TÒRIA
SECURE SYSTEMS

Webinar: *La cybersecurity è superata?*

ISACA – Rome Chapter

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Obiettivi del Webinar

- Capire dove stiamo andando
- Comprendere le vulnerabilità del sistema in cui operano le nostre aziende
- Renderci conto che siamo in *guerra* e abbiamo un *nemico*
- Stabilire una strategia e un piano pratico di azione per difenderci

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

Agenda

1	Trent'anni di cybersecurity: siamo più al sicuro?
2	La cronaca recente: SolarWinds
3	L'infrastruttura tipica di cybersecurity di una media azienda
4	Non è più un problema: è una GUERRA
5	Gli obiettivi e le strategie del *nemico*
6	Le risorse del *nemico*
7	La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

1991 – Gli inizi

Virus e altri aggressori informatici: uno schema di prevenzione

di Stefano Toria (MC0170 su MC-Link)

Siamo arrivati a delineare, negli scorsi articoli, uno schema degli elementi costitutivi del rischio-virus. Naturalmente ogni esposizione di un rischio presuppone la proposta di un metodo di protezione dal rischio, o quantomeno di valutazione dell'entità del rischio stesso. Come si vedrà, non è possibile dare un valore attendibile alla probabilità di essere «infettati»; per contro, è

Virus informatici e comportamenti a rischio

Si è detto negli scorsi articoli che molta parte della fortuna dell'argomento «virus» nella stampa di informazione trae origine dall'associazione, del tutto errata ma di forte impatto psicologico, tra i programmi virus e l'agente causale dell'AIDS. Capita nuovamente l'occasione di ripetere che i due fatti non hanno nulla in comune tra di loro se non il modo di trattarne, e proprio perché l'argomento di questo capitolo è il comportamento a rischio in relazione alla diffusione dei virus informatici.

La stampa, la televisione e le affissio-

Si delineerà infine uno schema di protezione, con le misure fondamentali da prendere per garantirsi una tutela ottimale contro il rischio dei virus.

Il virus, si è detto, è un programma. In quanto tale, si avvale degli stessi supporti utilizzati dagli altri programmi, cioè principalmente dei dischi. Ma un virus non può svilupparsi di propria iniziativa dal nulla, come taluni filosofi e scienziati dell'antichità ipotizzavano riguardo a particolari forme di vita. Un programma virus deve necessariamente avere un creatore, che scrive le specifiche di comportamento del virus, lo realizza materialmente a mezzo di un compilatore o assemblatore, lo utilizza

TÒRIA
SECURE SYSTEMS

1992 – Il *nemico* si attrezza

Il «Mutation Engine»

