



Threat Report

Messaging Applications: The New Dark Web

Why Read This Report?

In this report, IntSights looks to identify which mobile platforms are gaining traction and may be the future backbone of the illegal cyber-economy. The data in this report will help you understand how dark web communication is changing with mobile adoption and how this impacts the way security teams monitor dark web activity. By reading this report, security teams can better prepare for this shift and be better resourced to evolve with it.

Methodology

Using scraped data from thousands of black markets, paste sites, hacking forums, IRC channels, messaging apps, and social media pages over a twelve month period from July 2016 to July 2017, the IntSight threat research team conducted an analysis of how the frequency of mobile messaging app invites have changed over time.

About IntSights

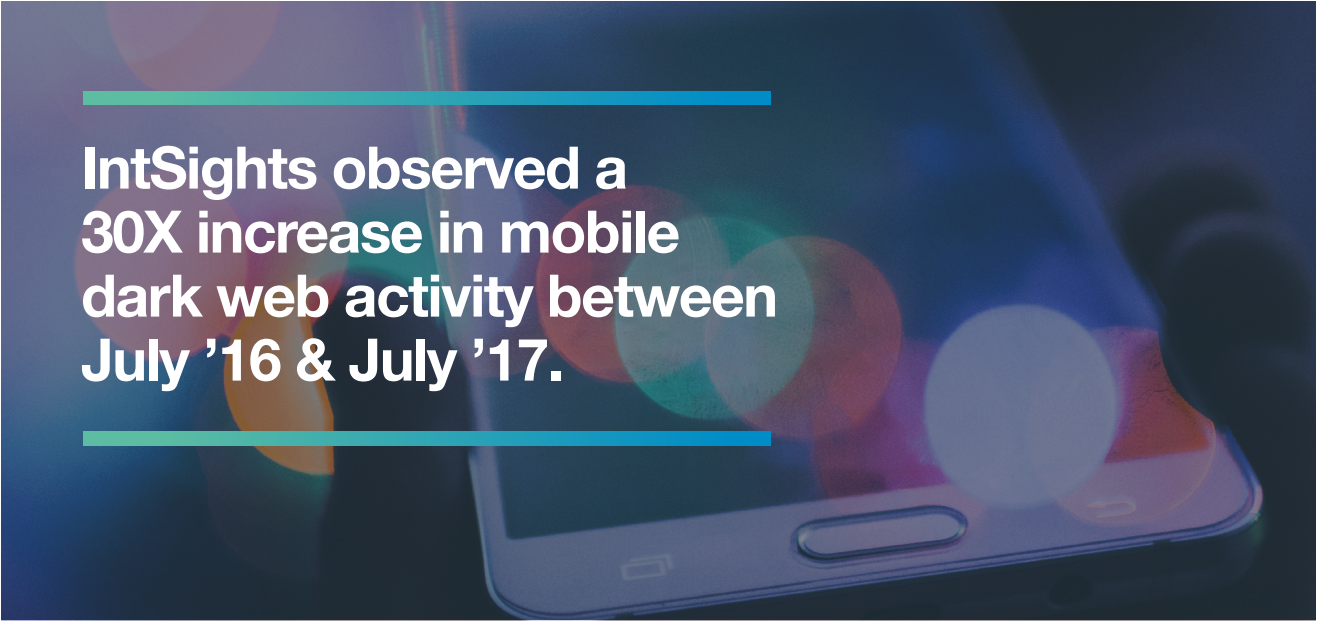
IntSights is redefining cyber security with the industry's first and only enterprise threat management platform that transforms tailored threat intelligence into automated security operations. Our ground-breaking data-mining algorithms and unique machine learning capabilities continuously monitor an enterprise's external digital profile across the surface, deep and dark web, categorize and analyze tens of thousands of threats, and automate the risk remediation lifecycle — streamlining workflows, maximizing resources and securing business operations. This has made IntSights' one of the fastest growing cyber security companies in the world. IntSights has offices in Tel Aviv, Amsterdam, New York and Dallas and is backed by Glilot Capital Partners, Blumberg Capital, Blackstone and Wipro Ventures. To learn more, visit www.intsights.com.

Executive Summary

As more and more online activity moves to mobile devices, and the veil of secrecy provided by Tor and I2P begins to fade, it is clear that hackers will need to respond and adjust how they communicate online. To find out, **IntSights analyzed conversations, data and files taken from thousands of dark-web sites to see how the dark-web's usage of mobile messaging apps have changed over time.**

While the use of mobile messaging apps for illicit activity have been on the rise for some time, the closure of Alphabay, Hansa and suspected compromise of Dream Market and the Tor Network have shaken confidence in more traditional dark web channels. In this analysis, we identify which mobile platforms are gaining traction and may be the future backbone of the illegal cyber-economy.

