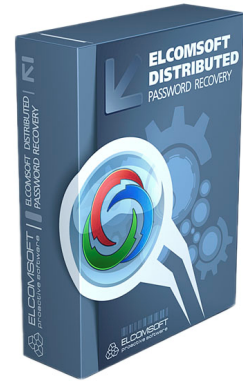


ElcomSoft Updates Distributed Password Recovery with Dictionary Attacks

Moscow, Russia – October 14, 2009 – ElcomSoft Co.Ltd. updates Distributed Password Recovery, a widely scalable password recovery solution with multi-CPU and multi-GPU support, with dictionary attacks and a password cache, making near-instant recovery of strong encryption keys possible. The newly added password cache automatically stores all discovered passwords in order to unlock other documents protected with the same password momentarily. ElcomSoft is committed to providing the best possible forensics tools to help investigate criminal activities. Enhancements to Distributed Password Recovery will help forensics and government authorities to combat crime and prevent criminal and terrorist activities by unlocking up to 40-50 per cent of protected documents in real-time.



Dictionary Attack

The newly added dictionary attack enables the users of Elcomsoft Distributed Password Recovery to quickly unlock encrypted documents and information protected with strong passwords. Dictionary attack can quickly recover the majority of passwords used by general computer users, and up to 40 per cent of passwords employed in corporate environments. By adding the dictionary attack, ElcomSoft greatly reduces time required to unlock information protected with strong encryption algorithms and long, complex passwords.

A brute-force attack on encryption keys can take significant time even with Elcomsoft's patent-pending GPU acceleration; sometimes in the range of weeks or months even on the most powerful workstations.

According to Visa EU Password Selection Survey¹, more than 50 per cent of all passwords used by individual consumers can be broken by using plain dictionary attack, while up to 78 per cent of their passwords can be recovered by adding numbers and suffixes to dictionary words. According to ElcomSoft own experience², up to 40 per cent of passwords used in corporate environments are susceptible to dictionary attacks. With GPU acceleration and zero-overhead scalability available in Elcomsoft Distributed Password Recovery, the time required to recover the majority of passwords with a quick dictionary attack can be greatly reduced.

Password Cache

Despite many corporate security policies strongly advised otherwise, protecting multiple documents and the different types of information with a shared password is common. Elcomsoft Distributed Password Recovery is now able to store all passwords it discovers, forming a separate dictionary that is tried first when recovering the next document. The dictionary of discovered passwords is being used in order to recover other documents and information protected with the same password.

By attacking the weakest link and creating a dictionary of discovered passwords, Elcomsoft Distributed Password Recovery allows users to dramatically decrease time required to recover strong encryption algorithms.

About Elcomsoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery enables accelerated password recovery for Microsoft Office documents, Adobe PDF, PGP disks and archives, personal security certificates and exchange keys, MD5 hashes and Oracle passwords, Windows and UNIX login and domain passwords. With ElcomSoft's patent-pending GPU acceleration technology, supporting multiple CPUs and CPU cores and being able to scale to over 10,000 workstations with zero scalability overhead, Elcomsoft Distributed Password Recovery is a high-end password recovery solution offering the speediest recovery with the most sophisticated commercially available technologies.

Prices for Elcomsoft Distributed Password Recovery start from \$599. For more information about the product and to download an evaluation version of Elcomsoft Distributed Password Recovery, visit ElcomSoft Co. Ltd. at <http://distributed.elcomsoft.com>

About ElcomSoft Co. Ltd.

Established in 1990 in Moscow, Russia, ElcomSoft Co.Ltd. manufactures state-of-the-art computer forensics tools and provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft was serving the needs of businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools and products are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, governments, and all major accounting firms. ElcomSoft and its officers are members of the Russian Cryptology Association. ElcomSoft is a Microsoft Gold Certified Partner and an Intel Software Partner.

[1] Visa EU Password Selection Survey (c) VISA Europe (2004)

[2] ElcomSoft Password Security Survey (2009) <http://survey.elcomsoft.com>