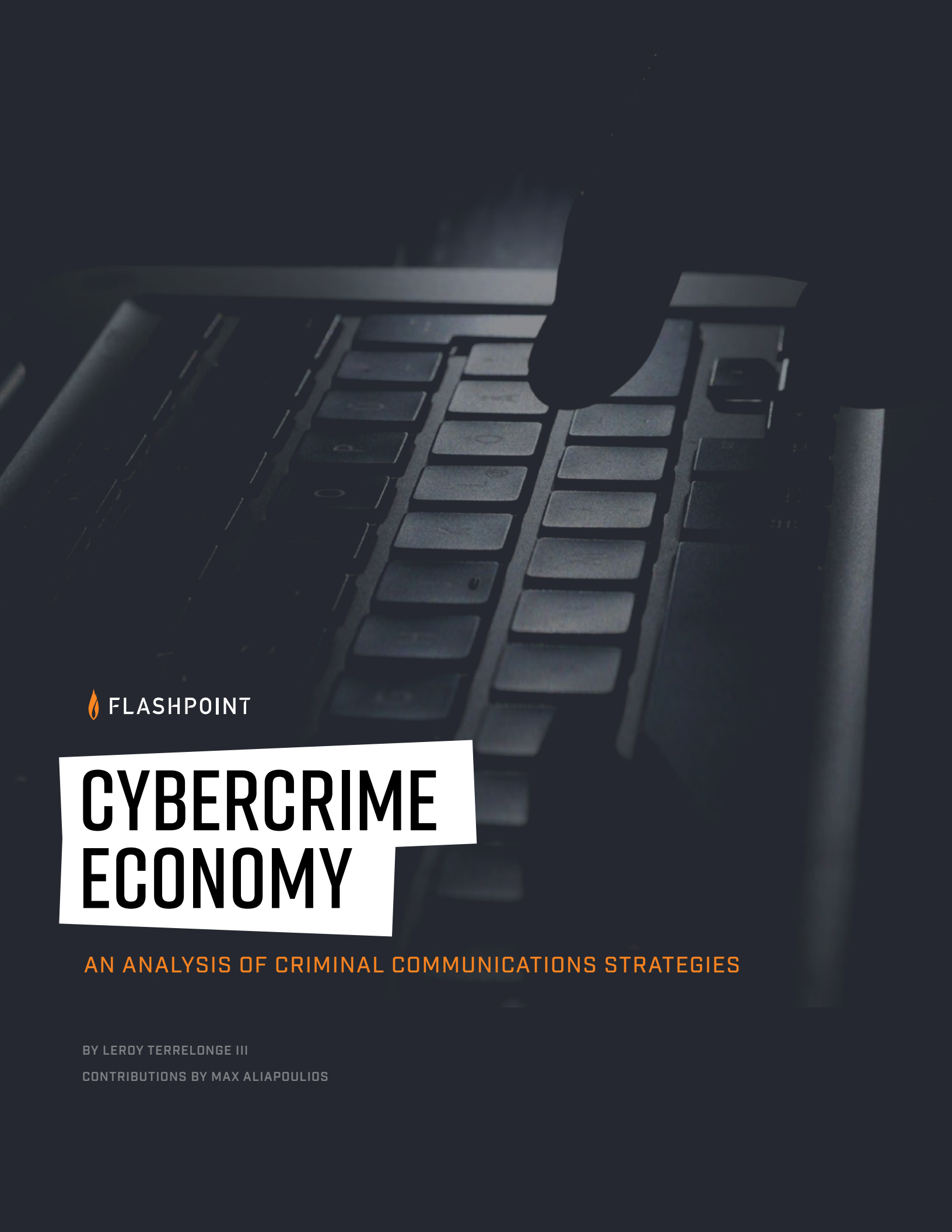

FLASHPOINT

CYBERCRIME ECONOMY

AN ANALYSIS OF CRIMINAL COMMUNICATIONS STRATEGIES

BY LEROY TERRELONGE III

CONTRIBUTIONS BY MAX ALIAPOULIOS

FLASHPOINT

CYBERCRIME ECONOMY

An Analysis of Criminal Communications Strategies

In the continuous game of cat and mouse between cybercriminals and the information security community, the criminals have long understood that they can act much more effectively together than they can individually. In addition, cybercriminals' unrelenting drive to conceal their activities presents countless challenges for organizations seeking to protect themselves from cyber threats. Often operating within the exclusive confines of the Deep & Dark Web, cybercriminals are known to utilize various tools to engage with one another and advance their tactics all while evading detection. In order to provide greater visibility into the interconnected nature of the cybercrime economy, this paper examines the most common communication strategies and tools used by cybercriminals across seven different communities.

First, criminal communities provide a place for actors to collaborate by sharing tips and tricks that help them defeat security measures and evade detection. Indeed, criminal communities resemble research communities in that each member of the community can learn from the successes and failures of other members.

Second, cybercriminal communities allow for the division of labor and, consequently, economies of scale for the cybercriminal ecosystem. Many cybercrime schemes depend on the actions of a cast of characters working in concert, including malware developers, cryptor writers, spammers, botnet masters, payment card specialists, and cashers, among others. If cybercriminals were required to carry out their schemes on an individual basis, it would take them many years to develop the necessary cross-domain expertise. The substantial resource expenditure required to obtain the equipment needed to support a crime campaign would also serve as a barrier. In a cybercrime community, however, members specialize according to their interests and talents; this allows them to reach higher levels of proficiency in just one link of the cybercrime chain. They can then share this knowledge with other community members (for free or for pay), which raises the overall level of activity, expertise, and efficiency in the entire system.

