curezza:
ementi di attenzione e possibili soluzioni

poli, 23 ottobre 2015

Silvio FERRARI | Head of Sales Eng
Puntoit Servizi Informatici

è Puntoit

ntoit è una società specializzata nel mercato italiano dell'IT Security

importanti accordi di partnership con i principali vendor di soluzioni e servizi di sicurezza

presente sul mercato ICT italiano dal 1998, con sedi a Milano, Roma e Modena

organico è composto da circa 50 security specialist, in possesso delle certificazioni su tecnologie leader di settore

fortemente orientata all'innovazione tecnologica

ell'ambito security si occupa di:

- Sicurezza, IT governance e compliance
- Progettazione, realizzazione e gestione delle infrastrutture
- Aspetti organizzativi e impatti funzionali sui processi

on si parla più di virus o malware, ma di gruppi organizzati di hacker, che:

- dispongono di finanziamenti superiori alla capacità di spesa di chi si difende
- sono veri e propri gruppi di lavoro organizzati in modo «industriale»
- sono specializzati su mercati verticali
- operano su un ampio arco temporale

mbia la superficie esposta agli attacchi:

- la rete, gli endpoint e i server
- ATM (bancomat)
- reti di produzione (ICS/SCADA)
- smartphone e tablet
- IoT (frigoriferi, lavatrici…)
- aerei
- automobili
- apparati elettromedicali

Hacker prendono il controllo di una Jee wireless

Vulnerabilità di sicurezza nei dispositivi per la regolazione de somministrazione dei medicinali

Pubblicato il 19 maggio 2015

Hacker preso i di un a durant

Uno hackathon per lo he

on 25 maggio 2015 |

Le maratone del codice avvantaggiano anche il r

Il concetto di Hacking Health, nato in Canada, è arrivat
L'obiettivo è usare una serie di *camp* Hacking Health p
Hackers & Makers (progettisti, sviluppatori, ricercatori
dell'interfaccia utente), professionisti healthcare (medi
ospedaliera) e altri soggetti interessati come pazienti,
investitori per fare nascere *soluzioni realistiche e uma*
primari, come recita il sito. Dopo Montreal, Città del C
continua il proprio tour mondiale.

hacker.
ell'account Google attraverso una scorretta implementazione di SSL da Samsu

so che
ca Hos
hack
o ren
Ava
sun comm
ù lunga, d
avete capit
egolare il b
tatile. Allo s
portando u
omessi da

attacchi oggi

Ricognizione esterna

Compromissione iniziale

Consolidamento della posizione

Movimenti laterali

Estrazione dei dati

Attacchi sempre più sofisticati

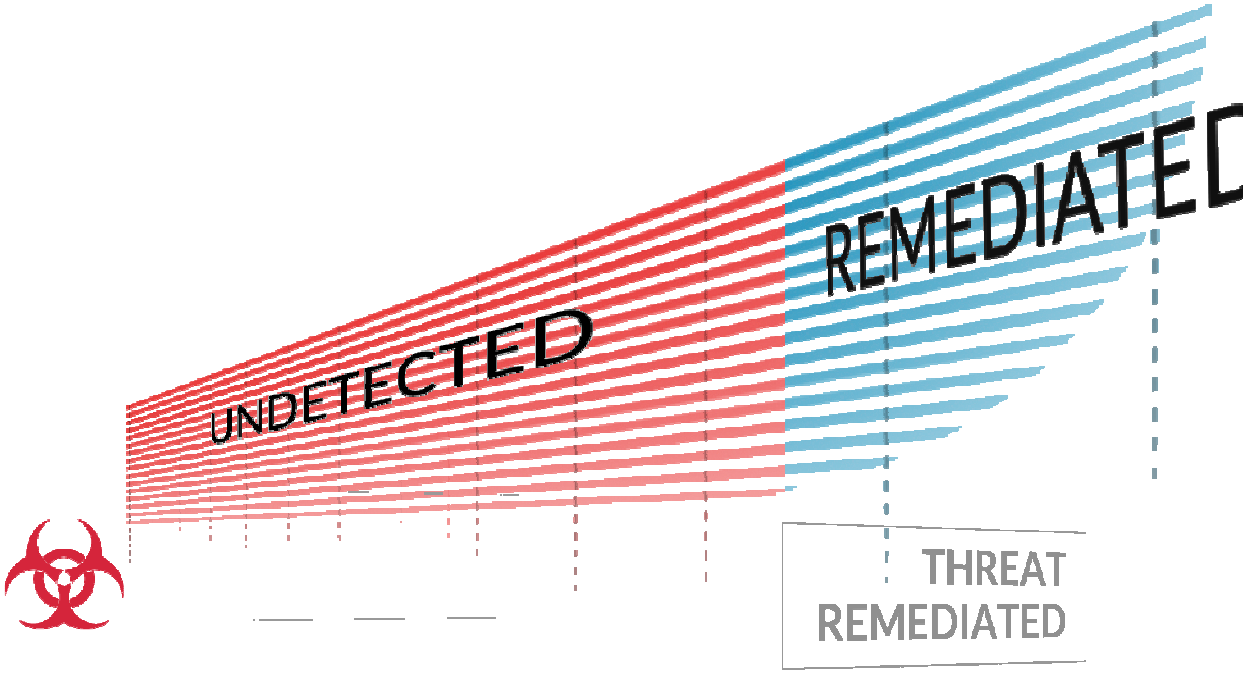
- Non si concludono mai all'interno di una sola sessio TCP (multi-flow)
- Non vengono mai veicolati attraverso un solo canal (multi-vector)
- Generano evidenze estremamente basse e si confo con il «rumore di fondo» (low&slow)
- Sfruttano tecniche di offuscamento, per nasconder loro vera natura
- Sono in grado di cifrare / decifrare al volo parti di c per ingannare i sistemi di difesa
- Sono consapevoli del contesto in cui operano, cono il sistema su cui si installano e possono adattarsi all molteplici condizioni (polimorfismo)

