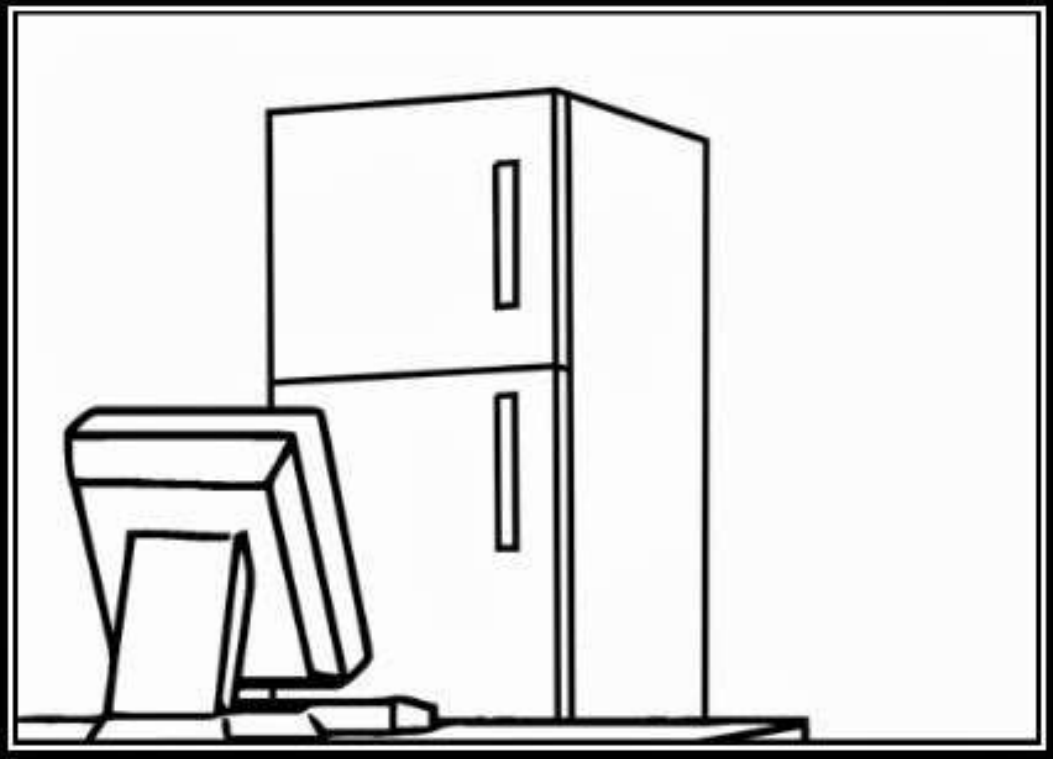


Vostro Onore, sono il frigo! L'IoT alla sbarra...

Problemi tecnico-giuridici con gli oggetti intelligenti

Pavia, 24 novembre 2016

Chi Siamo

Davide ‘Rebus’ Gabrini

Per chi lavoro non è un mistero.

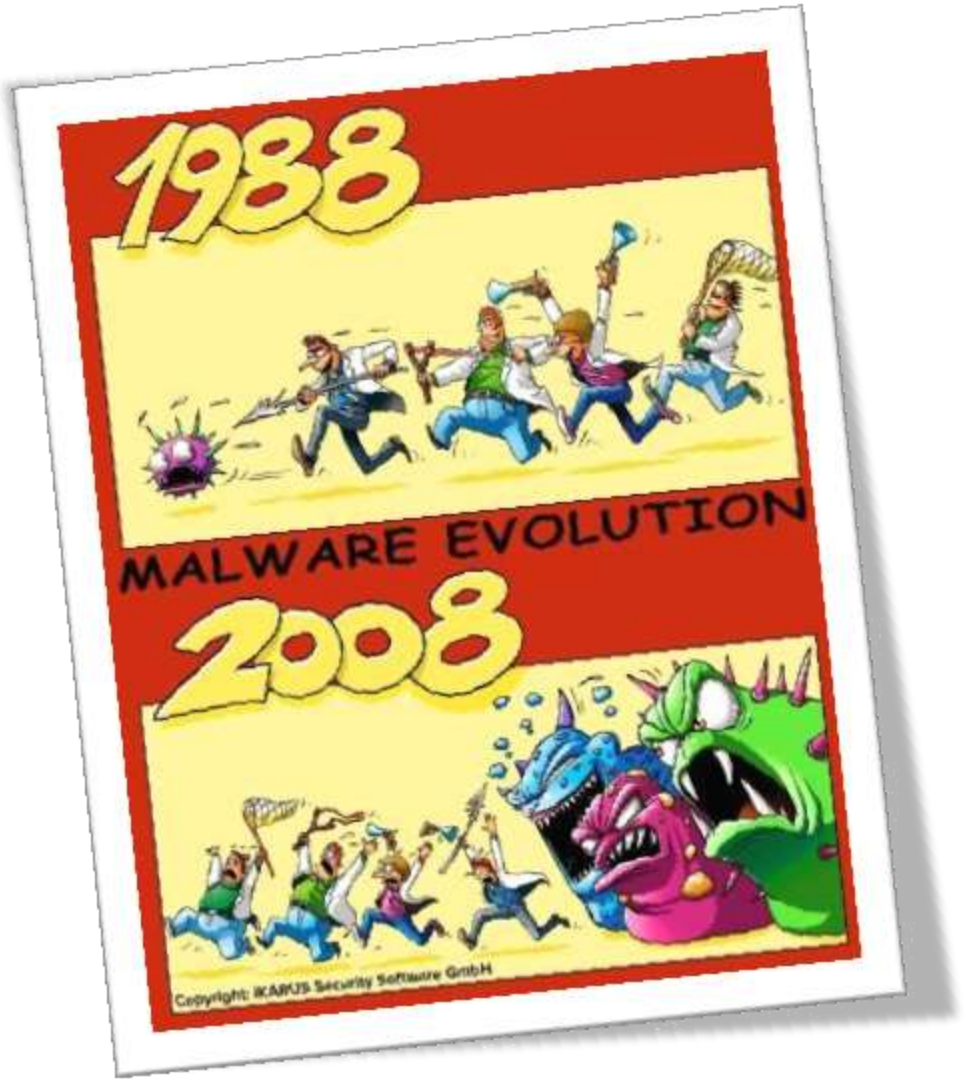
Oltre a ciò:

- Perito informatico
- Consulente tecnico e Perito forense
- Collaboratore UniPV
- Docente di sicurezza informatica e digital forensics per privati e P.A.
- Certificazioni CIFI, ACE, AME
- Socio Mensa, DEFTA, IISFA, Tech&Law fellow
- Socio fondatore Italian Gr.A.P.P.A.
- Presidente Nutria-LUG
- Sensei Zanshin Tech

