Taking Action Against Hackers in Palestine

about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/

April 7, 2022

Today, we're sharing actions we took against two separate groups of hackers in Palestine — a network linked to the Preventive Security Service (PSS) and a threat actor known as Arid Viper — removing their ability to use their infrastructure to abuse our platform, distribute malware and hack people's accounts across the internet. To the best of our knowledge, this is the first public reporting of this PSS activity.

Facebook 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 people if they should take steps to protect their accounts, sharing our findings publicly and continuing to improve the security of our products.

Today we're sharing our latest research into two clusters of unconnected cyber espionage activity. One of them targeted primarily domestic audiences in Palestine. The other cluster targeted audiences in the Palestinian territories and Syria and to a lesser extent Turkey, Iraq, Lebanon and Libya.

To disrupt both these operations, we took down their accounts, released malware hashes, blocked domains associated with their activity and alerted people who we believe were targeted by these groups to help them secure their accounts. We shared information with our industry partners including the anti-virus community so they too can detect and stop this activity, strengthening our collective response against these groups across the internet. We encourage people to remain vigilant and take steps to protect their accounts, avoid clicking on suspicious links and downloading software from untrusted sources that can compromise their devices and information stored on them.

The groups behind these operations are persistent adversaries, and we know they will evolve their tactics in response to our enforcement. However, we keep improving our detection systems and collaborating with other teams in the security community to continue making it harder for these threat actors to remain undetected. We'll keep sharing our findings when possible so people are aware of the threats we're seeing and can take steps to strengthen the security of their accounts.

Here's What We Found

PSS-Linked Group

This activity originated in the West Bank and focused on the Palestinian territories and Syria, and to a lesser extent Turkey, Iraq, Lebanon and Libya. It relied on social engineering to trick people into clicking on malicious links and installing malware on their devices. Our investigation found links to the Preventive Security Service — the Palestinian Authority's internal intelligence organization.

This persistent threat actor focused on a wide range of targets, including journalists, people opposing the Fatah-led government, human rights activists and military groups including the Syrian opposition and Iraqi military. They used their own low-sophistication malware disguised as secure chat applications, in addition to malware tools openly available on the internet.

Our investigation analyzed a number of notable tactics, techniques and procedures (TTPs):

- **Android malware:** This group's custom-built Android malware had relatively simple functionality and required a limited set of device-level permissions, which likely helped it to stay under the radar for most anti-virus detection systems. This malware masqueraded as secure chat applications. Once installed, it collected information such as device metadata (e.g. manufacturer, OS version, IMEI), call logs, location, contacts and text messages. In rare cases, it also contained keylogger functionality — an ability to record every keystroke made on a device. Once collected, the malware would upload the data to Firebase, a mobile app development platform. In addition to their custom-made malware, this group also utilized publicly available Android malware called SpyNote which had more functionality including remote device access and the ability to monitor calls.
- **Windows malware:** This group occasionally deployed publicly available malware for Windows, including NJRat and HWorm, commonly used in the region. They also bundled Windows malware in the installer package for their own decoy application for journalists to submit human rights-related articles for publication. This app had no legitimate functionality.
- **Social engineering:** This group used fake and compromised accounts to create fictitious personas posing primarily as young women, and also as supporters of Hamas, Fatah, various military groups, journalists and activists to build trust with people they targeted and trick them into installing malicious software. Some of their Pages were designed to lure particular followers for later social engineering and malware targeting. Likely to build audiences, these Pages posted memes criticizing Russian foreign policy in the Middle East, Russian military contractor Wagner Group and its involvement in Syria and Libya and the Assad government.

Threat Indicators:

Android C2 Domains

```
news-fbcb4.firebaseio[.]com
news-fbcb4.appspot[.]com
chaty-98547.firebaseio[.]com
chaty-98547.appspot[.]com
jamila-c8420.firebaseio[.]com
jamila-c8420.appspot[.]com
showra-22501.firebaseio[.]com
showra-22501.appspot[.]com
goodwork-25869.firebaseio[.]com
goodwork-25869.appspot[.]com
advance-chat-app.firebaseio[.]com
advance-chat-app.appspot[.]com
filtersapp-715ee.firebaseio[.]com
filtersapp-715ee.appspot[.]com
humanrights-1398b.firebaseio[.]com
humanrights-1398b.appspot[.]com
jamilabouhaird-c0935.firebaseio[.]com
jamilabouhaird-c0935.appspot[.]com
hotchat-f0c0e.appspot[.]com
hotnewchat.appspot[.]com
```