vogliono in media 205 giorni per scoprire che è
nuta una compromissione

si mette 32 giorni per rispondere ad una
promissione

lo nel 33% dei casi sono le vittime ad accorgersi di
nto avvenuto

na compromissione ha un costo medio di $3,5M



o questo, nonostante il 100% delle aziende
promesse avesse **tutti** i sistemi di difesa correttamente
ornati e configurati

Dati tratti da un'analisi Ponemon Institute che ha analizzato tutti gli incid
di sicurezza che nel 2014 hanno interessato 350 aziende in 11 paesi

servizi / interruzione delle attività

ni alle infrastrutture non-IT
pianti, sistemi elettromedicali…)

ni alle infrastrutture IT (server,
nt…)

razione / estorsione di denaro

Rischi operativi

Rischi reputazionali

Furto di brevetti e proprietà intellettu

Furto di informazioni finanziarie e pian
strategici

Furto di dati personali e dati sensibili
(dati dei pazienti, cartelle cliniche…)

Danni all'immagine aziendale

li aree di intervento?

PUNTO
SECURITY & INNOVA

- Verifiche di conformità
- Policy e procedure
- Privacy e protezione dati personali
- Proprietà intellettuale

- Infrastruttura
- Endpoint
- Dati
- Mobile

- Disaster Recovery
- Business Continuity

- Procedure operative
- Piani di BCDR
  Procedure di backup e recovery

- Architetture di sicurezza
- Segmentazione e segregazione carrier

Protezione

- NGFW / UTM / IPS
- Web Security
- NAC
- Sicurezza Wi-Fi

Prevenzione

- Soluzioni di prevenzione Advanced Persistent Threat

Governance

- Monitoraggio rete
- SIEM
- Verifiche di sicurezza (VA/PT)

Identità

- Identity Management / Governance
- Single Sign On

Protezione

- Protezione degli endpoint
- Protezione dei server
- Virtual patching
- Sicurezza ambienti virtuali

Governance

- Gestione asset
- Patch management
- Backup/Recovery

Identità

- Role-based Access Control
- Gestione utenze privilegiate

Protezione

- Data Loss Prevention
- Cifratura dei dati

Governance

- Classificazione dei da
- Information Management

- Gestione degli accessi da parte di utenti da terminali mobili

Protezione

- Accesso sicuro ai dati in mobilità
- Cifratura dei dati sui terminali mobili

Prevenzione

- Soluzioni di prevenzione APT dedicate alla piattaforma mobile

Governance

- Gestione del sicurezza di smatphone e tablet

security model» di Puntoit

PUNTO
SECURITY & INNOVA

Remediate

plicare le misure correttive

quisire la capacità di remediation

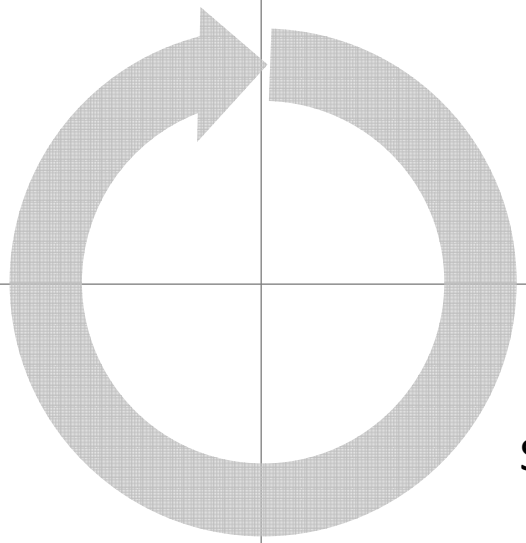
ntenere, migliorare, standardizzare

Assess

Analizzare la situazi

Scegliere interventi e prio

Pianificare gli interventi neces



nitorare, misurare e valutare

alizzare gli scostamenti

diare i risultati

Acquisire gli strumenti più adeg

Studiare, progettare e implementare le soluz

Verify

Secure

razie per l’attenzione

PUNTOIT
SECURITY & INNOVATION

Silvio FERRARI | Head of Sales Er

Puntoit Servizi Informati

Milano | Roma | tel. 02-2708.0780 | www.puntoitse