Chi Siamo

Paolo Dal Checco

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- Professore a Contratto di Sicurezza Informatica @ UniTO (SUISS)
- Consulente Informatico Forense per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- Tra i fondatori dell'Associazione DEFTA (www.deftlinux.net) e ONIF (www.onif.it)
- Direttivo Associazione IISFA, socio AIP, Tech & Law, Clusit, AssoB.it
- www.ransomware.it/www.bitcoinforensics.it/www.dalchecco.it/www.difob.it



Malware e IoT

Insecurity by design

- La sicurezza costa e intralcia la facilità d'uso
- Non è una priorità dei costruttori
  - Feature carenti
  - Configurazioni deboli
  - Password hard encoded
  - Aggiornamenti sporadici, raramente automatizzati
  - Assenza di antivirus
  - …

Profitto del malware per IoT

- Un malware per **spiarli**
  - Non solo ciò che passa dal dispositivo…
    - Informazioni memorizzate, dati dai sensori
  - …ma anche ciò a cui può accedere
    - in LAN o in Cloud
- Un malware per **derubarli**
  - Impossessandosi di informazioni di valore
- Un malware per **ricattarli**
  - Occupando una risorsa e chiedendo il pagamento di un riscatto per rilasciarla
- Un malware per **usarli**
  - Proxy per il cybercrime

Ransomware

- Dalla prima pagina del Rapporto Clusit 2016: «*E poi c'è la modalità di attacco che più di ogni altro ha fatto parlare del tema nel corso del 2015:* ***i ransomware****. Vera e propria estorsione informatica la cui diffusione, e la conseguente capacità di generare denaro, non conosce limiti.*»
- Una minaccia così nuova che il primo ransomware è del 1989, ma il reboot in chiave moderna è del 2012 con Reveton (il «malware della polizia») e dal 2013 con Cryptolocker

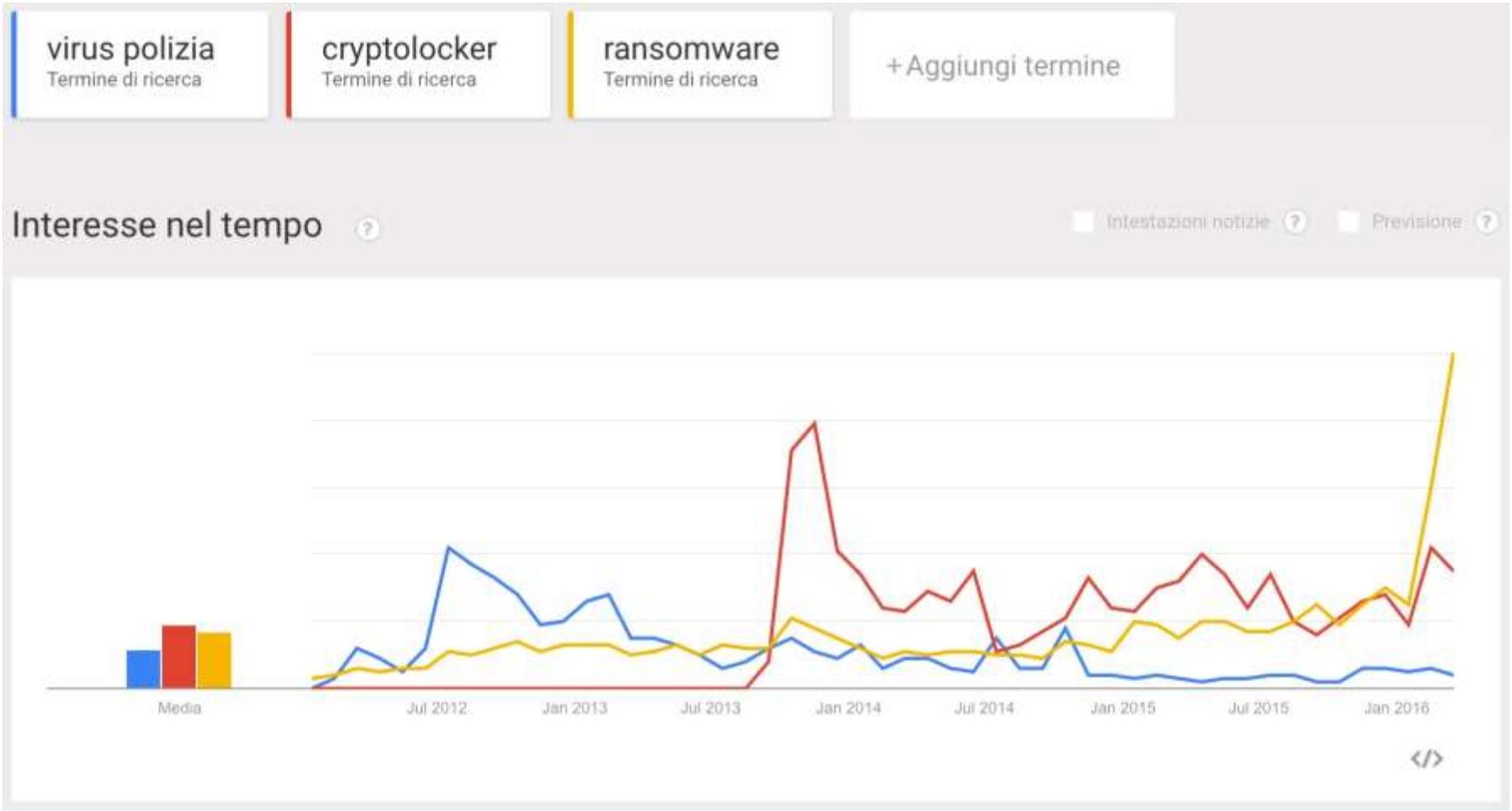
La preistoria

- Innocuo, non criptava i dati
- Modificava registro o avvio, facile da rimuovere

Le cose si fanno più serie

- Da settembre 2013 compaiono diverse versioni che **infettano PC con Windows**: CryptoLocker, SimpleLocker, CryptorBit, CryptoDefense, CryptoWall, TorrentLocker, CTB-Locker, TeslaCrypt, etc…
- Il trojan arriva **via email**
- I documenti vengono **criptati davvero**, anche quelli in rete raggiungibili dal PC infettato, viene chiesto un riscatto in **bitcoin** (da 300 a 1.000 euro) che aumenta se non si paga subito
- **Prime versioni con cifratura debole**, con alcuni bachi e niente sovrascrittura reale dei file, col tempo queste "leggerezze" vengono colmate e il **sistema irrobustito**
- Alcune organizzazioni eseguono **infezioni mirate** e chiedono 10 volte tanto (episodi molto più rari)

