

Caught in the Act: Uncovering SpyNote in Unexpected Places

 hunt.io/blog/caught-in-the-act-uncovering-spynote-in-unexpected-places

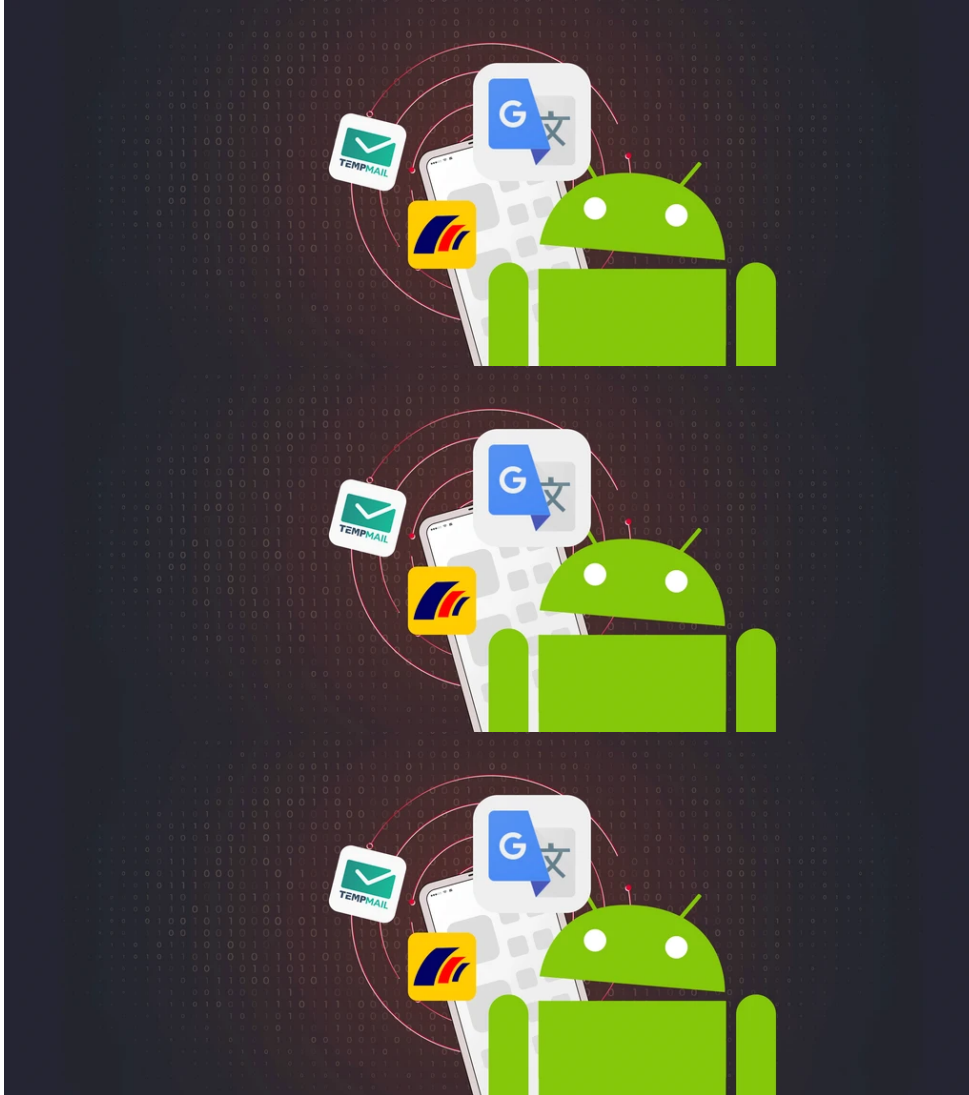


TABLE OF CONTENTS

Introduction

In hidden corners of the Internet, open directories often serve as treasure troves, offering a glimpse into the unguarded secrets of digital repositories. While sometimes mundane, these directories can occasionally reveal attention-grabbing discoveries.

Our team recently unearthed multiple samples of SpyNote, a well-known spyware targeting Android devices, cleverly disguised as legitimate apps such as **Google Translate**, **Temp Mail**, **Deutsche Postbank**, and even an app supposedly meant to discourage intoxicated

driving.

This finding highlights how innocuous-seeming servers can often host dangerous threats. To stay protected, apply for a demo on [Hunt](#) and proactively access up-to-date threat information.

What is SpyNote, and How Does it Operate?

SpyNote is a sophisticated piece of malware that, as the name suggests, emphasizes spying on its victims. It has become a significant threat to Android users, especially after its source code was leaked in late **2022**.

The spyware exploits accessibility services and device administrator privileges, allowing the malicious software to steal sensitive information such as **device location, contacts, SMS messages**, etc.

SpyNote samples routinely use deception, disguising itself by using legitimate app icons to trick users into believing it is a harmless application while silently collecting their data.

For further information on the technical analysis of SpyNote, check out the following articles:

Fortinet – [Android/SpyNote Moves to Crypto Currencies](#)

McAfee – [Android SpyNote attacks electric and water public utility users in Japan](#)

ThreatFabric – [SpyNote: Spyware with RAT capabilities targeting Financial Institutions](#)

Our Discoveries: SpyNote Samples in OpenDirs

The Hunt platform provides hundreds of tags for known malware families and open-source tools in open directories, including SpyNote, as shown in **Figure 1**.

Exposed Open Directories

Total Open Directories

7,403

Malicious Open Directories

Past 30 days: 743

Hostname	Files	Tags	Trigger	Last seen	First Seen
http://47.57.7.44 Alibaba US Technology Co., Ltd. Hong Kong, HK	1		tweet	10 hours ago	1 week ago
https://47.57.7.44 Alibaba US Technology Co., Ltd. Hong Kong, HK	1		tweet	10 hours ago	1 week ago
https://103.142.244.32 Antbox Networks Limited HK	2	Spynote	tweet	5 days ago	1 week ago
http://47.57.184.164 Alibaba US Technology Co., Ltd. Hong Kong, HK	7		tweet	2 hours ago	1 week ago
http://103.142.244.32 Antbox Networks Limited HK	2	Spynote	tweet	5 days ago	1 week ago

Figure 1: Tags for SpyNote samples in open directories

Users can navigate directly to a page listing all the latest SpyNote samples hosted on misconfigured servers by clicking on any of these tags. In **Figure 2**, you'll see that the historical data for discovered .apk files covers the past two months, providing an overview of the spyware's recent activity. This tagging system ensures users can quickly track and analyze the presence of SpyNote and other threats across various open directories.

Open Directory Search Malicious Files

Files

42

Q Search files by keyword Search

Hostname	File URL	Labels	SHA256	Modified
http://85.66.165.13:9000	85.66.165.13_9000/client.apk	📄	# 🗑️ (1)	4 days ago
http://18.219.97.209:8081	18.219.97.209_8081/Google.apk	📄	# 🗑️ (2)	1 week ago
http://18.219.97.209:8081	18.219.97.209_8081/Translate.apk	📄	# 🗑️ (2)	1 week ago
http://193.161.193.99:30600	193.161.193.99_30600/ready.apk__rev4	🔍 📄	# 🗑️ (1)	1 week ago
http://193.161.193.99:48627	193.161.193.99_48627/ready.apk__rev4	🔍 📄	# 🗑️ (1)	1 week ago
https://45.138.50.149:443	45.138.50.149_443/vegas.apk	📄	# 🗑️ (1)	1 week ago
https://45.138.50.149:443	45.138.50.149_443/sk.apk	📄	# 🗑️ (2)	1 week ago
http://156.245.13.61:8000	156.245.13.61_8000/Temp_20Mail.apk	📄	# 🗑️ (3)	2 weeks ago
http://156.245.13.61:8000	156.245.13.61_8000/123.apk	📄	# 🗑️ (6)	2 weeks ago
http://156.245.13.61:8000	156.245.13.61_8000/ready.apk	📄	# 🗑️ (6)	2 weeks ago
http://156.245.13.61:8000	156.245.13.61_8000/read1y.apk	📄	# 🗑️ (3)	2 weeks ago
https://103.142.244.32:443	103.142.244.32_443/ready.apk	📄	# 🗑️ (1)	2 weeks ago
http://45.138.50.149:80	45.138.50.149_80/sk.apk	📄	# 🗑️ (2)	2 weeks ago

