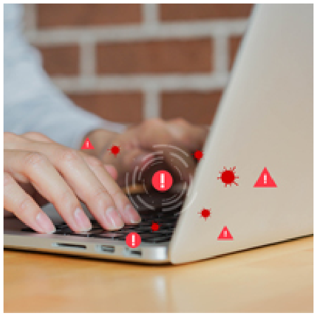
Roaming Mantis Amplifies Smishing Campaign with OS-Specific Android Malware

kashifali.ca/2021/05/05/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/

May 5, 2021 feed

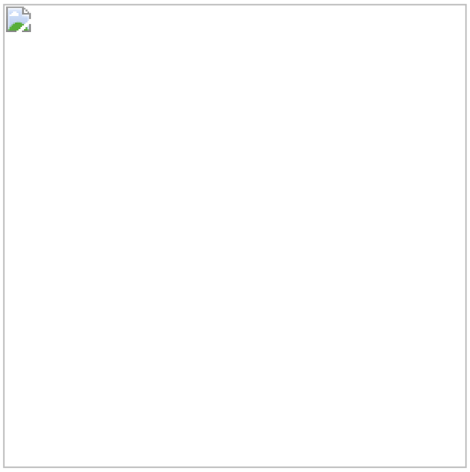


The Roaming Mantis smishing campaign has been impersonating a logistics company to steal SMS messages and contact lists from Asian Android users since 2018. In the second half of 2020, the campaign improved its effectiveness by adopting dynamic DNS services and spreading messages with phishing URLs that infected victims with the fake Chrome application MoqHao.

Since January 2021, however, the McAfee Mobile Research team has established that Roaming Mantis has been targeting Japanese users with a new malware called SmsSpy. The malicious code infects Android users using one of two variants depending on the version of OS used by the targeted devices. This ability to download malicious payloads based on OS versions enables the attackers to successfully infect a much broader potential landscape of Android devices.

Smishing Technique

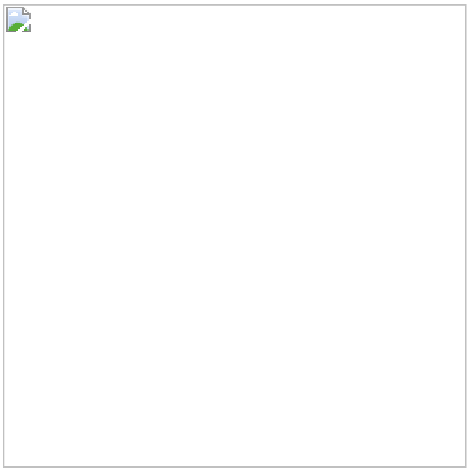
The phishing SMS message used is similar to that of recent campaigns, yet the phishing URL contains the term “post” in its composition.



Japanese message: I brought back your luggage because you were absent. please confirm. hxxps://post[.]cioaq[.]com

Fig: Smishing message impersonating a notification from a logistics company. (Source: Twitter)

Another smishing message pretends to be a Bitcoin operator and then directs the victim to a phishing site where the user is asked to verify an unauthorized login.



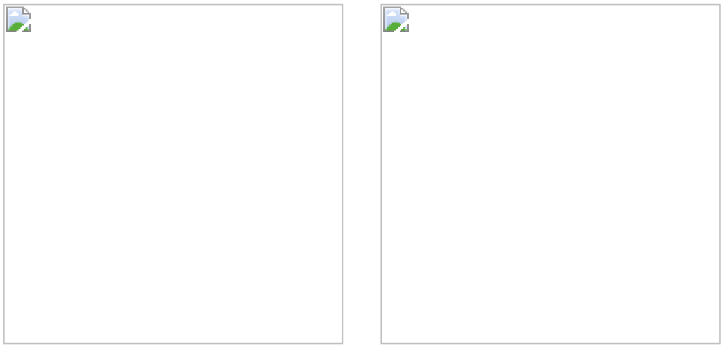
Japanese message: There is a possibility of abnormal login to your [bitFlyer] account. Please verify at the following URL: hxxps://bitfiye[.]com

Fig: Smishing message impersonating a notification from a bitcoin operator. (Source: Twitter)

During our investigation, we observed the phishing website hxxps://bitfiye[.]com redirect to hxxps://post.hygvv[.]com. The redirected URL contains the word "post" as well and follows the same format as the first screenshot. In this way, the actors behind the attack attempt to expand the variation of the SMS phishing campaign by redirecting from a domain that resembles a target company and service.

