DIGITAL EXTORTION

Let's call it what it is: Ransomware is a digital mechanism for extortion. The most common ransomware attack scenarios encrypt the victim's data before a ransom demand is even delivered. Because users place a high value on their data, many are willing to pay to get it back. However, paying the ransom is unwise, primarily because it does not guarantee that the corrupted data will be decrypted. Modern crypto malware uses encryption schemes that — up to now — seem to be unbreakable, so victims face a choice between paying up or losing those files forever.

This eBook will describe common ransomware scenarios, trends in this type of cybercrime and recommendations to help your organization avoid victimization.

RANSOMWARE 101

As cybercriminals realize that victims are often willing to pay for the release of their precious files, the prevalence of ransomware and its variations are on the rise. Here's a common scenario: The victim receives an email from "a friend" with an executable file attached. Disguised as an innocuous document, the file is opened, which triggers the immediate download of crypto malware and the victim's files are encrypted — effectively held hostage until they pay a ransom to get the decryption key.

Another, more sophisticated crypto malware mechanism is delivered via a Trojan of the Zeus/Zbot family, Citroni, which can be purchased online for only $3,000— a small sum given that a single ransom can earn a cybercriminal hundreds or even thousands of dollars. Once it's in the hands of the criminals, Citroni can be dropped on victims' computers using the Angler exploit kit. According to Threatpost, this particular ransomware includes a number of unusual features, and researchers say it's the first ransomware that uses the Tor network for command and control.[1]

However it's delivered, victims typically learn of the crime with the appearance of a dialogue box, notifying the user of the infection and demanding a payment for a key to decrypt the files. According to the message, victims have 72 hours to pay the ransom or the decryption key will be destroyed forever.

1. Threatpost, "Critroni Crypto Ransomware Seen Using Tor for Command and Control," July, 2014, https://threatpost.com/critroni-crypto-ransomware-seen-using-tor-for-command-and-control/107306

RANSOMWARE IS BIG BUSINESS

Many victims pay the ransom for encrypted files, probably assuming it's just the cost of doing business in the digital age. According to Threatpost, "CryptoLocker, one of the most famous variations, has infected tens of thousands of machines and generated millions of dollars of revenue for the gang behind it." [2]

The crypto malware threat is increasing: Kaspersky Security Network shows that in 2013 about 2.8 million crypto attacks were registered — that is nine times more than in 2012 — and all the evidence suggests that their number will continue to rise because many people are still willing to pay the ransom. According to a survey conducted by Interdisciplinary Research Centre in Cyber Security at the University of Kent in February 2014, more than 40 percent of CryptoLocker victims agreed to pay. Moreover, a Dell SecureWorks report shows that the same malware rakes in up to $30 million every 100 days.

Furthermore, the inability to decipher files encrypted by the modern malware spawns an additional threat — false remedy. Desperate users who lose their files search the Internet for any help and sometimes find software that claims to "fix" encrypted data. In the best case, it is a swindle selling a useless "solution"; at worst it distributes additional malware.

2. Threatpost, "Critroni Crypto Ransomware Seen Using Tor for Command and Control," July, 2014, https://threatpost.com/critroni-crypto-ransomware-seen-using-tor-for-command-and-control/107306

*According to a survey conducted by Interdisciplinary Research Centre in Cyber Security at the University of Kent in February 2014, more than **40 percent** of CryptoLocker victims agreed to pay.*

THE EVOLUTION OF RANSOMWARE

Criminal methods become more and more sophisticated each year. The first crypto malware used a symmetric-key algorithm, with the same key for encryption and decryption. Usually, with some help from anti-malware vendors, corrupted information could be successfully deciphered. Then cybercriminals began to implement public-key cryptography algorithms that use two separate keys — public, to encrypt files, and private, which is needed for decryption. One of the first practicable public-key crypto systems to be used by cybercriminals was called RSA (named after Ron Rivest, Adi Shamir and Leonard Adleman, who first described the algorithm). Back in 2008, Kaspersky Lab's experts managed to crack a 660-bit RSA key used by the GPCode Trojan, but soon its authors upgraded the key to 1,024 bits, making it practically impossible to decrypt.