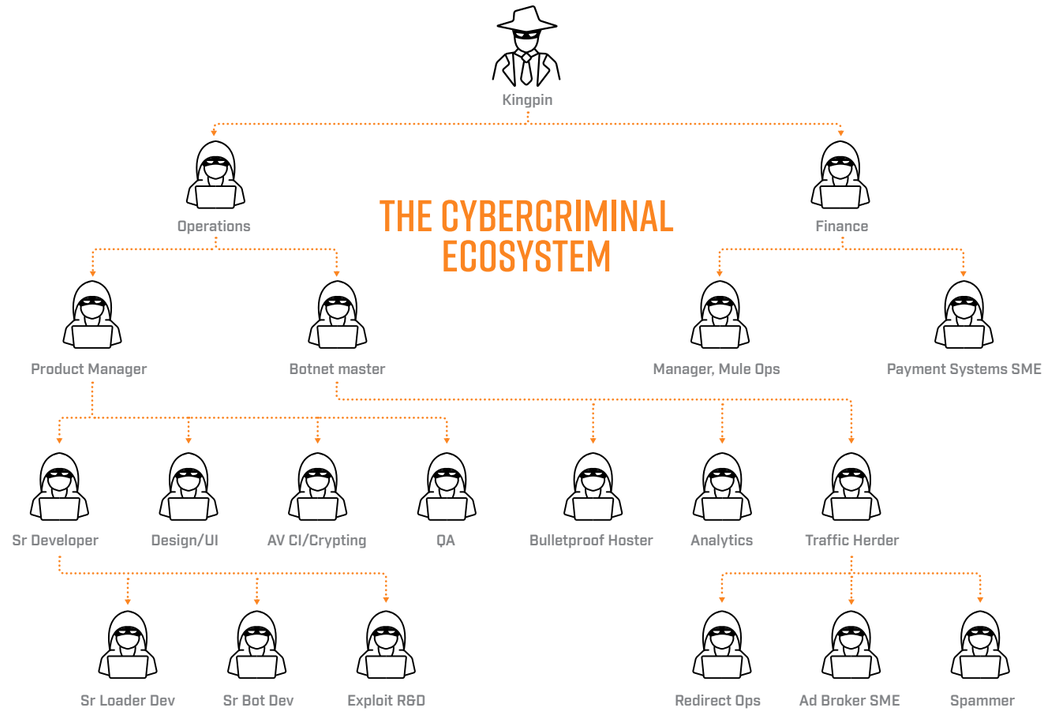

Image 1 - The cybercriminal ecosystem

Image 1: Depiction of the cybercrime ecosystem: The division of labor allows actors to specialize in domains for which they have a comparative advantage or special talent, advancing the level of expertise in their particular area of specialization beyond what could be accomplished if each individual actor were responsible for all elements of the cybercrime chain. In addition, the barrier of entry is lower for new participants because they can merely purchase the goods and services they need, as opposed to spending significant time and money building capacity themselves.

The traditional meeting place for cyber actors, including cybercriminals, has been and continues to be the online messaging board, or web forum. In many ways, these forums are the beating heart of the cybercrime economy. Members meet, recruit additional support, buy technical tools (e.g. malware), and sell their illicit goods and services through online forums. Like any other community, cybercrime communities have rules (both explicit and implicit), enforcers (moderators), an organizer (administrator), unique jargon, and varying barriers to entry. But, once they gain acceptance into the "club," members have access to the institutional knowledge and resources afforded by the forum and its members.

Image 2 on following page: Screenshot of Darkode (now defunct), one of the most well-known online forums and marketplaces for malware, stolen data, credit card numbers, botnets, and malicious tools. The site was seized and many of its members were arrested in July 2015 as part of a coordinated international law enforcement effort.

Despite the central role of the forum for cybercriminal enterprises -- not to mention its crucial

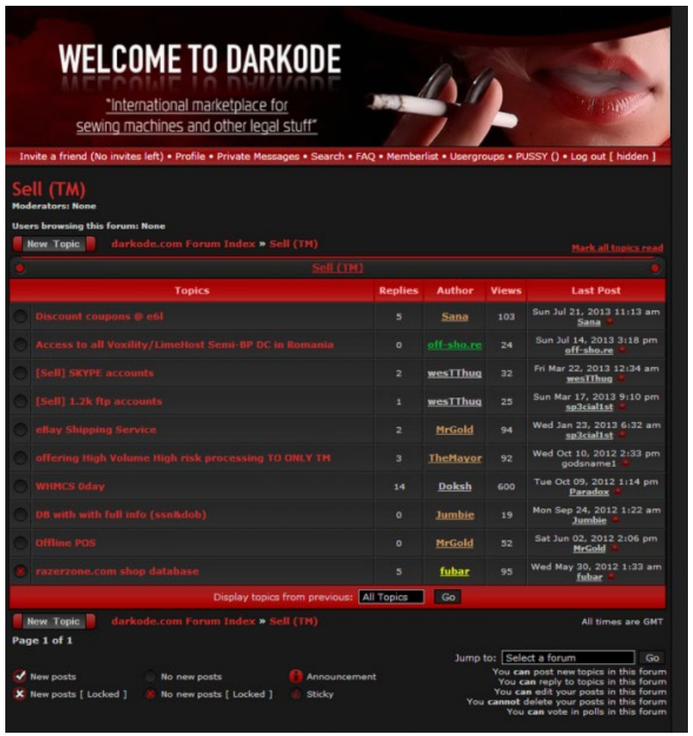

Image 2 - Darkode Homepage

function of bringing criminals together and allowing them to find each other -- once criminals meet, they may choose to move their communications outside of the forum for a number of reasons -- even though the forums have native private messaging platforms. One reason for this behavior is that criminals can never be quite sure exactly who has access to the backend of the forum on which they are operating. Even in the unlikely scenario that a criminal could trust that the forum administrator had their best interests at heart, administrator accounts can be compromised. Such a compromise would put any unencrypted personal communications into the hands of an unknown and untrusted party.

