

12 PREVISIONI SULLA SICUREZZA PER IL 2012





Ogni anno, in questo periodo, mi riunisco con i miei team di ricerca per parlare di ciò che l'anno appena iniziato porterà in termini di minacce ai nostri clienti. È un dialogo importante che ci consente non solo di condividere con voi ciò a cui pensiamo vi dobbiate preparare, ma che ci permetterà di orientarci mentre continuiamo a creare prodotti e servizi che assicurano la vostra protezione da queste minacce.

Quest'anno, guardando verso il futuro, abbiamo individuato 12 previsioni per il 2012 articolate in quattro categorie principali:

- Grandi tendenze IT
- Panorama dei dispositivi mobili
- Panorama delle minacce
- Fughe e violazioni di dati

Osservando queste previsioni, emerge come comune denominatore una tendenza verso aggressori sempre più sofisticati e un allontanamento dai desktop PC-centrici. La speranza che riponevamo sui nuovi sistemi operativi, affinché rendessero più sicuro l'ambiente globale, è naufragata. Ciò significa che nel 2012 i nostri clienti dovranno continuare ad andare nella direzione di un modello più data-centrico, per assicurarsi una protezione e una riservatezza efficaci nel momento in cui accolgono

consumerizzazione, virtualizzazione e il cloud. E noi di Trend Micro dobbiamo continuare ad occuparci di questi ambiti per consentire ai nostri clienti di affrontare e di proteggersi da queste tendenze per il 2012.

Presso Trend Micro, ci impegniamo sempre per cercare di capire non solo le minacce di oggi, ma anche quelle di domani; del resto lo dice anche il nostro nome (trend = tendenza). Tutto ciò ci aiuta ad aiutarvi a proteggere meglio i vostri dati e le vostre risorse.

Ci auguriamo che le previsioni per quest'anno possano essere per voi non solo interessanti ma soprattutto utili per rendere il 2012 un anno sicuro e protetto.

Raimund

Raimund Genes
CTO, Trend Micro



GRANDI TENDENZE IT



1 Anche se molte aziende sono tuttora in difficoltà con la consumerizzazione, gli incidenti legati alla sicurezza e alle violazioni dei dati nel 2012 imporranno loro di affrontare le sfide legate al concetto di BYOD (Bring-Your-Own-Device o porta il tuo dispositivo).

L'epoca del Bring-Your-Own-Device, del BOYD o "porta il tuo dispositivo", non accenna a sparire. Man mano che si archiviano o che si accede a un numero sempre maggiore di dati mediante dispositivi che non sono totalmente controllati dagli amministratori IT, la probabilità di incidenti che causano un perdita di dati attribuibile all'uso di dispositivi personali con misure di protezione insufficienti aumenterà. Vedremo senza dubbio incidenti di questa natura nel 2012.



A photograph of three men in a server room. They are crouching in front of several rows of server racks. The man on the left is wearing glasses and a grey patterned shirt. The man in the middle is wearing a light blue shirt. The man on the right is wearing a blue shirt. The server racks are filled with equipment, and there are cables visible. The room has a greenish tint from the lighting.

La vera sfida per i titolari dei datacenter sarà affrontare le sempre maggiori complessità insite nel garantire la protezione dei sistemi fisici, virtuali e in-the-cloud.

2

Mentre gli attacchi mirati specificamente alle macchine virtuali (VM) e ai servizi di cloud computing restano una possibilità, gli aggressori non avranno il bisogno immediato di far ricorso a questi ultimi poiché gli attacchi mirati convenzionali resteranno efficaci in questi nuovi ambienti. Le piattaforme virtuali e in-the-cloud sono sempre facili da attaccare, ma più difficili da proteggere. L'onere ricadrà quindi sugli amministratori IT, che devono proteggere i dati critici delle rispettive aziende mentre adottato queste tecnologie. Installare patch in un grande insieme di server virtualizzati è una sfida, perché può consentire agli hacker di assumere il controllo dei server, di deviare il traffico e/o di impadronirsi di dati dai sistemi vulnerabili.

