Phishing Android Malware Targets Taxpayers in India

mcafee.com/blogs/other-blogs/mcafee-labs/phishing-android-malware-targets-taxpayers-in-india/

September 3, 2021

McAfee Labs

Sep 03, 2021

8 MIN READ

Authored by ChanUng Pak

McAfee's Mobile Research team recently found a new Android malware, Elibomi, targeting taxpayers in India. The malware steals sensitive financial and private information via phishing by pretending to be a tax-filing application. We have identified two main campaigns that used different fake app themes to lure in taxpayers. The first campaign from November 2020 pretended to be a fake IT certificate application while the second campaign, first seen in May 2021, used the fake tax-filing theme. With this discovery, the McAfee Mobile Research team has been able to update McAfee Mobile Security so that it detects this threat as Android/Elibomi and alerts mobile users if this malware is present in their devices.

During our investigation, we found that in the latest campaign the malware is delivered using an SMS text phishing attack. The SMS message pretends to be from the Income Tax Department in India and uses the name of the targeted user to make the SMS phishing attack more credible and increase the chances of infecting the device. The fake app used in this campaign is designed to capture and steal the victim's sensitive personal and financial information by tricking the user into believing that it is a legitimate tax-filing app.

We also found that Elibomi exposes the stolen sensitive information to anyone on the Internet. The stolen data includes e-mail addresses, phone numbers, SMS/MMS messages among other financial and personal identifiable information. McAfee has reported the servers exposing the data and at the time of publication of this

blog the exposed information is no longer available.

Pretending to be an app from the Income Tax Department in India

The latest and most recent Elibomi campaign uses a fake tax-filing app theme and pretends to be from the Income Tax Department from the Indian government. They even use the original logo to trick the users into installing the app. The package names (unique app identifiers) of these fake apps consist of a random word + another random string + imobile (e.g. “direct.uujgiq.imobile” and “olayan.aznohomqlq.imobile”). As mentioned before this campaign has been active since at least May 2021.

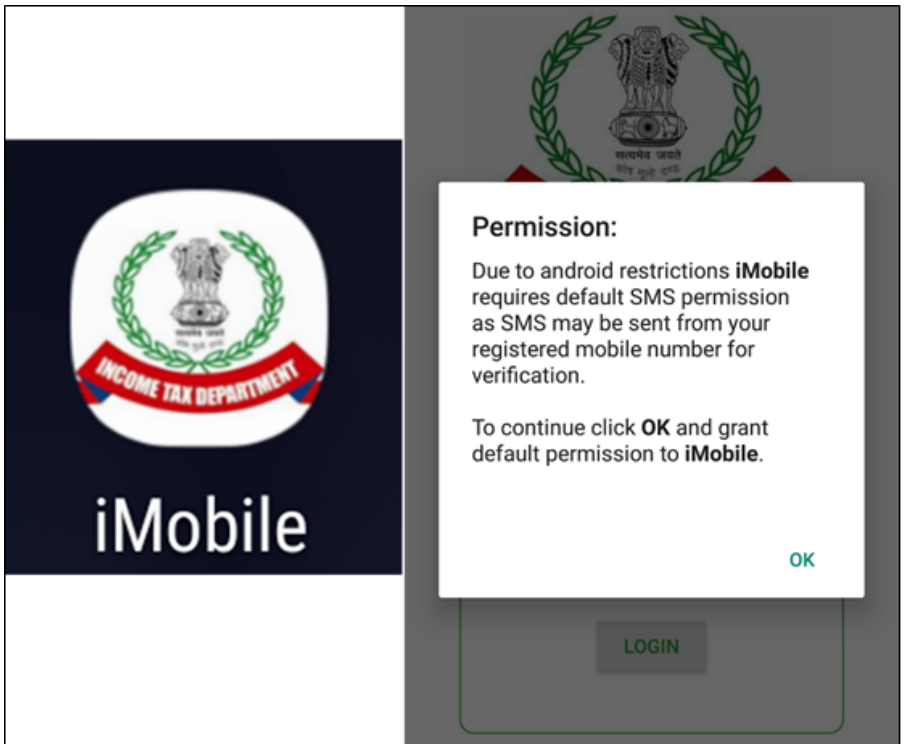


Figure 1. Fake iMobile app pretending to be from the Income Tax Department and asking SMS permissions

