Emerging Intelligence Report

(U) PREPARED BY FBI CRIMINAL INVESTIGATIVE DIVISION
TRANSNATIONAL ORGANIZED CRIME INTELLIGENCE UNIT
CO-AUTHOR FBI LOS ANGELES FIELD OFFICE

21 JANUARY 2020
FBI EIR093 20200121

(U//LES) Darknet Actors Almost Certainly Transitioning Communications to Encrypted Platforms, Obscuring US Law Enforcement Visibility into Illicit Activities

(U) This document is classified: Unclassified//Law Enforcement Sensitive
(U) EIR template approved for fiscal year 2020, as of 1 October 2019.

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of the Federal Bureau of Investigation and may be distributed within the federal government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network without first obtaining FBI approval.

(U//LES) The FBI assesses Darknet actors almost certainly[a] are transitioning their communications away from Darknet marketplaces to encrypted communications platforms, further obscuring US law enforcement visibility into illicit activities. This assessment is made with high confidence,[b] based on FBI investigative activity and human source reporting with direct access, and open source reporting with varying degrees of access and corroboration. The FBI makes this assessment based on the assumption Darknet markets are designed for criminal activity and the vast majority of activity originating from the market is for illicit purposes. The FBI further assumes users of Wall Street Market[c] are representative of users on other Darknet markets in the use of encrypted communications platforms. If these key assumptions are wrong, the FBI's confidence in the assessment would decrease, since this could indicate the observed activity represents legitimate business activity of users desiring privacy or that Darknet actors are using other communication means the FBI currently has not identified. The FBI bases this assessment on how encrypted communications platforms provide individuals with a relatively reliable way to conduct and conceal illegal activity. The FBI also bases this assessment on reporting of incidences in which Darknet actors used or discussed using encrypted communications platforms, such as Wickr, ProtonMail, Jabber, and Telegram, to conduct direct transactions, prioritize secure and anonymous communications, and maintain contact in the event a market went offline or exit scammed.[d] The FBI did not conduct analysis of alternatives because searches of seized Darknet marketplace data revealed discussions among Darknet actors about transitions to encrypted communications platforms, which clearly support the assessed use of the platforms specifically to facilitate the sale and purchase of illicit drugs.

- (U//LES) As of April 2019, Wall Street Market users were using encrypted messaging platforms to conduct off-market deals; share sensitive information, such as shipping addresses; or maintain contact in case the market went offline or exit scammed, according to a search of seized historical marketplace data. The encrypted communications platforms most frequently referenced by Wall Street Market users on the site's internal messaging platform were Wickr, ProtonMail, Jabber, Telegram, ICQ, and Kik (See Appendix C).[1]

- (U//FOUO) As of January 2019, experienced Darknet actors prioritized security and anonymity in communication, according to a human source with direct access, some of whose reporting had been corroborated for less than one year. Darknet actors viewed Jabber as the best platform for fast and safe communication between market staff. Administrators for the Darknet forum Dread

[a] (U) See Appendix A: Expressions of Likelihood.

[b] (U) See Appendix B: Confidence in Assessments and Judgments Based on a Body of Information.

[c] (U) Wall Street Market was a Darknet marketplace facilitating the sale of drugs and other illicit goods and services. The site was seized by international law enforcement in May 2019. See Appendix C for additional information.

[d] (U) An "exit scam" is when marketplace administrators close the marketplace and steal all of the cryptocurrency held in escrow from orders, defrauding users.

and Darknet markets Rapture Market, Cerberus Market, Nightmare Market, and Luna Market also used Jabber accounts. Customers and vendors, outside of Darknet markets, used Wickr more frequently because many customers lacked the technical expertise to install and use Jabber.[2]

