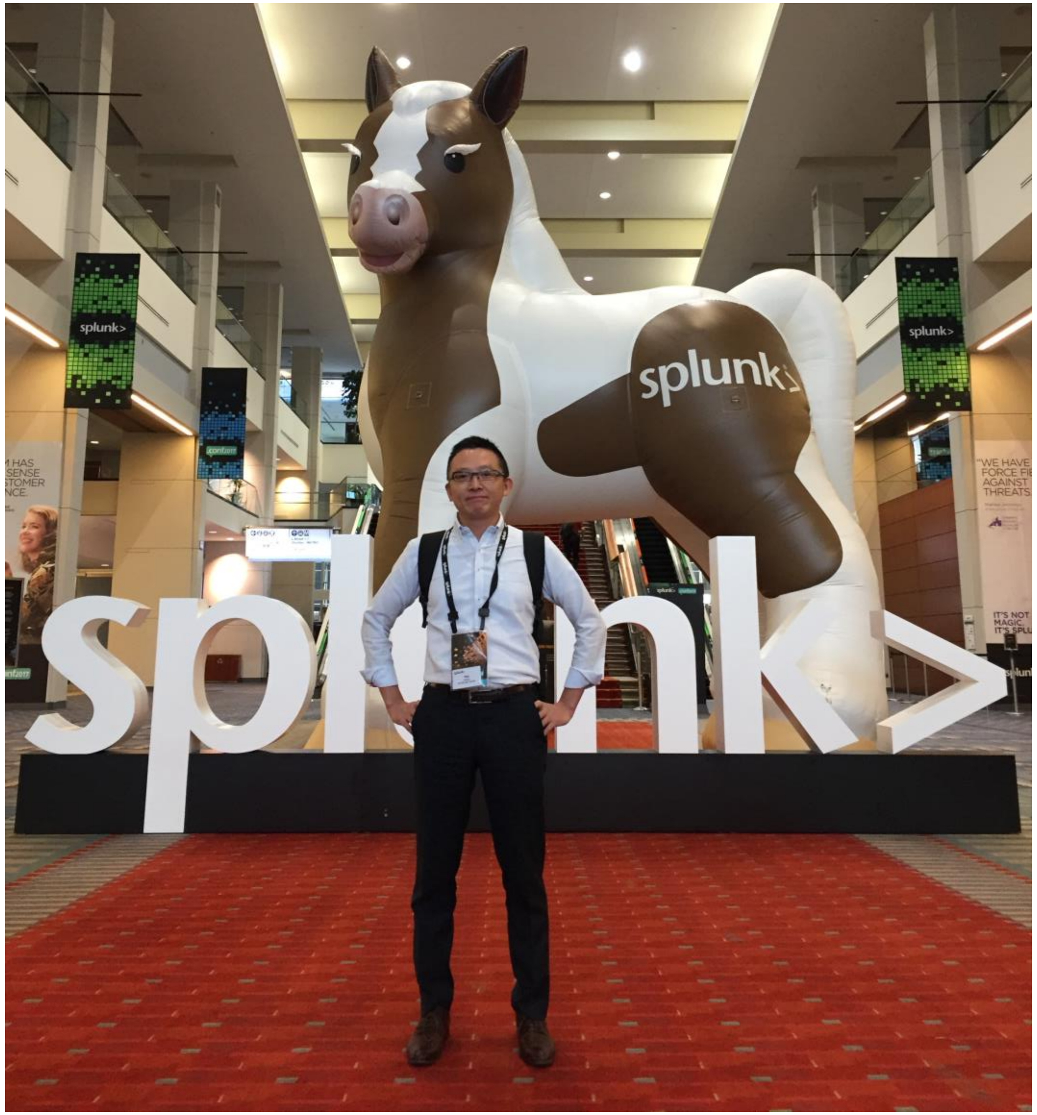
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

KAZ OZAWA

Senior IT Security Officer
Japan Net Bank

KAZ OZAWA

- JNB-CSIRT Member
- Security Business Experience 4 Years
- Splunk Experience 3 Years
- Financials ISAC Japan 2016,2017
    - Achievement for expanding the method of unauthorized access monitoring to Japanese financial institution by using Splunk



RIE TOKITA

Macnica Networks

TAKASHI KOMATSUBARA

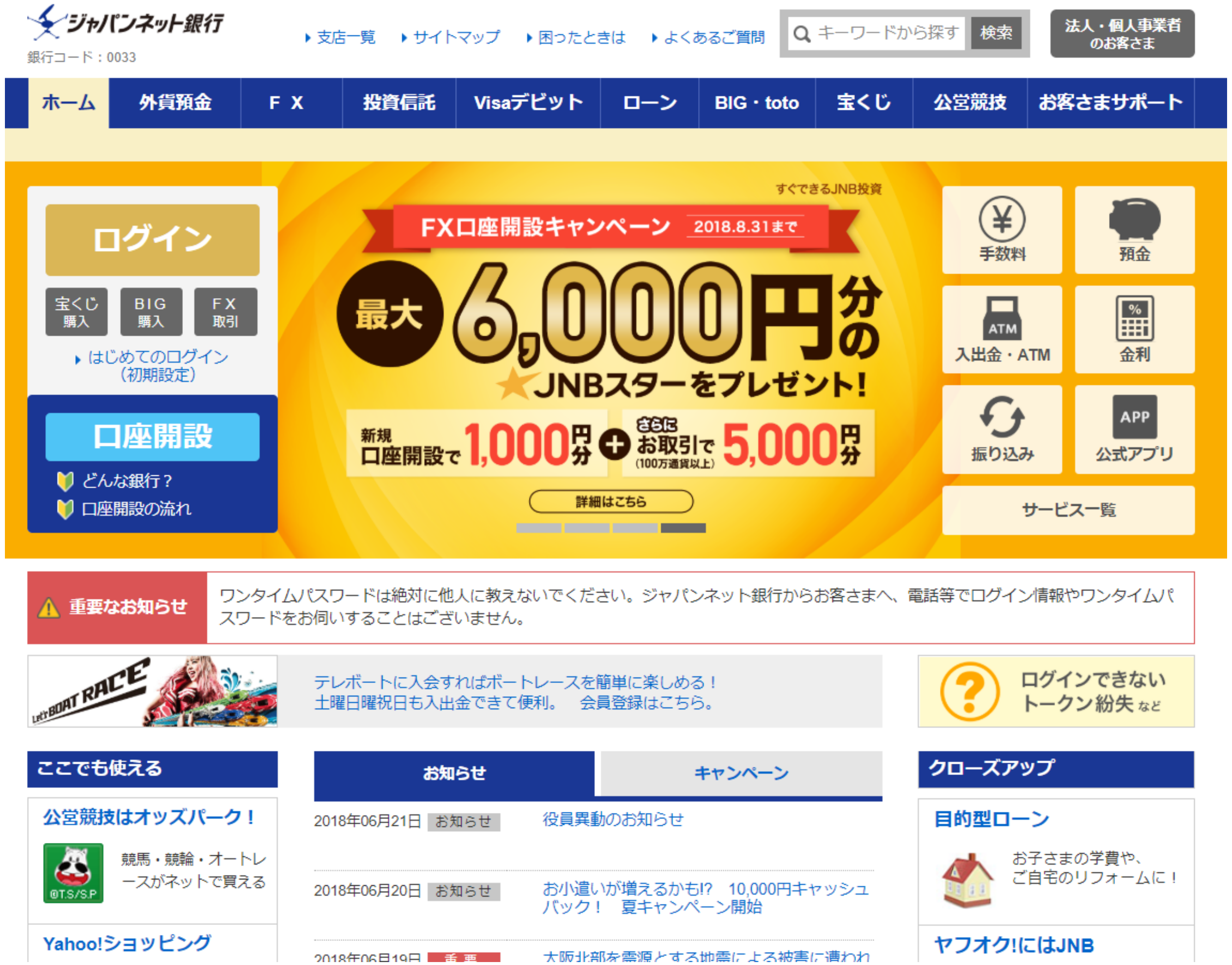
Splunk Japan

Japan Net Bank

Japan Net Bank

http://www.japannetbank.co.jp

- Exclusive Internet Banking Launched In Japan for the first time
  - Established in Oct, 2000
- # Of Account 370,000,000
- Credit Balance 700Billion Yen
- Service they provide
  - Credit, Transfer, Credit Deposit, Direct Deposit, Visa Debit Card, Foreign Currency Deposit, FX, Investment, Loan, Lottery



ジャパンネット銀行
銀行コード：0033

支店一覧　サイトマップ　困ったときは　よくあるご質問　キーワードから探す　検索　法人・個人事業者のお客さま

ホーム　外貨預金　F X　投資信託　Visaデビット　ローン　BIG・toto　宝くじ　公営競技　お客さまサポート

ログイン
宝くじ購入　BIG購入　FX取引
はじめてのログイン（初期設定）

口座開設
どんな銀行？
口座開設の流れ

すぐできるJNB投資
FX口座開設キャンペーン　2018.8.31まで
最大6,000円分のJNBスターをプレゼント！
新規口座開設で1,000円分 ＋ さらにお取引で（100万通貨以上）5,000円分
詳細はこちら

手数料　預金　入出金・ATM　金利　振り込み　公式アプリ
サービス一覧

重要なお知らせ
ワンタイムパスワードは絶対に他人に教えないでください。ジャパンネット銀行からお客さまへ、電話等でログイン情報やワンタイムパスワードをお伺いすることはございません。