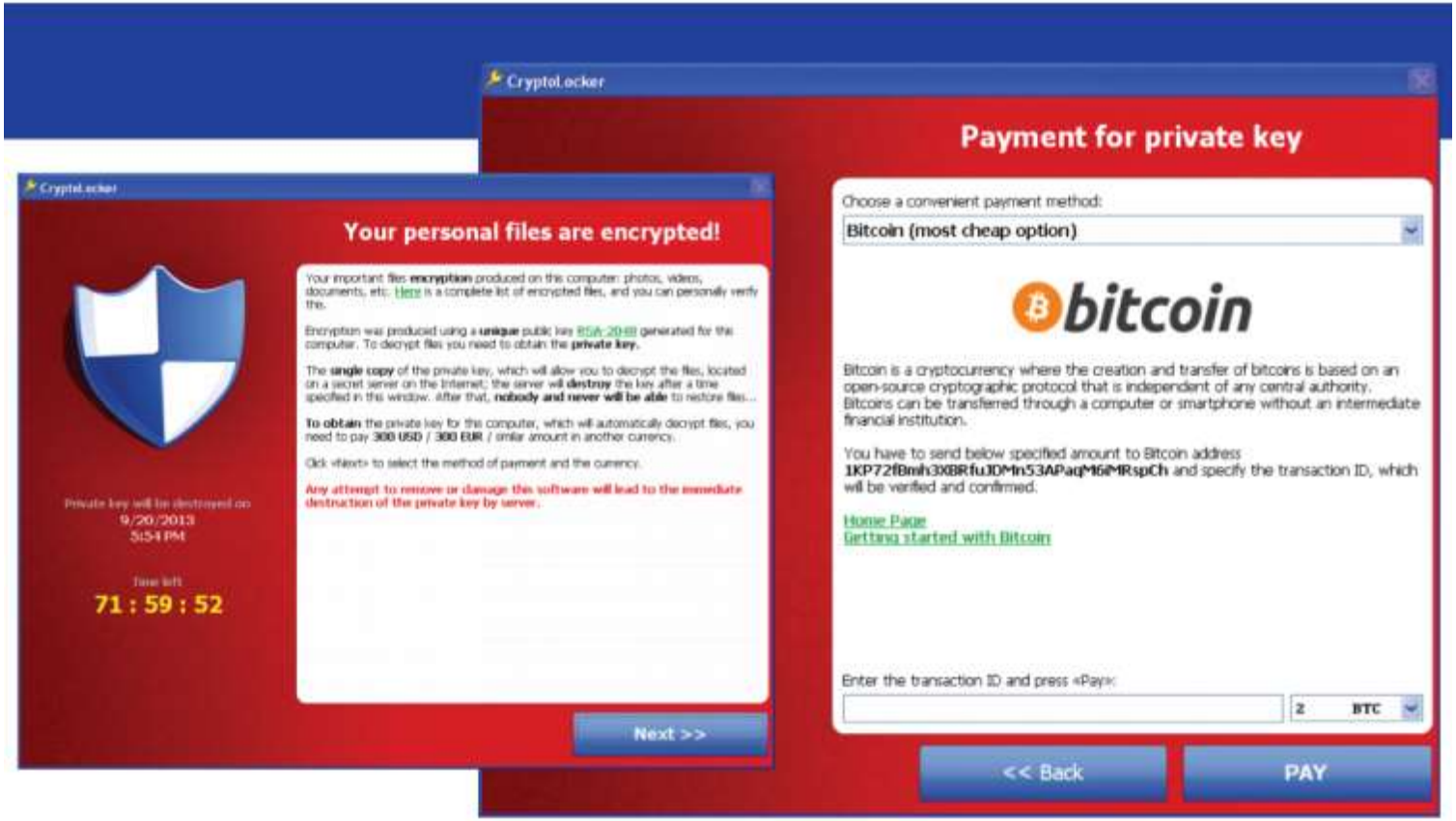
Le cose si fanno più serie



Fonte: Google Trends

Cryptolocker: allegato alla mail

- Stesso indirizzo bitcoin per tutte le vittime
- Trovate diverse soluzioni per decriptare senza pagare



TorrentLocker: attacco ai comuni

La mail pirata attacca i Comuni E il riscatto va pagato in bitcoin

Parte dalla Russia e beffa gli antivirus, decine di amministrazioni colpite in Italia

MILANO L'anagrafe non può più rilasciare i certificati, la contabilità non riesce a pagare, il protocollo è fermo perché anche lì i documenti sono bloccati: sono gli effetti del virus informatico di ultima generazione che sta infestando i pc di decine di Comuni in tutta Italia. Per eliminarlo si deve pagare un riscatto: 400 euro, ovviamente in bitcoin, il doppio se lo si fa dopo tre giorni.

Arriva da San Pietroburgo (Russia) l'ultimo «ransomware» (dall'inglese *ransom*: ri-

400

Euro Quanto bisogna pagare (non in contanti, ma in Bitcoin, la moneta virtuale) per farsi sbloccare i computer

excel, ma anche le foto, rendendoli inutilizzabili. «Una cosa inimmaginabile che ci ha bloccati per tre giorni. Avevamo l'antivirus, ma non è bastato», racconta Maria Grazia Mazzolari, segretario comunale a Bussoleno (Torino), centro di poco più di seimila anime in Val di Susa noto per le proteste sulla Tav.

«I pc continuano a funzionare, i documenti sono ancora al loro posto ma non si aprono e nelle cartelle compaiono dei file dal nome preoccupante "decript_instructions.html"», spiega Paolo Dal Checco della Di.Fo.B., lo studio di consulenza informatica forense che collabora con le Procure in molte inchieste, come quelle sull'Expo a Milano, sulla Concordia a Grosseto e sul Mose a Venezia e che sta fornendo assistenza a molti dei Comuni infettati. «Solo chi ha una copia di riserva dei documenti si salva, gli altri devono pagare i criminali» aggiunge il collega Giuseppe Dezzani. In che modo? Sullo schermo appare un messaggio che invita ad acquistare un «software di decodifica» per 400 euro in bitcoin, spiegando anche come fare. «Purtroppo — dice Dal Checco — il sistema bitcoin prevede che le transazioni e gli indirizzi su cui vengono fatte, una sorta di Iban, siano pubblici, ma non c'è modo di attribuire un indirizzo a un nome». Monitorando due di questi indirizzi, la Di.Fo.B.