Another reason cybercriminals choose to communicate outside of forums is so they can maintain access to logs of their previous communications. These forums are notorious for suddenly disappearing or experiencing unexpected downtimes, during which criminals' forum correspondence becomes temporarily or permanently inaccessible. The causes for this instability can be nefarious, as in the case of "exit scams" wherein forum administrators close the board and abscond with all the funds held in member's accounts or in the forum's escrow service. Forums can also disappear or be disrupted during law enforcement busts when officers seize forum servers. Forums may also go down for more benign reasons, such as instances where there is no longer enough interest in maintaining the forum or if the administrators are no longer able to pay the hosting fee.

CHOICE OF MESSAGING PLATFORM

Cybercriminals can choose from a wide variety of platforms to conduct their peer-to-peer (P2P) communications. This choice is typically influenced by a combination of factors, which can include:

Ease of use — All other factors held equal, cybercriminals, like any other user, prefer services that are simple, have a clean graphical user interface (GUI), are intuitive to use, and are not "buggy". They may also appreciate customizations and/or localizations that make it easier for them to use the tool. Such features may be especially appealing to speakers of less-common languages or those who use operating systems other than the commercially-popular Windows and OS X.

Country and/or language — Communication platforms are sometimes promoted heavily, or even exclusively, to speakers of a particular language. When these platforms are the dominant communication medium for a language group, cybercriminals are likely to use them in their "civilian" lives to interact with friends and family. Indeed, this usage may creep into their criminal endeavors as well. It is also worth noting that services may become unavailable in countries as a result of government actions. For example, in December 2015 and May 2016, the Brazilian government banned WhatsApp for failing to deliver data requested as part of a criminal investigation.

Security and/or anonymity concerns — Messaging platforms have differing anonymity and encryption capabilities that make them less or more attractive to cybercriminals. Cybercriminals will evaluate platforms based on the encryption protocol used (for instance, is it end-to-end?), where encryption keys are stored, the jurisdiction in which the services' servers are located (can they be accessed by law enforcement agencies?), the privacy policy of the service, the information collected from users to set up an account on the service, etc.

Image 3 - Secure Messaging Scorecard from the EFF

Image 3: The Electronic Frontier Foundation developed a Secure Messaging Scorecard in which it ranked the security/encryption practices of thirty-seven popular messaging applications along seven basic criteria:

- Is data encrypted in transit?
- Is data encrypted so the provider cannot read it?
- Can users verify contacts' identities?
- Are past communications secure if encryption keys are stolen?
- Is the code open to independent review?
- Is the security design properly documented?
- Has there been a recent code audit?

Cybercriminals use similar criteria to inform their choice of messaging platform[1].

[1] https://www.eff.org/node/82654

METHODOLOGY

To conduct this study, the authors relied on mentions of social media platforms in the underground communities monitored by Flashpoint. These observations were used as a proxy for gauging interest in and use of these messaging services. The communities in this study are primarily composed of actors involved or interested in financially-motivated cybercrime (with the notable exception of Iranian actors).

Flashpoint analysts have observed that when criminals invite other community members to interact with them outside of the forum, they often leave their contact information at the end of the message (e.g. “ICQ: 9999999”) or express a preference for the platform on which they prefer to interact. Underground communities also constantly discuss the merits of the different messaging services available and advise each other on which services are best to use. For this reason, comparing the number of mentions of messaging services should provide a rough approximation of the relative popularity of these various services.

This methodology, of course, has limits — not every mention of a social media service indicates that the actor who posted the message uses this platform. It is certainly possible that criminals are posting about and discussing platforms that they themselves do not actually use. While this is plausible, however, in practice and in the aggregate, it is more likely than not that the criminals are discussing services they use or are interested in.

It is also the case that some posts with mentions of messaging services are meant to dissuade others from using that platform (typically due to security concerns). Since only mentions are counted, the nuance of whether these mentions are positive or negative is not reflected in the data results. Based on analysts’ observations, however, negative posts about messaging services are far less prevalent than other types of posts (e.g. positive reviews, or provision of contact information). As such, the presence of this noise is unlikely to skew the results significantly.

Analysts started with a list of approximately 80 instant messenger platforms/protocols, and created filters for these platforms to query against Flashpoint’s Deep & Dark Web dataset. In most cases, five instant messenger platforms accounted for 80 to 90 percent of the mentions across an underground language community. Analysts then took the top 8 to 10 results and compared them with each other to visualize the relative frequency of mentions of these instant messenger platforms.

It is worth mentioning that the messaging services Signal and Line presented extraordinary challenges based on the ubiquity of these words in English, as well as in programming languages. Given the high degree of noise associated with the results from these services, Signal and Line are not included in most results. Based on the results of our research, however, Signal and Line do not constitute a significant number of mentions in any language community included as part of this research.

