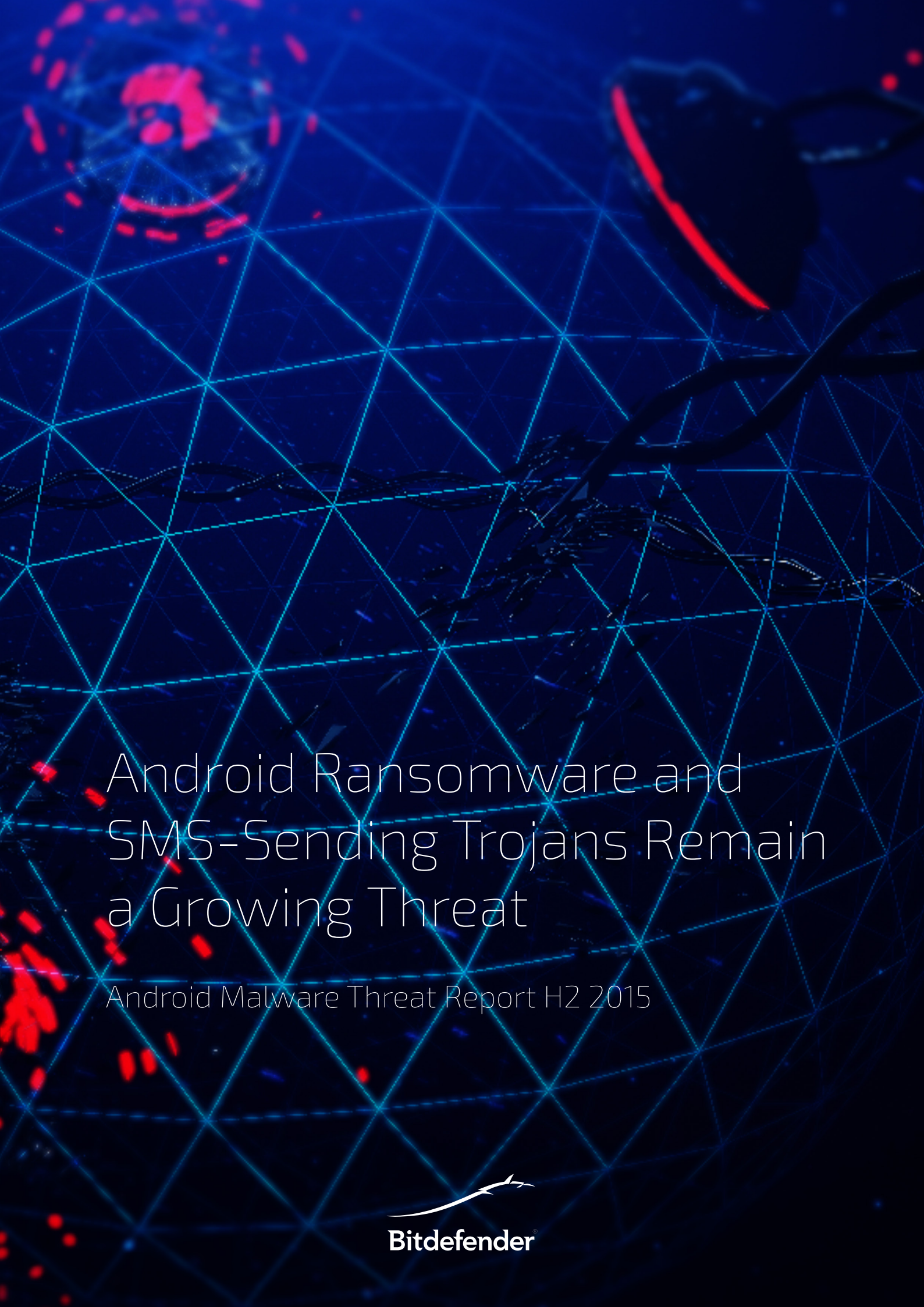

Android Ransomware and SMS-Sending Trojans Remain a Growing Threat

Android Malware Threat Report H2 2015

Bitdefender

Contents

Author

Liviu Arsene – Senior E-Threat Analyst

Technical information provided courtesy of Bitdefender Labs.

Executive summary

Ransomware has been plaguing Windows PC for the past couple of years, but recently it seems to have developed platform-agnostic capabilities and has moved towards Linux and Android.

While not yet as advanced as its Windows counterpart, Android ransomware can still cause massive headaches, disruptions and financial losses. Bitdefender Android telemetry shows the Android.Trojan.Slocker ransomware family ranked first in UK, German and Australian charts, based on the number of devices that reported it.

Android ransomware could be considered more important than it's PC counterpart because mobile devices have access to and store a lot of personal and even corporate data that's usually not backed up. Losing that data or simply being denied access to it could be irreversible and users would be far more inclined to pay to recover their contacts, conversations, pictures and documents.

Key Findings:

- 19.55 percent of global threats are fake apps that install malware or highly aggressive adware;
- 45.53 percent of all globally reported Android ransomware points to the US;
- 78.36 percent of all globally SMS-sending malware targets the US;
- Ransomware ranks first in Germany, UK and Australia top threats;

Ransomware is Good Business

A Bitdefender study conducted in November 2015 revealed that ransomware victims would be willing to pay up to **$500 to recover their data**.

