



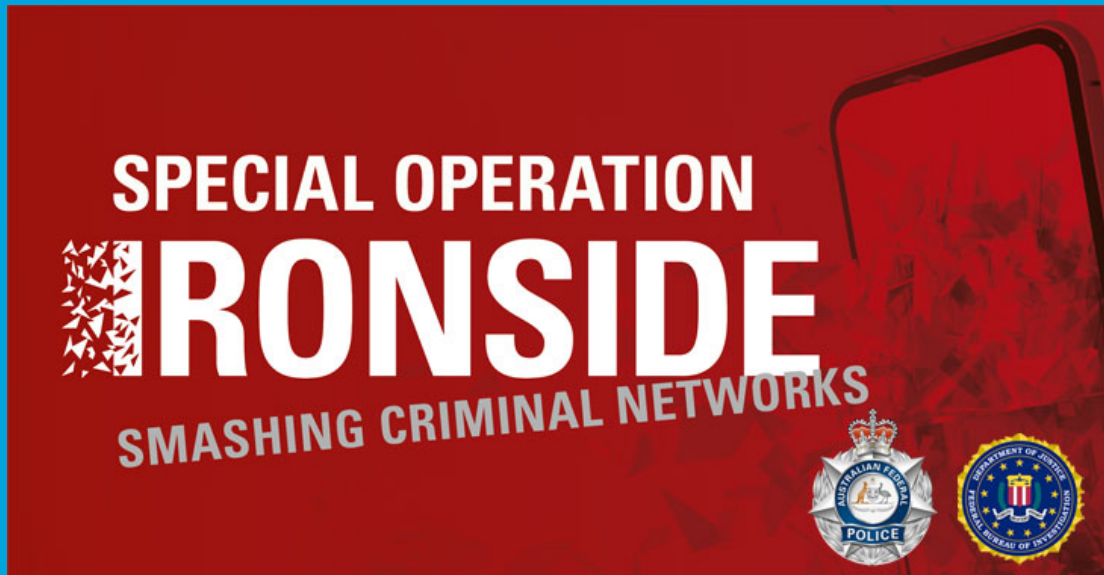
---

## Security Newsletter

14 Jun 2021

[Subscribe to this newsletter](#)

# Trojan Shield: How the FBI Secretly Ran a Phone Network for Criminals



For years the FBI has secretly run an encrypted communications app used by organized crime in order to surreptitiously collect its users' messages and monitor criminals' activity on a massive scale, according to a newly unsealed court document. In all, the elaborate operation netted more than 20 million messages from over 11,800 devices used by suspected criminals.

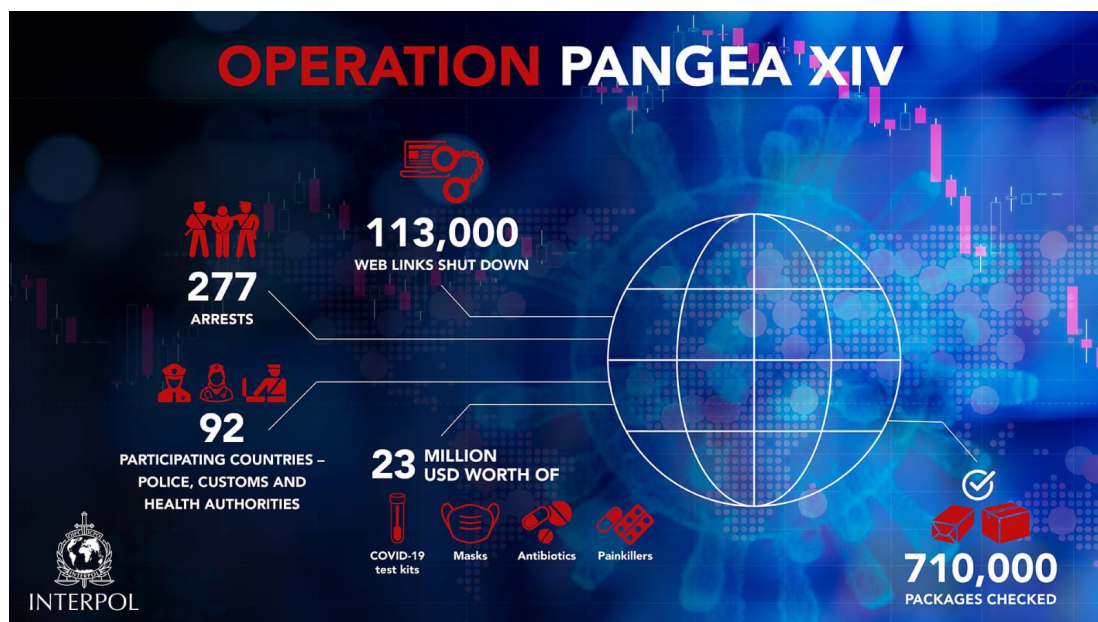
The news signals a major coup for law enforcement: ordinarily, agencies either shut down or crack messages on an already established service, such as Phantom Secure or Encrochat, two similar encrypted messaging networks.