Let's BOAT RACE
テレボートに入会すればボートレースを簡単に楽しめる！
土曜日曜祝日も入出金できて便利。　会員登録はこちら。

ログインできない　トークン紛失 など

ここでも使える

公営競技はオッズパーク！
競馬・競輪・オートレースがネットで買える

Yahoo!ショッピング

お知らせ　キャンペーン

2018年06月21日　お知らせ　役員異動のお知らせ

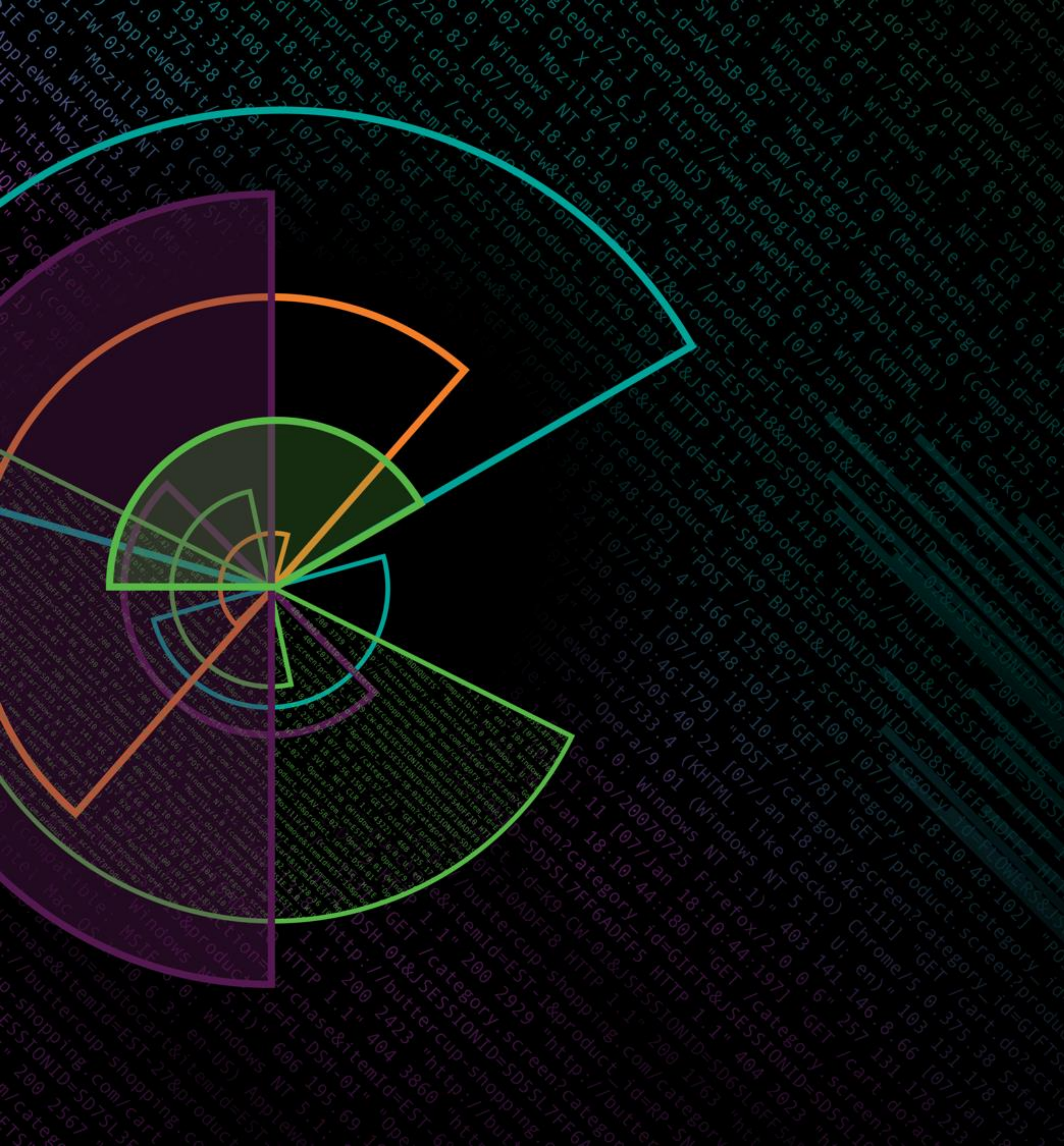
2018年06月20日　お知らせ　お小遣いが増えるかも!?　10,000円キャッシュバック！　夏キャンペーン開始

2018年06月19日　重 要　大阪北部を震源とする地震による被害に遭われ

クローズアップ

目的型ローン
お子さまの学費や、ご自宅のリフォームに！

ヤフオク!にはJNB



Splunk License & Captured Log

Internal System Log

Total 5.0G/day

- Firewall
  - 0.5G/day
  - Syslog
  - Real-time

- NG Firewall
  - 1.0G/day
  - Syslog
  - Real-time

- Proxy
  - 2.0G/day
  - Access Log
  - Real-time

- Active Directory
  - 2.0G/day
  - Event Log
  - Real-time

Online Banking System Log

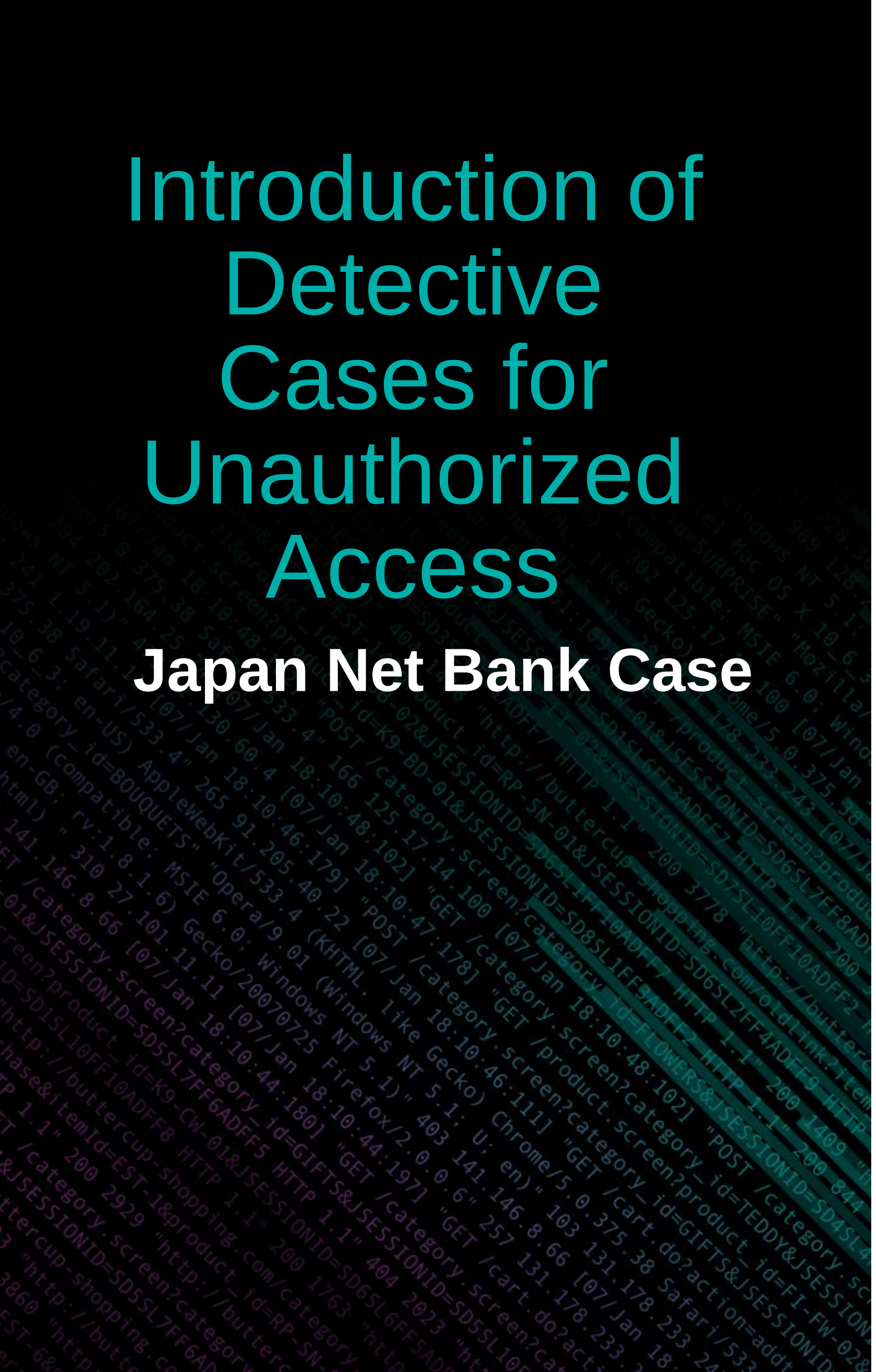
Total 18.5G/day

- WEB Server (akamai)
  - 7.0G/day
  - Access Log
  - 3hours delay

- Cloud Monitor (akamai)
  - 9.0G/day
  - Request/Response, IP Geo,WAF
  - 30minutes delay

- Banking Database
  - 1.5G/day
  - Bank Transaction Log
  - 30minutes delay

- Other Servers
  - 1.0G/day
  - Performance Log
  - Once a day



Introduction of Detective Cases for Unauthorized Access

Japan Net Bank Case

1. Log Analysis of Internal System Environment
   - How to detect malware infection with internal Traffic Analysis of Online banking
2. Log Analysis of Online Traffic
   - How to detect unauthorized access from uncommon traffic
3. How to detect phishing site
4. How to detect account takeover activities
5. How to detect the end-user's banking trojan infection

Log Analysis within Internal System Environment

Detect Malware Infection

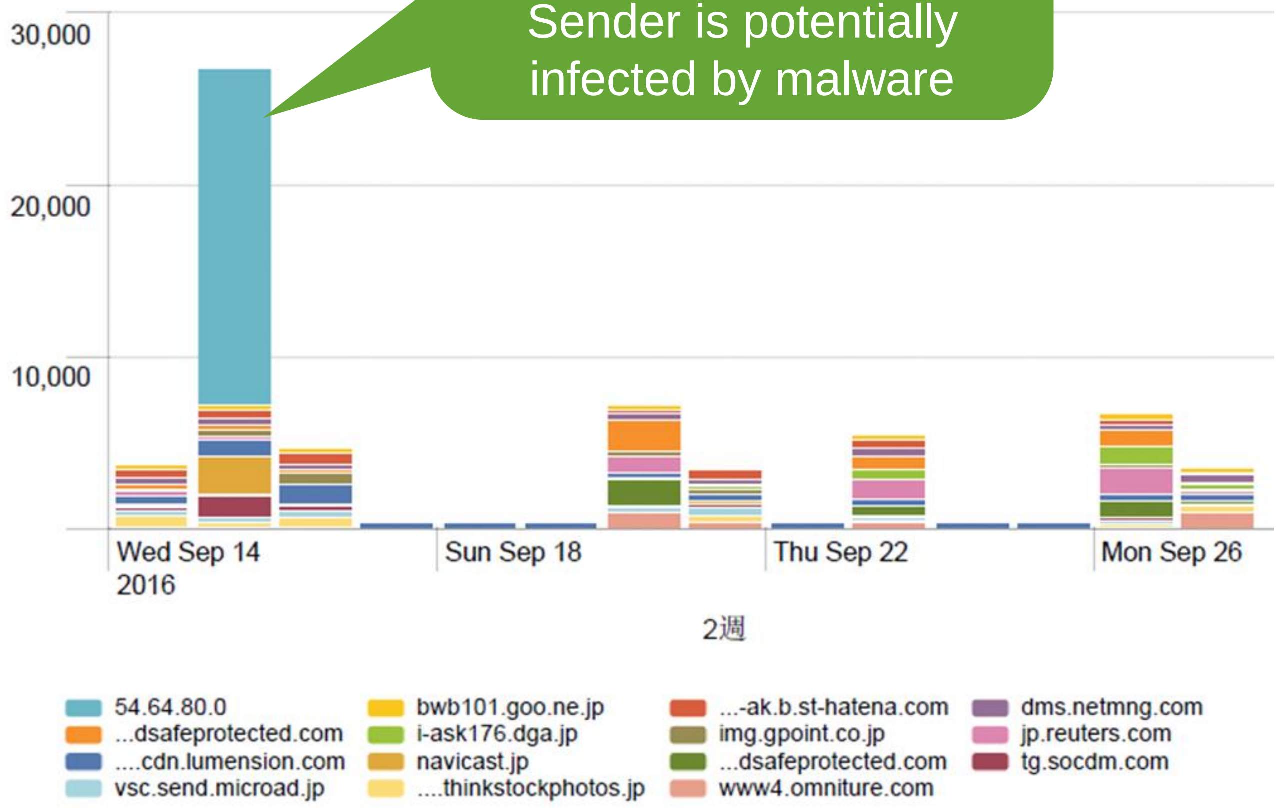
Detection of Malware Infection

Analyzing the proxying transmission destination

- Aggregate the date and time of proxy logs and find the suspicious internet transmission
  - Aggregate per FQDN of Transmission Destination
  - If no issue is found to the transmission destination, it will be added to the whitelist, and excluded from the aggregation