One of the most recent and most dangerous pieces of crypto malware, the previously mentioned CryptoLocker Trojan, also uses a public-key algorithm. After each computer is infected, it connects to the command-and-control server to download the public key, so another key, the private one, is accessible only to CryptoLocker's authors. Usually the victim has no more than 72 hours to pay the ransom before their private key is deleted forever. It is impossible to decrypt any files without this key. Kaspersky Lab's products successfully detect this Trojan and block infection, but if the system is already infected, then nothing can be done with the corrupted files.

*"**CryptoLocker**, one of the most famous variations, has infected tens of thousands of machines and generated millions of dollars of revenue for the gang behind it."* [3]

3. Threatpost, "Critroni Crypto Ransomware Seen Using Tor for Command and Control," July, 2014, https://threatpost.com/critroni-crypto-ransomware-seen-using-tor-for-command-and-control/107306
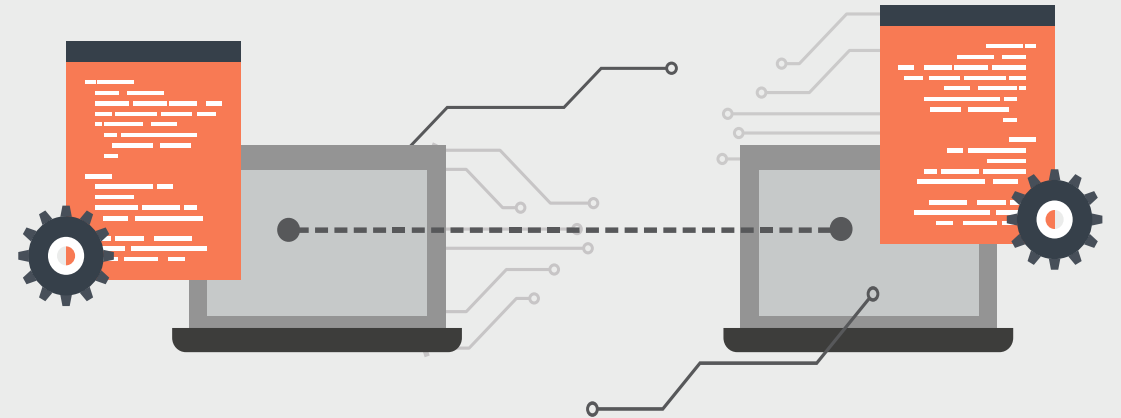
DEFENDING AGAINST RANSOMWARE

It is impossible to decipher files encrypted by modern crypto malware, so the only countermeasure to keep user's data safe is file backup. But general backup, even a regular one, is not enough, because it leaves recently changed files unprotected. Many ransomware variants are smart enough to also encrypt every backup they are able to locate, including those residing on network shares. That is why Kaspersky Lab developed an alternative countermeasure, based on the System Watcher module.

According to the Kaspersky Security Network, about

2.8 Million

crypto attacks were registered in 2013.

