Europol coordinates global action against criminal abuse of Cobalt Strike

By Europol

Published: 2024-07-03 · Archived: 2026-04-05 13:58:08 UTC

Law enforcement has teamed up with the private sector to fight against the abuse of a legitimate security tool by criminals who were using it to infiltrate victims' IT systems. Older, unlicensed versions of the Cobalt Strike red teaming tool were targeted during a week of action coordinated from Europol's headquarters between 24 and 28 June.

Throughout the week, law enforcement flagged known IP addresses associated with criminal activity, along with a range of domain names used by criminal groups, for online service providers to disable unlicensed versions of the tool. A total of 690 IP addresses were flagged to online service providers in 27 countries. By the end of the week, 593 of these addresses had been taken down.

Known as Operation MORPHEUS, this investigation was led by the UK National Crime Agency and involved law enforcement authorities from Australia, Canada, Germany, the Netherlands, Poland and the United States. Europol coordinated the international activity, and liaised with the private partners. This disruptive action marks the culmination of a complex investigation initiated in 2021.

Abuse by cybercriminals

Cobalt Strike is a popular commercial tool provided by the cybersecurity software company Fortra. It is designed to help legitimate IT security experts perform attack simulations that identify weaknesses in security operations and incident responses. In the wrong hands, however, unlicensed copies of Cobalt Strike can provide a malicious actor with a wide range of attack capabilities.

Fortra has taken significant steps to prevent the abuse of its software and has partnered with law enforcement throughout this investigation to protect the legitimate use of its tools. However, in rare circumstances, criminals have stolen older versions of Cobalt Strike, creating cracked copies to gain backdoor access to machines and deploy malware. Such unlicensed versions of the tool have been connected to multiple malware and ransomware investigations, including those into RYUK, Trickbot and Conti.

Cooperation with the private sector

Cooperation with the private sector was instrumental in the success of this disruptive action. A number of private industry partners supported the action, including BAE Systems Digital Intelligence, Trellix, Spamhaus, abuse.ch and The Shadowserver Foundation. These partners deployed enhanced scanning, telemetry and analytical capabilities to help identify malicious activities and use by cybercriminals.

This novel approach is possible thanks to Europol's amended Regulation which has strengthened the Agency's capacity to better support EU Member States, including by collaborating with the private sector. Through this novel approach, Europol can gain access to real-time threat intelligence and a broader perspective on cybercriminal tactics. This partnership enables a more coordinated and comprehensive response, ultimately enhancing the overall resilience of the digital ecosystem across Europe.

Europol support

Europol's European Cybercrime Centre (EC3) has been supporting this case since September 2021 by providing analytical and forensic support, and facilitating the information exchange between all the partners.

Law enforcement used a platform, known as the Malware Information Sharing Platform, to allow the private sector to share real-time threat intelligence with law enforcement. Over the span of the whole investigation, over 730 pieces of threat intelligence were shared containing almost 1.2 million indicators of compromise.

In addition, Europol's EC3 organised over 40 coordination meetings between the law enforcement agencies and the private partners. During the week of action, Europol set up a virtual command post to coordinate law enforcement action across the globe.

The disruption does not end here. Law enforcement will continue to monitor and carry out similar actions as long as criminals keep abusing older versions of the tool.

The following authorities were part of the investigation:

- **Australia:** Australian Federal Police (AFP)
- **Canada:** Royal Canadian Mounted Police (RCMP)
- **Germany:** Federal Criminal Police Office (Bundeskriminalamt)
- **The Netherlands:** National Police (Politie)
- **Poland:** Polish Central Cybercrime Bureau (Centralne Biuro Zwalczania Cyberprzestępczości)
- **United Kingdom:** National Crime Agency (NCA)
- **United States:** U.S. Department of Justice, Federal Bureau of Investigation (FBI)

Authorities in the following countries supported the disruption activity:

- Bulgaria
- Estonia
- Finland
- Lithuania
- Japan
- South Korea