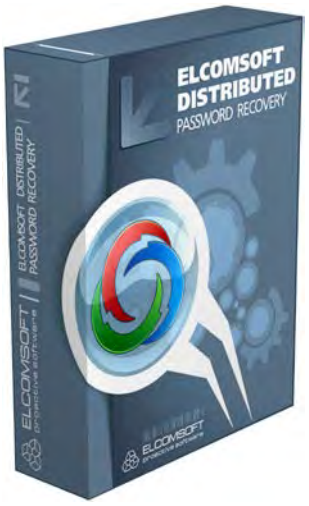
Elcomsoft Distributed Password Recovery Unlocks 1Password, KeePass, LastPass and Dashlane Vaults



Moscow, Russia – August 10, 2017 - ElcomSoft Co. Ltd. updates Distributed Password Recovery, enabling the recovery of master keys protecting encrypted vaults of four popular password managers: 1Password, KeePass, LastPass and Dashlane. By attacking a single master password, experts can gain access to the entire database containing all of the user's saved passwords, authentication credentials and other highly sensitive information. Password managers' protected vaults may contain images of user's documents, various identity-related information, payment and loyalty card numbers.

*"We're continuing our quest on expanding the types of passwords we can break", says **Vladimir Katalov**, ElcomSoft CEO. "This time we are targeting four of the most popular password managers, allowing experts gaining access to protected vaults containing users' authentication credentials, stored logins, passwords and forms to numerous resources. With today's password managers this only requires breaking a single master password."*

One Password to Rule Them All

The idea behind all password management apps is simple: allowing users to securely store, organize and use passwords required to authenticate into various resources. As the user no longer has to remember the many different passwords, the use of password managers effectively cuts password re-use and stimulates the use of strong, unique passwords to protect different resources. Password managers can even automatically generate strong, random passwords that are unique per Web site or resource, rendering both dictionary and brute-force attacks ineffective. These passwords are stored in encrypted vaults, and can be only decrypted once the user enters their master password.

Back in 2012, ElcomSoft has conducted a research of then-popular password keepers. The report https://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf indicated that very few were significantly more secure compared to storing passwords in a plain-text file. In 2017, there quire a few truly secure options, including 1Password, KeePass, LastPass and Dashlane.

All four password managers make use of industry-standard encryption and hashing algorithms to encrypt their password vaults. Each password keeper employs a strong encryption algorithm and several thousand rounds of hashing of the master password to derive the encryption key for the protected vault. In other words, the vault is extremely well protected against brute-force attacks.

Breaking into Encrypted Vaults

Security of the vault containing all of the users' passwords is extremely important; the vault can be only decrypted by brute-forcing the original plain-text master password. However, breaking that one master password would expose the entire vault, enabling access to tens or hundreds passwords that are used to authenticate into various resources.

Password managers use several thousand iterations to derive the binary encryption key from the text-based master password. As a result, the speed of brute force attack is severely limited. This is exactly the reason for employing GPU units available in today's AMD and NVIDIA video cards to accelerate the recovery 50 to 200 times compared to a CPU alone. Even then, the brute force speed is in the range of 100,000 passwords a second, which would only allow brute-forcing reasonably short passwords. Longer and more complex passwords can still be broken with a dictionary attack, by targeting the human factor or using one of the many custom attacks available in Elcomsoft Distributed Password Recovery.

Elcomsoft Distributed Password Recovery 3.40 can use the power of GPU-accelerated attacks distributed over a network of up to 10,000 computers to run a highly efficient attack against the user's master password protecting 1Password, KeePass, LastPass and Dashlane encrypted vaults. Once the master password is recovered, the expert can decrypt the protected vault and access all passwords, authentication credentials and other data stored in the password manager's encrypted database.

New Password Types

The updated release adds the ability to attack master keys used to encrypt protected vaults of the following password managers:

- 1Password
- KeePass
- LastPass
- Dashlane

About Elcomsoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery is a one-stop forensic solution to helping investigators access protected data and extract critical evidence in the shortest timeframe possible. The product enables hardware-accelerated password recovery for over a hundred data formats including 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. Supporting ElcomSoft's patent-pending GPU acceleration technology 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.

Pricing and Availability

Elcomsoft Distributed Password Recovery is available immediately. Licensing starts from 599 EUR for 5 clients. A license for 100 clients is available for 4999 EUR. Other tiers are available on request. Customers are welcome to contact ElcomSoft about larger purchases. Local pricing may vary.

An additional licensing option is now available for smaller networks. The affordable option covers concurrent GPU-accelerated distributive recovery on up to 5 computers. Even this minimal 5-PC license supports up to 8 GPU cores, offering a maximum computational power of 40 GPU cores per license.

Elcomsoft Distributed Password Recovery supports Windows 7, 8.x, 10, as well as the corresponding versions of Windows Server.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co. Ltd. develops state-of-the-art computer forensics tools, provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, foreign governments, and all major accounting firms. ElcomSoft is a Microsoft Partner (Gold Application Development), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.