PHOENIX INFORMATICA DAL 1989

NEWSLETTER10 | **marzo 2017**

Ahi ahi!!! Abbiamo l'influenza. **Parliamo di Virus Informatici.**

In questa newsletter desideriamo approfondire un tema di grande attualità che rappresenta troppo spesso un elemento sottovalutato dalle aziende: la protezione dei dati e la sicurezza informatica contro Virus e Malware. Il nostro staff Ricerca e Sviluppo ha voluto approcciare con un tutorial la gestione della problematica. ***La sensibilità sulla sicurezza è un must imprescindibile per approcciare una logica Industria 4.0. Le fondamenta per l'evoluzione.***

... ALTRO CHE MAL DI MARE, ABBIAMO PRESO IL MAL*di*WARE ... UN PO' DI STORIA.

La tecnologia ha ormai radicalmente **trasformato il nostro modo di lavorare** migliorando l'efficienza dei nostri ambienti lavorativi e della gestione aziendale. La digitalizzazione dei processi produttivi offre quindi grandi **opportunità**, ma se non viene gestita in modo responsabile può anche aumentare i rischi per la sicurezza informatica. Ormai i dati a cui accedono i nostri dispositivi sono decine di migliaia: dati di fatturato, elenchi dei clienti, piani strategici e di investimento, dati personali dei dipendenti, numeri e codici di carte di credito e di debito, conti bancari, contratti, email riservate.

Ci sono dei rischi e i più pericolosi sono i **virus** che possono cancellare l'intero disco, eliminare o alterare documenti, permettere a qualcun'altro di usare un computer per attaccarne altri o rubare informazioni e dati sensibili. Tra i più recenti e pericolosi virus in circolazione c'è il **virus del riscatto**, o **Cryptolocker:** un virus che crittografa i file contenuti in un computer rendendoli illeggibili. Nella maggior parte dei casi si diffonde attraverso un allegato ad un'email fraudolenta e una volta inoculato nel sistema chiede al possessore del computer un riscatto per ottenere un decrittatore in grado di recuperare i file danneggiati. Per fronteggiare e risolvere criticità così delicate per la sicurezza informatica di un'azienda **è importante rivolgersi a dei professionisti.**

APPROFONDISCI

...UNA BATTAGLIA IMPARI DA COMBATTERE CON IL GIUSTO ALLEATO .... LE STRATEGIE.

Abbiamo avuto modo, in più occasioni, di renderci perfettamente conto di come un eventuale **attacco malware informatico** possa **determinare le sorti** di questa o quell'altra azienda, così come è sempre più frequente che questi argomenti coincidano con **eventi socio-politici di portata planetaria.** Tant'è che ogni governo nazionale ha ormai definito ed attuato una lunga serie di pratiche racchiuse nel più complesso mondo della **Cyber Security.** È indubbio che si tratta di una **battaglia impari:** certezza degli obiettivi da colpire ed incognita da dove arriverà il prossimo colpo.

PHOENIX INFORMATICA ha attuato da tempo una propria **Politica di Sicurezza Informatica** che viene applicata al proprio interno e presso la propria clientela. Non sappiamo se la **guerra** può essere vinta, ma sicuramente può essere **contenuta**, adottando una serie di **strumenti diversificati** che permettano la corretta operatività e **continuità di servizio** dei sistemi informativi dei clienti, oltre a garantire flessibilità e libertà di azione quanto basta. È ovvio che se ogni azienda bloccasse il proprio sistema informativo **all'interno delle proprie mura**, dentro una **bella cassaforte** inaccessibile potrebbe affermare di avere i propri dati al sicuro, ma questo, oggigiorno, non è attuabile. È importante sottolineare che tutta la Politica di Sicurezza Informativa **proposta**

APPROFONDISCI

PHOENIX INFORMATICA SRL SOFTWARE & INFORMATION TECHNOLOGY

Via Giovanni Quarena, 124
25085 GAVARDO (BS) Italy

t +39 (0)365 371 796
f +39 (0)365 376 640

info@phoenix.it
www.phoenix.it

PHOENIX INFORMATICA DAL 1989

NEWSLETTER10 | marzo 2017

... ALTRO CHE MAL DI MARE, ABBIAMO PRESO IL MAL*di*WARE ... UN PO' DI STORIA.

