INTSIGHTS
Defend Forward™

Instant Messaging Mayhem
Communication Channel of Choice for Cybercriminals

Research by Alon Grosglik

www.intsights.com

The cybercriminal underground is a sprawling network of communities with unique features and methods of sharing information, hacking techniques, and stolen assets. While plenty of the action takes place in dark web forums and black markets, cybercrime groups and individual hackers often operate in settings that might otherwise be innocuous by nature – like instant messaging (IM) applications.

IM platforms allow mobile or web users to send real-time text messages, voice messages, picture messages, video messages, or files to individuals or groups. The evolution of smartphone technologies, along with the decreasing cost and convenience of mobile data plans and public Wi-Fi accessibility, have driven the popularity and explosion of IM apps in recent years. Many threat actors have followed suit, adopting secure or encrypted peer-to-peer communication networks as a means to avoid increased government scrutiny of popular black markets and forums on the dark web.

IntSights researchers actively monitor threat actor activity in numerous IM platforms, such as Telegram, Discord, Whatsapp, XMPP/Jabber, Skype, IRC, Signal, ICQ, and others. This report breaks down the recent overall increase in IM platform usage among threat actors between January 2019 and January 2020, with data pulled from our proprietary external threat intelligence platform and enhanced by manual research efforts.

The following are some of the key findings and highlights from our research:

- There is an overall increase in threat actor usage of IM platforms. Telegram appears to be experiencing the most growth, with more than 56,800 Telegram invite links shared across cybercrime forums and over 223,000 general mentions of the application across forums. Telegram is also the platform most often discussed in foreign language forums.

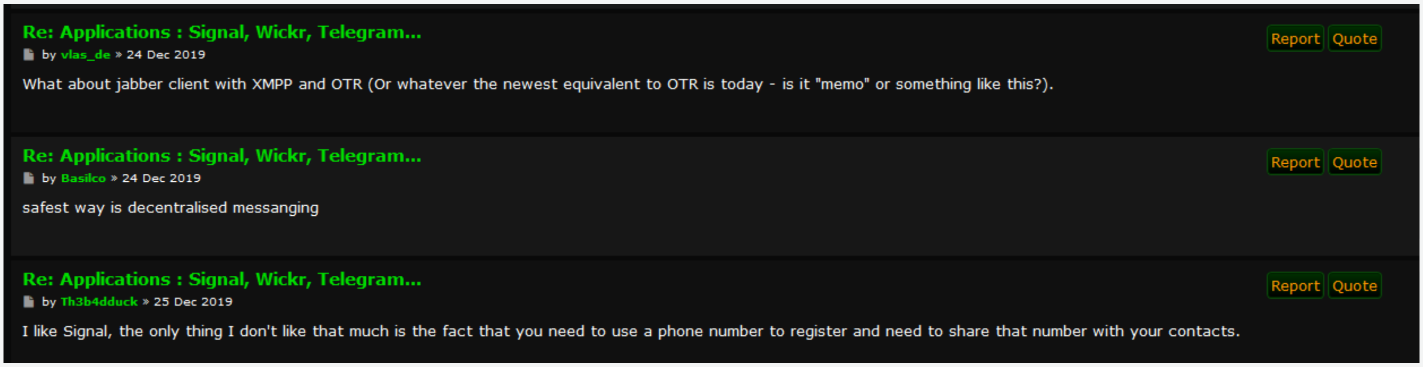
- Discord is the second fastest-growing platform among threat actors, and the most-talked-about platform, with over 392,000 general mentions on our scraped cybercrime forums.

- Threat actors are leveraging popular IM platform capabilities for advertising and communication. Criminals plug their goods for sale in instant messaging platforms, in addition to the traditional cybercrime forum and black market channels.

- We noticed several warnings and security concerns expressed by threat actors due to law enforcement focus on IM platforms and security vulnerabilities discovered in the past year.

Advantages of Using Instant Messaging Platforms

While traditional cybercrime sources (e.g., forums, black markets, credit card shops, etc.) continue to see regular traffic, there is an ongoing shift toward alternative peer-to-peer communication networks and chat channels among threat actors. The migration to these platforms is at least partially the result of the 2017 Operation Bayonet, a multinational law enforcement initiative that targeted the AlphaBay and Hansa markets, as well as the ongoing law enforcement takedowns of major marketplaces and cybercrime forums.