Android Hashes

```
aeb0c38219e714ab881d0065b9fc1915ba84ad5b86916a82814d056f1dfaf66d
3c21c0f64ef7b606abb73b9574d0d66895e180e6d1cf2ad21addd5ade79b69fb
d2787aff6e827809b836e62b06cca68bec92b3e2144f132a0015ce397cf3cac2
2580f7afb4746b223b14aceab76bd8bc2e4366bfa55ebf203de2715176032525
f7ea82e4c329bf8e29e9da37fcaf35201dd79c2fc55cc0feb88aedf0b2d26ec2
0540051935145fb1e3f9361ec55b62a759ce6796c1f355249805d186046328dc
03de278ec4c4855b885520a377f8b1df462a1d8a4b57b492b3b052aafe509793
fe77e052dc1a8ebea389bc0d017191e0f41d8e47d034c30df95e3d0dc33cfe10
6356d55c79a82829c949a46c762f9bb4ca53da01a304b13b362a8a9cab20d4d2
9a53506c429fa4ff9113b2cbd37d96c708b4ebb8f3424c1b7f6b05ef678f2230
bf61c078157dd7523cb580672273190de5de3d41577f5d66c5afcdfeade09213
154cb010e8ac4c50a47f4b218c133b5c7d059f5aff4c2820486e0ae511966e89
44ccafb69e61139d9107a87f58133c43b8586931faf620c38c1824057d66d614
```

SpyNote C2

```
lion20810397.ddns[.]net
```

Windows Malware C2 Domains

```
camera.dvrcam[.]info
facebooks.ddns[.]me
google.loginto[.]me
```

Windows Malware Hashes

```
05320c7348c156f0a98907d2b1527ff080eae36437d58735f2822d9f42f5d273
```

Links to Android Malware

```
app-chat1.atwebpages[.]com
app-showchat.atwebpages[.]com
showra-chat.atwebpages[.]com
```

Arid Viper

This activity originated in Palestine and targeted individuals in the same region, including government officials, members of the Fatah political party, student groups and security forces. Our investigation linked this campaign to Arid Viper, a known advanced persistent threat actor. It used sprawling infrastructure to support its operations, including over a hundred websites that either hosted iOS and Android malware, attempted to steal credentials through phishing or acted as command and control servers.

They appear to operate across multiple internet services, using a combination of social engineering, phishing websites and continually evolving Windows and Android malware in targeted cyber espionage campaigns.

We shared threat indicators with industry peers and security researchers as part of a concerted effort to disrupt this group's operations. We're also sharing a detailed technical report with our findings, including threat indicators to help advance our industry's understanding of this adversary (below).

Here are our key findings and some of the notable tactics, techniques and procedures (TTPs) we've observed:

Custom iOS Surveillanceware:

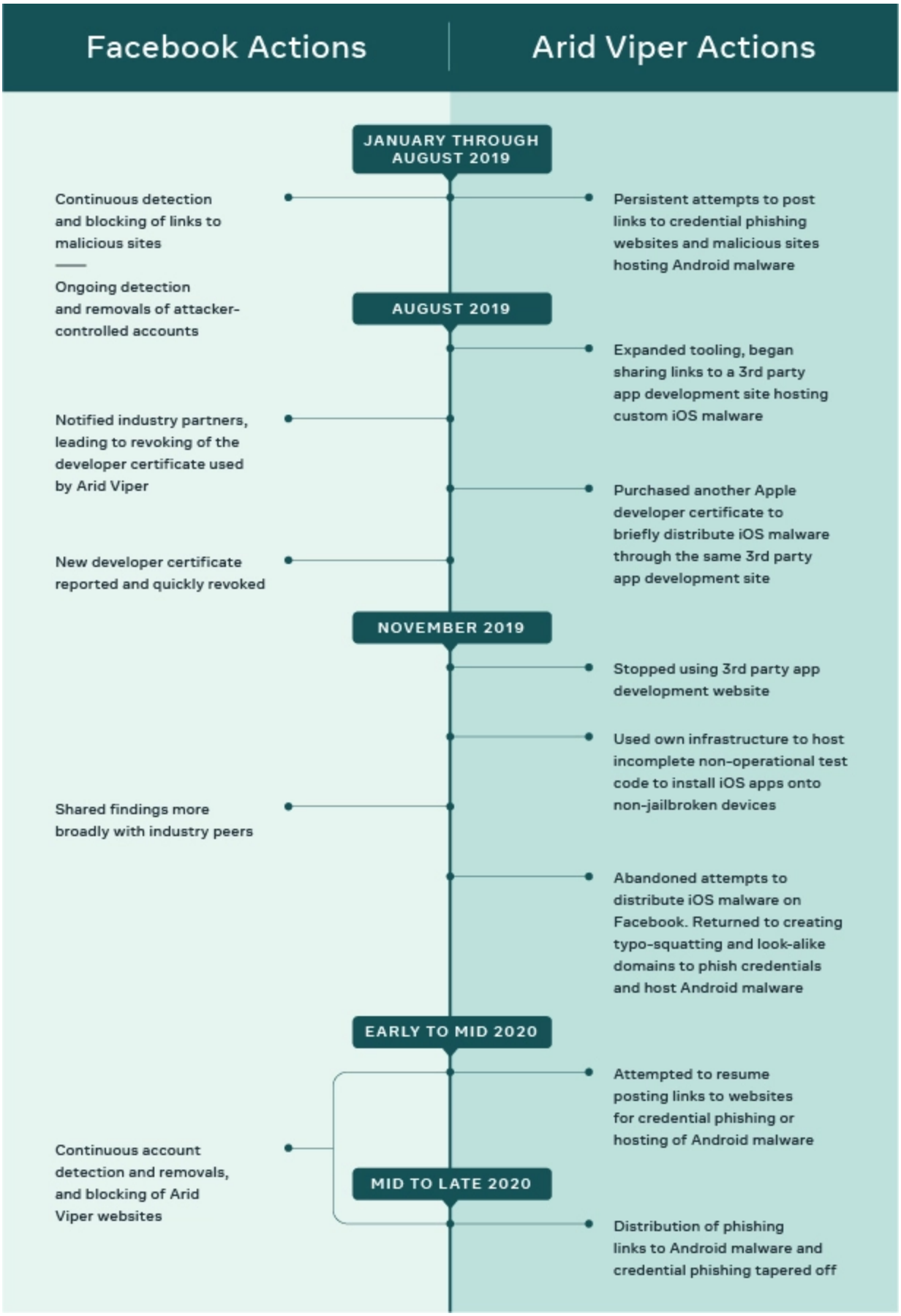
- Arid Viper used custom-built iOS surveillanceware which hasn't been previously reported and reflects a tactical shift. We call this iOS component Phenakite due to it being rare and deriving its name from the Greek word Phenakos, meaning to deceive or cheat.
- Installation of Phenakite required that people be tricked into installing a mobile configuration profile. This allowed for a device-specific signed version of the iOS app to be installed on a device. A jailbroken device wasn't required.
- Post-installation, a jailbreak was necessary for the malware to elevate its privileges to retrieve sensitive user information not accessible via standard iOS permission requests. This was achieved with the publicly available Osiris jailbreak that made use of the Sock Port exploit, both of which were bundled in the malicious iOS app store packages (IPAs).
- Arid Viper's iOS surveillanceware was trojanized inside a fully functional chat application that used the open-source RealtimeChat code for legitimate app functionality. This malware could also direct people to phishing pages for Facebook and iCloud to steal their credentials for those services.
- Arid Viper's use of custom iOS surveillanceware shows that this capability is becoming increasingly attainable by adversaries believed to be of lower sophistication.