BACKGROUND ON THE TOP INSTANT MESSAGERS APPEARING IN THIS STUDY

ICQ — This messaging service began in 1996 under the auspices of Israeli company Mirabilis; it is considered to be the first stand-alone instant messenger service. AOL bought Mirabilis in 1998 and controlled ICQ until 2010, at which point the company sold ICQ to Digital Sky Technologies. Digital Sky Technologies (now Mail.Ru group) is headed by Alisher Usmanov, an Uzbek-born Russian businessman. This connection to Usmanov and the Mail.Ru group played a significant role in ICQ’s continued popularity among Russian-speakers and citizens of countries of the former Soviet Union. The service’s heavy use in the cybercrime ecosystem is likely due to the prominence of Russian-speakers in financially-motivated cybercrime activity, as well as the desire for speakers of other language communities to interact with and learn from these actors. ICQ’s offered features include group chats, video chats, stickers, free calls, file transfers, and unlimited texting. As of the most recent information available, ICQ encrypts voice and video calls, but does not encrypt written messages. Users who wish to encrypt their communications can use a third-party app that works with the ICQ protocol via a downloadable plug-in. ICQ has an estimated active user base of 11 million users.

Skype — Skype was founded in 2003 based on software written by Estonian developers. In 2005, eBay acquired Skype and later sold it to Microsoft in 2011. Since then, Microsoft has embedded the application in many of the devices it sells, further increasing Skype’s availability and cementing its presence among the population. Skype allows for instant messaging, free video and audio calls, free file and screen sharing, paid calls to mobile and landline numbers, paid text messaging, and paid call forwarding, among others. While Skype encrypts data in transit, the application does not provide end-to-end encryption, does not allow for verification of contacts’ identities, and does not secure past communications in the event that encryption keys are stolen -- otherwise known as “forward secrecy”. In addition, documents leaked by former NSA contractor Edward Snowden showed that the US National Security Agency (NSA) was able to collect Skype video calls through its Prism program, thereby potentially exposing Skype users’ communications to government surveillance. Skype has an estimated active user base of 300 million.

Jabber (XMPP) — The Extensible Messaging and Presence Protocol (XMPP), more commonly known in the underground by its original name, Jabber, is an open-source, Extensible Markup Language (XML)-based platform that allows for the near-real-time exchange between network entities. It was created in 1998 by Jeremie Miler and has since been incorporated into social networking, instant messaging, voice over IP (VoIP), and file transfer services, among others. Instant message users typically download an instant messaging client with XMPP functionality, such as Adium, Gajim, iChat, Pidgin, or others. Certain XMPP clients (whether through additional plugin or by default) also include the option for Off-the-Record (OTR) messaging, which is a cryptographic protocol that encrypts instant messages. By enabling OTR, users can communicate with end-to-end encryption, forward secrecy, and user authentication. Criminals are drawn to this service

because it is free, secure, open-source (anyone can review the XMPP and OTR and report vulnerabilities), and decentralized (anyone can run a Jabber server and the technology is not controlled by any single entity).

Pretty Good Privacy (PGP) — Although not a messaging service, PGP was included in this study based on the popularity of encrypted communications in certain communities. Developed by Philip Zimmerman in 1991, PGP is an encryption program used to encrypt and decrypt texts, emails, files, and disk partitions, as well as authenticate messages with digital signatures. To send a message to another user with PGP, two (or more) users must create public and private cryptographic keys and share the public keys with each other. User A encrypts their message via User B's public key and sends the message to User B who can then decrypt the messaging with their private key. Given the extra burden on users (swapping keys, manually encrypting and decrypting messages), sending messages with PGP would generally seem to be less attractive than using an instant messaging service with built-in encryption functionality. Furthermore, PGP is end-to-end encrypted but does not provide forward secrecy. In other words, if users' encryption keys become known, all of their previous messages can be decrypted.

AOL Instant Messenger (AIM) — Originally part of the AOL package, AIM was launched as a standalone program in 1997 and quickly became the dominant messaging program of the late 1990s and early 2000s. Usage of the service waned in the mid to late 2000s following the introduction of competitors (such as Google Chat), free and widespread SMS services, and social network sites. AIM allows for instant messaging, group messaging, file transfers, and free text messaging. AIM does not provide end-to-end encryption, forward secrecy, or user authentication. AOL is also believed to have participated in the NSA's Prism program. Data on numbers of active users could not be found for AIM.

Telegram — Created by Nikolai and Pavel Durov, both of whom are also known for launching VK, Russia's most popular social networking platform, Telegram is a cloud-based messaging service that was launched in 2013. Once users sign up using their phone number, Telegram allows them to send messages, stickers, files, photos, and videos. One important feature of the service is the secret chat feature. When secret chat functionality is enabled, users have end-to-end encryption, user authentication, and forward secrecy. Messages can also be set to self-destruct after a predetermined amount of time. Additional important features include channels that allow administrators to blast messages to an unlimited number of recipients. This combination of features has made the service attractive to jihadist groups, who use have been known to use Telegram to disseminate official statements, claims of credit, videos, and propaganda. Invite-only group chats also allow for curated distribution of materials. Flashpoint has previously reported on jihadist use of Telegram in its publication Tech for Jihad. Telegram has an estimated 100 million users.

