TG Soft
Software House
www.tgsoft.it

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

Virus di ieri e virus/malware di oggi… quali pericoli per le aziende, gli enti e i professionisti

Relatori: ing. Enrico Tonello, ing. Gianfranco Tonello

Macerata, 22/06/2013

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 computer.

A seconda del loro comportamento vengono classificati secondo diverse tipologie: virus, spyware, worms, trojan, backdoor, rootkit, ecc ecc…

Tipologie di Malware 1/6

- Tecnicamente per **virus** si intende un programma che abbia la capacità di autoreplicarsi ed infettare altre macchine
- Negli ultimi anni si è utilizzata, erroneamente, la parola «***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**.

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, sfruttando programmi «ospiti» ed infettando altri file per replicarsi

- ***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

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 che tenta di mascherarsi da programma legittimo e 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

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, per autenticarsi nel computer senza possedere le credenziali necessarie, rimanendo non identificato.

Tipologie di Malware 5/6

- ***Adware:*** sono malware che visualizzano finestre pubblicitarie, modificano la home page e il motore di ricerca del browser. Questo 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.

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.

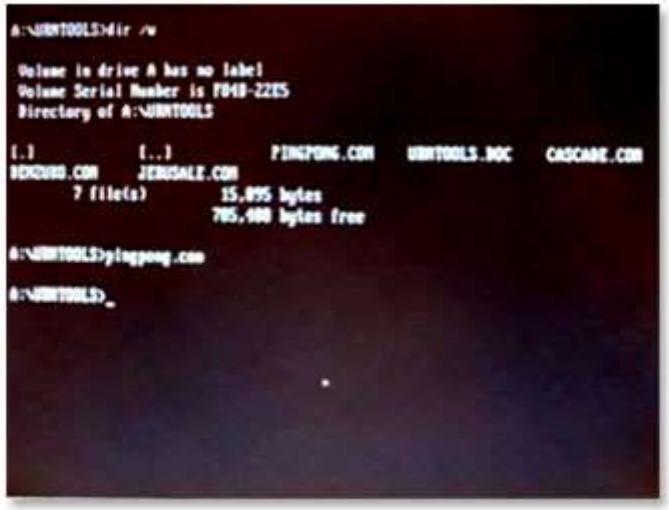
Un po' di storia…: Pakistan Brain 1/4

Il ***Pakistan Brain*** è il virus più vecchio 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.....
$#@%$@!!

Un po' di storia… 2/4

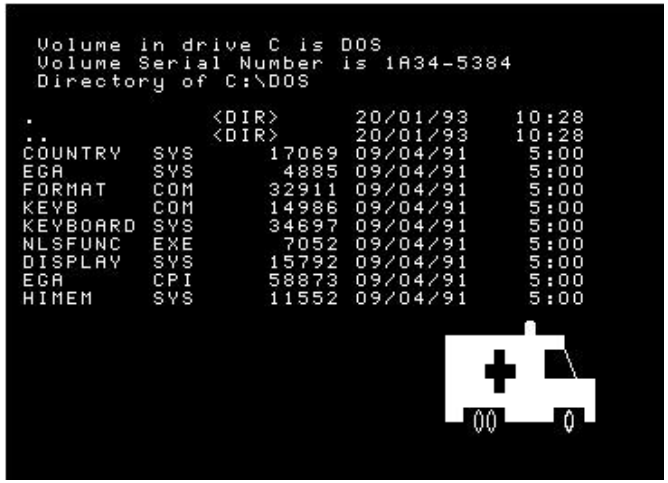
- 1987: ***Cascade*** *(file)*, ***Jerusalem*** *(file)*
- 1988: ***Stoned*** (boot sector), ***Ping Pong*** (scoperto all'università di Torino)
- 1989: ***Dark Avenger*** *(file)*, ***AIDS*** *(file)*
- 1990*:* ***Form*** *(boot sector)*, ***Flip*** *(file)* ***Ambulance*** *(file)*, ***Itavir*** *(file)*
- 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), ***Berlusca*** (file)
- 1995: ***AntiEXE*** (boot sector), ***WM/Concept*** (macro virus)

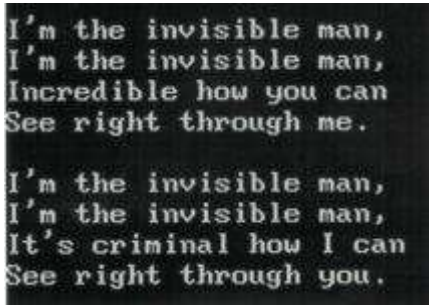


Un po' di storia… 3/4

- 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), ***R0P*** (rootkit)
- 2013: ***ACCDFISA*** (ransomware)

Un po’ di storia…: payload 4/4





Malware moderni

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

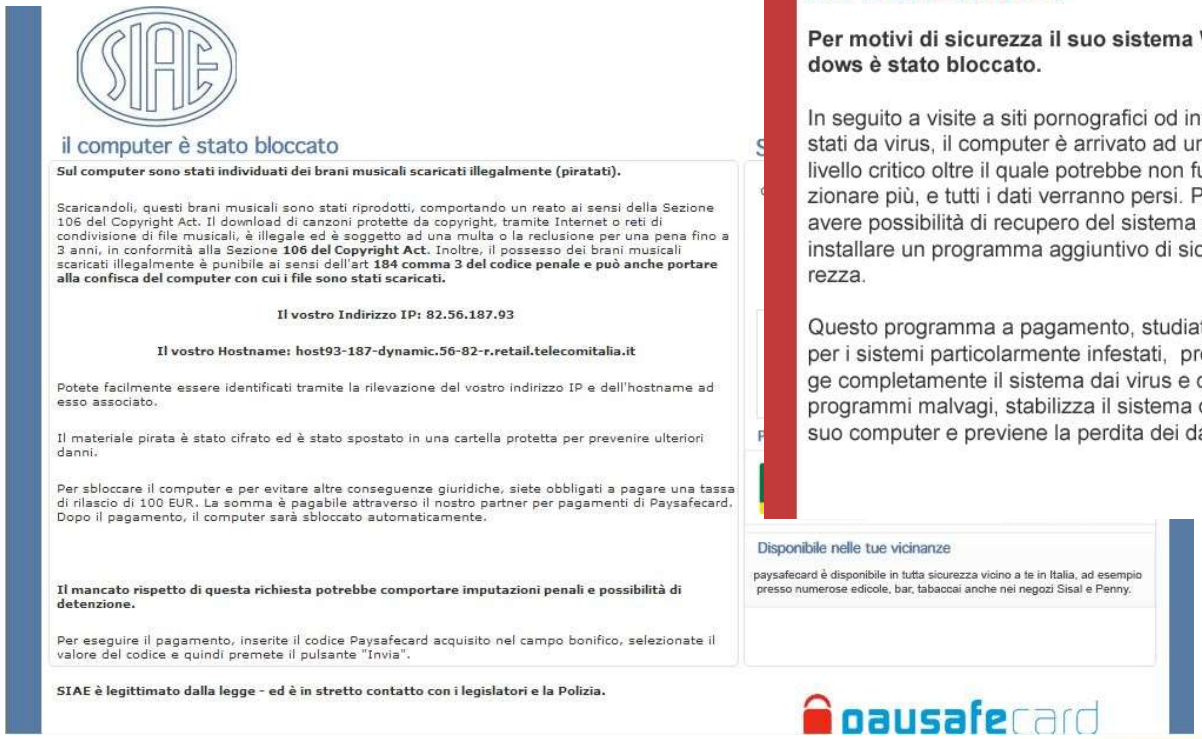
- Ransomware
- Trojan Banker
- FraudTool
- Trojan Clicker
- Trojan Spammer

