Taking Action Against Hackers in Pakistan and Syria

about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/

April 7, 2022

- **We took action against four distinct groups of hackers from Pakistan and Syria.**
- **The malicious activity from Pakistan targeted people in Afghanistan.**
- **Three separate hacking groups from Syria targeted a wide range of people in Syria, including civil society, journalists, humanitarian organizations and the anti-regime military forces. Each of these three hacking groups had links to the Syrian government, including Syria's Air Force Intelligence.**

Today, we are sharing actions we've taken against four distinct groups of hackers in Pakistan and Syria over the past several months. To disrupt these malicious groups, we disabled their accounts, blocked their domains from being posted on our platform, shared information with our industry peers, security researchers and law enforcement, and alerted the people who we believe were targeted by these hackers.

The group from Pakistan — known in the security industry as SideCopy — targeted people who were connected to the previous Afghan government, military, and law enforcement in Kabul. In Syria, we removed three distinct hacker groups with links to the Syrian government. The first network in Syria — known as the Syrian Electronic Army — targeted human rights activists, journalists and other groups opposing the ruling regime. We linked this activity to Syria's Air Force Intelligence. The second network from Syria — known in the security community as APT-C-37 — targeted people linked to the Free Syrian Army and former military personnel who had since joined the opposition forces. Our investigation linked this activity by APT-C-37 to what we believe is a separate unit in Syria's Air Force Intelligence. Finally, the third network from Syria targeted minority groups, activists, opposition, Kurdish journalists, activists, members of the People's Protection Units (YPG), and Syria Civil Defense or White Helmets, a volunteer-based humanitarian organization. Our investigation found links between this activity and individuals associated with the Syrian government.

Meta's threat intelligence analysts and security experts work to find and stop a wide range of threats including cyber espionage campaigns, influence operations and hacking of our platform by nation-state actors and other groups. As part of these efforts, our teams routinely disrupt adversary operations by disabling them, notifying users if they should take steps to protect their accounts, sharing our findings publicly and continuing to improve the security of our products.

Here are the details on each disruption:

1. Pakistan

In August, we removed a group of hackers from Pakistan, known in the security industry as SideCopy, that targeted people in Afghanistan, particularly those with links to the Afghan government, military and law enforcement in Kabul.Given the ongoing crisis and the government collapse at the time, we moved quickly to complete the investigation and take action to protect people on our platform, share our findings with industry peers, law enforcement and researchers, and alert those who we believe were targeted. In addition, we rolled out a number of security measures for people in Afghanistan to protect their Facebook accounts.

This malicious activity had the hallmarks of a well-resourced and persistent operation while obfuscating who's behind it. On our platform, this cyber espionage campaign ramped up between April and August of 2021 and manifested primarily in sharing links to malicious websites hosting malware.

We identified the following tactics, techniques and procedures (TTPs) used by this threat actor across the internet, including on our apps (threat indicators can be found at the end of the report):

- This group created fictitious personas — typically young women — as romantic lures to build trust with potential targets and trick them into clicking on phishing links or downloading malicious chat applications.
- They operated fake app stores and also compromised legitimate websites to host malicious phishing pages to manipulate people into giving up their Facebook credentials.

- SideCopy attempted to trick people into installing trojanized chat apps (i.e. they contained malware that misled people about its true intent), including messengers posing as Viber and Signal, or custom-made Android apps that contained malware to compromise devices. Among them were apps named HappyChat, HangOn, ChatOut, TrendBanter, SmartSnap, and TeleChat — some of which were in fact functioning chat applications.
- These apps typically included two malware families: PJobRAT and a previously unreported Android malware strain we are calling Mayhem. These two families have the ability to retrieve people's contact list, text messages, call logs, location information, media files on the device or connected external storage, and general device metadata. They can also scrape content on the device's screen via accessibility services.
- In August, 2021, the group shifted to using bit[.]ly URL shortener links to mask the final destination they were redirecting their targets to after they clicked on the malicious link.