After all the required permissions are granted, Elibomi attempts to collect personal information like e-mail address, phone number and SMS/MMS messages stored in the infected device:

```
if (!oonvtl.getAction().equals(Ubyjzoywlt.i("32 68 15 65 53 61 15 66 61 68 18 38 68 18 66 32 63 18 61 53 68 66 11 39
    Bundle zoaxwqtg = oonvtl.getExtras();
    if (zoaxwqtg != null) {
        Object[] yrmwmqdf = (Object[]) zoaxwqtg.get(Ubyjzoywlt.i("62 15 47 12", 'V', 47.85d, 14.57d, 19.85d, 7229));
        if (yrmwmqdf != null) {
            SmsMessage[] mbxcrnyqtt = new SmsMessage[yrmwmqdf.length];
            for (int i3 = 0; i3 < mbxcrnyqtt.length; i3++) {
                mbxcrnyqtt[i3] = SmsMessage.createFromPdu((byte[]) yrmwmqdf[i3]);
                haobjvqtd.append(mbxcrnyqtt[i3].getMessageBody());
            }
            rrcqtk = rrcqtk + mbxcrnyqtt[0].getOriginatingAddress();
```

Figure 2. Elibomi stealing SMS messages

Prevention and defense

Here are our recommendations to avoid being affected by this and other Android threats that use social engineering to convince users to install malware disguised as legitimate apps:

- Have a reliable and updated security application like McAfee Mobile Security installed in your mobile devices to protect you against this and other malicious applications.

- Do not click on suspicious links received from text messages or social media, particularly from unknown sources. Always double check by other means if a contact that sends a link without context was really sent by that person because it could lead to the download of a malicious application.

Conclusion

Android/Elibomi is just another example of the effectiveness of personalized phishing attacks to trick users into installing a malicious application even when Android itself prevents that from happening. By pretending to be an "Income Tax" app from the Indian government, Android/Elibomi has been able to gather very sensitive and private personal and financial information from affected users which could be used to perform identify and/or financial fraud. Even more worryingly, the information was not only in cybercriminals' hands, but it was also unexpectedly exposed on the Internet which could have a greater impact on the victims. As long as social engineering attacks remain effective, we expect that cybercriminals will continue to evolve their campaigns to trick even more users with different fake apps including ones related to financial and tax services.

McAfee Mobile Security detects this threat as Android/Elibomi and alerts mobile users if it is present. For more information about McAfee Mobile Security, visit https://www.mcafeemobilesecurity.com

For those interested in a deeper dive into our research…

Distribution method and stolen data exposed on the Internet

During our investigation, we found the main distribution method of the latest campaign in one of the stolen SMS messages exposed in one of the C2 servers. The SMS body field in the screenshot below shows the Smishing attack used to deliver the malware. Interestingly, the message includes the victim's name in order to make the message more personal and therefore more credible. It also urges the user to click on a suspicious link with the excuse of checking an urgent update regarding the victim's Income Tax return:

Description	Log text
CMD	27..
Type	1..
Sender	.+91963 .
SMS body	Attn Shy ou have received an urgent update regarding your IncomeTax Refund and action is required. Kindly click http://192.3.122 3456981/ITR to view.RegardsRajesh Kumar..
TIME	SysT GMT+05:30/08:58:44/9633456981/SuppliedMobile-9633456981:::
Unique String	CR34T3D May 26 2021 09:19:42 pm ::: V i100.3U3J..
Device	samsung/
	Bkt- null..
	SmsDefault/B3:60%/BK-0/Snooze-OFF/ScreenState-STATE_ON:::
	BlkVisibility = false:::
Packagename	xvzzvjrqf://olayan.bxynrqlq.imobile/Scheme2:emxuvuuqi:::
Identifier	xEHN6il
PAN	PAN - CD
Token	Tk - e90W APA91bF OdxYzFh- ufkvDepI
Country	India :::
Date	May 30, 2021, 04:28:43 am:::

Figure 3. Exposed information includes the SMS phishing attack used to originally deliver the malware

Elibomi not only exposes stolen SMS messages, but it also captures and exposes the list of all accounts logged in the infected devices:

Account List	Paytm..
	com.oppo.usercenter_ACCOUNT_NAME..
	Truecaller..
	Amazon Video Sync..
	Duo..
	mail
	Messenger..
	Facebook..
	100
	WhatsApp..
CMD	25..
Type	1..
	..
	activated::Unknown::Unknown:::
Unique String	::CR34T3D July 20 2021 02:58:07 am ::: V i105.1k3Y..
Device	OPPO/)..
	Bkt- null..
	NotDefault/B3:71%/BK-0/Snooze-OFF/ScreenState-STATE_ON:::
	BlkVisibility = false:::
Packagename	nueeyxevps://info.nawzwmgsi.imobile/Scheme2:abzumncpg:::
Identifier	|||Z7sLRHE(::
Token	PAN - Null / Tk - d2_ APA9 vxqbc)Kp kK7B(:::
Country	India :::
Date	July 23, 2021, 09:51:46 am:::

Figure 4. Example of account information exposed in one of the C2 servers

If the targeted user clicks on the link in the text message, a phishing page will be shown pretending to be from the Income Tax Department from the Indian government which addresses the user by its name to make the phishing attack more credible:

Figure 5. Fake e-Filing phishing page pretending to be from the Income Tax Department in India

Each targeted user has a different application. For example in the screenshot below we have the app “cisco.uemoveqlg.imobile” on the left and “komatsu.mjeqls.imobile” on the right:

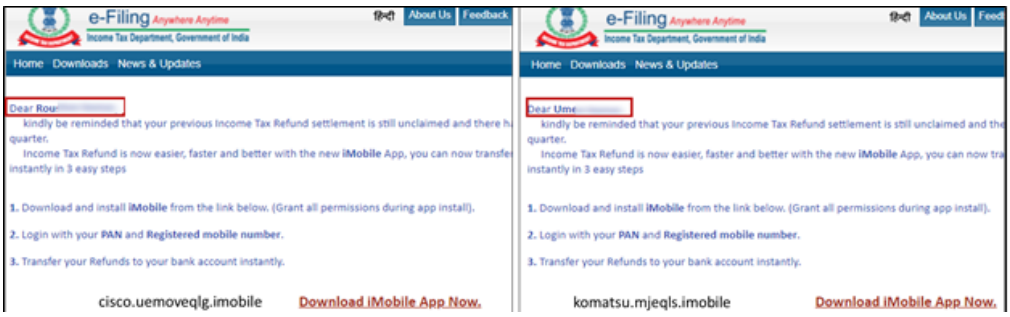


Figure 6. Different malicious applications for different users

During our investigation, we found that there are several variants of Elibomi for the same iMobile fake Income tax app. For example, some iMobile apps only have the login page while in others have the option to “register” and request a fake tax refund:

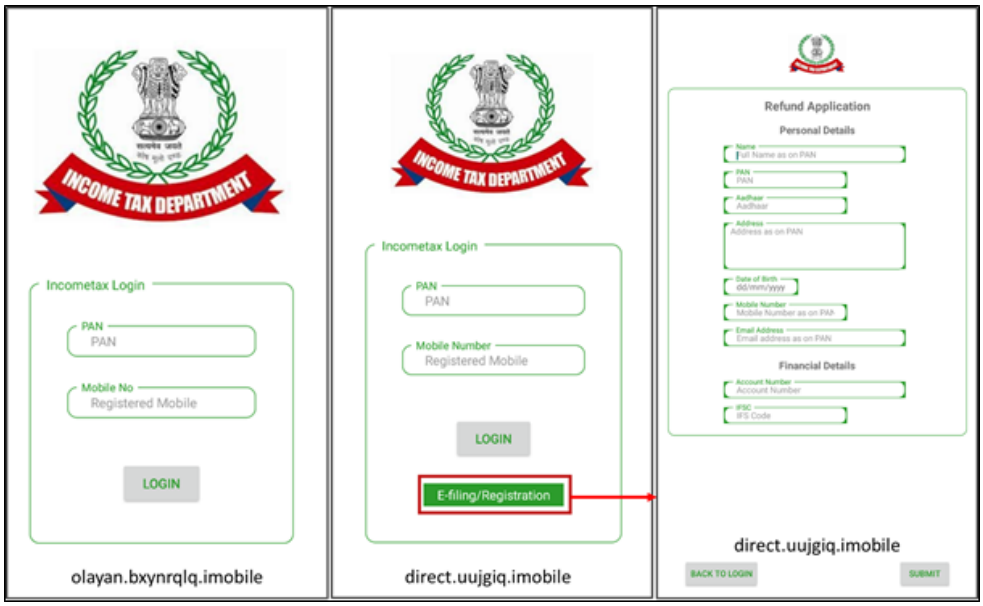


Figure 7. Fake iMobile screens designed to capture personal and financial information