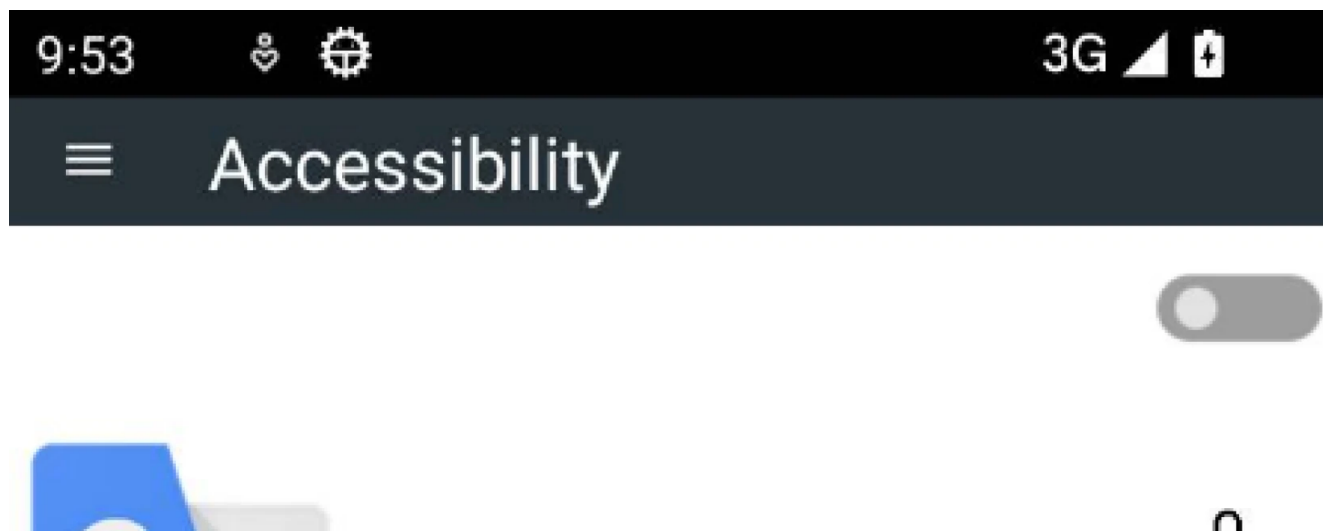
Figure 2: Result of clicking on the SpyNote tags. [Try it!](#)

Let's examine some particularly interesting samples we've found and their connections to Command and Control (C2) infrastructure.

Translate.apk

This directory, hosted on AWS at IP **18.219.97_209:8081**, contained just three files: Google.apk, Translate.apk, and desktop.ini. Curiously, the first two files are identical, only differing in name.

Upon installation, the app perfectly mirrors the legitimate Google Translate application, but a likely developer slip-up stands out. When requesting accessibility permissions, the instructions read “- **Enable [MY-NAME]**,” a placeholder that should have been replaced. This error is shown in **Figure 3**.





Google Translate



This App Request Accessibility Service:

- Click on Enable
- Go to Downloaded Service
- Enable [MY-NAME]

Enable

Figure 3: Accessibility services request screen (Source: [Hatching Triage](#))

At the same time, the malicious app starts making network requests to its C2, **kyabhai.duckdns_org**, hosted on the same IP address at port 8080.

Directory Details

- Open Directory & C2 IP: 18.219.97_209:8081
- Google.apk & Translate.apk SHA-1 hash:
3aad911b21907053a69b49086a6396c50714accb
- C2 domain: kyabhai.duckdns_org:8080

- Triage Link: <https://tria.ge/240617-lwchbavhme>

Malware Config

Extracted

Family: spynote

C2: kyabhai.duckdns.org:8080

Signatures

Spynote
Spynote is a Remote Access Trojan first seen in 2017.

SPYNOTE BANKER TROJAN INFESTEALER RAT

Loads dropped Dex/Jar • 1 TTPs 1 IoCs
Runs executable file dropped to the device during analysis.

EVASION

Makes use of the framework's Accessibility service • 4 TTPs 3 IoCs
Retrieves information displayed on the phone screen using AccessibilityService.

COLLECTION EVASION CREDENTIAL_ACCESS

Obtains sensitive information copied to the device clipboard • 2 TTPs 1 IoCs
Application may abuse the framework's APIs to obtain sensitive information copied to the device clipboard.

COLLECTION CREDENTIAL_ACCESS IMPACT

Acquires the wake lock • 1 IoCs

Makes use of the framework's foreground persistence service • 1 TTPs 1 IoCs
Application may abuse the framework's foreground service to continue running in the foreground.

EVASION PERSISTENCE

Performs UI accessibility actions on behalf of the user • 1 TTPs 8 IoCs
Application may abuse the accessibility service to prevent their removal.

EVASION

Queries information about active data network • 1 TTPs 1 IoCs

DISCOVERY

Requests disabling of battery optimizations (often used to enable hiding in the background). • 1 TTPs 1 IoCs

EVASION

Schedules tasks to execute at a specified time • 1 TTPs 1 IoCs
Application may abuse the framework's APIs to perform task scheduling for initial or recurring execution of malicious code.

EXECUTION PERSISTENCE

Uses Crypto APIs (Might try to encrypt user data) • 1 TTPs 1 IoCs

IMPACT

Checks CPU information • 2 TTPs 1 IoCs

Checks memory information • 2 TTPs 1 IoCs

Figure 4: File metadata for Translate.apk (Source: [Hatching Triage Sandbox](#))

Temp_20Mail.apk

Moving on, we explored an open directory hosted by SonderCloud Limited at IP **156.245.13_61:8000**. This directory not only contained several SpyNote APKs but also hosted Cobalt Strike and Sliver binaries targeting the Windows operating system.

Among these, a file named **"Temp_20Mail.apk"** caught our eye. This file disguises itself as the legitimate Temp Mail app, which allows users to generate disposable email addresses. However, unlike the previous samples, once installed, this program begins beaconing to the C2 IP address **156.245.20_17:7771**.

Figure 5 displays the malicious app using the legitimate icon, while **Figure 6** shows the Temp Mail app on the Google Play Store.





