‘Avalanche’ network dismantled in international cyber operation

By Europol

Published: 2016-12-01 · Archived: 2026-04-05 21:46:47 UTC

On 30 November 2016, after more than four years of investigation, the Public Prosecutor’s Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney’s Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners, dismantled an international criminal infrastructure platform known as ‘Avalanche’.

The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform.
The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries. As a result, 5 individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries. Also, 221 servers were put offline through abuse notifications sent to the hosting providers. The operation marks the largest-ever use of sinkholing[1] to combat botnet[2] infrastructures and is unprecedented in its scale, with over 800 000 domains seized, sinkholed or blocked.

On the action day, Europol hosted a command post at its headquarters in The Hague. From there, representatives of the involved countries worked together with Europol’s European Cybercrime Centre (EC3) and Eurojust officials to ensure the success of such a large-scale operation.

In addition Europol supported the German authorities throughout the entire investigation by assisting with the identification of the suspects and the exchange of information with other law enforcement authorities. Europol’s cybercrime experts produced and delivered analytical products.

Eurojust’s Seconded National Expert for Cybercrime assisted by clarifying difficult legal issues that arose during the course of the investigation. Several operational and coordination meetings were also held at both Europol and Eurojust.

Julian King, European Commissioner for the Security Union, said: "Avalanche shows that we can only be successful in combating cybercrime when we work closely together, across sectors and across borders. Cybersecurity and law enforcement authorities need to work hand in hand with the private sector to tackle continuously evolving criminal methods. The EU helps by ensuring that the right legal frameworks are in place to enable such cooperation on a daily basis".

Rob Wainwright, Europol Director, said: “Avalanche has been a highly significant operation involving international law enforcement, prosecutors and industry resources to tackle the global nature of cybercrime. The complex trans-national nature of cyber investigations requires international cooperation between public and private organisations at an unprecedented level to successfully impact on top-level cybercriminals. Avalanche has shown that through this cooperation we can collectively make the internet a safer place for our businesses and citizens”.

Michèle Coninsx, President of Eurojust, said: “Today marks a significant moment in the fight against serious organised cybercrime, and exemplifies the practical and strategic importance of Eurojust in fostering international cooperation. Together with the German and US authorities, our EU and international partners, and with support from Eurojust and EC3, Avalanche, one of the world’s largest and most malicious botnet infrastructures, has been decisively neutralised in one of the biggest takedowns to date.”

The criminal groups have been using the Avalanche infrastructure since 2009 for conducting malware, phishing and spam activities. They sent more than 1 million e-mails with damaging attachments or links every week to unsuspecting victims.

The investigations commenced in 2012 in Germany, after an encryption ransomware[3] (the so-called Windows Encryption Trojan), infected a substantial number of computer systems, blocking users’ access. Millions of private and business computer systems were also infected with malware, enabling the criminals operating the network to harvest bank and e-mail passwords.

With this information, the criminals were able to perform bank transfers from the victims’ accounts. The proceeds were then redirected to the criminals through a similar double fast flux[4]infrastructure, which was specifically created to secure the proceeds of the criminal activity.

The loss of some of the network’s components was avoided with the help of its sophisticated infrastructure, by redistributing the tasks of disrupted components to still-active computer servers. The Avalanche network was estimated to involve as many as 500,000 infected computers worldwide on a daily basis.

What made the ’Avalanche’ infrastructure special was the use of the so-called double fast flux technique. The complex setup of the Avalanche network was popular amongst cybercriminals, because of the double fast flux technique offering enhanced resilience to takedowns and law enforcement action.

Malware campaigns that were distributed through this network include around 20 different malware families such as goznym, marcher, matsnu, urlzone, xswkit, and pandabanker. The money mule schemes operating over Avalanche involved highly organised networks of “mules” that purchased goods with stolen funds, enabling cyber-criminals to launder the money they acquired through the malware attacks or other illegal means.

In preparation for this joint action, the German Federal Office for Information Security (BSI) and the Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) analysed over 130 TB of captured data and identified the server structure of the botnet, allowing for the shut-down of thousands of servers and, effectively, the collapse of the entire criminal network.

The successful takedown of this server infrastructure was supported by INTERPOL, the Shadowserver Foundation, Registrar of Last Resort, ICANN and domain registries involved in the takedown phase. INTERPOL has also facilitated the cooperation with domain registries. Several antivirus partners provided support concerning victim remediation.

Figures at a glance

Countries involved: Armenia, Australia, Austria, Azerbaijan, Belgium, Belize, Bulgaria, Canada, Colombia, Finland, France, Germany, Gibraltar, Hungary, India, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Norway, Poland, Romania, Singapore, Sweden, Taiwan, Ukraine, United Kingdom and United States of America.

Arrests: **5**
Searches conducted: **37**
Servers seized: **39**
Servers taken offline through abuse notifications: **221**

Computer users should note that this law enforcement action will NOT clean malware off any infected computers – it will merely deny the Avalanche users' ability to communicate with infected victims' computers. Avalanche victims' computers will still be infected, but shielded from criminal control.

Victims of malware operating over the Avalanche network may use the following webpages created for assistance in removing the malware:

- www.bsi-fuer-buerger.de/botnetz and www.bsi-fuer-buerger.de/avalanche, in German;
- www.bsi-fuer-buerger.de/EN/botnetz and www.bsi-fuer-buerger.de/EN/avalanche, in English;
- https://us-cert.gov/avalanche;
- www.nationalcrimeagency.gov.uk/news/962-avalanche-takedown;
- www.getsafeonline.org/news/avalanche;
- www.actionfraud.police.uk/news-police-takedown-computer-network-used-to-infect-millions-of-devices-dec16;
- www.cyberaware.gov.uk/blog

The Shadowserver Foundation have supported this operation and will be making the sinkhole data available globally to responsible bodies via their free daily remediation feeds. More information can be found in their blog article.

[1] **Sinkholing** is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses. When employed at a 100% scale, infected computers can no longer reach the criminal command and control computer systems and so criminals can no longer control the infected computers. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.

[2] **Botnets** are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

[3] **Ransomware** is a type of malware that infects the victim's PC and encrypts the victim's files, so that the victim is unable to access them. The criminal behind the ransomware then uses intimidation and misinformation to force the victim to pay a sum of money in exchange for the password that unlocks the encrypted files. Even if a password is eventually provided, it does not always work.

[4] **Fast flux** technique is an evasion technique used by botnet operators to quickly move a fully qualified domain name (a domain that points to one specific Internet resource such as www. domain .com) from one or more computers connected to the Internet to a different set of computers. Its aim is to delay or evade the detection of criminal infrastructure. In the double fast flux setup, both the domain location and the name server queried for this location are changed.