Based on our findings, IntSights saw a 30x increase in mobile dark web activity over the past 12 months and estimates that as many as several hundred thousand users are actively abusing popular mobile messaging apps, such as Discord, Telegram and Whatsapp, to trade stolen credit cards, account credentials, malware, drugs and to share hacking methods and ideas. Of these, **our findings suggest Discord is becoming the go-to-app for mobile dark web discussions with nearly 9x more dark web invitations than competing messaging apps.**

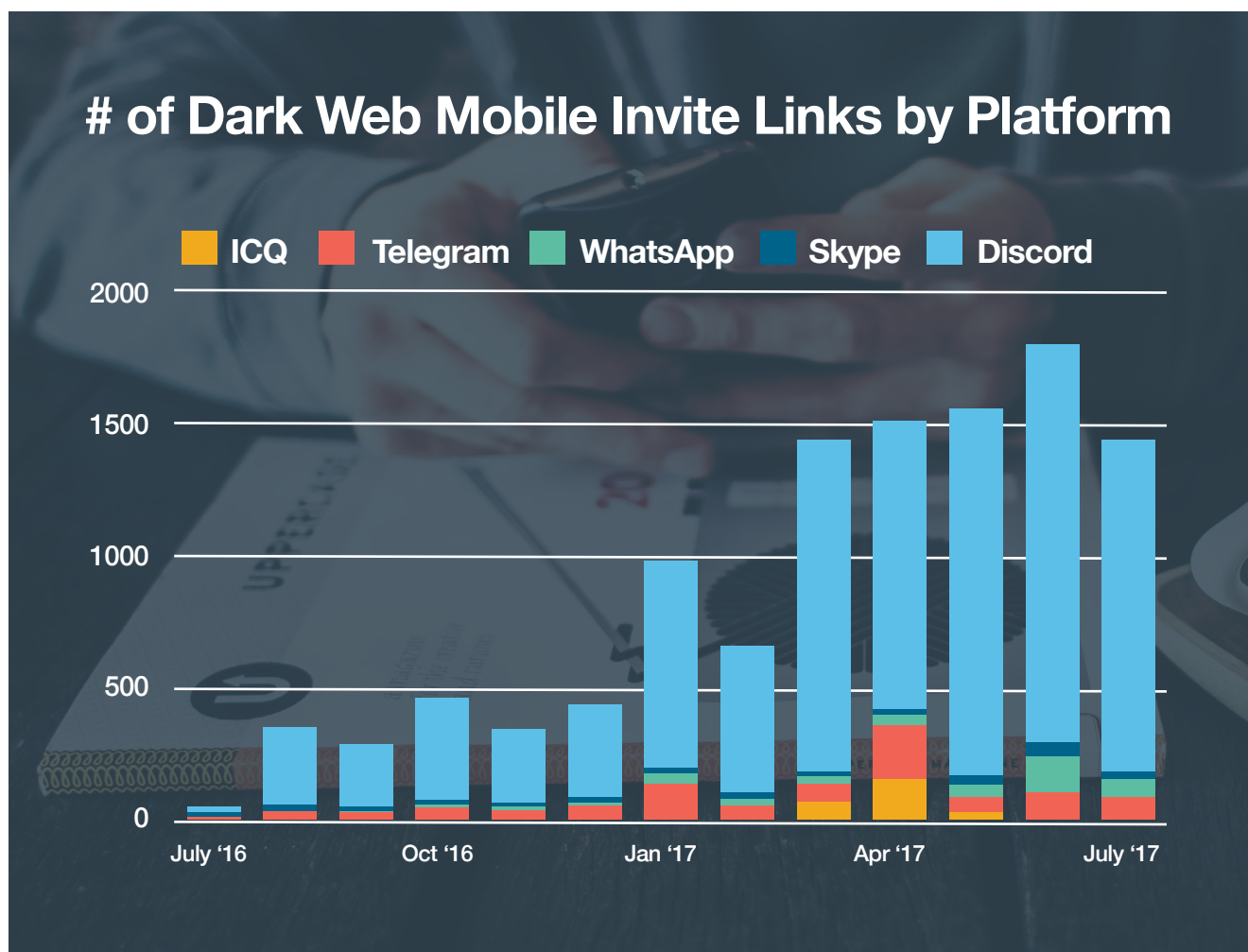


**IntSights observed a
30X increase in mobile
dark web activity between
July '16 & July '17.**

Detailed Findings

In order to estimate the growing usage of mobile apps for cyber-criminal activity, IntSights conducted an analysis of the number of appearances of invite links shared on the dark web. This data came from the IntSights database and looked at data from July 2016 to July 2017.

The results show a clear pattern - mobile apps usage for dark web activity is growing with a consistent rise in the number of mobile messaging invite links shared on dark-web platforms over the past year. Of these, **Discord was the most common platform shared, with nearly 9X the number of invites as the second most popular app**. Discord's popularity is surprising, given that it is one of the smaller mobile messaging app platforms with 45 million users.¹



¹ Venture Beat - 2017

App	Number of Dark Web Invite Links	Number of Users
Discord	9046	45M
Telegram	916	100M
WhatsApp	427	1.2B
Skype	300	300M
ICQ	256	11M