Ransomware: computer sotto riscatto 1/3

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

Ransomware: computer sotto riscatto 2/3

- Siae
- Polizia di Stato
- Altre istituzioni



il computer è stato bloccato

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

Scaricandoli, 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 scaricati illegalmente è punibile ai sensi dell'art **184 comma 3 del codice 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.56-82-r.retail.telecomitalia.it

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

Il materiale pirata è stato cifrato 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 rilascio di 100 EUR. 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 imputazioni penali e possibilità di detenzione.

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

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

Disponibile nelle tue vicinanze

paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisal e Penny.

paysafecard

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 malvagi, stabilizza il sistema del suo computer e previene la perdita dei dati.

Scelga la modalità di pagamento desiderata

ukash DISPONIBILE

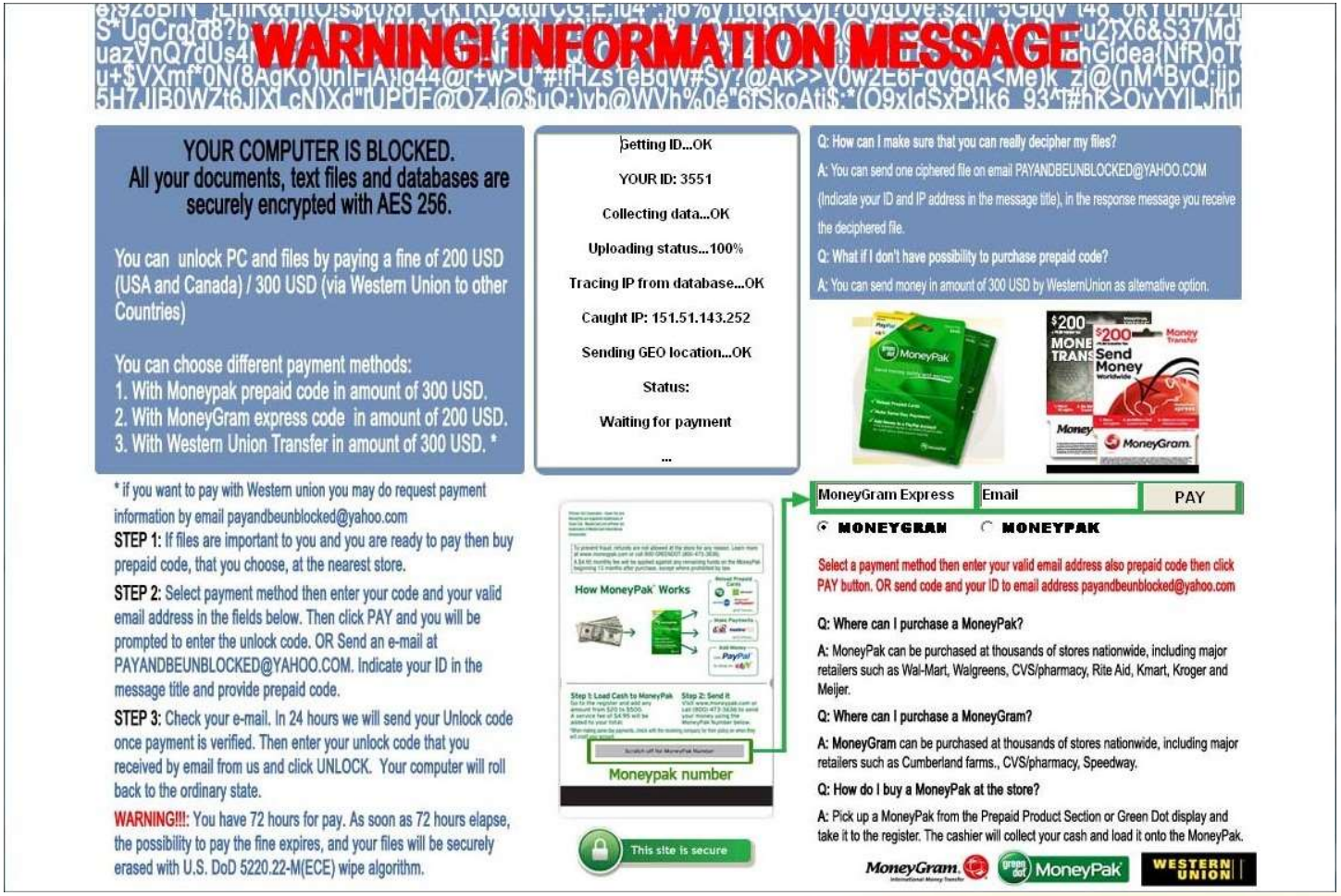
paysafecard DISPONIBILE

Per migliorare (far guarire) 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.

