Careful, the Next Premium SMS Offer You Subscribe to May Be Malicious

Table of Contents

Executive Report

Premium Short Message Service (SMS) abuse is no longer new. But it's pretty rare for such threats to rack up hundreds of dollars in additional phone bill costs for every victim each year.

Somehow, the threat actors behind the SMSFactory Android Trojan managed to do that. Avast reported that as many as 165,000 users worldwide have lost as much as US$336 a year to the perpetrators. What else should you know about the threat?

Our investigation uncovered additional artifacts and findings, including:

- Two of the domain IoCs were newly registered domains (NRDs), which could mean they were specifically created for the malicious campaign.
- The domain IoCs resolved to three unique seemingly dedicated IP addresses.
- Close to 200 domains shared the IoCs' IP addresses, three of which have been dubbed "malicious."
- Almost half of the possibly connected domains hosted the same content as the three malicious web properties identified.
- Nearly 1,200 domains shared common strings with the IoCs, four of which are already considered malicious.

What We Know about the SMSFactory Android Trojan So Far

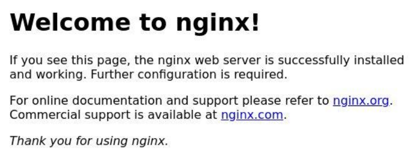
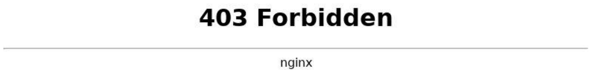
A publicly available report by AlienVault provided us three domains—mobilelinks[.]xyz, relario[.]xyz, and krinterro[.]com—named as indicators of compromise (IoCs) that served as jump-off points for our deep dive into the threat.

We also know that the SMSFactory Android Trojan has affected users in countries including Russia, Brazil, Argentina, Turkey, Ukraine, the U.S., France, and Spain. Apart from earning from charges for premium SMS, the malware also racks up phone bills with premium-rate calls. And at the rate the campaign is going, the attackers stand to gain as much as US$55.44 million annually.

What Our Deep Dive Revealed

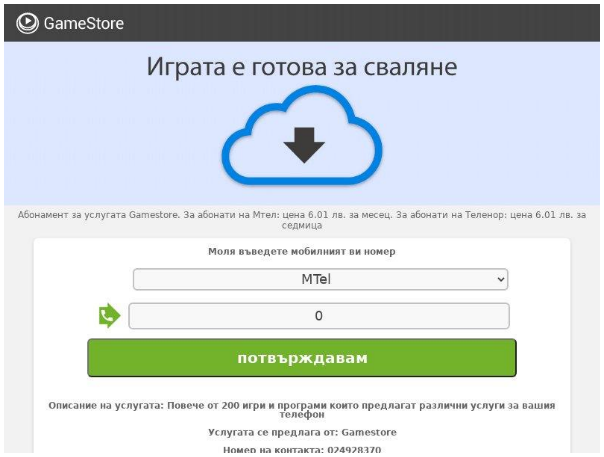
Only one of the domain IoCs—mobilelinks[.]xyz—was relatively aged, around 2 years old at the time the campaign was uncovered. The two remaining IoCs—relario[.]xyz and krinterro[.]com—were relatively new, around 3 months old at the time of discovery. All their current WHOIS records were redacted.

Screenshot lookups for the domain IoCs showed they didn't host live content. Two of them—mobilelinks[.]xyz and relario[.]xyz—seem to be under construction, while krinterro[.]com led to an error page.

 **Welcome to nginx!** If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. *Thank you for using nginx.*	 **403 Forbidden** nginx
Screenshot of mobilelinks[.]xyz and relario[.]xyz	*Screenshot of krinterro[.]com*

Subjecting the domain IoCs to DNS lookups showed they resolved to three unique IP addresses—159[.]65[.]198[.]99, 159[.]223[.]228[.]223, and 94[.]24[.]114[.]44. Reverse IP lookups for these IP resolutions led to the discovery of 181 possibly connected domains, given that the IP addresses seem to be dedicated.

Three of the additional domains—bg[.]game-store[.]mobi, gr[.]scout-apps[.]com, and mubulomokijo[.]xyz—were dubbed "malicious" by various malware engines, according to our bulk Threat Intelligence Platform (TIP) malware check results. Here are screenshots of their live content.