PANORAMA DEI DISPOSITIVI MOBILI



A woman with blonde hair is looking down at her smartphone. She is wearing a light-colored blazer. The background is a blurred office setting with white blinds. The image is partially obscured by a blue vertical bar on the right side.

3

Le piattaforme smartphone e tablet, specie *Android*, subiranno molti attacchi di criminali informatici.

Mentre l'uso degli smartphone continua a crescere in tutto il mondo, le piattaforme mobili diventeranno obiettivi sempre più allettanti per i criminali informatici. La piattaforma *Android*, in particolare, è diventata uno dei bersagli preferiti per via del suo modello distributivo, che la rende completamente aperta a tutti. Crediamo che questo trend continuerà nel 2012 e che altre piattaforme subiranno un analogo fuoco di fila.

A man in a white shirt and striped tie is holding a smartphone with a stylus. The background is a blurred office setting with light-colored blinds.

Verranno rilevate vulnerabilità della sicurezza in applicazioni mobili legittime, tanto da facilitare l'estrazione di dati ai criminali informatici.

4

A oggi, le minacce alle piattaforme mobili arrivano sotto forma di app dannose. In futuro, prevediamo che i criminali informatici prenderanno di mira anche le app legittime. Riusciranno probabilmente a individuare vulnerabilità o errori di codifica da sfruttare per compiere furti o esposizione dei dati utenti. A questo va ad aggiungersi il fatto che sono molto rari gli sviluppatori di app che dispongono di un processo maturo di gestione e ripristino delle vulnerabilità, tanto che la finestra di esposizione di questi difetti potrebbe anche risultare più lunga.

PANORAMA DELLE MINACCE





5

Anche se i botnet diventeranno più piccoli, aumenteranno di numero e renderanno le efficaci retate delle forze dell'ordine assai più difficili da effettuare.

I botnet, lo strumento tradizionale dei criminali informatici, si evolveranno in risposta alle azioni adottate dal settore della protezione. I giorni dei grandi numeri per i botnet potrebbero essere finiti. Potrebbero invece venire sostituiti da botnet più numerosi, più piccoli e maggiormente gestibili. Botnet più piccoli ridurranno i rischi per i criminali informatici, tanto che la perdita di un singolo botnet non sarà più così sentita come in passato.



Gli hacker prenderanno di mira bersagli non tradizionali tanto che potranno venire attaccate le apparecchiature collegate a Internet con problemi, dalle macchine industriali pesanti controllate tramite SCADA alle apparecchiature mediche.

6

Gli attacchi che prendono di mira i sistemi SCADA (Supervisory Control And Data Acquisition) e altre apparecchiature accessibili tramite le reti si intensificheranno nel 2012 e gli aggressori andranno oltre il furto di denaro o di dati importanti. Nel 2011, STUXNET e altre minacce hanno evidenziato come SCADA sia diventato un obiettivo di punta. Si prevede che ne conseguiranno attacchi proof-of-concept (POC) contro i sistemi collegati alle reti, tra cui le apparecchiature mediche.



