

Contributo tecnico di

TG Soft
Software House
www.tgsoft.it

C.R.A.M.
CENTRO
RIEQUILIBRO
ANTI-MALWARE

Con il Patrocinio del

Clusit
Associazione Italiana
per la Sicurezza Informatica

Organizzato da

CNA
Padova


Confederazione Nazionale dell'Artigianato
e della Piccola e Media Impresa

Virus&Malware di ieri, di oggi e di domani...
Come difendere i propri dati
dai Ransomware / Crypto-Malware

Relatore: ing. Enrico Tonello
Collaborazione tecnica: Federico Girotto

Padova, 21/11/2016

Cos'è un virus/malware



Software sviluppato per:

- **danneggiare o**
- **sfruttare per propri scopi**


il computer che infetta con la capacità di diffondersi ed autoinfettare altri file/computer.

A seconda del loro **comportamento** vengono **classificati** secondo **diverse tipologie**: virus, spyware, rootkit, trojan horse, worm, backdoor, adware, fraudtool, keylogger, adware ecc. ecc...

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft
Software House
www.tgsoft.it


2




Tipologie di Malware 1/6

- Tecnicamente per **virus** si intende un programma che abbia la capacità di autoreplicarsi ed infettare altre macchine
- Non è raro vedere utilizzato erroneamente il termine «**virus**» per indicare anche altri tipi di software dannosi quali *spyware* e *adware* anche se non hanno la capacità di infettare altre macchine autonomamente. Per questo motivo si preferisce utilizzare il termine generico **Malware**.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




3



Tipologie di Malware 2/6

- **Malware**: definizione generica per software dannoso che risiede su un computer ed include tutte le sotto-categorie
- **Virus**: software autoreplicante che infetta il computer ospite e cerca di diffondersi su altri computer attaccando i file eseguibili oppure modificando il boot-sector e/o l'MBR di modo da garantirsi la presenza in memoria fin dall'avvio aumentando così la sua diffusione.
- **Spyware**: tipo di malware che risiede silenziosamente sul computer per catturare informazioni sensibili sull'utente (e.g. siti visitati, password, keyloggers, ecc.). Generalmente non si autoreplica







C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




4





Tipologie di Malware 3/6

- 


• **Rootkit:** software che garantisce l'accesso privilegiato (a livello di root) mentre usa tecniche attive per nascondere la sua presenza sfruttando a suo favore funzioni del sistema operativo eventualmente modificandole. Può anche sfruttare queste capacità stealth per nascondere altri malware o per garantirgli l'accesso al computer
- 


• **Trojan Horse (Cavallo di Troia):** programma malevolo mascherato da programma legittimo e che al momento della sua esecuzione introduce nel computer software dannoso oppure fornisce l'accesso al computer dall'esterno.
Un hacker può prendere il controllo di un computer infetto da un Trojan ed utilizzarlo per i propri scopi.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it  5





Tipologie di Malware 4/6

- 


• **Worm:** programma auto-replicante che utilizza una rete di computer per mandare copie di se stesso ad altri nodi della rete stessa, senza l'intervento dell'utente, spesso sfruttando vulnerabilità di sicurezza. A differenza dei virus, generalmente non si «attacca» ad altri programmi esistenti ma è un software autonomo e non modifica i file pre-esistenti del computer che infetta.
- 

• **Backdoors:** una backdoor è una porta di servizio aperta sul computer infetto per permettere l'infiltrazione da parte di terze parti, così da autenticarsi nel computer senza possedere le credenziali necessarie, rimanendo non identificato.


C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it  6



Tipologie di Malware 5/6




- **Adware:** sono malware che visualizzano finestre pubblicitarie, modificano la home page e il motore di ricerca del browser. Questa tipologia di malware non è particolarmente pericolosa, ma molto invasiva.




- **Fraudtools:** Potrebbero essere classificati come adware. Sono principalmente programmi che si spacciano per antivirus facendo credere all'utente di essere infetto con messaggi allarmistici, cercando di far comprare una licenza completa del falso antivirus. In realtà si tratta di un trucco per rubare numeri di carte di credito. Ancora attivi su AndroidTM


C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




7



Tipologie di Malware 6/6




- **Keylogger:** sotto tipologia di trojan e spyware, ha lo scopo di rubare informazioni riservate come login e password. Il loro obiettivo è quello di catturare ogni tasto premuto sul computer della vittima e di inviarlo ad un server C&C server remoto di controllo.



- **Dialer:** sotto tipologia dei trojan, ha lo scopo di connettere il computer ad internet attraverso un accesso remoto a pagamento. Il dialer necessita di un modem collegato al computer, di solito si collega a numeri telefonici che iniziano per 899. L'avvento dell'ADSL sta comportando l'estinzione di questa tipologia.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



8



Un po' di storia...: Pakistan Brain 1/4


Il **Pakistan Brain** è il più vecchio virus conosciuto, fu scoperto nel 1986, infettava i sistemi PC-DOS. Gli autori sono 2 fratelli pakistani: **Amjad Farooq Alvi** e **Basit Farooq Alvi**. Avevano realizzato il virus per proteggere un loro software dalla pirateria. Il virus infettava il boot sector dei floppy disk. Attualmente i 2 fratelli vivono ancora a Lahore in Pakistan, hanno fondato la società «Brain Telecommunication Ltd» e si occupano di Internet Service Provider.

Welcome to the Dungeon
 (c) 1986 Basit & Amjad (pvt) Ltd.
 BRAIN COMPUTER SERVICES
 730 NIZAB BLOCK ALLAMA IQBAL TOWN
 LAHORE-PAKISTAN PHONE
 :430791,443248,280530.
 Beware of this VIRUS....
 Contact us for vaccination.....
 \$#@%\$@!!



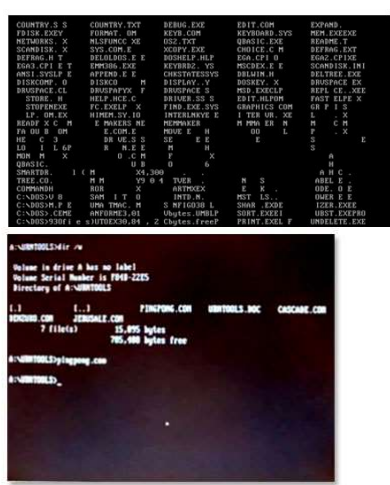
C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


9




Un po' di storia... 2/4

- 1987: *Cascade (file), Jerusalem (file)*
- 1988: *Stoned (boot sector), Ping Pong (scoperto all'università di Torino)*
- 1989: *Dark Avenger (file), AIDS (file)*
- 1990: *Form (boot sector), Flip (file) Ambulance (file), Itavir (file)*
- 1991: *Michelangelo (boot sector)*
- 1992: *November17th (file), Invisible_Man (multipartito)*
- 1993: *Bloody_Warrior (file), RebelBase (file), Italian Boy (file)*
- 1994: *B1 (boot sector), Junkie.1027 (multipartito), Berlusconi (file)*
- 1995: *AntiEXE (boot sector), WM/Concept (macro virus)*



C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


10



Un po' di storia... 3/4

- 1998: **Win32.CIH** (file, bios)
- 1999: **Happy99, Melissa, Kak** (worm)
- 2000: **Win32.MTX** (file), **LoveLetter** (worm)
- 2001: **Nimda** (worm)
- 2002: **MyLife** (worm)
- 2003: **Blaster, SoBig, Swen, Sober** (worm)
- 2004: **Beagle, MyDoom, NetSky, Sasser** (worm), **Vundo** (trojan)
- 2005: **Zlob** (trojan)
- 2006: **Brontok, Stration** (worm), **Gromozon-LinkOptimizer** (rootkit)
- 2007: **Storm** (worm), **Zbot-Zeus** (trojan-banker), **Rustock** (rootkit)
- 2008: **Sinowal** (boot sector), **Conficker** (worm), **Koobface** (worm), **FraudTool, TDL2** (rootkit)
- 2009: **TDL3** (rootkit)
- 2010: **Stuxnet** (trojan-worm), **TDL4** (rootkit), **ZeroAccess** (trojan), **Safetad** (ransomware), **Carberp** (trojan banker)
- 2011: **Morto** (worm), **Duqu** (worm), **FakeGdF** (ransomware)
- 2012: **DorkBot** (worm), **ROP** (rootkit)
- 2013: **ACCDFISA** (ransomware)

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it





Un po' di storia...: payload 4/4

```
Volume in drive C is DOS
Volume Serial Number is 1a34-5384
Directory of C:\DOS

.<DIR>          20/01/93    10:28
.<DIR>          20/01/93    10:28
COUNTRY  SVS      17059 09/04/91    5:00
EGA      SVS      4885 09/04/91    3:00
FORMAT  COM      32911 09/04/91    3:00
KEYB    COM      14986 09/04/91    3:00
KEYBOARD SVS      34937 09/04/91    3:00
NLSFUNC  EXE      2052 09/04/91    3:00
DISPLAY  SVS      15792 09/04/91    3:00
EGA      COM      58973 09/04/91    3:00
HIMEM   SVS      11552 09/04/91    5:00
```



```
Happy Birthday KAORI!
Dedicato a tutte le meravigliose ragazze giapponesi
(C) BitLabs (The RebelBase) 1993, N. Italy.
```

```
I'm the invisible man,
I'm the invisible man,
Incredible how you can
See right through me.

I'm the invisible man,
I'm the invisible man,
It's criminal how I can
See right through you.
```