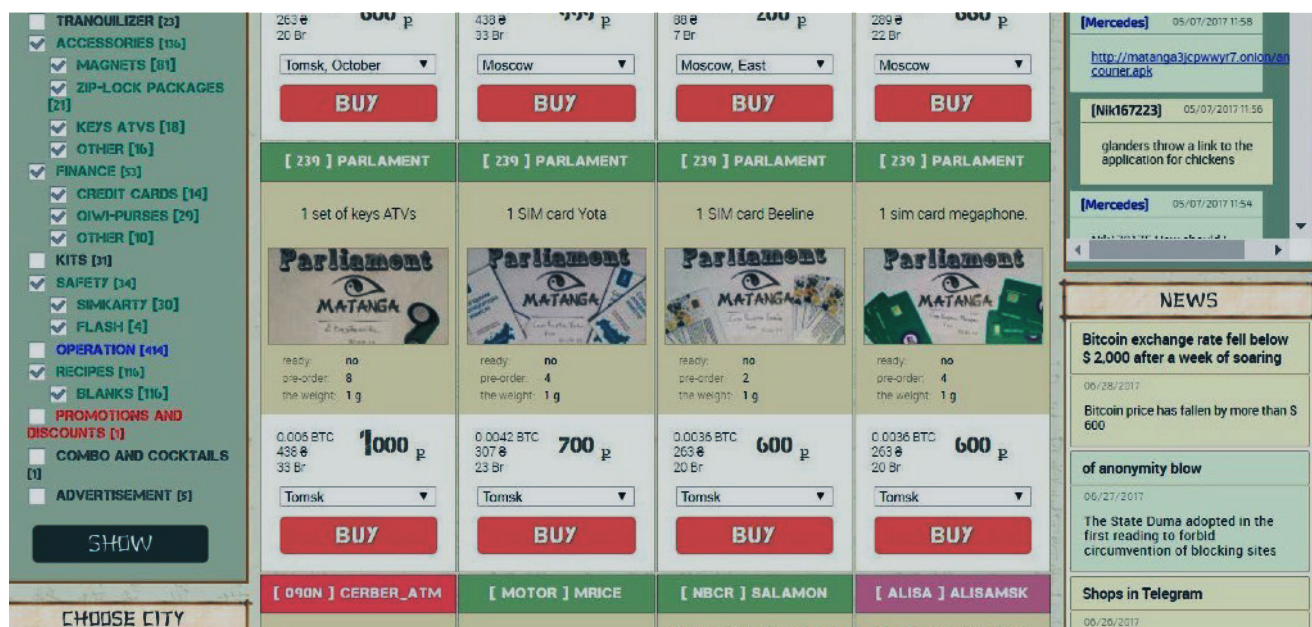
In addition to mobile messaging apps, TOR itself also appears to be seeing an increase in mobile usage with a steady rise in the number of installs for ORbot, Tor's mobile application. As of December 2016, **ORbot has been installed over 10 million times, suggesting that traditional dark web channels are likely to remain highly relevant as users conduct more of their dark web activities on mobile devices.**

App	Jan'14	Jan'14	Jan'14
ORbot Installs	1,000,000	5,000,000	10,000,000

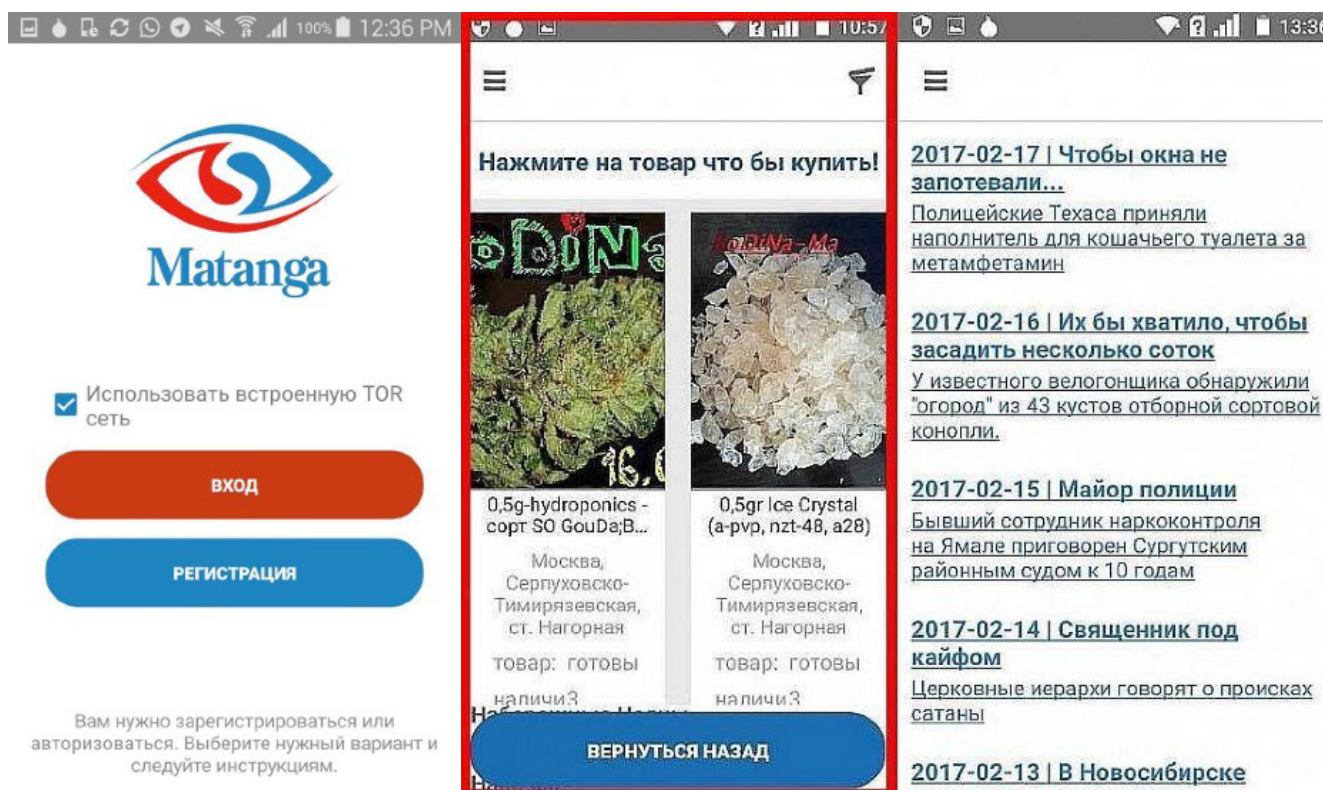
One example of how cyber-criminals are leveraging TOR on mobile devices can be taken from the Russian black market Matanga.