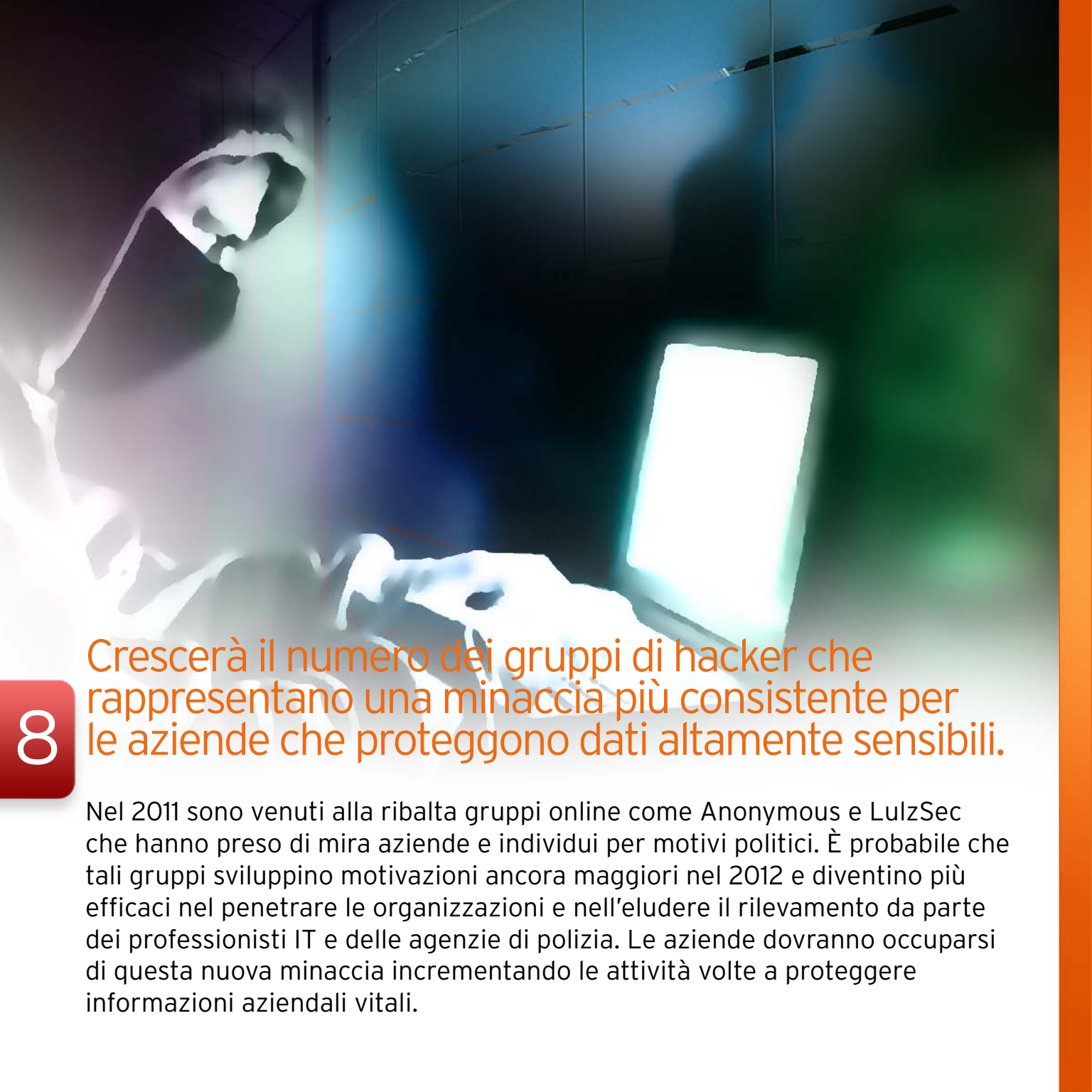
7

I criminali informatici troveranno metodi più creativi per nascondersi dalle forze dell'ordine

e cercheranno sempre più di arricchirsi sfruttando fonti di reddito online legittime come la pubblicità online. In tal modo potranno più facilmente nascondersi dagli occhi della legge e dagli addetti ai controlli antifrode ingaggiati dalle banche e da altri istituti finanziari.

FUGHE E VIOLAZIONI DI DATI





8

Crescerà il numero dei gruppi di hacker che rappresentano una minaccia più consistente per le aziende che proteggono dati altamente sensibili.

Nel 2011 sono venuti alla ribalta gruppi online come Anonymous e LulzSec che hanno preso di mira aziende e individui per motivi politici. È probabile che tali gruppi sviluppino motivazioni ancora maggiori nel 2012 e diventino più efficaci nel penetrare le organizzazioni e nell'eludere il rilevamento da parte dei professionisti IT e delle agenzie di polizia. Le aziende dovranno occuparsi di questa nuova minaccia incrementando le attività volte a proteggere informazioni aziendali vitali.



