FEDERAL BUREAU OF INVESTIGATION INTELLIGENCE BULLETIN

(U//FOUO) Administrators Operating on the Darknet Likely Relying on Legal Gateways to Route Users, Facilitating the Trafficking of Illicit Products and Services

(U) PREPARED BY FBI KANSAS CITY FIELD OFFICE
CO-AUTHORS, FBI NEW YORK FIELD OFFICE, FBI CYBER DIVISION

7 MAY 2020
FBI IB103 20200507

(U//FOUO) The FBI assesses administrators operating on the Darknet[a] likely[b] are relying on legal gateways[c] to route users to Darknet marketplaces, facilitating the trafficking of illicit products and services[d] by legitimate means. This assessment is made with medium confidence,[e] based on two human sources with direct access, and open source reporting from the Empire Market.[f]

(U//FOUO) The FBI makes this assessment with the key assumption that administrators of Darknet marketplaces are aware of the illegality associated with gateways collating links to Darknet markets and profiting from the facilitation of the sale of illicit products and services on those marketplaces. Over the next one to two years, the FBI judges administrators of criminal Darknet marketplaces likely will increase reliance on legal gateways for visitor traffic and approach gateway administrators to offer payment in return for illegal cooperation, facilitation, or promotion,[g] reducing the effectiveness of future law enforcement takedowns. Indicators that would lead the FBI to revise this judgment would be observing the impact of a law enforcement Darknet marketplace takedown, and monitoring the migration of vendors and buyers to other marketplaces listed by the legal gateways.

[a] (U) *Analyst Note*: The Darknet is a portion of the Internet consisting of services and sites that can only be accessed by individuals using the Tor anonymization software.
[b] (U) See Appendix A: Expressions of Likelihood.
[c] (U) *Analyst Note*: A "gateway" is a website accessible through the Internet that aggregates the .onion addresses of hidden services, to include Darknet marketplaces and forums.
[d] (U) *Analyst Note:* Illicit products and services include narcotics, fraudulent and digital products, and software and malware delivery services.
[e] (U) See Appendix B: Confidence in Assessments and Judgments Based on a Body of Information.
[f] (U) *Analyst Note:* The Empire Market is currently the largest Darknet marketplace, facilitating the sale of narcotics, fraudulent and digital products, and software and malware.
[g] (U) *Analyst Note:* Promotion includes recommending users visit a specific marketplace or valuing certain marketplaces above others through means of unique display or stated intention by an administrator of a gateway platform.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Source Summary Statement

(U//FOUO) Reporting in this intelligence bulletin was derived from two human sources with direct access and open source reporting. The first human source was deemed credible because of the source's extensive reporting record over the last two years and direct access to the information provided. The second human source maintains direct access at the direction of the FBI and their reporting has been corroborated over the last four years. Furthermore, reporting provided by each human source was corroborated in part by the reporting from the other human source. The FBI deemed the human source reporting as reliable in making the assessment because of the direct access to the information and partial corroboration. Both human sources provided critical information for the assessment and provided additional context. Open source information from one Darknet marketplace was used to supplement the human source reporting. The human source collection occurred between August 2019 and March 2020, while the open source collection occurred between May 2019 and February 2020. The reporting was current as of March 2020.

(U//FOUO) Administrators Operating on the Darknet Likely Relying on Legal Gateways to Route Users, Facilitating the Trafficking of Illicit Products and Services

(U//FOUO) The FBI assesses administrators operating on the Darknet likely are relying on legal gateways to route users to Darknet marketplaces, facilitating the trafficking of illicit products and services by legitimate means. This assessment is based on reporting indicating the administrators of Darknet marketplaces, forums, and websites rely on services via communication through email or Jabber[h] provided by Dark.Fail, DarknetLive, and other legal gateways for visitor traffic.[i] In addition, the administrator of Empire Market indicated Dark.Fail was the preferred method of obtaining Uniform Resource Locators (URLs) to access Empire Market; and the administrator of Dread engaged with Dark.Fail to prove authenticity to keep the site listed on the Dark.Fail gateway.

- (U//FOUO) According to a human source with direct access who has been reporting over the last two years, as of 20 March 2020, Darknet administrators used personal connections with gateway administrators to get the Darknet market URLs listed on the gateway.[1] As of 28 November 2019, Darknet administrators and moderators engaged with DarknetLive and Dark.Fail to provide advice and opinions on the existing Darknet markets. A known moderator for several Darknet markets interacted with DarknetLive to provide a list of markets to display on DarknetLive.com and advised on adding and removing markets when given proper information about them from other Darknet market administrators and moderators, according to the same source.[2]

[h] (U) *Analyst Note:* Jabber is a secure and encrypted decentralized instant-messaging platform used by cyber criminals to communicate in real-time.

[i] (U) *Analyst Note:* The current notable gateways that appear to be operating legally include but are not limited to Dark.Fail (Dark.Fail), DarknetLive (Darknetlive.com), DNStats (DNStats.net), and Dark Eye (t7tb43a7gvl6wb7j.onion).