Cosa sono

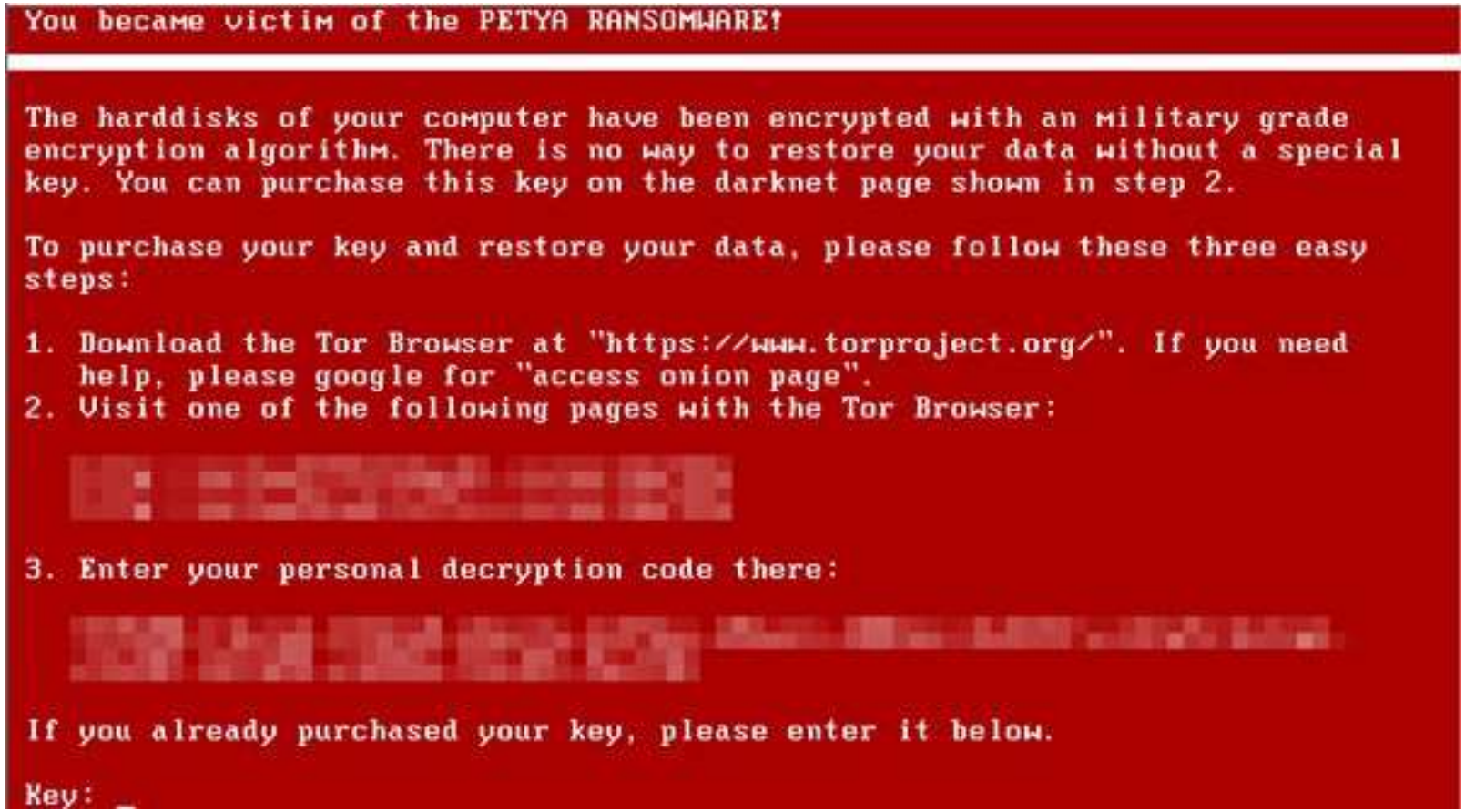
- I Bitcoin sono una valuta elettronica virtuale: esistono soltanto per gli acquisti via web
- Si comprano da un privato che li ha già

Autunno con l'ombrellone

Corriere della Sera, 11 novembre 2014

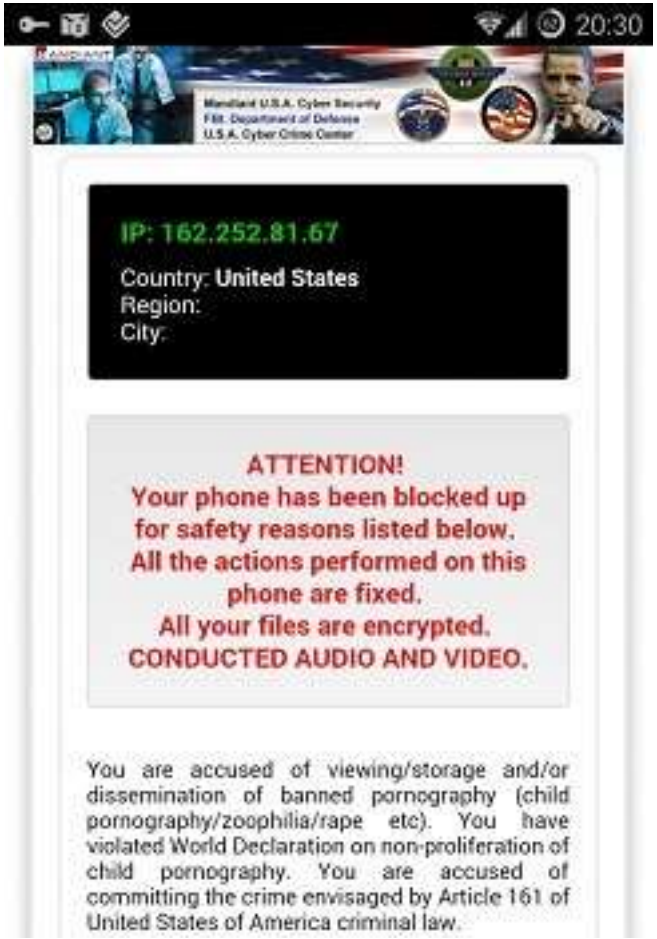
Si comincia a cifrare tutto...

- Non cripta i documenti, ma la parte del disco che permette di avviare il sistema e accedere ai documenti
- Richiede privilegi di amministratore

