Have You Seen These Roaming Mantis Connected Artifacts Wandering into Your Phone?

Table of Contents

Executive Report

A financially motivated threat group called "Roaming Mantis" was seen targeting Android and iOS device users through malicious SMS communications. The messages sent Android phone users to download pages while iOS users were redirected to credential-stealing login pages.

WhoisXML API researchers gathered more than 90 publicly available indicators of compromise (IoCs) and analyzed and expanded them using WHOIS, IP, and DNS intelligence. Our findings include:

- 7,000+ connected domains sharing the exact historic WHOIS details as one of the domain IoCs
- 1,100+ connected domains resolving to the IP addresses tagged as IoCs
- Dozens of artifacts tagged "malicious" by different malware engines
- Six countries and territories and nine different Internet service providers (ISPs) connected to the IP addresses
- Domain IoCs had the same WHOIS details, with GoDaddy as registrar and Domains By Proxy, LLC as privacy protection service provider

We discussed the details of our findings below.

Probing the IoCs Using DNS Intelligence

SEKOIA-IO published Roaming Mantis IoCs on GitHub, comprising 90 IP addresses used as payload servers and seven subdomains (belonging to three domains) contained in the SMS. A majority of the IP addresses were geolocated in China and South Korea, according to Bulk IP Geolocation lookup results.

The rest of the IoCs were distributed across four other locations—the Netherlands, France, the U.S., and Germany. See the chart below for the geolocation distribution of the IP addresses.

