# DEBELLARE IL VIRUS GUARDIA DI FINANZA, POLIZIA

12 COMPANY	
Attenz	ione!!!
E stata risuita una veguente violatione: Dal tos rich Regule. B interne operativo è stata È stata fisiata una veguente violatione: Dal tos richizzo P "95.236.187.73" era esegui nonché la violenza dei barribri. Nei tue computer sono stati trova vide- Dalla posta elettronica era effettuato anche la distrib E bioccaggio di computer serve per tro	blocata per una violenta delle leggi della Repubblica Italianal to un accesso alle web-pagne contenenti la pomografia, la pomografia minorile, ao Ne contenenti la pomografia, elementa il violenza e la pomografia minorile, uzione dello spam con un senso recondito terroristico, oncare l'attività diegale dalle parte tua.
I tuoi dati:	IP:95. Poizzon ISP: Teleconi Iniia 8.p.a.
Per togliere il bloccaggio devi pagare una multa di 100 euro. Nai due seguenti varianti di pagamento:	<b>Ø kash</b> Dove passo trovare Ukash?
1) Effettuare il pagamento tramite l'Ukash.	Pubi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, etazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di
Per questo inseriaci il numero ncevuto nella colonna di pagamento, dopodiché	terminale Epay, Epipoli.
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)	terminale Epay, Epipoli. Recati presso il punto vendita dotato di terminale Epay, Epipoli a te pi vicno, Richiedi un voucher in contanti al negoziante. Il negoziante dovr
Per questo inseriad il numero ricevuto nella colonna di pagamento, dopodiché premi premi OK (se hai più numeri, allora inserisciti uno dopo l'altro, dopodiché premi OK) Se il otterna regnalariti un errora, allora diorai mandare di numero per la posta elettronca <u>deposto Dicher poli nes</u>	Recati presso il purbo vendita dotato di terminale Epay, Epipoli a te pi vicno, Richiedi un voucher in contanti al negoziante. Il negoziante dovr stampare e consegnanti un voucher Ukash con codice PIN da 13 cfre.
Per questo inserted il numero ricevuto nella colonna di pagamenta, dapodiché premi CK (se hai più numeri, allora insertsoli uno dopo l'altro, dopodiché premi OK) Se il unterna regnalaria un errora, allora diversi manifare di numero per la posta elettroran deposito@poler_gdf.net 2) Effettuare il pagamento tramite il Paysafecard:	Recat presso i purbo vendita dotato di terminale Epay, Epipoli a la pu vicino, Richiedi un voucher in contanti al negoziante. I negoziante dovr stampare e cansegnarti un voucher Ukash con codore PIN da 19 cfre.
Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi CK (se hai più numero, allora inserisciii uno dopo l'altro, dopodiché premi CK) Se il conterna regnalaria un errore, allora dioral mendare di numero per la public riettorna deposito@cuber-gdi.net: 2) Effettuare il pagamento tramite il Paysafecard. Per questo inserisci per finore il numero ricevuto (nel caso di necessità inseme con la passurord) nella cionana di pagamento. dopodiché premi CK (se hai più numeri, altora inseriscii uno dopo l'altro, dopodiché premi CK)	Terminale Epay, Epipoli Recati presso il purbo vendita dotato di terminale Epay, Epipoli a te p vicno, Richiedi un voucher in contanti al negoziante. Il negoziante dovr stampare e consegnanti un voucher Likash con codice FIII da 19 cfre.

Ultimamente è molto diffuso un virus relativo ad un falso annuncio della *Guardia di Finanza* o della *Polizia*. Dopo avere preso l'infezione, avviando il computer resterete bloccati in una finestra che riporta:

## Il logo della guardia di finanza o della polizia

Una scritta che ci accusa di avere nel computer contenuti illegali.

## La richiesta di un pagamento di 100 euro per ripristinare le funzionalità del PC.

#### Non vi sarà possibile andare avanti ed il computer resterà bloccato.

In questo caso sappiate che si tratta di un un virus (dal nome Trojan.Win32.FakeGdF.A) e che stanno cercando di truffarvi. Non dovete assolutamente PAGARE NULLA. Per eliminare il virus seguite le istruzioni sotto riportate.