On July 2017, a wide advertising campaign for a new Russian black market was conducted via Jabber - a messaging XMPP-based application that is popular among hackers. Interestingly, the new black market, called Matanga, offers its users an unprecedentedly easy-access via a dedicated Android app.

The market sells a variety of drugs, stolen credit cards, SIM cards and other illegal merchandise. It also features a “Wanted” section for what appears to be questionable tasks.



Leveraging ORbot, Matanga built their own dedicated mobile app that connects to TOR utilizing ORbot. This offers it's mobile-first clients easy access to the services of the dark web from their mobile device and we expect to see more dark web vendors creating similar apps in the future as mobile usage grows.



Group Chats - The Dark Web Forums of the Future

Generally speaking, IntSights observes a growing reliance of hackers on closed, small and distributed networks that are based on social media groups and/or messaging apps. Such networks might be easily discovered, but threat-actors can reinstate groups easily - should the need to close an old one arises - making mobile group chat communication potentially far more resilience than traditional moderated web forums. The replacement of such forums and markets may take more time due to the logistics and marketing that are required, but it is clear from the data that mobile communication is becoming increasingly common.

While the pace of this transition is unknown, nearly all popular messaging apps have implemented group chat features that enable groups of individuals to connect in a private conversation. These invite-only groups can be joined in one of two ways 1. an individual could join the chat by being added directly by the group admin/member or 2. by being sent an invite link. With an invite link, an individual simply clicks on the link and is directed to the group and can begin participating in its activity. Invite links have become commonly used by cybercrime oriented groups to form ad-hoc groups around common topics of interest or trusted groups because they make it easy to lure-in relevant crowds.

Below we detail the group chat capabilities and characteristics for a few of the mobile applications tracked for this report.



Whatsapp: Whatsapp invite links typically are structured as follows:

<https://hatwhatsapp.com/invite/> A Whatsapp group has a maximum size of 256 users. We noticed during our research that the app is popular amongst Indians, Nigerians, and Brazilians.



Telegram: The app has become infamous for the use globaljihadists make of it for communicating and sending out propaganda. A Telegram invite link would be structured as follows: <https://t.me/joinchat>

Telegram is most popular amongst Russian hackers, Uzbeks, Brazilians and Iranians. Telegram groups could reach as many as tens of thousands of members. The biggest group that has been observed by IntSights during the research consists of about 60K members, in Brazil.



Skype: The app, that is mostly known for its video-chat function, also offers group chats, that are widely popular in Brazil. Such groups would consist of tens to hundreds of users. Skype invite links would be structured as follows: <https://join.skype.com>.



ICQ: This classic messaging app is popular among Brazilians and Russians. An invite link would be structured as follows: <https://icq.com/chat/> and a group would typically consist of hundreds of users.



Discord: The messaging app is also commonly used on desktop computers. Several groups were found for illegal trade from Brazil and one group from Turkey. Each group could consist of tens to hundreds of users, as the biggest group had about 800 members. A Discord invite would typically be structured as follows: <https://discord.gg/>



On the Mobile Dark Web - Geography Matters.

One trend IntSight has monitored closely and continues to do research into, is the fragmentation of the mobile dark web by geography. While Tor and illicit markets universally dominate traffic on the dark web, user traffic on the mobile dark web is far more fragmented with specific mobile messaging applications rising to prominence in specific geographic regions. These regional preferences has led to the development of unique mobile dark web cultures and will require enterprises to dedicate greater resources to properly monitor various mobile dark web platforms for activity. Below we detail the history, platform preferences and actor characteristics developing on the mobile dark web unique to Russia, Iran and Nigeria.

Russia - IQT and Telegram

Russia has one of the largest and most advanced hacking communities in the world. Entering into this well established community can require a significant commitment, with many Russian hacking forums and black markets requiring frequent participation and posting a significant amount of material to retain access to closed areas inside the forums and the ability to direct message other members.

While this has the positive benefit of filtering members and pushing the community further, it also excludes many in the community and creates a barrier to entry that new hackers may not wish to overcome. Mobile messaging apps such as IQT and Telegram allow quick and easy access and provide a more flexible open structure of communication that is more accessible to many new members of the community or those not able or willing to fully commit.

Below we break down the differences and history of these two growing platforms in Russia's mobile dark-web.

IQT - the universal integrator

Russian citizens have a long history with ICQ, or as they call it: "Asya", with a history going back more than 10 years. While a popular messaging platform across Russia, what makes ICQ mobile app especially popular among Russian attackers in particular, is the ability to communicate not only through ICQ, but also through a number of other popular Russian apps - Mailer, VKontakte, GTalk, Ya.Online, Jeje and even Jabber. In addition, authenticated accounts can be transferred to new users, making it possible to acquire seniority and credibility, and there is an ICQ app for Linux making these apps very attractive for Russian hackers.