ARIANNA VIRUS

```
*****
ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accidentally %$@Q$%
yourself over; again, that's %$@Q$% yourself over. No, it cannot
be: YES, it CAN be, a $!T$ has infected your system. Now what do
you have to say about that? %$@Q$%!! How? %$@Q$% with this one and
remember, there is NO cure for
```

AIDS

```
DISK DESTROYER - A SOURCE OF PAIN
I have just DESTROYED the FAT on your Disk !!
However, I have a copy in ROM, and I'm giving you a last chance
to restore your precious data.
WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER !!
Your Data depends on a game of JACKPOT

CASINO DE MALTE JACKPOT


[ ] [ ] [ ]
CREDITS : 3

!!! = Your Disk
??? = My Phone No.

ANY KEY TO PLAY
```

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it







Malware moderni

Il trend registrato negli ultimi anni è lo sviluppo di malware con lo scopo di avere un forte ritorno economico:

- Trojan Spammer
- Trojan Clicker
- FraudTool
- Trojan Banker
- Ransomware (1°, 2° e 3° generazione)





C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



FraudTool: le truffe dei falsi antivirus 1/3




#	Vendor	Type	Location	Threat Level
1	Trojan-Cookie.Win32.Agent.gm	Malware	C:\Documents and Se...	Medium
2	GayCodec.LookAlert	Malware	C:\WINDOWS\Syste...	Medium
3	webSearch.Win32	Malware	C:\WINDOWS\Syste...	Medium
4	PORN.perversion.RJO	Malware	C:\WINDOWS\Syste...	Medium
5	Wirus.Win32.Epicode.ak	Viruses	E:\WINDOWS\Syst...	High
6	Email-Worm.Win32.NetSky.q	Network War...	C:\WINDOWS\Syst...	High
7	Net-Worm.Win32.Mytob.t	Network Wor...	C:\WINDOWS\Syst...	High
8	Net-Worm.Win32.DipNet.d	Network Wor...	C:\WINDOWS\Syst...	High
9	Trojan-Downloader.JS.Multi.ca	Trojan Programs	C:\WINDOWS\Syste...	Medium
10	Backdoor.Win32.Agent.ich	Malware	C:\WINDOWS\Syste...	Medium



Registration required
There were found 10 dangerous viruses on your computer. It is strongly recommended to remove them ASAP.

Vulnerability	Alert level
Backdoor.Win32.Agent.ich	Medium
Email-Worm.Win32.NetSky.q	High
GayCodec.LookAlert	Medium
Net-Worm.Win32.DipNet.d	High
Net-Worm.Win32.Mytob.t	High
PORN.perversion.RJO	Medium
Trojan-Cookie.Win32.Agent.gm	Medium

Activate your copy



C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

FraudTool: le truffe dei falsi antivirus 2/3

The image shows two screenshots of a fraudulent website. The left screenshot displays a 'Customize Your Order' page with a table of options:

Option	Value	Discount	Subtotal
Subscription length	Lifetime	\$51.00 (\$13.04 (26%))	148.00
Support Service	Premium	\$22.00 (\$11.00 (50%))	118.00

The total price is \$79.50, with a savings of \$24.04. The right screenshot shows an 'Order Form' with fields for personal and payment information, including a 'Submit My Order' button.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft Software House 15 www.tgsoft.it

FraudTool: le truffe dei falsi antivirus 3/3

The image shows a Windows desktop with several windows. The primary focus is a 'Security Tool' warning dialog box that reads: 'WARNING! 33 infections found!!! Last scan detected malicious programs (11), viruses (11), adware (3), spyware (4), tracking cookies (4). These harmful programs causes: System crash, Permanent Data loss, System startup failures, System slowdowns, Internet connection loss, Infecting other computers on your network.' Below the list are buttons for 'Remove all threats now', 'Continue unprotected', and 'Save Report'. In the background, a 'Windows Recovery' window displays a 'Critical Hard Disk Drive Error' message: 'Critical hard disk drive error has been detected! Windows Recovery detected a bad sector on your hard disk drive. This error may cause the following problems: Data corruption and loss, Hard drive inaccessibility, System errors and failures. It is strongly recommended that you fix the detected problem immediately. Please run a full system scan and fix errors.' Buttons for 'Fix problem', 'Cancel', 'Fix Errors', and 'Advanced Problem Solving' are visible.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft Software House 16 www.tgsoft.it




Frodi bancarie: tecniche utilizzate



- **Phishing:** si intende una tecnica attraverso la quale un soggetto malintenzionato (chiamato *phisher*), riesce a raccogliere dati personali di accesso, tramite tecniche di ingegneria sociale che negli anni si sono fatte sempre più raffinate.
- **Trojan Banker:** malware che sono in grado di rubare le credenziali di accesso della propria banca, modificando le schermate di login di alcuni dei più diffusi siti di *home banking*.

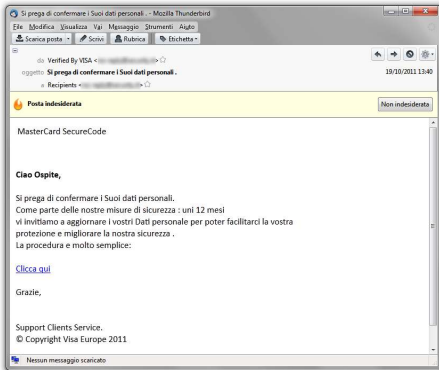
Scopo: rubare soldi dal conto corrente eseguendo bonifici su conti esteri.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it





Frodi bancarie: Phishing 1/2

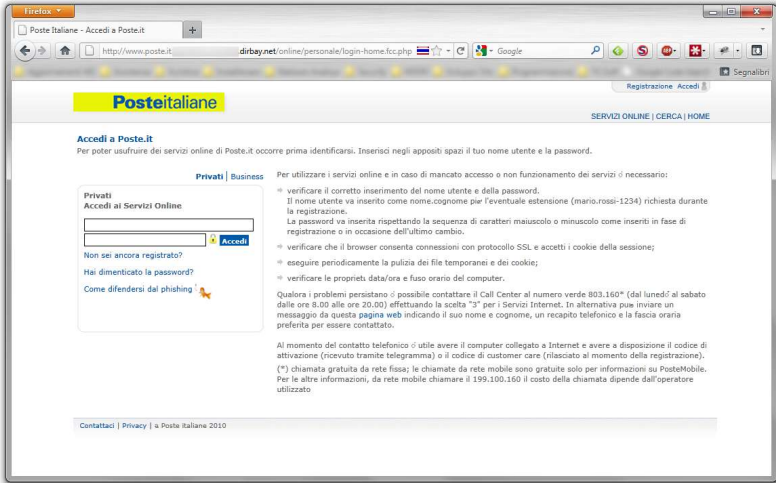
La tecnica è quella di inviare email relative al proprio conto corrente, nelle quali si invita il destinatario ad accedere immediatamente al proprio conto, per verificare i suoi dati oppure per convalidare vincite o premi che il proprio istituto ha deciso di erogare.



C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



Frodi bancarie: Phishing 2/2



C.R.A.M.
C.R.A.M. S.p.A. - MALWARE

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft
Software House
www.tgsoft.it 19

Frodi bancarie: Trojan Banker 1/3

- **Zbot (Zeus - Citadel):** file eseguibile che infetta il pc, metodo di diffusione siti infetti o installato da altri malware
- **Sinowal:** rootkit che infetta il Master Boot Record, metodo di diffusione siti infetti o installato da altri malware
- **Trojan.Win32.Banker:** file eseguibile che infetta il computer, metodo di diffusione via email
- **Carberp:** file eseguibile che infetta il pc, metodo di diffusione siti infetti o installato da altri malware
- **SpyEye:** file eseguibile che infetta il pc, metodo di diffusione siti infetti o installato da altri malware
- **Gataka:** file eseguibile che infetta il pc, metodo di diffusione siti infetti o installato da altri malware
- **Dridex – Retefe - TrickyBot**

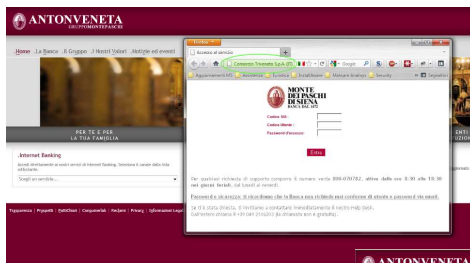
C.R.A.M.
C.R.A.M. S.p.A. - MALWARE

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

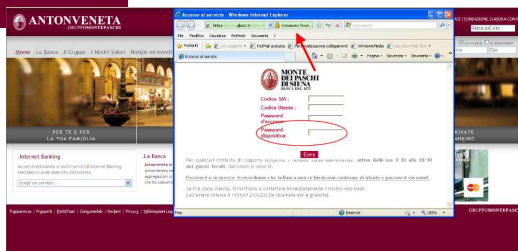
TG Soft
Software House
www.tgsoft.it 20



Frodi bancarie: Trojan Banker 2/3




Il trojan Banker modifica (lato client) la pagina di login della banca, richiedendo anche la password dispositiva. Gli autori del malware possono accedere al conto online della vittima e eseguire bonifici su conti esteri a sua insaputa.