Ransomware: non solo in Italia 3/3

Computer sotto riscatto: documenti crittati



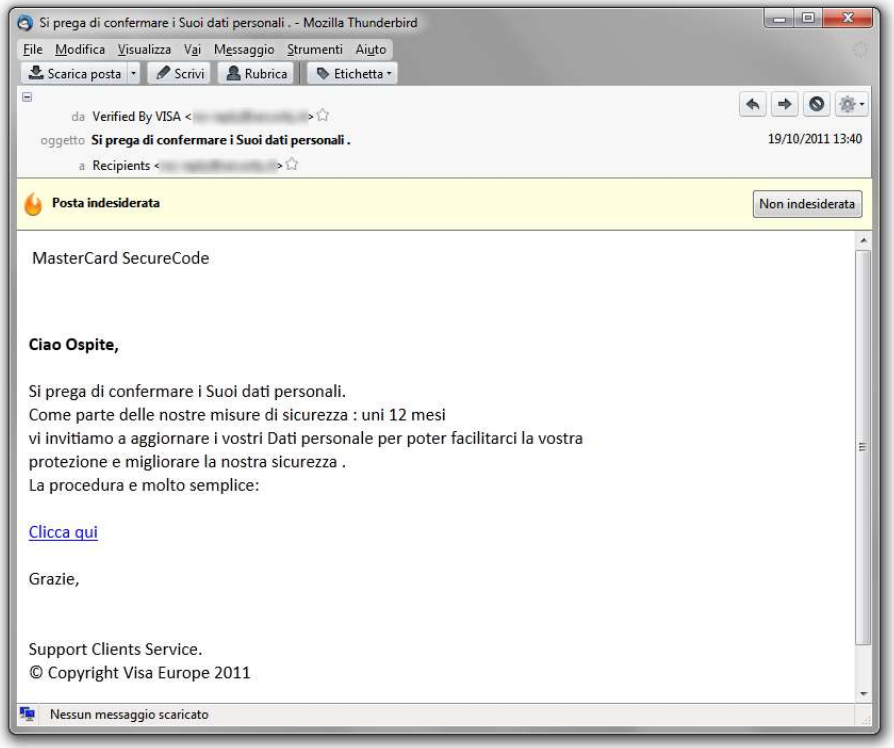
Frodi bancarie: tecniche utilizzate

- **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 ai più diffusi siti di ***home banking***.

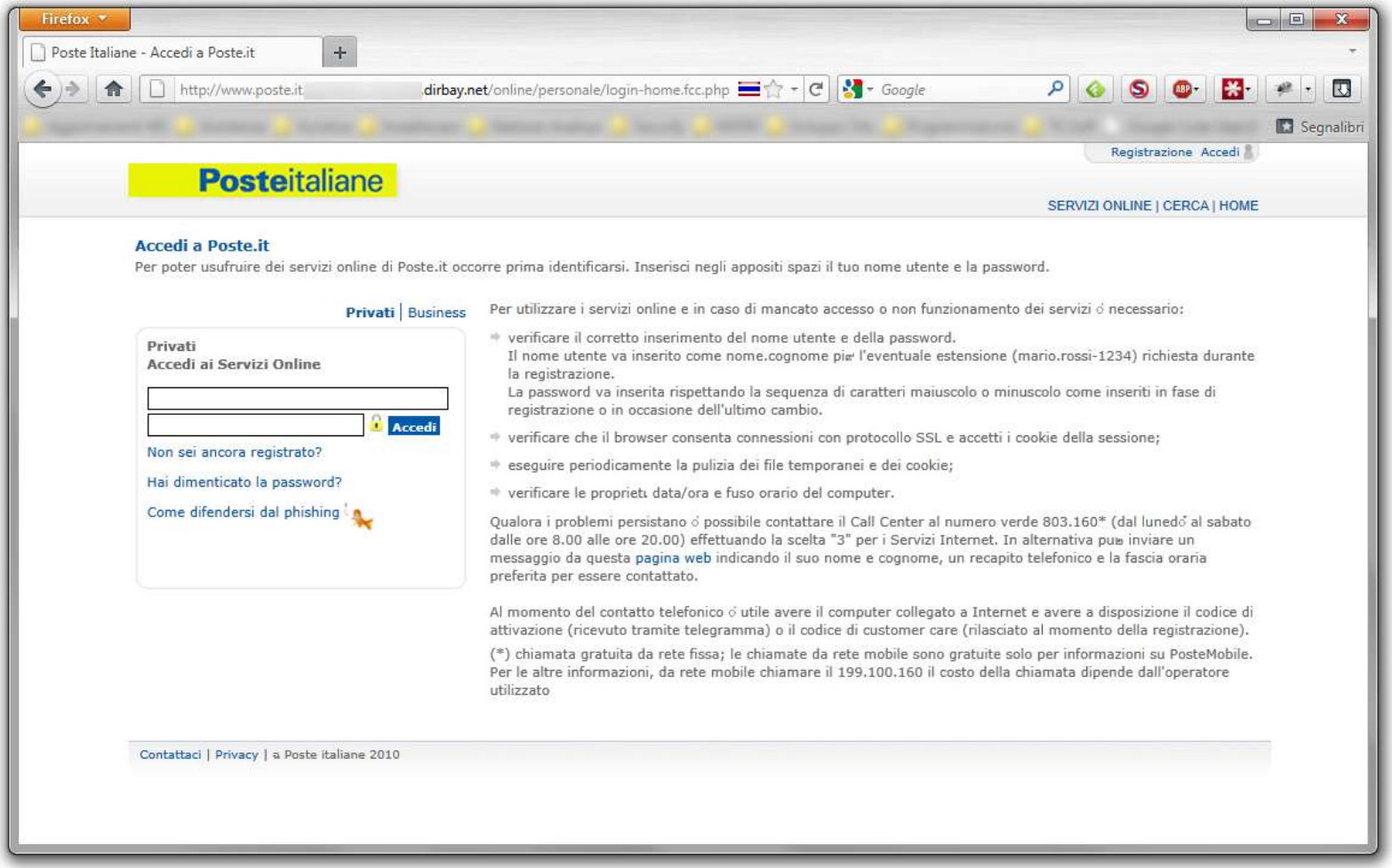
Scopo: rubare soldi dal conto corrente eseguendo bonifici su conti esteri.

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.