Re: Applications : Signal, Wickr, Telegram...
by vlas_de » 24 Dec 2019
What about jabber client with XMPP and OTR (Or whatever the newest equivalent to OTR is today - is it "memo" or something like this?).

Re: Applications : Signal, Wickr, Telegram...
by Basilco » 24 Dec 2019
safest way is decentralised messanging

Re: Applications : Signal, Wickr, Telegram...
by Th3b4dduck » 25 Dec 2019
I like Signal, the only thing I don't like that much is the fact that you need to use a phone number to register and need to share that number with your contacts.

Conversation regarding the differences between discussion applications, found on the notorious crypto-focused "Torum"

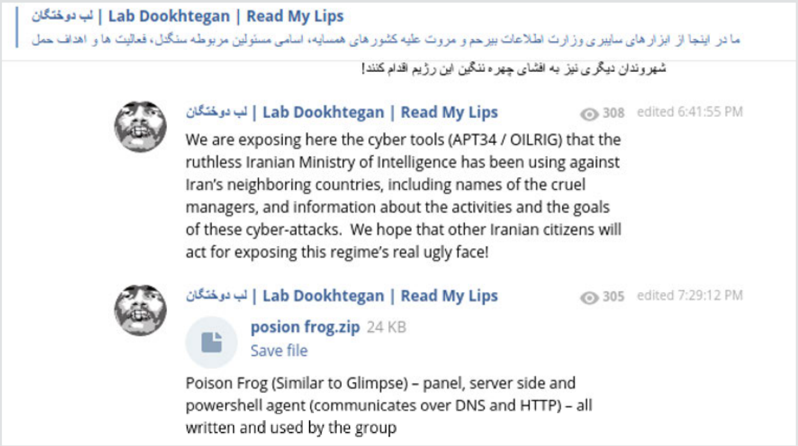
Cybercriminals are choosing such platforms as an alternative for sharing their goods and services outside of the traditional centralized one-stop-shop black marketplaces, which law enforcement agencies are eager to take down. There are many advantages of using IM channels compared to dark web forums and black markets, including:

Increased Customization

Cybercriminals have been using older IM platforms, such as IRC, Jabber, or ICQ, as fast-pace communication tools since the genesis of underground cybercrime. In the past, trades or exchanges existed mostly on internet-based chat forums or black markets. Threat actors had to rely on those as the exclusive platforms for marketing or trading their goods.

In recent years, however, many threat actors have figured out that they can use IM platforms for advertising purposes, in addition to the traditional avenues. The fast growth and widespread use of modern IM platforms, such as WhatsApp, Telegram, Discord, and Skype, have created a space for cybercriminals to operate in the open while remaining undetected due to the privacy of such platforms.

An example of the surging popularity of IM platforms is the April 2019 leak of Iranian hacking group APT34's toolset. A rival Iranian hacking group called "Lab Dookhtegan" leaked the information with the full source code exclusively on Telegram without first offering it on any well-known black market or forum.



لب دوختگان | Lab Dookhtegan | Read My Lips
ما در اینجا از ابزارهای سایبری وزارت اطلاعات بیرحم و مروت علیه کشورهای همسایه، اسامی مسئولین مربوطه سنگدل، فعالیت ها و اهداف حمل
شهروندان دیگری نیز به افشای چهره ننگین این رژیم اقدام کنند!

لب دوختگان | Lab Dookhtegan | Read My Lips 308 edited 6:41:55 PM
We are exposing here the cyber tools (APT34 / OILRIG) that the ruthless Iranian Ministry of Intelligence has been using against Iran's neighboring countries, including names of the cruel managers, and information about the activities and the goals of these cyber-attacks. We hope that other Iranian citizens will act for exposing this regime's real ugly face!