## A) Se il pc parte e subito dopo compare la schermata del virus:

1. Scollegate il pc dalla rete e da internet, quindi avviatelo;

2. Bisogna essere veloci, **prima** che il pc carichi tutto il sistema, appena compare la schermata del desktop premere ctrl-alt-canc e attendere che si apra il Task manager, portarsi **subito** nel tab "Processi", e se notate qualche nome strano tipo: wgwgwgwg.exe o simile, selezionatelo **immediatamente** e premete "Termina". Potrebbero essere anche più di uno;

3. Se siete riusciti a non far caricare il virus, eliminiamo tutte le altre tracce del malware entrando nell'utilità *Ripristino configurazione di sistema* di Windows (Start – tutti i programmi – accessori – utilità di sistema). Qui possiamo ripristinare il pc alle impostazioni di qualche giorno prima dell'infezione. Fine.

**B**) **Se non è possibile entrare nel task manager** (ctrl-alt-canc), bisogna far partire il pc da modalità provvisoria, avviatelo e dopo il controllo del bios premete F8. Caricata la modalità

provvisoria, andate nel registro di sistema (start – esegui – scrivete regedit e poi premete invio), e verificare queste chiavi di registro:

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ policies \ system$ 

se presente, il valore DisableTaskMgr deve essere impostato a 0 altrimenti non si potrà aprire il task manager di Windows. Poi controllare le seguenti voci:

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ Run$ 

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ RunOnce$ 

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ Run \ Ext{Ext} \ Never \ N$ 

 $HKEY\_CURRENT\_USER \ Software \ Microsoft \ Windows \ Current \ Version \ Run$ 

 $HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current\Version\RunOnce$ 

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ Run$ 

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ RunOnce$ 

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current \ Version \ Run \ Ext{Ext} \ Nev \ Soft \ \ Soft \ \ Soft \ Soft \ Soft \ Soft \ Soft \ Soft \ \ Sof$ 

Verificare che non ci siano file strani in avvio tipo WPBT0.dll, Oxxxxxx.exe, wgwgwggw.exe, etc. Poi posizionarsi su:

 $HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ NT \ Current \ Version \ Winlogon$ 

controllate che il valore "Shell" sia solo Explorer.exe.

## Se non c'è dovrete inserirlo voi manualmente.

Più sotto, sempre nel ramo "shell" trovate un'altra voce denominata **Userinit.** Deve avere come valore **SOLO** C:\Windows\system32\userinit.exe, (con la virgola).

Fatto questo riavviate il pc e il virus dovrebbe essere debellato.

**C) Se non funziona ctrl-alt-canc e non funziona la modalità provvisoria** in quanto visualizziamo una schermata blu, abbiamo bisogno di un altro strumento per far partire il pc anziché il nostro disco fisso. Dobbiamo preparare un CD autopartente o meglio una chiavetta USB autopartente che carichi in RAM un Sistema Operativo di Emergenza che ci consenta di modificare il sistema bloccato.

Da un altro computer funzionante scarichiamo <u>questo file ISO</u>, successivamente preleviamo il software aggiuntivo *Rescue2USB* (<u>cliccare qui</u> per il download).

*Rescue2USB* è un programma che consente di preparare una qualunque chiavetta USB rendendola avviabile e memorizzandovi il file ISO di Kaspersky Rescue Disk. Così facendo, lasciando inserita all'avvio del personal computer la chiavetta, si potrà avviare Kaspersky Rescue CD. Una volta scaricato ed avviato *Rescue2USB*, si potrà inserire automaticamente il Rescue Disk di Kaspersky in una chiavetta USB: basta selezionare il file ISO di Kaspersky Rescue Disk precedentemente scaricato, l'unità USB di destinazione quindi fare clic sul pulsante *Start*. *Rescue2USB* cancellerà tutto il contenuto della chiavetta USB, perciò usate una chiavetta vuota.