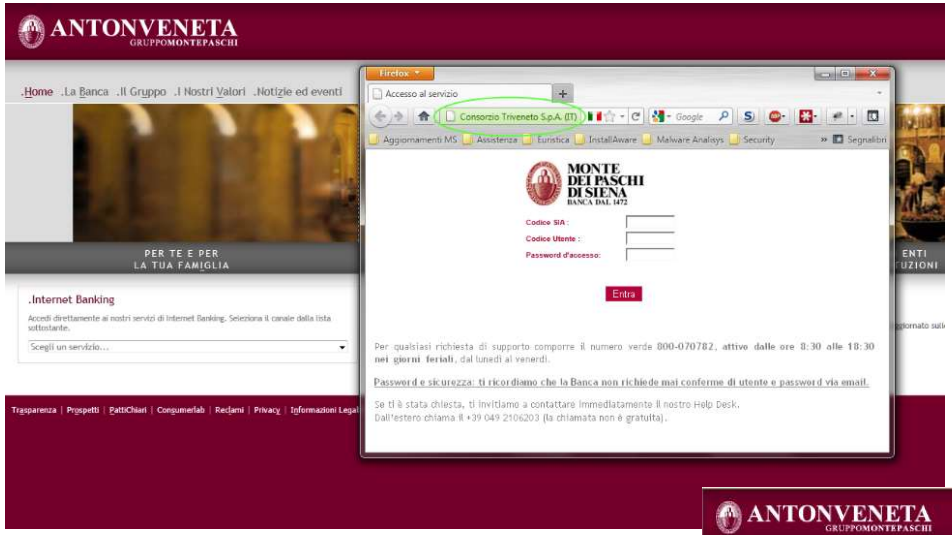
Frodi bancarie: Phishing 2/2



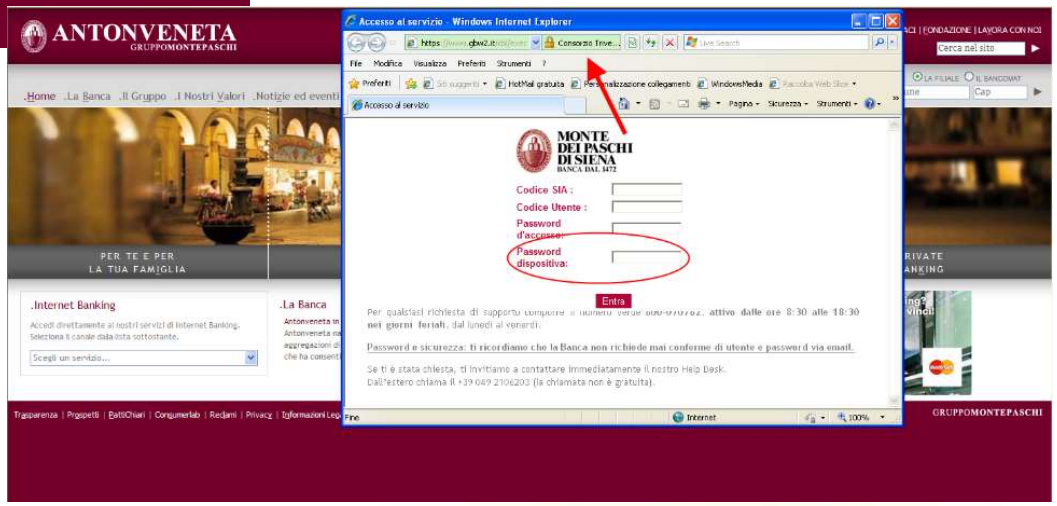
Frodi bancarie: Trojan Banker 1/3

- **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

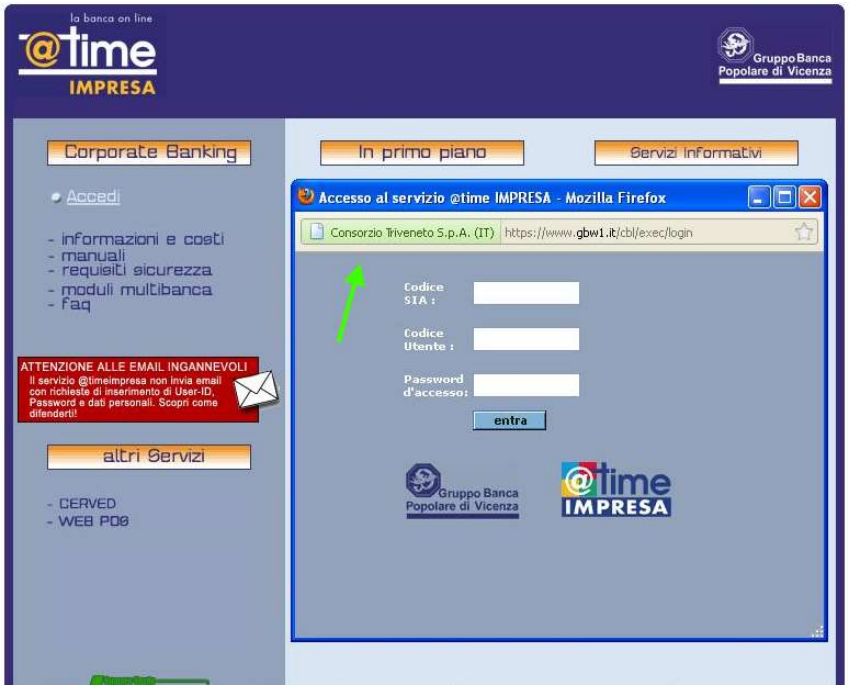
Frodi bancarie: Trojan Banker 2/3



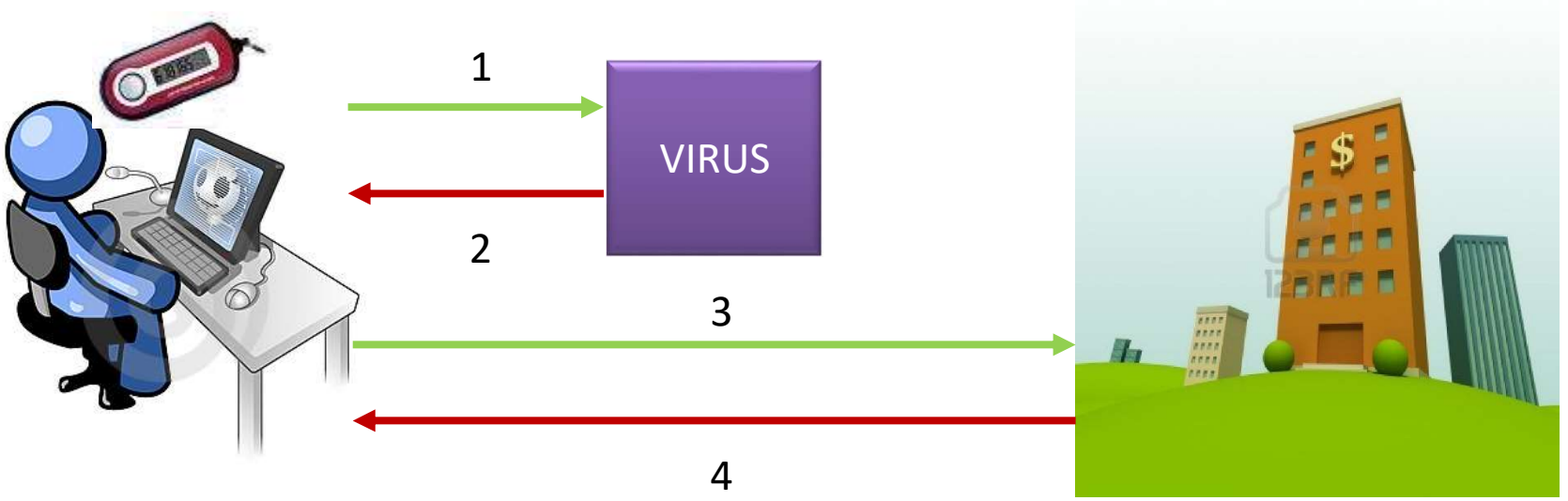
Il trojan Banker modifica (lato client) la pagina di login della banca, richiedendo anche la password dispositiva. Gli autori del malware possono accedere al conto online della vittima e eseguire bonifici su conti esteri alla sua insaputa.