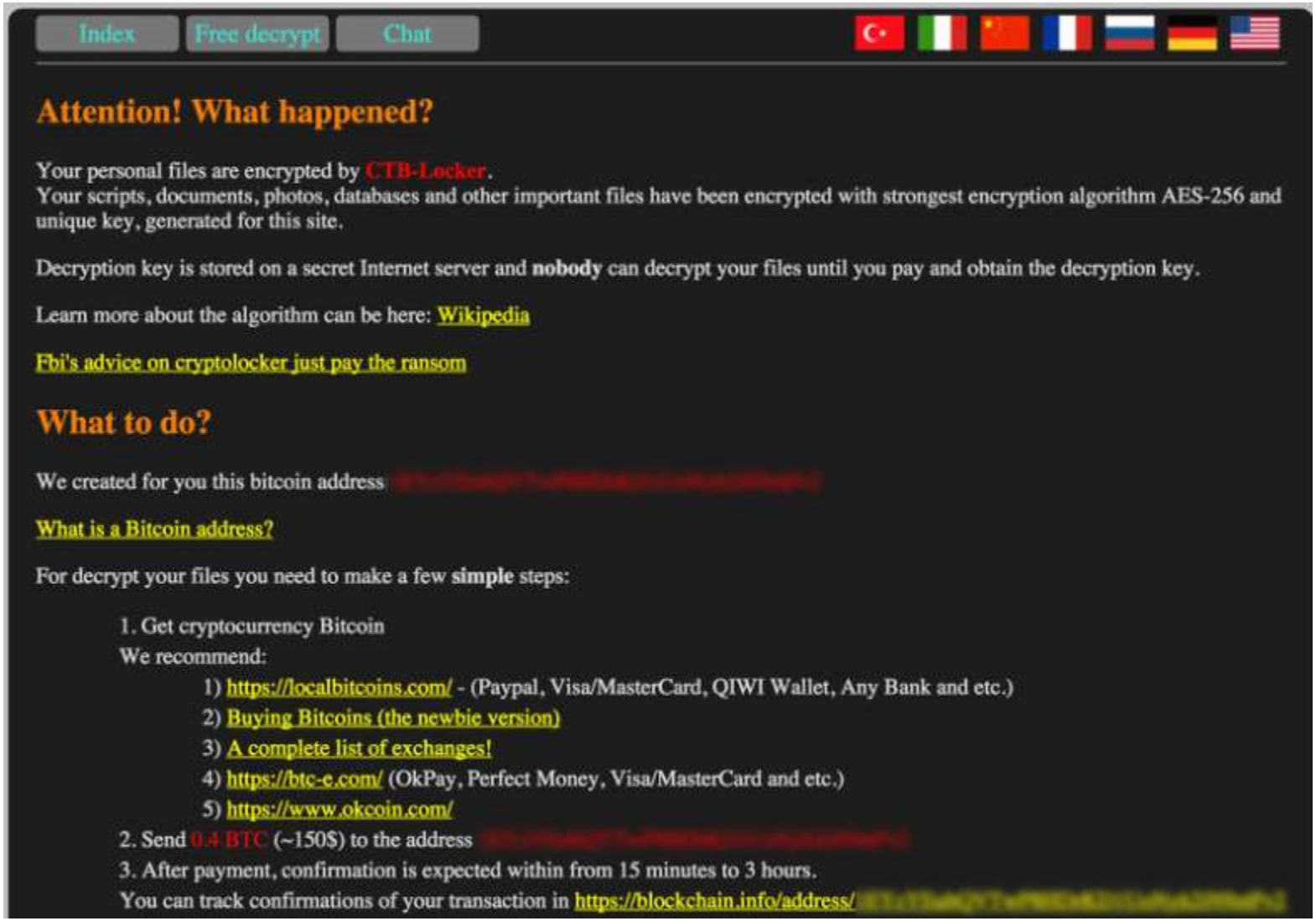


… infettando anche gli smartphone…

- Come nel 2012, ma su smartphone
- Non cripta i documenti, blocca l'avvio
- No bitcoin ma PaysafeCard
- Safe boot, uninstall e si rimuove



… i siti web…



Index | Free decrypt | Chat

Attention! What happened?

Your personal files are encrypted by CTB-Locker.
Your scripts, documents, photos, databases and other important files have been encrypted with strongest encryption algorithm AES-256 and unique key, generated for this site.

Decryption key is stored on a secret Internet server and **nobody** can decrypt your files until you pay and obtain the decryption key.

Learn more about the algorithm can be here: Wikipedia

Fbi's advice on cryptolocker just pay the ransom

What to do?

We created for you this bitcoin address [redacted]

What is a Bitcoin address?

For decrypt your files you need to make a few **simple** steps:

1. Get cryptocurrency Bitcoin
We recommend:
   1) https://localbitcoins.com/ - (Paypal, Visa/MasterCard, QIWI Wallet, Any Bank and etc.)
   2) Buying Bitcoins (the newbie version)
   3) A complete list of exchanges!
   4) https://btc-e.com/ (OkPay, Perfect Money, Visa/MasterCard and etc.)
   5) https://www.okcoin.com/
2. Send 0.4 BTC (~150$) to the address [redacted]
3. After payment, confirmation is expected within from 15 minutes to 3 hours.
You can track confirmations of your transaction in https://blockchain.info/address/[redacted]

… e le Smart TV.


MINISTRY OF JUSTICE.CRIMINAL POLICY
犯罪者情報
オフェンス情報
ファインのお支払い
取扱説明の解除
注意！お使いのデバイスがロックされている、その理由を以下に示します
残り時間は、罰金を支払います
71:58:24
それ以外の場合はケースファイルは、裁判所に転送されます
履歴クエリは、国土安全保障省のデータベースに格納されています
犯罪者情報
SAMSUNG

A quando i frigoriferi?

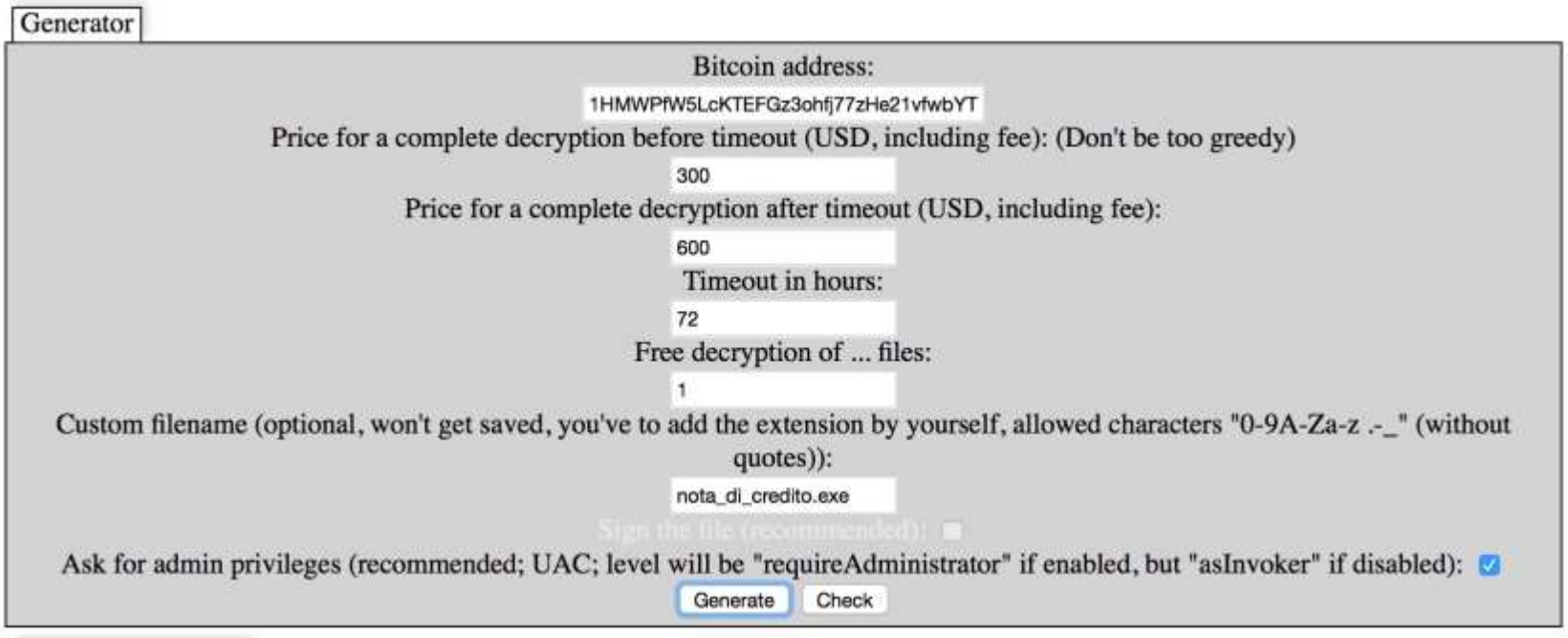
Cambia il business model: arriva il franchising