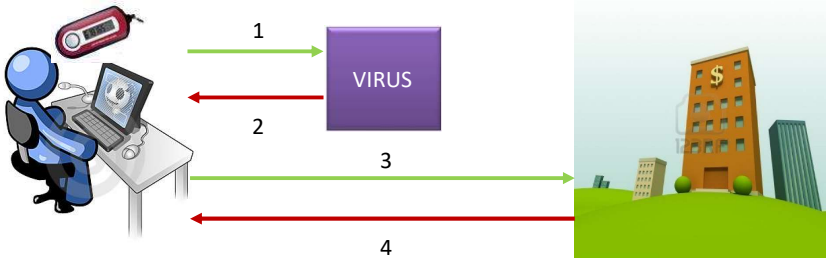


Frodi bancarie: Trojan Banker 3/3





C.R.A.M.
C.R.A.M. di T.G. Soft
SOFTWARE HOUSE

Frodi bancarie: Carberp e OTP



1. L'utente invia le sue credenziali di accesso alla banca: login, password, Paskey Internet banking (OTP = One Time Password).
2. Le credenziali vengono intercettate dal virus, che non le inoltra alla banca, ma le memorizza. Il virus visualizza un falso messaggio di inserimento errato di login/password
3. L'utente re-inserisce login/password e un nuovo valore della Paskey Internet banking.
4. La Banca conferma la correttezza dei dati inseriti e l'utente accede al suo conto online

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


TG Soft
Software House
www.tgsoft.it 23


C.R.A.M.
C.R.A.M. di T.G. Soft
SOFTWARE HOUSE

Vir.IT Safe Browser


Tecnologia che evidenzia la compromissione del Browser e segnala la possibilità del furto delle proprie credenziali bancarie e non solo...



**Simulazione di un attacco da Trojan.Banker
dal vivo e segnalazione della
compromissione del sistema, in
particolare, per l'esecuzione di attività di
Home Banking**

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



TG Soft
Software House
www.tgsoft.it




Maggiori cause di infezione

- Navigazione su siti non raccomandabili
- Navigazione su siti attendibili ma che sono stati compromessi (infettati)
- Email con allegati infetti o link su siti infetti
- Social Network
- Sistema operativo non aggiornato con le ultime patch di sicurezza
- Chiavette usb di fonte non sicura
- Attacchi da parte di nodi già infetti presenti su una rete
- Utilizzo di password banali

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




25



Navigazione su siti non sicuri

- Molti siti poco attendibili includono nelle loro pagine script (principalmente **JavaScript o Flash**) che sono in grado di scaricare ed eseguire codice sul computer di chi lo sta visitando. Questo può essere tanto più dannoso quanto più alto è il livello di privilegi con il quale è eseguito il browser (ad esempio Administrator).
- Exploit kit: **Black Hole, Cool Exploit** (sfruttano vulnerabilità)
- Molto spesso questo tipo di siti include **pubblicità fraudolente**, ingannevoli o banner pubblicitari che, se cliccati, portano ad altri siti infetti o al download di software dannoso

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




26



C.R.A.M.
C.R.A.M. di TG Soft
SOFTWARE HOUSE

Black Hole: Vulnerabilità utilizzate

Vulnerabilità	Descrizione	Vulnerabilità	Descrizione
CVE-2013-0422	Java	CVE-2010-1423	Java
CVE-2012-4681	Java	CVE-2010-0886	Java
CVE-2012-1889	Windows	CVE-2010-0842	Java
CVE-2012-1723	Java	CVE-2010-0840	Java
CVE-2012-0507	Java	CVE-2010-0188	Adobe Reader
CVE-2011-3544	Java	CVE-2009-1671	Java
CVE-2011-2110	Adobe Flash Player	CVE-2009-0927	Adobe Reader
CVE-2011-0611	Adobe Flash Player	CVE-2008-2992	Adobe Reader
CVE-2010-3552	Java	CVE-2007-5659	Adobe Reader
CVE-2010-1885	Windows	CVE-2006-0003	Internet Explorer

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


TG Soft
Software House
www.tgsoft.it 27


C.R.A.M.
C.R.A.M. di TG Soft
SOFTWARE HOUSE


Malware dei Social Network 1/4

Negli ultimi anni, i virus writer hanno iniziato ad utilizzare i social network per diffondere i malware. I social più utilizzati sono:

- Facebook
- Skype
- Twitter

facebook Ricerca

questo è davvero scioccante..)




Il video dell'esecuzione di bin laded

www.facebook.com

guarda cosa fanno questi soldati ad Osama!

51 minuti fa · Mi piace · Commenta · Condividi · Vedi dettagli amicizia

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


TG Soft
Software House
www.tgsoft.it 28

Malware dei Social Network: facebook 2/4

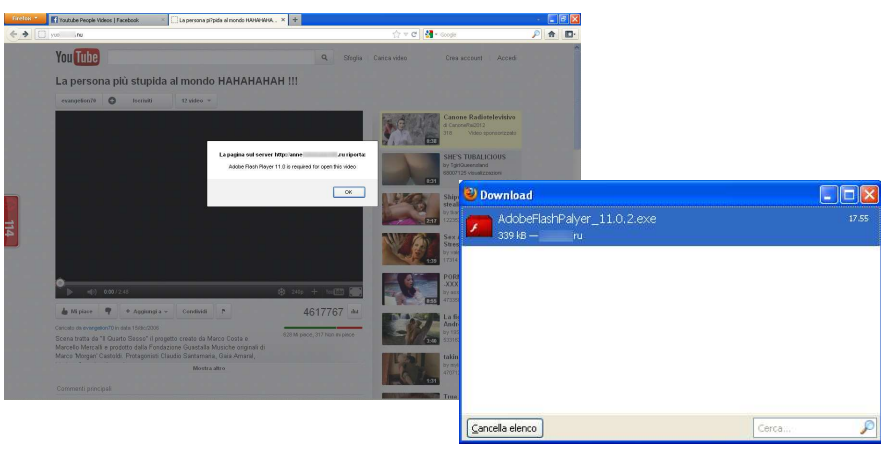


The screenshot shows a Facebook profile page. The user's name is partially visible as '... Università degli Studi di Padova'. The profile picture is a red and black image. The main content area shows a post with a link to 'TG Soft Official Website - AntiVirus - AntiSpyware - AntiMalware - Personal Firewall'. The link text is: 'http://www.tgsoft.it TG Soft Official Website - AntiVirus - AntiSpyware - AntiMalware - Personal Firewall'. Below the link, there is a small image of a person and some text: 'TG Soft Software House'. The post has 14 likes and 1 comment. The comment says: 'M piace - Commenta - Condividi - 10 dicembre 2011 alle ore 15:00'. The right sidebar shows 'Persone che potresti conoscere' and 'Sponsorizzate'.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft
Software House
www.tgsoft.it 29

Malware dei Social Network: facebook 3/4




The screenshot shows a YouTube video player. The video title is 'La persona più stupida al mondo HAHHAHAH !!!'. The video player is showing a black screen with a white error message: 'La pagina sul server http://www... non risponde. Adobe Flash Player 11.0.2 è richiesto for open this video'. A download window is open in the foreground, showing the file 'AdobeFlashPalyer_11.0.2.exe' with a size of 339 KB and a download time of 17:55. The download window has a 'Cancella elenco' button and a search field.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft
Software House
www.tgsoft.it 30


Malware dei Social Network: Skype 4/4






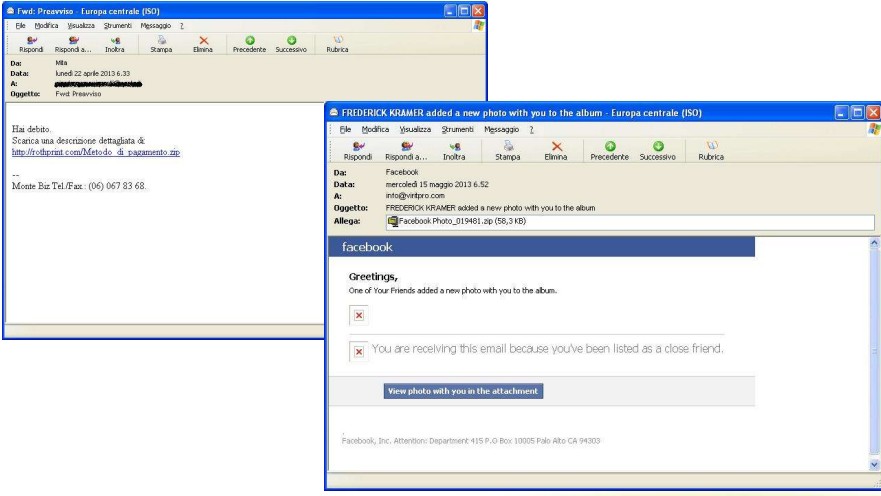
The screenshot shows a Skype chat window with a list of messages. Each message contains the text "mi piace molto questa foto di te" followed by a URL and a timestamp. The URLs are variations of "http://www.ly/4Lq?eg=gantony73" and "http://www.ly/117Mw?7id=gantony73". The timestamps range from 11:59 to 17:06. The chat window is titled "Skype" and shows a contact list on the left.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




Virus/Malware dell'email... 1/2






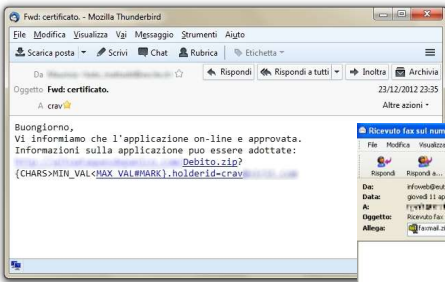
The screenshot shows an email client window with a message from Facebook. The subject line is "FRIDERICK KRAMFR added a new photo with you to the album - Europa centrale (ISO)". The message body contains a greeting and a link to "View photo with you in the attachment". The email header shows the date as "mercoledì 15 maggio 2013 6:52" and the sender as "FRIDERICK KRAMFR".