ALL SECURITY IS NOT CREATED EQUAL

Kaspersky Lab Provides Best in the Industry Protection

IN 2014, KASPERSKY LAB PRODUCTS PARTICIPATED IN 93 INDEPENDENT TESTS AND REVIEWS. OUR PRODUCTS WERE AWARDED 51 FIRSTS AND RECEIVED 66 TOP-THREE FINISHES.
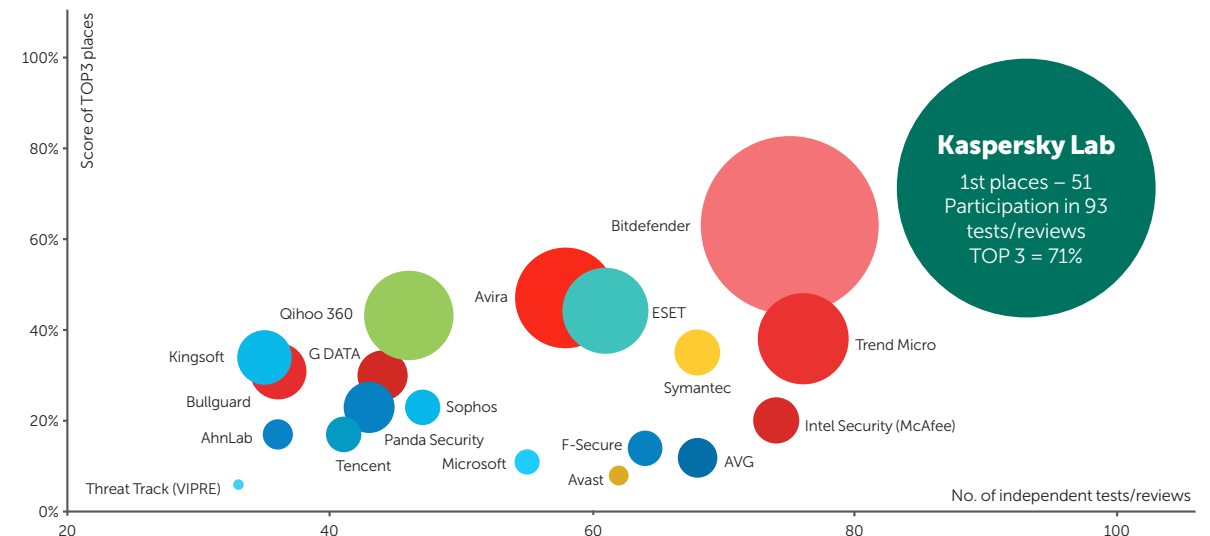
ACCESS REPORT

Information security is in Kaspersky Lab's DNA. The Kaspersky Security Network (KSN) has more than 60 million Kaspersky Security Network volunteers worldwide. This security cloud processes over 600,000 requests every second. Kaspersky users around the globe provide real-time information about threats detected and removed. This data and other research are analyzed by an elite group of security experts — the Global Research and Analysis Team. Their main focus is the discovery and analysis of new cyberweapons, along with the prediction of new types of threats.

A purely technology-driven company, more than one third of Kaspersky Lab's employees work in research and development. All solutions are developed in-house on a single code base. Kaspersky Lab's leadership and expertise is proven in multiple independent tests. In calendar year 2014, Kaspersky participated in 93 independent tests and reviews. Sixty-six times Kaspersky Lab was named in the Top 3 and 51 times was rated first place.

Score of TOP3 places

100%
80%
60%
40%
20%
0%

20   40   60   80   100

No. of independent tests/reviews

Bitdefender
Avira
Qihoo 360
ESET
Kingsoft
G DATA
Trend Micro
Bullguard
Symantec
Sophos
AhnLab
Panda Security
Intel Security (McAfee)
Tencent
Microsoft
F-Secure
AVG
Threat Track (VIPRE)
Avast

Kaspersky Lab
1st places – 51
Participation in 93
tests/reviews
TOP 3 = 71%

* **Notes:** According to summary results of independent tests in 2014 for corporate, consumer and mobile products. Summary includes tests conducted by the following independent test labs and magazines: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. The size of the bubble reflects the number of 1st places achieved.

PROTECT YOUR BUSINESS NOW.

GET YOUR FREE TRIAL NOW

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Visit Knowledge Center

Learn more at kaspersky.com/business

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users.* Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

To learn more, call Kaspersky Lab today at (866) 563-3099 or email corporatesales@kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.

KASPERSKY lab

THE POWER OF PROTECTION