- (U//FOUO) According to a human source with direct access who has been reporting over the last four years, as of 30 March 2020, the administrators of gateways to the Darknet posed as journalists or news sites and were contacted directly by Darknet marketplace administrators using email or Jabber.[3] As of 4 February 2020, Darknet marketplaces relied on gateways to function as a phishing solution to avoid scammers and to serve as a repository for reputable links to each site, according to the same source.[4]

- (U) According to open source reporting from the Empire Market, as of 24 February 2020, the banner on its main page states "Don't get Phished! Never login using random links and only get links from Dark.Fail or darkfailllnkf4vf.onion."[5]

- (U//FOUO) According to a human source with direct access who has been reporting over the last two years, as of 1 October 2019, HugBunter, the administrator of the Dread forum, confirmed his identity to the administrator of Dark.Fail to ensure the Dread forum had not been taken over by law enforcement. HugBunter answered 10 specific questions that only HugBunter knew the answer to for authentication purposes, ensuring the Dread criminal forum remained listed on Dark.Fail.[6]

(U) Perspective

(U//FOUO) Administrators of Darknet marketplaces, including historical marketplaces such as AlphaBay, Hansa, Dream, and Wall Street, relied on DeepDotWeb (DDW)[j] for visitor traffic to bolster sales and profits of illegal contraband and services. In response to the DDW takedown, gateways to Darknet marketplaces adopted lessons learned to operate legally, primarily by avoiding receiving money from administrators in exchange for listing URLs to the markets or taking referral fees for visitors routed to Darknet marketplaces. This resulted in a shift in the modus operandi of gateways and how they interact and cooperate with Darknet marketplaces and forum administrators. According to a human source with direct access, as of November 2019, the administrator of Dark.Fail did not accept payments for marketplace listings in order to stay within legal boundaries.[7] According to another human source with direct access, as of December 2019, Dark.Fail was different from previous gateways in order to be 100 percent legal.[8] According to a post on the Darknet forum Dread by the administrator of DarknetLive, as of 25 May 2019, sites dedicated to information and news were legal as long as the sites avoided the modus operandi employed by DeepDotWeb, which was to receive money from marketplaces in exchange for listing the URLs to the markets, which is a violation of US laws.[9]

(U//FOUO) This bulletin is the first FBI external product evaluating the shift in the extent of the relationship between Darknet marketplaces and forum administrators and gateways that route users to aforementioned marketplaces and forums. Furthermore, this bulletin advances the understanding of this threat by examining the gateways to the Darknet that have emerged to take the place of DDW that are relied upon by administrators to facilitate Darknet illicit contraband and services.

[j] (U) *Analyst Note*: DDW was a gateway to Darknet marketplaces that was seized in May 2019 for profiting from the facilitation of the sale of illegal contraband.

(U) Analysis of Alternatives

(U//FOUO) The FBI considered the alternative hypothesis that administrators operating on the Darknet likely engage with gateways at an illicit level, while the gateways present an effective façade of legitimacy by appearing to be legal services, deterring law enforcement interdiction. The FBI discounted this alternative because a combination of human source and open source reporting provide the unified impression that current gateway administrators are meticulously avoiding any violations of US laws following the takedown of the DDW seizure in May 2019. The FBI will reexamine this hypothesis and adjust the likelihood if information or human source reporting arises indicating that the administrations of gateways to the Darknet are receiving profits for their services via virtual currency transfers from Darknet marketplaces.

(U) Outlook

(U//FOUO) Over the next one to two years, the FBI judges administrators of criminal Darknet marketplaces likely will increase reliance on legal gateways for visitor traffic and approach gateway administrators to offer payment in return for illegal cooperation, facilitation, or promotion, reducing the effectiveness of future law enforcement takedowns. Opportunities to exploit this shift in the modus operandi of Darknet marketplaces relying on legal gateways requires more extensive placement and access of human sources and a coordinated strategy among the law enforcement agencies and the US Department of Justice to further integrate the current approach to Darknet investigations. Additionally, debriefings and proffer interviews of apprehended subjects involved in running Darknet marketplaces and forums will provide law enforcement with opportunities to further understand how marketplaces and gateways to the Darknet interact. Indicators of this increasing reliance on legal gateways and incentive payments to gateway administrators include:

- (U//FOUO) Observing the impact of a law enforcement Darknet marketplace takedown, and monitoring the migration of vendors and buyers to other marketplaces listed by the legal gateways;
- (U//FOUO) Human source reporting indicating administrators of marketplaces are attempting to send virtual currency to administrators of gateways; and
- (U//FOUO) Administrators of gateways receiving suspicious virtual currency transfers from Darknet marketplaces, suggesting payment in return for cooperation.

(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 Cyber Division, FBI Kansas City Field Office, and FBI New York Field Office prepared this intelligence bulletin. Please direct comments and queries to the Kansas City Field Intelligence Group at 1-816-512-8200, the New York Field Intelligence Group at 1-212-384-1000, or the Major Cyber Crimes Intelligence Unit at 703-633-6059.

(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.