Malware, abbreviazione di **mal**icious soft**ware**, indica un qualsiasi software usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata. Il termine malware è stato coniato nel 1990 da Yisrael Radai, precedentemente veniva chiamato virus per computer; **in italiano viene anche comunemente chiamato codice maligno.** Il principale modo di propagazione del malware consiste di frammenti di software parassiti che si inseriscono in codice eseguibile già esistente. Il frammento di codice può essere scritto in codice macchina ed inserito in un'applicazione esistente, in codice di utility, in un programma di sistema o può inserirsi anche nel codice del sistema di boot di un computer. Un malware è caratterizzato dal suo **intento malevolo**, agendo contro le necessità dell'utente, e non include software che causa un danno non voluto a causa di qualche suo difetto. Il malware non necessariamente è creato per arrecare danni tangibili ad un computer o un sistema informatico, ma va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private, senza essere rilevato dall'utente anche per lunghi periodi di tempo. Oltre a **carpire informazioni di nascosto**, un malware può essere creato con l'intento di arrecare danni ad un sistema informatico, spesso tramite sabotaggio, oppure può criptare i dati del computer della vittima, estorcendo denaro per la decriptazione. Malware è un termine generico che fa riferimento a varie tipologie di software intrusivo o malevolo, inclusi Virus informatici, Worm, Trojan, Ransomware, Spyware, Adware, Scareware, e altri programmi malevoli. **Può assumere diverse forme**, come Codice eseguibile, Script, e altro software. Il malware si diffonde principalmente inserendosi all'interno di file non malevoli. La diffusione del malware risulta in **continuo aumento**: si calcola che nel solo anno 2008 su Internet siano girati circa 15 milioni di malware, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti; tali numeri sono destinati ad aumentare con l'espansione della Rete e il progressivo diffondersi della cultura informatica. Nel 2011 la più grande minaccia malware era costituita da worm e trojan, piuttosto di altri virus. Altri malware sono a volte trovati all'interno di programmi forniti da compagnie, ad esempio scaricabili da siti web, che appaiono utili o accattivanti, ma potrebbero avere delle funzionalità aggiuntive nascoste indesiderate, che raccolgono dati statistici di marketing. Un esempio di questi software, dichiarato illegittimo, è il **Sony rootkit**, un **trojan** inserito nei CD venduti da Sony, che viene installato sul computer dell'acquirente, con l'intento di impedire copie illecite. Molti dei primi programmi malevoli sono stati scritti come esperimento o

... UNA BATTAGLIA IMPARI DA COMBATTERE CON IL GIUSTO ALLEATO .... LE STRATEGIE.

alla nostra clientela si basa su **servizi continuativi** che vengono tagliati sulle specifiche esigenze del singolo cliente. Non si tratta di mera movimentazione di box o vendita di licenze software ma di **un servizio a 360°** che faccia completamente perno sulle capacità tecniche e di sviluppo di **team di esperti italiani.**

Per coloro che hanno avuto la pazienza di leggere quanto riportato nella sezione a sinistra ... **altro che MALdiMARE, abbiamo preso un MALdiWARE** ad opera del nostro responsabile Ricerca e Sviluppo si può affermare che ogni tipologia di malware necessita della propria **tecnica di attacco e combattimento**. Lo staff Ricerca e Sviluppo è impegnato quotidianamente nella implementazione di soluzioni innovative per attuare tutto quanto utile e necessario ad innalzare il livello di sicurezza del sistema informativo contro i malware.
Tra gli strumenti implementati merita una doverosa nota il sistema AntiVirus adottato e proposto alla clientela. Si tratta della soluzione sviluppata dalla principale casa di produzione software antivirus italiana (TGSoft) che permette, dati alla mano, di bloccare praticamente tutte le tipologie di infezione virale attualmente presenti sul mercato. In particolare è doveroso citare che in tutte le occasioni necessarie si è rilevato **estremamente efficace** contro agenti di **cryptolocking**, bloccando completamente o limitando a poche unità di documenti l'infezione virale.