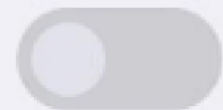
All files access



Temp Mail

81.9.78.72

Allow access to manage all files



Allow this app to read, modify and delete all files on this device or any connected storage volumes. If

granted, app may access files without your explicit

Figure 5: Screenshot of the malicious Temp Mail application

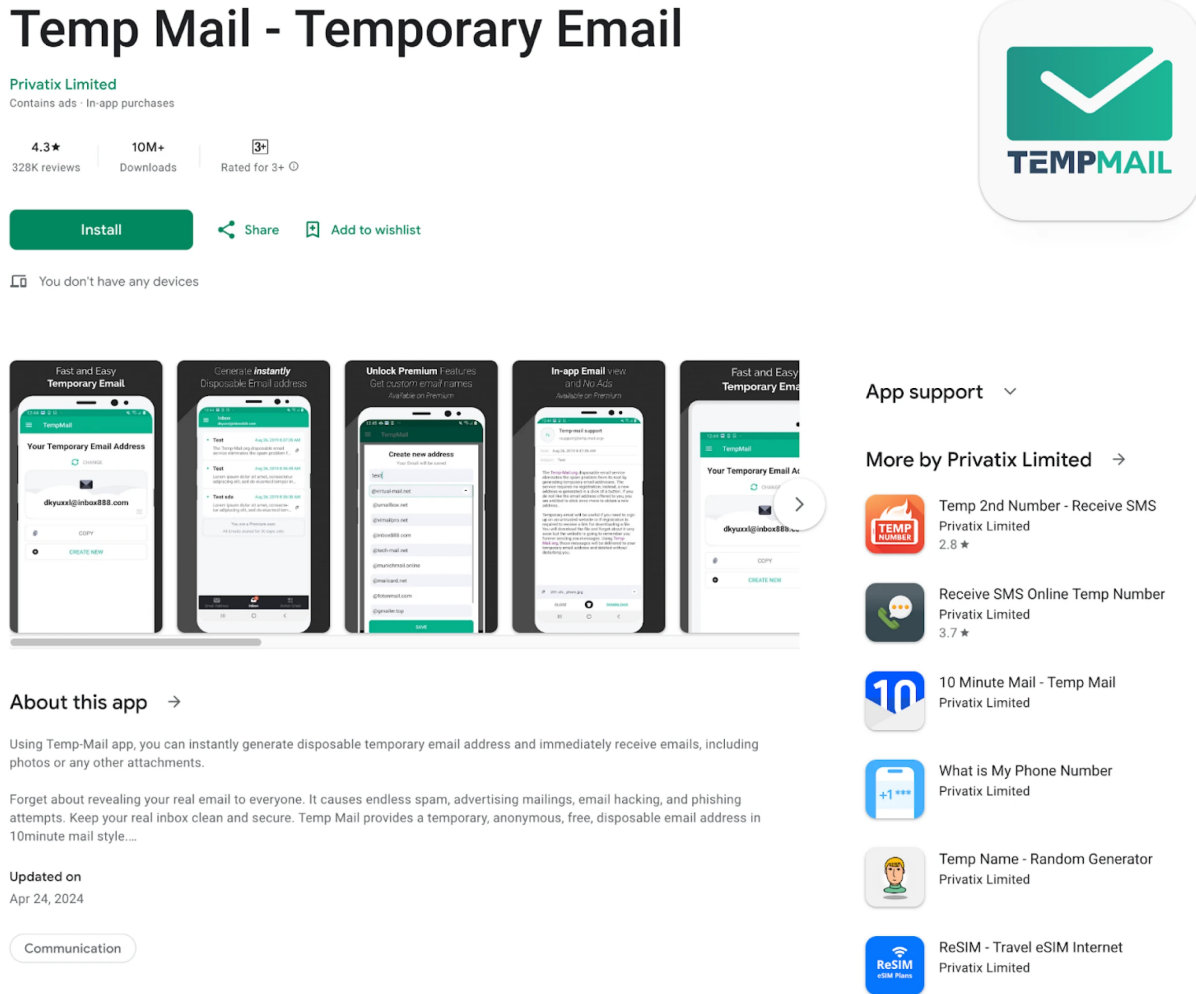


Figure 6: Legitimate Temp Mail app in the Google Play Store

Additional information on the C2 was limited, but we did discover that the IP recently resolved to two domains: **gw.585822_vip** and **nerjowmqw_com**.

Directory Details

- Open Directory: 156.245.13_61:8000
- C2: 156.245.20_17:7771
- Temp_20Mail.apk SHA-1 hash: 5b9bfa06d05172f61d1ee19724fcd12cec110353
- Triage Link: <https://tria.ge/240617-l875rawdph/behavioral2>

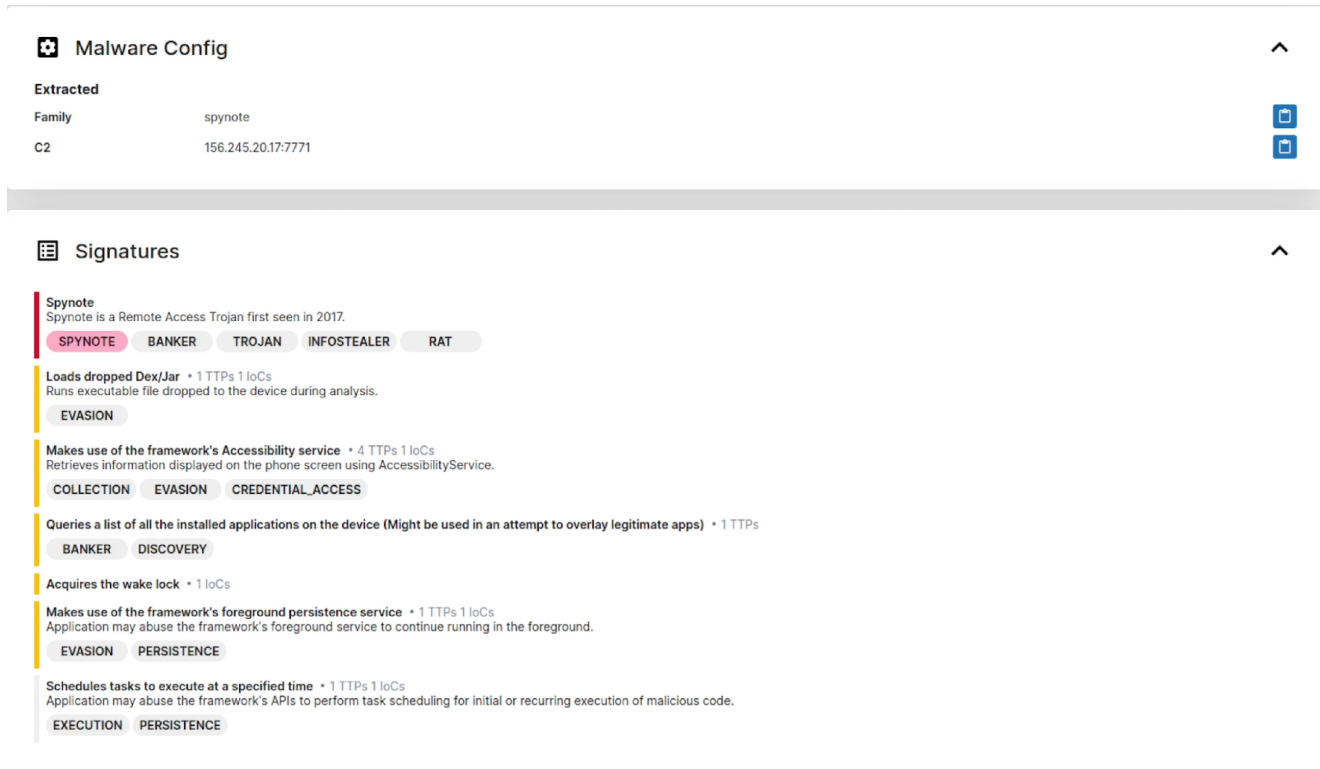
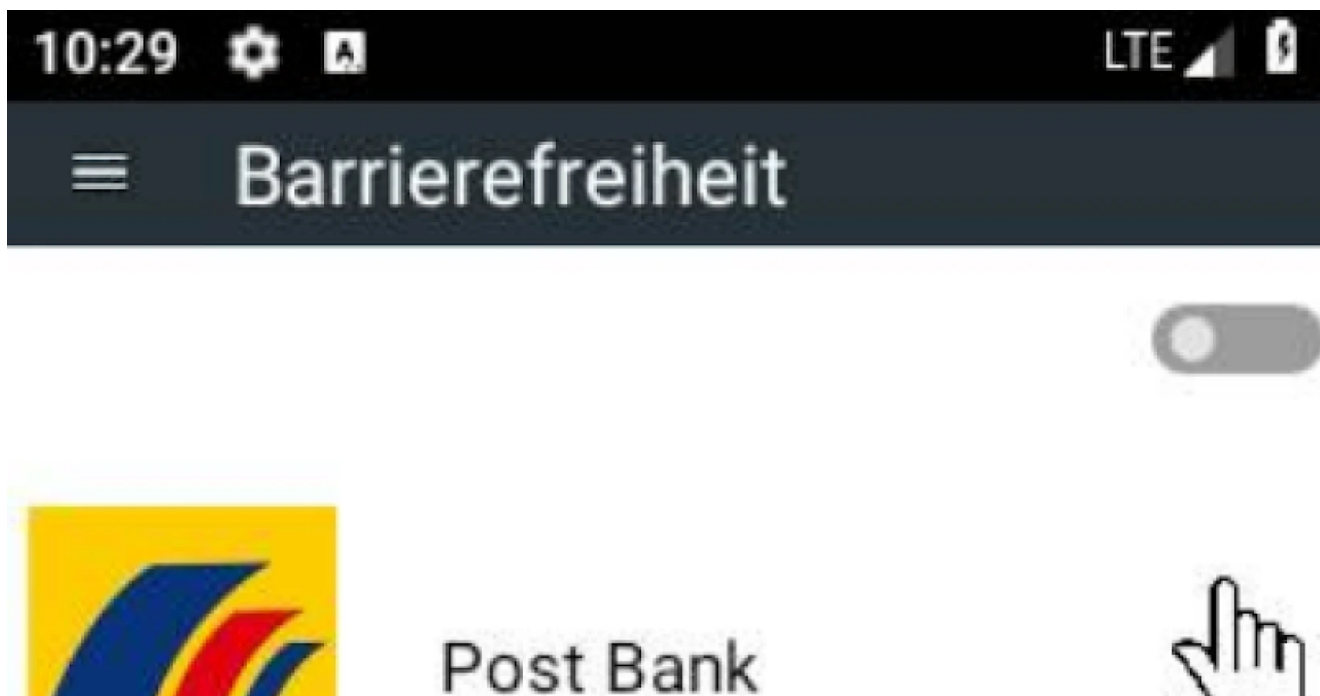