لب دوختگان | Lab Dookhtegan | Read My Lips 305 edited 7:29:12 PM
posion frog.zip 24 KB
Save file
Poison Frog (Similar to Glimpse) – panel, server side and powershell agent (communicates over DNS and HTTP) – all written and used by the group

The "Lab Dookhtegan" Telegram group sharing an APT34 toolset

IM platform easy-to-use features and capabilities, like automated answers and chat bots, have enabled threat actors to create alternative marketplaces alongside the traditional static chat forums and black markets. Cybercriminals can now establish and control their own marketplaces with minimal effort – from their own mobile devices. They can also avoid having to follow rules set by moderators on black markets and forums restricting advertisements, the frequency of publishing and trading, and the types of goods they can sell.

Privacy and Security

Other advantages offered to threat actors using IM platforms include enhanced security features and data encryption. Unlike cybercrime forums, which are often built on unencrypted technologies (like forums that are stored on the clear web), modern IM platforms offer an easy, accessible medium for threat actors to avoid detection. Users can ensure privacy by using some of the built-in features in IM platforms like end-to-end encrypted groups, data encryption chats or servers, capabilities like "ghost mode" that obscure location and IP address, and invitation-only groups that prevent unwanted outsiders from joining.

As awareness and fear of law enforcement takedown activities increase in the cybercriminal underground community, more threat actors are choosing to use seemingly secure IM platforms to circumvent detection algorithms and lock out would-be infiltrators. IM services like WhatsApp, Telegram, Skype, and WeChat are a major concern for global governments, given their hundreds of millions of users, end-to-end encryption, and the potential malicious activity that can find safe harbor behind their walls.