Accanto alla soluzione di AntiVirus vengono messe in campo, principalmente, **tre ulteriori soluzioni** a completamento della politica di sicurezza attiva del sistema informativo. Contro i tentativi di trasmissione degli agenti malware su veicoli quali la messaggistica elettronica sono state messi in campo (a bordo del sistema stesso di gestione della messaggistica) **soluzioni di antispam e mail-antivirus** completamente open source che beneficiano della velocità di rilevazione ed aggiornamento delle tracce virali generate da popolose community globali.
Nulla è più efficace di un **sistema globale di rilevazione** dei virus ed aiuto vicendevole nella risoluzione delle minacce stesse. In altre parole, se si vuole minimamente pensare di bloccare un attacco è **inutile chiudersi** nei laboratori ed aspettare: è necessario **scendere in campo** ed agire dialogando con più soggetti possibili. Contro i tentativi di accesso **fraudolento** alla rete informatica aziendale sono in campo tutti gli **agenti e controlli del nostro Director Center**: soluzione open source di controllo delle linee dati e di firewalling.

Non vi è alcuna connessione dati da e verso il vostro sistema

PHOENIX INFORMATICA SRL SOFTWARE & INFORMATION TECHNOLOGY

Via Giovanni Quarena, 124
25085 GAVARDO (BS) Italy

t +39 (0)365 371 796
f +39 (0)365 376 640

info@phoenix.it
www.phoenix.it

PHOENIX INFORMATICA DAL 1989

NEWSLETTER10 | marzo 2017

... ALTRO CHE MAL DI MARE, ABBIAMO PRESO IL MAL*di*WARE ... UN PO' DI STORIA.

scherzo. Oggi il malware viene usato sia da hackers che dai governi, per **rubare informazioni personali**, finanziarie o d'affari. Il malware viene usato a volte anche contro enti governativi o siti web aziendali, per carpire informazioni riservate, o, in generale, per interferire con le loro operazioni. Tuttavia, il malware viene usato anche contro singoli individui per ottenere informazioni personali, come numeri identificativi, id e password, o numeri di carte di credito. **I bersagli a più alto rischio di essere colpiti da malware sono i computer personali incustoditi**, soprattutto quelli collegati ad una rete informatica, dato che è possibile propagare l'attacco a tutti i computer collegati in rete: per questo motivo è necessario prendere varie precauzioni su ogni computer collegato alla rete informatica, come l'uso di Firewall e Antivirus. Con l'avanzare dello sviluppo di internet e la crescita degli utenti collegati, il malware viene sempre più utilizzato per fini di lucro. Fin dal 2003, la maggior parte dei virus e worm sono stati creati per prendere il controllo del computer dell'utente vittima per scopi illeciti. Vengono usati Computer zombie per l'invio di email di Spam, per salvare materiale pornografico o per effettuare attacchi distribuiti Denial of Service (DoS). I programmi malware con lo scopo di monitorare la navigazione web, di mostrare a video pubblicità indesiderate, o di reindirizzare i ricavi di affiliate Marketing, vengono chiamati Spyware. Uno spyware non si diffonde come i virus, ma viene installato sfruttando delle debolezze nella sicurezza informatica. Possono anche essere nascosti e inseriti all'interno di software che verranno usato dall'utente vittima. I Ransomware sono creati con lo scopo di infettare un computer e di richiedere un pagamento alla vittima, per eliminare lo stesso malware dalla macchina vittima dell'attacco. Per esempio, **un CryptoLocker cripta i dati presenti sul computer vittima** ed effettua la decriptazione solo su pagamento di una somma di denaro cospicua. Alcuni malware sono usati per **generare denaro** con la tecnica Click fraud, simulando un click sul computer dell'utente su una pubblicità su un sito, generando un pagamento da parte dell'inserzionista della stessa pubblicità. È stato stimato che nel 2015, all'incirca **il 60-70% di tutto il malware** attivo usasse una sorta di Click fraud, e che il 22% di tutti gli ad-click fosse fraudolento. Il malware viene spesso usato per scopi criminali, ma può essere usato anche per sabotare, spesso senza un beneficio diretto agli autori del malware. Un esempio di **sabotaggio** è stato Stuxnet, usato per distruggere dell'attrezzatura industriale specifica. Ci sono stati degli **attacchi con motivi politici** che hanno colpito delle grandi reti di computer con lo scopo di sabotare la rete stessa, ma anche per effettuare massicce cancellazioni di file o per corrompere il Master boot record, descritto come "computer killing". Attacchi simili sono stati stati fatti a Sony Pictu-