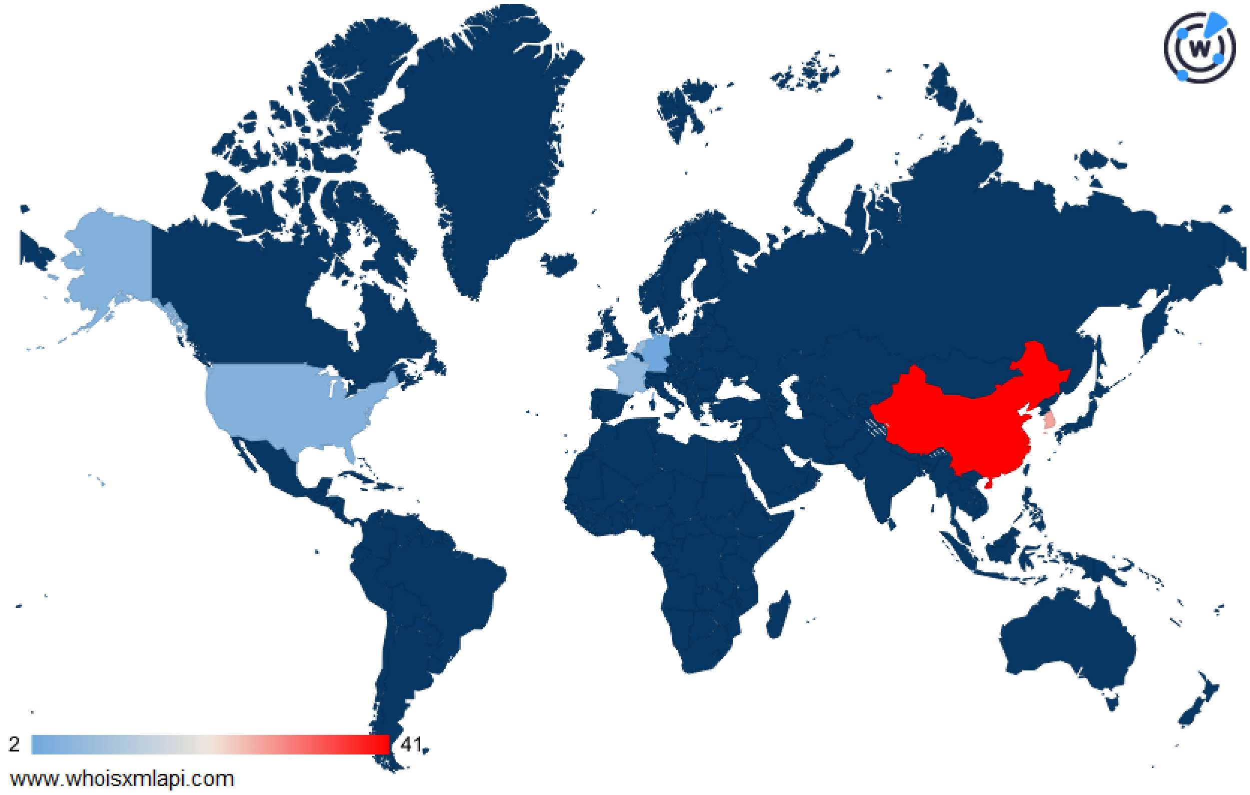
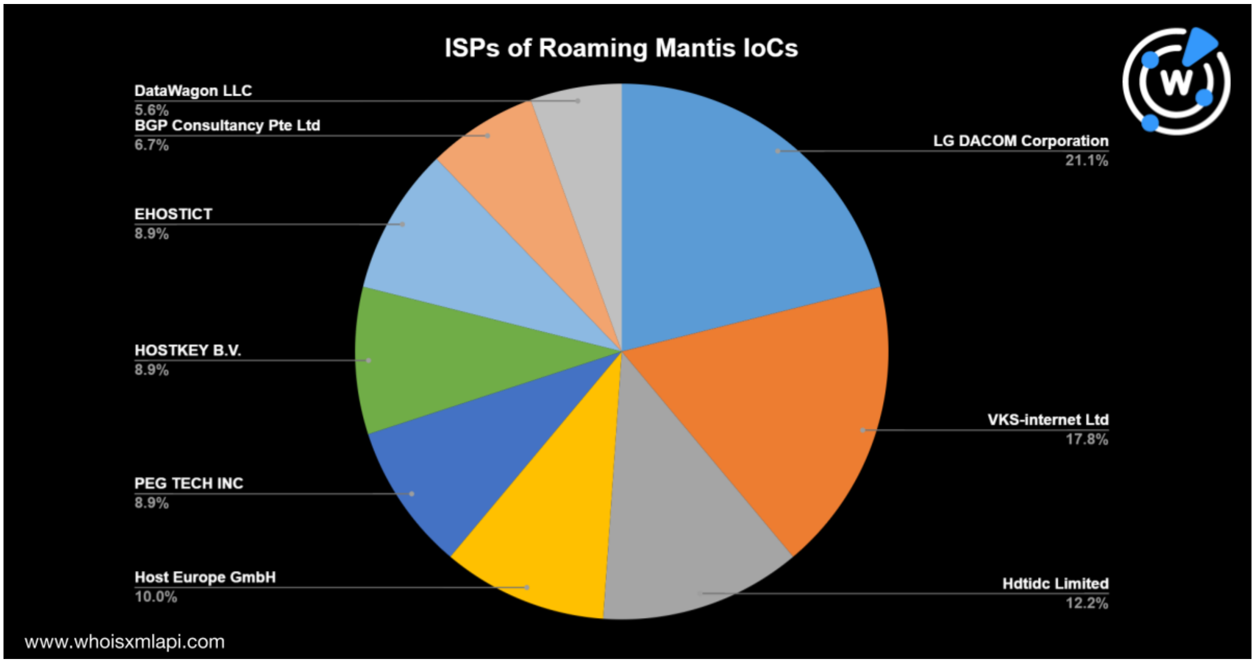


Chart 1: *IP Geolocation Distribution of Roaming Mantis IoCs*

On the other hand, the top ISPs were LG DACOM Corporation and VKS-Internet Ltd. The other ISPs are reflected in the chart below.



We also examined the WHOIS records of the three domain IoCs using WHOIS API and found that they had the same details. Their registrar was GoDaddy and the rest of their WHOIS details were privacy-protected by Domains By Proxy, LLC.

All the domains were recently registered (June 2022) but one (xpddg[.]com) had a deeper WHOIS history that can be traced as far back as 2016. Threat actors seemingly got their hands on it in June but it was created way before that. The domain IoC also appears to have been created using a domain generation algorithm (DGA).

Expanding the IoCs

We began our threat expansion with the malicious IP addresses listed as IoCs. Using Reverse IP/DNS API, we retrieved 1,170 domains that have resolved to the IP addresses at some point. These can be considered artifacts. About 88.55% were Duck DNS-hosted subdomains, while the rest were mostly DGA-created domains.