2. Syria

In October, we took down a hacking group, known in the security community as the Syrian Electronic Army (SEA) or APT-C-27, that targeted people in Syria, including humanitarian organizations, journalists and activists in Southern Syria, critics of the government, and individuals associated with the anti-regime Free Syrian Army. Our investigation found that this threat actor has been subsumed into the Syrian government forces in recent years, with this latest activity linked to Syria's Air Force Intelligence. On our platform, this campaign manifested primarily in targeting people with social engineering tactics to trick them into clicking on links or downloading malicious software.

We identified the following TTPs used by this threat actor across the internet, including on our apps (threat indicators can be found at the end of the report):

- This group shared phishing links to lead people to either websites hosting credential phishing pages or malware. The phishing campaigns were designed to manipulate their targets into giving away their credentials to Facebook accounts.
- They used a combination of commercially available (e.g., HWorm/njRAT for Windows) and custom-built malware families (e.g., HmzaRat Desktop for Windows and SilverHawk aka HmzaRAT for Android). For example, they deployed Android malware as part of trojanized applications, including those named the United Nations, VPN Secure and several popular chat apps like Telegram — all hosted on attacker-controlled websites.
- This group also used new Android malware built with the open-source mobile app development tool Xamarin and, as of now, it's only being detected by one anti-virus engine in public virus repositories. We found this malware in trojanized versions of Telegram and a Syrian news app, that are being distributed exclusively through phishing websites hosted on the Vercel cloud platform.

- The malware families SEA relied on are capable of collecting a range of sensitive user information, once the device is compromised, including the ability to record audio and video, edit or retrieve files, call logs, address book, and text messages.

3. Syria

In October, we took down a hacking group, known in the security community as APT-C-37, that targeted people linked to the Free Syrian Army and former military personnel who had since joined the opposition forces. Our investigation linked this activity by APT-C-37 to what we believe is a separate unit in Syria's Air Force Intelligence.This operation on our platform involved social engineering tactics to trick people into clicking on links to malicious websites hosting malware or credential phishing campaigns aimed at obtaining access to people's Facebook accounts.

We identified the following TTPs used by this threat actor across the internet, including on our apps (threat indicators can be found at the end of the report):

- APT-C-37 has continued to use commodity malware known as SandroRAT in addition to an Android malware family known as SSLove, likely developed in-house.
- This group relied on social engineering to distribute malware to manipulate their targets into visiting attacker-controlled websites. Some of these sites focused on content about Islam, others masqueraded as legitimate app stores or used look-alike domains posing as popular services, including Telegram, Facebook, YouTube, and WhatsApp.
- APT-C-37 relied on Android malware with common malicious functionality to retrieve sensitive user data, including call logs, contact information, device information, user accounts, take photos, and retrieve attacker specified files.

4. Syria

We took down a hacking group that targeted minority groups; activists; opposition in Southern Syria, including in Sweida, Huran, Qunaitra and Daraa; Kurdish journalists, activists in Northern Syria, including Kamishl, Kubbani, Manbij, and Al-Hasakah; members of the People's Protection Units (YPG); and Syria Civil Defense (the White Helmets, a volunteer-based humanitarian organization). Our investigation found links between this activity and individuals associated with the Syrian government. On our platform, this operation manifested primarily as social engineering and sharing links to malicious websites.

We identified the following TTPs used by this threat actor across the internet, including on our apps (threat indicators can be found at the end of the report):

- This group shared links to attacker-controlled websites hosting Android malware masquerading as apps and updates themed around the United Nations, White Helmets, YPG, Syrian satellite TV, COVID-19, WhatsApp and YouTube.

- Likely due to this operation’s reliance on commercially available malware, this group has not been separately tracked by the security community. While this likely limited their effectiveness thanks to the existing anti-virus detection aimed at these commodity tools, it has also perhaps allowed them to hide in the noise.
- Among the commodity Android malware this group used: SpyNote and SpyMax.