... UNA BATTAGLIA IMPARI DA COMBATTERE CON IL GIUSTO ALLEATO .... LE STRATEGIE.

informativo che non venga **controllata e tracciata** e dove è necessario bloccata. Infine è opportuno citare anche la soluzione adottata per la protezione nel tempo dei propri documenti, anche contro **l'errore involontario** umano o l'azione dolosa: si tratta del sistema **File Disaster Cloning & Versioning**, una serie di agenti software dialogano con i vostri sistemi di archiviazione dati copiando in remoto (secondo una cronologia temporale modificabile) tutti i vostri archivi attuando una vera e propria politica di **Disaster Recovery** delle informazioni aziendali, mantenendo anche versioni successive del medesimo documento oppure trattenendo i documenti cancellati (di solito erroneamente) sull'archivio principale per un predeterminato periodo di tempo. Inutile affermare che, considerando la **velocità di obsolescenza** degli strumenti informatici, le soluzioni adottate sono già vecchie ancor prima di essere installate presso la clientela, appunto per questo le nostre soluzioni **non sono un prodotto/scatola** venduta al cliente, **ma un servizio** erogato mensilmente e costantemente aggiornato. Avremo modo di parlarne nelle prossime edizioni.

Buon lavoro ... ed **attenzione ai raffreddori di stagione ed al mal di mare.**

PHOENIX INFORMATICA SRL SOFTWARE & INFORMATION TECHNOLOGY

Via Giovanni Quarena, 124
25085 GAVARDO (BS) Italy

t +39 (0)365 371 796
f +39 (0)365 376 640

info@phoenix.it
www.phoenix.it

NEWSLETTER10 | marzo 2017

... ALTRO CHE MAL DI MARE, ABBIAMO PRESO IL MAL*di*WARE ... UN PO' DI STORIA.

res Entertainment (25 novembre 2014, usando un malware conosciuto come Shamoon o W32.Disttrack) ed a Saudi Aramco (Agosto 2012). La preferenza di usare il malware come strumento per compiere crimini su Internet, insieme alla sfida del software anti-malware che cerca di tenere il passo per contrastare i nuovi programmi malevoli, hanno portato alla necessità di prendere delle contromisure sia da parte dei singoli utenti, sia delle aziende, comprese le aziende che vendono prodotti tramite Internet: questo significa che devono offrire servizi web con una certa sicurezza per la tutela del cliente. L'aumento e la facile diffusione del malware, **impongono un'analisi approfondita** sui sistemi di sicurezza da usare per proteggersi dal malware avanzato che opera dai computer dei clienti dell'azienda stessa. I tipi di malware più conosciuti, ovvero virus e worm, sono noti più per il modo in cui si diffondono che per il loro effettivo comportamento. Il termine virus viene usato per un programma che si integra in qualche codice eseguibile (incluso il sistema operativo) del sistema informatico **vittima**, in modo tale da diffondersi su altro codice eseguibile quando viene eseguito il codice che lo ospita, senza che l'utente ne sia a conoscenza. Per quanto riguarda i worm, questi sono del software completo a sé stante (senza la necessità di doversi integrare in altri programmi) e si diffondono su una rete per infettare altri computer. **Merita attenzione** la tipologia **Trojan**: in informatica un Trojan (comunemente chiamato anche Cavallo di Troia) è un programma malevolo che falsa la sua vera identità per sembrare utile o interessante per persuadere la **vittima** ad installarlo. Il termine deriva dalla **storia greca del Cavallo di Troia** che venne usato dalle truppe greche per invadere la città di Troia di nascosto. I Trojan di solito vengono diffusi con qualche tecnica di Ingegneria sociale, per esempio quando un utente viene ingannato ad eseguire un allegato di una e-mail non sospettabile o ad effettuare un download. **Molti di questi Trojan** moderni, agiscono come dei Backdoor, contattando un controller che può avere accesso non autorizzato al computer infettato. Mentre i Trojan e i Backdoor non sono rilevabili di per sé, il computer vittima potrebbe risultare rallentato a causa dell'uso notevole del processore e dal traffico di rete. Al contrario dei virus e dei worm, i Trojan non tentano di iniettarsi in altri file o di propagarsi. Esiste poi la tipologia di malware definita **Rootkit**: una volta che un programma malevolo è stato installato su un sistema, è necessario che questo rimanga nascosto per evitare di essere scoperto e rimosso. I pacchetti software conosciuti come rootkit permettono **l'occultamento**, modificando il sistema operativo del computer in modo tale **da nascondere le tracce del malware**. I rootkit possono evitare che un processo malware risulti visibile nella lista dei processi attivi del sistema, e possono anche impedire che i file del malware possano essere aperti e letti. Alcuni programmi malevoli contengono procedure che **impediscono la rimozione** dal sistema dello stesso malware.
Infine merita la dovuta attenzione la tipologia definita Backdoor. Una backdoor è un metodo per bypassare le procedure standard per l'autenticazione tramite una connessione ad una rete o su internet. Una volta che il sistema è compromesso, una o più backdoor possono essere installate per permettere accessi futuri, in modo del tutto invisibile all'utente. L'idea di fondo che le compagnie produttrici di computer preinstallino delle backdoor nei propri sistemi per provvedere supporto tecnico ai clienti, non è mai stata veramente verificata. Le backdoor possono essere installate tramite Trojan, worm o altri metodi.