Figure 7: Metadata for Temp_20Mail.apk (Source: [Hatching Triage Sandbox](#))

postbank.apk

The following file masquerades as an app for the German bank Post Bank. This app communicates with the domain **oebonur600.duckdns_org**, which resolves to IP address **95.214.177_114** on port 3210 in a pattern that's becoming alarmingly familiar.

A screenshot of the app during dynamic analysis is provided in **Figure 8**, showcasing its deceptive interface.





Dieser App-Request-Barierefreiheitsdienst:

- Klicken Sie auf Aktivieren
- Gehen Sie zu Heruntergeladener Dienst
- [MEIN NAME] aktivieren

Genehmigung



Figure 8: Screenshot of postbank.apk during dynamic analysis (Source: [Hatching Triage Sandbox](#))

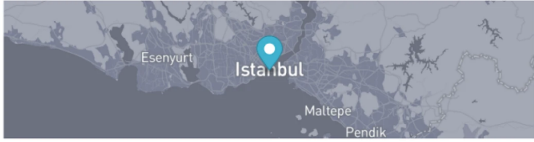
The C2 is hosted on Cloudflare London at the Yusuf Kemal TURKMENOGU ASN.

95.214.177.114 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

95.214.177.114

Cloudflare London, LLC



Istanbul, Istanbul, TR

DNS

Reverse DNS: undefined

Forward DNS: oebonur600.duckdns.org... 1

Tag: duckdns.org - Dynamic DNS

ASN

AS210538 95.214.177.0/24 Yusuf Kemal TURKMENOGU

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
HTTP	80	HTTPD	2.4.58	-	1 week ago	1 year ago
Unknown	135	-	-	-	1 week ago	7 months ago
Unknown	139	-	-	-	4 hours ago	

Figure 9: IP Overview for C2 in Hunt

In late May 2024, a web page hosted on port 80 of the C2 contained the defacement message "HACKED BY PersoDev." This page included a JavaScript script that turned off the right-click context menu and displayed an alert message. Additionally, it featured CSS to alter the opacity of images with a hover effect.

We don't believe the two are related, but it is an interesting finding.

Ports protocols

Port	Protocol	Header Data
80	http	HTTP/1.1 200 OK Date: Wed, 29 May 2024 02:03:50 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.1.25 L...-Modified: Tue, 28 May 2024 17:11:42 GMT ETag: "2090-61986ba4a5e80" Accept-Ranges: bytes Content-Length: 8336 Content-Type: text/html <html> <head> <title> HACKED BY PersoDev </title> <html><head> <script language="JavaScript"> var message = "Nbr Güzelim :P"; function rtclickcheck(key){ if (navigator.appName == "Netscape" && keyp.which == 3){ alert(message); return false; } if (navigator.appVersion.indexOf("MSIE") != -1 && event.button == 2) { alert(message); return false; } document.onmousedown = rtclickcheck; </script> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <style type="text/css"> img{opacity: 0.5; -webkit-transition: all 250ms ease; -moz-transition: all 250ms ease; -o-transition: all 250ms ease; transition: all 250ms ease;} img:hover{opacity:
443	tls	HTTP/1.1 400 Bad Request Date: Tue, 11 Jun 2024 01:03:47 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Content-Length: 468 Connection: close Content-Type: text/html; charset=iso-8859-1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>400 Bad Request</title> </head><body> <h1>Bad Request</h1> <p>Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, pl
445	smb	#SMB<NT L
3389	tls	MfS...j...v...%...o...ne...N...!4...5...1...z...MaU...0...0...0...7...m...C...1H...0... *...H...010U KEYUBUW/IN0 240210083849Z 240811083849Z010U KEYUBUW/IN0... *...H...0...0...0...VJs...#...xa...5B)...z...g...v...h...T...K...-S...V...w...x...O...R...2...C...N...C...U...h...uL1...E...M...z...4...@...T...-...#...h...a...j...@...n...W...["...k...z...4e...h...nf...Papw...>...K...-c...T...l...N...Z...K...g...C..._...T...K...<...d...y...S...0...U...%...+
3389	tcpwrapped	
5985	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 10 May 2024 05:36:27 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY><h2>Not Found</h2> <hr><p>HTTP Error 404. The requested resource is not found.</p> </BODY></HTML>
47001	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sat, 11 May 2024 04:11:09 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY><h2>Not Found</h2> <hr><p>HTTP Error 404. The requested resource is not found.</p> </BODY></HTML>

Figure 10: Screenshot of ports and protocols for the associated IP in Hunt. Try it out!
Directory Details

- Open Directory & C2 IP: 5.252.74.45_443
- postbank.apk SHA-1 hash: dc9a821f1e061098188503dbf7518bf263334fcd
- C2 domain: oebonur600.duckdns_org
- Triage Link: <https://tria.ge/240617-mhv8yawgqb>

Impacts on Users and Devices

The discovery of SpyNote samples in open directories poses significant risks to users, as these malicious files utilize additional infrastructure, including dynamic domains, for data exfiltration.

Once infected, users' sensitive information can be continuously siphoned to ever-changing locations, making detection and mitigation more challenging.

Conclusion

The SpyNote samples we've discussed show how even everyday apps like Google Translate and Temp Mail can be repurposed for malicious intent. These examples are just a handful of the over 40 SpyNote APKs available in Hunt, with many more likely operating undetected and stealing sensitive information.