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

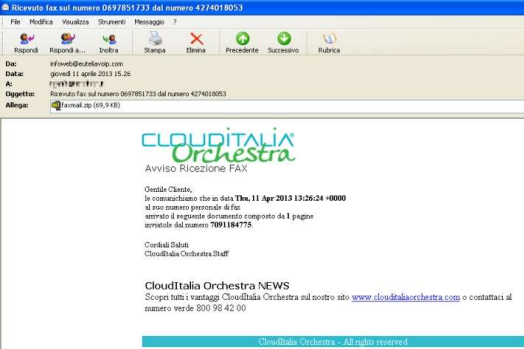


Virus/Malware dell'email... 2/2





Buongiorno,
Vi informiamo che l'applicazione on-line è approvata.
Informazioni sulla applicazione puo essere adottate:
debito.zip?
{CHARS>MIN_VAL<MAX_VAL#MARK}.holderId=crav



Ricevuto fax sul numero 0977851733 dal numero 4274018053

Da: info@clouditalia.com
Data: giovedì 11 aprile 2013 15:26
A: [redacted]
Oggetto: Ricevuto fax sul numero 0977851733 dal numero 4274018053
Allegati: [redacted].zip (19,9 KB)

CLOUDITALIA Orchestra
Avviso Ricezione FAX


Onesta Cliente,
In data odierna che si data 11 Apr 2013 13:26:24 +0800
il suo numero personale di fax
arrivato il seguente documento composto da 1 pagina
arrivato dal numero 1901184775.

CloudItalia Staff
CloudItalia Orchestra Staff


CloudItalia Orchestra NEWS
Scopri tutti i vantaggi CloudItalia Orchestra sul nostro sito www.clouditaliaorchestra.com o contattaci al numero verde 800 99 42 00

CloudItalia Orchestra - All rights reserved

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



33


Sistema operativo non aggiornato



- Le patch rilasciate dalle software house sono, in molte occasioni, volte a risolvere bug o falle di sicurezza, soprattutto nel caso di quelle rilasciate da Microsoft per i propri sistemi operativi.
- È molto importante che i computer siano impostati per scaricare e installare le patch tramite Windows Update in modo automatico non appena sono rese disponibili da Microsoft (generalmente l'8 di ogni mese)
- Se alcuni computer critici per l'ambiente di produzione non possono essere interrotti in orario lavorativo è comunque importante impostare il download automatico delle patch per poi procedere con l'installazione manuale quando è possibile riavviarli
- L'aggiornamento automatico dei computer è importante per due motivi:
 1. Le patch di sicurezza chiudono vulnerabilità che possono essere sfruttate da malware per attaccare con successo il computer esposto
 2. Una volta rilasciata la patch i virus writer, attraverso tecniche di reverse engineering, possono scrivere malware in grado di sfruttare tale vulnerabilità prima sconosciuta ed in questo modo tutti i computer non patchati saranno vulnerabili all'ondata di nuovi malware

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



34




Vulnerabilità 1/2

Anno	Malware	Tipo	Vulnerabilità
1999	Happy99, Kak	email	CVE-1999-0668 (Internet Explorer 5.0, Outlook Express)
2001	Nimda	email, lan, web server	CVE-2000-0884 (Microsoft IIS 4.0 e 5.0) - CVE-2001-0154 (Internet Explorer 5.5 HTML e-mail)
2003	Blaster	DCOM RPC TCP 135	CVE-2003-0352 (buffer overflow in DCOM RPC Windows NT,2000,XP, Server 2003)
2003	Swen	Email, kaza, irc	CVE-2001-0154
2004	Sasser	MS04-11	CVE-2003-0533 (buffer overflow in LSASS Windows 98, ME, NT, 2000, XP, 2003 e Microsoft NetMeeting)
2008	Conficker	MS08-067 - MS08-068 - MS09-101 - chiavette usb - lan	CVE-2008-4250 (Server Service Vulnerability Windows 2000,XP,2003,VISTA,Server 2008). KB95864, KB957097 e KB958687

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




35



Vulnerabilità 2/2

Anno	Malware	Tipo	Vulnerabilità
2009	TDL3	rootkit	MS10-015 / KB977165 (Windows 2000, XP, 2003, Vista, 2008)
2010	Stuxnet	Rootkit, chiavette usb, LAN, plc	CVE-2010-2568 (MS10-046 LNK vulnerability) CVE-2010-2729 (MS10-061 print spooler service esecuzione codice) CVE-2010-2743 (MS10-073 kernel mode privilegi) CVE-2010-3338 (MS10-092 task scheduler privilegi) CVE-2008-4250 (MS08-067) Windows XP, 2003, VISTA, 2008, 7
2010	TDL4	rootkit	CVE-2010-3338 (MS10-092 task scheduler privilegi)
2011	Duqu	Rootkit, usb, LAN, plc	CVE-2011-3402 (MS11-087 doc file)
2012	Dorkbot	Worm (skype, facebook)	CVE-2012-4681 (Java SE 7 Update 6)
2013	Black Hole	Exploit kit	CVE-2013-0422 (Java SE 7 Update 11)

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



36




Chiavette USB come veicolo di infezione

- Con la scomparsa dei floppy disk e l'avvento di internet si pensava che il maggiore veicolo di trasmissione di virus informatici degli anni '90 fosse stato sconfitto
- Con la diffusione delle chiavette e dei dispositivi di archiviazione rimovibili USB a basso costo ed alta capacità, si è tornati «nel passato», con la differenza che le chiavette USB sono un mezzo di diffusione molto più potente dei floppy disk di qualche anno fa. La maggiore potenza di diffusione risiede soprattutto nel metodo di utilizzo di queste ultime rispetto ai floppy disk
- Un virus presente in un floppy disk doveva essere eseguito lanciando il file infetto o facendo il boot da un floppy con il boot sector infetto
- Un virus presente in una chiavetta USB riesce ad eseguirsi automaticamente tramite la funzione di autorun di Windows per i dispositivi rimovibili e i dischi CD/DVD sfruttando le funzionalità del file autorun.inf presente all'interno del dispositivo collegato

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



37



Condivisione – Password utenti


Condivisione

- Molti malware sfruttano le condivisioni per infettare i computer della rete lan
- Condividere solamente cartelle dati
- Non condividere **MAI** tutto il disco

Password degli utenti

- Tutti gli utenti devono avere una password
- Usare password complesse
- Disabilitare il desktop remoto agli utenti esterni

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



38



Come mi difendo dai Malware

- Antivirus sempre aggiornato e installato su tutti i computer (PC e SERVER) della rete
- Aggiornamenti di Windows Update
- Aggiornare: Java, Adobe Reader, Adobe Flash Player
- Chiavette usb/unità mappate: disabilitare l'autorun.inf (<http://support.microsoft.com/kb/967715>)
- Adottare delle policy: password complesse (non banali), divieto di utilizzare chiavette usb



C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



39



Ransomware «I malware che ti ricattano!!!»



TG Soft Software House www.tgsoft.it





Ransomware: cosa sono ?

Con il termine **Ransomware** definiamo tutti quei programmi o software che bloccano l'accesso al computer o ai file di documenti chiedendo un riscatto in denaro per riaverne l'accesso.

Esempi di Ransomware:


- Trojan.Win32.FakeGdF (Ransomware di 1° generazione)
- **Crypto-Malware** (Ransomware di 2° generazione)

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

FakeGDF: computer sotto ricatto 1/3

- Emulazione di siti pseudo istituzionali
- Panico nell'utente
- accuse di reati gravi
- Facile guadagno
- Non rintracciabile



The screenshot shows a ransomware message from the Guardia di Finanza. It states that the system is blocked and demands a 100 euro ransom. It provides instructions for payment via Ukash or Paysafecard, along with contact information for the ransomware authors.


Per togliere il bloccaggio devi pagare una multa di 100 euro. Hai due seguenti varianti di pagamento:

- 1) Effettuare il pagamento tramite Ukash. Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).
- 2) Effettuare il pagamento tramite i Paysafecard: Per questo inserisci per favore il numero ricevuto (nel caso di necessità insieme con la password) nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



C.R.A.M. C.R.I.M.I.N.A.L.E P.A.T.R.I.S.T.A.N.T.E

FakeGDF: computer sotto ricatto 2/3

- Siae
- Polizia di Stato
- Altre istituzioni



il computer è stato bloccato

Sul computer sono stati individuati dei brani musicali scaricati illegalmente (piratati).