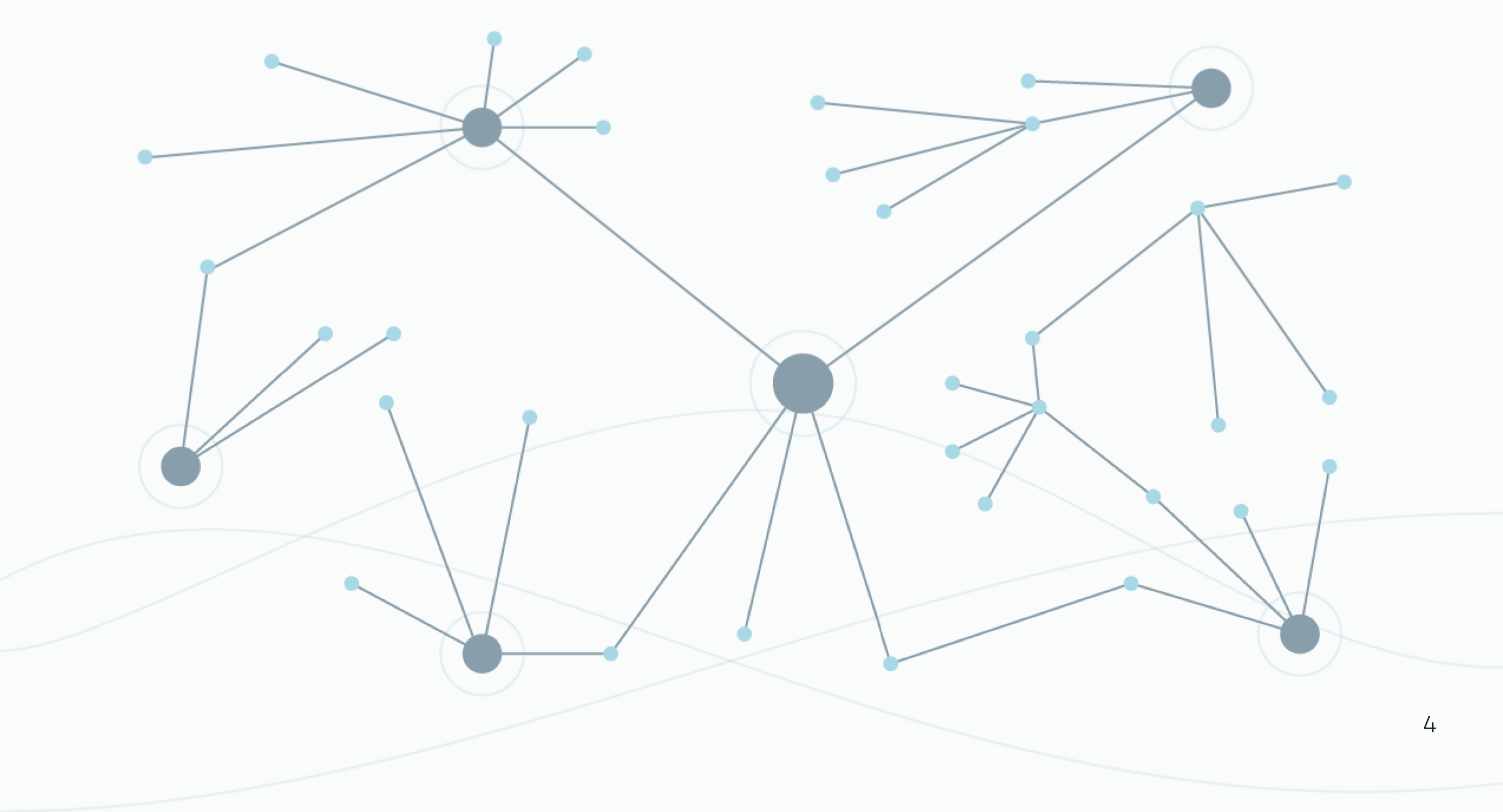
Decentralized Messenger Protocols

Some IM platforms offer decentralized protocols, with which users can create their own servers. This allows cybercriminals to create private networks with full ownership, further avoiding outside interference. The most well-known and widely used decentralized messenger protocol is XMPP (Extensible Messaging and Presence Protocol), formerly known as Jabber.

XMPP is open source, end-to-end encrypted, and can be easily leveraged by any ordinary user. Threat actors can open servers and run them as they see fit, which is immensely attractive to criminals trying to avoid the attention of law enforcement agencies, corporate threat hunters, and other white hat hackers. One of the most secure methods threat actors use and recommend to avoid detection is the combination of Off-the-Record (OTR) messaging protocols with a XMPP client over the TOR network.

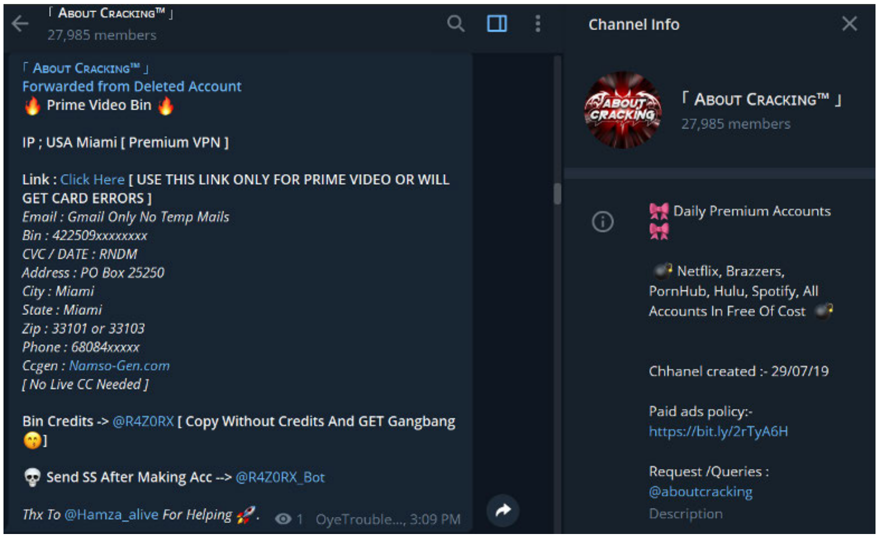
A prominent example is the XMPP server of the notorious cybercrime forum Exploit.In, which offers verified and trusted forum users a reliable chat service with strong privacy measures in place.

In addition to XMPP, we see an ever-growing number of mentions regarding "new" secured IM apps, such as Signal, Wickr, and Silent Phone. Each of these platforms is open source, carries end-to-end encryption, and claims it will not save any information on the IM Server side.