To stay ahead of these threats, apply for a free demo of Hunt. Track and analyze numerous threats identified in open directories, analyze the infrastructure of over 80 malware families, and effectively protect your digital environment.

TABLE OF CONTENTS

Introduction

In hidden corners of the Internet, open directories often serve as treasure troves, offering a glimpse into the unguarded secrets of digital repositories. While sometimes mundane, these directories can occasionally reveal attention-grabbing discoveries.

Our team recently unearthed multiple samples of SpyNote, a well-known spyware targeting Android devices, cleverly disguised as legitimate apps such as **Google Translate**, **Temp Mail**, **Deutsche Postbank**, and even an app supposedly meant to discourage intoxicated driving.

This finding highlights how innocuous-seeming servers can often host dangerous threats. To stay protected, apply for a demo on [Hunt](#) and proactively access up-to-date threat information.

What is SpyNote, and How Does it Operate?

SpyNote is a sophisticated piece of malware that, as the name suggests, emphasizes spying on its victims. It has become a significant threat to Android users, especially after its source code was leaked in late **2022**.

The spyware exploits accessibility services and device administrator privileges, allowing the malicious software to steal sensitive information such as **device location**, **contacts**, **SMS messages**, etc.

SpyNote samples routinely use deception, disguising itself by using legitimate app icons to trick users into believing it is a harmless application while silently collecting their data.

For further information on the technical analysis of SpyNote, check out the following articles:

Fortinet – [Android/SpyNote Moves to Crypto Currencies](#)

McAfee – [Android SpyNote attacks electric and water public utility users in Japan](#)

ThreatFabric – [SpyNote: Spyware with RAT capabilities targeting Financial Institutions](#)

Our Discoveries: SpyNote Samples in OpenDirs

The Hunt platform provides hundreds of tags for known malware families and open-source tools in open directories, including SpyNote, as shown in **Figure 1**.

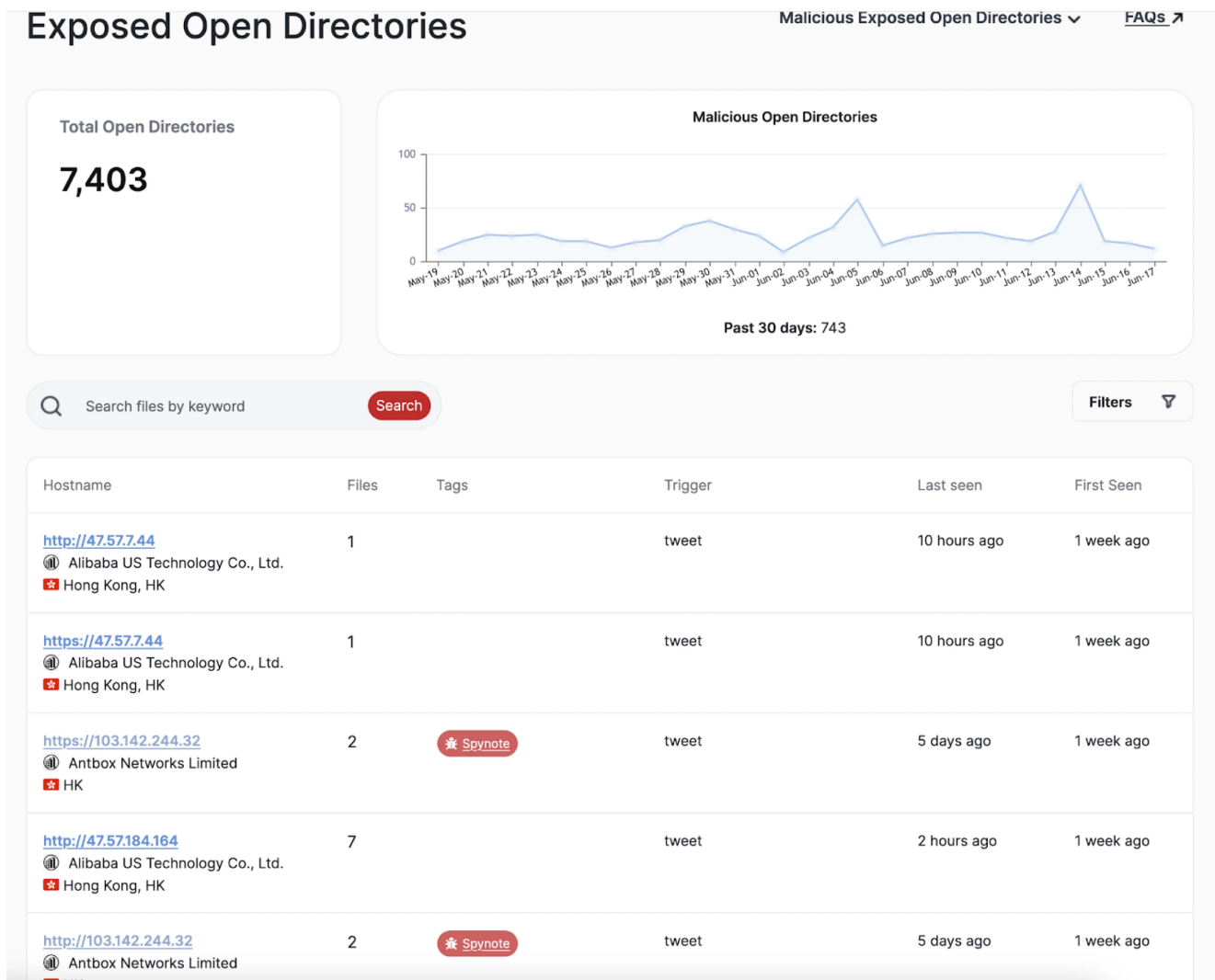


Figure 1: Tags for SpyNote samples in open directories

Users can navigate directly to a page listing all the latest SpyNote samples hosted on misconfigured servers by clicking on any of these tags. In **Figure 2**, you'll see that the historical data for discovered .apk files covers the past two months, providing an overview of the spyware's recent activity. This tagging system ensures users can quickly track and analyze the presence of SpyNote and other threats across various open directories.

Open Directory Search Malicious Files

Files

42

Search

Hostname	File URL	Labels	SHA256	Modified
http://85.66.165.13:9000	85.66.165.13_9000/client.apk	📄	# 🗂️ (1)	4 days ago
http://18.219.97.209:8081	18.219.97.209_8081/Google.apk	📄	# 🗂️ (2)	1 week ago
http://18.219.97.209:8081	18.219.97.209_8081/Translate.apk	📄	# 🗂️ (2)	1 week ago
http://193.161.193.99:30600	193.161.193.99_30600/ready.apk__rev4	🔍 📄	# 🗂️ (1)	1 week ago
http://193.161.193.99:48627	193.161.193.99_48627/ready.apk__rev4	🔍 📄	# 🗂️ (1)	1 week ago
https://45.138.50.149:443	45.138.50.149_443/vegas.apk	📄	# 🗂️ (1)	1 week ago
https://45.138.50.149:443	45.138.50.149_443/sk.apk	📄	# 🗂️ (2)	1 week ago
http://156.245.13.61:8000	156.245.13.61_8000/Temp_20Mail.apk	📄	# 🗂️ (3)	2 weeks ago
http://156.245.13.61:8000	156.245.13.61_8000/123.apk	📄	# 🗂️ (6)	2 weeks ago
http://156.245.13.61:8000	156.245.13.61_8000/ready.apk	📄	# 🗂️ (6)	2 weeks ago
http://156.245.13.61:8000	156.245.13.61_8000/read1y.apk	📄	# 🗂️ (3)	2 weeks ago
https://103.142.244.32:443	103.142.244.32_443/ready.apk	📄	# 🗂️ (1)	2 weeks ago
http://45.138.50.149:80	45.138.50.149_80/sk.apk	📄	# 🗂️ (2)	2 weeks ago