Caspersky USB Rescue Disk Maker 📃 🔲 🔤					
	Welcome to Kasp Rescue Disk Mak This utility is designed Rescue Disk on USB m	ersky USB er! for recording the nedia			
Path to the Kasp	Path to the Kaspersky Rescue Disk image (.iso):				
USB medium: E:\ ( USB I	USB medium: E:\ ( USB DISK 2.0 ) (1.9 GB) -				
START					

Una volta concluso il procedimento di creazione della chiavetta autopartente, inserirla in una porta USB del computer, avviatelo da supporto USB (controllare dal BIOS **la corretta sequenza di avvio:** unità **USB prima**, hard disk poi).

Così facendo al boot del sistema ci ritroveremo la schermata di Kaspersky Rescue Disk, premiamo un tasto qualsiasi e scegliamo la lingua, poi premiamo 1 per accettare la licenza, scegliamo *Kaspersky Rescue Disk Graphic mode*. Al termine della fase di caricamento dell'ambiente di lavoro, ci si troverà dinanzi ad una finestra simile al desktop di windows.

		KASPERSKY
	🖌 Какрепану Rescue Disk	
He manager	Kaspenky Rescue Disk	tlings
Asperty Registric Xasperty Rescue Disk Keb browser	Otherst State:	0
🕄 🔍 📄 📈 🔥 Kespe	rsky Rescue Disk	() 📑 🖬 👥 🦂 🔘 83:18 pm

Premiamo il tasto in basso a sinistra (al posto di start di windows), e dal menù a tendina verifichiamo la correttezza delle impostazioni di rete, premendo web browser. Proviamo a navigare in qualche sito e verifichiamo che funzioni internet.

In caso contrario, è necessario cliccare sulla voce *Network setup* del menù di avvio quindi selezionare l'interfaccia di rete da impostare (wired o wireless):

× N	Network Connections		-0 X
É	📱 Wired 📩 Wireless 🕅 Mobile	e Broadband	VPN 📑 DSL
[	Name	Last Used	📥 📥
	Auto eth0	2 minutes ago	<u>e</u> dit
			Pelete
1			
			X <u>C</u> lose

Facendo clic sul pulsante *Edit*, si potranno eventualmente assegnare in modo manuale le impostazioni di rete (indirizzo IP, gateway, DNS).

Dopo aver completato quest'operazione, si dovrà tornare alla schermata iniziale, fare clic sulla scheda *My Update Center* quindi su *Start update*:



Così facendo aggiorneremo i database delle firme di Kaspersky. Queste informazioni verranno automaticamente salvate, all'interno di C:\Kaspersky Rescue Disk 10.0. In questo modo, ogniqualvolta si riutilizzerà il supporto di Kaspersky Rescue Disk, non saremo costretti a riscaricare manualmente gli aggiornamenti dell' antivirus.

Per avviare una scansione antimalware, si dovrà tornare alla scheda Objects scan, selezionare tutte

le voci in elenco (*Disk boot sectors*, *Hidden startup objects* e la lettera identificativa di unità corrispondente al disco C:):



Dopo aver spuntato le caselle corrispondenti premiamo *Start objects scan*. Al termine della scansione potremo anche stampare il report della stessa sotto forma di file. A questo punto suggeriamo di avviare lo strumento *Kaspersky Windows Unlocker* eseguibile cliccando sul pulsante in basso a sinistra, scegliendo *Terminal* quindi digitando windowsunlocker:



Questa applicazione provvederà a controllare il registro di sistema rilevando e rimuovendo ogni traccia di eventuali infezioni da malware.

Alla comparsa del menù seguente, si dovrà premere semplicemente il tasto Invio:



Suggeriamo quindi di premere il tasto "2" ed Invio (*Save boot sector copies*) ed uscire dall'utilità premendo "0" quindi ancora Invio.

A questo punto, dal desktop di Kaspersky Rescue Disk, fare doppio clic sull'icona *Kaspersky Registry Editor*, una utilità che permette di aprire il registro di sistema di Windows, verificarne la configurazione ed eventualmente modificarne chiavi e valori.

Ora possiamo fare un'ultima verifica alle chiavi descritte nel punto B) e debellare finalmente il virus.