WeChat — Known in China as Weixin, WeChat was launched in 2011 by Chinese technology giant Tencent. WeChat offers free video calls, group chats, broadcast messaging, and file transfers. Far more than a messaging service, however, WeChat is also used to check news, play video games, shop online, pay bills, book taxis, and conduct mobile payments. WeChat encrypts messages in transit but does not offer end-to-end encryption, user authentication, or forward secrecy. In addition, there are concerns surrounding allegations that the Chinese government has access to WeChat communications, particularly for users in China. It has an estimated 806 million active users, primarily in China.

QQ — Also developed by Tencent, QQ is another instant messaging service popular among Chinese users. It was patterned after the ICQ instant message service and was launched by Ma Huateng in 1999. QQ offers chatrooms, games, online file storage, internet dating services, and virtual currency. Like its sister company WeChat, QQ has been criticized for being complicit in the Chinese government's alleged surveillance and censorship initiatives. It does not provide end-to-end encryption, user authentication, or forward secrecy, but does encrypt data in transit. QQ has an estimated 899 million active users, primarily in China.

WhatsApp — With over 1 billion estimated active users around the globe, WhatsApp is the most popular stand-alone messaging application. The messaging service was launched in 2009 by former Yahoo! employees Jan Koum and Brian Acton and was acquired by Facebook in 2014. The service offers messaging, group chats, video and voice calls, and file transfers. WhatsApp worked with Open Whisper Systems to start providing end-to-end encryption for the app in 2014; the service also provides user authentication and forward secrecy. The company's provision of these security and encryption features have put it at odds with law enforcement, most notably in Brazil where it has been banned on multiple occasions for not complying with court requests to turn over users' communications.

Kik — Released in 2010, Kik is the brainchild of university students in Canada and has become very popular among teenagers in the United States. Unlike many other messaging services, Kik users do not have to provide their mobile phone numbers, which helps users preserve a bit of anonymity in their interactions with the app. Some of Kik's features include messaging, file transfers, group chats, and video chats. The service claims 300 million total users, but has not provided information on how many of them are active users.

LANGUAGE GROUP SPECIFIC FINDINGS

RUSSIAN

In 2012, the top eight instant messengers mentioned in the Russian underground were as follows:

1. **ICQ (51.83%)**
2. Skype (25.98%)
3. Jabber (XMPP) (18.7%)
4. Quiet Internet Pager (1.55%)
5. Pretty Good Privacy (0.74%)
6. Pidgin (0.41%)
7. PSI (0.41%)
8. AOL Instant Messenger (AIM) (0.37%)

Four years later, the landscape looked very different. The 2016 breakdown of instant messenger mentions was as follows:

1. **Skype (38.72%)**
2. Jabber (24.77%)
3. ICQ (21.05%)
4. Telegram (7.26%)
5. Viber (4.47%)
6. WhatsApp (2.01%)
7. Zephyr (0.85%)
8. Pretty Good Privacy (PGP) (0.81%)

The most interesting changes over the four-year period include the ascendance of popular messaging services Telegram and Viber to the top rang of instant messaging services used in the Russian underground. Mentions of Skype grew significantly, while mentions of Jabber (XMPP) increased slightly and mentions of ICQ dropped precipitously, in part ceding ground to other messaging services.

The story is even more interesting when we consider the distribution of mentions in elite Russian forums. In 2012, that distribution was as follows:

1. **ICQ (60.63%)**
2. Jabber (XMPP) (17.93%)
3. Skype (16.93%)
4. PGP (1.87%)
5. Quiet Internet Pager (1.61%)
6. Pidgin (0.42%)
7. Tencent QQ (0.34%)
8. AOL Instant Messenger (0.26%)

Jabber and ICQ accounted for 78.56% of the top instant messenger mentions. This observation is realistic given the heavy usage of ICQ by Russian speakers and the emphasis on anonymity and privacy provided by Jabber.

By 2016, however, ICQ ceded ground to Jabber, which moved into first place among the relative mentions, and Telegram, which grew to occupy a sizable share of the pie. This evidences a shift in user preferences towards messaging platforms that are more secure, provide better anonymity, and are either decentralized or otherwise make it difficult for law enforcement to access logs of user activity. The breakdown for instant messenger mentions in 2016 was as follows:

1. **Jabber (28.3%)**
2. Skype (24.26)
3. ICQ (18.74%)
4. Telegram (16.39%)
5. WhatsApp (3.93%)
6. PGP (3.79%)
7. Viber (3.01%)
8. Signal (1.58%)

SPANISH

Compared to members of Russian-language underground forums, members of Spanish-language underground forums tend to be less technologically sophisticated and less aware of issues pertaining to privacy and anonymity. These characteristics are reflected in the mix of instant messaging services mentioned across the Spanish-language underground.

In 2012, that mix consisted of the following services:

1. **Skype (48.76%)**
2. WhatsApp (13.64%)
3. Pidgin (7.23%)
4. ICQ (5.99%)
5. Windows Live Messenger (5.58%)
6. Jabber (XMPP) (6.4%)
7. AOL Instant Messenger (AIM) (4.55%)
8. Trillian (2.89%)
9. PGP (2.89%)
10. Nimbuzz (2.07%)

Far and away, the service most often mentioned was Skype, while the most popular services among the most elite Russian-speaking cybercriminals (ICQ and Jabber) are mentioned much less frequently.