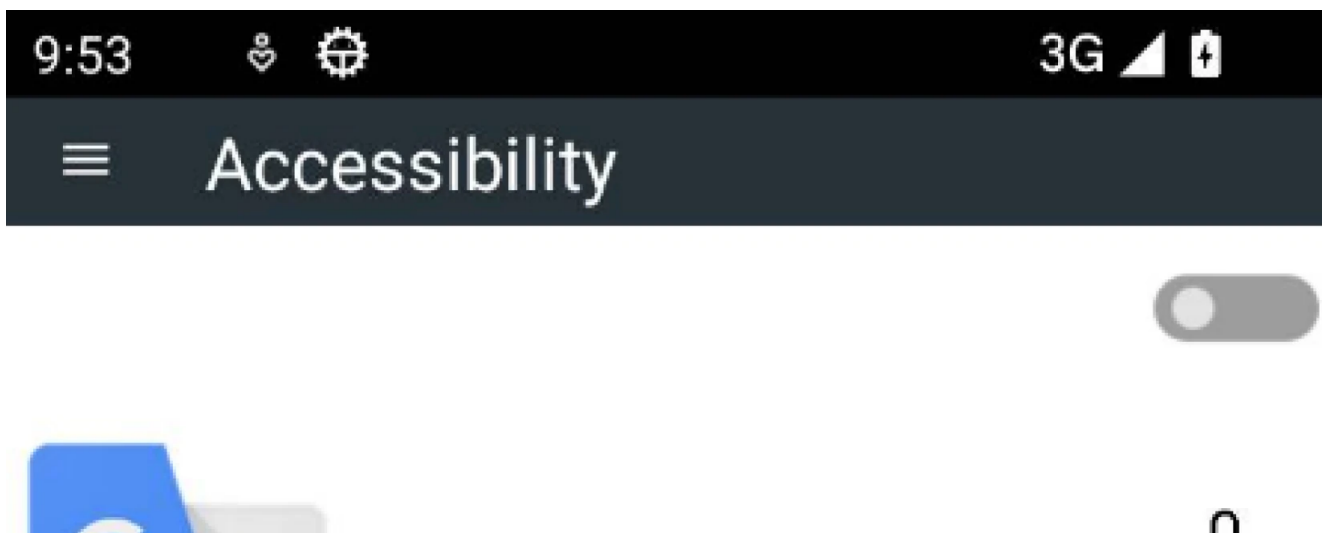
Figure 2: Result of clicking on the SpyNote tags. [Try it!](#)

Let's examine some particularly interesting samples we've found and their connections to Command and Control (C2) infrastructure.

Translate.apk

This directory, hosted on AWS at IP **18.219.97_209:8081**, contained just three files: Google.apk, Translate.apk, and desktop.ini. Curiously, the first two files are identical, only differing in name.

Upon installation, the app perfectly mirrors the legitimate Google Translate application, but a likely developer slip-up stands out. When requesting accessibility permissions, the instructions read “- **Enable [MY-NAME]**,” a placeholder that should have been replaced. This error is shown in **Figure 3**.





Google Translate



This App Request Accessibility Service:

- Click on Enable
- Go to Downloaded Service
- Enable [MY-NAME]

Enable

Figure 3: Accessibility services request screen (Source: [Hatching Triage](#))

At the same time, the malicious app starts making network requests to its C2, **kyabhai.duckdns_org**, hosted on the same IP address at port 8080.

Directory Details

- Open Directory & C2 IP: 18.219.97_209:8081
- Google.apk & Translate.apk SHA-1 hash:
3aad911b21907053a69b49086a6396c50714accb
- C2 domain: kyabhai.duckdns_org:8080

- Triage Link: <https://tria.ge/240617-lwchbavhmk>

Malware Config

Extracted

Family	spynote
C2	kyabhai.duckdns.org:8080

Signatures

Spynote
Spynote is a Remote Access Trojan first seen in 2017.

SPYNOTE **BANKER** **TROJAN** **INFOSTEALER** **RAT**

Loads dropped Dex/Jar • 1 TTPs 1 IoCs
Runs executable file dropped to the device during analysis.
EVASION

Makes use of the framework's Accessibility service • 4 TTPs 3 IoCs
Retrieves information displayed on the phone screen using AccessibilityService.
COLLECTION **EVASION** **CREDENTIAL_ACCESS**

Obtains sensitive information copied to the device clipboard • 2 TTPs 1 IoCs
Application may abuse the framework's APIs to obtain sensitive information copied to the device clipboard.
COLLECTION **CREDENTIAL_ACCESS** **IMPACT**

Acquires the wake lock • 1 IoCs

Makes use of the framework's foreground persistence service • 1 TTPs 1 IoCs
Application may abuse the framework's foreground service to continue running in the foreground.
EVASION **PERSISTENCE**

Performs UI accessibility actions on behalf of the user • 1 TTPs 8 IoCs
Application may abuse the accessibility service to prevent their removal.
EVASION

Queries information about active data network • 1 TTPs 1 IoCs
DISCOVERY

Requests disabling of battery optimizations (often used to enable hiding in the background). • 1 TTPs 1 IoCs
EVASION

Schedules tasks to execute at a specified time • 1 TTPs 1 IoCs
Application may abuse the framework's APIs to perform task scheduling for initial or recurring execution of malicious code.
EXECUTION **PERSISTENCE**

Uses Crypto APIs (Might try to encrypt user data) • 1 TTPs 1 IoCs
IMPACT

Checks CPU information • 2 TTPs 1 IoCs

Checks memory information • 2 TTPs 1 IoCs

Figure 4: File metadata for Translate.apk (Source: [Hatching Triage Sandbox](#))

Temp_20Mail.apk

Moving on, we explored an open directory hosted by SonderCloud Limited at IP **156.245.13_61:8000**. This directory not only contained several SpyNote APKs but also hosted Cobalt Strike and Sliver binaries targeting the Windows operating system.

Among these, a file named **"Temp_20Mail.apk"** caught our eye. This file disguises itself as the legitimate Temp Mail app, which allows users to generate disposable email addresses. However, unlike the previous samples, once installed, this program begins beaconing to the C2 IP address **156.245.20_17:7771**.

Figure 5 displays the malicious app using the legitimate icon, while **Figure 6** shows the Temp Mail app on the Google Play Store.





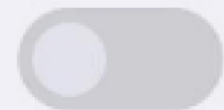
All files access



Temp Mail

81.9.78.72

Allow access to manage all files



Allow this app to read, modify and delete all files on this device or any connected storage volumes. If