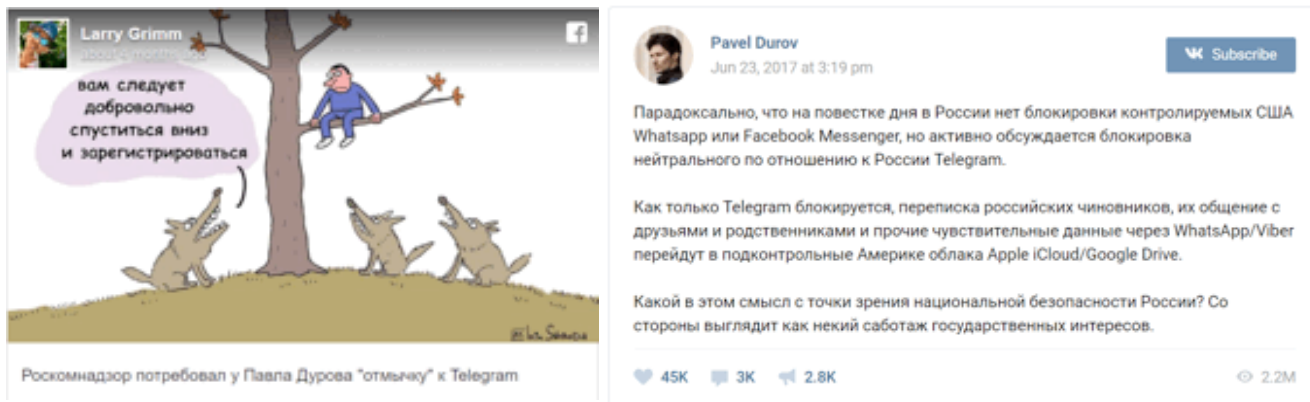
Telegram - The forbidden fruit

Telegram was created in 2013 by Russian, Pavel Valierovich Durov, who had formally co-founded VKontakte, an IQT supported social network. Telegram is a privacy oriented open source instant messenger, with features that include encrypted conversations that may only be decrypted by keys which are held at the end user's devices, and secret chats that are deleted from all parts of the system, servers and user devices alike. Additionally, push notifications for secret chats contain no actual conversation data.

Telegram also uses a distributed server network, with each region holding limited sovereignty over the data in its region. Currently, there are five main Telegram servers in different regions throughout the world, each serving its geographical region. No central server stores all of the information, and all servers are run on encrypted hard drives. According to Telegram, physically breaking into the site where the servers are held will still prove useless due to the fact that every cluster is encrypted using a key that is stored at a different cluster at a different region. The development team of Telegram claim that even they do not possess the ability to access ones private messages and data.

Telegram is held under the GNU GPLv2 open source license, meaning that use of Telegrams code is allowed under specific conditions, as well as allowing anyone who meets the sufficient requirements on his code to contribute to Telegrams codebase on GitHub.

Since Telegram is a freeware developed outside of the United States, it has become very popular amongst Russian and Chechnyan politicians and hackers seeking to operate outside American jurisdiction. However recently Telegram has come under scrutiny by the Russian FSB which has declared Telegram must register as an information distributor with the Russian state and provide authorities with access or risked being blocked. It is believed that the recent focus and crack down on Telegram use in Russia is due to its increased popularity with political adversaries of the current Russian administration.



"You should come down voluntarily and register"- Russian Political Cartoon.

In response, Telegram announced support for Proxy servers for Telegrams Android app, allowing users to use the app through other countries. In addition, Telegram's founder has warned that the blocking Telegram services will only push political dissidents to use western services such as WhatsApp and Viber. Since coming under pressure in June, the Russian's government crackdown has backfired with Telegram surging to become one the most popular app on Russian app stores. Given this rise in popularity, it is unclear if the Russian government will follow through on its threats to crack down on Telegram and IntSight continues to monitor the situation.

Telegram - The forbidden fruit

As to September 2017, more than 40 million Iranians are using Telegram; and according to publications, 86% of the Iranian cyber activities happen in Telegram.

The reasons for this are many fold - First, many popular western social media platforms, such as Facebook and Twitter, are blocked in Iran. Then, in 2014 authorities blocked the widely used Viber, further enhancing the popularity of Telegram.

In addition, Telegram's channels feature allows users to form an encrypted broadcast of content. This provides a comfortable platform for media outlets and politicians to bypass formal authorities and censorship.

This rare platform for free information came under threat in 2015, when Iranian authorities demanded Telegram host its Iranian operations inside Iran, and even leaked to the media that such change is about to happen, but Telegram refused and denied the publications. Typically this would have resulted in the blockage of service, similar to Twitter, but Telegram was protected from blockage by the Iranian president, Hassan Rouhani, due to the fact that the platform played a major role in supporting his presidential reelection bid in 2017.

In the lead up to the election, Telegram was breached and as many as 15 millions of phone numbers and ID numbers of Iranian citizens were exposed.

Experts attributed the breach to the Iranian state-sponsored APT group, Rocket Kitten, that targeted journalists, human rights activists and political opponents. Currently, the Iranian judiciary continues to challenge Telegram's legality and usage inside Iran and in April blocked voice call services on the platform.

On September 26th, Iran's Prosecutor General, Abbas Jafari-Dolatabadi, announced a lawsuit against Telegram, claiming that the platform has become "appropriate" for the activities of organized criminal groups, terrorists, and promoting child pornography, human trafficking and drugs. This lawsuit is on-going so while Telegram remains the platform of choice for hackers in Iran, its future in the state remains uncertain.

Nigeria & Sub-Saharan Africa: Mobile First

Through our research, IntSight observed that abuse of mobile application for a malicious activity is especially popular in third world countries, such as the Sub-Saharan African states, such as Nigeria. Several economic and technical forces have contributed to this phenomena, particularly the continent's timeline for development meant that for most part the population skipped the PC era and leapfrogged directly into the smartphone era - never owning or using a PC. This helps explain the relative lack of African participation in traditional hacking forums and their enthusiastic adoption for mobile messaging platforms.