Another way to uncover more artifacts is by looking for properties sharing the IoCs' WHOIS details. Since the IoCs' current WHOIS records were redacted, we used the historic WHOIS information of xpddg[.]com, which included a registrant name and an email address. We found 7,086 artifacts currently and historically tied to these registrant details.

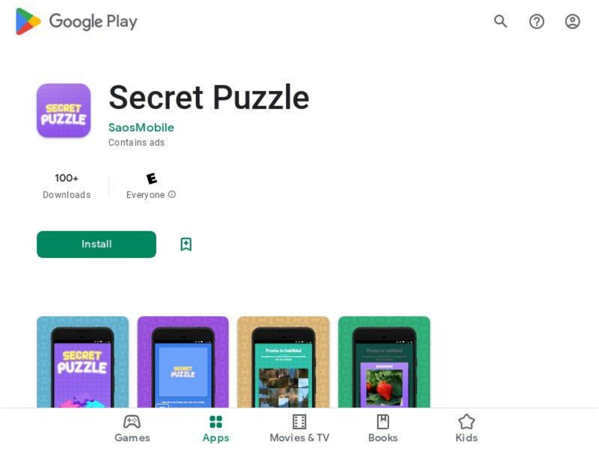
How Were the Artifacts Used?

While some domain connections may be coincidental, nearly 1% of the artifacts were flagged as malicious as of 1 August 2022. Several connected domains appear to be five-character DGA-created domains, just like the IoCs.

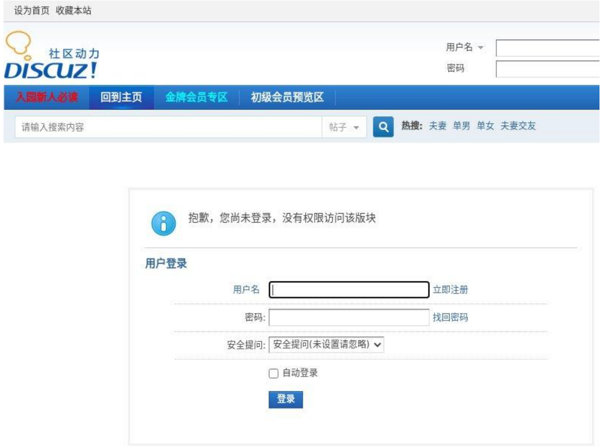
About 24% of the artifacts actively resolved to 890 unique IP addresses. Alarmingly, 23 IP addresses were on the Roaming Mantis IoC list.

We also performed a screenshot analysis of the resolving properties with the help of [Website Screenshot API](). Several domains were parked, but some content types stood out, such as news, gambling, and adult content.

Aside from these, some domains also hosted or redirected to login and download pages. To recall, these were the lures used by Roaming Mantis in their recent smishing campaign. We provided a few examples of these domains below.