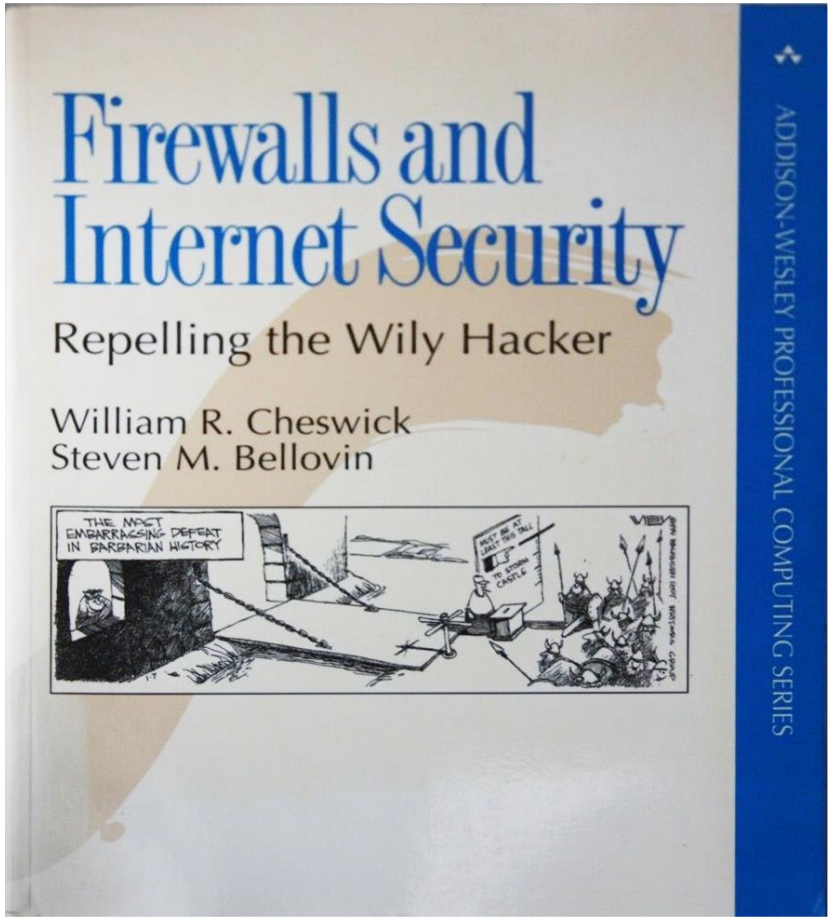
Le prime notizie su questo nuovo prodotto giungono personalmente da John McAfee. Con un messaggio spedito il 12 marzo in una conferenza elettronica sui virus, l'esperto californiano segnala la presenza di tre nuovi virus generati servendosi di un «Dark Avenger Mutation Engine».

Si tratta di un notevole passo avanti nella tecnologia dei virus, che dà motivo di temere che si stia aprendo un nuovo capitolo in questa fastidiosa storia. È il primo esempio di applicazione di tecniche avanzate di programmazione allo sviluppo dei virus.

- Tu crei il virus? E io ti metto l'antivirus per scoprirti e bloccarti
- *Tu metti l'antivirus per scoprirmi e bloccarmi? E io creo il virus che cambia ogni volta, così non mi scopri*
- Tu crei il virus che cambia ogni volta? E io etc. etc…

TÒRIA
SECURE SYSTEMS

1994 – Ci attrezziamo anche noi



- Adesso c'è Internet
- Il *nemico* entra più facilmente
- Bisogna tenerlo fuori

TÒRIA
SECURE SYSTEMS

1998 – A caccia di intrusi

- Acquisito il concetto di «intruso»
- Non basta un firewall per tenere il *nemico* alla larga
- Aggiunto uno strumento all'armamentario della sicurezza

2021 – Siamo più al sicuro?
Gli investimenti salgono a livelli stellari

- Cloud security tools
  - 2018: $5.6B
  - 2020: $12.6B
- Infrastructure protection
  - 2020: $18.3B
  - 2023 pred.: $24.6B
- Endpoint security
  - 24% IT spending
  - 2020: $128B
- Zero Trust …

(Forbes)

2021 – Siamo più al sicuro?
Gli attacchi salgono a livelli stellari

- Solo nel 2020:
  - SolarWinds *(ne parliamo tra poco)*
  - Twitter
  - Marriott
  - MGM Resorts
  - Zoom
  - Magellan Health
  - Greek Banking System

- Nel 2021 si prevedono danni per $6tn *(Cybersecurity Ventures)*
- Se fosse un PIL, sarebbe il *terzo del mondo* (dopo USA e Cina)

