Dutch police, Kaspersky Lab fight against CoinVault

April 16 2015, by Nancy Owano

Dutch police obtained CoinVault cryptokeys and in turn victims may find their way out of the mess, reports Loek Essers, Amsterdam correspondent, IDG News Service. Computer users hit by this extortion version of ransomware—they find it blocks their access to their computer system or encrypts data on a disk—may be able to decrypt their files thanks to a tool from Kaspersky Lab. The app makes use of the keys that were found by the police, said IDG's Essers.

He explained that ransomware such as CoinVault makes its way to victims via phishing emails or links to malicious websites. CoinVault asks the victims to pay up. According to Essers, The National High Tech Crime Unit (NHTCU) of the Dutch police obtained a database from a

CoinVault command-and-control server which had the keys.

Kaspersky stepped up to the occasion and constructed the decryption tool. The National High Tech Crime Unit (NHTCU) of the Netherlands' police, the Netherlands' National Prosecutors Office and Kaspersky Lab have been working together to fight the CoinVault ransomware campaign.

The Lab can provide both the keys and the application. Jornt Van Der Wiel and Santiago Pontiroli of Kaspersky Lab said the database had "IVs, keys and private Bitcoin wallets." The Lab team created a website and started a communications campaign to notify victims that it might be possible to get their data back without paying.

According to the report from the IDG News Service, the tool is not 100 percent effective but there is reason to hope for progress, as the police hope to discover new keys and improve the tool's success rate. Kaspersky Lab said that "this is an ongoing investigation and new keys will be added in the future." Police suspect the CoinVault ransomware perpetrator is in the Netherlands.

Last year, Pontiroli shared some observations about the CoinVault: This type of ransomware, he said, "involves some interesting details worth mentioning, including the peculiar characteristic of offering the free decryption of one of the hostage files as a sign of good faith." He said at a certain point "if everything went well (for the cybercriminals) your personal documents and files have been encrypted and a payment is demanded in less than 24 hours or the price will rise. The bitcoin address used is dynamic too, making the tracing of the funds a lot more complex than usual."

Lucian Constantin of the IDG News Service last year shared his observations about the nature of CoinVault: "Users are asked to pay 0.5

bitcoins—around $200 at the current exchange rate—in order to receive the key that decrypts their files, but the cost increases every 24 hours. One aspect that sets CoinVault apart from other file-encrypting ransomware programs is that it allows users to see a list of encrypted files on their computer and choose one they can decrypt for free."

Meanwhile, John Biggs, East Coast Editor of *TechCrunch*, offered this advice about ransomware, saying "there are three simple rules to surviving such an attack: first, back up your computer. Then you need to back up your computer. Finally, you really have to back up your computer."