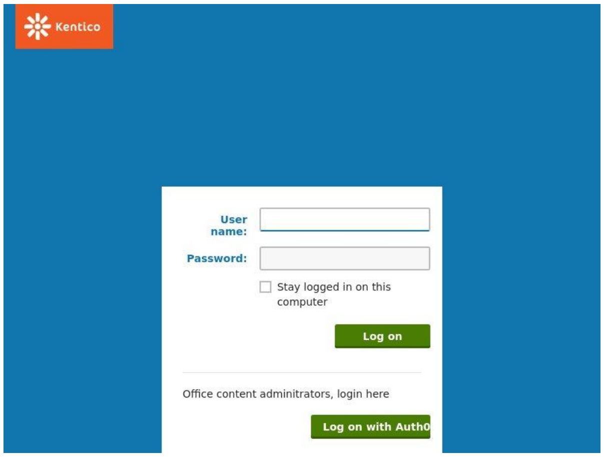


Screenshot of spzzl[.]com

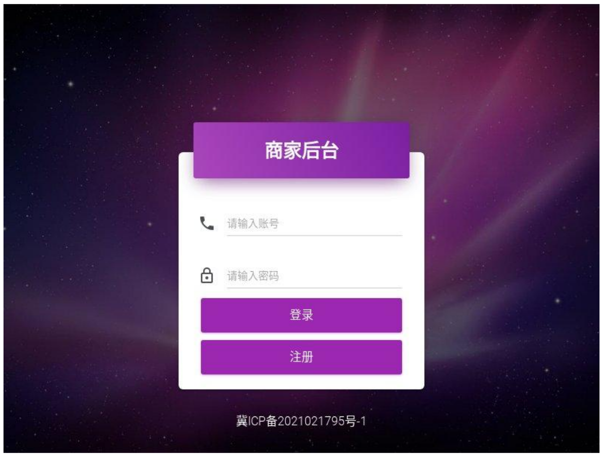


抱歉，您尚未登录，没有权限访问该版块

Screenshot of tlyfq[.]com


Kentico
User name:
Password:
□ Stay logged in on this computer
Log on
Office content adminitrators, login here
Log on with Auth0

Screenshot of ljhdb[.]com



Screenshot of tcpyp[.]com

—

The recent Roaming Mantis operation may have already duped thousands of users. SEKOIA-IO says that more than 90,000 unique IP addresses have already communicated with the command-and-control (C&C) servers.

Detecting IoC associations can help thwart malicious intentions behind the properties and ultimately aid in protecting end-users from phishing, credential theft, and other cybercrime. That is the goal of this threat report—from 97 IoCs, we uncovered thousands of connected domains, several of which were either suspicious or outright malicious.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Domains

Publicly Available Roaming Mantis IoCs

- 134[.]119[.]193[.]106
- 134[.]119[.]193[.]108
- 134[.]119[.]193[.]109
- 134[.]119[.]193[.]110
- 134[.]119[.]205[.]18
- 134[.]119[.]205[.]21
- 134[.]119[.]205[.]22
- 142[.]0[.]136[.]49
- 142[.]0[.]136[.]50
- 142[.]0[.]136[.]52
- 142[.]4[.]97[.]105
- 142[.]4[.]97[.]106
- 142[.]4[.]97[.]107
- 142[.]4[.]97[.]108
- 142[.]4[.]97[.]109
- 146[.]0[.]74[.]157

- 146[.]0[.]74[.]197
- 146[.]0[.]74[.]199
- 146[.]0[.]74[.]202
- 146[.]0[.]74[.]203
- 146[.]0[.]74[.]205
- 146[.]0[.]74[.]206
- 146[.]0[.]74[.]228
- 192[.]51[.]188[.]107
- 192[.]51[.]188[.]108
- 192[.]51[.]188[.]109
- 192[.]51[.]188[.]142
- 192[.]51[.]188[.]145
- 192[.]51[.]188[.]146
- 27[.]124[.]36[.]32
- 27[.]124[.]36[.]34
- 27[.]124[.]36[.]52
- 27[.]124[.]39[.]241
- 27[.]124[.]39[.]242
- 27[.]124[.]39[.]243
- 91[.]204[.]227[.]19
- 91[.]204[.]227[.]20
- 91[.]204[.]227[.]21
- 91[.]204[.]227[.]22
- 91[.]204[.]227[.]23
- 91[.]204[.]227[.]24
- 91[.]204[.]227[.]25
- 91[.]204[.]227[.]26
- 91[.]204[.]227[.]27
- 91[.]204[.]227[.]28
- 172[.]81[.]131[.]12
- 172[.]81[.]131[.]14
- 172[.]81[.]131[.]10
- 172[.]81[.]131[.]11
- 172[.]81[.]131[.]13
- 103[.]80[.]134[.]41
- 103[.]80[.]134[.]40
- 103[.]80[.]134[.]42
- 61[.]97[.]248[.]6
- 61[.]97[.]248[.]7
- 61[.]97[.]248[.]8
- 61[.]97[.]248[.]9
- 103[.]249[.]28[.]206
- 103[.]249[.]28[.]207
- 103[.]249[.]28[.]208
- 103[.]249[.]28[.]209
- 92[.]204[.]255[.]172
- 103[.]80[.]134[.]26
- 103[.]80[.]134[.]27
- 103[.]80[.]134[.]29
- 103[.]80[.]134[.]30
- 103[.]80[.]134[.]31
- 103[.]80[.]134[.]33
- 103[.]80[.]134[.]34
- 103[.]80[.]134[.]37
- 103[.]80[.]134[.]38
- 103[.]80[.]134[.]51
- 103[.]80[.]134[.]52
- 103[.]80[.]134[.]53
- 103[.]80[.]134[.]54
- 103[.]80[.]134[.]55
- 103[.]80[.]134[.]58
- 115[.]91[.]26[.]2
- 192[.]51[.]188[.]101
- 192[.]51[.]188[.]103
- 192[.]51[.]188[.]106
- 192[.]51[.]188[.]111
- 192[.]51[.]188[.]14
- 91[.]204[.]227[.]79
- 91[.]204[.]227[.]80
- 91[.]204[.]227[.]81
- 91[.]204[.]227[.]82
- 91[.]204[.]227[.]83
- 91[.]204[.]227[.]84
- 92[.]204[.]248[.]66
- coqrf[.]xpddg[.]com
- znjjq[.]udsuc[.]com
- gesee[.]udsuc[.]com
- bswhd[.]mrheu[.]com
- xpddg[.]com
- udsuc[.]com