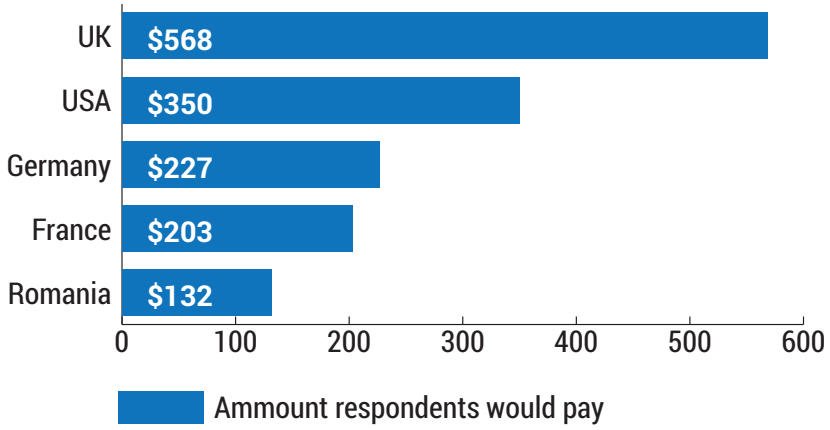

Fig. 1 – Amount of money respondents would pay to recover their data

Regardless of whether it is Android ransomware, PC ransomware, or even Linux ransomware, malware-as-a-service has become a financially driven industry that's willing and able to supply malware to anyone who will pay for it.

For instance, the Cryptolocker/Cryptowall ransomware kit for PCs is being reportedly sold for as little as **$3,000,** and with various business models that favor both the customer and the malware developers. The return on investment could be stellar if an effective distribution method is found and many victims are infected.

```
Information for customers:
- JID: whiterocks@[redacted].org
- Price of binary: $400 (8/1 customers)
- Price of source code and manual how edit code wallet btc i give you: $3000 (1 customer)
- You keep 100% of payments
- Free recompiles and support
- Escrow accepted
- Bitcoin (BTC) only!

- VPS or dedi required - we can recommend servers
- Additional binary which decrypts files (key required)
```

Fig. 2 - Cryptolocker/Cryptowall ransomware kit selling information

Linux ransomware is the latest thing to have made an entrance and, although it has been easily dismissed by security researchers as prone to encryption vulnerabilities that allow the recovery of data without paying the ransom, they do agree that future iterations could be far more complex and versatile.

With Linux-powered servers running most of the internet's infrastructure, the consequences of ransomware infections locking down webservers could be more disruptive than anticipated.

As for Android, the mobile operating system with the largest market share, ransomware has also been spotted attempting to lock devices and becoming increasingly more difficult to remove from one iteration to another.

Android Device Proliferation

The number of worldwide Android devices has been growing steadily for the past couple of years, with shipment volumes estimated to have topped **1.2 billion units in 2015**. In 2014, the same shipment volumes were estimated at around 1.1 billion. This steady proliferation of Android devices – while no longer as accelerated as during previous years – does mean that a huge number of device out there are all running Google's mobile OS.

Vendor	2015 Shipment Volumes	2015 Market Share	2014 Shipment Volumes	2014 Market Share	Year-Over-Year Growth
1. Samsung	324.8	22.7%	318.2	24.4%	2.1%
2. Apple	231.5	16.2%	192.7	14.8%	20.2%
3. Huawei	106.6	7.4%	73.8	5.7%	44.3%
4. Lenovo	74.0	5.2%	59.4	4.6%	24.5%
5. Xiaomi	70.8	4.9%	57.7	4.4%	22.8%
Others	625.2	43.6%	599.9	46.1%	4.2%
Total	**1,432.9**	**100.0%**	**1,301.7**	**100.0%**	**10.1%**
Lenovo + Motorola	73.9	5.16%	93.7	7.20%	-21.1%

Fig. 3 - Source: IDC

As more people embrace Android and contribute to an ever-increasing market share, malware developers are also turning to it to maximize profit. Malware has seen the same development trend as PC malware years back. If at first malware coders were developing threats that were more of a nuisance than damaging, today's PC threats are as serious as they get.

Android is much like that in this respect and its **81 percent market share in 2015** encourages malware developers to tackle the mobile OS platform with threats designed to covertly collect data or financially extort victims.

Android Ransomware Evolution

Because the Android operating system is more permissive than other mobile operating systems, allowing users to sideload applications from untrusted or unauthorized sources, it also opened up the platform to new threats.

Some of the most notorious Android ransomware variants have also made it in the media, although the number of victims being affected at the time was pretty narrow. From simple apps that just display scareware, ransomware has advanced to the point where command and control servers are used to deliver instructions to each victim, receive personal information, and push updates to infected devices.

1. Fake Applications and Scareware

One of the first ransomware variants on Android was spotted in 2013. While it wasn't as sophisticated as its PC counterpart, it's purpose was to pose as a legitimate application – usually a security solution – and scare users into thinking their device is infected with some form of data-stealing malware.

```
private void showSuccessDialog(BaseActivity paramBaseActivity)
{
  paramBaseActivity = new AlertDialog.Builder(paramBaseActivity);
  paramBaseActivity.setTitle("MoneyPak information");
  paramBaseActivity.setMessage("Your payment accepted. Thank you.").setCancelable(false).setPositiveButton("OK", new DialogInterface.OnClickListener()
  {
    public void onClick(DialogInterface paramAnonymousDialogInterface, int paramAnonymousInt)
    {
      MPActivity.this.makeMeHome();
    }
  });
  paramBaseActivity.create().show();
}
```

Fig.4 - Android.Fakedefender.B sample showing MoneyPack payment method

"Fixing" those threats would require purchasing the "full license" of the so-called security solution to remove all identified malware. Of course, if the average users tried to manually remove the fake application, he would find that he couldn't kill the process.