Scaricando, questi brani musicali sono stati riprodotti, comportando un reato ai sensi della Sezione 106 del Copyright Act, il download di canzoni protette da copyright, tramite Internet o reti di condivisione di file musicali, è illegale ed è soggetto ad una multa o la reclusione per una pena fino a 3 anni, in conformità alla Sezione 106 del Copyright Act. Inoltre, il possesso dei brani musicali piratati (legalmente è possibile il reo) è punito come il delitto penale e può anche portare alla confisca del computer con cui i file sono stati scaricati.

Il vostro Indirizzo IP: 82.56.187.93

Il vostro Hostname: host93-187-dynamic.56-92-c.net.it.telecomitalia.it

Potete facilmente essere identificati tramite la rilevazione del vostro indirizzo IP e del hostname ad esso associato.

Il materiale pirata è stato offeso ed è stato spostato in una cartella protetta per prevenire ulteriori danni.

Per sbloccare il computer e per evitare altre conseguenze giuridiche, siete obbligati a pagare una tassa di riscatto di 100 Euro. La somma è pagabile attraverso il nostro partner per pagamenti di Paysafecard. Dopo il pagamento, il computer sarà sbloccato automaticamente.

Il mancato rispetto di questa richiesta potrebbe comportare implicazioni penali e possibilità di detenzione.

Per eseguire il pagamento, inserite il codice Paysafecard acquistato nel campo bonifico; selezionate il valore del codice e quindi premete il pulsante "Invia".

SIAE è legittimata dalla legge - ed è in stretto contatto con i legislatori e la Polizia.



POLIZIA DI STATO

ATTENZIONE!

Per motivi di sicurezza il suo sistema Windows è stato bloccato.

In seguito a visite a siti pornografici od infestati da virus, il computer è arrivato ad un livello critico oltre il quale potrebbe non funzionare più, e tutti i dati verranno persi. Per avere possibilità di recupero del sistema deve installare un programma aggiuntivo di sicurezza.

Questo programma a pagamento, studiato per i sistemi particolarmente infestati, protegge completamente il sistema dai virus e dai programmi maligni, stabilizza il sistema del suo computer e previene la perdita dei dati.

Disponibile nelle tue vicinanze

paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso benzinere edicola, nei tabacchi anche nei negozi Siae e Pagine Gialle.

Sceglia la modalità di pagamento desiderata

Ukash DISPONIBILE ✓

paysafecard DISPONIBILE ✓

Per migliorare (per quarant'ore) il suo sistema, metta il codice per trasferire 100 Euro nei sistemi PaysafeCard o Ukash. Il codice può essere acquistato presso quasi tutti i fornitori di benzina oppure nelle tabaccherie. Tali codici si trovano in vendita anche presso qualsiasi locale dove si vendono le carte per ricaricare il cellulare.

Subito dopo la digitazione del codice e dopo la sua verifica, il suo computer sarà completamente aggiornato e protetto. Tutti i virus ed i cavalli di troia saranno eliminati.





43

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

C.R.A.M. C.R.I.M.I.N.A.L.E P.A.T.R.I.S.T.A.N.T.E

Ransomware: non solo in Italia 3/3




BUNDESPOLIZEI

E "l'attività illegale trovata!"

Attenzione utenti!

Le operazioni su attività illegali sono state rilevate sul computer. L'utente di un indirizzo IP di questo computer ("95.232.191.78"). Ha usato per guardare video carattere pornografico, pedopornografico, bestialità, e scene di abusi sui minori. Oltre al vostro e-mail personale sono stati trovati, e-mail inviate come spam, e trovato messaggi di posta elettronica con una natura terroristica. Il sistema operativo è stato bloccato per questa violazione. Le vostre azioni sono considerate illegali in Italia, l'Unione europea. Vi facciamo un richiamo ufficiale e definitiva.

I tuoi dati: IP: 95.232.191.78 Browser: OS: Windows XP Country: ITALY City: PADOVA ISP: TELECOM ITALIA WIRELINE SERVICES

Per sbloccare il computer, è necessario pagare una penale di € 100,00. Garantiamo discrezione e sicurezza delle informazioni al ricevimento del pagamento della multa. Qui ci sono modalità di pagamento:

1) Pagamento "Ukash": È necessario inserire un codice acquistato nella finestra che appare sullo schermo. Dopo aver inserito un codice valido, fare clic su OK. (Se si dispone di più codici, inserirli uno dopo l'altro). È possibile acquistare voucher "Ukash" centinaia di migliaia di località in tutto il mondo, distributori di benzina, chioschi, bancomat, così come acquistare on-line.

2) Pagamento "Paysafecard": È necessario inserire un codice acquistato nella finestra che appare sullo schermo. Dopo aver inserito un codice valido, fare clic su OK. (Se si dispone di più codici, inserirli uno dopo l'altro). "Paysafecard", così come Ukash possono essere acquistati in diversi punti vendita in tutto il mondo.

Se il sistema genera un errore dopo aver inserito il codice è necessario inviare il codice tramite e-mail - (info@stopkriminal.net).

Ci sono innumerevoli modi per ottenere Ukash, ad esempio nei chioschi, tramite bancomat, online o tramite e-borsellino (dorso elettronico). Di seguito è riportato un elenco che indica dove si acquistano Ukash nel vostro paese:

stazioni - ora disponibile anche nelle seguenti stazioni: Agip, Esso, OMV Q1 e Vestfalia

AVIA **ESSO** **OMV** **Q1** **Westfalia**

epay - Ukash acquistare a migliaia di supermercati o call-center vede questo logo

paysafecard
pay cash, pay safe.





44

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


C.R.A.M.
C.R.A.M. - C.R.A.M. - C.R.A.M.

Computer sotto ricatto: documenti CIFRATI

WARNING INFORMATION MESSAGE

YOUR COMPUTER IS BLOCKED.
All your documents, text files and databases are securely encrypted with AES 256.

You can unlock PC and files by paying a fine of 200 USD (USA and Canada) / 300 USD (via Western Union to other Countries)

You can choose different payment methods:

1. With MoneyPak prepaid code in amount of 300 USD.
2. With MoneyGram express code in amount of 200 USD.
3. With Western Union Transfer in amount of 300 USD.*

* If you want to pay with Western union you may do request payment information by email payandbeunlocked@yahoo.com

STEP 1: If files are important to you and you are ready to pay then buy prepaid code, that you choose, at the nearest store.

STEP 2: Select payment method then enter your code and your valid email address in the fields below. Then click PAY and you will be prompted to enter the unlock code. OR Send an e-mail at PAYANDBEUNLOCKED@YAHOO.COM. Indicate your ID in the message title and provide prepaid code.

STEP 3: Check your e-mail. In 24 hours we will send your Unlock code once payment is verified. Then enter your unlock code that you received by email from us and click UNLOCK. Your computer will roll back to the ordinary state.

WARNING!!: You have 72 hours for pay. As soon as 72 hours elapses, the possibility to pay the fine expires, and your files will be securely erased with U.S. DoD S220.22-M(EE) wipe algorithm.

Setting ID...OK
YOUR ID: 3551
Collecting data...OK
Uploading status...100%
Tracing IP from database...OK
Caught IP: 151.51.143.252
Sending GEO location...OK
Status:
Waiting for payment

Q: How can I make sure that you can really decipher my files?
A: You can send one opened file on email PAYANDBEUNLOCKED@YAHOO.COM (Indicate your ID and IP address in the message title), in the response message you receive the deciphered file.

Q: What if I don't have possibility to purchase prepaid code?
A: You can send money in amount of 300 USD by Western Union as alternative option.



MoneyGram Express Email PAY

MONEYGRAM MONEYPAK

Select a payment method then enter your valid email address also prepaid code then click PAY button. OR send code and your ID to email address payandbeunlocked@yahoo.com

Q: Where can I purchase a MoneyPak?
A: MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Wal-Mart, Walgreens, CVS/Pharmacy, Rite Aid, Kmart, Kroger and Meijer.

Q: Where can I purchase a MoneyGram?
A: MoneyGram can be purchased at thousands of stores nationwide, including major retailers such as Carrefour, Sainsbury, CVS/Pharmacy, Sainsbury, Sainsbury.


Q: How do I buy a MoneyPak at the store?
A: Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.



Think you're locked?

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


TG Soft
Software House
www.tgsoft.it 45


C.R.A.M.
C.R.A.M. - C.R.A.M. - C.R.A.M.


Ransomware di 2° Generazione alias Crypto-Malware!