Frodi bancarie: Trojan Banker 3/3



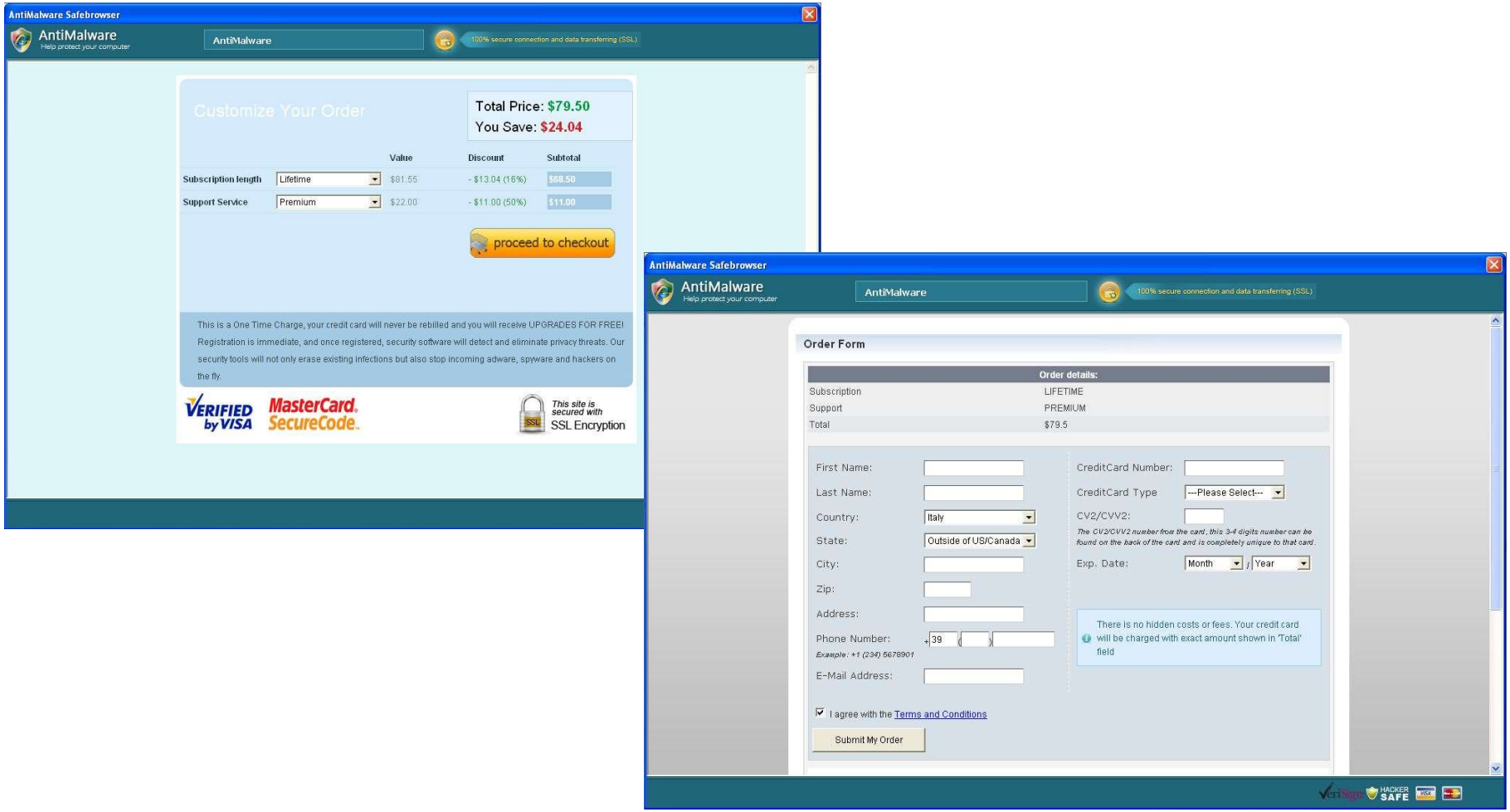
Frodi bancarie: Carberp e OTP



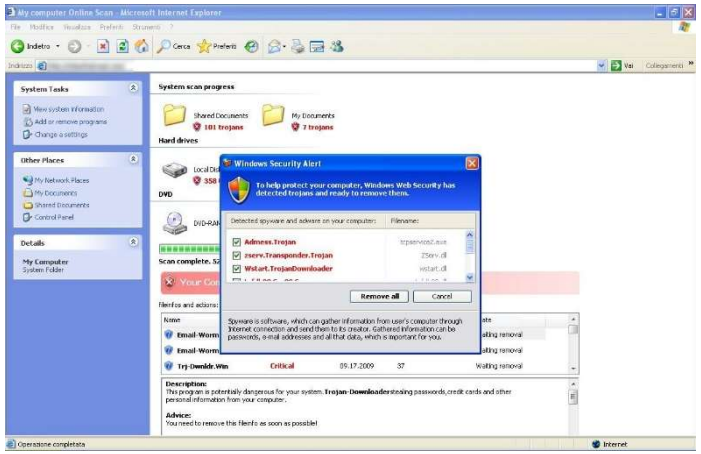
1. L'utente invia le sue credenziali di accesso alla banca: login, password, Paskey Internet banking (OTP = One Time Password).
2. Le credenziale vengono intercettate dal virus, che non le inoltra alla banca, ma le memorizza. Il virus visualizza un falso messaggio di inserimento errato di login/password
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