The malware development group behind the Reveton / IcePol ransomware for PCs was also developing something similar for Android. Dubbed Android.Trojan.Koler.A, this Android ransomware variant pretended to be a video player that promised premium access to pornographic content.

Unlike its Windows counterpart, Android ransomware does require user interaction for sideloading the malicious .apk file, stirring suspicion for advanced users but still tricking less tech-savvy victims.

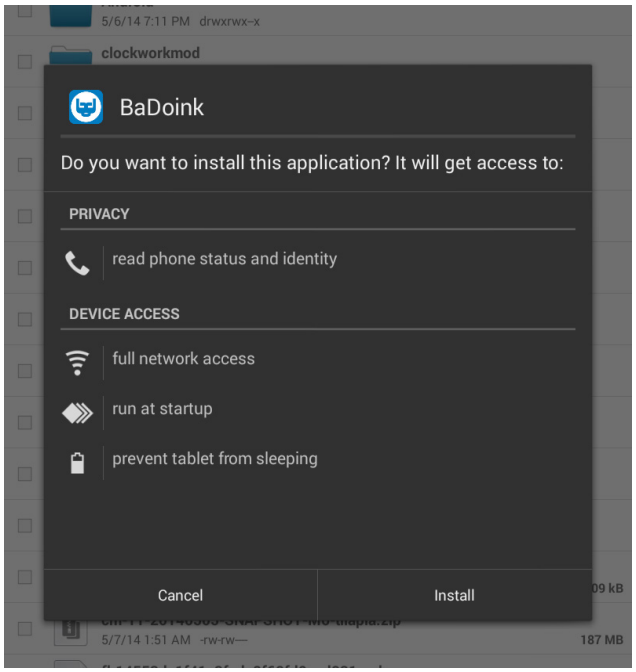

Fig. 5 - Android.Trojan.Koler.A permission screen during installation.

Once installed, it started sending the victim's IMEI number to the command and control server and then fetched a .HTML webpage that displayed a message related to how much the victim should pay to regain access to their device.

Because the actual message was displayed in a browser window on top of the home screen, removing the application was only a matter of quickly uninstalling it before it pushed the pop-up again or by booting the device in Safe Mode and removing it from there.

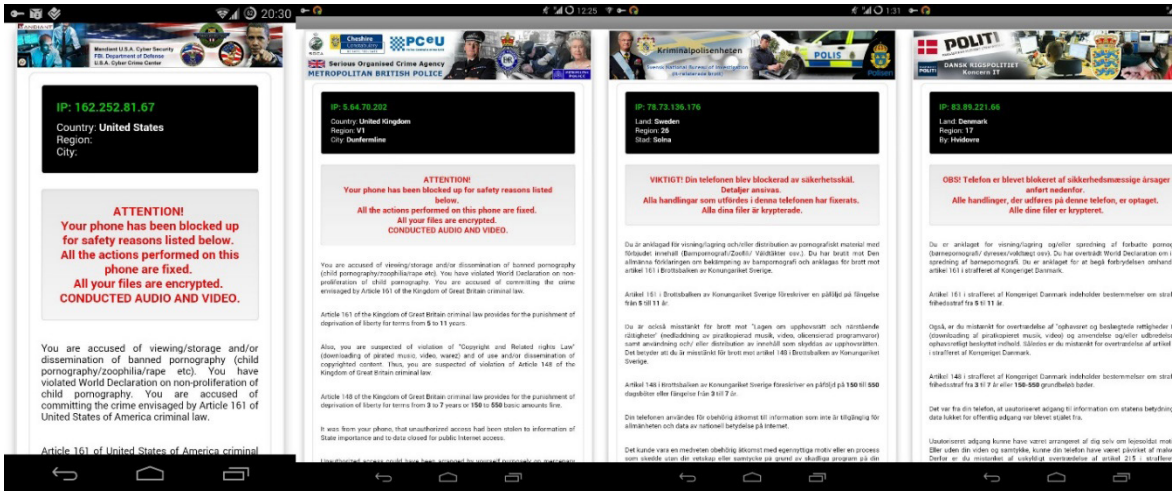

Fig. 6 - Android.Trojan.Koler.A ransom messages localized based on IP region.

While this variant didn't actually encrypt any on-device data, it proved that malware coders were interested in targeting Android next, using the same scareware tactics.

2. PIN Lockers

Another leap in innovation involved the emergence of what we call PIN Locker, a type of ransomware that changes the device's PIN lock and demands around **$500 to unlock** it.

By posing as a system update notification, it tries to obtain device administrator privileges and change the PIN lock with a randomly generated one. If until now ransomware was all about a ransom window constantly brought forward to intimidate users into paying, this new approach was far more devious.

Regaining access to the device without losing all stored data would have required the device to have been previously rooted or for an MDM solution to have been present before the infection. If the device was rooted, it was simply a matter of connecting the device by ADB (Android Debug Bridge) and deleting the file containing the PIN (e.g. password.key). Otherwise, resetting the device to factory settings would have been the only way to regain access to it.

3. File Encryptors

Perhaps one of the few Android ransomware samples that closely resembles the PC version – in terms of actually encrypting files – was dubbed by the media as Simplelocker. As the first of its kind, the ransomware exhibited a high degree of maturity in terms of development.

Security restrictions built into the Android OS prevented the malware from encrypting files stored on the device's internal memory, but the ransomware could encrypt data stored on external SD memory cards. Since users often rely on such SD cards to extend their storage capacity, the ransomware had the potential to affect a lot of victims.