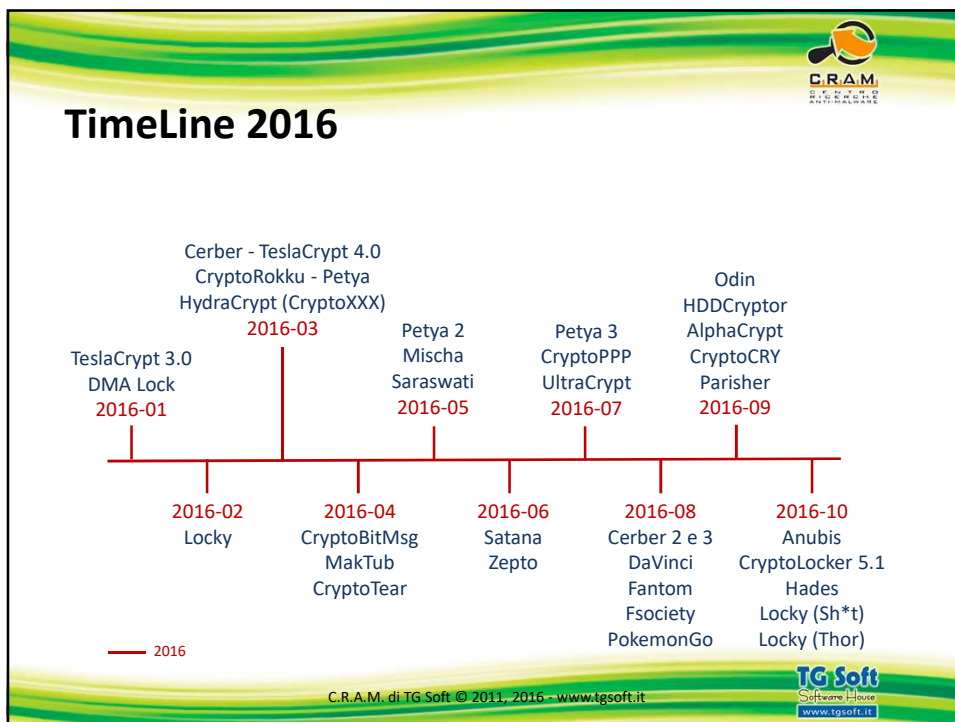
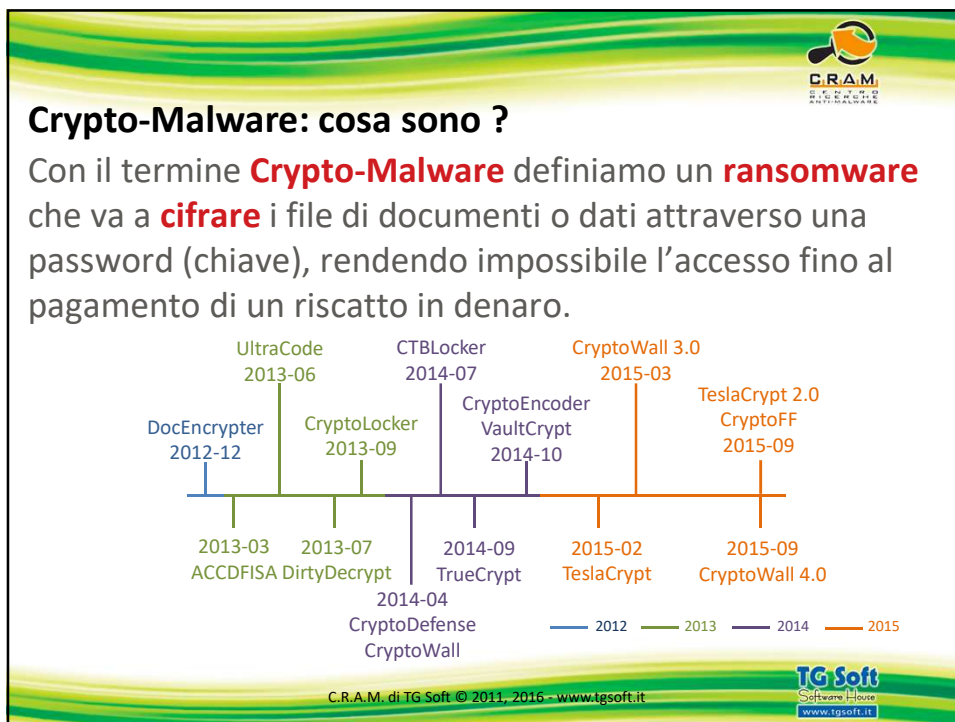
Malware che cifrano i file di dati di PC e SERVER e richiedono un riscatto in denaro per decifrarli / de-crittografarli.


Il riscatto richiesto è generalmente in BIT-COIN da pagare attraverso il Dark/Deep WEB (rete Tor-Onion) su conti anonimi e difficilmente rintracciabili.

CryptoLocker, CryptoWall, TeslaCrypt, HydraCrypt, TorrentLocker, CryptoLocky... etc.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


TG Soft
Software House
www.tgsoft.it



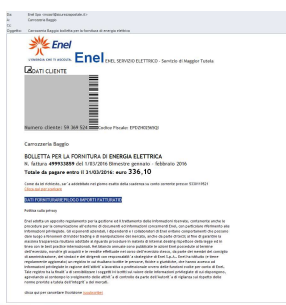


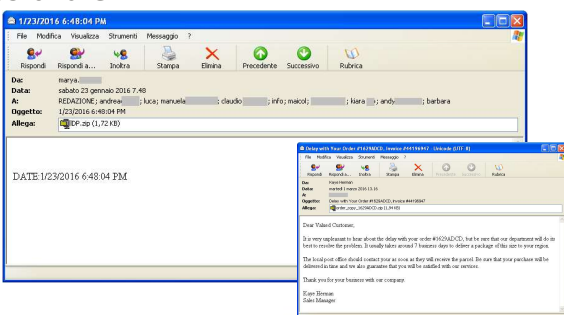
Metodo di diffusione

- via email (ingegneria sociale)
- siti infettati (utilizzo di vulnerabilità)
- altri malware: SathurBot - HydraBot
- in bundle con altri software


TeslaCrypt 3.0


- 4000 account SMTP compromessi
- 45 milioni di indirizzi email






C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




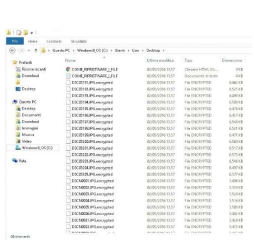



CryptoLocker - TorrentLocker

- anno: 2013 settembre
- estensione: .encrypted
- algoritmo: AES
- riscatto: 300/600 euro (in bitcoin)
- rete: Tor-Onion











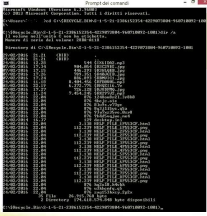
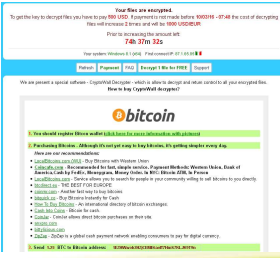

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




CryptoWall




- anno: 2014 aprile
- estensione: <casuale>
- algoritmo: RSA-2048
- riscatto: 500/1000 USD (in bitcoin)
- rete: Tor-Onion
- versione: 4.0




C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




CTBLocker: Curve Tor Bitcoin Locker



- anno: 2014 luglio
- estensione: .<casuale di 7 char>
- algoritmo: AES
- riscatto: 2 BTC
- rete: Tor-Onion

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it





Cerber

- anno: 2016 marzo
- estensioni: .cerber(2)(3), casuale
- algoritmo: RSA - AES
- riscatto: 1 – 2 - 2.4 BTC
- rete: Tor-Onion
- diffusione: siti compromessi, HydraBot, in bundle con Ammyy

CERBER

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».
For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://decryptcerber.dconnect.eu/5446-7C12-B1E9-004E>
2. <http://decryptcerber.tor2web.org/5446-7C12-B1E9-004E>
3. <http://decryptcerber.onion.cab/5446-7C12-B1E9-004E>
4. <http://decryptcerber.onion.to/5446-7C12-B1E9-004E>
5. <http://decryptcerber.onion.lnk/5446-7C12-B1E9-004E>

I documenti personali, le foto, i database e altri file importanti sono stati crittografati.

Per decrittografare i file è necessario acquistare il software specifico – «Cerber Decryptor». Tutte le transazioni devono essere eseguite esclusivamente tramite la rete **Bitcoin**. Per 5 giorni è possibile acquistare questo prodotto a un prezzo speciale: **B2.4099** (= \$999). Trascorsi 5 giorni, il prezzo di questo prodotto passerà a: **B4.8198** (= \$1999).


Il prezzo speciale è disponibile:

05 . 00:00:01






C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



Petya => Ransomware di 3° generazione / Crypto-Malware di 2° generazione

- anno: 2016 marzo
- cifra la Master File Table
- algoritmo: Salsa20
- riscatto: 0,99 BTC
- rete: Tor-Onion
- versione: 3.0

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
[http://petya\[REDACTED\]](http://petya[REDACTED])
[http://petya\[REDACTED\]](http://petya[REDACTED])
3. Enter your personal decryption code there:
2MERC-2[REDACTED] iJ3Nh

If you already purchased your key, please enter it below.

