L’anno che verrà: le minacce informatiche del 2016.

Come ogni anno, nel mese di dicembre si assiste alla pubblicazione di diversi rapporti sul Cybercrime da parte delle aziende di antivirus e di sicurezza informatica, con le previsioni per le “cyber minacce” del 2016.

Grazie al rapporto di collaborazione di lunga data con ANSA, ogni anno offro ai lettori della più importante agenzia di stampa italiana una chiave di lettura diversa, basata sulla Cyber Intelligence e su molteplici analisi sul campo da parte di Security Brokers e dei diversi team internazionali con cui collaboriamo operativamente.

Negli anni passati era stato proprio il sottoscritto ad anticipare all’ANSA novità davvero eclatanti, centrando regolarmente le previsioni: dagli oramai famosi “*hacking ai frigoriferi”* piuttosto che la proliferazione di “0-days” nel mondo mobile, sino all’escalation dell’hacking nel mondo dell’Information Warfare, come il conflitto in Ucraina ha peraltro pienamente confermato.

Anche per il 2016 ho spiegato in esclusiva ad ANSA le mie visioni (e previsioni), per prepararci in tempo a quello che vedremo nei prossimi dodici mesi; una lista diversa dal solito, un’analisi oggettiva e personalizzata di un mondo che continua a cambiare, sotto i nostri occhi. Anche se sono in pochi ad accorgersene. Al convegno ABI “Banche & Sicurezza” ho voluto fare il punto, dopo quasi sei mesi, rispetto a quanto avevo previsto. Purtroppo anche quest’anno, così come per tutte le previsioni espresse negli anni precedenti, non ho sbagliato…. Come ho detto pubblicamente durante il mio intervento, questo è uno dei rari casi in cui avrei decisamente preferito sbagliare.

1. Cybercriminali d’oltre cortina: l’Occidente di nuovo nel mirino

Quasi il 90% del crimine digitale mondiale ha origine, e viene gestito, dall’Europa dell’Est, in particolare dalla Russia, dall’Ucraina e dalla Bielorussia: è il cosiddetto *Cybercrime d’oltre cortina*, composto da un insieme di organizzazioni criminali internazionali che ci derubano ogni anno di oltre 20 miliardi di Euro.

Se il 2015 ha visto un focus di queste organizzazioni verso i continenti di diversi Paesi emergenti, come l’America Latina, l’Asia-Pacifico, l’area del Golfo e l’Africa, per il 2016 i miei analisti prevedono un ritorno verso l’Occidente, in particolare verso l’Europa e gli USA.

La chiave di lettura delle principali minacce portate da queste organizzazioni criminali è molto semplice, vanno dove c’e’ il denaro, come confermano la maggior parte delle previsioni per il 2016 illustrate nei prossimi punti.

2. ATM sempre più esposti

I moderni sistemi ATM altro non sono che computer su cui gira Windows e che offrono funzionalità evolute: non solo il "banale" prelievo, ma anche pagamenti di utenze, deposito di contanti e molto altro.

Come gli esperti che combattono ogni giorno il Cybercrime sanno bene, esistono alcuni gruppi criminali specializzati nella scrittura di *ATM malware*, ovverosia software maligno scritto appositamente per il mondo degli ATM. Ad oggi però nessuno di loro, per quanto pubblicamente noto, è mai stato individuato ed arrestato.

Questo fa sì che il numero di incidenti relativi al furto di contante dai Bancomat mediante "hacking" sia purtroppo destinato ad aumentare.

3. Hacking automatizzato ai POS

Anticipai ad ANSA il fenomeno delle *Next Generation POS frauds* già nel 2014. Purtroppo, neppure in questo caso la mia previsione si è rilevata "error free": da allora il numero di carte clonate proprio nei sistemi POS è aumentato drasticamente.

Sino al 2012 circa la preoccupazione principale dei possessori di carte di credito era diretta verso i Bancomat modificati con "skimmer" per clonare la carta stessa (nel caso di prelievo con carta di credito) e sempre maggiori erano le preoccupazioni per gli acquisti via Internet e le transazioni di e-banking.

"Già nei primi mesi del 2016 assisteremo invece a clonazioni di carte causate da POS e Totem infetti", predissi all'ANSA. Con *totem* intendiamo quelle casse automatiche che utilizziamo per pagare con le nostre carte di credito diversi servizi, come ad esempio i parcheggi degli aeroporti, o le biglietterie automatiche per treni ed autobus: probabilmente l'ultimo posto dove un correntista si aspetterebbe una clonazione. I POS verranno anch'essi attaccati da remoto, via Internet, e non più fisicamente "sul posto", come accadeva negli anni precedenti.