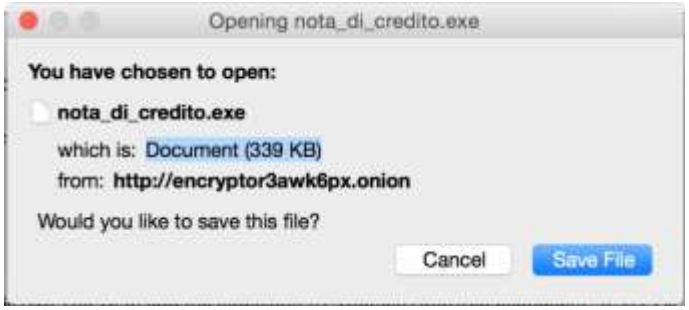
Welcome to Encryptor RaaS. (Ransomware as a Service)

Informations

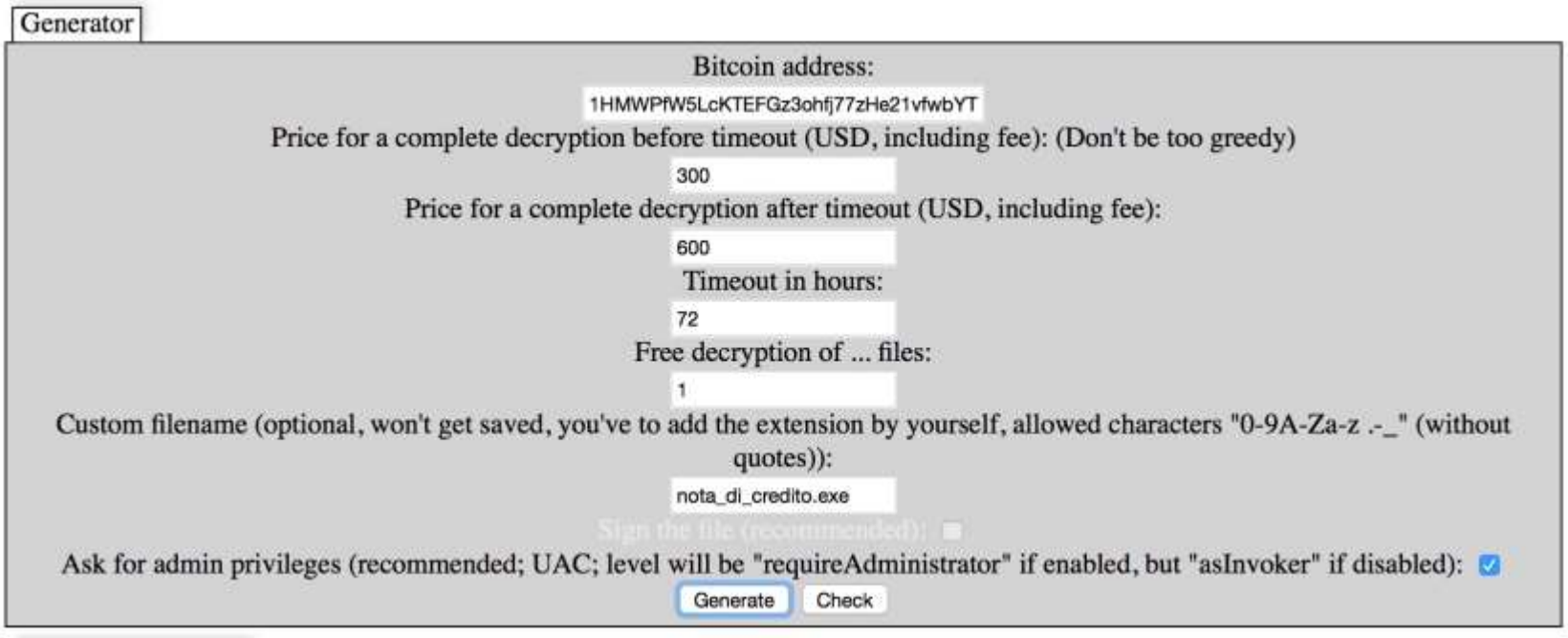
The bitcoin address acts as an identifier, so don't use a shared bitcoin address!
An incoming payment will be cleared and forwarded fully automated once the full amount has been payed.
Decryptor links: **Decryptor interface**, **Decryptor demo**.
I won't release private executables, except for very good reasons, because the maintenance would be too time consuming.
Requestable customizations: Victims page template, readme filename, readme content and an unique hidden service address.
Please see **this** file for rudimentary informations about the victims page template and contact me.
Fee: 5 percent.
Fixed BTC/USD rate: 409.05 USD.
Number of victims (excluding demo victims): 1840
Payed (excluding demo victims; automatically updated): 8 (0.43%)
Incomplete payments (excluding demo victims; manually updated): 3
FAQ: **faq.html**
2016-02-12: I've added informations about a hidden feature to the FAQ.
2016-02-17: It came to my attention that developers of other ransomware families are using my free file signing service. It's not kind to make financial profit and not even donate to me!
2016-03-09: Code signing is disabled until further notice due to a lack of certificates. I would be glad if I would receive some donations and/or certificates.
2016-03-18: I've got two stolen authenticode certificates for sale. The highest bid wins. It's OK to bid just for one and the end of the auction is not determined yet. (Details: SHA1 and SHA256, both are valid until late 2018, they aren't issued to the same name and I would use them for my service instead if they wouldn't be valid for that long)

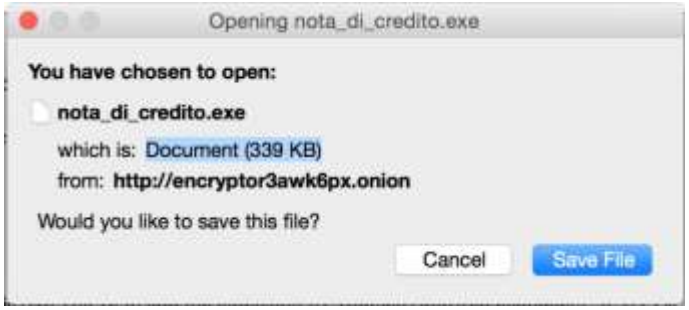
Cambia il business model: arriva il franchising