TÒRIA
SECURE SYSTEMS

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

I fatti

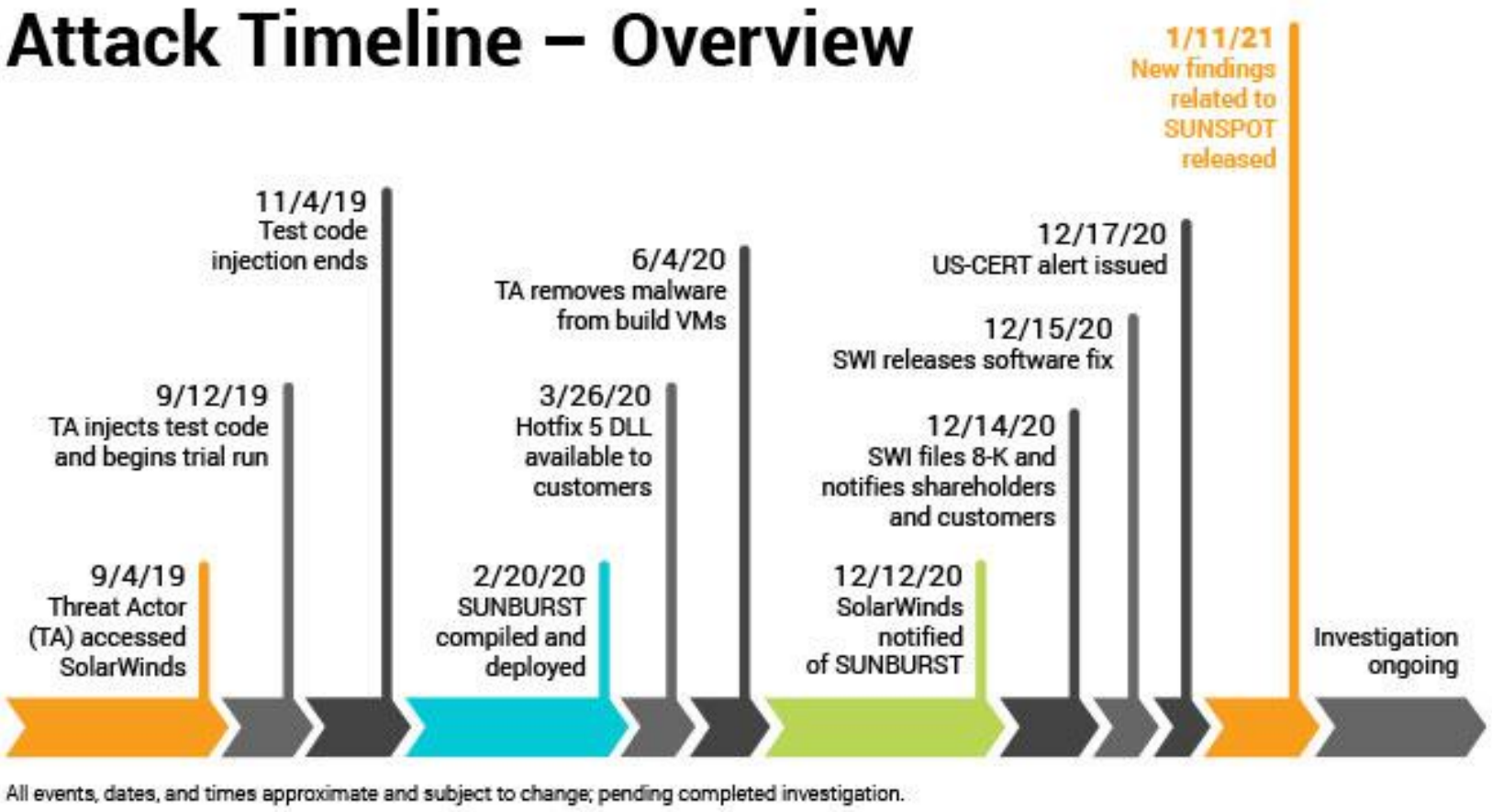
- Scoperto nel dicembre 2020 un attacco di dimensioni rilevanti
  - Circa 18'000 enti e aziende vittime dell'attacco
- Alla base dell'attacco un prodotto software di larga diffusione
  - Utilizzato da decine di migliaia di aziende per operazioni di *back-office*
- L'attacco si svolge in occasione della diffusione di un aggiornamento
  - Tramite il sistema di *live update* del prodotto
- Classico caso di *supply chain attack*
  - Molti punti importanti da considerare

Il prodotto

- SolarWinds distribuisce «Orion»
  - Monitoraggio di reti e database
  - Sistema molto diffuso
  - «Gestiamo le reti di tutti»