Tips: Exclude white list traffic based on source ip / servers, then easily visualize C & C server communications

Huge Access to VPS appeared all of the sudden.
Sender is potentially infected by malware

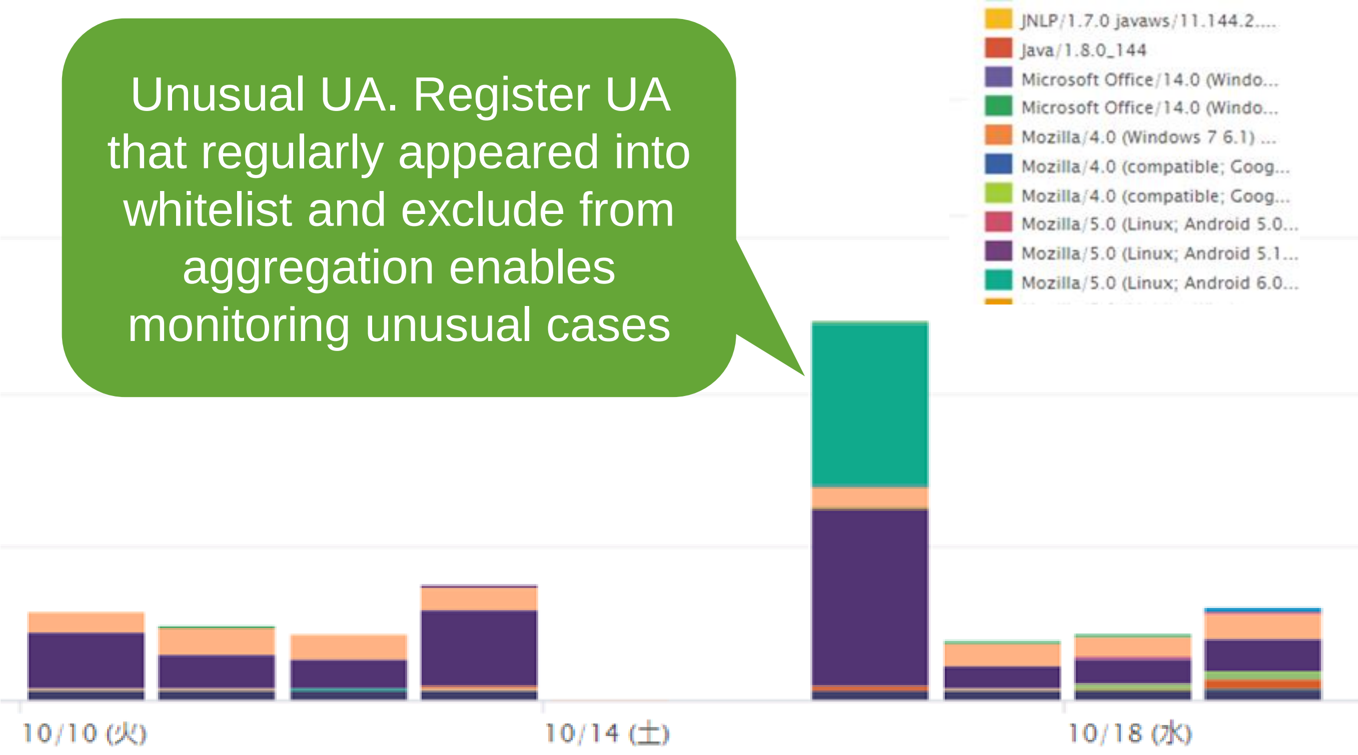


Detection of Malware Infection

Analyze Useragent from proxy logs

- Find the occurrence of any transmission to internet by suspicious Useragent
  - Not IE, Edge, Chrome, Firefox
  - No UA
  - Old version of browser
  - No precedent UA cases

Tips: UserAgents give us hints whether they are malware/C&C communications



Unusual UA. Register UA that regularly appeared into whitelist and exclude from aggregation enables monitoring unusual cases

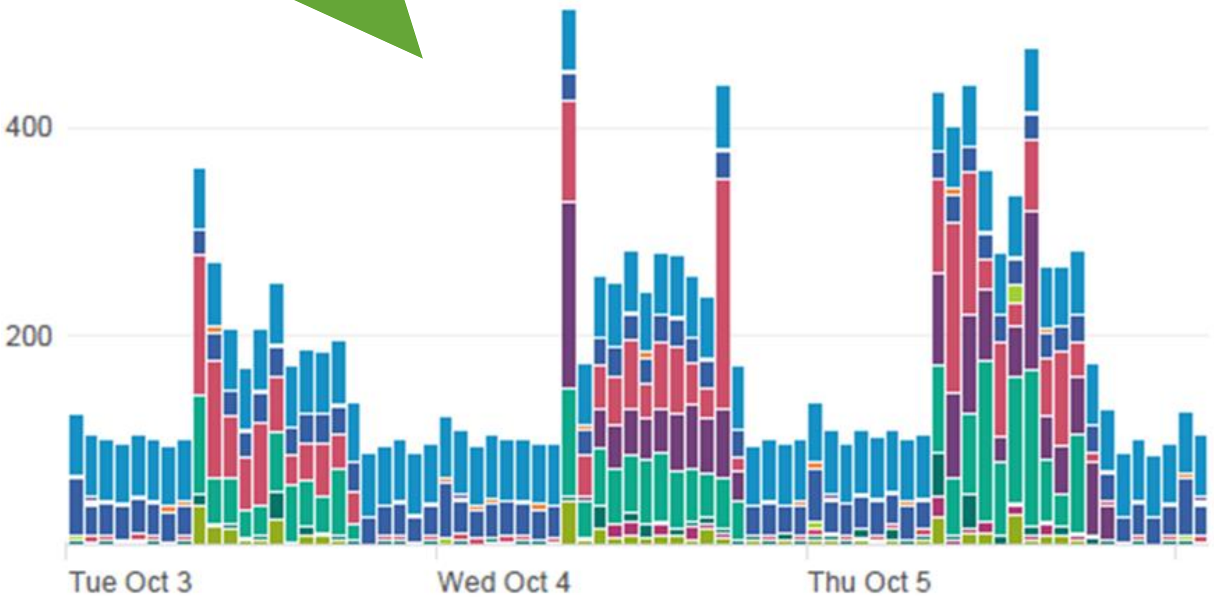
Detection of Malware Infection

Analysis of AD event log

- Aggregate per event code and check if there is any usage of suspicious account
  - Usage of unexpected privilege ID
    - 4672
  - Below is the failure of event code authorization
    - 4625、4672、4768、4771、4776
  - Event code that doesn’t appear in regular operation
    - 4618、4649、4719、4765、4766、etc

Very effective by just aggregating event code and confirming the date and time

Visualize suspicious accounts by count, event code and time/date



Analysis of Online Traffic

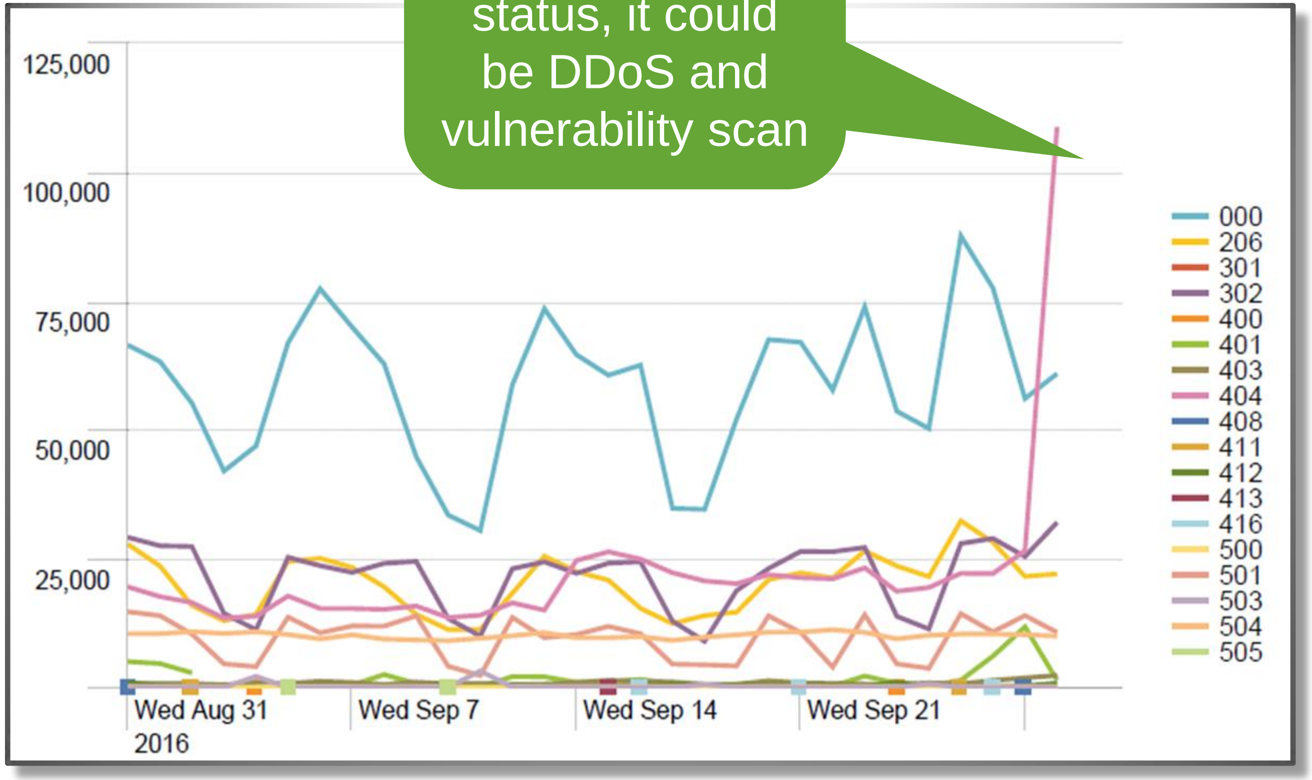
Detect unauthorized access from unusual traffic