In 2017, the mobile penetration rate in the African Nations was 50%, adding nearly 300 million subscribers in the last five years. In Nigeria, the rate is much higher, at 82%. As mobile phones have become more available, it is natural that they would become more widely used by local cyber criminals and potential victims alike given the lack of desktop PCs in the region.

The proliferation of cheap Chinese smartphones have made smartphones available to a greater share of the population, many of whom make less than \$2/day, and the mobile first approach taken by many local banks, such as SafariCom, have made mobile phone ownership financially advantageous for many of the regions agricultural farmers where as much as 35% of transactions are conducted electronically.

In this environment, mobile messaging platforms have become the primary platform for communication and greatly expanded access to those who might wish to leverage the mobile dark web for illicit means.

What the Mobile Dark Web Means for Enterprise Security.

1. The “Deep Web” is becoming shallower.

While the traditional “dark-web” proves to be less-dark than believed, hackers move to the surface web, using platforms such as social-media and mobile apps. While more traditional forms of communication required an individual to have at least a basic level of knowledge of which sites to visit and how, in addition to the use of a dedicated browser over a desktop computer, today’s black market is accessible more than ever, with the tap of a finger over a portable pocket-held device. This could prove to cause a proliferation of low-level cybercrime, that is conducted by less qualified perpetrators.

2. Monitoring of criminal activity will become a more challenging task

As hacker seek distributed networks over the existing more centralized platforms (black markets, forums), more advanced solutions are required for collecting and analyzing the abundance of data, that is now to be retrieved from a higher and more dynamic number of resources than-ever. The development of avatars in order to collect such data is also a huge part of any successful intelligence operation, since interaction with threat-actors is required in order to locate and join relevant cyber-crime groups.

Select Invite Data by Mobile Messaging App

NOTICE: “Invite Link” URLs have been redacted in the tables below for security reasons. If you would like access to this information, please contact us at info@intsights.com

Discord

Name	Group Tags	Group Type	Country	User Total	Invite Link
A TRIBO	#trambiques, #lottery, #tkomy-comandos	Carding, transfers, fraud, stolen account credentials	Brazil	84	https://discord.gg/Dz5XXXXXX
Carding & Spamming	#general, #spammers, #help-me, #free-stuff	Carding, spamming, transfers, fraud, stolen account credentials	Brazil	82	https://discord.gg/PCrXXXXXX
Experian	#entrada, #checker, #anuncios, #lottery	Stolen credit cards, carding, stolen account credentials	Brazil	27	https://discord.gg/JZzXXXXXX
Fednation	#fednation	Doxing	Global (English)	56	https://discord.gg/G2XXXXXX
Lanet Federallar	#general	Stolen account credentials, CCs,	Turkey	8	https://discord.gg/36vXXXXXX
Los Santos	#general, #referencias_thiago	CCs, carding	Brazil	100	https://discord.gg/srRXXXXXX
Ragnarok	#general, #sales, #requests, #giveaways	Stolen account credentials, VPN, data dumps.	Global (English)	37	https://discord.gg/YqXXXXXX
The Yakuza	#general, #lottery, #esquemas, #checkers, #referencias, #sorteio, #tramos	Banking malware, scam pages for Android, stolen account credentials, CCs, dorks.	Brazil	36	https://discord.gg/fQqXXXXXX
TR4MPO-171	#general	Carding, CCs	Brazil	52	https://discord.gg/9bZXXXXXX
TRAMPOS REIS	#geral, #lottery, #regras, #ajuda	Banking malware, scam pages for Android, stolen account credentials, fake bills, CCs, carding, flights and hotels.	Brazil	50	

WhatsApp

Host	Country	Users	Invite URL
☒ v-ejIsLIFE	India	256	https://chat.whatsapp.com/invite/GFphm0XXXXXX
Phaltu group ☒	India	84	https://chat.whatsapp.com/invite/20j7lxPrqL6CjBXXXXXX
FAKE CARDER	India	29	https://chat.whatsapp.com/invite/9YjJE177H6cKFTHXXXXXX
Indore carding need	India	65	https://chat.whatsapp.com/invite/BJECcpNK1QdAfNXXXXXX
100% Carding	India	24	https://chat.whatsapp.com/invite/Fjd5uRHJbXXXXXX
ESCROW	India	14	https://chat.whatsapp.com/invite/2Y1dO9uXXXXXX
Amazon Deals.!!	India	97	https://chat.whatsapp.com/invite/JWcC4i9LWzXXXXXX
Online Deals 11	India	191	https://chat.whatsapp.com/invite/C1z2FnylKN0XXXXXX
Carding COD Buyers	India	32	https://chat.whatsapp.com/invite/0xm1RFkwUEzXXXXXX
Bitcoin Buy and Sell	India	57	https://chat.whatsapp.com/invite/6uwRf2stXpJ0OmXXXXXX
Shorte.st links only	India	21	https://chat.whatsapp.com/invite/Bx9HCstbmXXXXXX
Redmi4&4A book@350.4Arun	India	23	https://chat.whatsapp.com/invite/85NkNulZuqXXXXXX
Flipkart amazon deals	India	164	https://chat.whatsapp.com/invite/CXCF9xDjlt1XXXXXX
Online Shopping Mall	India	198	https://chat.whatsapp.com/invite/JmLDttpOpCTIjDkXXXXXX
Admin Sell CC	India	91	
⚡.A.K	India	156	https://chat.whatsapp.com/invite/A05kJT6MyKclXXXXXX

