Featured news

- Researchers map out hard-to-kill, multi-layered spam botnet
- Hard-hitting insights into global attacks targeting organizations
- Open source tool checks for vulnerabilities on Android devices
- Signal for Android finally out, offers end-to-end encrypted calls and messages
- Stanford researchers identify potential security hole in genomic data-sharing network
- Open source KeeFarce tool loots encrypted passwords stored in KeePass
- Security update kills several critical bugs in Android Marshmallow
- Cyber operational readiness and a complex threat landscape
- Chimera crypto-ransomware is hitting German companies
- Researchers can identify people through walls by using wireless signals
- Hacking Team pitches encryption-cracking tools to US law enforcement
- Nearly 2% of all smartphones are compromised or high risk
- CoinVault and Bitcryptor ransomware victims don't need to pay the ransom
- Review: Change and configuration auditing with Netwrix Auditor 7.0

Chimera crypto-ransomware is hitting German companies

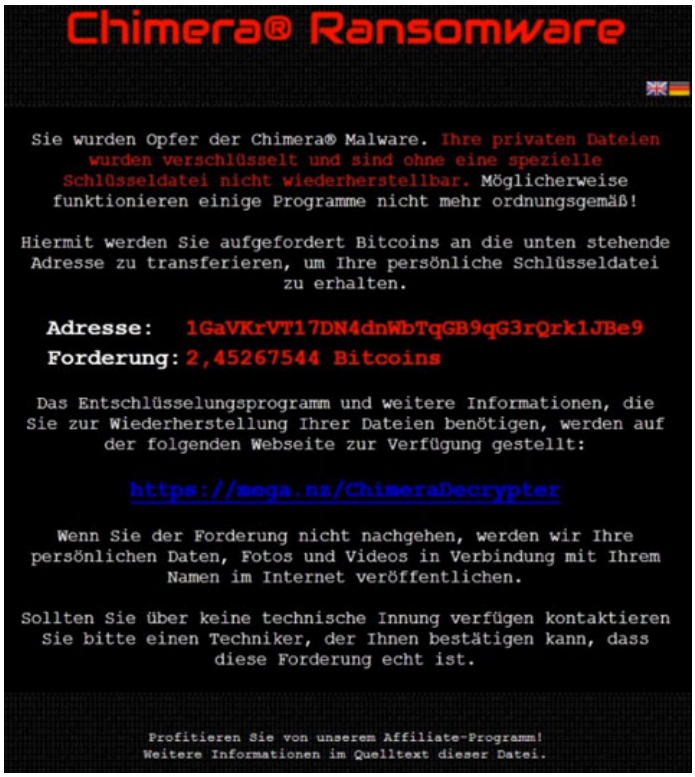
Posted on 03.11.2015

A new piece of crypto-ransomware is targeting German companies: it's called Chimera, and the criminals behind the scheme are threatening to release sensitive corporate data on the Internet if the targets don't pay the ransom.

The threat is delivered via fake emails from different addresses, apparently from individuals who want to either get a job with the target company or offer a job to an employee of the company.

Whatever the variant of the email is, it contains a link pointing to a Dropbox address, where additional information is ostensibly stored, waiting to be perused by the targets.

Unfortunately for those who fall for the trick, the downloaded file is actually the ransomware. Once installed, it proceeds to encrypt local data and that on other network drives, to lock the computer and show the following ransom note:



The criminals are asking for 2.45 Bitcoin (around €630/$694) to decrypt the files, and if the victim doesn't pay up, they promise to publish his or her personal documents, photos and videos, along with their name, on the Internet.

According to Botfrei researchers, who first warned (original in German) about the malware, there is no indication or evidence that the criminals have actually stolen files from infected systems before encrypting them, or that they have published any of them online.

In fact, it's very likely that this is an empty threat, made simply to spur users to pay the ransom. As Bob Covello rightly notes, exfiltrating that many documents from victims would mean the attacker have to have huge amounts of storage space, and the trail to the storage location would be easy for the authorities to trace.

"Another problem with the edentulous threat posed by this ransomware is

Spotlight

1 2 3 4 5

Open source KeeFarce tool loots encrypted passwords stored in KeePass

A researcher with security consultancy Security-Assessment.com has released the source code for KeeFarce, a tool that can export all information stored in the database of a user's KeePass password manager.

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address Subscribe

Daily digest

Receive a daily digest of the latest security news.

Email @ Address Subscribe

that the implication of a threatened personal information disclosure would assume that someone is combing through the files for that personal information," he pointed out.

"This is a level of involvement that most ransomware criminals do not want to broach. Ransomware is designed for a quick payday for the criminals with little interaction with the victim."

Nevertheless, people who haven't backed up their important files will be tempted to pay the requested amount. Hopefully there aren't many of them.

Author: Zeljka Zorz, HNS Managing Editor

Follow @zeljkazorz

cybercrime | Europe | malware | ransomware

DON'T MISS
Wed, Nov 4th

Researchers map out hard-to-kill, multi-layered spam botnet

Security update kills several critical bugs in Android Marshmallow

Cyber operational readiness and a complex threat landscape

Identify people through walls by using wireless signals

Nearly 2% of all smartphones are compromised or high risk

Back to TOP