But in this case, the FBI took control of a communications company called Anom in its infancy and turned that into a wide-reaching honeypot, with the suspected criminal users instead coming to them.

[Read More on Vice](#)

[Even More in Europol's press release](#)

## Interpol shuts down thousands of fake online pharmacies



The Interpol (International Criminal Police Organisation) has taken down thousands of online marketplaces that posed as pharmacies and pushed dangerous fake and illicit drugs and medicine.

This record number of illicit online pharmacies was shut down during Operation Pangea XIV, which targeted online sellers of counterfeit and illegal pharmaceuticals and medical devices.

Law enforcement agencies, customs, and health regulatory authorities from 92 countries coordinated by Interpol took down "113,020 web links including websites and online marketplaces being closed down or removed."

[Read More on BleepingComputer](#)

[Even More in Interpol's press release](#)

## More #News

- [How Hackers Used Slack to Break into EA Games](#)
- [U.S. Authorities Shut Down Slilpp—Largest Marketplace for Stolen Logins](#)
- [Top 10 Privacy and Security Features Apple Announced at WWDC 2021](#)
- [Avaddon ransomware shuts down and releases decryption keys](#)
- [Network security firm COO charged with medical center cyberattack](#)
- [Summary of June 8 Fastly outage](#)
- [Hacked drones and busted logistics are the cyber future of warfare](#)

- Hacked drones and busted logistics are the cyber future of warfare

## #Breach Log

- [Beef Supplier JBS Paid Hackers \\$11 Million Ransom After Cyberattack](#)
- [Crypto-Mining Attacks Targeting Kubernetes Clusters via Kubeflow Instances](#)
- [US truck and military vehicle maker Navistar discloses data breach](#)
- [US recovers most of Colonial Pipeline's \\$4.4M ransomware payment](#)
- [Audi, Volkswagen data breach affects 3.3 million customers](#)
- [McDonald's discloses data breach after theft of customer, employee info](#)
- [Foodservice supplier Edward Don hit by a ransomware attack](#)
- [CD Projekt: Data stolen in ransomware attack now circulating online](#)
- [Hackers breach gaming giant Electronic Arts, steal game source code](#)
- [Spain's Ministry of Labor and Social Economy hit by cyberattack](#)

## #Patch Time!

- [Hackers Can Exploit Samsung Pre-Installed Apps to Spy On Users](#)
- [7-Year-Old Polkit Flaw Lets Unprivileged Linux Users Gain Root Access](#)
- [New Chrome 0-Day Bug Under Active Attacks](#)
- [Intel fixes 73 vulnerabilities in June 2021 Platform Update](#)
- [Microsoft June 2021 Patch Tuesday fixes 6 exploited zero-days, 50 flaws](#)
- [Adobe issues security updates for 41 vulnerabilities in 10 products](#)
- [New UAF Vulnerability Affecting Microsoft Office](#)
- [Computer memory maker ADATA hit by Ragnar Locker ransomware](#)

## #Tech and #Tools

- [Codecov ditches Bash Uploader for a NodeJS executable](#)
- [GitHub now scans for accidentally-exposed PyPI, RubyGems secrets](#)
- [ALPACA: Application Layer Protocol Confusion](#)
- [The Walls Have Ears - Compromising a Conference Table Microphone](#)
- [Impacket Release v0.9.23](#)
- [Pop-Ups in a good-world](#)
- [Microsoft warns of cryptomining attacks on Kubernetes clusters](#)
- [Researchers Discover First Known Malware Targeting Windows Containers](#)
- [Two weeks of securing Samsung devices: Part 1](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

## Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on [www.kindredgroup.com](http://www.kindredgroup.com).

You can access the previous newsletters at <https://news.infosecgur.us>