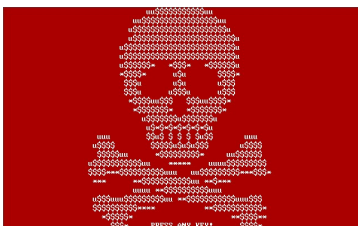
Key:


Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHKDSK is repairing sector 6506 of 43712 (14%)










C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

C.R.A.M.
C.R.A.M. di TG Soft
C.R.A.M. di TG Soft

Come funziona il CryptoMalware

-  email o sito infetto
-  esecuzione cryptomalware
-  invio/ricezione della chiave al/dal server C/C
-  cifratura documenti locali e di rete
-  richiesta riscatto

TG Soft
Software House
www.tgsoft.it

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

C.R.A.M.
C.R.A.M. di TG Soft
C.R.A.M. di TG Soft

Statistiche: da Luglio a Dicembre 2015 (Italy)

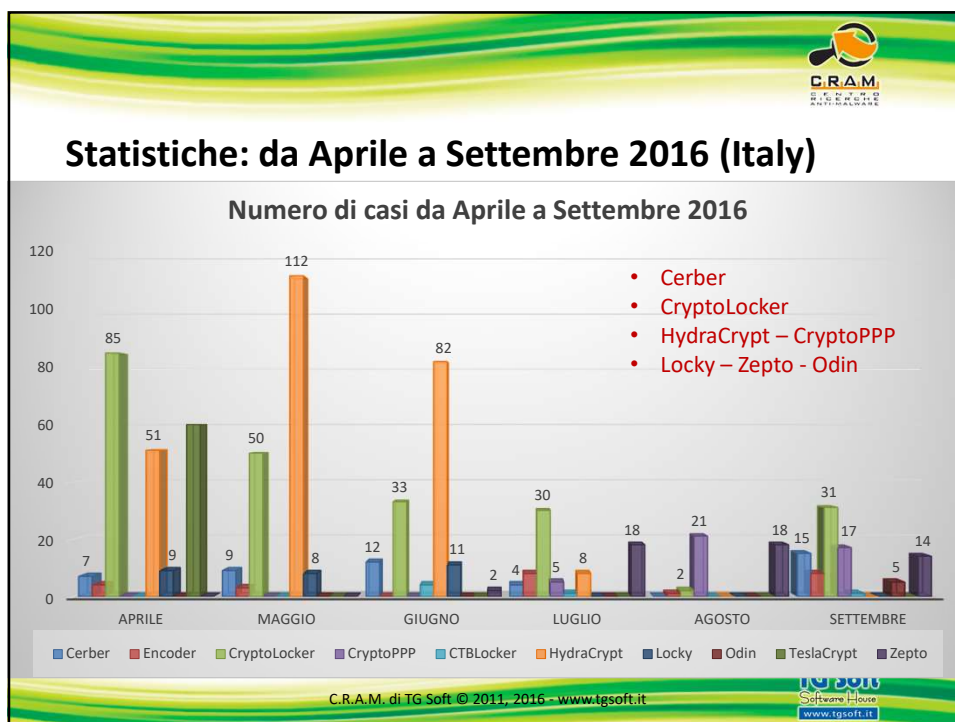
Numero di casi da Luglio a Dicembre 2015: 574


Mese	Casi
Luglio	129
Agosto	54
Settembre	48
Ottobre	75
Novembre	142
Dicembre	126

Malware	Casi
TeslaCrypt	118
CTBLocker	37
CryptoWall 4.0	40
CryptoWall 3.0	143
CryptoVault	2
CryptoLocker	176
CryptoFile BIG	1
CryptoFF	5
CryptoEncoder	52

TG Soft
Software House
www.tgsoft.it

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it






C.R.A.M.
C.R.A.M. S.p.A.
C.R.A.M. S.p.A.

Considerazioni sui CryptoMalware

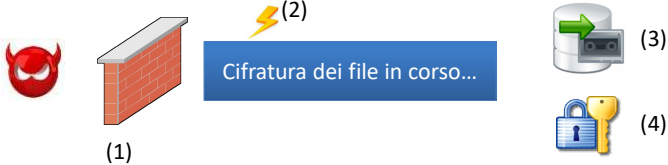
- Il CryptoMalware è una minaccia ATIPICA rispetto a quelle tradizionali (Trojan.Banker, Rootkit, Backdoor, Adware, Virus, etc)
- organizzazioni criminali
- guadagnare denaro (estorsione, richiesta piccola somma)
- non rintracciabili: moneta bitcoin – conti anonimi
- rilascio di nuove varianti di cryptomalware ad ogni ora
- Al cryptomalware è sufficiente essere eseguito solo 1 volta !!!
- Al termine della cifratura si cancella
- Può colpire anche i computer in rete

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



TG Soft
Software House
www.tgsoft.it


C.R.A.M.
C.R.I.T.I.C.O.
ANTI-MALWARE

Come mi difendo



- (1) Bloccare il CryptoMalware prima che arrivi sul PC o che venga eseguito (anti-virus)
- (2) Mitigazione dell'attacco: tecnologie euristico-comportamentali
AntiRansomware protezione Crypto-Malware
- (3) Backup
- (4) Recuperare i file cifrati


TG Soft
Software House
www.tgsoft.it

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


C.R.A.M.
C.R.I.T.I.C.O.
ANTI-MALWARE

Mitigazione dell'attacco: protezione Anti-Crypto Malware



- E' un approccio euristico, che va ad analizzare il "comportamento" dei processi
- Se il processo si comporta da "crypto-malware", allora la protezione andrà ad inibire l'accesso al file system del processo
- Disattivazione della connessione di rete LAN


TG Soft
Software House
www.tgsoft.it

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

C.R.A.M.
C.R.A.M. di TG Soft
ANTI-MALWARE

Esempi di schemi di "comportamento" da CryptoMalware

(1)

file.doc file.doc

(2.a)

file.doc file.doc.<new ext>

(2.b)

file.doc file.doc.<new ext>

(3.a)

file.doc <nome casuale>

(3.b)

file.doc <nome casuale>

(4.a)

file.doc <nome casuale>.<ext>

(4.b)

file.doc <nome casuale>.<ext>

Nome	Tipo
DirtyDecrypt	1
CryptoLocker	2
CTBLocker	2
CryptoEncoder	2
TeslaCrypt	2
CryptoWall 4.0	3
Locky – Zepto - Odin	4
Cerber	2 - 3

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft
Software House
www.tgsoft.it

C.R.A.M.
C.R.A.M. di TG Soft
ANTI-MALWARE


Vir.IT eXplorer PRO

Tecnologie AntiRansomware protezione Crypto-Malware

- **Protezione Anti-Crypto Malware:** permette di bloccare cryptomalware anche di nuova generazione
- **Backup on-the-fly:** backup al volo di file documenti (da 2 KB a 3 MB) in fase di cancellazione, la copia dei file è mantenuta per 48 ore
- **Disattivazione automatica connessione di rete LAN**
- **Protezione da attacco esterno delle cartelle condivise**

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TG Soft
Software House
www.tgsoft.it




Vir.IT eXplorer PRO

AntiRansomware protezione Crypto Malware

Nome	Prot. Anti-Crypto Malware	Backup on-the-fly	Recupero Chiave privata
CryptoLocker	Si	Si	-
CTBLocker	Si	Si	-
CryptoWall 3.0	Si	Si	-
TeslaCrypt (1.0, 2.0, 3.0, 4.0)	Si	No	Si
CryptoEncoder	Si	No	-
CryptoFF	Si	No	Si
CryptoWall 4.0	Si	Si	-
Cerber	Si	No	-
Locky – Zepto - Odin	Si	No	-
HydraCrypt (CryptoXXX)	Si	No	-
DMA Locker	Si	No	-
Petya	No	-	-
Mischa	Si	No	-
CryptoPPP	Si	Si	-

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it






Vir.IT eXplorer PRO integra tecnologie euristico-comportamentali AntiRansomware protezione Crypto-Malware

Simulazione di un attacco da
CryptoMalware su macchina virtuale dal
vivo oppure

Video su youtube:
https://youtu.be/_SyKqqZu6-8

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it








Efficacia della protezione AntiRansomware protezione Crypto-Malware integrata in Vir.IT eXplorer PRO

Statistica Ottobre 2015	
Media dei file crittografati su PC / SERVER con la protezione Anti-CryptoMalware integrata in Vir.IT eXplorer PRO	157
Media dei file crittografati con Anti Virus-Malware diverso da Vir.IT	42.452
Efficacia della tecnologia Anti-CryptoMalware integrata in Vir.IT eXplorer PRO	99,63%*

* Aspettativa percentuale media di file salvati dalla crittografazione grazie alle tecnologie euristico-comportamentali AntiRansomware protezione Crypto-Malware di Vir.IT eXplorer PRO: http://www.tgsoft.it/italy/news_archivio.asp?id=664

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


Efficacia del Backup


- Il **Backup** è l'unica soluzione che ci permette di recuperare i nostri file
 1. Le copie di "backup" devono essere scollegate dalla rete, per non incorrere nella cifratura da parte del crypto-malware
 2. Tenere più copie di "backup" separate
 3. Non tenere le copie di "backup" sul NAS, pensando che essendo sotto "linux" siano inattaccabili !!!
 4. **Dropbox** e la **sincronizzazione**: i file cifrati in locale verranno sincronizzati da Dropbox, in questo modo i file originali verranno sostituiti con quelli cifrati
- **Vir.IT Backup**: permette di eseguire **copie di "backup"** come i tradizionali software, ma queste saranno **protette dalla cifratura**, con ragionevole aspettativa, **anche da Crypto-Malware di nuova generazione**.

Punti di criticità dei sistemi di Backup:

- Tempo per eseguire il backup o il ripristino dei dati
- Copie obsolete

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it






E' possibile recuperare i file cifrati ?

- L'utilizzo di algoritmi di cifratura come **AES o RSA**, rende il recupero dei file cifrati nella maggior parte dei casi di difficile realizzazione, a meno che non si conosca la chiave utilizzata.
- In passato sono state recuperate le **chiavi private dal server di C/C**, grazie all'ausilio delle forze dell'ordine (sequestro del computer).
- In alcuni casi gli autori dei crypto-malware hanno commesso degli errori e hanno lasciato dei punti deboli nel loro sistema, come nel caso del **TeslaCrypt** (versioni precedenti alla 3.0).
- In altri è possibile recuperare i file cifrati attraverso le **shadow copies** di Windows (da Vista in su), sempre che queste non sono state cancellate dal crypto-malware.
- Con software di recupero dati (come Recuva) è possibile tentare di ripristinare file "accidentalmente" cancellati

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it

TeslaCrypt

Per le versioni precedenti alla 3.0 del TeslaCrypt (.vov e altre) è possibile recuperare i file con i seguenti tool: **TeslaDecoder** (BloodDolly), **TeslaCrack** (Googulator) e **The Talos TeslaCrypt Decryption Tool** (Cisco).

