Operation Lyrebird: Group-IB assists INTERPOL in identifying suspect behind numerous cybercrimes worldwide

group-ib.com/media/gib-interpol-lyrebird/

Group-IB, one of the leading providers of solutions dedicated to detecting and preventing cyberattacks, identifying online fraud, investigation of high-tech crimes and intellectual property protection, has supported INTERPOL in its Lyrebird operation that resulted in the identification and apprehension of a threat actor presumably responsible for multiple attacks, including on French telecommunications companies, the county's major banks and multinational corporations, following a two-year investigation. The alleged perpetrator, who turned out to be a citizen of Morocco, was arrested in May by the Moroccan police based on the data about his cybercrimes that was provided by Group-IB.

According to Group-IB's Threat Intelligence team, the suspect, dubbed Dr HeX by Group-IB based on one of the nicknames that he used, has been active since at least 2009 and is responsible for a number of cybercrimes, including phishing, defacing, malware development, fraud, and carding that resulted in thousands of unsuspecting victims. The starting point of Group-IB's research to identify and deanonymize the cybercriminal was the extraction of a phishing kit (a tool used to create phishing web pages) exploiting the brand of a large French bank by Group-IB's Threat Intelligence & Attribution system.

The set-up of the detected phishing kit followed a common technique, with the creation of a spoofed website of a targeted company, the mass distribution of emails impersonating it and asking users to enter login information on the spoofed site. The credentials left by unsuspecting victims on the fake page were then redirected to the perpetrator's email. Almost each of the scripts contained in the phishing kit had its creator's nickname, Dr HeX, and contact email address.

The email mentioned in the phishing kit enabled Group-IB threat intelligence analysts find the alleged attacker's YouTube channel signed up under the same name — Dr HeX. In the description to one of the videos, the attacker left a link leading to an Arabic crowd funding platform, which enabled Group-IB researchers to record another name associated with the cybercriminal. According to the DNS data analysis, this name was used to register at least two domains, which were created using the email from the phishing kit.

Using its patented graph network analysis technology, Group-IB researchers built a network graph, based on the email address from the phishing kit, that showed other elements of the threat actor's malicious infrastructure employed by him in various campaigns along with his personal pages. A total of five email addresses associated with the accused were identified, along with six nicknames, and his accounts on Skype, Facebook, Instagram, and Youtube.

The further analysis of Dr Hex' digital footprint revealed his association with other malicious activities. Over the period from 2009 to 2018, the threat actor defaced over 130 web pages. Group-IB analysts have also found the cybercriminal's posts on several popular underground platforms intended for malware trading that indicate the latter's involvement in malware development. In addition, Group-IB has also discovered evidence suggesting Dr Hex' involvement in attacks on several huge French corporations with the aim of stealing customer's bank card data.

Under Operation Lyrebird, Group-IB worked closely with INTERPOL's Cybercrime Directorate, which, in turn, cooperated with Moroccan Police via the INTERPOL National Central Bureau in Rabat to eventually locate and apprehend the individual who remains under investigation.

This is a significant success against a suspect who is accused of targeting unsuspecting individuals and companies across multiple regions for years, and the case highlights the threat posed by cybercrime worldwide. The arrest of this suspect is down to outstanding international investigative work and new ways of collaboration both with Moroccan police and our vital private sector partners such as Group-IB.

Stephen Kavanagh

INTERPOL Executive Director of Police Services

Having zero-tolerance to cybercrime, Group-IB has always stressed its focus not only on protecting our customers against cyberattacks, but also on identifying perpetrators behind them to ensure that they're duly punished. Lyrebird operation is yet another example of strong coordinated cooperation between international law enforcement agencies, regional police and cybersecurity players. These are international cooperation, data exchange, and the long-standing experience in cyber investigations that help Group-IB lead its work to a logical conclusion — bring cybercriminals to justice. Over years of successful cooperation between INTERPOL and Group-IB, we have been setting an example of synergy between the private sector and police forces that ensures that cybercrime isn't exempt from punishment.

Dmitry Volkov

Group-IB CTO and Head of Threat Hunting Intelligence