"Nel 2016 assisteremo dunque ad un proliferare di *trojan* scritti appositamente per sistemi POS e Totem, oltre che all'automatizzazione di alcuni processi propri di questa catena industriale-criminosa, che permette la clonazione di migliaia di carte di credito per ogni terminale POS infettato e compromesso". Purtroppo, un'altra previsione azzeccata.

4. Attacchi ai sistemi di scambio borsistico

"E' un tema molto caldo", spiegai all'ANSA, e di cui ovviamente si parla poco: c'è una sorta di "omertà", nel settore della Borsa, ancora di più che nel mondo bancario; diciamo che vi è un'estrema attenzione verso la reputazione e l'immagine.

Nel 2015 abbiamo assistito al primo attacco pubblicamente noto ad un sistema di Financial Trading della storia (alla vittima furono sottratti circa 300 milioni di rubli, corrispondenti ad oltre 5 milioni di Euro) ; la diretta conseguenza è stata una sorta di incertezza verso questi sistemi, mentre quella indiretta è che già oggi alcuni malware altamente specializzati già includono al proprio interno funzionalità dedicate ai sistemi di scambio finanziario.

Seppur non scritti per attaccare *direttamente* le società che gestiscono le Borse, questi malware opereranno invece contro i clienti dei sistemi di trading, come già accaduto per realtà come TRANSAQ, E*Trade e QUIK.

5. Il numero di incidenti relativi ai cryptolocker aumenterà

Sembra davvero che i navigatori – italiani inclusi – non abbiano ancora compreso bene il pericolo che viene dai cosiddetti Cryptolocker, una categoria di "ransomware", ovverosia malware che richiedono un riscatto per restituirci i nostri dati. Tantissimi gli incidenti eclatanti avvenuti nel 2015 anche in Italia, incluse grosse organizzazioni, aziende famose e, purtroppo, diverse Pubbliche Amministrazioni, sia Centrali che Locali, tra cui ASL, Comuni ed Anagrafi di varie dimensioni.

"Le differenze nel 2016 saranno principalmente due", spiegai all'ANSA. Innanzitutto, nuove tipologie di ransomware scritti appositamente per gli utenti della mela, chiamati appunto *Apple Locker*, scritti proprio per attaccare gli utenti Apple. In seconda istanza, quella che se vogliamo potremmo chiamare la rottura di un simulacro, la violazione di un porto sicuro: ransomware verso i sistemi Linux, gli unici ad oggi ritenuti davvero sicuri da questa tipologia di malware.

Avevo inoltre lanciato un allarme molto serio e preoccupante verso la PA: "a quanto ci risulta, diverse organizzazioni di Cybercrime hanno deciso di puntare proprio alle pubbliche amministrazioni: questo mi fa purtroppo ipotizzare un elevato fattore di rischio per i dati dei cittadini.", conclude Chiesa.

6. Dispositivi mobili sempre più a rischio

I cybercriminali continuano imperterriti a sviluppare nuove funzionalità per i propri trojan, dopo aver deciso già nel 2013 di aggiungere il mondo del mobile ai propri obiettivi.

In questo caso l'obiettivo è prendere il controllo completo del telefono della vittima, dall'elenco delle chiamate agli SMS, comprese le fotografie ed i video presenti sullo smarphone. Nel caso di alcuni spyware per il mondo mobile, i miei colleghi hanno individuato funzionalità molto innovative, che permettevano non solo l'accesso a tutti i file presenti sullo smartphone, ma anche alle informazioni di geolocalizzazione ed all'archiviazione (e copia/backup) su server Cloud.

Tutti i trojan di nuova generazione esaminati dai miei colleghi, specialmente quelli per piattaforme Android (notoriamente più vulnerabile e più esposta a rischi rispetto all'iOS di casa Apple) avevano funzionalità completamente automatizzate per il furto di denaro (mediante abuso delle piattaforme Google Play ed Apple Store) e la raccolta incondizionata delle carte di credito ivi utilizzate: possiamo ben comprendere come, a questo punto, non abbia più alcuna importanza quale sia l'istituto bancario della vittima.

7. Il cloud ed i nostri dati

Il Cloud sarà un successo, che piaccia o no; io sono personalmente favorevole ad un modello di *Hybrid Cloud*, un mix tra Cloud privato e Cloud Pubblico, ma questo ben poco toglie ad una certezza: i dati su Cloud continueranno ad aumentare, perché il Cloud porta risparmio economico e benefici (seppur apparenti, almeno per la maggior parte) alle aziende, specialmente le PMI. E poi c'è il discorso della PA, dove il Cloud diverrà quasi una parola d'ordine.

Il 2015 ci ha purtroppo resi testimoni della violazione di moltissimi Cloud provider, così come del furto di dati (inclusi foto e video) di diversi VIP: le previsioni per il 2016 narrano di un aumento del rischio quasi esponenziale, complice la non capacità o la non volontà degli utenti Cloud di proteggere i propri dati, magari mediante tecniche di cifratura.