Играта е готова за сваляне

Абонамент за услугата Gamestore. За абонати на Мтел: цена 6.01 лв. за месец. За абонати на Теленор: цена 6.01 лв. за седмица

Моля въведете мобилният ви номер

MTel

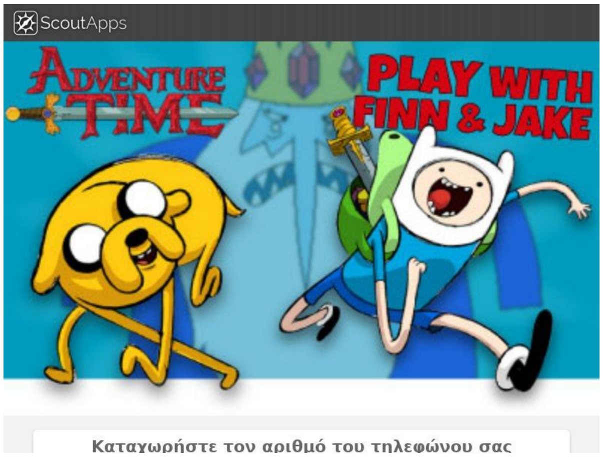
0

Описание на услугата: Повече от 200 игри и програми които предлагат различни услуги за вашия телефон

Услугата се предлага от: Gamestore

Номер на контакта: 024928370

Screenshot of bg[.]game-store[.]mobi



Καταγωρήστε τον αριθμό του τηλεφώνου σας

Screenshot of gr[.]scout-apps[.]com

403 Forbidden

nginx

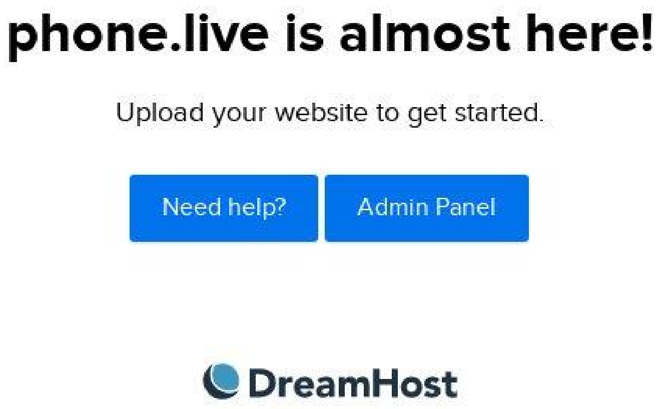
Screenshot of mubulomokijo[.]xyz

Entering your credentials to bg[.]game-store[.]mobi could give cybercriminals access to your gaming account. Downloading games from gr[.]scout-apps[.]com or visiting mubulomokijo[.]xyz, meanwhile, may lead to malware infections.

Interestingly, 76 of the 181 possibly connected domains hosted the same content as the malicious properties we uncovered. Their domain names, however, weren't limited to gaming but also dating and other apps. They may belong to the same people and could be lying in wait to get weaponized.

Given the importance of the financial toll SMSFactory Android Trojan can take on users, we used [Domains & Subdomains Discovery]() to uncover other suspicious domains. Using the strings “sms.” and “phone.” as search terms gave us an additional 1,196 domains, four of which—sms[.]ceo, sms[.]beauty, sms[.]earth, and phone[.]live—are already considered malicious.

Three of the malicious domains are unreachable, which could mean they’ve already been taken down. One—phone[.]live—however, continues to be live, hosting what seems to be a website under development.



phone.live is almost here!

Upload your website to get started.

Screenshot of phone[.]live

What Users Can Do

Users the world over should avoid accessing the IoCs and additional artifacts uncovered through our in-depth analysis if they wish to avoid the repercussions of SMSFactory Android

Trojan infection. Monitoring the artifacts, both old and new, may also be worthwhile for organizations.

