

Ransomware: Many victims, few solutions

Ransomware.

Rebirth of a lucrative attack

Over the past few months, we have been witnessing a boom in ransomware attacks. With attacks such as Cryptolocker or the more recent Petya, ransomware has been under the media spotlight due to its lucrative side as well as how quickly and devastatingly it spreads.

In a few words

Ransomware is malicious software that **holds private data hostage**.





Such malware encrypts private data, and through a message, demands that the owner **sends money in exchange for the key** that would allow decrypting the data.

2 types of ransomware:

First category: Classic "police" ransomware that freezes your browsers (called Browlock) or completely paralyzes your computer.

The second, increasingly widespread and probably the more nefarious, includes crypto-ransomware or "cryptoware". Malicious software of this kind will encrypt documents stored on your computer, making them unreadable without the decryption key held by the hacker who will then demand a ransom in exchange for this key.

EMERGENCE OF THE FIRST RANSOMWARE

 Name PC Cyborg Trojan.	 Modus Operandi Issued warnings that the software license has expired	 Ransom demanded 189\$	 Created by Joseph Popp in 1989
---	---	--	---



AN ACTIVE AND VARIED FAMILY

-
- GPoada (AG, AK)
- Magnitude
- TRJ RANSOM.A
- Arctivus
- Krotten
- RSA4096
- Cerber
- Cryzip
- MayArchive
- Petya
- CryptoLocker
- TorrentLocker
- Cryptowall
- TeslaCrypt
- Locky Ransomware
- KeRanger
- CTB-Locker
- WinLock
- Reveton
- VirusShare
-

OBSERVATION
Such attacks are constantly on the rise (new attacks or variants)

ALL OF US ARE AFFECTED
Private users & Organizations of all sizes and sectors

COMMUNITY OF HACKERS
Various ransomware campaigns are no longer carried out by a single group but by several groups of people.

COMPLEXITY OF ENCRYPTION
Ransomware has become harder and harder to decrypt, shrinking chances of getting back data without having to pay the ransom demanded.
In a very short time, encryption keys have grown considerably both in size and in strength.

ALL OSs affected

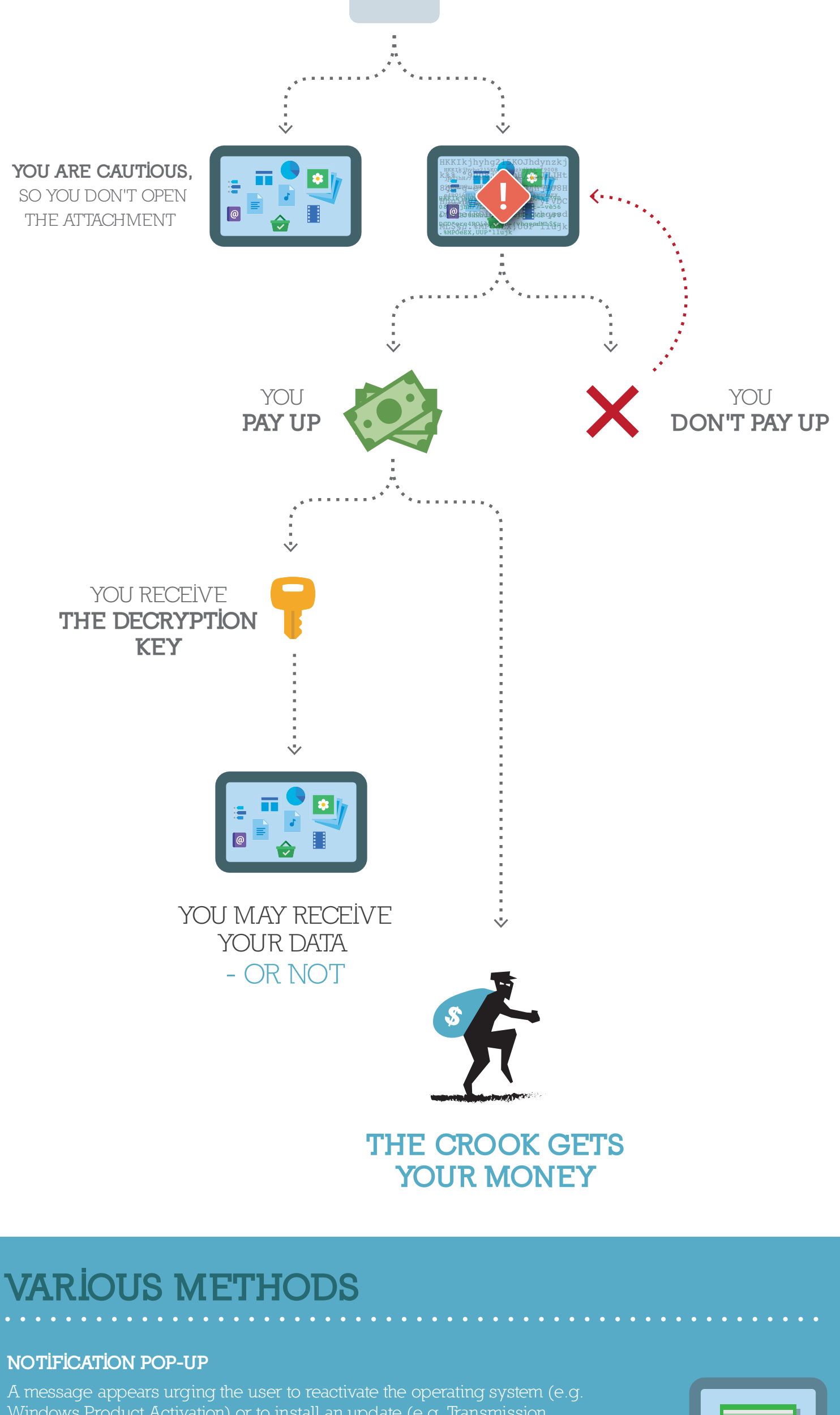
KERANGER
THE FIRST RANSOMWARE TARGETING MAC OS X SYSTEMS (2016)