- (U//FOUO) As of April 2019, Darknet drug vendor *CaliforniasFinest* used a ProtonMail email account to sell crystal methamphetamine and inform customers of product price and shipping methods, according to an FBI employee with direct access and placement.[3]
- (U) Between February 2019 and June 2019, Darknet vendor *Letswork*, an administrator for the Darknet market Rapture Market and vendor on Dream Market, offered direct deals on a Telegram channel, according to an FBI employee with direct access and placement. *Letswork* posted about the availability of different drugs being sold, including cocaine, 3,4-methylenedioxymethamphetamine, amphetamines, ketamine, and ecstasy; as well as quantities, prices, and accepted cryptocurrencies for the drugs. *Letswork* also used Telegram to advertise when listings would be set up on different Darknet markets, including Tochka and Wall Street Markets.[4]

(U//LES) This assessment is consistent with previous assessments made by the FBI, including the 12 July 2019 Strategic Perspective: Executive Analytical Report, titled "(U//LES) Increased Use of Encrypted Communication by Criminal Actors Very Likely Adopted to Evade Law Enforcement Interception and Detection," which assessed criminal actors very likely adopted encrypted technology to purposely evade interception and detection of communications by law enforcement. This emerging intelligence report expands on the previous assessment by identifying new threat actors using encrypted communications platforms for evasive purposes, as well as new platforms being exploited. The FBI judges Darknet actors likely will increasingly shift from conducting illicit business on Darknet markets to encrypted messaging platforms in the next year, obscuring law enforcement visibility, in the wake of numerous law enforcement seizures, distributed denial of service attacks, and exit scams. Indicators of Darknet actors using encrypted communications platforms include an increase in reporting about the use of encrypted communications platforms to make purchases from Darknet vendors, and an increase in recommendations on Darknet market forums to use encrypted communication platforms or alternative platforms for communication and purchases. Changes in the manner or frequency of Darknet actors' use of encrypted communications platforms would cause the FBI to adjust its confidence level accordingly.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Source Summary Statement

(U//FOUO) Reporting in this emerging intelligence report was derived from FBI investigative reporting, including searches of a database of seized Darknet marketplace data; human source reporting from a source with direct access, some of whose reporting has been corroborated; and open source reporting with varying degrees of access and corroboration. The seized marketplace data was critical to understanding the extent and use of encrypted communications by Darknet actors. The open source reporting described the referenced encrypted communication platforms and provided general context regarding their use. Reporting in this emerging intelligence report was collected from 27 February 2019 to 12 November 2019, and was current as of 12 December 2019.

(U) If you would like to provide qualitative feedback on this product, please send an email to the appropriate address with the product title as the subject line: DI_Customer_Feedback@fbi.gov; DI_Customer_Feedback@fbi.sgov.gov; or DI_Customer_Feedback@fbi.ic.gov.

(U) FBI Criminal Investigative Division Transnational Organized Crime Intelligence Unit (TOCIU) and FBI Lost Angeles prepared this emerging intelligence report. Please direct comments and queries to the TOCIU Unit Chief at 1-202-323-8911.

(U) Appendix A: Expressions of Likelihood

(U) Phrases such as “the FBI judges” and “the FBI assesses,” and terms such as “likely” and “probably” convey analytical judgments and assessments. The chart below approximates how expressions of likelihood and probability correlate with percentages of chance. Only terms of likelihood should appear in FBI products; the chart includes terms of probability strictly for comparison, as they sometimes appear in reporting of other government agencies. Furthermore, the FBI does not arrive at judgments through statistical analysis and will not use terms of probability to convey uncertainty in FBI external intelligence products.

UNCLASSIFIED

Terms of Likelihood	**Almost No Chance**	**Very Unlikely**	**Unlikely**	**Roughly Even Chance**	**Likely**	**Very Likely**	**Almost Certain(ly)**
Terms of Probability	Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
Percentages of Chance	1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

(U) Table showing terms of likelihood aligned with terms of probability and percentages of chance.

(U) Appendix B: Confidence in Assessments and Judgments Based on a Body of Information

(U) Confidence levels reflect the quality and quantity of the source information supporting a judgment. Consequently, the FBI ascribes high, medium, or low levels of confidence to assessments, as follows:

(U) **High confidence** generally indicates the FBI's judgments are based on high quality information from multiple sources. High confidence in a judgment does not imply the assessment is a fact or a certainty; such judgments might be wrong. While additional reporting and information sources may change analytical judgments, such changes are most likely to be refinements and not substantial in nature.