Detection of Unusual Traffic

Analyze access log by status code

- Except normal status code（ex. 200、304）, aggregate and confirm unusual status request

By grasping daily baseline, unusual patterns can be recognized

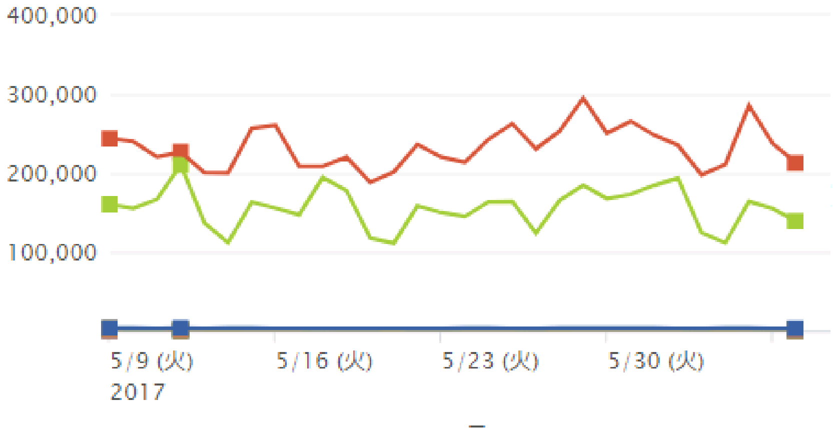


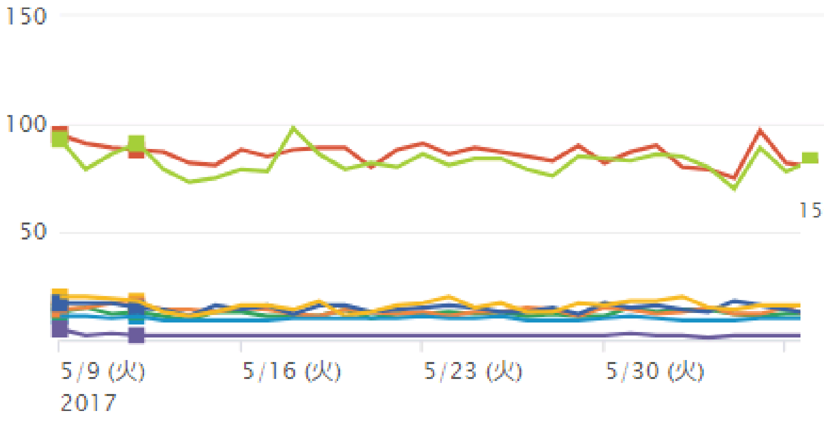
Too many requests for 404 status, it could be DDoS and vulnerability scan

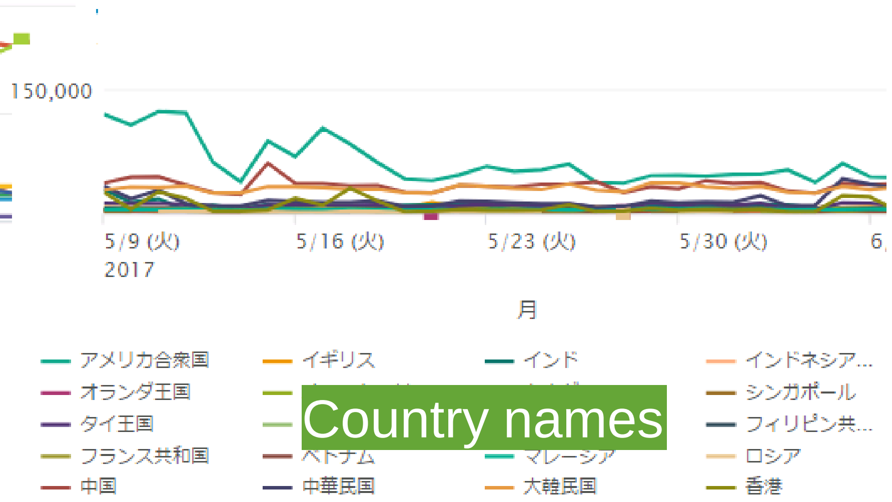
Detecting Unusual Traffic

Other Methods of Analyzing Access Log

- Aggregate the number of access sources/IP addresses by day
  - Approx. 20,000 Addresses/Day
- Aggregate the access number for each country by day
  - Approx. 100 Countries/Day
- Aggregate the number of requests for each country by day







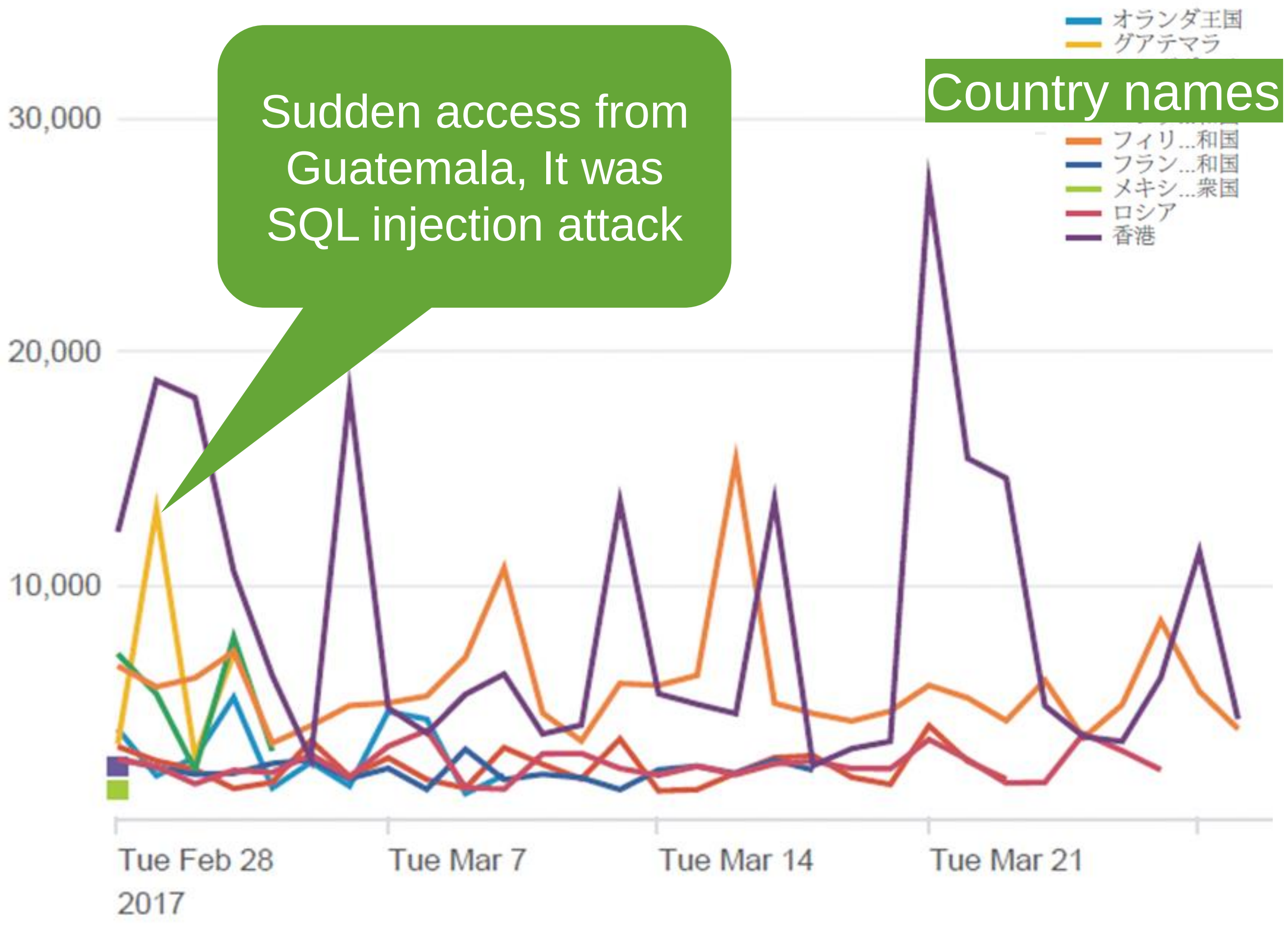
Country names

Either way, there is a regular trend

Detection of Unusual Traffic

Trend Analysis from the countries where there is not a lot of regular access

- By excluding the major countries, aggregate only the request from the countries where there are no regular access