Most Popular Instant Messaging Platforms

Based on the data we scraped, Telegram appears to be the most popular IM platform for cybercriminals during the past year. We found nearly 57,000 Telegram invite links shared across cybercrime forums, with well over 200,000 general mentions of the app across these forums. Moreover, Telegram is the most widespread platform, mentioned most in many different regions and areas of interest.



「 About Cracking™ 」
Forwarded from Deleted Account
🔥 Prime Video Bin 🔥

IP ; USA Miami [Premium VPN]

Link : Click Here [USE THIS LINK ONLY FOR PRIME VIDEO OR WILL GET CARD ERRORS]
Email : Gmail Only No Temp Mails
Bin : 422509xxxxxxxx
CVC / DATE : RNDM
Address : PO Box 25250
City : Miami
State : Miami
Zip : 33101 or 33103
Phone : 68084xxxxx
Ccgen : Namso-Gen.com
[No Live CC Needed]

Bin Credits -> @R4Z0RX [Copy Without Credits And GET Gangbang 😗]

💀 Send SS After Making Acc --> @R4Z0RX_Bot

Thx To @Hamza_alive For Helping 🚀. 1 OyeTrouble..., 3:09 PM

「 About Cracking™ 」
27,985 members

🎀 Daily Premium Accounts 🎀

💣 Netflix, Brazzers, PornHub, Hulu, Spotify, All Accounts In Free Of Cost 💣

Chhanel created :- 29/07/19

Paid ads policy:-
https://bit.ly/2rTyA6H

Request /Queries :
@aboutcracking
Description

Example of a major carding Telegram group offering automation abilities

Discord, which has emerged as the go-to IM and chat platform for gamers, also appears to be gaining popularity among cybercriminals. It ranked second, according to our data in growth among chatter in cybercriminal forums.

The third most-used platform, ICQ, is an older service that remains very active. Our data included 3,500 invite links to ICQ chat groups and 132,000 general mentions in cybercrime forums over the past year.

The IM landscape includes platforms with one or multiple protocols, chat, and file capabilities and features, all of which can be used for different purposes. Here is a comparison of some major IM platform monthly active user counts and capabilities:

IM Platform	Monthly Active users	General Term in scrapes	Registration requirement	Peer-To-Peer Text chat?	Open Source Servers?	Enable FTP?	Read receipts?	Deleting Sent messages?	End-To-End Encryption - protocols?
ICQ	11 Million (2018)	983,398 Results	Phone number	X	X	V	V	X	No
Telegram	400 million (2020)	14,414,975 Results	Phone number	X	X	V	V	V	MTProto - Yes
WhatsApp	2 billion (2020)	305,673 Results	Phone number	X	X	V	V	Partial	Signal Protocol - Yes
Discord	250 million (2019)	1,159,381 Results	Email	X	X	V	X	V	VoIP - No
Wechat	1.1 billion (2019)	26,580 Results	Phone number/QQ number	X	X	V	X	-	No
Tencent QQ	823 million (2019)	168,934 Results	-	X	X	V	X	-	No
Viber	260 million (2019)	65,992 Results	Phone number	X	X	V	V	V	No
Slack	10 Million and 85,000 Paid organizations	147,359 Results	Email	X	X	V	X	-	No
Skype	300 million (2018)	697,471 Results	Email	X	X	V	X	-	No
Jabber (Pidgin client)	-	15,476,337 Results	-	V	V	V	X	X	XMPP - Yes
Vipole	-	13,743,989 Results	-	X	X	-	-	-	-
Signal	-	-	Phone number	X	V	V	V	Partial	Signal Protocol - Yes

IM applications are most often used by financial fraud communities. Financial threat actors and fraudsters exchange stolen carding information, selling or trading all kinds of credit card dumps, and publishing methods or techniques relevant for the fraud community. In addition, there is also trade of physical items stolen or counterfeited from organizations in the retail industry.

Although IM platforms are growing in popularity among threat actors, they have various limitations when compared to dark web forums and black markets. In addition to security issues that are unique to IM applications and some of the intrinsic advantages of posting in anonymized forums, there are many reasons for threat actors to pair their IM and forum use.