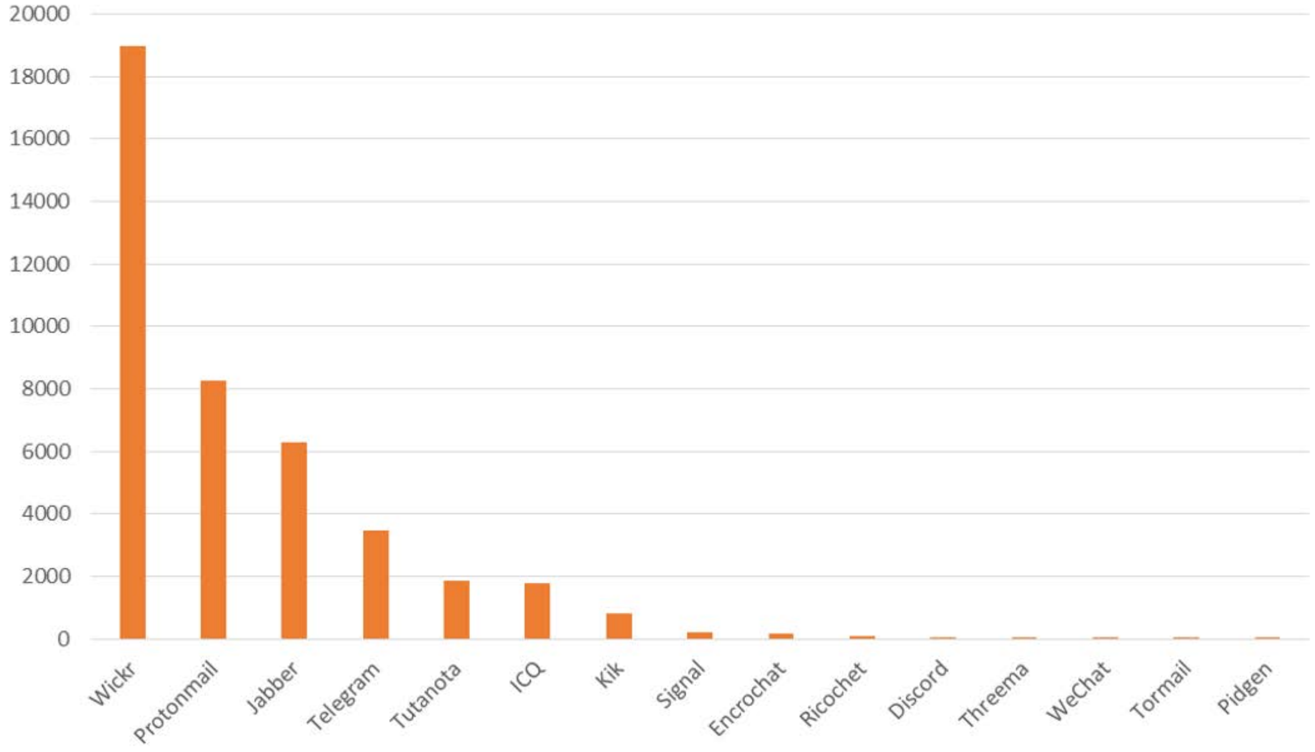
(U) **Medium confidence** generally means the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. Additional reporting or information sources have the potential to increase the FBI's confidence levels or substantively change analytical judgments.

(U) **Low confidence** generally means the information's credibility or plausibility is uncertain, the information is too fragmented or poorly corroborated to make solid analytic inferences, or the reliability of the sources is questionable. Absent additional reporting or information sources, analytical judgments should be considered preliminary in nature.