Sudden access from Guatemala, It was SQL injection attack

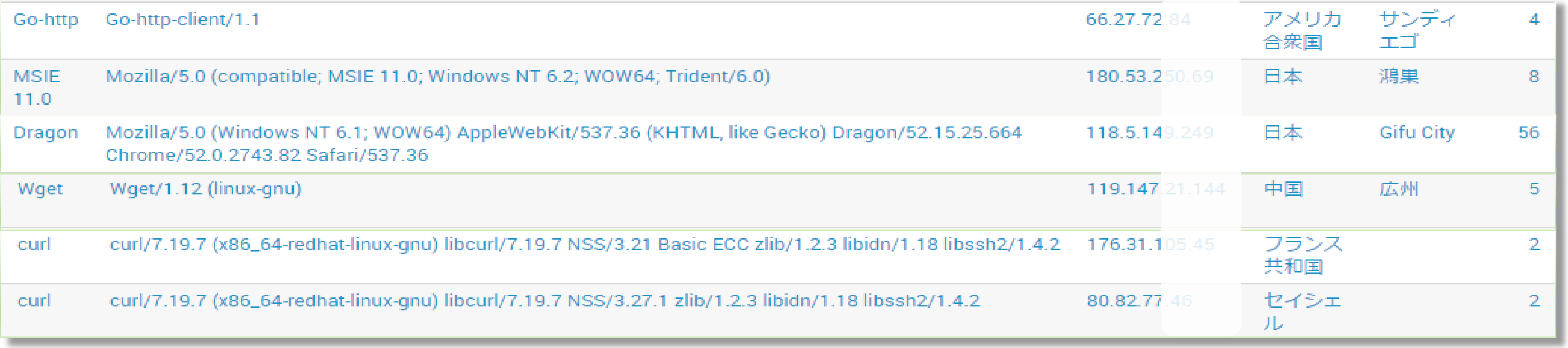
Country names

Sudden access from unusual countries shows potential attack

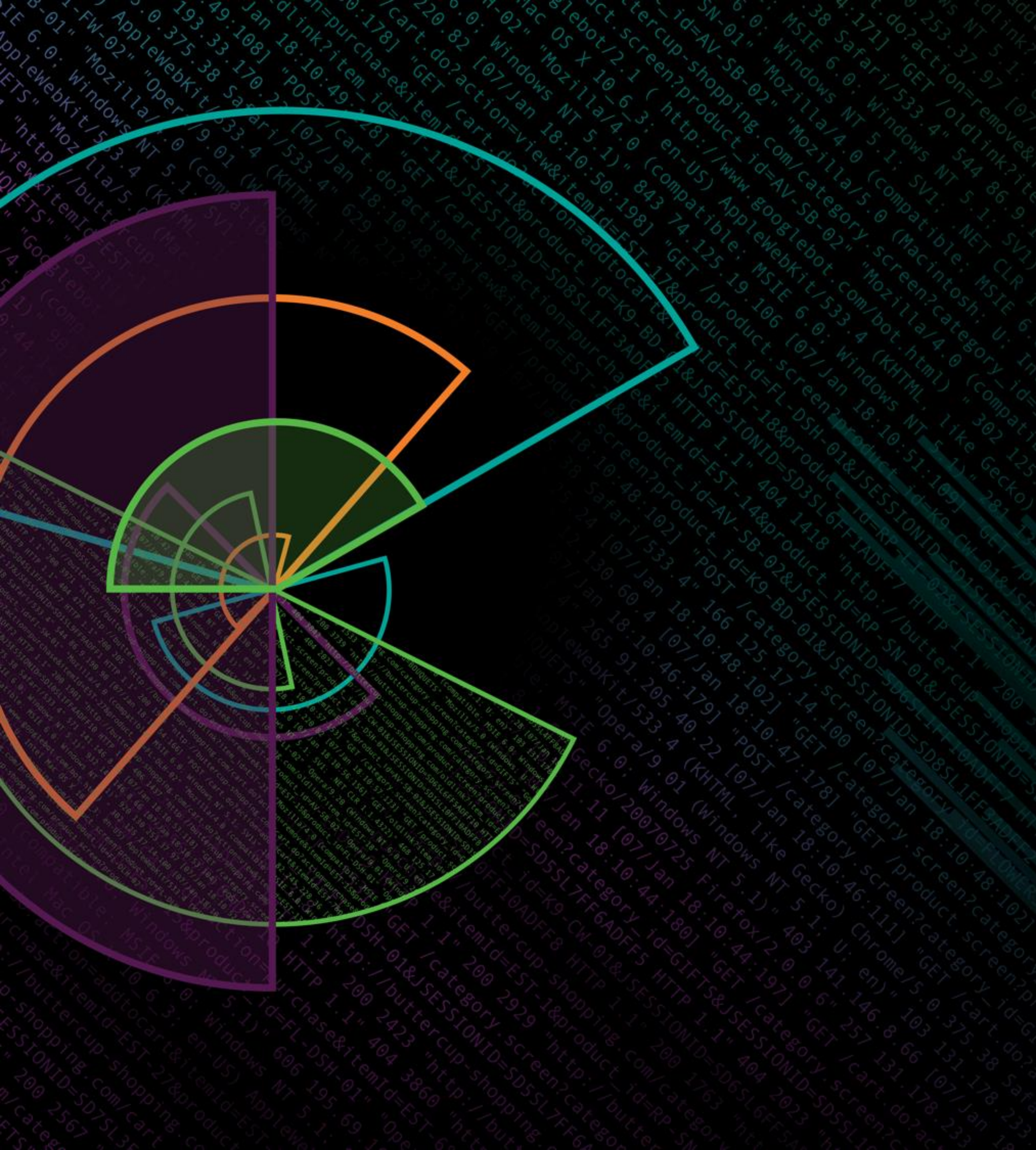
Detecting Suspicious Access

Monitor Useragent that regular browsers are not used

- Monitor suspicious Useragent as staged below, and block wrongful access if it is not legitimate
  - Unexciting UA such as IE11.0 （Formally rv:11.0）
  - Browser that is used by certain countries
  - Command system such as wget, curl. etc.
  - Suspicious tool such as Go-http and access from vulnerability scanners



Go-http	Go-http-client/1.1	66.27.72.84	アメリカ合衆国	サンディエゴ	4
MSIE 11.0	Mozilla/5.0 (compatible; MSIE 11.0; Windows NT 6.2; WOW64; Trident/6.0)	180.53.250.69	日本	鴻巣	8
Dragon	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Dragon/52.15.25.664 Chrome/52.0.2743.82 Safari/537.36	118.5.149.249	日本	Gifu City	56
Wget	Wget/1.12 (linux-gnu)	119.147.21.144	中国	広州	5
curl	curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.21 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2	176.31.105.45	フランス共和国		2
curl	curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.27.1 zlib/1.2.3 libidn/1.18 libssh2/1.4.2	80.82.77.46	セイシェル		2



How to Detect Phishing Site

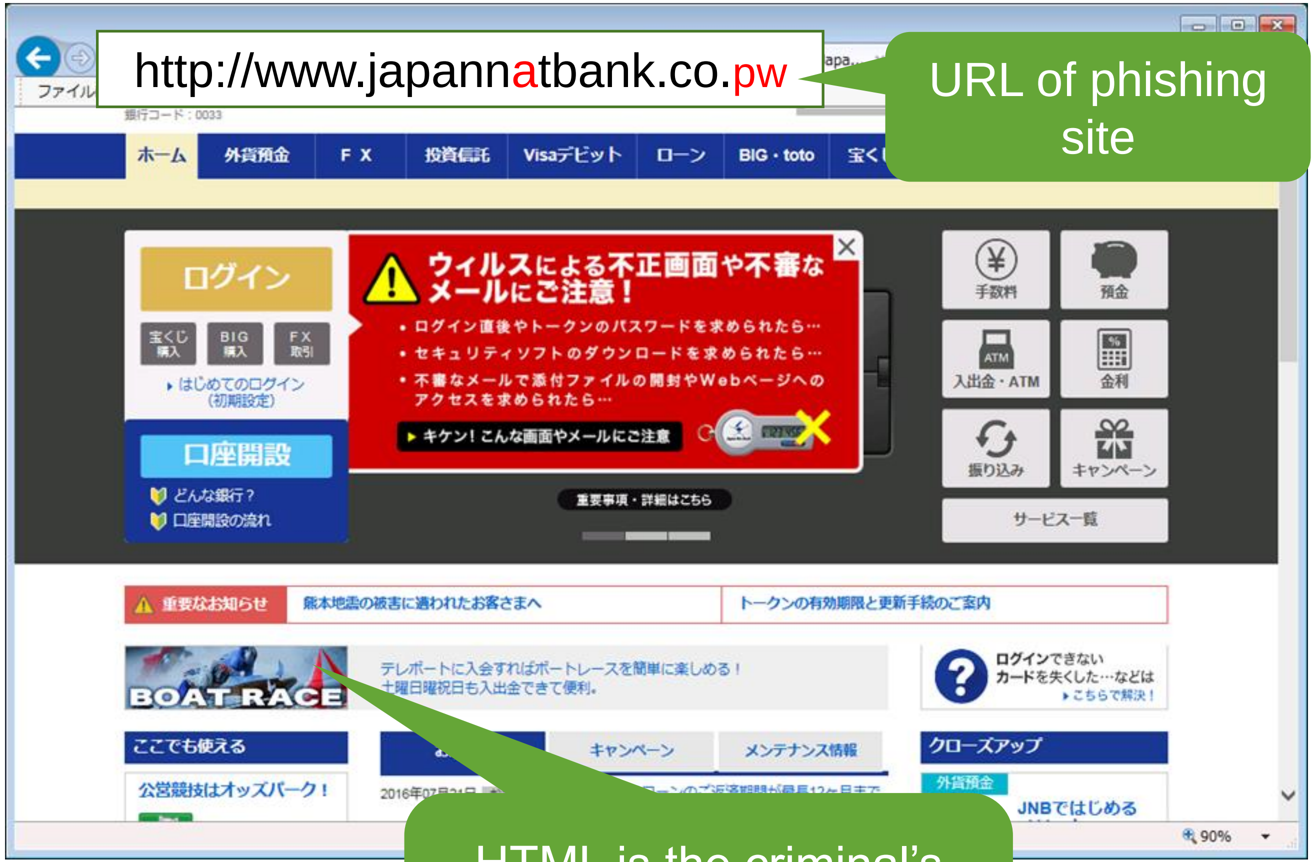
Finding out phishing site generated wrongfully from access logs

Detecting Phishing Site

Possible to find out before a criminal spreads out to the phishing site

- Check domain names of Referer that belong to online banking access log and confirm if there is any access from similar domain names that are similar to own domains.
- Most phishing sites are referring to original image, CSS, JS, etc. if so, URL of phishing site remains in Referer of original content's logs

Needs caution for requesting only images but not for html



http://www.japannatbank.co.pw

URL of phishing site

ウィルスによる不正画面や不審なメールにご注意！

- ログイン直後やトークンのパスワードを求められたら…
- セキュリティソフトのダウンロードを求められたら…
- 不審なメールで添付ファイルの開封やWebページへのアクセスを求められたら…

▸ キケン！こんな画面やメールにご注意

重要なお知らせ　熊本地震の被害に遭われたお客さまへ　トークンの有効期限と更新手続のご案内

テレボートに入会すればボートレースを簡単に楽しめる！
土曜日曜祝日も入出金できて便利。

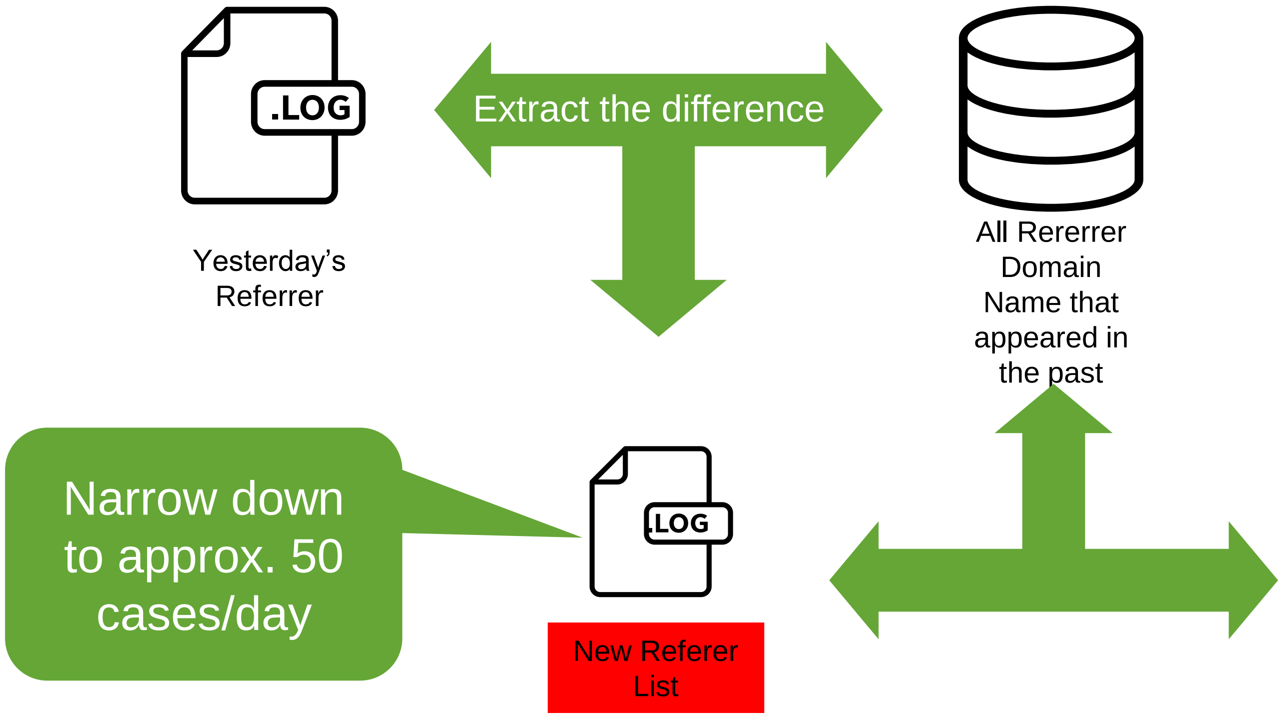
ログインできない
カードを失くした…などは
▸ こちらで解決！

HTML is the criminal's content, but the image is referred to the original

Detecting phishing site

How to analyze Referer

- Cannot check all Referer everyday, check by extracting **Referer domain names newly appeared the day before Referer** by using Title Get Tool