9 La nuova generazione avvezza ai social network ridefinirà il concetto di "privacy".

Le informazioni riservate degli utenti finiscono online, in gran parte grazie agli utenti stessi. La nuova generazione di giovani frequentatori dei social network ha un diverso atteggiamento verso la protezione e la condivisione delle informazioni. Sono più inclini a rivelare informazioni personali a terzi come avviene nei siti dei social network. È anche assai meno probabile che adottino provvedimenti per limitare la divulgazione delle informazioni a specifici gruppi di persone, ad esempio gli amici. In pochi anni, le persone a cui sta a cuore la privacy saranno una minoranza, una prospettiva ideale per gli aggressori.



10

Man mano che l'ingegneria sociale si diffonde a tutti i livelli, anche le aziende diventeranno facili bersagli.

A oggi, le più astute manovre di ingegneria sociale sono state dirette contro le grandi aziende. Tuttavia i criminali informatici sono oggi talmente esperti di ingegneria sociale che le attività volte a prendere di mira le aziende individualmente si fanno sempre meno costose. Questo aspetto e il volume sempre maggiore di informazioni personali disponibili online consentiranno ai criminali informatici di lanciare attacchi più personalizzati e affinati contro aziende di ogni taglia. Come negli attacchi precedenti, i criminali informatici continueranno a tentare di acquisire l'accesso ai conti bancari online delle aziende.

A person is shown in profile, looking at a computer monitor. The monitor displays a login interface with fields for 'Username' and 'Password', a 'Login' button, and a 'Connecting to Database' dialog box. The dialog box contains an error message: 'An error has occurred while connecting to Database P1212.' Below the dialog box, a red banner with the text 'ACCESS DENIED' is overlaid on the screen. The background is dark with bokeh light effects.

11

Nuovi perpetratori di minacce utilizzeranno strumenti criminali sofisticati per raggiungere i propri scopi.

Il numero degli attacchi mirati continuerà a crescere nel 2012. I criminali informatici non saranno tuttavia i soli a sferrare questi attacchi. Man mano che l'efficacia delle minacce persistenti avanzate si intensifica, altre figure come i gruppi di attivisti, le grandi società e i governi si troveranno a dover usare analoghi strumenti e tattiche criminali per conseguire i propri obiettivi.

12

Nel 2012 ci saranno più incidenti di perdita dei dati di alto profilo tramite infezioni da minacce informatiche e azioni di hacking.

Nel 2012 gli attacchi di alto profilo continueranno a colpire la maggioranza delle aziende. Dati aziendali fondamentali verranno estratti tramite le infezioni da minacce informatiche e le azioni di hacking. Ne conseguiranno quindi gravi incidenti di perdita di dati che potranno potenzialmente riguardare migliaia di utenti e i loro dati personali. Tali incidenti possono causare significative perdite dirette e indirette alle parti interessate.





Trend Micro Incorporated, leader mondiale delle soluzioni di sicurezza in-the-cloud, crea un mondo sicuro per lo scambio di informazioni digitali grazie alla protezione dei contenuti Internet e alle soluzioni di gestione delle minacce per aziende e privati. Come pionieri della protezione dei server con più di 20 anni di esperienza, offriamo una sicurezza di punta per client, server e in-the-cloud che si adatta perfettamente alle esigenze dei nostri clienti e partner, blocca più rapidamente le nuove minacce e protegge i dati in ambienti fisici, virtualizzati e in-the-cloud. Basati sull'infrastruttura Trend Micro™ Smart Protection Network™, la nostra tecnologia e i nostri prodotti e servizi leader del settore per la protezione in ambito di cloud computing bloccano le minacce non appena si presentano, su Internet, e sono supportati da più di 1.000 esperti di minacce informatiche a livello globale. Per ulteriori informazioni visitate www.trendmicro.com.



Securing Your Journey
to the Cloud

©2011 by Trend Micro, Incorporated. Tutti i diritti riservati. Trend Micro e il logo Trend Micro della sfera con il disegno di una T sono marchi o marchi registrati di Trend Micro Incorporated. Tutti gli altri nomi di aziende o prodotti potrebbero essere marchi o marchi registrati dei rispettivi proprietari.