DOJ hiring new liaison prosecutor to hunt cybercriminals in Eastern Europe

therecord.media/doj-hiring-new-liaison-prosecutor-to-hunt-cybercriminals-in-eastern-europe/

May 2, 2021

The Justice Department is hiring a new Liaison Prosecutor to work with authorities in Eastern Europe to combat the rising wave of organized cybercrime activity, The Record has learned.

The new Liaison Prosecutor will be delegated with Eurojust, an European Union agency that coordinates judicial cooperation and joint investigations.

Under this role, the Liaison Prosecutor will have the following responsibilities:

1. Train and develop skills for prosecutors, police, and judges, including through case-based mentoring on transnational organized cybercrime cases;
2. Identify gaps in existing laws, advise legislative bodies on the enactment of effective legislation and amendment of existing laws to increase enforcement efficacy;
3. build capacity within the law enforcement agencies to combat transnational organized cybercrime.

The role is not new. The selected attorney will replace Richard D. Green, who previously served as the DOJ's Transnational Organized Cybercrime Liaison Prosecutor for Eastern Europe between December 2018 and December 2020.

The move to hire a new Eastern Europe Liaison Prosecutor also came on the same day the DOJ said it would soon begin a 120-day review of cybersecurity challenges.

DOJ Deputy Attorney General Lisa Monaco said during the Munich Cyber Security Conference that the Justice Department would work to analyze the biggest cybersecurity threats the US is facing today, and the tools prosecutors have at their disposal to go after threat actors, and then make changes to adapt to the current threat landscape.

The Friday announcements also come after three days earlier, the DOJ, together with private sector partners, submitted an 80-page report to the Biden administration with a long series of aggressive measures aimed at curbing ransomware attacks and going after ransomware groups.

Prioritizing the prosecution of ransomware groups was one of the report's main recommendations.

The soon-to-be-hired Eastern Europe Liaison Prosecutor will play a big role in the DOJ's future plans since many of today's cybercrime groups, and especially ransomware gangs, are suspected to be operating out of Eastern European countries.

GOAL #1:	**Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy**
Objective 1.1:	**Signal that ransomware is an international diplomatic and enforcement priority**
Action 1.1.1:	*Issue declarative policy through coordinated international diplomatic declarations that ransomware is an enforcement priority*
Action 1.1.2:	*Establish an international coalition to combat ransomware criminals*
Action 1.1.3:	*Create a global network of ransomware investigation hubs*
Action 1.1.4:	*Convey the international priority of collective action on ransomware via sustained communications by national-leaders*
Objective 1.2:	**Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House**
Action 1.2.1:	*Establish an Interagency Working Group for ransomware*
Action 1.2.2:	*Establish an operationally focused U.S. Government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub*
Action 1.2.3:	*Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign*
Action 1.2.4:	*Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public*
Action 1.2.5:	*Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat*
Action 1.2.6:	*Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns*
Objective 1.3:	**Substantially reduce safe havens where ransomware actors currently operate with impunity**
Action 1.3.1:	*Exert pressure on nations that are complicit or refuse to take action*
Action 1.3.2:	*Incentivize cooperation and proactive action in resource-constrained countries*

Action 1.3.2:	*Incentivize cooperation and proactive action in resource-constrained countries*

GOAL #2:	**Disrupt the ransomware business model and decrease criminal profits**
Objective 2.1:	**Disrupt the system that facilitates the payment of ransoms**
Action 2.1.1:	*Develop new levers for voluntary sharing of cryptocurrency payment indicators*
Action 2.1.2:	*Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws*
Action 2.1.3:	*Incentivize voluntary information sharing between cryptocurrency entities and law enforcement*
Action 2.1.4:	*Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes*
Action 2.1.5:	*Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation*
Action 2.1.6:	*Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs*
Action 2.1.7:	*Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management*
Objective 2.2:	**Target the infrastructure used by ransomware criminals**
Action 2.2.1:	*Leverage the global network of ransomware investigation hubs*
Action 2.2.2:	*Clarify lawful defensive measures that private-sector actors can take when countering ransomware*
Objective 2.3:	**Disrupt the threat actors, including ransomware developers, criminal affiliates, and ransomware variants**
Action 2.3.1:	*Increase government sharing of ransomware intelligence*
Action 2.3.2:	*Create target decks of ransomware developers, criminal affiliates, and ransomware variants*
Action 2.3.3:	*Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure*

Tags

- cybercrime
- DOJ
- Eastern Europe
- job
- Justice Department
- liaison prosecutor
- Ransomware
- Russia

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.