Approfondiamo ora uno dei malware in assoluto più antichi e diffusi, il **Virus Informatico**. Un virus, in informatica, è un software appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da fare copie di se stesso, generalmente senza farsi rilevare dall'utente (da questo punto di vista il nome è in perfetta analogia con i virus in campo biologico). Coloro che creano virus sono detti virus writer e sfruttando le vulnerabilità di un sistema operativo, arrecano danni al sistema, rallentano o rendeno inutilizzabile il dispositivo infetto. I virus comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento. Nel 1949 John von Neumann dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente. Il concetto di programma auto-replicante trovò la sua evoluzione pratica nei primi anni '60 nel gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T chiamato "Core Wars", nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici. Il termine virus venne adottato per la prima volta da Fred Cohen della University of Southern California nel suo scritto Experiments with Computer Viruses, dove questi indicò Leonard Adleman come colui che aveva adattato dalla biologia tale termine. La definizione di virus era la seguente: «Un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di se stesso». Ma il termine era già stato utilizzato prima. Nel 1972 David Gerrold scrisse un romanzo di fantascienza "La macchina di D.I.O.", dove è presente una descrizione di un programma

Via Giovanni Quarena, 124
25085 GAVARDO (BS) Italy
t +39 (0)365 371 796
f +39 (0)365 376 640
info@phoenix.it
www.phoenix.it

PHOENIX INFORMATICA DAL 1989

... ALTRO CHE MAL DI MARE, ABBIAMO PRESO IL MAL*di*WARE ... UN PO' DI STORIA.