(U) Appendix C: Mentions of Communications Platforms in Wall Street Market Messages, by Communications Platform

(U//LES) In April 2019, administrators of Wall Street Market conducted an exit scam, transferring any funds that remained in escrow on the marketplace to their own wallets. Marketplace administrators did not shutdown the marketplace or its messaging platform, however, allowing marketplace users to communicate with each other after the exit scam. According to seized marketplace data, marketplace vendors used the marketplace messaging function to reach out to their marketplace clients and share alternate forms of contact, and marketplace users reached out to their preferred vendors to share and request alternate forms of contact. The following chart outlines the communications platforms referenced by marketplace users, by frequency of mention. The most popular communications platforms were Wickr (18,953 mentions), ProtonMail (8,272 mentions), Jabber (6,284 mentions), Telegram (3,471 mentions), ICQ (1,763 mentions), and Kik (797 mentions).

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



(U) Communications platforms referenced by Wall Street Market users, by frequency of mention

(U//LES) *Source:* FBI | Case Information | 12 November 2019 | 3 May 2019 | “(U//LES) Mentions of communications platforms in Wall Street Market messages” | UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE | UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE.

(U) Appendix D: Overviews of Top Communications Platforms Referenced in Wall Street Market Messages

(U//LES) The most popular communications platforms referenced by Wall Street Market users were Wickr, ProtonMail, Jabber, Telegram, ICQ, and Kik. Below are overviews of each of these communications platforms. The FBI is providing the logos for situational awareness, in the event operators and analysts discover them on subjects' computers or electronic devices, indicating possible use.

(U) Wickr

UNCLASSIFIED

(U) Wickr is a free instant messaging application that allows users to communicate across various platforms (mobile, desktop, and tablets). Wickr users can share messages, images, audio messages, and video chats, all of which are end-to-end encrypted. It allows for secure screen sharing and location sharing. It allows for user-defined burn-on-read settings so users can decide what is done with their communications once they are sent. It also detects screenshots and alerts the sender when screenshots are taken of what they have sent, and sends them a picture of what on the screen was captured. Wickr is available for download on iOS, Android, Windows desktop, Mac OSX, Linux 32 Bit, and Linux 64 Bit platforms. Wickr is produced by an American software company based in San Francisco.[e]

(U) ProtonMail

UNCLASSIFIED

ProtonMail

(U) ProtonMail is an email service with built-in end-to-end encryption. ProtonMail uses zero access architecture, meaning that users' data are encrypted and inaccessible to ProtonMail administrators. All ProtonMail servers and network traffic are encrypted, which means there is no tracking or logging of personally identifiable information. Users can set an optional expiration time on ProtonMail's encrypted emails, so they will be automatically deleted from the recipient's inbox once they have expired. ProtonMail uses Secure Sockets Layer to secure communication between its server and the user's computer. ProtonMail supports sending encrypted communication to non-ProtonMail users via symmetric encryption. When an encrypted message is sent to a non-ProtonMail user, the recipient receives a link that loads the encrypted message onto the recipient's browser, which can be decrypted using a passphrase that the sender has shared with the recipient. ProtonMail is incorporated in Switzerland, which according to ProtonMail offers some of the strongest privacy protection in the world for both individuals and corporations.[f]

(U) Jabber

UNCLASSIFIED

(U) Jabber, paired with the off-the-record protocol, is a free, secure, open source, and decentralized communications platform that can be set up anonymously. Jabber is a protocol, not a mobile application, but other applications, such as Pidgin, support Jabber with off-the-record and can be used to send text messages using Jabber. Jabber does not work smoothly on mobile phones, as the protocol needs an almost continuous connection between the message sender and recipient. The difficulty in installing and using the platform, along with its lack of features (that is, users cannot send attachments), may deter most users. For those who need an extremely secure communications platform and are willing to deal with the obstacles presented by this platform, however, Jabber is viewed as the best encrypted communications platform.[g]

[e] (U) Website | Wickr.com | "Why Wickr?" | https://wickr.com/why-wickr/ | accessed on 30 October 2019.

[f] (U) Website | ProtonMail.com | "About" | https://protonmail.com/about | accessed on 30 October 2019.