Il punto debole delle versioni precedenti alla 3.0 è stato quello di aver reso disponibile il valore **session_ecdh_secret_mul**:

$$\text{session_ecdh_secret_mul} = \text{session_ecdh_secret} * \text{session_chiave_privata}$$


Il **teorema fondamentale dell'aritmetica** afferma che:


Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori.

$$n = p_1 * p_2 * \dots * p_k$$

Attraverso la fattorizzazione è stato possibile determinare la chiave privata.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




C.R.A.M.
C R A M
C R I M I N A L
M A L W A R E

TeslaCrypt 3.0 e 4.x

- Dalla versione 3.0 del TeslaCrypt **NON è possibile recuperare i file** (senza conoscere la chiave privata), perchè gli autori hanno corretto l'errore introdotto nelle versioni precedenti.
- La chiave pubblica è un punto della curva ellittica secp256k1
- La chiave privata è un numero casuale a 256 bit
- Progetto chiuso da Maggio 2016

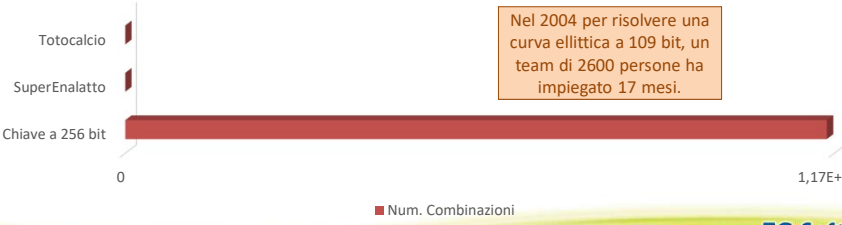
Numero di combinazioni:

Totocalcio (13 partite) = $3^{13} = 1.594.323$

SuperEnalotto = $C(90,6) = 622.614.630$


Chiave a 256 bit = 115792089237316195423570985008687907853269984665640564039457584007913129639935

Project closed
master key for decrypt
440A241DD80FC5664E861989DB716E08CE627D8D40C7EA360AE85C727A49EE
wait for other people make universal decrypt software
we are sorry!




Nel 2004 per risolvere una curva ellittica a 109 bit, un team di 2600 persone ha impiegato 17 mesi.

■ Num. Combinazioni



TG Soft
Software House
www.tgsoft.it

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it


C.R.A.M.
C R A M
C R I M I N A L
M A L W A R E

Considerazioni finali sui Crypto-Malware

- Nei primi 4 mesi del 2016 abbiamo visto un'impennata di crypto-malware rispetto al 2015.
- Gli autori sono vere e proprie organizzazioni criminali, che lavorano a livello industriale, sfornando ad ogni ora nuove varianti di Crypto-Malware.
- I classici prodotti AV sono in difficoltà contro queste tipologie di minacce.
- Il recupero dei file cifrati è molto complicato, a meno che non vi siano errori da parte degli autori dei crypto-malware.
- Il riscatto richiesto è una somma "bassa", pagare o non pagare ?
- Il backup è un'ottima soluzione, ma non sempre viene eseguito oppure, quando i file di backup non siano cifrati, può essere obsoleto.
- La protezione pro-attiva Anti-Crypto malware può mitigare l'attacco salvando la vittima.


TG Soft
Software House
www.tgsoft.it

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



Vir.IT eXplorer PRO AntiVirus-AntiSpyware-AntiMalware ITALIANO



Licenze / Multilicenze dei nostri prodotti:

- Licenza d'Uso flessibilizzabile per PC / SERVER di Vir.IT eXplorer PRO per Windows® Microsoft
- Licenza d'uso per dispositivi Android™ smartphone/tablet di VirIT Mobile Security PRO utilizzabile su Android™ 4+.

Supporto Tecnico compreso, senza costi aggiuntivi, nè per il cliente nè per il rivenditore:



- A mezzo e-mail;
- A mezzo telefono con supporto diretto dei ricercatori del C.R.A.M. di TG Soft
- A mezzo assistenza remota/teleassistenza.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




Vir.IT eXplorer PRO => Principali Caratteristiche

Vir.IT eXplorer PRO
L'AntiVirus, AntiSpyware, AntiMalware ITALIANO

Vir.IT eXplorer: modulo di identificazione/rimozione di virus, spyware, trojan, backdoor, BHO, LSP, dialer, adware, hijacker, keylogger, worm, rootkit, fraudtool e malware informatici. Scansioni manuali o automatiche tramite Scheduler.



Per tutti i S.O. Windows Microsoft
... e ora anche per ANDROID

PROTEZIONE Credito/Militare
Vir.IT Safe Browser
Assistenza telefonica in italiano

Windows 10 compatibile | Windows 8 / 8.1 | Windows Server 2012

Vir.IT eXplorer PRO è certificato ICSAlabs poichè ha superato vari test di identificazione a livello internazionale.

« ICSAlabs An independent Division of Verizon » è il primo soggetto certificatore internazionale indicato/preferito da Microsoft® per testare i software AntiVirus-AntiMalware.






Vir.IT explorer-PRO
L'AntiVirus, AntiSpyware, AntiMalware ITALIANO



Vir.IT Security Monitor: protegge in tempo reale dagli attacchi di virus/malware.

Integra le tecnologie:

-  ✓ **Vir.IT Safe Browser** che segnala eventuali tentativi di frodi informatiche.
-  ✓ **Vir.IT AntiRansomware protezione Crypto-Malware** in grado di bloccare nella fase iniziale dell'attacco la cifratura/crittografia dei file di dati anche da varianti di nuova generazione.
-  ✓ **Vir.IT Backup**, per creare copie di sicurezza dei file di dati e proteggerle dalla cifratura anche da attacchi Crypto-Malware di nuova generazione.
-  ✓ **Vir.IT Controllo Genitori** filtra l'accesso al web in ambito privato e aziendale (Policy aziendali) con approccio WhiteList e BlackList.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



TG Soft
Software House
www.tgsoft.it



Vir.IT explorer-PRO
L'AntiVirus, AntiSpyware, AntiMalware ITALIANO



Vir.IT Console SERVER-Client: modulo centralizzato per la gestione e l'aggiornamento di Vir.IT eXplorer PRO in rete LAN.

-  ✓ **Vir.IT Console SERVER**, installato su un unico computer della rete LAN che abbia accesso ad internet, permette di scaricare e distribuire gli aggiornamenti della suite (motori e firme) su tutti i client.
-  ✓ **Vir.IT Console Client**, è il componente che interroga Vir.IT Console SERVER, provvedendo a prelevare l'ultima release delle firme e, se disponibile, anche del motore per il sistema operativo di competenza, aggiornando automaticamente i client.

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



TG Soft
Software House
www.tgsoft.it





Vir.IT Mobile Security PRO

Suite progettata specificatamente per proteggere smartphone e tablet Android™ da 4.0 a 6.0...

- ✓ Protezione malware Android™ con rilevamento app malevole all'installazione e/o ad ogni aggiornamento delle firme.
- ✓ Protezione in tempo reale SD Card.
- ✓ Protezione SMS spam con rilevamento URL malevole.
- ✓ Navigazione WEB sicura, tramite l'analisi automatica URL pagine web.
- ✓ Monitoraggio traffico di rete Entrante ed Uscente.
- ✓ Protezione della Privacy.
- ✓ Gestione App ed invio applicazioni sospette al C.R.A.M. per analisi e ricerca malware.
- ✓ Gestione online dei vostri dispositivi Android™ ove installato.



C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it




Domande



C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it





Relatore

- Ing. Enrico Tonello (enrico.tonello@pd.ordineingegneri.it)
Ricercatore AntiMalware e co-autore di Vir.IT eXplorer PRO

Collaborazione Tecnica

- Federico Girotto (f.girotto@viritpro.com)
Responsabile supporto tecnico TG Soft

Grazie per l'attenzione



TG Soft
Software House
www.tgsoft.it



C.R.A.M.
CENTRO
RICERCHE
ANTI-MALWARE

C.R.A.M. di TG Soft © 2011,2016 - www.tgsoft.it



81



Referenze

- <http://www.tgsoft.it>
- TeslaDecoder:
<http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/>
- TeslaCrack: <https://github.com/Googulator/TeslaCrack>
- The Talos TeslaCrypt Decryption Tool:
<http://blogs.cisco.com/security/talos/teslacrypt>
- Let's ride with TeslaCrypt: <http://thisissecurity.net/2016/03/02/lets-ride-with-teslacrypt/>
- Il punto debole di Petya Ransomware!:
http://www.tgsoft.it/italy/news_archivio.asp?id=718
- Petya Ransomware ai raggi X !!!:
http://www.tgsoft.it/italy/news_archivio.asp?id=712

C.R.A.M. di TG Soft © 2011, 2016 - www.tgsoft.it



82