This distribution was starkly different during 2016. ICQ moved into the number one spot, displacing Skype, and upstart Kik Messenger came to occupy a large share of the mentions among Spanish-speaking users. In 2016, mentions of instant message platforms were distributed as follows:

1. **ICQ (51.5%)**
2. Skype (15.11%)
3. Kik Messenger (13.44%)
4. Jabber (8.21%)
5. WhatsApp (7.07%)
6. Telegram (2.11%)
7. PGP (0.98%)
8. AOL Instant Messenger (0.86%)
9. Threema (0.56%)
10. Pidgin (0.5%)

The dramatic shift to mentions of ICQ likely highlights Spanish-speaking cybercriminals' efforts to mimic the communication patterns of more sophisticated users in Russian-speaking communities. Flashpoint analysts have observed numerous instances of information flows from Russian and English-language communities into Spanish-language communities. These flows take place through connectors -- individuals active across a number of different language communities who facilitate exchanges of information between these otherwise siloed groups. In the same way that analysts have observed that malware introduced on Russian forums typically take a few months to find their way into Spanish language communities, it appears that usage of platforms is also influenced by trends in more elite forums.

The large volume of Kik Messenger mentions is more difficult to explain. The service is not popular among elite cybercriminals from other language communities, and given that Kik has existed since 2010 but did not rise in prominence in the Spanish-language underground until near the end of 2016, it is unclear what caused the sudden recent spike in popularity. One potential answer could be the fact that Kik (like ICQ and Telegram) facilitates group chats among members of the service. In light of the rather turbulent nature of Spanish-language communities that appear and disappear sudden-

ly and without warning, analysts have observed members forming groups on Kik and ICQ, likely in part for redundancy reasons should the main forum go down.

FRENCH

Many of the French-language cybercrime communities included in this study are very conservative when it comes to their communication choices. Historically, they have tended to be very distrustful of instant messaging services and generally prefer to use email or the forum messaging system to send messages encrypted with Pretty Good Privacy (PGP) software. Indeed, most forums have a special field for members to publish their public PGP key, some forums strongly encourage members to publish their public key and encrypt their communications, and still other forums do not admit member prospects who do not provide a public PGP key. Some forums have even integrated PGP encryption capability into the forum messaging platform to make it easier for members to send encrypted messages to each other.

Members of the French underground take their privacy and anonymity seriously. This characteristic is reflected in the distribution of messenger services found in that community as far back as 2012. The distribution is as follows:

1. **Pretty Good Privacy (58.62%)**
2. Skype (16.55%)
3. Jabber (14.48%)
4. Pidgin (10.34%)

Of the four most mentioned services, all but Skype are well-known for providing the option of encrypted communications.

Since 2012, French actors have embraced the use of Jabber, and this is reflected in the share of mentions of this service during 2016. The distribution of mentions for 2016 is as follows:

1. **Jabber (45.84%)**
2. PGP (40.11%)
3. ICQ (8.49%)
4. Skype (2.18%)
5. Pidgin (1.3%)
6. Tox (0.59%)
7. AOL Instant Messenger (0.46%)
8. Telegram (0.31%)
9. Ricochet (0.29%)
10. WhatsApp (0.19%)
11. Wickr (0.15%)

While some members of French communities continue to insist on PGP as the only secure means of communication, many have started to use Jabber alongside PGP to conduct their communications outside of the forum. Based on Flashpoint's long experience monitoring these forums, the French-language underground is by and large the most security-conscious language community in the Deep & Dark Web. Even novice members of French underground communities are indoctrinated very quickly into the best ways to maintain their privacy, security, and anonymity. In fact, those who do not comply are often ridiculed or refused membership in more elite communities. The results of this study tend to confirm those observations.

ARABIC

In 2012, Arabic-language forums were dominated by mentions of Skype and Windows Live Messenger. Jabber, Yahoo! Messenger, and ICQ were close behind. The 2012 distribution was as follows:

1. **Skype (32.82%)**
2. Windows Live Messenger (18.45%)
3. Jabber (15.73%)
4. Yahoo! Messenger (9.45%)
5. ICQ (6.55%)
6. Paltalk (3.82%)
7. Nimbuzz (3.73%)
8. AOL Instant Messenger (3.73%)
9. MSN Messenger (3%)
10. WhatsApp (2.73%)

Overall, there does not appear to be a noticeable trend of using secure or anonymous messaging platforms based on the 2012 snapshot.

In 2016, WhatsApp leapt to the top of the charts in terms of mentions on Arabic-language forums. Skype remained a close number two, and interestingly, AOL Instant Messenger came in third with a much higher number of mentions than analysts would have expected. It is not clear what may have spurred increased discussion of this particular messenger, especially since its popularity has been in decline since approximately 2009.

Interestingly, Arabic-language communities do not appear to exhibit the common trend of increased discussions pertaining to more sophisticated messaging systems. While it is true that WhatsApp introduced end-to-end encryption in 2016, it is unclear whether this feature played a role in shaping preferences around the use of this tool and its rise to number one in the Arabic-speaking underground. It is possible that the communities we monitor are so isolated that they have not been able to learn communication best practices from other groups of threat actors. It could also be the case that members of these communities have not felt the need to update their communication practices because they have not felt pressure from their host governments or local law enforcement agencies.