Distribution and Attack Vectors

While one of the most popular distribution mechanisms remains third-party marketplaces, there have been instances where **malware creeped its way into Google Play**. Several instances of CAPTCHA-bypassing Android malware have been reported in Google's official marketplace, two of them having between **100,000 and 500,000 installs each**.

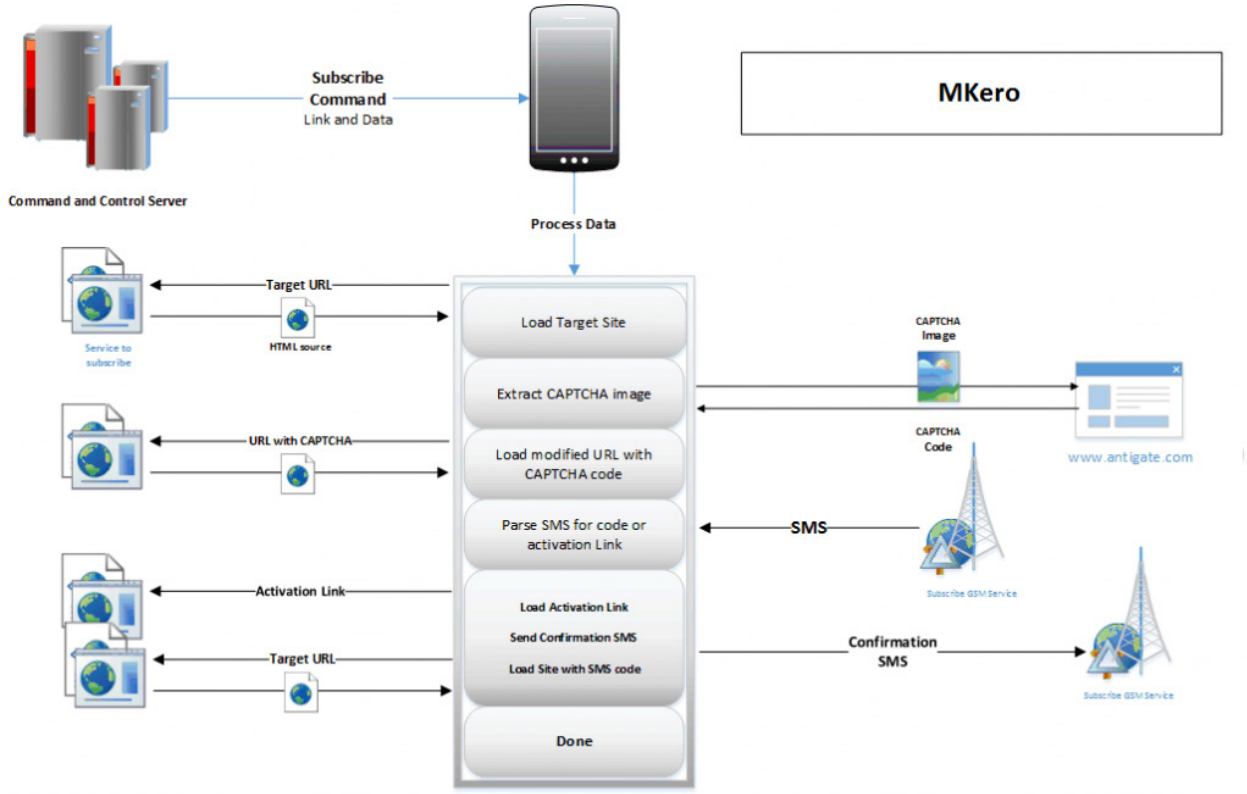

Fig. 7 – CAPTCHA-bypassing mechanism for Android.Trojan.MKero.A

Besides subscribing users to premium rated services, it also employed some highly advanced obfuscation techniques designed to hide classes, functions, and command and control servers from where it received instructions.

```
String source = MkProcess.this.Helper.select(element, MkOpen$MkSource$2.a("\u0442\u34d4\u93ea\u1630\udf03\uf314"));
if (source != null) {
    String[] sor = source.split(MkOpen$MkSource$2.a("\u041c\u34f6\u93d4\u166f"));
    intent = new Intent(MkProcess.this.getApplicationContext(), MkSource.class);
    intent.putExtra(MkOpen$MkSource$2.a("\u0444\u34c9\u93f3"), sor[0]);
    intent.putExtra(MkOpen$MkSource$2.a("\u045c\u34d4\u93fb\u1627"), sor[1]);
    a = MkOpen$MkSource$2.a("\u0443\u34de\u93f9\u1627\udf12\uf314\ua202");
    if (sor[2].equals(MkOpen$MkSource$2.a("\u045f\u34ce\u93f3\u162e"))) {
        str = BuildConfig.FLAVOR;
    } else {
        str = sor[2];
    }
    intent.putExtra(a, str);
    intent.putExtra(MkOpen$MkSource$2.a("\u0455\u34d4\u93f2\u1623\udf09\uf31f"), domain);
    MkProcess.this.getApplicationContext().startService(intent);
}
```

Fig. 8 - MKero obfuscated strings

Other delivery methods for Android ransomware involved spam messages and hoping that they'll be read by users of Android devices. Bitdefender detected more than **15,000 spam emails** that also include zipped files, the ransomware demanding $500 to restore access to the device.