granted, app may access files without your explicit

Figure 5: Screenshot of the malicious Temp Mail application

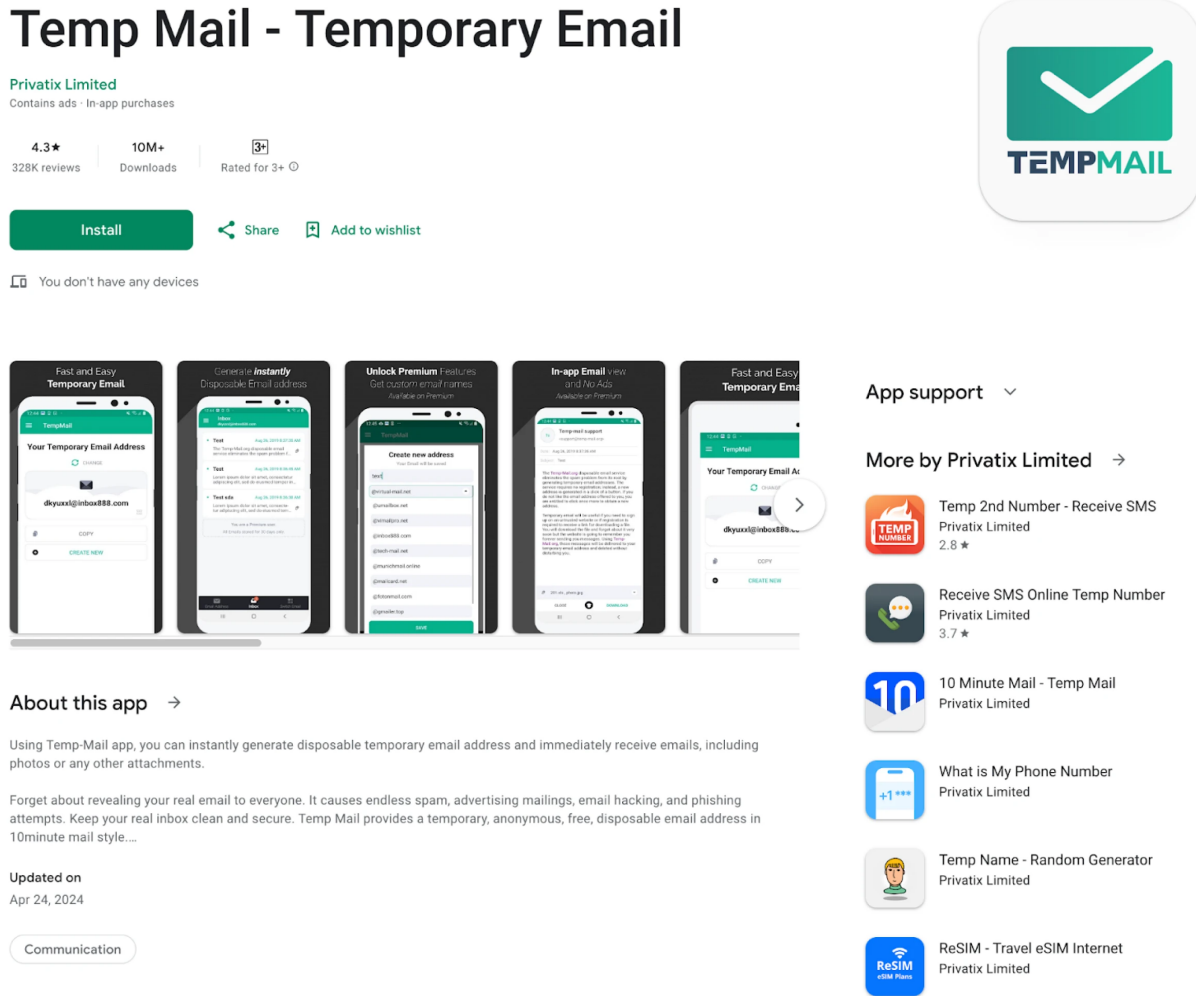


Figure 6: Legitimate Temp Mail app in the Google Play Store

Additional information on the C2 was limited, but we did discover that the IP recently resolved to two domains: **gw.585822_vip** and **nerjowmqw_com**.

Directory Details

- Open Directory: 156.245.13_61:8000
- C2: 156.245.20_17:7771
- Temp_20Mail.apk SHA-1 hash: 5b9bfa06d05172f61d1ee19724fcd12cec110353
- Triage Link: <https://tria.ge/240617-l875rawdph/behavioral2>

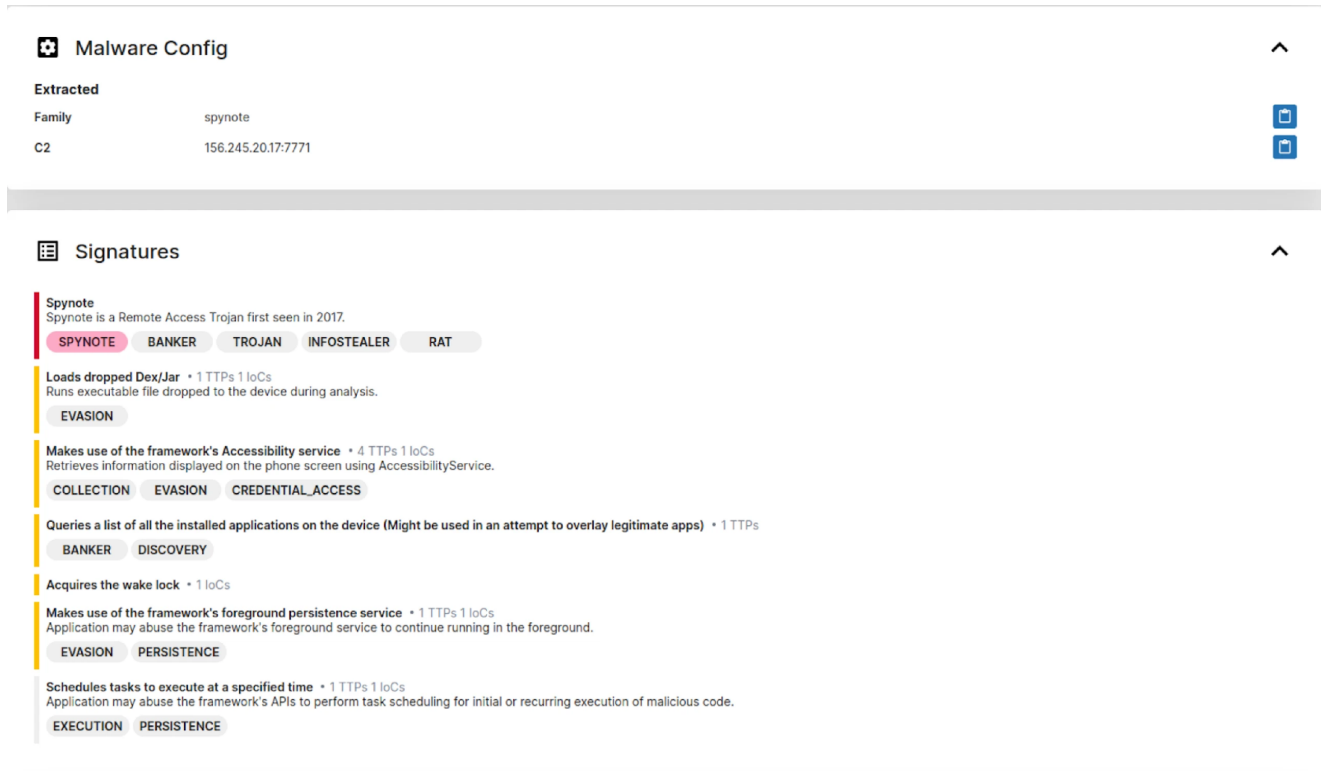
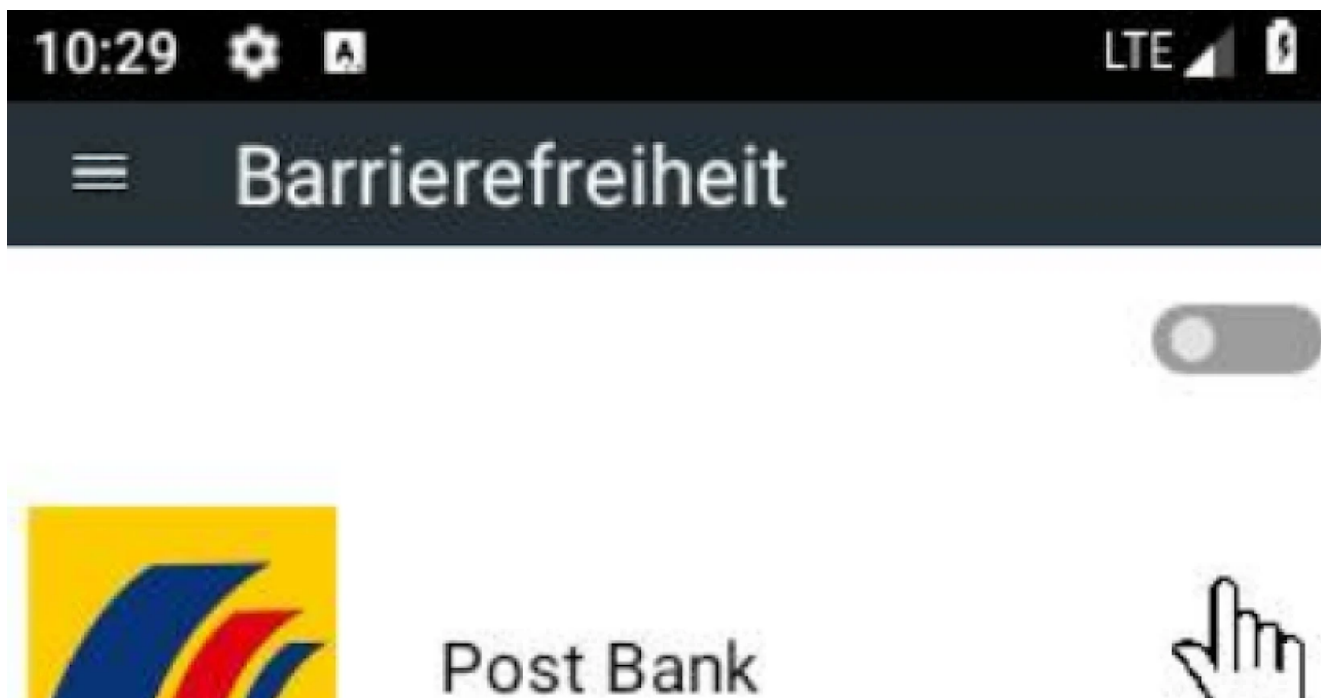


