PC Users Threatened by Conficker Worm and new Internet-browser Modifier

eset.com/int/about/newsroom/press-releases/announcements/press-threatsense-report-july-2009/

05 Aug 2009

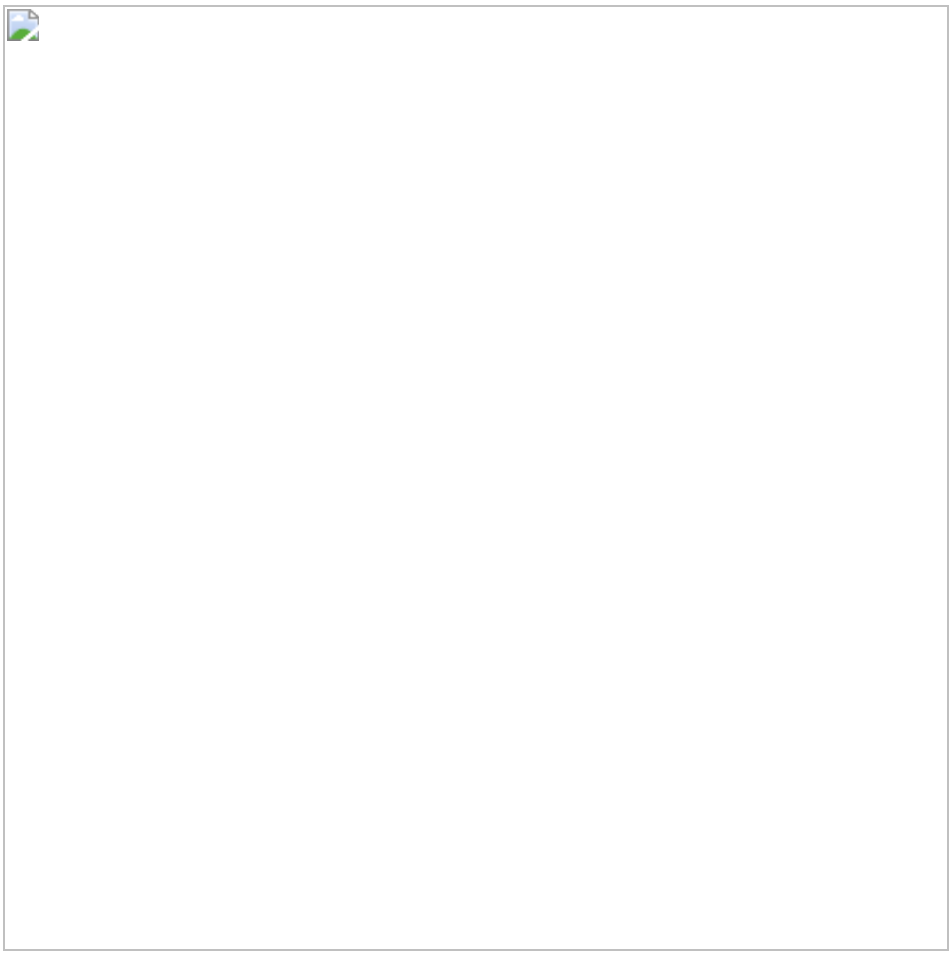
05 Aug 2009

- Conficker most widespread in Eastern Europe
- New Threat, Win32/FlyStudio most widespread in China
- High share of threats exploiting MS Windows autorun.inf function

For the month of July, ESET's statistical threat evaluation system - ThreatSense.Net has evaluated the variant of Win32/Conficker worm as the single most widespread form of malware with a share of 10.67% globally. Other forms of malware still spreading on a mass scale include the types such INF/Autorun , exploiting the MS Windows autorun.inf function. Their share of 8.39% places them second on ESET's threat list. Third place (7.92%) went to a family of Win32/PSW.OnLineGames Trojans and their variants especially targeting online gamers.

Win32/Agent designed to steal information from PCs placed fourth with 2.59%. The newcomer - Win32/FlyStudio closes the top 5 list with 2.38% share of threats detected. The Win32/FlyStudio threat is designed to modify information inside the victim's Internet browser. This threat will modify search queries, with the intention of delivering advertisements to the user. Win32/FlyStudio uses a scripting language popular among malware writers and ranks among the most widespread threats China. USA, Mexico and Argentina are also among countries with high occurrence rates of this type of malware.

Global Threats as tabulated by ESET ThreatSense.Net® (July 2009)



EUROPE, MIDDLE EAST, AFRICA (EMEA)

Conficker remains top threat in Easter Europe, on rise in UK and Italy. For the month of July, Slovakia and the Czech Republic remain among regional exceptions where Win32/TrojanDownloader.Bredolab.AA is the most widespread threat, with a share of 5.89% and 6.48%, respectively. This kind of malware has the capability to copy itself into the system files and executing itself with every boot-up. At the same time, it establishes communication with a remote server via HTTP protocol. In other words, when this trojan horse is in the PC system, its only mission is downloading additional malware – especially adware, spyware or other threats out from different servers and places on the internet.

Also afflicting other European countries, Win32/TrojanDownloader.Bredolab.AA ranks lower to Win32/Conficker that remains top threat in Ukraine (32.55%); Russia (23.02%); Bulgaria and Lithuania (15.43%); Romania (15.4%); South Africa (12.22%); Italy (10.4%); Great Britain (7.97%); Austria (5.31%), and Germany (4.46%).

For the month of July, Poland and France were dominated by a mixture of Trojans of the Win32/PSW.OnLineGames family targeting the virtual identities of online gamers. The share of intercepted infiltrations of this type of threat reached 14.12% in Poland and 11.23% in France.

As far as the region of Northern Europe is concerned, it is dominated by an array of malware grouped under the WMA/TrojanDownloader.GetCodec category. The same applies for the countries of Benelux. These Trojans are engineered to go through all the digital music files, modifying their format in such a way that upon execution, a malicious content is downloaded from a pre-defined web-site. The share of occurrence of this form of malware has reached 4.01% in Sweden, 12.66% in Norway; 12.46% in Estonia and 15.53% in Belgium.

INF/Autorun remains a top threat in the United Arab Emirates (9.55%) and Israel (4.64%).

About ESET

Founded in 1992, ESET is a global provider of security solutions for corporate customers and households. From a small family-sized venture, ESET has evolved into a leader in proactive malware detection and is in the front lines of combating emerging cyberthreats. Its flagship solutions - ESET NOD32 Antivirus and ESET Smart Security, built on the award-winning ThreatSense® engine are trusted by millions of users to protect their computers against a host of Internet-borne malware, such as viruses, trojans, worms, adware, spyware, phishing, rootkits. ESET has headquarters in Bratislava, Slovakia with branch offices in Prague, Czech Republic; San Diego, USA; and Buenos Aires, Argentina. ESET‘s security solutions are available in more than 160 countries worldwide. In 2008, ESET opened its new development center in Krakow, Poland and was ranked by Deloitte Technology Fast 500 as one of the fastest growing technology companies in the EMEA region.

ThreatSense.Net® collects anonymous statistical information packets about the types of infiltrations detected on the users' workstations. Thanks to this information, the ESET Virus Lab has access to real-time accurate and relevant information about the most wide-spread infiltrations. The infiltrations detected by the heuristic analysis are then tabulated, with the update against malware issued before it can spread or mutate into a different variant.