Fig. 9 – Email sample with Ransomware .apk file attachment

While ransomware was not usually distributed via malvertising campaigns, during 2015 there were reports of infected Android apps being distributed via in-app ads that directed users to third-party marketplaces. Since the PC counterpart has been known to infect victims via this method, it's safe to assume that Android ransomware will soon be distributed the same way.

How Victims React to Ransomware

A study conducted by Bitdefender revealed that 50 percent of US ransomware victims have actually paid the extortionists. While Americans are the ones most willing to pay, French and Romanian are close behind, with 44 percent and 48 percent, respectively, showing the same behavior.

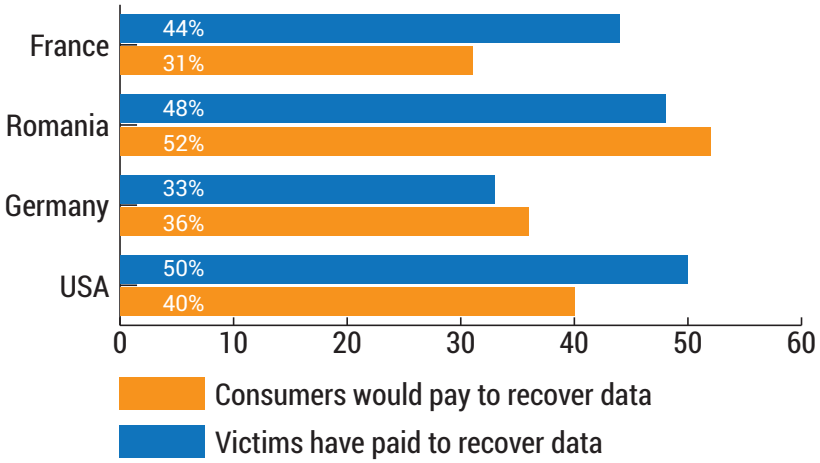

Fig. 10 – How victims react to ransomware

Top Android Malware Families during Second Half of 2015

Some of the most popular malware families spotted globally during H2 relate to ransomware, SMS-sending applications and Trojans aimed at stealing on-device data. The overall feeling for H2 2015 is that Android malware developers have been focused on monetizing their work at any cost, either by intimidating victims into coughing up cash or covertly subscribing them to premium rated services to which they're affiliated.

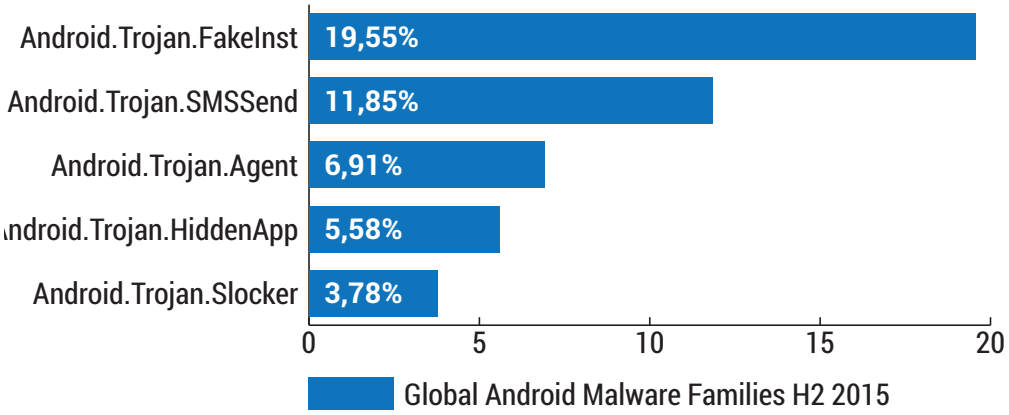

Fig. 11 – Global Android malware family distribution H2 2015

Malicious applications can pose as games or tools – while in fact they're not - to trick users into installing them. Whether they're Google Play applications or third-party marketplaces, users need to exercise maximum caution when downloading and installing apps.

While the same two malware families are encountered in other statistics for individual countries, they constantly trade places across the five most prevalent families in our statistics.

However, the UK, Germany and Australia show that, besides the previously mentioned threats, Android ransomware is still a major concern and will continue to claim victims, as Bitdefender 2016 predictions highlight.

Android Ransomware Scores Big in US and Germany

The Android ransomware family that Bidefender has dubbed Android.Trojan.Slocker was hitting German, Australian and UK users hard during the second half of 2015. More than 33.58% of all malware reports in Germany were ransomware-related, while in Australia and the UK, the numbers point to the same conclusion, with 30.25 percent and 22.39 percent.

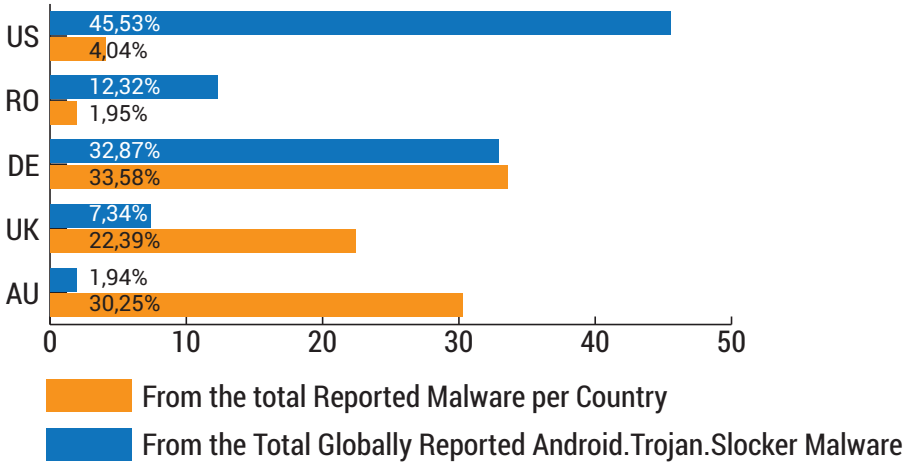

Fig. 12 –Android Ransomware malware family distribution during H2 2015

However, **45.53 percent of all globally reported ransomware came from the US**, meaning that nearly half of all Android.Trojan.Slocker reports come from America. Germany came second with 32.87 percent of all globally reported ransomware, showing that the two countries were the ones most targeted by this type of threat during H2 2015.