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 Artifacts and IoCs

Domains That Shared the IoCs' IP Addresses

- adsmyclick[.]com
- api[.]coolwixer[.]com
- api[.]smartverifysite[.]com
- api2[.]smartverifysite[.]com
- apkmods[.]world
- az[.]games-store[.]mobi
- bd[.]mega-mobi[.]com
- be[.]game-store[.]mobi
- be[.]pornococtel[.]com
- be2[.]game-store[.]mobi
- be2[.]pornococtel[.]com
- bg[.]game-store[.]mobi
- boxsmarty[.]com
- br[.]pornococtel[.]com
- br[.]scout-apps[.]com
- bw[.]game-storeplus[.]net
- bw[.]mega-mobi[.]com
- bw[.]scout-apps[.]com
- bw[.]thenewgamestore[.]com
- by[.]gamestoreplus[.]com
- by[.]mega-mobi[.]com
- by[.]thenewgamestore[.]com
- chat[.]flirtandmatch[.]com
- chat[.]smartclickleads[.]com
- clean-download[.]com
- confirmyourage[.]com
- coolwixer[.]com
- cy[.]game-storeplus[.]net
- cy[.]games-store[.]mobi
- cy[.]scout-apps[.]com
- cy[.]scout-apps[.]net
- cy2[.]scout-apps[.]com
- d[.]coolwixer[.]com
- d[.]easyweb4fun[.]com
- d[.]goodwinnersprize[.]com
- d[.]sunny-clicks[.]com
- down[.]boxsmarty[.]com
- down[.]gofunnytime[.]com
- easyweb4fun[.]com
- flirtandmatch[.]com
- flirtandmatchnow[.]com
- fr[.]game-store[.]mobi
- fr[.]game-storeplus[.]com
- fr[.]games-store[.]mobi
- fr[.]gamestoreplus[.]com
- fr[.]gamestoreplus[.]net
- fr[.]thenewgamestore[.]com
- fr2[.]game-store[.]mobi
- game-store[.]by
- games[.]smartverifysite[.]com

Domains That Hosted the Same Content as the IoCs

- api[.]smartverifysite[.]com
- api2[.]smartverifysite[.]com
- az[.]games-store[.]mobi
- bd[.]mega-mobi[.]com
- be[.]game-store[.]mobi
- be2[.]game-store[.]mobi
- bg[.]game-store[.]mobi
- by[.]gamestoreplus[.]com
- by[.]thenewgamestore[.]com
- chat[.]flirtandmatch[.]com
- clean-download[.]com
- confirmyourage[.]com
- cy[.]game-storeplus[.]net
- cy[.]games-store[.]mobi
- cy[.]scout-apps[.]com
- cy[.]scout-apps[.]net
- cy2[.]scout-apps[.]com
- d[.]goodwinnersprize[.]com
- flirtandmatch[.]com
- flirtandmatchnow[.]com

Domains That Contained the Same Strings as the IoCs

- sms[.]gz[.]cn
- sms[.]irish
- sms[.]university
- sms[.]diet
- sms[.]sexy
- sms[.]place
- sms[.]supply
- sms[.]today
- sms[.]ac[.]th
- sms[.]studio
- sms[.]com[.]pe
- sms[.]link
- sms[.]in[.]th
- sms[.]win
- sms[.]cymru
- sms[.]health
- sms[.]london
- sms[.]ch
- sms[.]co[.]it
- sms[.]ma
- sms[.]com[.]ru
- sms[.]sh
- sms[.]me
- sms[.]gives
- sms[.]email
- sms[.]co[.]nz
- sms[.]firm[.]in
- sms[.]or[.]jp
- sms[.]christmas
- sms[.]social
- sms[.]com[.]ua
- sms[.]gratis
- sms[.]bayern
- sms[.]hb[.]cn
- sms[.]vet
- sms[.]vip
- sms[.]ro
- sms[.]red
- sms[.]africa
- sms[.]co[.]ma
- sms[.]moda
- sms[.]cricket
- sms[.]co[.]at
- sms[.]mk
- sms[.]com[.]pg
- sms[.]graphics
- sms[.]rs
- sms[.]me[.]uk
- sms[.]web[.]pk
- sms[.]attorney

- sms[.]kg
- sms[.]tel
- sms[.]cl
- sms[.]ist
- sms[.]wiki
- sms[.]support
- sms[.]at
- sms[.]org[.]sg
- sms[.]co[.]jp
- sms[.]co[.]im
- sms[.]com[.]do
- sms[.]archi
- sms[.]wales
- xn--sm-mta[.]lv
- sms[.]xn--3ds443g
- sms[.]bid
- sms[.]fj[.]cn
- sms[.]com[.]ec
- sms[.]name[.]tr
- sms[.]claims
- sms[.]co[.]pl
- sms[.]domains
- sms[.]tau[.]ac[.]il
- sms[.]com[.]ve
- sms[.]com[.]mx
- sms[.]co[.]rs
- sms[.]farm
- sms[.]ge
- sms[.]financial
- sms[.]construction
- sms[.]ne[.]kr
- sms[.]surf
- sms[.]engineer
- sms[.]mt
- sms[.]pm
- sms[.]ceo
- sms[.]world
- sms[.]ryukyu
- sms[.]tw
- sms[.]beauty
- sms[.]energy
- sms[.]family
- sms[.]club
- sms[.]lv
- sms[.]realty
- sms[.]li
- sms[.]name
- sms[.]fishing
- sms[.]ninja
- sms[.]com[.]ps