- È installato in un grandissimo numero di grandi aziende e gli enti pubblici

L’attacco



(blog SolarWinds)

TÒRIA
SECURE SYSTEMS

L’attacco

- Quando viene scoperto andava avanti da mesi
  - Per caso da un’azienda di cybersecurity
  - Colpita anch’essa dall’attacco

Le vittime – Pubblica Amministrazione USA

- Dipartimento dell'Agricoltura
- Dipartimento del Commercio
- Dipartimento della Difesa
- Dipartimento dell'Energia
- Dipartimento della Salute
- Dipartimento della Sicurezza Interna
- Dipartimento di Giustizia
- Dipartimento del Lavoro
- Dipartimento di Stato
- Dipartimento del Tesoro
- …più vari enti statali e locali

TÒRIA
SECURE SYSTEMS

Le vittime – settore privato

- Belkin
- Cisco Systems
- Cox Communications
- Equifax
- FireEye
- Malwarebytes
- Microsoft
- Mimecast
- Nvidia
- Palo Alto Networks
- Vmware
- ...e altri

Le vittime – settore privato

- Nelle settimane fra la scoperta dell'attacco e le feste natalizie, gravi preoccupazioni per il settore dell'energia elettrica

- L'attacco rischia di compromettere il *grid*?

- NERC chiede alle utility di indicare il proprio grado di esposizione al software SolarWinds

I danni

- Difficile, forse impossibile stimare il danno complessivo
- Il danno maggiore risulta dal «movimento collaterale»
  - Gli attaccanti penetrano in una rete e poi si spostano alla ricerca di obiettivi
  - Dati possono essere rubati, alterati o distrutti
  - Le configurazioni dei sistemi incontrati possono essere alterate
- Per scoprire tutto ciò che è successo potrebbero servire anni
  - Sistemi in continua evoluzione
  - Non sempre sono disponibili log e audit trail
- Alcuni arrivano a dire che le reti colpite vanno rimpiazzate del tutto

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

Il sistema di cyber security in azienda

- Sicurezza dei sistemi d’impresa
- Sicurezza perimetrale
- Rilevamento di incidenti ed eventi; reazione e ripristino
- Gestione delle identità e degli accessi
- Protezione degli utenti finali

TÒRIA
SECURE SYSTEMS

Enterprise

- Firewall
- Network Access Control (NAC)
- DNSsec
- IT Service Monitoring
- Vulnerability Management

Perimetro

- Firewall
- IDS-IPS
- Cloud Access Security Broker (CASB)
- Web Application Firewall (WAF)
- Reverse Proxy
- Web & E-mail security
- Load Balancing
- DDoS protection

Rilevamento e reazione

- Endpoint Detection & Response (EDR)
- Network Detection & Response (NDR)
- Security Incident & Event Management (SIEM)
- User & Entity Behaviour Analytics (UEBA)
- Threat Intelligence

Identity & Access Management (IAM)

- Multi-Factor Authentication (MFA)
- Permission Governance
- Single Sign-on (SSO)
- Privileged Access Management (PAM)

Endpoint

- EDR
- Endpoint Protection Platform (EPP)
- Vulnerability Management
- Compliance Management
- Asset Management
- File Encryption
- Remote Access
- Mobile Device Management & Security

…è aumentata la sicurezza?

- Centinaia di miliardi di investimenti
- Migliaia di miliardi di danni
- Milioni di esperti e specialisti impiegati nella difesa

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

Cyberwar

TIME

Onward Cyber Soldiers

THE U.S. MAY SOON WAGE WAR BY MOUSE, KEYBOARD AND COMPUTER VIRUS. BUT IT IS VULNERABLE TO THE SAME ATTACKS

By Douglas Waller/Washington Monday, Aug. 21, 1995

Like 1 Tweet Share Read Later

Email Print Share Reprints Follow @TIME

In a secure vault in the U.S. Army's super-secret Intelligence and Security Command in northern Virginia, Colonel Mike Tanksley sketches the barest outlines of the new Armageddons. These are only "What ifs?" he insists, so there cannot really be details. Yet his war scenario resounds with almost biblical force. The next time a tyrant out of some modern Babylon (Baghdad, Tehran or Tripoli, for example) threatens an American ally (Riyadh, Cairo, Jerusalem) the U.S. doesn't immediately send legions of soldiers or fleets of warships. Instead Washington visits upon the offending tyranny a series of thoroughly modern plagues, born of mice, video screens and keyboards.