.LOG

Yesterday's Referrer

Extract the difference

All Rererrer Domain Name that appeared in the past

Narrow down to approx. 50 cases/day

.LOG

New Referer List

The result of Title Get Tool. If domain name is similar with the own domain or IP address, needs caution

New Referer	Page Title
http://100.100.50.50	Japan Net Bank
http://www.abc123.co.jp	-----
http://www.japannatbank.co.pw	Japan Net Bank

How to Handle Phishing Site

- Request National CERT to close phishing site
- Report unsafe sites from each browser
- Enter fake (Non-existing) account into phishing site, block access to use the fake account by using IP address
- Let Referer redirect the request with phishing site URL to another page prepared by bank
  - Even though customers have accessed to phishing site, it is still possible to display the bank’s page

Reference Gophish

Creating Phishing Site, Open Source to actualize campaign

Do Not Misuse! !

https://getgophish.com/

Open-Source Phishing Framework

Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.

For free.

- Detect if phishing site is created and confirm by using Gophish
- Function of Gophish
  - By scraping, targeted Web site can be copied
  - By spreading phishing mails, target with the clicked link can be managed
  - Fake log in screen at leading destination, exploit ID and password

Detecting Method of Taking over Accounts

Detect log into the illegitimate account by the third party

Detecting Hacked Account Logins

Analysis of Browser Language

- Confirm **Browser Language** per account at the time of login, and alert when the language is different from the ones in the past.
  - Detect potential account takeover every 15min and alert
  - You can obtain browser language from Request Header
  - Use caution if the provider is different from the ones the customers normally use

Account Num	IP Address	Lang	Country	Provider	Network	Term	Comment
001-1234567	202.***.***.15	ja-JP	Japan	S.Net	A Line	2016/9/3 - 2016/9/21	Same language and same provider
001-1234567	202.***.***.18	ja-JP	Japan	S.Net	A Line	2016/9/3 - 2016/9/21	Same language and same provider
001-1234567	202.***.***.54	ja-JP	Japan	S.Net	A line	2016/9/3 - 2016/9/21	Same language and same provider
001-1234567	114.***.***.192	xx-XX	Japan	O.Com	Z Line	2016/10/20 - 2016/10/20	Different language and Different provider

Detecting Hacked Account Logins

Analysis of Open Port IP

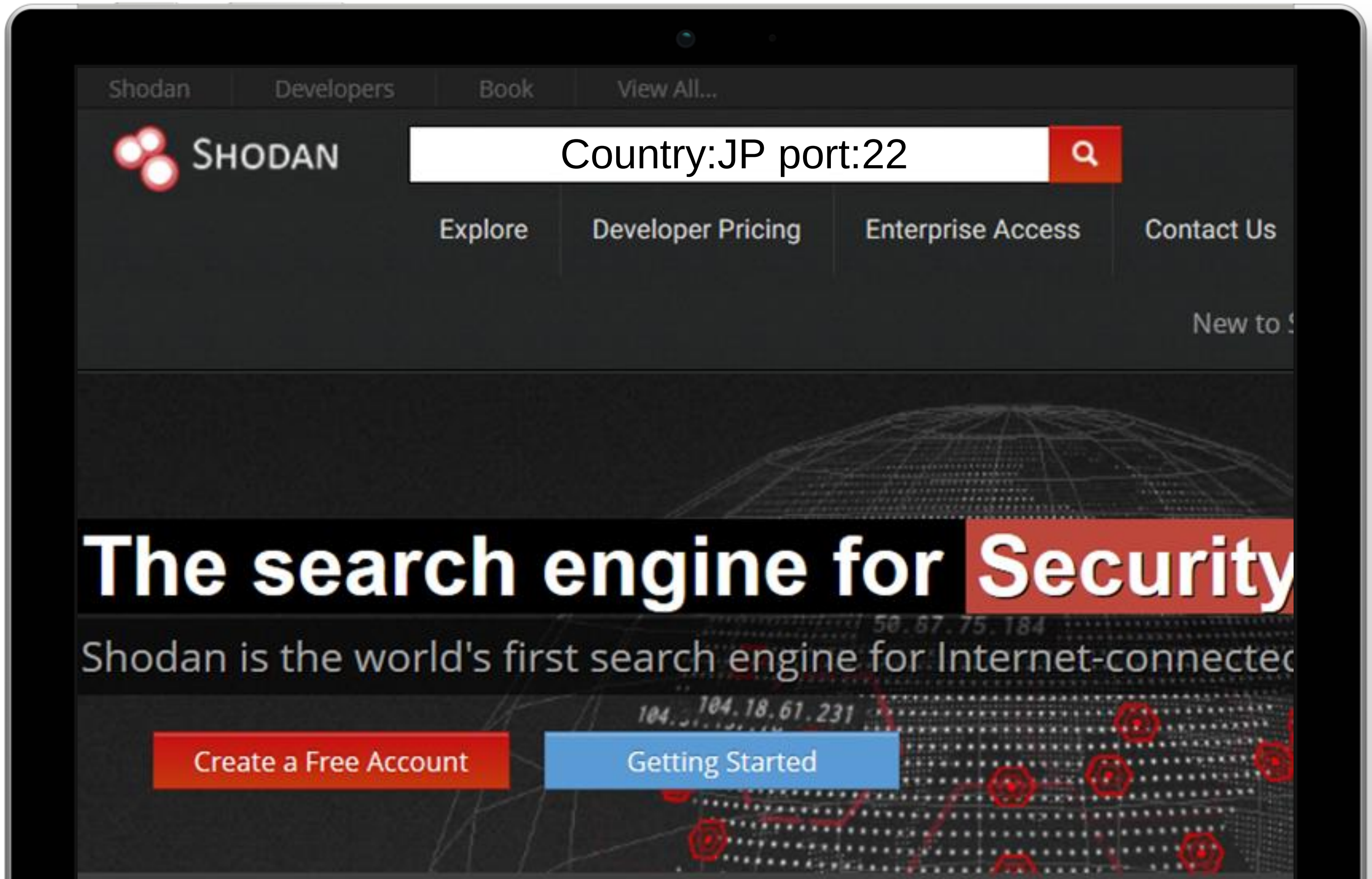
- Confirm if there is any designated **Open Port** to IP address at the time of login. Alert if the IP address has not been used in the past for each account
  - Since criminals often use VPS, someone else's server and router in order to access, there are cases that they might use IP address available remote Open Port as stated below
    - **22, 1723, 3389**
  - Schedule alert in every 15 minutes. Check all histories of login that occurred during the time You can obtain Open Port information from external site such as SHODAN, censys, etc.
  - **Confirm if the VPS is used by our customers or not**

Account Num	IP Address	Port	Country	Provider	Network	Term	Comment
001-1234567	202.***.***.15	-	Japan	S.Net	A Line	2016/9/3 - 2016/9/21	No Open Port
001-1234567	202.***.***.18	-	Japan	S.Net	A Line	2016/9/3 - 2016/9/21	No Open Port
001-1234567	202.***.***.54	-	Japan	S.Net	A line	2016/9/3 - 2016/9/21	No Open Port
001-1234567	114.***.***.192	22	Japan	VPS	Z Line	2016/10/20 - 2016/10/20	Open Port, Suspicious VPS

Reference SHODAN

Able to obtain various information related to IP address

https://www.shodan.io/



Shodan
Developers
Book
View All...

SHODAN

Country:JP port:22

Explore
Developer Pricing
Enterprise Access
Contact Us

New to S

The search engine for Security

Shodan is the world's first search engine for Internet-connected

Create a Free Account
Getting Started

- Download IP address list in Open Port and import to Splunk in order to leverage
- Or it can be done by requesting API of SHODAN from Splunk

Detecting Hacked Account Logins

Analysis of Cookie

- Issue Unique **Key Value** per **Cookie**, Check log into multiple accounts by the same key value（Same Key Value＝Same Terminal／Same Browser）
  Alert if the same terminal is used to log into multiple accounts
  - It is extremely unusual to log into multiple accounts from the same terminal/same browser since each one has the same single account
    - If it is used within the same company or same family and share PC, there is no issue. Thus it is excluded from alert
  - Schedule alert for every 15 minutes. Check all histories of log in that are occurred every 60 minutes
  - Various hacking cases are detected. For example, commonly purchasing accounts, etc.