The distribution of mentions for Arabic language forums in 2016 was as follows:

1. **WhatsApp**
2. Skype
3. AOL Instant Messenger
4. ICQ
5. Yahoo! Messenger
6. Jabber
7. Viber
8. Palatal
9. Windows Live Messenger
10. Pretty Good Privacy (PGP)

CHINESE

The Chinese-language instant messaging market is dominated by Tencent in the form of its two applications, QQ and WeChat. This dominance appears to be reflected in the cyber domain as well. It is understandable that QQ would have a prominent position since it has been around since 1999. However, only one year after its 2011 launch, WeChat had already garnered close to 10 percent of mentions in the Chinese underground. The distribution among Chinese-language communities in 2012 was as follows:

1. **QQ (88.39%)**
2. WeChat (8.62%)
3. Skype (1.03%)
4. Pretty Good Privacy (0.62%)

5. Windows Live Messenger (0.47^)
6. Line (0.46%)
7. ICQ (0.14%)
8. FaceTime (0.09%)
9. AOL Instant Messenger (0.08%)
10. Miranda (0.05%)
11. WhatsApp (0.04%)

Over the last four years, mentions of WeChat have gained considerably on mentions of QQ; although it appears that QQ is still the most popularly discussed platform in the Chinese underground. The two platforms even managed to further displace other platforms, collectively accounting for just shy of 99 percent of mentions of instant message platforms in 2016. The distribution in 2016 is as follows:

1. **QQ (63.33%)**
2. WeChat (35.58%)
3. Skype (0.44%)
4. WhatsApp (0.22%)
5. Jabber (0.31%)
6. PGP (0.13%)
7. ICQ (0.1%)
8. AOL Instant Messenger (0.08%)

Interestingly, cybercriminals in other language groups tend to avoid messaging services that are strongly suspected of collaborating with their host governments, as is the case with QQ and WeChat. In contrast, Chinese-speaking actors embrace QQ and WeChat, but in their communications employ specialized slang to evade the notice of censors and "hide" in plain sight. While cybercriminals in many other language groups use specialized jargon in their communications, this jargon is not typically meant to intentionally obfuscate their messages. In this regard, the Chinese-speaking underground is unique among the language groups in this study.

The near exclusive mentions of QQ and WeChat combined with their absence from other language communities also suggests that the Chinese underground is relatively isolated from other language communities. While Flashpoint analysts have observed limited instances of crossover between Russian and Chinese communities, interactions on the whole between Chinese and other language communities appear to be much more limited than interactions between French, Spanish, Portuguese, English, Russian, and other language communities.

PERSIAN/FARSI

In 2012, members of Persian-language underground communities most actively discussed Yahoo! Messenger and Nimbuzz. The popularity of Yahoo! Messenger makes sense given that Yahoo was the most popular email service in Iran with over 63 percent using the company's email service as their primary email account. The factors behind the popularity of Nimbuzz are less obvious; it is known to be widely-used in India, but not particularly so in Iran. The distribution of messaging service mentions in 2012 was as follows:

1. **Yahoo! Messenger (51.28%)**
2. Nimbuzz (17.15%)
3. Skype (7.37%)
4. ICQ (5.45%)
5. Kik Messenger (4.97%)
6. AOL Instant Messenger (4.01%)
7. Pidgin (2.88%)
8. Jabber (2.72%)
9. Windows Live Messenger (2.24%)
10. MSN Messenger (1.92%)

In 2016, Telegram became the undisputed leader among messaging services in Iran, with an estimated 20 million Iranians (one in four Iranian citizens) using the service. The reason for Telegram's success was two-fold. First, other services that had been popular among Iranian users in recent years (such as Viber and social media platforms Facebook and Twitter) were blocked by Iranian authorities, making it more difficult to access them inside the country.

The Iranian government has discussed blocking Telegram on a number of occasions and has attempted to pressure the company to relocate its servers that handle Iranian traffic onto Iranian soil. Despite these tensions, the government has yet to make the decision to ban or block the service. In fact, a number of Iranian newspapers, politicians, and government ministries operate Telegram channels. In December 2016, however, administrators of Telegram channels with more than 5,000 members were informed they must register with the Ministry of Culture and Islamic Guidance by February 25, 2017, or face prosecution.

Image 4: Telegram CEO Pavel Durov claimed in October 2015 that the Iranian Ministry of Information and Communications Technology had blocked Telegram for refusal to collaborate in spying on Iranian citizens. The incident is shrouded in mystery, however, as many Iranian Telegram users reported that they experienced no disruptions in the service, and a spokesperson for Iran's Ministry of ICT told Iranian media outlets that the government had taken no steps to block Telegram in the country.

Image 4 - Telegram CEO, Pavel Durov on Twitter

The second reason for Telegram's success is its emphasis on encrypted communications. Iranians are very conscious of the role that surveillance plays in their society. For example, after controversial results in Iran's 2009 presidential election, many members of Iran's Green Movement were arrested in light of suspicions that their mobile phone communications had been monitored.

The results in this study confirm Telegram's popularity in Iran. Telegram is by far the most frequently discussed instant messaging platform in the Persian-language underground; it eclipses all other instant messaging platforms. The distribution for 2016 was as follows:

1. **Telegram (88.5%)**
2. Line (4.54%)
3. Skype (2.9%)
4. Yahoo! Messenger (0.96%)
5. Viber (0.92%)
6. Kik Messenger (0.64%)
7. WhatsApp (0.64%)
8. Tennent (0.44%)
9. PGP (0.24%)
10. AOL Instant Messenger (AIM) (0.24%)

ENGLISH

Across the English-language underground in 2012, Skype commanded a large majority of mentions while AOL Instant Messenger was less popular. The distribution of mentions across English-language communities in 2012 was as follows:

1. **Skype (80.29%)**
2. AIM (11.57%)
3. ICQ (3.25%)
4. Jabber (2.99%)
5. Kik Messenger (0.74%)
6. Xfire (0.56%)
7. Zephyr (0.32%)
8. Yahoo! Messenger (0.29%)