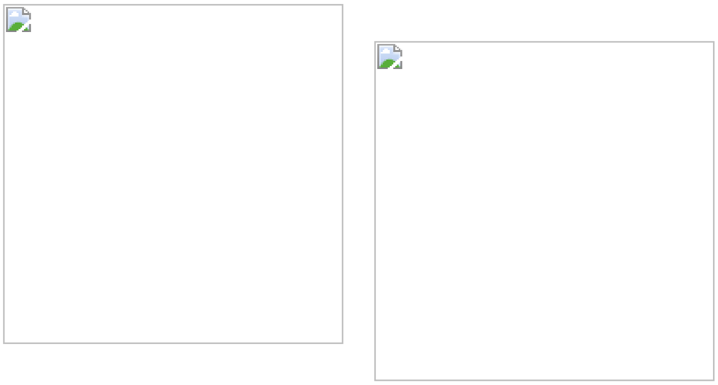
Malware Download

Characteristic of the malware distribution platform, different malware is distributed depending on the Android OS version that accessed the phishing page. On Android OS 10 or later, the fake Google Play app will be downloaded. On Android 9 or earlier devices, the fake Chrome app will be downloaded.



Japanese message in the dialog: "Please update to the latest version of Chrome for better security."

Fig: Fake Chrome application for download (Android OS 9 or less)



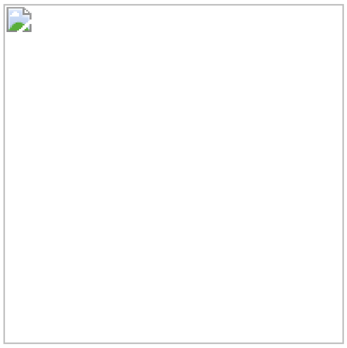
Japanese message in the dialog: "[Important] Please update to the latest version of Google Play for better security!"

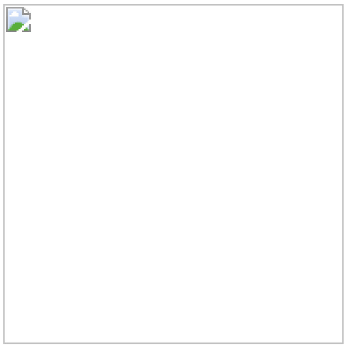
Fig: Fake Google Play app for download (Android OS 10 or above)

Because the malicious program code needs to be changed with each major Android OS upgrade, the malware author appears to cover more devices by distributing malware that detects the OS, rather than attempting to cover a smaller set with just one type of malware

Technical Behaviors

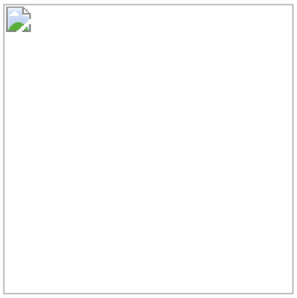
The main purpose of this malware is to steal phone numbers and SMS messages from infected devices. After it runs, the malware pretends to be a Chrome or Google Play app that then requests the default messaging application to read the victim’s contacts and SMS messages. It pretends to be a security service by Google Play on the latest Android device. Additionally, it can also masquerade as a security service on the latest Android devices. Examples of both are seen below.

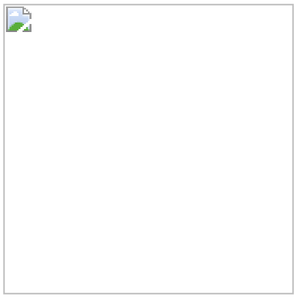




Japanese message: “At first startup, a dialog requesting permissions is displayed. If you do not accept it, the app may not be able to start, or its functions may be restricted.”

Fig: Default messaging app request by fake Chrome app





Japanese message: “Secure Internet Security. Your device is protected. Virus and Spyware protection, Anti-phishing protection and Spam mail protection are all checked.”

Fig: Default messaging app request by fake Google Play app

After hiding its icon, the malware establishes a WebSocket connection for communication with the attacker’s command and control (C2) server in the background. The default destination address is embedded in the malware code. It further has link information to update the C2 server location in the event it is needed. Thus, if no default server is detected, or if no response is received from the default server, the C2 server location will be obtained from the update link.