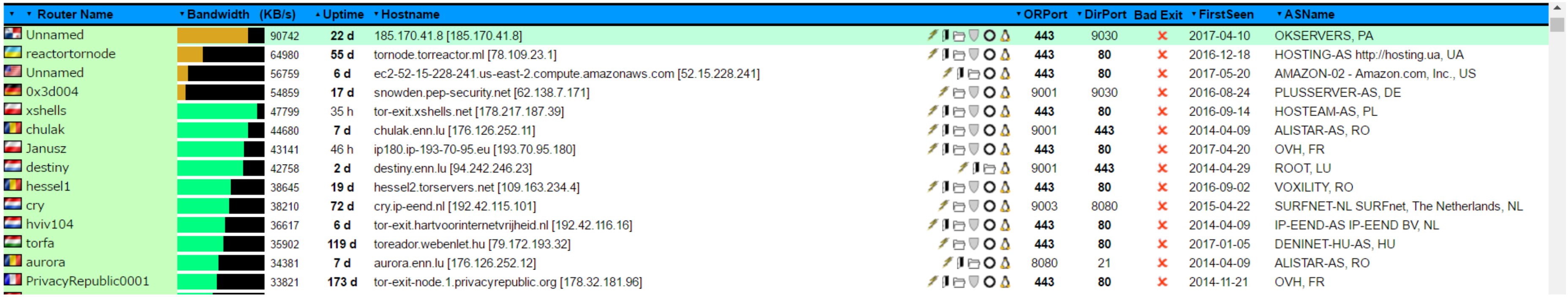
Account Num	IP Address	Key Value	Country	Provider	Network	Term	Comment
001-1234567	202.***.***.15	ZF09UYXS09122	Japan	S.Net	A Line	2016/10/20 15:30:00	Same Key in Cookie
002-2234568	202.***.***.15	ZF09UYXS09122	Japan	S.Net	A Line	2016/10/20 15:32:00	Same Key in Cookie
003-3234569	202.***.***.15	ZF09UYXS09122	Japan	S.Net	A Line	2016/10/20 15:34:00	Same Key in Cookie
004-4234560	202.***.***.15	ZF09UYXS09122	Japan	S.Net	A Line	2016/10/20 15:36:00	Same Key in Cookie

Detecting Hacked Account Logins

Analysis of Tor IP Address

- Confirm if the IP address used when the time of log is **Node Address of Tor** Set alert if there is no history of using Tor per account in the past.
  - Regular customers barely use Tor
  - Schedule alert in every 15 minutes. Check all histories of log in that occurred during the time
  - Exit Node of Tor Address information is able to obtain from external site below
  - In general, Various cases are found to use someone else's accounts such as financial crime, fraud. Etc.

https://torstatus.blutmagie.de/



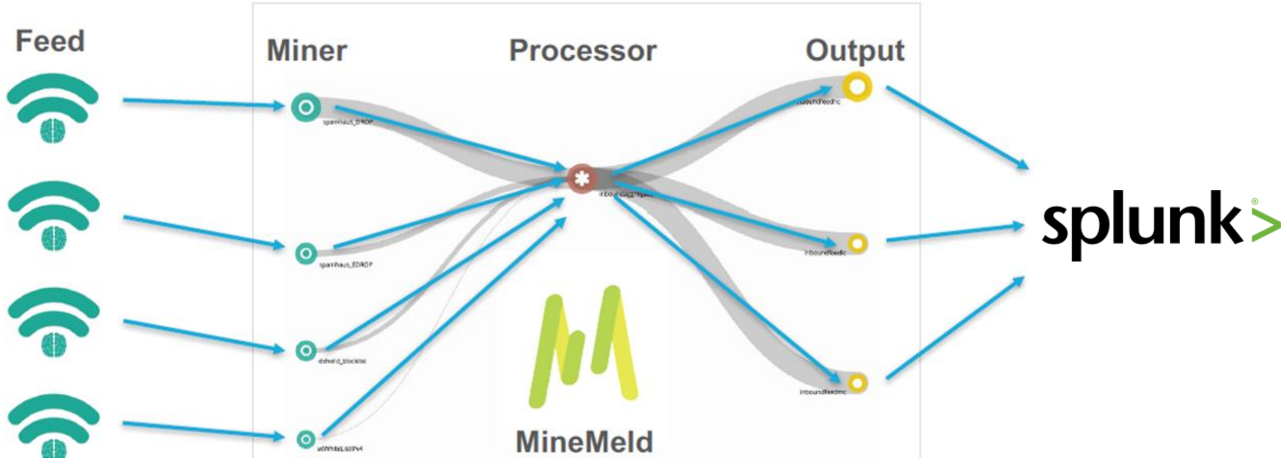
Router Name	Bandwidth (KB/s)	Uptime	Hostname	ORPort	DirPort	Bad Exit	FirstSeen	ASName
Unnamed	90742	22 d	185.170.41.8 [185.170.41.8]	443	9030	✗	2017-04-10	OKSERVERS, PA
reactortornode	64980	55 d	tornode.torreactor.ml [78.109.23.1]	443	80	✗	2016-12-18	HOSTING-AS http://hosting.ua, UA
Unnamed	56759	6 d	ec2-52-15-228-241.us-east-2.compute.amazonaws.com [52.15.228.241]	443	80	✗	2017-05-20	AMAZON-02 - Amazon.com, Inc., US
0x3d004	54859	17 d	snowden.pep-security.net [62.138.7.171]	9001	9030	✗	2016-08-24	PLUSSERVER-AS, DE
xshells	47799	35 h	tor-exit.xshells.net [178.217.187.39]	443	80	✗	2016-09-14	HOSTEAM-AS, PL
chulak	44680	7 d	chulak.enn.lu [176.126.252.11]	9001	443	✗	2014-04-09	ALISTAR-AS, RO
Janusz	43141	46 h	ip180.ip-193-70-95.eu [193.70.95.180]	443	80	✗	2017-04-20	OVH, FR
destiny	42758	2 d	destiny.enn.lu [94.242.246.23]	9001	443	✗	2014-04-29	ROOT, LU
hessel1	38645	19 d	hessel2.torservers.net [109.163.234.4]	443	80	✗	2016-09-02	VOXILITY, RO
cry	38210	72 d	cry.ip-eend.nl [192.42.115.101]	9003	8080	✗	2015-04-22	SURFNET-NL SURFnet, The Netherlands, NL
hviv104	36617	6 d	tor-exit.hartvoorinternetvrijheid.nl [192.42.116.16]	443	80	✗	2014-04-09	IP-EEND-AS IP-EEND BV, NL
torfa	35902	119 d	toreador.webenlet.hu [79.172.193.32]	443	80	✗	2017-01-05	DENINET-HU-AS, HU
aurora	34381	7 d	aurora.enn.lu [176.126.252.12]	8080	21	✗	2014-04-09	ALISTAR-AS, RO
PrivacyRepublic0001	33821	173 d	tor-exit-node.1.privacyrepublic.org [178.32.181.96]	443	80	✗	2014-11-21	OVH, FR

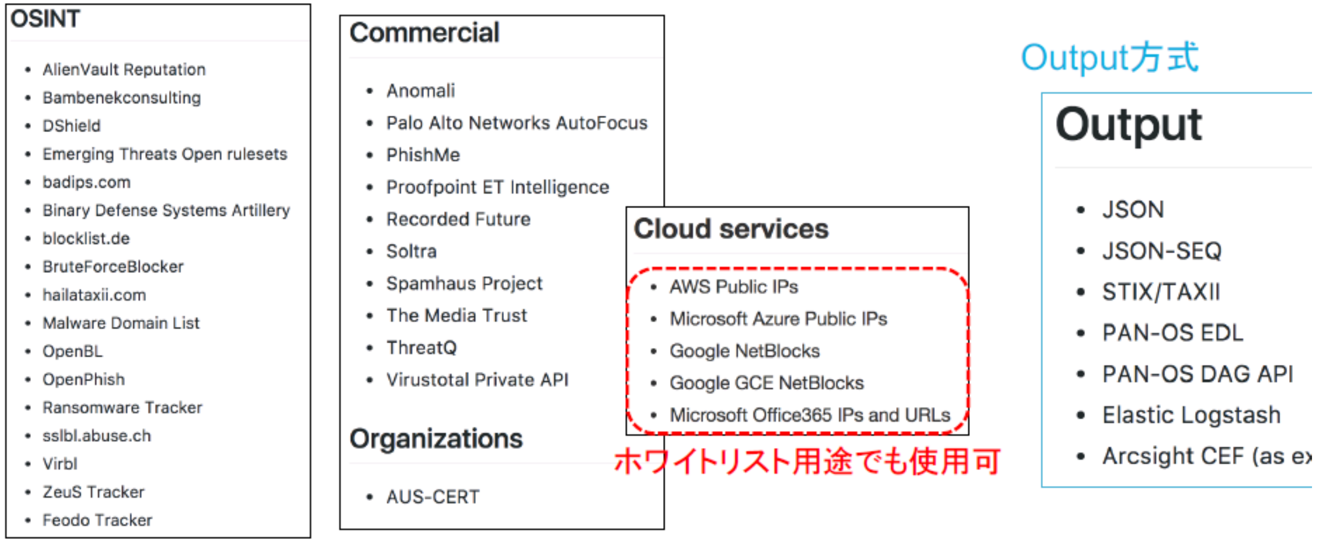
Reference MINEMELD

https://github.com/PaloAltoNetworks/minemeld

Opensource that can be automatically gathered IOC from various sites

- As a default, MINEMELD is corresponding to various IOC delivered WEB site (Feed)
- Install REST Apps into Splunk, Obtain IOC from Output node of MINEMELD
- By collaborating with MINEMELD, possible for autorenewal of Tor Node list imported to Splunk





OSINT

- AlienVault Reputation
- Bambenekconsulting
- DShield
- Emerging Threats Open rulesets
- badips.com
- Binary Defense Systems Artillery
- blocklist.de
- BruteForceBlocker
- hailataxii.com
- Malware Domain List
- OpenBL
- OpenPhish
- Ransomware Tracker
- sslbl.abuse.ch
- Virbl
- ZeuS Tracker
- Feodo Tracker

Commercial

- Anomali
- Palo Alto Networks AutoFocus
- PhishMe
- Proofpoint ET Intelligence
- Recorded Future
- Soltra
- Spamhaus Project
- The Media Trust
- ThreatQ
- Virustotal Private API

Organizations

- AUS-CERT

Cloud services

- AWS Public IPs
- Microsoft Azure Public IPs
- Google NetBlocks
- Google GCE NetBlocks
- Microsoft Office365 IPs and URLs

ホワイトリスト用途でも使用可

Output方式

Output

- JSON
- JSON-SEQ
- STIX/TAXII
- PAN-OS EDL
- PAN-OS DAG API
- Elastic Logstash
- Arcsight CEF (as ex