Threat Indicators

1. Pakistan

Domains & C2s:

Domain	Description
androappstore[.]com	Hosting PJobRAT and Mayhem
www[.]apphububstore[.]in	Hosting PJobRAT
appsstore[.]in	Hosting PJobRAT
apkstore.filehubspot[.]com	Believed to be hosting PJobRAT
helloworld.bounceme[.]net	Command and control server for PJobRAT
dasvidaniya.ddns[.]net	Command and control server for PJobRAT
gemtool.sytes[.]net	Command and control server for PJobRAT
saahas.servecounterstrike[.]com	Command and control server for Mayhem

Hashes:

MD5	Description	Malware Family
7804aa608d73e7a9447ae177c31856fe	ViberLite v4	PJobRAT
a80a1b022fdcaa171e454086711dcf35	ViberLite v3	PJobRAT
a4f104e2058261c7dbfc1c69e1de8bce	ViberLite v2	PJobRAT
4ce92da8928a8d1d72289d126a9fe2f4	HangOn V4e	PJobRAT
a53c74fa923edce0fa5919d11f945bcc	HangOn v4	PJobRAT
9fd4b37cbaf0d44795319977118d439d	HangOn	PJobRAT
7bef7a2a6ba1b2aceb84ff3adb5db8b3	TrendBanter	PJobRAT

v21b4327d6881be1893fd2a8431317f6b	Happy Chat	Mayhem

2. SEA / APT-C-27

Domains & C2s:

Domain / IP	Description
faccebookaccunt[.]blogspot[.]com	Credential phishing
ruba-bakkour-facebook[.]blogspot[.]com	Credential phishing
chatsafe[.]tecnova.com[.]br	Distribution of SilverHawk in 2020
download-telegram.vercel[.]app	Used by SEA affiliated individuals to distribute a new unnamed Android family
download-revo.vercel[.]app	Used by SEA affiliated individuals to distribute a new unnamed Android family
82.137.218[.]185	Command and control server. Used to distribute a variety of commodity and custom Android malware.

Hashes:

MD5	Description	Malware Family
df196bd42e1da1d34c23c8d947561618	Fake version of Telegram	Unnamed
ccabc8f4868184a04b032b34d9303810	Trojanized Syrian News app	Unnamed

3. APT-C-37

Domains & C2s:

Domain / IP	Description
82.137.255[.]0	Long running command and control server

Hashes:

MD5	Description	Malware Family
969fe5597a44bf4eb66ebdc7b09ef2c8	Fake version of WhatsApp	SSLove

4. Unnamed Cluster

Domains & C2s:

Domain / IP	Description
f-b[.]today	Hosting SpyMax
messengers[.]video	Hosting SpyMax
whatsapp-sy[.]com	Hosting SpyMax
horan-free[.]com	Believed to have been hosting SpyMax
druze[.]life	Believed to have been hosting SpyMax
suwayda-24[.]com	Believed to have been hosting SpyMax
t-me[.]link	Believed to have been hosting SpyMax
lamat-horan[.]com	Hosting unnamed Android malware
anti-corona[.]app	Believed to have been hosting SpyMax
what-sapp[.]site	Believed to have been hosting SpyMax
informnapalm[.]net	Hosting trojanized apps for the YPG, Syrian Civil Defense, and malware pretending to be an update for WhatsApp.
facebook-helps-center[.]com	Older infrastructure hosting SpyMax malware pretending to be a WhatsApp update.
46.4.83[.]140	Command and control server
sputniknews[.]news	Believed to be attacker controlled
emmashop[.]app	Believed to be attacker controlled
face-book[.]xyz	Believed to be attacker controlled.

Hashes:

MD5	Description	Malware Family
762acdd53eb35cd48686b72811ba9f3c	Hosted on lamat-horan[.]com. First seen in 2019. 0 detections on VT.	Unnamed

fcf357556c3af14bab820810f5e94436	Hosted on f-b[.]today. Masquerading as a Syrian satellite TV app.	SpyMax
e8a528491b28e4d62a472da7396c7047	Hosted on f-b[.]today. Masquerading as a YouTube update.	SpyMax
1c16ee8b2f0dff7280e1d97522ee7e3f	Hosted on informnapalm[.]net. A Syria themed APK.	SpyNote
ce274c0bd0743695529a43d7992e2d2c	Hosted on informnapalm[.]net. Masquerading as a WhatsApp update.	SpyMax
185062606b168f04b8b583045d300be5	Hosted on informnapalm[.]net. Masquerading as an app for the YPG.	SpyMax
c2e55b0d7be1c1991a5b70be7280e528	Hosted on informnapalm[.]net. Masquerading as an app for the Syrian Civil Defence.	SpyMax