Lingering Security Concerns for Threat Actors

Despite the encryption capabilities and private nature of IM services, there are some existing security issues inherent to the platforms. Instant messaging is based on client-server architecture in which clients (like desktop computers/mobiles devices) communicate with an IM server. The IM server then reroutes the message to the intended recipient. The core features and advantages these platforms provide are peer-to-peer, real-time chatting, encryption, and file transfer capabilities.

However, law enforcement can “break” encryption using **sophisticated algorithms and security vulnerabilities**, or by collecting frame details and digital clues that were stored in the IM servers. While the data itself is fully encrypted and law enforcement needs sophisticated algorithms in order to decrypt it, some countries have authorized law enforcement agencies to access the private information of their citizens if sanctioned by courts or other judicial authorities – including information that lives in IM platforms. Threat actors are worried about the **cooperation between technology companies and law enforcement agencies**, especially in the United States.

Advantages of Traditional Cybercrime Forums

Entrenched Popularity

Despite the rapid increase in IM use among threat actors, it is likely that well-established forums and black markets across the clear, deep, and dark web will remain the primary sources for hacker activity. Cybercrime forums tend to have long histories and respected pedigrees within the community, so they generally serve as entry points for hackers looking to get into the game and as linchpins for longer-tenured users. In addition, cybercriminals build up their reputations over years of using these forums, which instills a certain level of trust for more veteran and prominent users. Threat actors can view sellers’ post histories and reputation ratings, allowing them to assess their credibility before making a purchase. The payment and escrow processes in many forums also increase confidence in the legitimacy of a given transaction.

Advertising Features

While users have more control over their ads on IM platforms, the traditional black markets and forums have some advantages. For example, forum posts are more detailed and can reach many additional users with a single post. On the other hand, IM platform chat functions can cause messages to disappear instantly, due to the fast-paced and continuous nature of the conversation. Only group administrators can create pinned messages, unlike many forums where such privileges exist for ordinary users.

Anonymity

The Tor browser, the most commonly used dark web browser, automatically ensures anonymity by randomly directing all traffic through a network of servers. This is something that cannot be said of IM platforms, despite their encryption capabilities. Almost all IM services require some form of authentication to create an account, such as a phone number or email address, which could, in theory, give authorities a trace back to the user. Threat actors on dark web forums and black markets can instigate transactions without divulging contact information.

Evolving Communication in the Cybercriminal Ecosystem

The underground ecosystem is complex, and there is no one standard method for the flow of communication between threat actors. Many prominent cybercriminals use a combination of anonymous dark web forums and black markets coupled with more accessible and customizable IT protocols to operate at maximum efficiency. Threat actors use each feature the various platforms offer to achieve different goals.

Using our extensive observations and data scraping, we can assess the trends in threat actor communication and project how communication flow will evolve in the underground. For example, it is clear that the majority of threat actors initially publish their goods in cybercrime forums and include their IM contact information for interested parties. Forums and black markets have a substantially larger audience, but sellers can use customized IM protocols to ensure privacy and security when completing a transaction. IM platforms also offer cybercriminals the ability to engage in active, real-time conversations to facilitate faster deals.

The Top Reasons Cybercriminals Use Instant Messaging

While instant messaging has been around for decades, the recent surge in use throughout the cybercriminal underground is indicative of a trend worth following. We concluded that threat actors are primarily using IM platforms for the following reasons:

- **Threat actors are using the instant messaging platform as an alternative black marketplace.** They are selling, buying, and exchanging criminal goods, such as account login credentials, website configurations, and tools and methods.
- **Threat actors are using forums as a marketing and sales tool.** They still often connect with buyers from known forums but usually seal the deal in chat services. This is done in order to leverage the encryption that IM platforms offer and slip under the radar of law enforcement authorities.
- **Threat actors are taking advantage of enhanced IM features.** Capabilities like automated processes and chatbots make IM platforms a viable alternative where cybercriminals can interact instantaneously, rather than waiting on delayed forum responses.
- **Threat actors are using instant messaging chat channels as an instant information hub.** Users share news, spread details surrounding new vulnerabilities or exploits, and cite new white papers or research from the cyber community. Threat actors leverage the real-time communication to inform each other of any fresh cyber landscape news that could impact their future efforts.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.