Figure 7: Metadata for Temp_20Mail.apk (Source: [Hatching Triage Sandbox](#))

postbank.apk

The following file masquerades as an app for the German bank Post Bank. This app communicates with the domain **oebonur600.duckdns_org**, which resolves to IP address **95.214.177_114** on port 3210 in a pattern that's becoming alarmingly familiar. A screenshot of the app during dynamic analysis is provided in **Figure 8**, showcasing its deceptive interface.





Dieser App-Request-Barrierefreiheitsdienst:

- Klicken Sie auf Aktivieren
- Gehen Sie zu Heruntergeladener Dienst
- [MEIN NAME] aktivieren

Genehmigung



Figure 8: Screenshot of postbank.apk during dynamic analysis (Source: [Hatching Triage Sandbox](#))

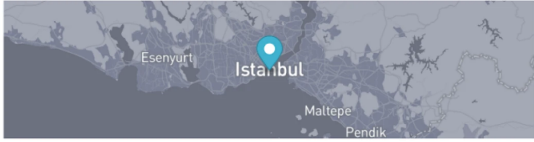
The C2 is hosted on Cloudflare London at the Yusuf Kemal TURKMENOGU ASN.

95.214.177.114 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

95.214.177.114

Cloudflare London, LLC



Istanbul, Istanbul, TR

DNS

Reverse DNS: undefined

Forward DNS: oebonur600.duckdns.org... 1

Tag: duckdns.org - Dynamic DNS

ASN

AS210538 95.214.177.0/24 Yusuf Kemal TURKMENOGU

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
HTTP	80	HTTPD	2.4.58	-	1 week ago	1 year ago
Unknown	135	-	-	-	1 week ago	7 months ago
Unknown	139	-	-	-	4 hours ago	

Figure 9: IP Overview for C2 in Hunt

In late May 2024, a web page hosted on port 80 of the C2 contained the defacement message "HACKED BY PersoDev." This page included a JavaScript script that turned off the right-click context menu and displayed an alert message. Additionally, it featured CSS to alter the opacity of images with a hover effect.

We don't believe the two are related, but it is an interesting finding.

Ports protocols

Port	Protocol	Header Data
80	http	HTTP/1.1 200 OK Date: Wed, 29 May 2024 02:03:50 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.1.25 L...-Modified: Tue, 28 May 2024 17:11:42 GMT ETag: "2090-61986ba4a5e80" Accept-Ranges: bytes Content-Length: 8336 Content-Type: text/html <html> <head> <title> HACKED BY PersoDev </title> <html><head> <script language="JavaScript"> var message = "Nbr Güzelim :P"; function rtclickcheck(key){ if (navigator.appName == "Netscape" && keyp.which == 3){ alert(message); return false; } if (navigator.appVersion.indexOf("MSIE") != -1 && event.button == 2) { alert(message); return false; } document.onmousedown = rtclickcheck; </script> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <style type="text/css"> img{opacity: 0.5; -webkit-transition: all 250ms ease; -moz-transition: all 250ms ease; -o-transition: all 250ms ease; transition: all 250ms ease;} img:hover{opacity:
443	tls	HTTP/1.1 400 Bad Request Date: Tue, 11 Jun 2024 01:03:47 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Content-Length: 468 Connection: close Content-Type: text/html; charset=iso-8859-1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>400 Bad Request</title> </head><body> <h1>Bad Request</h1> <p>Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, pl
445	smb	#SMB<NT L
3389	tls	MfS...j...v...%...o...ne...N...!4...5...1...z...MaU...0...0...0...7...m...C...1H...0... *...H...010U KEYUBUW\IN0 240210083849Z 240811083849Z010U KEYUBUW\IN0... *...H...0...0...0...VJs...#...xa...5B)...z...g...v...h...T...K...-S...V...w...x...O...R...2...C...N...C...U...h...uL1...E...M...z...4...T...-...#...h...a...j...@...n...W...["...k...z...4e...h...nf...Papw...>...K...-c...T...l...N...Z...K...g...C..._...T...K...<...d...y...S...0...U...%...+
3389	tcpwrapped	
5985	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 10 May 2024 05:36:27 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY><h2>Not Found</h2> <hr><p>HTTP Error 404. The requested resource is not found.</p> </BODY></HTML>
47001	http	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sat, 11 May 2024 04:11:09 GMT Connection: close Content-Length: 315 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY><h2>Not Found</h2> <hr><p>HTTP Error 404. The requested resource is not found.</p> </BODY></HTML>

Figure 10: Screenshot of ports and protocols for the associated IP in Hunt. Try it out!
Directory Details

- Open Directory & C2 IP: 5.252.74.45_443
- postbank.apk SHA-1 hash: dc9a821f1e061098188503dbf7518bf263334fcd
- C2 domain: oebonur600.duckdns_org
- Triage Link: <https://tria.ge/240617-mhv8yawgqb>

Impacts on Users and Devices

The discovery of SpyNote samples in open directories poses significant risks to users, as these malicious files utilize additional infrastructure, including dynamic domains, for data exfiltration.

Once infected, users' sensitive information can be continuously siphoned to ever-changing locations, making detection and mitigation more challenging.

Conclusion

The SpyNote samples we've discussed show how even everyday apps like Google Translate and Temp Mail can be repurposed for malicious intent. These examples are just a handful of the over 40 SpyNote APKs available in Hunt, with many more likely operating undetected and stealing sensitive information.

To stay ahead of these threats, apply for a free demo of Hunt. Track and analyze numerous threats identified in open directories, analyze the infrastructure of over 80 malware families, and effectively protect your digital environment.