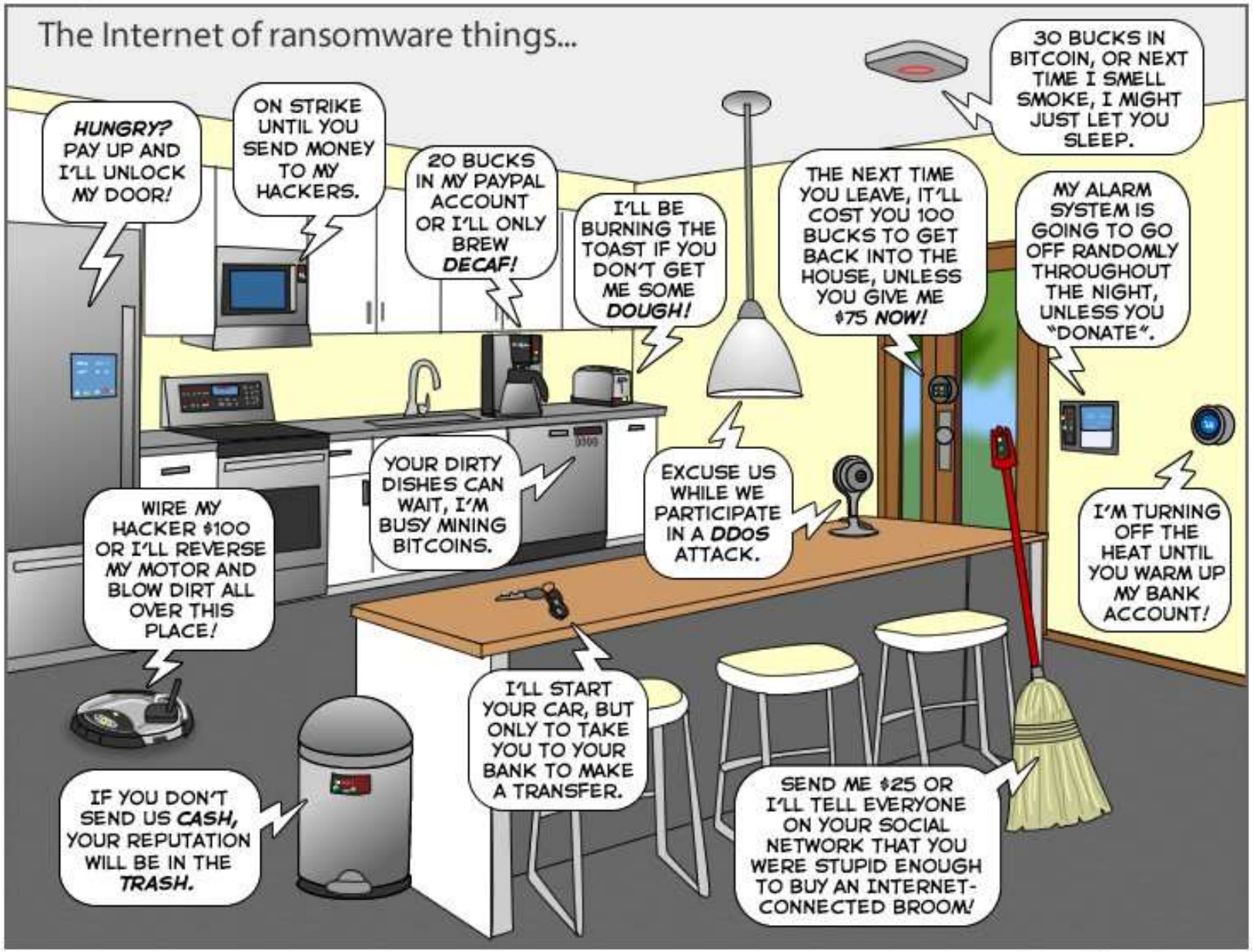
Cambia il business model: arriva il franchising





Il futuro

- Minaccia di divulgazione materiale privato
- Il ransomware propone “affiliazione” alle vittime



Scenari reali

Smart TV, DVR, Home Theatre, proiettori…

HELPNETSECURITY

b Zeljka Zorz - Managing Editor
June 13, 2016

a b c d

Ransomware targets Android smart TVs

If you own a Sharp and Philips smart TV running the Android TV OS, you should know that it could be hit by FLocker, a device-locking ransomware that targets both Android-powered mobile devices and smart TVs.

Quotidiano online sulla digital economy e la cultura del futuro, diretto da Raffaele Barberio

key4biz dal 2002

24/11/2016 - S. Crisogono martire

Smart Tv sotto attacco: richieste di riscatto in bitcoin dal cybercrime

La nuova frontiera dei criminali informatici sono le Smart Tv. In agguato il rischio di spionaggio industriale o il furto dei dati sensibili.

di Raffaella Natale | @RaffaNatale | 8 gennaio 2016, ore 11:05

Il Disinformatico

Un blog di Paolo Attivissimo, giornalista informatico e cacciatore di bufale

12.8.16 25 commenti

Ransomware per termostato, nuova tappa dell'Internet delle Cose

Non è la prima volta che metto in guardia contro la superficialità con la quale troppi produttori di elettrodomestici e altri apparati collegano a Internet qualunque cosa senza pensare alle implicazioni di sicurezza informatica: stavolta è il turno degli impianti di riscaldamento.

Dalla DEF CON di Las Vegas arriva infatti una dimostrazione dei ricercatori di sicurezza Andrew Tierney e Ken Munro, che hanno spiegato non solo come prendere il controllo di un termostato connesso a Internet ma anche come usarlo per chiedere un riscatto con la minaccia di far salire o scendere la temperatura di casa a livelli insopportabili: una forma di attacco molto simile a quella mostrata, guarda caso, poche settimane fa in una puntata di *Mr. Robot*.

I due ricercatori non hanno reso pubblico il nome del produttore del termostato vulnerabile, che hanno contattato privatamente in modo da consentirgli di preparare un aggiornamento correttivo, ma hanno spiegato la tecnica usata: il termostato, che usa Linux, non effettua alcun controllo sui file che gli vengono forniti tramite una scheda SD per consentire agli utenti di caricare impostazioni e sfondi. Non è difficile, quindi, convincere una vittima a caricare un file ostile, camuffandolo come un'immagine o un aggiornamento di sicurezza, prendendo così il controllo del dispositivo.

Il produttore del dispositivo preparerà l'aggiornamento, ma il vero problema sarà farlo arrivare a tutti gli utenti, che non sempre registrano il proprio dispositivo negli archivi del fabbricante e se lo fanno sono molto pigri nell'effettuare aggiornamenti, anche perché l'idea di dover aggiornare il software di un frigorifero, di un televisore o di un termostato non è ancora entrata nel sentire comune.

Furto/danneggiamento … profitto!

WIRED

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REM JEEP ON THE HIGHWAY—WI

Miller attempts to rescue the Jeep after its brakes were a ditch. ANDY GREENBERG/WIRED

International Business Times

Tesla Model S hack uses Android app exploit to track, unlock and steal car without the key

Norwegian app security firm Promon demonstrates how a Tesla can be driven away using malicious Android app.