FraudTool: le truffe dei falsi antivirus 1/3

FraudTool: le truffe dei falsi antivirus 2/3



FraudTool: le truffe dei falsi antivirus 3/3



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

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

Black Hole: Vulnerabilità utilizzate

Vulnerabilità	Descrizione
CVE-2013-0422	Java
CVE-2012-4681	Java
CVE-2012-1889	Windows
CVE-2012-1723	Java
CVE-2012-0507	Java
CVE-2011-3544	Java
CVE-2011-2110	Adobe Flash Player
CVE-2011-0611	Adobe Flash Player
CVE-2010-3552	Java
CVE-2010-1885	Windows

Vulnerabilità	Descrizione
CVE-2010-1423	Java
CVE-2010-0886	Java
CVE-2010-0842	Java
CVE-2010-0840	Java
CVE-2010-0188	Adobe Reader
CVE-2009-1671	Java
CVE-2009-0927	Adobe Reader
CVE-2008-2992	Adobe Reader
CVE-2007-5659	Adobe Reader
CVE-2006-0003	Internet Explorer

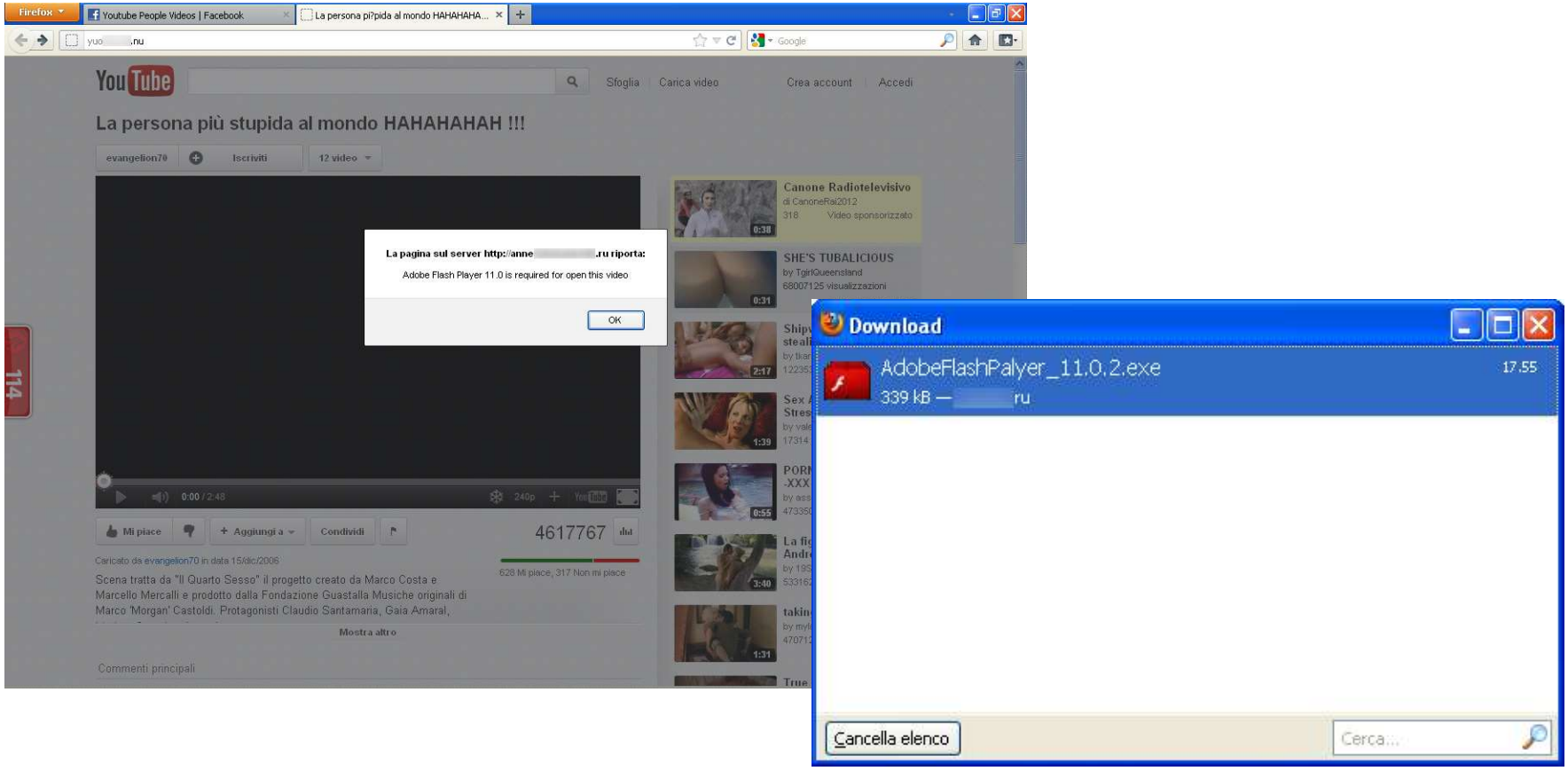
Malware dei Social Network 1/4

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

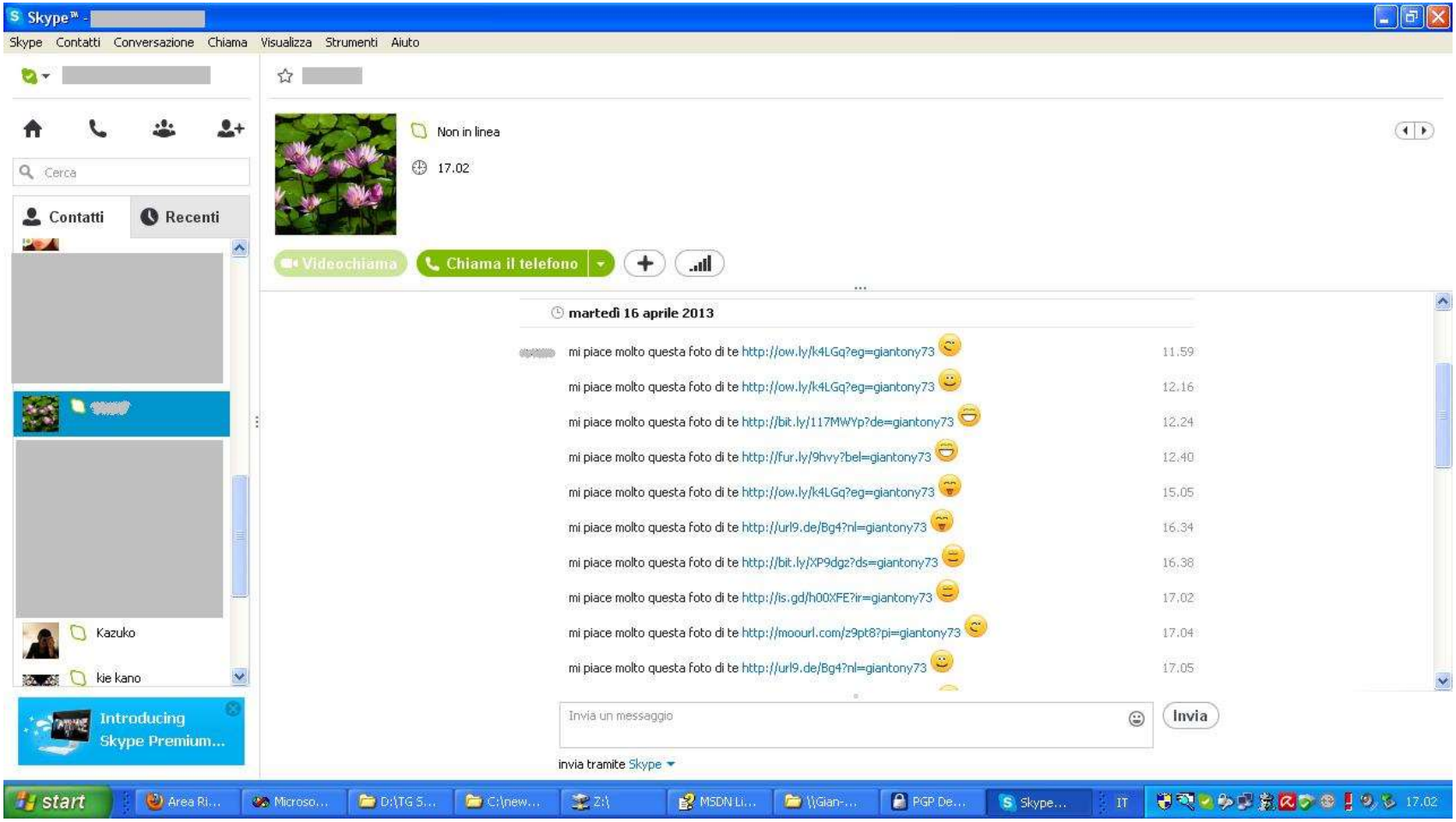
- Facebook
- Skype
- Twitter

Malware dei Social Network: facebook 2/4

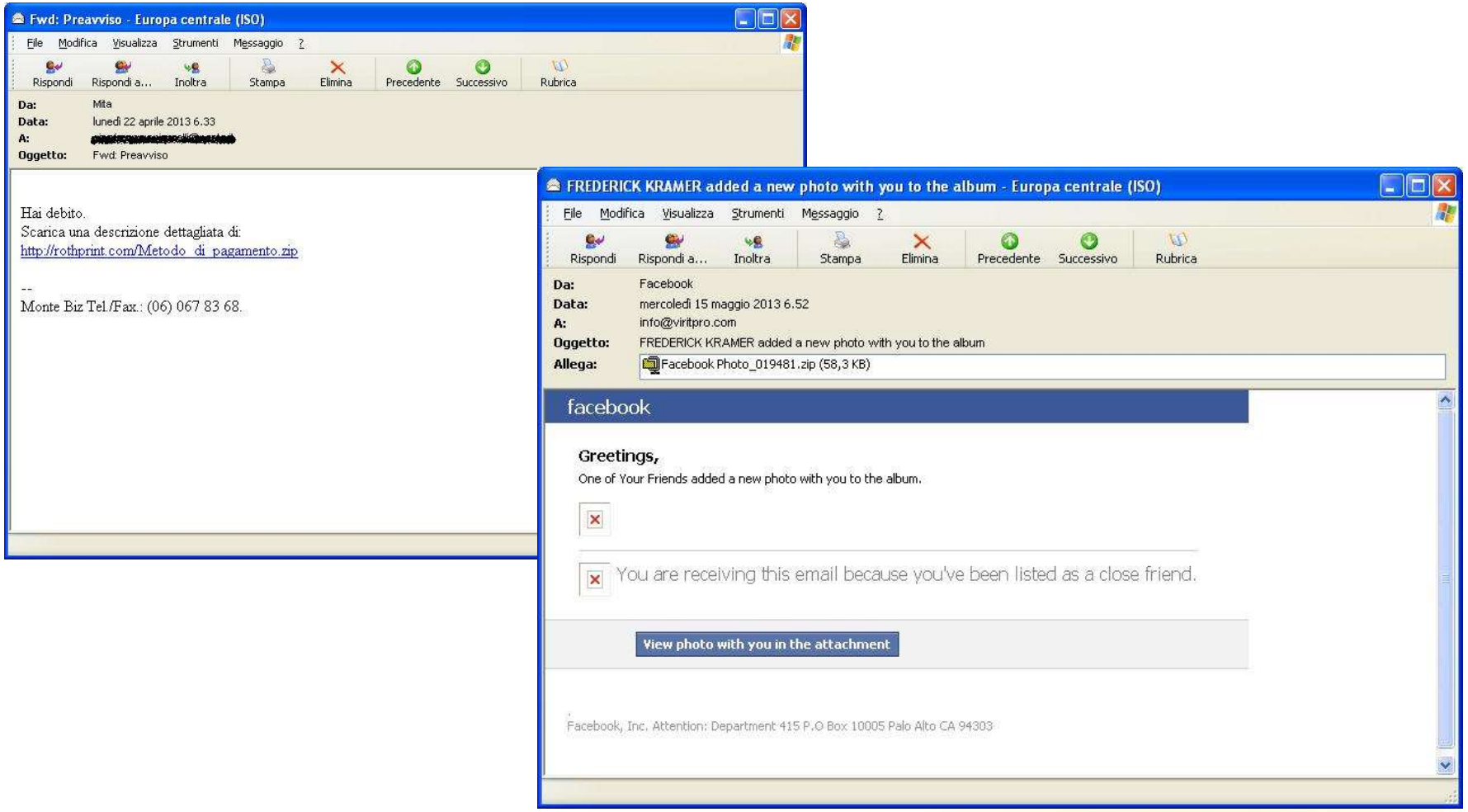
Malware dei Social Network: facebook 3/4