Evolving Android and Windows Malware

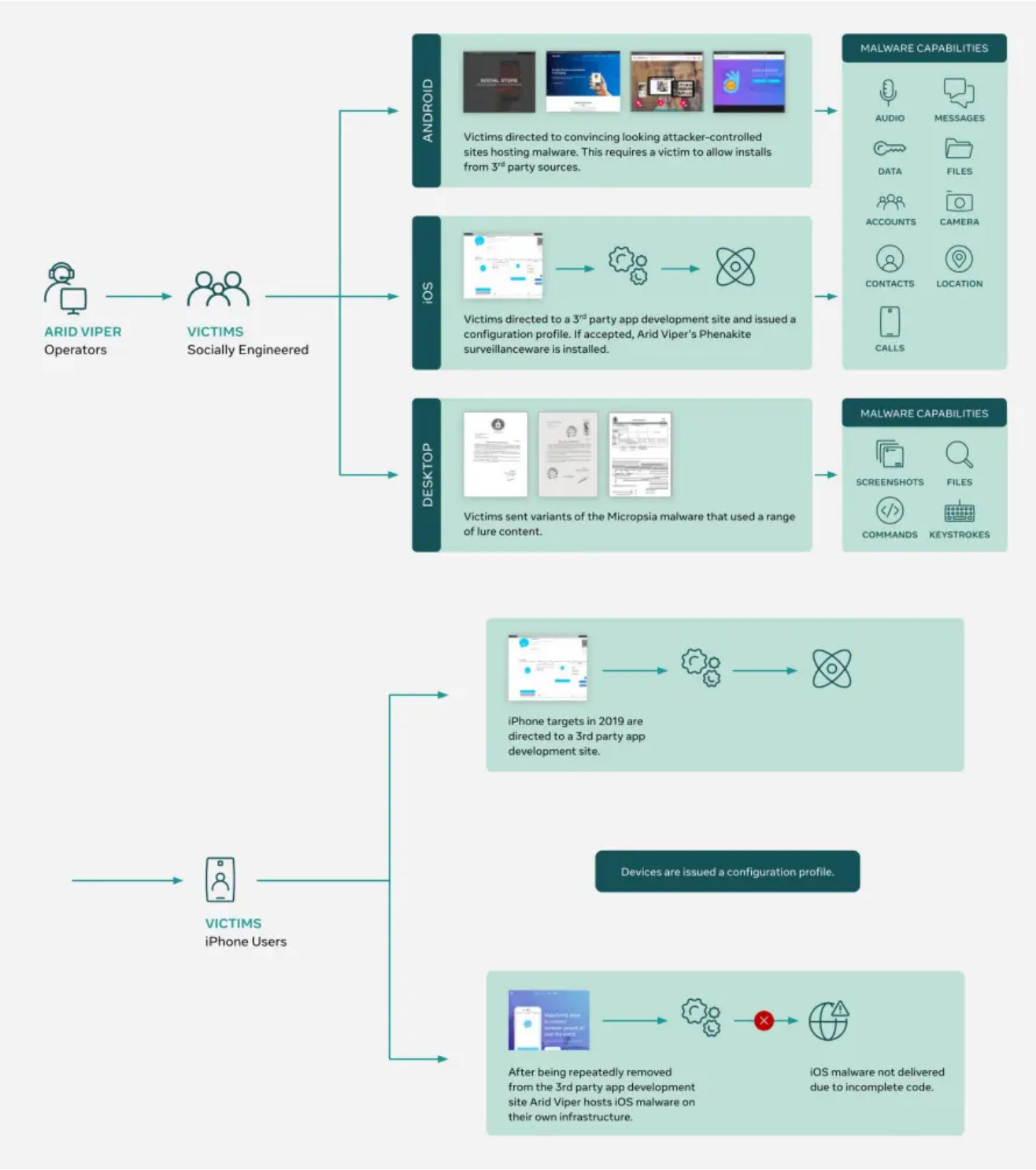
- The Android tooling used by Arid Viper shares many similarities with malware previously reported as FrozenCell and VAMP.
- The Android malware deployed by Arid Viper required people to install apps from third-party sources on their devices. The group used various convincing, attacker-controlled sites to create the impression that the apps were legitimate.
- Arid Viper's recent operations also used variants of a malware family known as Micropsia, which previously has been associated with this threat actor.

Malware Distribution

- Delivery of both the Android and iOS malware involved social engineering.
- Android malware was typically hosted on convincing looking attacker-controlled phishing sites. At the time of this writing, we discovered 41 such sites.
- iOS malware was previously found to be distributed from a 3rd party Chinese app development site. After we shared our findings with industry partners which led to the revocation of multiple developer certificates, Arid Viper's ability to distribute Phenakite was disrupted. We've since seen them try setting up their own infrastructure to distribute their iOS implant.
- While Arid Viper tooling has previously been discovered in official app channels like the Play Store, we didn't find it to be the case in this most recent campaign.



Compromise Flow:



See the full Threat Report on Arid Viper for more information and IOCs.

Downloads
Technical Threat Report: Arid Viper