Because this was the most common threat in all the above-mentioned countries, it's safe to speculate that it has also been one of the most prolific, potentially nabbing malware developers serious profit. These numbers are no surprise as we have already seen that Android ransomware is not only becoming more sophisticated, but also targeting more countries.

SMS-Sending Malware Also Goes for American Money

The Android.Trojan.SMSSend malware family has been plaguing Android users for the better part of the past couple of years, and some of it has actually made it to Google Play. (see MKero story above)

Again, malware developers have chosen the US as their main target, as more than **78.36 percent of all globally reported malware in this family** has been reported from the United States.

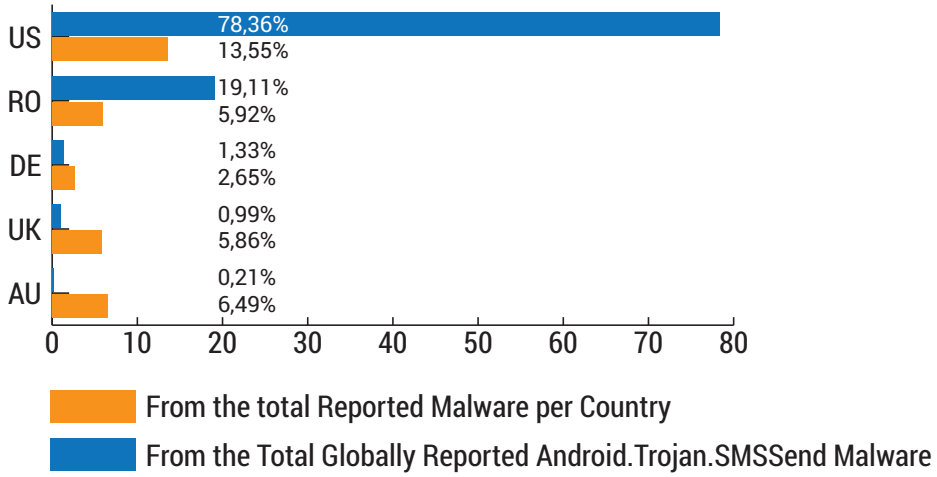

Fig. 13 - Android SMS-sending malware family distribution during H2 2015

While it doesn't rank first in individual country reports, it still continue to make the list of the five most notorious threats in particular regions, such as the UK (ranking fifth with 5.86 percent), the US (ranking second with 13.55 percent), and Australia (ranking fourth with 6.49 percent).

Trojans and Aggressive Adware

While the US and Romania have not seen many ransomware reports, they do rank first when aggressive adware and data-stealing Trojans are involved. The two malware families – although not as popular as ransomware - are Android.Trojan.Agent and Android.Trojan.HiddenApp.

The whopper here is that, while Android.Trojan.Agent ranked first in reports per country, the US leads the chart with **54.11 percent of all globally reported threats** in this family. Romania is not far behind, nabbing 40.91 percent of all global reports related to the malware family.

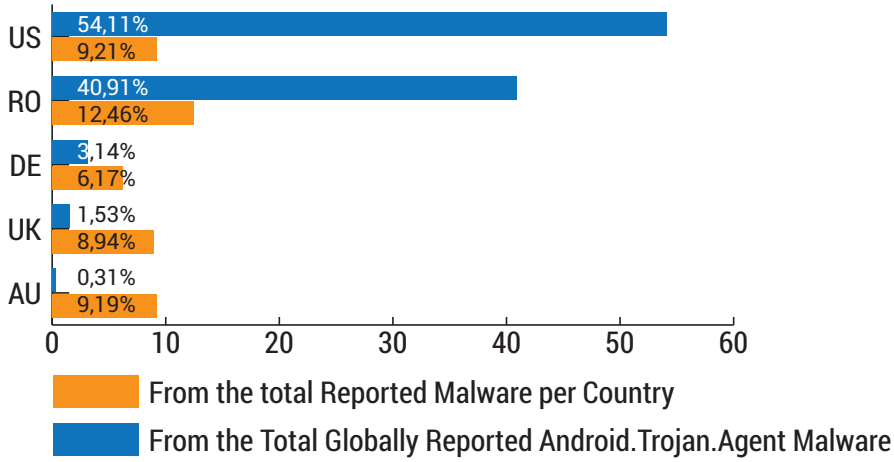

Fig. 14 - Android.Trojan.Agent malware family distribution per country during H2 2015

The above malware family is usually used to create a beachhead on targeted devices to either allow other applications to be installed or simply exfiltrate on-device data. They're usually packed with games distributed via third-party marketplaces. Although some of the games they're bundled with might work, as soon as the malware lands on the device, it starts performing various intrusive actions.

Romania ranked first with 12.46 percent of the total number of malware reports in that country, while the US, Australia and the UK are close behind with 9.21 percent, 9.19 percent and 8.84 percent, respectively.