XvTrusted Business οξ	India	133	https://chat.whatsapp.com/invite/D4q5Mfmj15jXXXXXX
Ethical hackers(carding)مم	India	116	https://chat.whatsapp.com/invite/6p0TrDRvyvXXXXXX
Best deals v*@	India	185	https://chat.whatsapp.com/invite/H5jxt1OTdrzhhttps://chat.whatsapp.com/invite/6p0TrDRvyvXXXXXX
Criptografia	Brazil	91	https://chat.whatsapp.com/9aam5jhUAPS5gS3vhhttps://chat.whatsapp.com/invite/6p0TrDRvyvXXXXXX
Tropa Hackers	Brazil	123	https://chat.whatsapp.com/3Rq7M4QpBVcCoXXXXX
Linux Pentest	Brazil	82	https://chat.whatsapp.com/6SmhDOuRU2s2LXXXXX
Linux	Brazil	123	https://chat.whatsapp.com/DnPTamtvv7EhQhttps://chat.whatsapp.com/3Rq7M4QpBVcCoXXXXX
IBINS CARDI	Brazil	49	https://chat.whatsapp.com/DaC7vIhXwYRDhS6https://chat.whatsapp.com/3Rq7M4QpBVcCoXXXXX
Computação Forense MM#3	Brazil	256	https://chat.whatsapp.com/3Rq7M4QpBVcCoXXXXX
GNU/Linux/Unix	Brazil	252	https://chat.whatsapp.com/0SpytZbCODh275IPXXXXX
👁️👁️👁️👁️👁️👁️👁️👁️👁️👁️	Brazil	25	
BAD USers 2.0	BRazil	53	https://chat.whatsapp.com/39VHrsPcWN6Ac2piTjSrlm
elastikslasteriskIA2 b	Brazil	151	https://chat.whatsapp.com/8b2vY8RfjKl1rgeSKKhuBw
Anonimato/Intercep t	Brazil		https://chat.whatsapp.com/0ielpX457d4kNous9JcY3

Group Name	Group Type	Country	User Total	Invite Link
Ø§ ŦøØP Ðä ÑeeŦ	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	10461	https://t.me/XXXXXX
† ŦĤĖ CĂŦÐĖR †	Stolen account redentials, stolen edit-cards, proxies.	Brazil	373	https://t.me/XXXXXX
† FSociety Hackers †	Stolen account redentials, stolen edit-cards, proxies.	Brazil	13780	https://t.me/ XXXXXX
Only BINs	Stolen account redentials, stolen credit-cards	Brazil	8335	https://t.me/XXXXXX
OFFICIAL MUNDO ANONYMOUS	Stolen account redentials, stolen edit-cards, proxies.	Brazil	8414	https://t.me/XXXXXX
C :mega Tech:rocket:	Stolen account redentials, stolen edit-cards, proxies.	Brazil	14231	https://t.me/ XXXXXX
DARK WEB	Stolen account redentials, stolen edit-cards, proxies.	Brazil	4009	https://t.me/ XXXXXX
Souza Droiid oficial	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	1593	https://t.me/XXXXXX
caṇaŧ jeff kılŧeя	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	6801	https://t.me/XXXXXX
HACKERS VIP	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	7377	https://t.me/XXXXXX
Zona Carder	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	4129	https://t.me/XXXXXX
((hacker saz)) کاناں گپ	Hacking and security discussions	Iran	83	https://t.me/XXXXXX

CreepyPasta	Global		https://chat.whatsapp.com/EnlFORbdal3bS1VuaFVr3
POSHYDOPE HUSTLERSnONL Y.	Nigeria	151	https://chat.whatsapp.com/invite/19PPrmKsBc14x24dSAthul
D-ATM	Nigeria	126	https://chat.whatsapp.com/invite/KtkxKbjYqwLLvRv1ui8MXy
C-ATM	Nigeria	129	https://chat.whatsapp.com/invite/GiZh7Bkcji132DVNznJWzt
Hackers station	Nigeria	84	https://chat.whatsapp.com/invite/7u1ljjkEJKvCSHL98QBEte
https://Hackornot.net	Nigeria		https://chat.whatsapp.com/invite/3bQvR9990iqLQmx7BXGA9K
Raba Nation	Nigeria	161	https://chat.whatsapp.com/invite/0CheYIXzJimCQijibGH6xn
Hustl Must Pay.	Nigeria	228	https://chat.whatsapp.com/invite/4NxGRjognLMGthjDKaY9yb
Great minds	Nigeria	92	https://chat.whatsapp.com/invite/lkevBgBjsDoAHOmm95YfMf
Ballers	Nigeria		https://chat.whatsapp.com/invite/G2ULYYE0g2JBOqZnPhBpmD
GEE CLASS#...	Nigeria	159	https://chat.whatsapp.com/invite/7NIT6bE8U9TIIaJvQoJXFU
Dreamers H	Nigeria	83	https://chat.whatsapp.com/invite/7YWvN5jUR490IHbGJLCRwC
TBC Global Market	Nigeria	169	https://chat.whatsapp.com/9qTDaf4wZ67ETwTyOxHOzJ