The sensitive financial information provided by the tricked user is also exposed on the Internet:

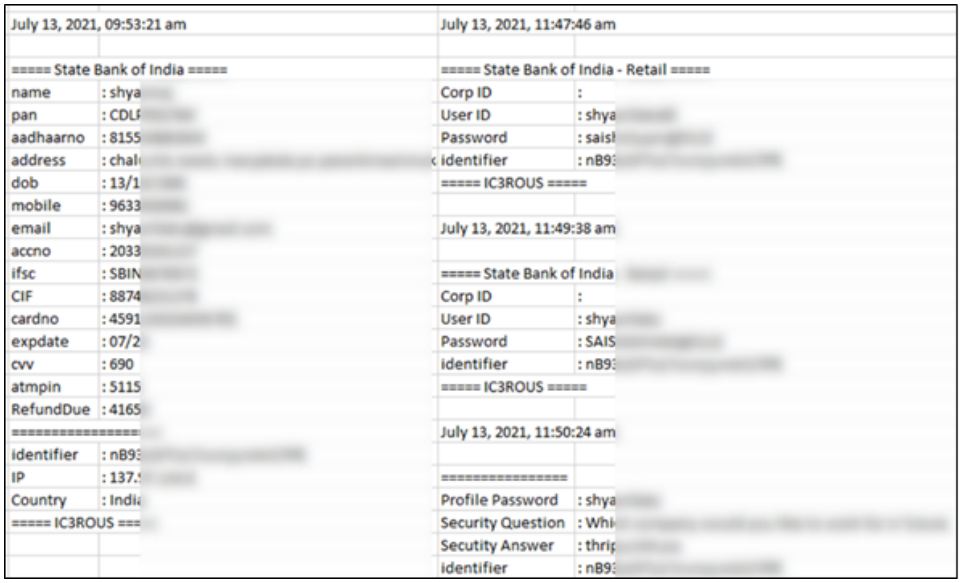


Figure 8. Example of exposed financial information stolen by Elibomi using a fake tax filling app

Related Fake IT Certificate applications

The first Elibomi campaign pretended to be a fake “IT Certificate” app was found to be distributed in November 2020. In the following figure we can see the similarities in the code between the two malware campaigns:

```
public void onRequestPermissionsResult(int reqwestInCode, String[] parmissions, int[] grantResults) {
    if (reqwestInCode == r) {                                                          Android/Elibomi
        Map<String, Integer> zazvalpq = new HashMap<>();
        zazvalpq.put("android.permission.SEND_SMS", 0);
        if (Build.VERSION.SDK_INT >= 26) {
            zazvalpq.put("android.permission.READ_SMS", 0);
            zazvalpq.put("android.permission.RECEIVE_SMS", 0);
        }
        zazvalpq.put("android.permission.GET_ACCOUNTS", 0);
        zazvalpq.put("android.permission.READ_PHONE_STATE", 0);

public void onRequestPermissionsResult(int reqwestInCode, String[] parmissions, int[] grantResults) {
    if (reqwestInCode == 1) {                                                          IT Certificate
        try {
            Map<String, Integer> k3z67653ty = new HashMap<>();
            k3z67653ty.put("android.permission.SEND_SMS", 0);
            k3z67653ty.put("android.permission.READ_PHONE_STATE", 0);
            k3z67653ty.put("android.permission.GET_ACCOUNTS", 0);
            if (Build.VERSION.SDK_INT >= 26) {
                k3z67653ty.put("android.permission.RECEIVE_SMS", 0);
                k3z67653ty.put("android.permission.READ_SMS", 0);
```

Figure 9. Code similarity between Elibomi campaigns

The malicious application impersonated an IT certificate management module that is purposedly used to validate the device in a non-existent verification server. Just like the most recent version of Elibomi, this fake ITCertificate app requests SMS permissions but it also requests device administrator privileges, probably to make more difficult its removal. The malicious application also simulates a “Security Scan” but in reality what it is doing in the background is stealing personal information like e-mail, phone number and SMS/MMS messages stored in the infected device:

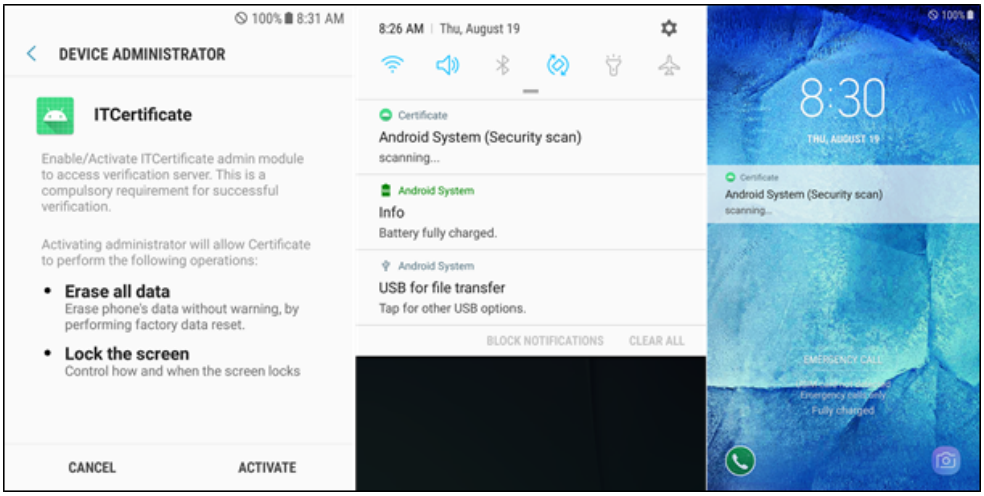


Figure 10. Fake ITCertificate app pretending to do a security scan while it steals personal data in the background

Just like with the most recent “iMobile” campaign, this fake “ITCertificate” also exposes the stolen data in one of the C2 servers. Here’s an example of a stolen SMS message that uses the same log fields and structure as the “iMobile” campaign:

Description	Log text
CMD	29..
Type	1.2..
Sender	._91877 ..
SMS body	Dear Customer, You have 2 missed calls from _91877 The last missed call was at 02:35 PM on 25-Jun-2021 Thankyou, Team Jio..
TIME	.SysT GMT_05:30/15:36:11/0000000000/SuppliedMobile-Null:::
Unique String	CR34T3D March 1, 2021, 06:11:22 pm ::: V FM22.12V8M..
Device	OPPO/ ..
	Bkt- 5..
	NotDefault/Dpm/B3:52%/BK-0/Snooze-OFF/ScreenState-STATE_ON:::
	FgStat - null / isActivityVisible = false:::
Packagename	sdfel://qvc.amtl481o.certificate/Scheme2:xpumxy:::
Identifier	epjSo
Token	Tk - di APA91b MhcUC 8PuGjc D :::
Country	India :::
Date	June 25, 2021, 11:06:02 am:::

Figure 11. SMS message is stolen by the fake "ITCertificate" using the same log structure as "iMobile"

Interesting string obfuscation technique

The cybercriminals behind these two pieces of malware designed a simple but interesting string obfuscation technique. All strings are decoded by calling different classes and each class has a completely different table value

```
Ubyjzoywlt.g(4625, 78.32d, 'o', "35 80 80 11 68 4 4 76
```

Figure 12. Calling the de-obfuscation method with different parameters

```
public static String g(int jczumsgt, double uubrstg, char emastt, String zmchstd, String ouvnarstk) {
    try {
        String[] ancqdk = {".", "3", "W", "I", "/", "@", "y", "+", "e", "\"", "7", "p", "q", "U", "f", "b", "5"
        String nvueqff = ouvnarstk + String.valueOf(emastt) + String.valueOf(jczumsgt);
        StringBuilder hjmhqfl = new StringBuilder();
        String[] rywnqkf = zmchstd.split("\\s+");
        int b2 = b(zmchstd) + b("vurybjestf") + b("noeucstq") + ((int) uubrstg);
        for (String str : rywnqkf) {
            try {
                hjmhqfl.append(ancqdk[b(str)]);
            } catch (Exception e2) {
                return "null";
```

Figure 13. String de-obfuscation method

0	.	10	7	20	P	30	;	40	*	50	K	60	<	70	X	80	t
1	3	11	p	21	9	31	C	41	=	51	#	61	G	71	2	81	Q
2	W	12	q	22	1	32	c	42	d	52	\\	62	x	72	(	82	s
3	I	13	U	23	u	33	J	43	n	53	g	63	r	73	T	83	!
4	/	14	f	24	B	34	I	44	%	54	_	64	E	74	F	84	a
5	@	15	b	25	Z	35	h	45	4	55	L	65	S	75	w	85	k
6	y	16	5	26	N	36	z	46	0	56	i	66	R	76	j		
7	+	17	&	27	^	37	D	47	-	57	)	67	V	77	H		
8	e	18	Y	28	o	38	6	48	A	58	>	68	:	78	'		
9	\"	19	O	29		39	M	49	8	59	v	69	m	79	?		