The **Android.Trojan.HiddenApp** family on the other hand is far more interesting as it has even been spotted in Google Play. The malware seems to have been particularly targeting Romania, as **73.32 percent** of all globally reported malware of this type seems to have originated from here.

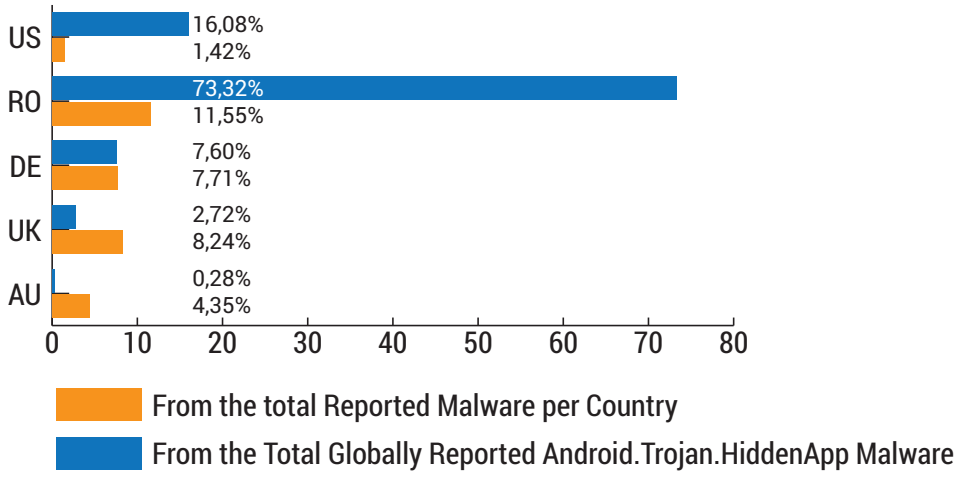

Fig. 15 – Android.Trojan.HiddenApp malware family distribution per country during H2 2015

Around **10 Google Play apps infected** with this malware strand were reported to Google by Bitdefender in early 2015, all of them employing advanced evasion techniques that made their removal highly difficulty by average users.

Although their purpose was to perform browser redirects every 60 seconds, pushing users to various advertising websites, their main objective was to trick users into installing other types of malware disguised as system performance updates.

These nasty apps also requested only two permissions on installation (Network Communication and System Tools) and changed their process names to "System Manager" making the apps difficult to find and uninstall.

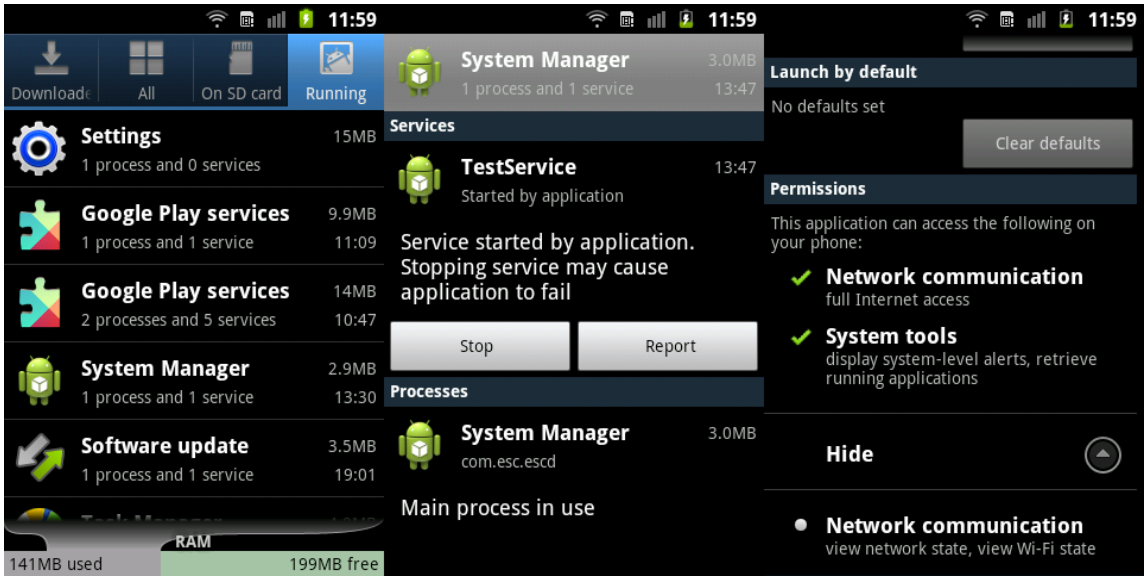

Fig. 16 – Android.Trojan.HiddenApp.E malware hiding its process name as “System Manager”

To make the application even more effective, its developers made sure that regardless of the used mobile browser, users would get bounced around from one ad-displaying website to another.