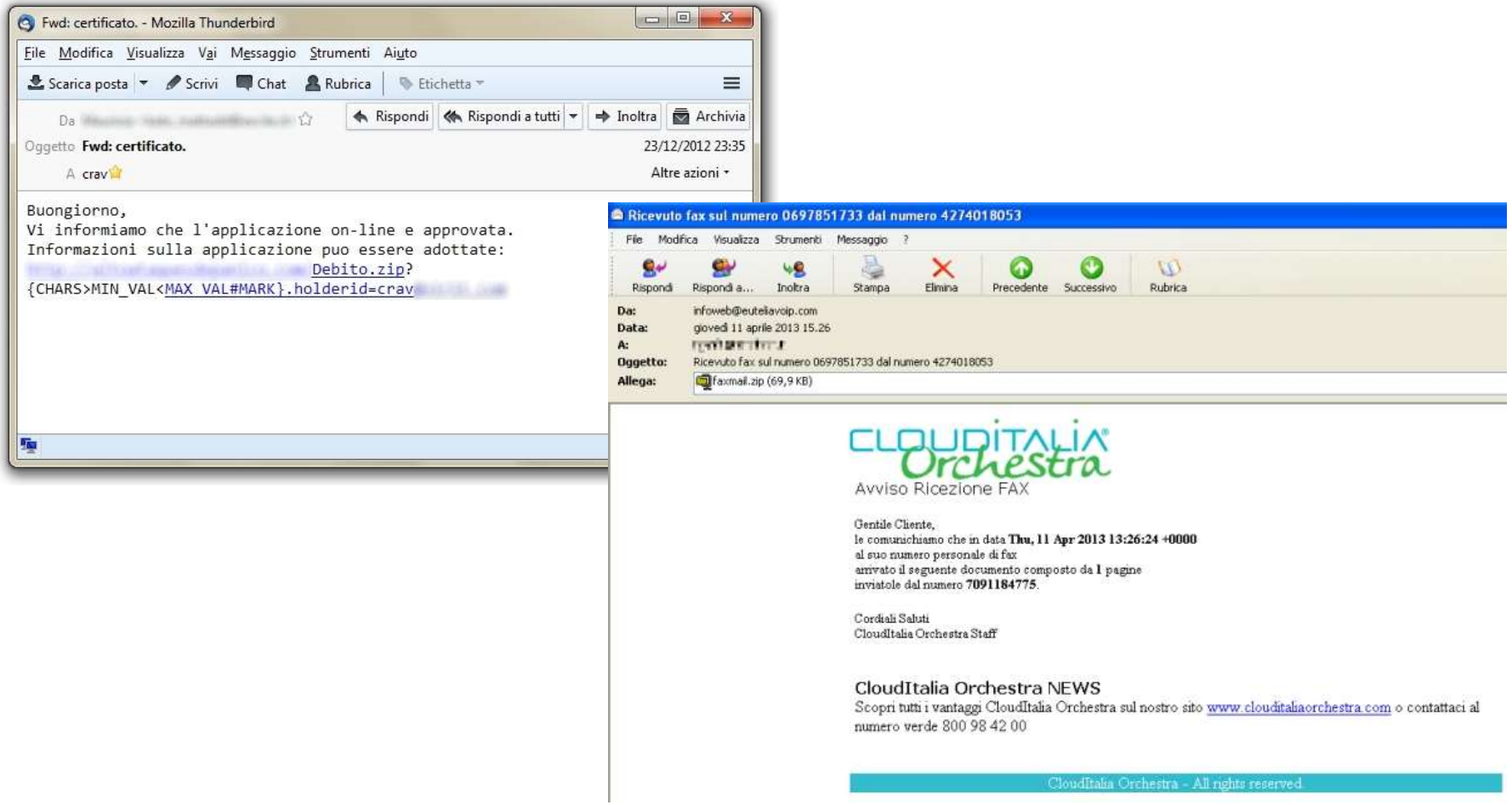
Malware dei Social Network: Skype 4/4



Virus dell'email… 1/2



Virus dell'email… 2/2



Sistema operativo non aggiornato

- Le patch rilasciate dalle software house sono, nella maggior parte dei casi, 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 disponibile 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 dowload automatico delle patch per poi procedere con l'istallazione 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

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, kazaa, 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

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)

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

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

Come mi difendo dai Malware

- Antivirus sempre aggiornato e installato su tutti i pc 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

Domande

Autori

- Ing. Enrico Tonello (enrico.tonello@pd.ordineingegneri.it)

  Ricercatore AntiMalware e co-autore Vir.IT eXplorer PRO
- Ing. Gianfranco Tonello (g.tonello@viritpro.com)

  CEO TG Soft S.a.s., Malware Analyst e co-autore Vir.IT eXplorer PRO
- Roberto Spagliccia (r.spagliccia@viritpro.com)

  Responsabile Supporto Tecnico TG Soft

Grazie per l'attenzione

Referenze

- http://www.tgosft.it
- http://campaigns.f-secure.com/brain/
- http://www.emezeta.com/articulos/23-virus-de-la-epoca-del-dos
- http://wiw.org/~meta/vsum/index.php