[g] (U) Website | ExpressVPN.com | "The most secure messaging apps in 2019" | 30 October 2019 | https://www.expressvpn.com/blog/best-messaging-apps | accessed on 5 November 2019.

(U) Telegram

UNCLASSIFIED

(U) Telegram is a free, cloud-based encrypted communications. Telegram allows users to send text messages, photos, videos, and other types of files. It is cross-platform, meaning that users can access their accounts from any browsing platform. Users can chat individually or in groups. Telegram uses its own protocol, MTProto, to encrypt users' messages. Messages are not encrypted by default; users have to create "secret chats" to encrypt them. Users can set messages to self-destruct across all devices automatically or at a set time. Messages not encrypted by users are stored on Telegram's servers. Security bugs have been found in Telegram, including one that allowed a security researcher to find a way to determine when users were online and, therefore, possibly who they were talking to and when, making some actors reluctant to use the platform. Telegram is based in Berlin, Germany.[h]

(U) ICQ

UNCLASSIFIED

(U) Originally developed in 1996, ICQ was one of the first standalone instant messaging clients. Revamped in recent years, ICQ is a multi-platform messenger that allows users to send text, video, audio, and stickers. ICQ provides end-to-end encryption for video calls, but not for normal text messages. It allows for individual or group messaging and has Snapchat-like filter features. ICQ has chatrooms, called Live Chats, which can host thousands of participants and focus on specific topics. ICQ includes photo and video-editing capabilities. ICQ is available for iOS, Android, PC, Web, Mac OS X, and Linux operating systems. ICQ is owned by Mail.ru in Russia.[i, j, k, l]

[h] (U) Website | ExpressVPN.com | "The most secure messaging apps in 2019" | 30 October 2019 | https://www.expressvpn.com/blog/best-messaging-apps | accessed on 5 November 2019.

[i] (U) Website | Medium.com | "ICQ Is Back, and There are 11 Things You Should Know About it" | 18 January 2017 | https://medium.com/@Dimitryophoto/icq-is-back-and-there-are-11-things-you-should-know-about-it-b993dddfc234 | accessed on 5 November 2019.

[j] (U) Website | ICQ.com | "ICQ" | https://icq.com | accessed on 5 November 2019.

[k] (U) Website | Techspot.com | "What Ever Happened to ICQ?" | 23 December 2018 | https://techspot.com/article/1771-icq/ | accessed on 5 November 2019.

[l] (U) Website | GaryWolff.com | "ICQ's Privacy Risks: Users Beware" | garywolff.com/subdir/icq.html | accessed on 5 November 2019.

(U) Kik

UNCLASSIFIED

(U) Kik is a free and anonymous messaging application that allows users to send text, pictures, videos, GIFs, stickers, and web browser links. Users can communicate individually or in public or private groups. Kik does not require a telephone number for registration, but does track Internet protocol addresses to determine users' locations. Kik messages are not end-to-end encrypted, but Kik claims it deletes messages from its servers as soon as they are delivered to a user's device. This means the time it would have to view messages would be very short. Kik was owned by Kik Interactive until October 2019, when it was sold to MediaLab after a legal fight with the US Securities and Exchange Commission about irregularities in its initial coin offering for its virtual currency, Kin.[m, n, o]

[m] (U) Website | Vox.com | "Is Your Messaging App Encrypted?" | 21 December 2015 | https://www.vox.com/2015/12/21/11621610/is-your-messaging-app-encrypted | accessed on 5 November 2019.

[n] (U) Website | Vice.com | "Kik Had a Huge Child Predator Problem. Now It's Shutting Down" | 24 September 2019 | https://www.vice.com/en_us/article/43k4dw/kik-had-a-huge-child-predator-problem-now-its-shutting-down | accessed on 5 November 2019.

[o] (U) Website | Kik.com | "Kik is here to stay!" | 18 October 2019 | https://www.kik.com/blog/kik-medialab-acquisition | accessed on 5 November 2019.