per computer chiamato VIRUS che adotta il medesimo comportamento di un virus.
Nel 1975 John Brunner scrisse il romanzo "Codice 4GH" in cui sono descritti programmi chiamati tapeworms che si infiltrano nella rete con lo scopo di cancellare tutti i dati. Il termine virus del computer con il significato corrente è inoltre presente anche nell'albo a fumetti Uncanny X-Men n. 158 pubblicato nel 1982. Si può dunque affermare che Cohen fece per primo uso della parola virus solo in campo accademico, dato che questa era già presente nella lingua parlata. Il primo malware della storia informatica è stato Creeper, un programma scritto per verificare la possibilità che un codice potesse replicarsi su macchine remote. Il programma chiamato Elk Cloner è invece accreditato come il primo virus per computer apparso al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata con lo scambio di floppy disk: il virus si copiava nel settore di boot del disco e veniva caricato in memoria insieme al sistema operativo all'avvio del computer. Nel corso degli anni ottanta e nei primi anni novanta fu lo scambio dei floppy la modalità prevalente di contagio da **virus informatici**. Dalla metà degli anni novanta, invece, con la diffusione di internet, i virus ed i cosiddetti malware in generale, iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni. Il primo virus informatico che si guadagnò notorietà a livello mondiale venne creato nel 1986 da due fratelli pakistani proprietari di un negozio di computer per punire, secondo la loro versione, chi copiava illegalmente il loro software. Il virus si chiamava Brain, si diffuse in tutto il mondo e fu il primo esempio di virus che infettava il settore di avvio del DOS. Il primo file infector apparve nel 1987, si chiamava Lehigh e infettava solo il file command.com. Nel 1988 Robert Morris Jr. creò il primo worm che si diffondeva via internet, il Morris worm. L'anno seguente, nel 1989, fecero la loro comparsa i primi virus polimorfi, con uno dei più famosi: Vienna, e venne diffuso il trojan AIDS (conosciuto anche come Cyborg), molto simile al trojan dei nostri giorni chiamato PGPCoder.
Entrambi infatti codificano i dati del disco fisso chiedendo poi un riscatto all'utente per poter recuperare il tutto. Nel 1995 il primo macrovirus, virus scritto nel linguaggio di scripting di programmi di Microsoft come MS-Word ed Outlook che infetta soprattutto le varie versioni dei programmi Microsoft attraverso lo scambio di documenti. Concept fu il primo macro virus della storia. Nel 1998 la nascita di un altro dei virus storici, Chernobyl o CIH, famoso perché sovrascriveva il BIOS della scheda madre e la tabella delle partizioni dell'hard disk infettato ogni 26 del mese. La diffusione di massa di Internet nella fine degli anni 90 determina la modifica delle tecniche di propagazione virale: non più floppy ma via e-mail. Tra i worm di maggior spicco antecedenti al 2000: Melissa, Happy99 e BubbleBoy, il primo worm capace di sfruttare una falla di Internet Explorer e di autoeseguirsi da Outlook Express senza bisogno di aprire l'allegato.
Nel 2000 il famoso I Love You che dà il via al periodo degli script virus, i più insidiosi tra i virus diffusi attraverso la posta elettronica perché sfruttano la possibilità, offerta da diversi programmi come Outlook e Outlook Express di eseguire istruzioni attive (dette script), contenute nei messaggi di posta elettronica scritti in HTML per svolgere azioni potenzialmente pericolose sul computer del destinatario. I virus realizzati con gli script sono i più pericolosi perché possono attivarsi da soli appena il messaggio viene aperto per la lettura. I Love You si diffuse attraverso la posta elettronica in milioni di computer di tutto il mondo, al punto che per l'arresto del suo creatore, un ragazzo delle Filippine, dovette intervenire una squadra speciale dell'FBI. Era un messaggio di posta elettronica contenente un piccolo programma che istruiva il computer a rimandare il messaggio appena arrivato a tutti gli indirizzi contenuti nella rubrica della vittima generando una specie di catena di sant'Antonio automatica che saturava i server di posta. Dal 2001 si è registrato un incremento di worm che, per diffondersi, approfittano di falle di programmi o sistemi operativi senza bisogno dell'intervento dell'utente. **L'apice nel 2003 e nel 2004:** SQL/Slammer, **il più rapido worm della storia** - in quindici minuti dopo il primo attacco, Slammer aveva già infettato metà dei server che tenevano in piedi internet mettendo fuori uso i bancomat della Bank of America, spegnendo il servizio di emergenza 911 a Seattle e provocando **la cancellazione per continui e inspiegabili errori nei servizi di biglietteria e check-in di alcune compagnie aeree; ed i due worm più famosi della storia: Blaster e Sasser.** Nel giugno 2009 è nata una nuova tipologia di virus che ha come bersaglio sistemi informatici industriali, il primo virus di questa nuova tipologia è stato Stuxnet che ha preso di mira i sistemi SCADA. **Oggigiorno è impossibile definire quante e quali tipologie di virus informatici** siano in circolazione, ma una cosa è certa: considerando il livello di inclusione ed interconnessione col tessuto informatico ed internet di ognuno di noi è imprescindibile ed estremamente importante affrontare l'argomento con pragmatismo e determinazione, **senza lasciare nulla al caso.**

PHOENIX INFORMATICA SRL SOFTWARE & INFORMATION TECHNOLOGY

Via Giovanni Quarena, 124
25085 GAVARDO (BS) Italy

t +39 (0)365 371 796
f +39 (0)365 376 640

info@phoenix.it
www.phoenix.it