By Alistair Charlton

November 24, 2016 00:01 GMT

Embed Feed Security researchers show how a Tesla can be stolen by hacking an Android app (Promon)

A team of computer hackers have demonstrated how the Tesla Model S can be located, unlocked and driven away without the key. By compromising the car's companion smartphone application, they used a laptop to remotely unlock the doors, start the electric car and 'steal' it from a

DAILY HEALTH INDUSTRY

Il progetto si avvale di un accordo di syndication con Reuters Health News

REUTERS

Medical device: pompa insulnica J&J a rischio hacking

MEDICAL DEVICE 5 ottobre, 2016 nessun commento

(Reuters Health) – La pompa insulinica Animas OneTouch Ping, prodotta da Johnson & Johnson, potrebbe essere esposta ad attacchi informatici, a causa di bug negli algoritmi di funzionamento. Il colosso statunitense ha iniziato da avvertire i pazienti USA. I dirigenti J&J hanno comunque dichiarato di non essere a conoscenza di attacchi hacker ai danni del dispositivo, "La probabilità di accesso non autorizzato al sistema di OneTouch Ping è estremamente bassa", ha affermato la casa farmaceutica nella comunicazione spedita lunedì 3 ottobre ai medici e ai circa 114.000 pazienti che usano il dispositivo negli Stati Uniti e in Canada. "Richiederebbe competenza tecnica, attrezzatura sofisticata e vicinanza fisica alla pompa, poiché il sistema di OneTouch Ping non è collegato a Internet o a qualsiasi altra rete esterna".

Animas OneTouch Ping, lanciata nel 2008, viene venduta con un telecomando *wireless* che i pazienti possono usare per ordinare alla pompa di dosare l'insulina; in questo modo, non hanno bisogno di accedere al dispositivo stesso, che solitamente viene indossato sotto i vestiti e può essere difficile da raggiungere. Secondo Jay Radcliffe, diabetico e ricercatore presso un'azienda di *cyber security,il* sistema è vulnerabile perché queste comunicazioni non sono criptate o codificate per impedire agli hacker di accedere al dispositivo.

Attacchi dimostrati su un robochirurgo

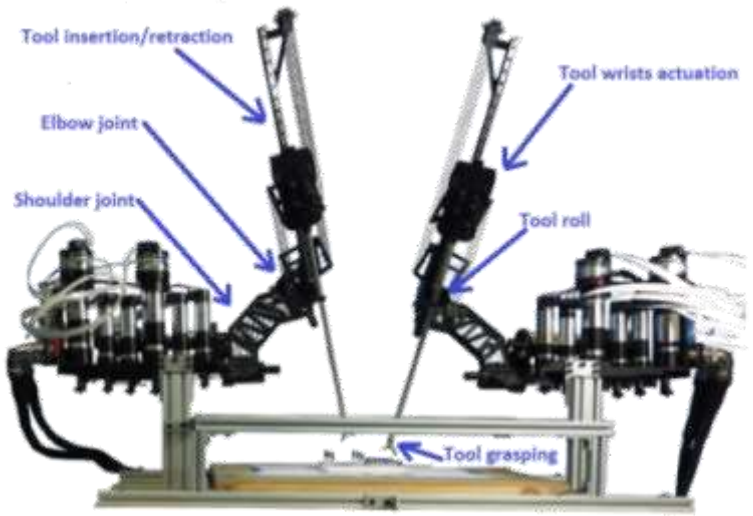
MIT Technology Review

A View from **Emerging Technology from the arXiv**

Security Experts Hack Teleoperated Surgical Robot

The first hijacking of a medical telerobot raises important questions over the security of remote surgery, say computer security experts.

April 24, 2015



- The team tries out **three type of attacks**. The first **changes the commands sent by the operator** to the robot by deleting, delaying or re-ordering them. This causes the robot's movement to become jerky and difficult to control.
- The second type of attack **modifies the intention of signals from the operator** to the robot by changing, say, the distance an arm should move or the degree it should rotate and so on.
- The final category of attack is a **hijacking that completely takes over the robot**. This turns out to be relatively easy since the Interoperable Telesurgery Protocol is publicly available.

Minaccia di danneggiamento

- Alle cose
  - Router, elettrodomestici, oggetti personali…
  - Droni, autoveicoli…
  - Impianti industriali
- Alle persone
  - Autoveicoli
  - Healtcare
    - Apparati biomedicali, peacemaker, pompe insuliniche

Contromisure

Pagare non è un'opzione

- Pagare il riscatto significa finanziare la criminalità organizzata
- Rende il business dell'estorsione redditizio e favorisce il proliferare delle minacce
- Incentiva e sostiene lo sviluppo di nuovi malware più sofisticati
- Produce un danno sociale per «riparare» ad una propria inadeguatezza
- Non risolve né riduce i propri problemi di sicurezza
- Non dà garanzia di risultato: stiamo parlando di criminali!

Blocco device o cifratura dati

- Tra i malware più facili da debellare: si pulisce il device e si ripristina il **backup**. E invece…
- Europol, 2013: «si stima che il 2% degli utenti infetti abbia ceduto al pagamento dando vita ad un business illegale da 1 milione di dollari annuo»
- FBI, 2015: in un anno, ricevute circa 1000 denunce relative a CryptoWall, con un totale di perdite di circa 18 milioni di dollari.
- Cisco, 2015, dopo aver debellato una campagna legata ad Angler Exploit Kit:
  - Circa 3600 utenti erano colpiti ogni giorni dal ransomware
  - Il 3% di essi ha pagato il riscatto richiesto
  - Si stima che la campagna abbia generato una rendita annuale di oltre 34 milioni di dollari

Hardening

- Password e configurazioni di default
- Interfacce amministrative in ascolto
- Abilitazione protocolli cifrati, sostituzione/rinnovo dei certificati
- Configurazione ACL
- Verifica degli account configurati
- Autenticazioni a 2 fattori
- Aggiornamento firmware
- Sostituzione firmware

Monitoraggio attivo

- Censimento dei dispositivi autorizzati in LAN
- Verifica degli accessi effettuati e in corso
- Attivazione notifiche e verifica contatti
- Verifica delle autorizzazioni e delle sessioni attive sui servizi cloud

Antivirus

Qualcuno ci sta provando…

- AVG Chime
  - Sicurezza centralizzata sul router
- SentinelOne
  - Monitoraggio + assicurazione
- Samsung GAIA
  - Separazione dei privilegi
  - Tastiera virtuale
  - Trasmissioni crittografate
  - Sistema anti-malware integrato
  - Custodia delle chiavi su chip
    - Soluzione disponibile anche per le SUHD TV che possono essere utilizzate come hub IoT per il controllo degli altri dispositivi presenti nell'abitazione.

...però le cose vanno fatte bene!

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

CODE BLUE! —

That time a patient's heart procedure was interrupted by a virus scan

Securing computers has never been easy. It's especially hard in hospitals.

DAN GOODIN - 5/16/2016, 7:58 PM

Enlarge

A heart patient undergoing a medical procedure earlier this year was put at risk when misconfigured antivirus software caused a crucial lab device to hang and require a reboot before


Happy
Ransomware

Credits

Vi hanno intrattenuto

Davide Rebus Gabrini
Paolo Dal Checco

facebook.com/gabrini

facebook.com/paolo.dalchecco

twitter.com/therebus

twitter.com/forensico

it.linkedin.com/in/rebus

www.linkedin.com/in/dalchecco