CTB-LOCKER (VARIANT)
TARGETS WEB SERVERS IN GNU/LINUX

CAMPAIGNS ARE TARGETED
A striking example: Locky
Targeting corporations, Locky spread through malicious email campaigns (emails containing false invoices, bearing an Operator logo, etc)
Customized emails made it all the more effective.

660 bits $>$ 1,024 bits
2006 2008

ILLUSTRATION OF A SIMPLE ATTACK



VARIOUS METHODS

NOTIFICATION POP-UP
A message appears urging the user to reactivate the operating system (e.g. Windows Product Activation) or to install an update (e.g. Transmission software on OSX).
Unsuspectingly, the user will click on the invitation without further verification and as such set off the attack which in several seconds will encrypt all his private data or part of the operating system.

THE NEW JIGSAW THREAT
Ransomware has come a long way in sophistication. And new techniques appear. The latest to date being Jigsaw, ransomware with a countdown.
If 150USD worth of Bitcoins are not purchased within the time limit given, a countdown will begin to delete files on the victim's computer whenever the counter reaches 0.
In this way, the user being held in a stressful state and with little time to think clearly, will prefer to pay the ransom.

PLAYING ON FEARS
Certain ransomware programs do not encrypt data, but misuse legal authority to extort from users by displaying pornography or child pornography.
To unlock their workstations, users need to send an SMS to a toll number. Such scams allegedly reaped about 14 million Euros.

CREATE YOUR OWN RANSOMWARE WITHOUT TECHNICAL KNOWLEDGE

RANSOMWARE AS A SERVICE

AS A SERVICE ?
The creation of malicious code is no longer the talent of a privileged handful. Currently, anyone can do it as the generation of malicious code is available as a service on the Dark Web. As a matter of fact, threats will increase sharply in the coming months.

HOW DOES IT WORK?
With very simple step-by-step tools, the hacker can quickly assemble his own ransomware. He rewards the provider of this service by paying him a 25% commission on transactions made through the campaign.



- RANSOMWARE DOES NOT ONLY SPREAD BY EMAIL -

- Multiple infection vectors**
- compromised or malicious websites,
 - a USB key,
 - a software/application installation from an unreliable source,
 - social networks (which facilitate social engineering), etc.

TELEPHONES ARE UNDER THREAT

ANDROID, A MASSIVE CHALLENGE.
Telephones today are no longer just telephones - our address book and all related information (contacts, numbers, addresses, birthdays, etc), messages, notes, photos and even applications are stored on them. Imagine their potential for hackers.

Having recently made its appearance, Dogspectus is a ransomware program that holds information hostage on Android smartphones in versions below version 4.4.

SOLUTIONS TO COUNTER RANSOMWARE

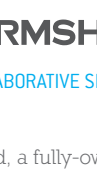
FOR REAL PROTECTION, THERE IS A PROACTIVE SOLUTION

Stormshield Endpoint Security

This proactive protection prevents malicious software from running on your computer and/or exploiting vulnerabilities (through an exploit kit).

Stormshield Endpoint Security with its proactive malicious behavior identification technology allows blocking most ransomware programs even before they are identified as such by the cybersecurity community.

Further information: www.stormshield.eu/endpoint-protection



STORMSHIELD
COLLABORATIVE SECURITY

Stormshield, a fully-owned subsidiary of Airbus Defence and Space, offers innovative end-to-end security solutions to protect:

- Networks** (Stormshield Network Security),
- Computers** (Stormshield Endpoint Security)
- Data** (Stormshield Data Security).

www.stormshield.eu

- SOME INDISPENSABLE ADVISE**
- To protect yourself from ransomware
 - Be wary of suspicious emails with attachments or from dubious websites.
 - Regularly perform backups.
 - Update your applications, plugging and operating systems.