Although they’re not malicious per se, by broadcasting sensitive user information to third parties, they resemble aggressive adware found on desktop PCs. The resulting barrage of pop-ups, redirects and ads irks users and seriously damages both the user experience and the performance of Android device

```
public class TestService extends Service {
    private final String BROWSER_CHROME;
    private final String BROWSER_DOLPHIN;
    private final String BROWSER_FIREFOX;
    private final String BROWSER_NATIVE;
    private final String FACEBOOK;
    private final String FIR;
    private final String PLAY;
    private ActivityManager am;
    private int floodControlSeconds;
    private int lastTimeWeLaunchedWebsite;
    private final Runnable mCheck;
    private final Handler mHandler;
    private String urlToLaunch;
    private boolean wasLastActivityBrowser;

    public TestService() {
        this.urlToLaunch = "http://www.mobilsitelerim.com/anasayfa";
        this.floodControlSeconds = 60;
        this.BROWSER_NATIVE = "com.android.browser";
        this.BROWSER_CHROME = "com.google.android.apps.chrome";
        this.BROWSER_FIREFOX = "org.mozilla.firefox";
        this.BROWSER_DOLPHIN = "mobi.mgeek.TunnyBrowser";
        this.FACEBOOK = "com.facebook.katana";
        this.PLAY = "com.android.vending";
        this.FIR = "com.fir.fir";
        this.am = null;
        this.wasLastActivityBrowser = false;
        this.lastTimeWeLaunchedWebsite = 0;
        this.mHandler = new Handler();
        this.mCheck = new Runnable() {
            public void run() {
                String currentRunningActivityName = ((RunningTaskInfo) TestService.this.am.getRunningTasks(1).get(0)).topActivity.getClassName();
                Log.e("ACTIVITY", currentRunningActivityName);
                if (!currentRunningActivityName.startsWith("com.android.browser") && !currentRunningActivityName.startsWith("com.google.android.apps.chrome") &
                    TestService.this.wasLastActivityBrowser = false;
                } else if (!TestService.this.wasLastActivityBrowser) {
                    int ts = (int) (System.currentTimeMillis() / 1000);
                    if (ts - TestService.this.lastTimeWeLaunchedWebsite > TestService.this.floodControlSeconds) {
                        TestService.this.launchUrl(TestService.this.urlToLaunch);
                        TestService.this.lastTimeWeLaunchedWebsite = ts;
                        TestService.this.wasLastActivityBrowser = true;
                    }
                }
                TestService.this.mHandler.postDelayed(TestService.this.mCheck, 100);
            }
        };
    }
```

Fig. 17 - Android.Trojan.HiddenApp.E identifying mobile browsers as to redirect users

Fake Apps Making Promises and Delivering Malware

Dubbed Android.Trojan.FakeInst by our labs, this malware family tricks users into installing them by usually promising full unlocked games or applications – that would otherwise have to be paid for.

While for some paying for Android games might not a popular practice, it's interesting to note that US users are the ones most likely to install such infected apps from third-party marketplaces. More than 24.15 percent of US malware reports have been identified as Android.Trojan.FakeInst.

Again, when looking at the global number of reports generated by this malware family alone, we've got a remarkable **98.27 percent**. This indicates that, while other countries may be affected by fake applications promising to deliver a particular type of content, the US gets the brunt of it. US users are most targeted, regardless of whether they willingly downloading apps from unofficial marketplaces or are simply targeted by phishing emails.

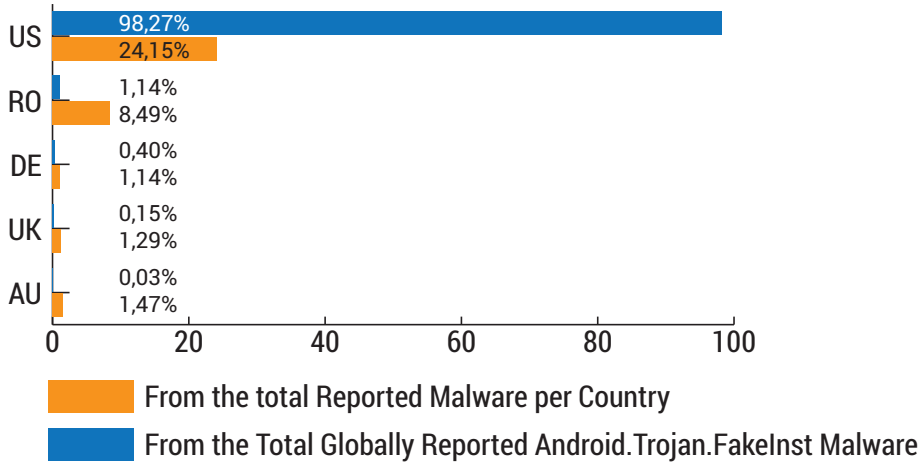

Fig. 18 - Android.Trojan.FakeInst malware family distribution per country during H2 2015

To understand the magnitude of this type of malware, a while back Bitdefender even spotted its own Android Mobile Security application duplicated, bundled with this malware, and distributed via various third-party marketplaces.

Fig. 19 – Fake Bitdefender Mobile Security app illegitimately distributed with the Android.Trojan.FakeInst malware family

Needless to say, malware coders will stop at nothing to trick victims into installing infected apps on their Android devices, especially if it requires leveraging popular applications in Google Play.

Takeaway and How to stay safe?

As Android continues to dominate the market, malware developers will continue to write code that fits their agenda. Whether it's stealo ing data or locking your device and asking for money to release access to it, Android malware is a lucrative business for malware coders and a gateway for other malicious actions.

Analyzing some of the most popular global Android malware families, it's clear that, while some target specific countries, others have a more holistic approach towards being distributed globally.

It's highly recommended that Android users install a mobile security solution that can identify malicious applications before they're installed on the terminal, and advise on the potential privacy impact of apps already installed.

Avoid installing applications from sources other than Google Play or trusted marketplaces. There is a high chance they will be riddled with malware, data-stealing Trojans and annoying aggressive adware. While there have been reports of malware in Google Play – we've found some ourselves – the alternative is far more dire.

About Bitdefender

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

Publication Date: January 2016

Bitdefender

BD-NGZ-Feb.22.2016-TK# 86847