The MoqHao family hides C2 server locations in the user profile page of a blog service, yet some samples of this new family use a Chinese online document service to hide C2 locations. Below is an example of new C2 server locations from an online document:

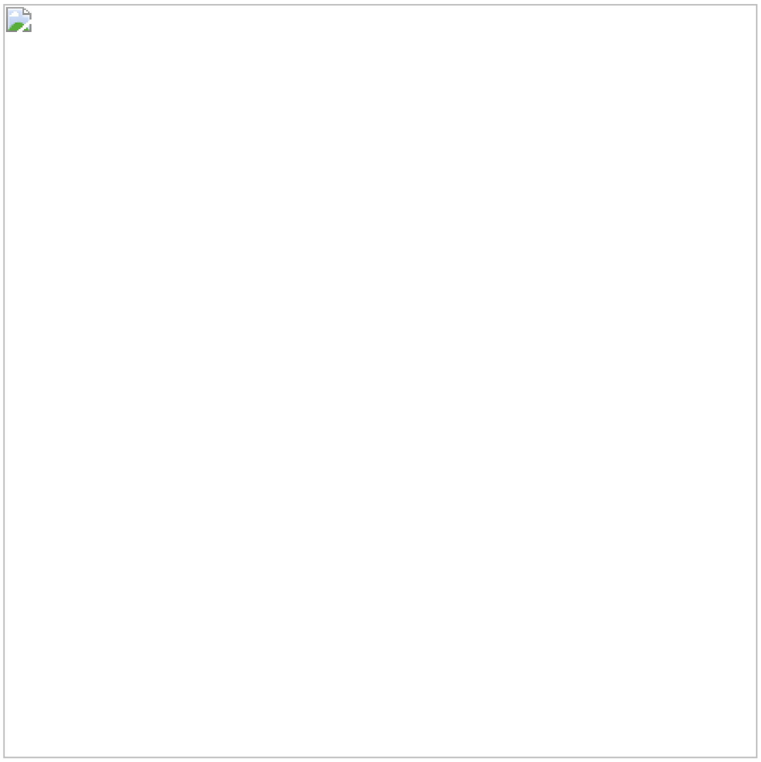


Fig: C2 server location described in online document

As part of the handshake process, the malware sends the Android OS version, phone number, device model, internet connection type (4G/Wi-Fi), and unique device ID on the infected device to the C2 server.

Then it listens for commands from the C2 server. The sample we analyzed supported the commands below with the intention of stealing phone numbers in Contacts and SMS messages.

Command String	Description
通讯录	Send whole contact book to server
收件箱	Send all SMS messages to server
拦截短信&open	Start <Delete SMS message>
拦截短信&close	Stop <Delete SMS message>
发短信&	Command data contains SMS message and destination number, send them via infected device

Table: Remote commands via WebSocket

Conclusion

We believe that the ongoing smishing campaign targeting Asian countries is using different mobile malware such as MoqHao, SpyAgent, and FakeSpy. Based on our research, the new type of malware discovered this time uses a modified infrastructure and payloads. We believe that there could be several groups in the cyber criminals and each group is developing their attack infrastructures and malware separately. Or it could be the work of another group who took advantage of previously successful cyber-attacks.

McAfee Mobile Security detects this threat as Android/SmsSpy and alerts mobile users if it is present and further protects them from any data loss. For more information about McAfee Mobile Security, visit https://www.mcafeemobilesecurity.com.

Appendix – IoC

C2 Servers:

- 168[.]126[.]149[.]28:7777
- 165[.]3[.]93[.]6:7777
- 103[.]85[.]25[.]165:7777

Update Links:

- r10zhzzfvj[.]feishu.cn/docs/doccnKS75QdvobjDJ3Mh9RlXtMe
- 0204[.]info
- 0130one[.]info
- 210302[.]top
- 210302bei[.]top

Phishing Domains:

Domain	Registration Date
post.jpostp.com	2021-03-15
manag.top	2021-03-11
post.niceng.top	2021-03-08
post.hygvv.com	2021-03-04
post.cepod.xyz	2021-03-04
post.jposc.com	2021-02-08
post.ckerr.site	2021-02-06
post.vioiff.com	2021-02-05
post.cioaq.com	2021-02-04
post.tpliv.com	2021-02-03
posk.vkiiu.com	2021-02-01
sagawae.kijjh.com	2021-02-01
post.viofrr.com	2021-01-31
posk.ficds.com	2021-01-30
sagawae.ceklf.com	2021-01-30
post.giioor.com	2021-01-30
post.rdkke.com	2021-01-29
post.japqn.com	2021-01-29
post.thocv.com	2021-01-28
post.xkdee.com	2021-01-27
post.sagvwa.com	2021-01-25
post.aiuebc.com	2021-01-24
post.postkp.com	2021-01-23
post.solomsn.com	2021-01-22

post.civrr.com	2021-01-21
post.jappnve.com	2021-01-19
sp.vvsscv.com	2021-01-16
ps.vjiir.com	2021-01-15
post.jpaeo.com	2021-01-12
t.aeomt.com	2021-01-2

Sample Hash information:

Hash	Package name	Fake Application
EA30098FF2DD1D097093CE705D1E4324C8DF385E7B227C1A771882CABEE18362	com.gmr.keep	Chrome
29FCD54D592A67621C558A115705AD81DAFBD7B022631F25C3BAAE954DB4464B	com.gmr.keep	Google Play
9BEAD1455BFA9AC0E2F9ECD7EDEBFDC82A4004FCED0D338E38F094C3CE39BCBA	com.mr.keep	Google Play
D33AB5EC095ED76EE984D065977893FDBCC12E9D9262FA0E5BC868BAD73ED060	com.mrc.keep	Chrome
8F8C29CC4AED04CA6AB21C3C44CCA190A6023CE3273EDB566E915FE703F9E18E	com.hhz.keeping	Chrome
21B958E800DB511D2A0997C4C94E6F0113FC4A8C383C73617ABCF1F76B81E2FD	com.hhz.keeping	Google Play
7728EF0D45A337427578AAB4C205386CE8EE5A604141669652169BA2FBA23B30	com.hz.keep3	Chrome
056A2341C0051ACBF4315EC5A6EEDD1E4EAB90039A6C336CC7E8646C9873B91A	com.hz.keep3	Google Play
054FA5F5AD43B6D6966CDBF4F2547EDC364DDD3D062CD029242554240A139FDB	com.hz.keep2	Google Play
DD40BC920484A9AD1EEBE52FB7CD09148AA6C1E7DBC3EB55F278763BAF308B5C	com.hz.keep2	Chrome
FC0AAE153726B7E0A401BD07C91B949E8480BAA0E0CD607439ED01ABA1F4EC1A	com.hz.keep1	Google Play
711D7FA96DFFBAEECEF12E75CE671C86103B536004997572ECC71C1AEB73DEF6	com.hz.keep1	Chrome
FE916D1B94F89EC308A2D58B50C304F7E242D3A3BCD2D7CCC704F300F218295F	com.hz.keep1	Google Play
3AA764651236DFBBADB28516E1DCB5011B1D51992CB248A9BF9487B72B920D4C	com.hz.keep1	Chrome
F1456B50A236E8E42CA99A41C1C87C8ED4CC27EB79374FF530BAE91565970995	com.hz.keep	Google Play
77390D07D16E6C9D179C806C83D2C196A992A9A619A773C4D49E1F1557824E00	com.hz.keep	Chrome
49634208F5FB8BCFC541DA923EBC73D7670C74C525A93B147E28D535F4A07BF8	com.hz.keep	Chrome
B5C45054109152F9FE76BEE6CBBF4D8931AE79079E7246AA2141F37A6A81CBA3	com.hz.keep	Google Play
85E5DBEA695A28C3BA99DA628116157D53564EF9CE14F57477B5E3095EED5726	com.hz.keep	Chrome
53A5DD64A639BF42E174E348FEA4517282C384DD6F840EE7DC8F655B4601D245	com.hz.keep	Google Play

80B44D23B70BA3D0333E904B7DDDF7E19007EFEB98E3B158BBC33CDA6E55B7CB	com.hz.keep	Chrome
797CEDF6E0C5BC1C02B4F03E109449B320830F5ECE0AA6D194AD69E0FE6F3E96	com.hz.keep	Chrome
691687CB16A64760227DCF6AECFE0477D5D983B638AFF2718F7E3A927EE2A82C	com.hz.keep	Google Play
C88C3682337F7380F59DBEE5A0ED3FA7D5779DFEA04903AAB835C959DA3DCD47	com.hz.keep	Google Play

The post Roaming Mantis Amplifies Smishing Campaign with OS-Specific Android Malware appeared first on McAfee Blogs.