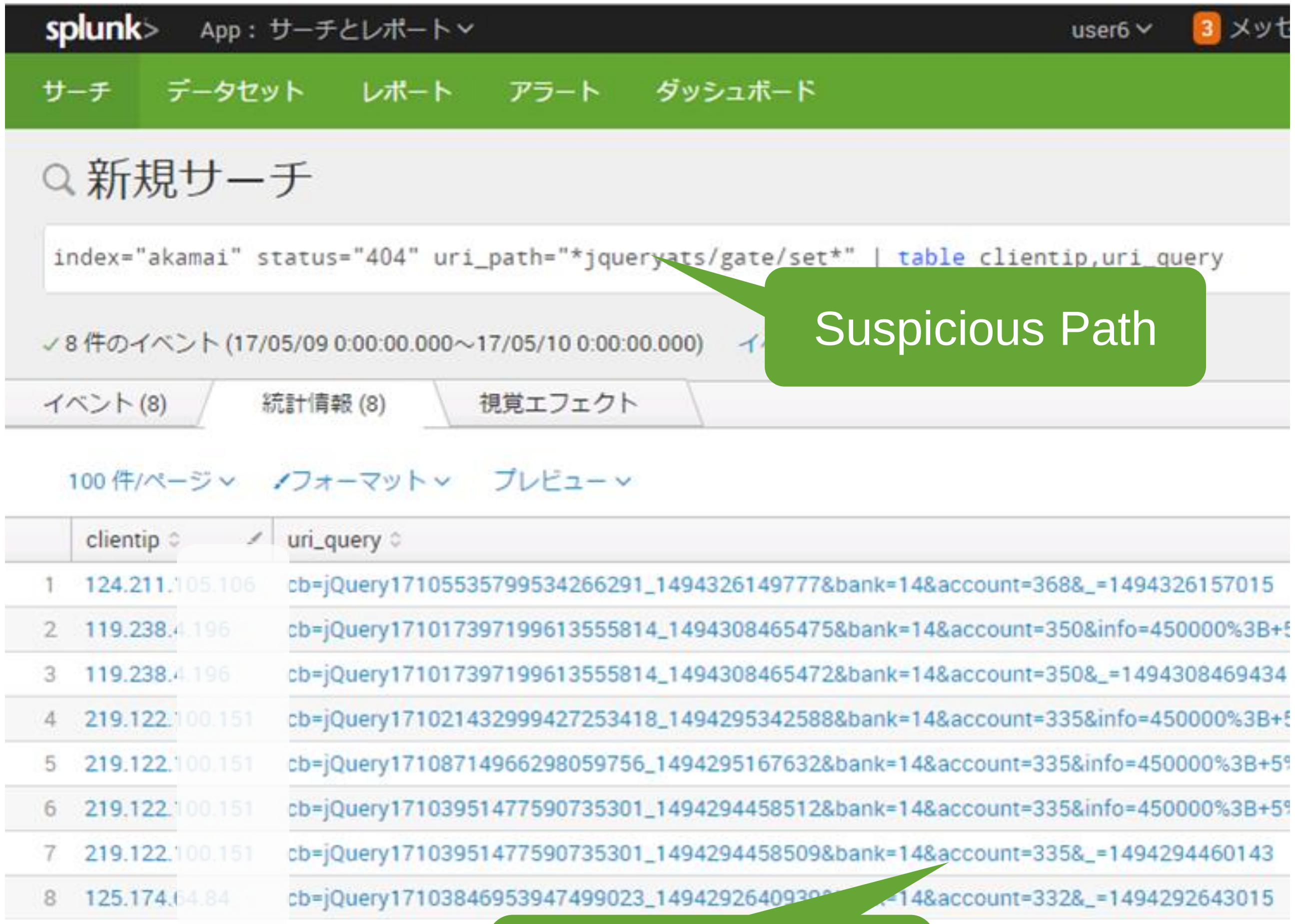
How to Detect the Infection of Banking Trojan

Detect if the customer’s PC is infected by banking trojan

Detection of Infection to Banking Trojan

Detect if a customer is infected by banking trojan

- If the terminal is infected by banking trojan, it requests for **non-existing path** of bank WEB site /jqueryats/, /uejei3j/, /iimgc/, etc.
- By analyzing the request for 404 status, we recognized there were many requests for same path
- Suspicious parameters such as bank= and account= Query Parameter are attached to query parameters



```
index="akamai" status="404" uri_path="*jqueryats/gate/set*" | table clientip,uri_query
```

✓8 件のイベント (17/05/09 0:00:00.000～17/05/10 0:00:00.000)

	clientip	uri_query
1	124.211.105.106	cb=jQuery17105535799534266291_1494326149777&bank=14&account=368&_=1494326157015
2	119.238.4.196	cb=jQuery171017397199613555814_1494308465475&bank=14&account=350&info=450000%3B+5
3	119.238.4.196	cb=jQuery171017397199613555814_1494308465472&bank=14&account=350&_=1494308469434
4	219.122.100.151	cb=jQuery171021432999427253418_1494295342588&bank=14&account=335&info=450000%3B+5
5	219.122.100.151	cb=jQuery17108714966298059756_1494295167632&bank=14&account=335&info=450000%3B+5
6	219.122.100.151	cb=jQuery17103951477590735301_1494294458512&bank=14&account=335&info=450000%3B+5
7	219.122.100.151	cb=jQuery17103951477590735301_1494294458509&bank=14&account=335&_=1494294460143
8	125.174.64.84	cb=jQuery17103846953947499023_14942926409[illegible]14&account=332&_=1494292643015

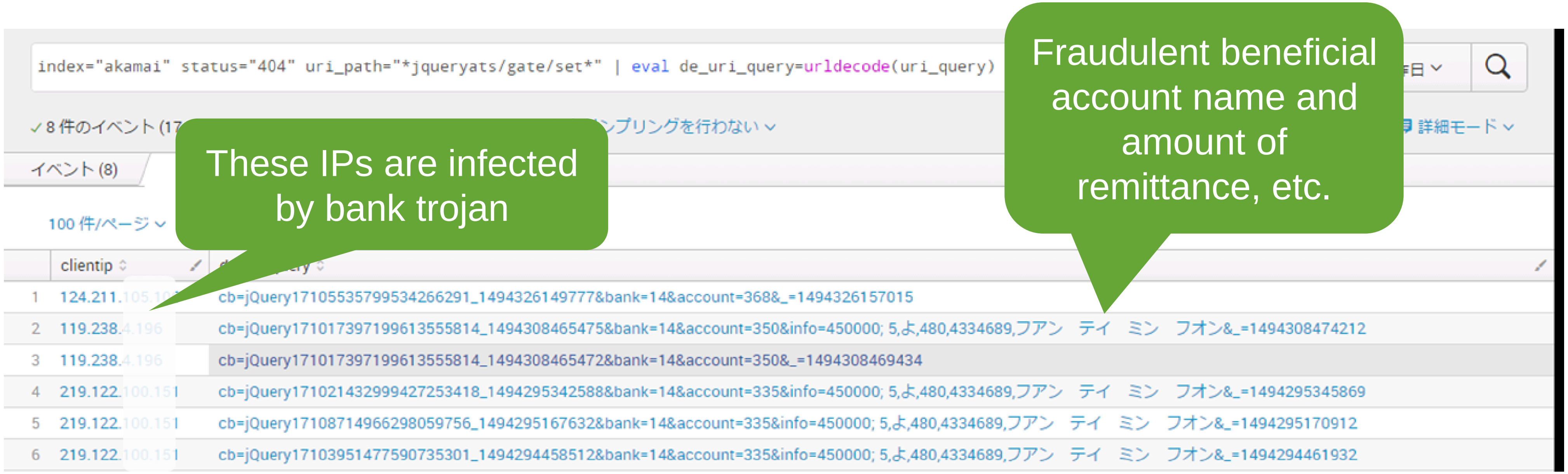
Suspicious Path

Suspicious Query Parameter

Detection of Banking Trojan Infection

Detect if a customer is infected by banking trojan

- Recognized that fraudulent beneficial information was included once query parameter was URL decoded
- All Destination IP Addresses requesting for this pass have terminals infected by banking trojan
- Within status 404 request, needs caution for any requests with suspicious query parameters such as **account=, password=,** etc.



```
index="akamai" status="404" uri_path="*jqueryats/gate/set*" | eval de_uri_query=urldecode(uri_query)
```

	clientip	de_uri_query
1	124.211.105.10	cb=jQuery17105535799534266291_1494326149777&bank=14&account=368&_=1494326157015
2	119.238.4.196	cb=jQuery17101739719961355814_1494308465475&bank=14&account=350&info=450000; 5,よ,480,4334689,フアン　テイ　ミン　フオン&_=1494308474212
3	119.238.4.196	cb=jQuery17101739719961355814_1494308465472&bank=14&account=350&_=1494308469434
4	219.122.100.151	cb=jQuery17102143299427253418_1494295342588&bank=14&account=335&info=450000; 5,よ,480,4334689,フアン　テイ　ミン　フオン&_=1494295345869
5	219.122.100.151	cb=jQuery17108714966298059756_1494295167632&bank=14&account=335&info=450000; 5,よ,480,4334689,フアン　テイ　ミン　フオン&_=1494295170912
6	219.122.100.151	cb=jQuery17103951477590735301_1494294458512&bank=14&account=335&info=450000; 5,よ,480,4334689,フアン　テイ　ミン　フオン&_=1494294461932

These IPs are infected by bank trojan

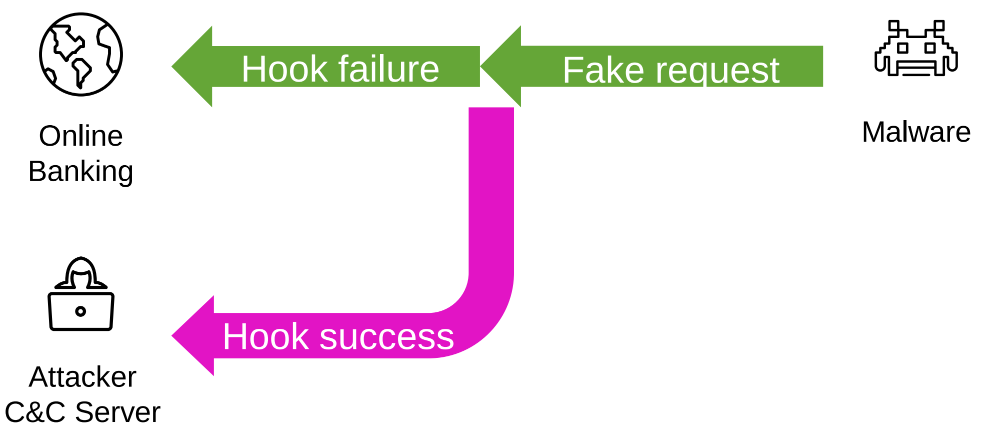
Fraudulent beneficial account name and amount of remittance, etc.

Reference Request for Banking Trojan

The reason why Banking tojan sends a request to Banking Site

- Banking trojan is pretending to be transmitting to bank server for the transmission of C&C server (Request to **jqueryats**, etc.)
- Disguised transmission is hooked by banking trojan and yielded to C&C server, yet it ends up as failure by depending upon the end-user's environment
- If it is failure, it just requests to bank server

https://login.japannetbank.co.jp/**jqueryats**/…



Online Banking

Hook failure

Fake request

Malware

Attacker C&C Server

Hook success

Key Takeaways

- Analysis Points for log collection
  - Most of normal traffic logs should be excluded from aggregate result with white list
- How fast to detect appearances of your phishing site
  - Leverage Refere-domain field and identify if it is phisling site or not
- How fast to detect hacked accounts
  - Browser langueage gives us hints for each accounts
  - Leverage cookie information if the customers' PC is used by multiple users
- How fast to detect banking malware on PCs
  - Check if there are many requests to non-exsisting path of your bank web site

Thank You

Don't forget to rate this session in the .conf18 mobile app