- mrheu[.]com

Sample IP-Connected Artifacts

- funcetiv[.]com
- aaawxrmkei[.]duckdns[.]org
- awumg[.]com
- ersqa[.]com
- aewdwqvbmq[.]duckdns[.]org
- avgecrzzis[.]duckdns[.]org
- yufab[.]cn
- aaayhmnezm[.]duckdns[.]org
- historiekobiece[.]casa
- aaytt[.]com
- shwnyburhy[.]ddns[.]net
- bvcbuezira[.]duckdns[.]org
- esdmz[.]com
- long9[.]games
- bndyu[.]com
- aaaaffrrdt[.]duckdns[.]org
- afgrpmjkft[.]duckdns[.]org
- hostmaster[.]svhrh[.]com
- chayanwang[.]com
- atzvmjbgid[.]duckdns[.]org
- gnjiptuszh[.]duckdns[.]org
- xykj156[.]com
- dw9918[.]net
- hostmaster[.]uadee[.]com
- 152109053184652wk[.]ml
- abqfukmovk[.]duckdns[.]org
- bwdbu[.]com
- tvzeu[.]com
- aeycvsobyt[.]duckdns[.]org
- aacthrxxex[.]duckdns[.]org
- aoxra[.]com
- carktyxmvd[.]duckdns[.]org
- gsoxy[.]com
- dcugq[.]com
- aaaannmyzz[.]duckdns[.]org
- aitqnclheo[.]duckdns[.]org
- mnecdohywl[.]duckdns[.]org
- awjwmaxncm[.]duckdns[.]org
- gqlfawppjs[.]duckdns[.]org
- xykj255[.]com
- cauterize-bare[.]trafficratio[.]net
- acijdeywqk[.]duckdns[.]org
- mggrh[.]com
- aisldkumdx[.]duckdns[.]org
- aadesggvah[.]duckdns[.]org
- ccvbwrpvib[.]duckdns[.]org
- hpmez[.]com
- dvvpn[.]com
- aabgtgffee[.]duckdns[.]org
- aiyejpmrke[.]duckdns[.]org
- bffwydxzcs[.]duckdns[.]org
- gzcsvcmxwq[.]duckdns[.]org
- xykj785[.]com
- contact[.]trafficratio[.]net
- admvjdkcwp[.]duckdns[.]org
- mrheu[.]com
- aivvwvnrrr[.]duckdns[.]org
- aanbbqekjx[.]duckdns[.]org
- bznrm[.]com
- cdtkevlbqg[.]duckdns[.]org
- hzxqv[.]com
- qmdeg[.]com
- aaobobnaot[.]duckdns[.]org
- ajuuuxxisu[.]duckdns[.]org
- brezjslpwu[.]duckdns[.]org
- hbcvqrimtg[.]duckdns[.]org
- xykj792[.]com
- importartyright[.]trafficratio[.]net
- aevijhnabe[.]duckdns[.]org
- nsqsm[.]com
- alxmqqqppc[.]duckdns[.]org
- aaoboobhuu[.]duckdns[.]org