First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. U.S. planes, specially outfitted for psychological operations, then jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his PC, he finds that the millions of dollars he has hoarded in his Swiss bank account have been zeroed out. Zapped. All without firing a shot. A glow comes over Colonel Tanksley as he talks

- Il concetto è vecchio (metà anni '90)
- Gli effetti sono attualissimi
- Si svolge diversamente da come molti pensavano

TÒRIA SECURE SYSTEMS

Guerra informatica: teoria vs. realtà

Nella teoria:

- Battaglioni di soldati specializzati
- Infrastrutture tecniche che si «combattono»
- Danni collaterali ridotti al minimo

Nella realtà:

- Nessuno scontro di eserciti
- Gruppi di specialisti aggrediscono i civili (aziende e privati)
- Enormi danni collaterali

TÒRIA
SECURE SYSTEMS

I danni

- Stima per il 2017: $1.5tn
  Il PIL della Russia

- Stima per il 2021: $6tn
  Il terzo PIL al mondo, dopo USA e Cina

Il *nemico*

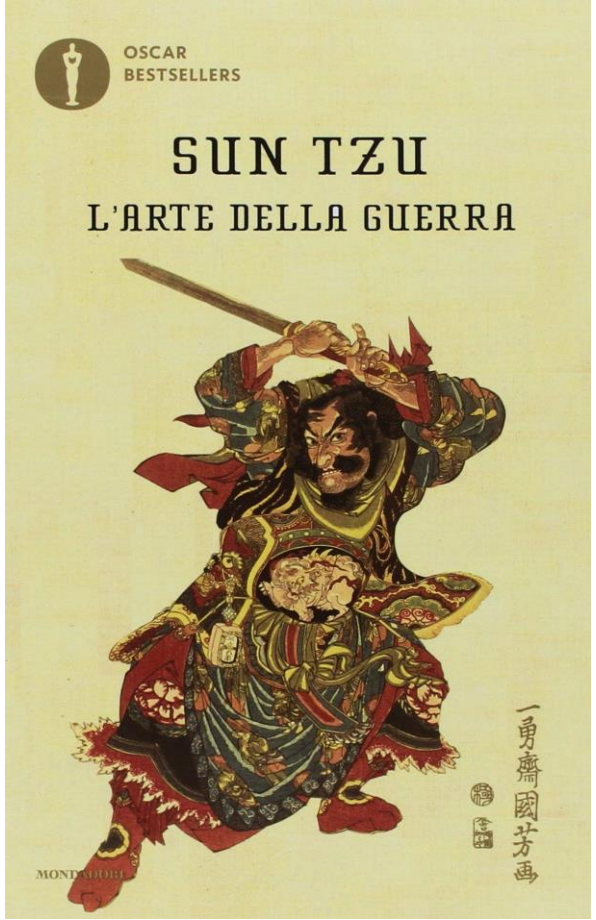
- Attori «non statuali»
- Gruppi di attivisti
- Criminalità comune organizzata
- Attori statuali

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

Conoscere il *nemico*



Conoscendo gli altri e conoscendo sé stessi,
in cento battaglie non si correranno rischi;
non conoscendo gli altri, ma conoscendo sé stessi,
una volta si vincerà e una volta si perderà;
non conoscendo né gli altri né sé stessi,
si sarà inevitabilmente in pericolo ad ogni scontro.