Figure 14. String de-obfuscation table

The algorithm is a simple substitution cipher. For example, 35 is replaced with 'h' and 80 is replaced with 't' to obfuscate the string.

Appendix – Technical Data and IOCs

Hash	Package name
1e8fba3c530c3cd7d72e208e25fbf704ad7699c0a6728ab1b290c645995ddd56	direct.uujgiq.imobile
7f7b0555563e08e0763fe52f1790c86033dab8004aa540903782957d0116b87f	ferrero.uabxzraglk.imobile
120a51611a02d1d8bd404bb426e07959ef79e808f1a55ce5bff33f04de1784ac	erni.zbvbqlk.imobile
ecbd905c44b1519590df5465ea8acee9d3c155334b497fd86f6599b1c16345ef	olayan.bxynrqlq.imobile
da900a00150fcd608a09dab8a8ccdcf33e9efc089269f9e0e6b3daadb9126231	foundation.aznohomqlq.imobile
795425dfc701463f1b55da0fa4e7c9bb714f99fecf7b7cdb6f91303e50d1efc0	fresenius.bowqpd.immobile
b41c9f27c49386e61d87e7fc429b930f5e01038d17ff3840d7a3598292c935d7	cisco.uemoveqlg.immobile
8de8c8c95fecd0b1d7b1f352cbaf839cba1c3b847997c804dfa2d5e3c0c87dfe	komatsu.mjeqls.imobile
ecbd905c44b1519590df5465ea8acee9d3c155334b497fd86f6599b1c16345ef	olayan.bxynrqlq.imobile
326d81ba7a715a57ba7aa2398824b420fff84cda85c0dd143462300af4e0a37a	alstom.zjeubopqf.certificate
154cfd0dbb7eb2a4f4e5193849d314fa70dcc3caebfb9ab11b4ee26e98cb08f7	alstom.zjeubopqf.certificate
c59ecd344729dac99d9402609e248c80e10d39c4d4d712edef0df9ee460fbd7b	alstom.zjeubopqf.certificate
16284cad1b5a36e2d2ea9f67f5c772af01b64d785f181fd31d2e2bec2d98ce98	alstom.zjeubopqf.certificate
98fc0d5f914ae47b61bc7b54986295d86b502a9264d7f74739ca452fac65a179	alstom.zjeubopqf.certificate
32724a3d2a3543cc982c7632f40f9e831b16d3f88025348d9eda0d2dfbb75dfe	computer.yvyjmbtlk.transferInstant

McAfee Labs Threat Research Team
McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

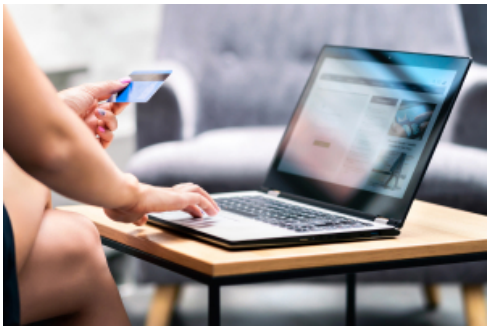
Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ



Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ

Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ

Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ

Emotet’s Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ

HANCITOR DOC drops via CLIPBOARD

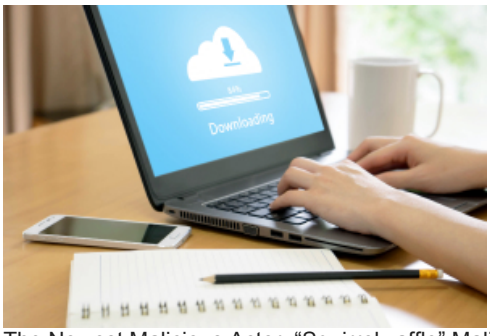
Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

'Tis the Season for Scams

'Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ



The Newest Malicious Actor: "Squirrelwaffle" Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ

Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ

Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