- cavxv[.]com
- cfyufrjsmg[.]duckdns[.]org
- mamcr[.]com
- vsndn[.]com
- abpcpcctgu[.]duckdns[.]org
- allykxkxcb[.]duckdns[.]org
- bubiounqxj[.]duckdns[.]org
- jvsegkplqq[.]duckdns[.]org
- xykj793[.]com
- karatetikwando[.]ml
- ajndeprlsq[.]duckdns[.]org
- ryybg[.]com
- anwqsfkbdm[.]duckdns[.]org
- aaopykgssl[.]duckdns[.]org
- dphqa[.]com
- mgonp[.]com
- xosux[.]com
- abprlzykrr[.]duckdns[.]org
- avowxtdaxw[.]duckdns[.]org
- cdgcdbxdua[.]duckdns[.]org
- kxxlmnkrug[.]duckdns[.]org
- xykj962[.]com
- usedwest[.]com
- arikelvxdx[.]duckdns[.]org
- udsuc[.]com
- anyqapzdab[.]duckdns[.]org
- aasblnmpvi[.]duckdns[.]org
- dxauw[.]com

Sample WHOIS-Connected Artifacts

- ljwdk[.]com
- ldwdk[.]com
- lbwdk[.]com
- jqwdk[.]com
- glwdk[.]com
- pywdk[.]com
- pxwdk[.]com
- pwwdk[.]com
- nqwdk[.]com
- lfwdk[.]com
- lhwdk[.]com
- nwwdk[.]com
- plwdk[.]com
- ptwdk[.]com
- pjwdk[.]com
- nywdk[.]com
- rpwdk[.]com
- qjwdk[.]com
- kfwdk[.]com
- ghwdk[.]com
- hxwdk[.]com
- hcwdk[.]com
- htwdk[.]com
- kdwdk[.]com
- jdwdk[.]com
- hywdk[.]com
- hmwdk[.]com
- jmwdk[.]com
- gywdk[.]com
- hdwdk[.]com
- hgwdk[.]com
- spclg[.]com
- yqfbf[.]com
- slqkb[.]com
- spgld[.]com
- ykqqs[.]com
- ykqqz[.]com
- qjfyq[.]com
- yqmfq[.]com
- spjpl[.]com
- yqqxk[.]com
- yqdmh[.]com
- xsbqm[.]com
- yqfhx[.]com
- ykqxq[.]com
- yqqzd[.]com

- smpjl[.]com
- qjgbg[.]com
- qjdqx[.]com
- qjdqz[.]com
- qjdtq[.]com
- qjdxq[.]com
- qjdqs[.]com
- qjhgq[.]com
- cbwdzz[.]com
- qjgmq[.]com
- fqqst[.]com
- hsjqk[.]com
- plctk[.]com
- hsjqj[.]com
- hswqk[.]com
- hswtq[.]com
- fqqkt[.]com
- fqqmg[.]com
- plcxm[.]com
- hskpq[.]com
- fqqks[.]com
- qjmxq[.]com
- hswcq[.]com
- hskgq[.]com
- hsjbq[.]com
- hswfq[.]com
- hsjmq[.]com
- plcfg[.]com
- fqqmh[.]com
- hsjfq[.]com
- plcsk[.]com
- qjqsz[.]com
- plggh[.]com
- fylzp[.]com
- kyjyt[.]com
- hsqkq[.]com
- hsqxq[.]com
- hsqfj[.]com
- hsqgq[.]com
- lbpym[.]com
- tlpym[.]com
- ldpym[.]com
- lgtym[.]com
- lpbym[.]com
- kyjth[.]com
- kyjfy[.]com
- kyjst[.]com
- hsqfd[.]com
- hsqgm[.]com
- hsqdx[.]com
- hsqfg[.]com
- lplym[.]com
- hsqdh[.]com
- kyjhx[.]com

Sample Malicious Artifacts Flagged during the Malware Check Dated 1 August 2022

- spmjl[.]com
- splzk[.]com
- splxq[.]com
- xkclp[.]com
- jfzlp[.]com
- xhjlp[.]com
- dwslp[.]com
- gbwlp[.]com
- qfqwt[.]com
- dwwgl[.]com
- bvcbuezira[.]duckdns[.]org
- carktyxmvd[.]duckdns[.]org
- ccvbwrpvib[.]duckdns[.]org
- aiyejpmrke[.]duckdns[.]org
- cdtkevlbqg[.]duckdns[.]org
- cavxv[.]com
- cfyufrjsmg[.]duckdns[.]org
- anyqapzdab[.]duckdns[.]org

- belwlcvrqe[.]duckdns[.]org
- azlqcdcooa[.]duckdns[.]org