A form of cybercrime, high-tech crime refers to crimes that use electronic and digitally based technology to attack computers or a computer network.

Such crimes include the hacking of computers or any unauthorised use or distribution of data, denial of service attacks and distribution of computer viruses.

High-tech criminals use a suite of malware tools, ranging from banking trojans to ransomware and phishing, to stage their attacks.

Malware, or malicious software, infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware, and they can complement each other when performing an attack.

- Adware displays advertising banners or pop-ups that include code to track the user’s behaviour on the internet.
- A backdoor/remote-access trojan (RAT) accesses a computer system or mobile device remotely. It can be installed by another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions, including:
    - monitoring actions
    - executing commands
    - sending files and documents back to the attacker
    - logging keystrokes
    - taking screen shots
- A botnet (short for robot network) is made up of computers communicating with each other over the internet. A command and control centre uses them to send spam, mount distributed denial-of-service (DDoS) attacks and commit other crimes.
- A file infector infects executable files (such as .exe) by overwriting them or inserting infected code that disables them.
- Ransomware stops users from accessing their devices and demands that they pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.
- Scareware is fake anti-virus software that pretends to scan and find malware/security threats on a user’s device so that they will pay to have it removed.
- Spyware is installed on a computer without its owner’s knowledge to monitor their activity and transmit the information to a third party.
- A rootkit is a collection of programmes that enable administrator-level access to a computer or computer network, thus allowing the attacker to gain root or privileged access to the computer and possibly other machines on the same network.
- A trojan poses as, or is embedded within, a legitimate programme, but it is designed for malicious purposes, such as spying, stealing data, deleting files, expanding a botnet, and performing DDoS attacks.
- A worm replicates itself over a computer network and performs malicious actions without guidance.

The flourishing cybercrime-as-a-service business model is continuously providing criminals with access to a large number of cybercrime techniques.

NUMBER OF ITEMS FOUND: 64

SEARCH

TYPE

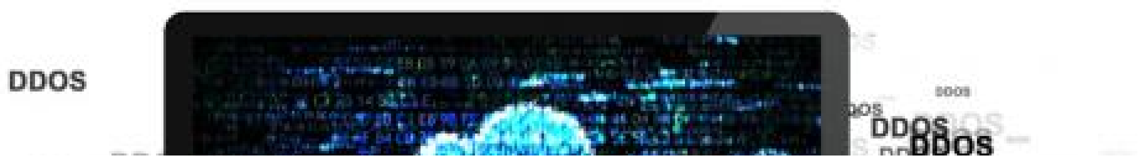
Article/Story, Event, How-To Guide, Landing Page, Multimedia, News/Press Release, Operation, Page, Publication/Document

TARGET GROUP

SEARCH

⊗ CLEAR ALL

12 Dec 2016



JOINT INTERNATIONAL OPERATION TARGETS YOUNG USERS OF DDOS CYBER-ATTACK TOOLS

NEWS/PRESS RELEASE

01 Dec 2016

‘AVALANCHE’ NETWORK DISMANTLED IN INTERNATIONAL CYBER OPERATION

NEWS/PRESS RELEASE

01 Dec 2016

OPERATION AVALANCHE - INFOGRAPHIC - TECHNICAL

PUBLICATION/DOCUMENT

01 Dec 2016

OPERATION AVALANCHE - INFOGRAPHIC

PUBLICATION/DOCUMENT

MOBILE MALWARE

HOW-TO GUIDE

EUROPOL IN BRIEF (ANNUAL REVIEW)

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA)

24 Oct 2016

MOBILE MALWARE INFOGRAPHICS

PUBLICATION/DOCUMENT

27 Sep 2016

THE RELENTLESS GROWTH OF CYBERCRIME

NEWS/PRESS RELEASE

EUROPEAN CYBERCRIME CENTRE - EC3

JOINT INVESTIGATION TEAMS - JITS

30 Sep 2015

3RD EUROPOL-INTERPOL CYBERCRIME CONFERENCE

EVENT

« FIRST ‹ PREVIOUS 1 2 3 4 5 6 NEXT › LAST »

Source URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime?page=3