Bokya	Nigeria	226	https:// chat.whatsapp.com/ lcSzC8hiUO4lBxyhVRBVI R
Gee transactions hood	Nigeria	161	https:// chat.whatsapp.com/invite/ APIIfaqJMKOAwha1l kND3j
Money must be made	Nigeria	82	https:// chat.whatsapp.com/invite/ E06eOHslZOLDjub5 fwRydt
let help each others	Nigeria	39	https:// chat.whatsapp.com/invite/ GP41lZeG37aDq9fJ waPXtZ
Carding Zone	Nigeria	237	
PAXS + CC FUZIL	Brazil	250	https:// chat.whatsapp.com/ Ez3xUKPjx9m8JkQOKLs G NR
Vr46 INFO CARDER	Brazil	41	https:// chat.whatsapp.com/ L2R5H75YOvy7ZtnSqS7 d YU
Os melhor do skype הוו:	Brazil	10	https:// chat.whatsapp.com/ 0aOz6yrSyFvDW9neL2S Q xG

Skype

Group	Group Type	Country	Total Users	Invite Link
Aprovações, INFO CC, PAX	Carding , CCs, flights,	Brazil	424	https:// join.skype.com/ XXXXX
MASTER PRIV 8- Kill Gonzales O REI DAS CC'S MAX MELHOR CCS		Brazil	531	https:// join.skype.com/ XXXXX
SMOKEEXE E\$QUEMAS!	CCs	Brazil	36	https:// join.skype.com/ XXXXX
arhiva scan privada : wget rootgoof.esy. es/arhivesca n/ gfq.zip`		Russia	82	https:// join.skype.com/ XXXXX
shkchecker.n et - Breve nova ATT Free	CCs	Brazil	22	https:// join.skype.com/ XXXXX
Quem faz Recarga vivo de 35, preciso de 100 por dia. skype: upsvelox	Carding, CCs, Banking	Brazil	389	https:// join.skype.com/ XXXXX
Carding Group Technology - Mudar Nome = BAN !!	Carding, CCs, Banking	Brazil	133	https:// join.skype.com/ XXXXX
SPAMMERS ME ADICIONEM PARA NEGOCIAR >> cosmos.hacking	CCs	Brazil	126	https:// join.skype.com/ XXXXX
Grupo \$Carders	CCs, Carding	Brazil	69	https:// join.skype.com/ XXXXX

IQT

Group	Group Type	Country	User Total	Invite Link
Hackerz-Club (Escrow)	Carding/Spam/Hacking	Global	158	https://icq.com/chat/XXXXXXXXO_zw
Weed and everything else	CCs, Carding, drugs, account credentials	Global (English)	840	https://icq.com/chat/AoLBr6wKXXXXXX
Billion	CCs, bank logins, RDPs, insider recruitment	Global (English)	141	https://icq.com/chat/AoKbxtXXXXXX
THE MONEY AND DEVICE PLACE	Carding, banking, CCs	Nigeria	40	https://icq.com/chat/AoLDnalXXXXXX

Telegraph

Group Name	Group Type	Country	User Total	Invite Link
SECRET STORY	Carding. Stolen account credentials	Brazil	40702	https://t.me/txt_XXXXX
NETFREE BRASIL	Stolen account credentials, SSH proxies.	Brazil	61135	https://t.me/XXXXX
Mundo Netflix	Stolen account credentials, VPS services.	Brazil	19457	https://t.me/XXXXX
Mundo Netflix	Stolen account credentials, VPS services.	Brazil	19457	https://t.me/XXXXX
Mundo Netflix	Stolen account credentials, VPS services.	Brazil	19457	https://t.me/XXXXX
TG@MovieZoneP H	Pirated movies and TV shows.	Brazil	760	https://t.me/XXXXX

Group Name	Group Type	Country	User Total	Invite Link
TG@MovieZone PH	Pirated movies and TV shows.	Phillipines	760	https://t.me/XXXXX
گروه رسمي کانال (Official Channel of shiyane Security Group)	Security and hacking-related discussions. The group is the Telegram outlet of a forum by same name, which very popular in the Iranian hacking community	Iran	26652	https://t.me/XXXXX
CANAL DO MASCARA	Stolen account credentials, SSH proxies, VPS.	Brazil	3113	https://t.me/XXXXX
CANAL DO MASCARA	Stolen Account	Brazil	24134	https://t.me/XXXXX
UzCyBeR		Uzbekistan	7798	https://t.me/XXXXX
Canaldo KILLER	Stolen Account	Brazil	4424	https://t.me/XXXXX
The Pro Channel	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	1015	https://t.me/XXXXX
KINGS OF TELEGRAM		Brazil		https://t.me/XXXXX HvNQZVa315qufoa w
Super Android	Stolen Account	Brazil	324	https://t.me/XXXXX
WIZARD	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	373	https://t.me/XXXXX
SYN Inovation	Stolen Account & VPN	Brazil	1083	https://t.me/XXXXX
IMPERADOR DAS EHI	Stolen account credentials, stolen credit cards, VPN proxies.	Brazil	5638	https://t.me/XXXXX

Group Name	Group Type	Country	User Total	Invite Link
(hacker_saz) هک ساز	Hacking discussions, licious applications, ccount credentials and leaked data.	Iran	2390	https://t.me/XXXXXX
(TrickLand)ترفندلند	Hacking discussions	Iran	1822	https://t.me/XXXXXX
["Contas prêmio"]	Stolen account redentials, proxies	Brazil	1521	https://t.me/XXXXXX
Hacker Club no.1	Hacking and security discussions	Russia	2432	https://t.me/XXXXXX

NOTICE: "Invite Link" URLs have been redacted in the tables below for security reasons. If you would like access to this information, please contact us at info@intsights.com