In 2016, Skype was still the leader among instant message services mentioned in English-language communities. However, Skype did cede ground to Jabber, ICQ, and Kik Messenger. In addition, numerous secure and/or encrypted chat messengers such as Telegram, Wickr, and WhatsApp joined the ranks of the most frequently discussed services. The distribution in 2016 was as follows:

1. **Skype (62.94%)**
2. Jabber (11.75%)
3. ICQ (9.81%)
4. Kik Messenger (5.63%)
5. Pretty Good Privacy (PGP) (3.68%)
6. AOL Instant Messenger (3.64%)
7. Telegram (1.54%)
8. WhatsApp (0.57%)
9. Wickr (0.24%)
10. Tox (0.2%)

OVERALL FINDINGS

SKYPE IS KING

Based on our findings, analysts observed that Skype is by far the most frequently mentioned messenger across the language communities in this study. Skype was among the top five messengers in all of the language groups, and only in the French, Persian, and Chinese language communities did Skype not constitute a significant share of the most mentioned messengers. Microsoft's bundling of Skype with its devices has likely played a large role in the application's popularity.

CYBERCRIMINALS ARE INCREASINGLY INTERESTED IN ENCRYPTED COMMUNICATIONS

Cybercriminals across the language communities in this study moved from discussing messaging services with fewer encryption and anonymity protections to more sophisticated applications with these protections built-in. Services that have become more popularly discussed in underground forums over the past few years include Jabber, Telegram, and WhatsApp. This shift can be explained by a number of factors:

- Revelations of NSA surveillance that likely prompted more users to adopt more secure communications practices
- The proliferation of encrypted communications apps, particularly in the wake of Edward Snowden's leaks
- Information sharing by connectors in more sophisticated underground communities, who have transferred knowledge about secure communication practices to other less-sophisticated communities.

RUSSIAN-SPEAKING CYBERCRIMINALS ARE TRENDSETTERS FOR OTHER CYBERCRIME COMMUNITIES

Russian-speaking cybercriminals are well-known for their prowess and universally considered the most innovative and sophisticated actors in the cybercrime ecosystem. For this reason, actors from other language communities often emulate Russian cybercriminals in an attempt to raise their own levels of competency. A practical example of this phenomenon is the number of mentions of ICQ across many cybercrime language communities. Based on usage patterns of ICQ in the general population (where ICQ has fallen into disfavor except in the countries of the former Soviet Union), one would expect to see a commensurate drop in the share of mentions across the cybercrime underground. In contrast, there was a general uptick across a number of communities. Given that there is no security rationale for increased mentions of ICQ (the service does not natively offer end-to-end encryption), the most plausible explanation is criminals' desire to model themselves more closely to Russian-speaking criminals or adopt the technology to facilitate communication with Russian-speaking actors.

BUSINESS RISK INTELLIGENCE ANALYSIS

The results of this study underscore the interconnected, agile nature of the cybercriminal ecosystem. Regardless of their language, skills, location, or affiliation, cybercriminal groups tend to share a strong desire to reap the benefits of cross-community collaboration, information sharing, and even mentorship. Such activities necessitate consistent access to reliable means of communication, which is why the digital communication tools examined within this study play such an integral role in facilitating cybercriminal behavior. In many instances, a cybercriminal's livelihood may depend on his or her ability to communicate with peers while evading third-party detection. As such, the decision to utilize one communication tool over others is not taken lightly and often influenced by numerous contextual social, cultural, and geopolitical factors.

For organizations seeking to address and mitigate cyber threats, these insights can help direct existing and future intelligence-led initiatives while cultivating an increased understanding of the complex variables driving cybercriminal behavior. However, it is crucial to recognize that for some organizations, cybercriminals' use of the aforementioned digital communication tools may have more substantial implications depending on the extent to which an organization and its stakeholders engage with and/or support such tools.

In order to evaluate the risks posed by cybercriminals' use of certain communication tools, organizations should consider and further analyze the relevancy and potential impact of the following questions:

- Does an acceptable use policy address employee usage of third-party communication tools such as those outlined in this report?
- Is employee usage of such tools within internal networks monitored and/or regulated?
- Is internal network traffic monitored for personal application usage, abnormal downloads, and other behaviors that diverge from what would be expected within a business environment?
- Does the organization have ample visibility into the Deep & Dark Web to monitor for and address emerging cybercrime threats and trends?

For organizations involved in the production and/or sale of tools similar to those examined in this study, the potential implications may be more substantial. The following questions can provide additional direction and help these organizations evaluate and address any relevant risks:

- Do compliance regulations exist to address cybercriminals' and other threat actors' use of the organization's' products to facilitate illicit behaviors?
- If yes, how does the organization achieve and maintain compliance?
- In the event that law enforcement subpoenas the communication records of cybercriminals or other threat actors, do formal policies and internal processes exist to minimize disruption and ensure operational continuity?
- What measures exist to mitigate damages to brand reputation in the event that the organization receives public attention for ties to cybercrime and/or other illicit behaviors?

Regardless of an organization's size, industry vertical, or location, cyber threats will continue to persist, grow more complex, and yield countless challenges across all business functions. While even the most robust, well-equipped security teams may never be able to detect and protect against each and every threat proactively, Business Risk Intelligence (BRI) derived from the Deep & Dark Web can provide organizations with additional visibility and critical insights to not only help address cyber threats but also inform strategic decisions and mitigate risk across the enterprise.