8. Automotive, Internet of Things

Il 2015 non sarà ricordato solo come l'anno del Gruppo Wolkswagen e del software modificato, ma anche per l'hack alle Jeep di FCA, Fiat Chrysler Automobiles, come peraltro già successo anni prima a Toyota (con la Prius, ma anche con altri modelli).

L'aumento della componente ICT dentro le automobili deve necessariamente accompagnarsi a serie analisi del livello di sicurezza informatica, se non addirittura ad un radicale cambio di approccio da parte di costruttori automobilistici, dove invece dell'attuale "progettiamo, poi nel caso verifichiamo" dovrebbe essere completamente sostituito da una "Progettazione sicura" anche a livello informatico, e non solo relativa ai crash-test.

La differenza è che non parliamo del rischio di conti bancari svuotati, bensì di vite umane: nel caso Jeep di FCA, Miller ed il suo team hanno dimostrato come fosse possibile intervenire remotamente sul sistema motore ed il sistema frenante. Io non voglio essere seduto su un'auto che è esposta a questa tipologia di attacchi…e voi?

Ed ancora di vite umane si parla con il secondo tema che affrontaii in queste previsioni per il 2016, il gettonatissimo "Internet of Things", l'Internet delle Cose.

Già oggi l'IoT (Internet of Things) è chiamata nel nostro settore *IoX*, Internet of Everything: nei prossimi anni tutto sarà interconnesso, ed ognuno di questi dispositivi intelligenti avrà un indirizzo IP. Tutto questo, per una persona come me che ama la tecnologia, è davvero bellissimo ed apre la strada a scenari di totale innovazione, per un mondo davvero migliore. Nel contempo però, espone anche il fianco a scenari di attacchi informatici, peraltro già ampiamente dimostrati da colleghi ethical hacker, i quali negli anni passati hanno scoperto vulnerabilità in pace maker, pompe di insulina ed altri dispositivi medici "smart", date le loro funzionalità di controllo e scambio dati via Wireless, Bluetooth o ZigBee.

Prevediamo quindi un aumento esponenziale del numero di vulnerabilità verso i device dell'Internet of Things", già nel corso del 2016 e per gli anni a venire, quantomeno sino al 2020.

9. Ethical Hackers e Governi

Non c'era bisogno di Edward Snowden, né dell'*affaire Hacking Team*, per capire come i Governi, ed in particolare le Agenzie di Intelligence ed i Ministeri della Difesa, facciano uso di hacker etici e di aziende private, esperte nel settore dell'Information Security.

Spiegai quindi all'ANSA come, "complice un'impennata nell'uso della tecnologia odierna da parte di diverse organizzazioni terroristiche, la lotta al terrorismo si combatterà sempre più (anche) mediante hacking, ovverosia la violazione - in questo caso "autorizzata" - di sistemi informatici e reti di telecomunicazione".

Parliamo di uno degli aspetti meno noti del mondo dell'Intelligence, della difesa nazionale e del contrasto al terrorismo; sono aspetti che, a volte, non sono noti nemmeno agli esperti del settore della Sicurezza Informatica o alle associazioni di categoria.

Questi "rapporti particolari" sono dunque, giocoforza, destinati ad aumentare per numero e tipologia, data l'evidente legge della domanda (molta) e dell'offerta (poca); naturalmente, è poco probabile che la gente comune ne verrà a conoscenza.

10. Frodi, frodi ed ancora frodi.

Concludiamo questo approfondimento e questa specialissima "classifica" delle minacce per il 2016 con quello che, forse, è da ritenere come uno degli aspetti più importanti tra le minacce cyber, una sorta di "fattor comune" a tante tipologie di cyber-attacchi: come l'attaccante fa "abboccare" la vittima.

Con il mio team abbiamo analizzato decine di migliaia di incidenti, alla base dei quali c'è sempre il furto di identità, che porta successivamente al furto di informazioni.

Per il 2016 prevedo l'utilizzo da parte delle organizzazioni criminose di diverse "campagne" per fare "abboccare" utenti e cittadini:

- ✓ Impersonificazione dell'Agenzia delle Entrate e della Polizia Postale;
- ✓ Falsificazione del numero chiamante (Caller ID spoofing) con impersonificazione del nostro istituto bancario;
- ✓ False organizzazioni di carità ed ONG;
- ✓ Impersonificazione di corrieri e delle Poste Italiane.

In tutti questi casi, l'obiettivo dei cyber criminali sarà quello di farsi comunicare dalle vittime le credenziali (utente, password) a loro necessarie per commettere frodi, ivi incluse altri informazioni utili o sensibili: facciamo quindi attenzione a comunicazioni e-mail e telefoniche: la frode potrebbe essere dietro l'angolo!