TÒRIA
SECURE SYSTEMS

Obiettivi del *nemico*

- Motivazione dell’attacco
- Difficoltà dell’attacco
- Remunerazione dall’attacco

Evoluzione nel tempo

- Anni '90: *geek* e ragazzini
  - Motivazione: voglio far vedere quanto sono bravo
  - Difficoltà: molto bassa
  - Remunerazione: psicologica

- Anni 2000: giovani professionisti ed attivisti
  - Motivazione: guadagno ma anche politica
  - Difficoltà: medio-bassa
  - Remunerazione: psicologica ed economica / politica

Evoluzione nel tempo

- Anni ‘10: crimine organizzato
  - Motivazione: attacco al «petrolio del 21° secolo»
  - Difficoltà: da medio-alta ad altissima
  - Remunerazione: principalmente economica

Cosa vuole ottenere il *nemico*

1. Entrare
2. Cercare
3. Procurarsi
4. Tornare

Entrare

- Sfruttare tutte le possibili vulnerabilità

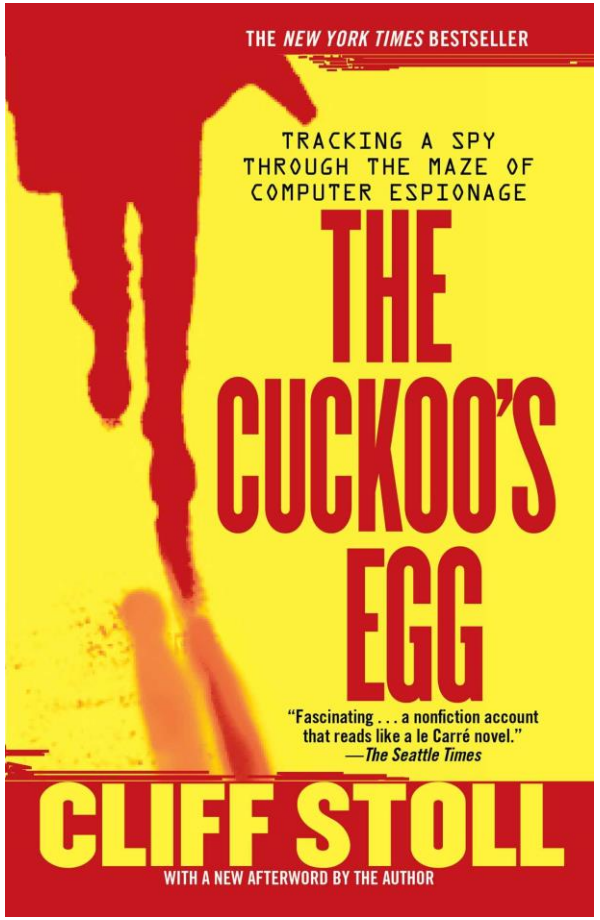
- Tecniche: sistemi perimetrali, infrastrutture, endpoint
  - 70% degli attacchi riusciti passano per un endpoint
  - Eppure spendiamo il 24% della spesa IT, $128B

- Umane
  - 98% degli attacchi riusciti sfrutta un errore umano

Entrare

- Conoscenza approfondita delle infrastrutture
- Conoscenza approfondita degli strumenti di cybersecurity

Cercare



- Movimento collaterale
- Non è una novità
- Consiste nell'esplorare la rete e le infrastrutture della vittima
  - in cerca di obiettivi

Procurarsi

- Materiali da sottrarre (copiare) per rivendere
  - Possibilmente nel *Dark Web*
- Materiali da sottrarre per utilizzare direttamente
  - Informazioni riservate di valore
  - Informazioni su ulteriori obiettivi di attacchi (Stoll)
- Materiali da alterare o distruggere
  - Per sabotaggio o richiesta di riscatto (ransomware)

Tornare

- Il *nemico* si riserva sempre la possibilità di rientrare
- Installazione di *backdoor* o simili
- Cancellazione delle tracce da log e audit trail

Strategia del *nemico*

- Obiettivi generalizzati
  - Es. phishing
- Obiettivi mirati
  - Settore, industria, categoria o territorio
- Obiettivi super-mirati
  - Spear-phishing, CEO fraud

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

Quali risorse servono al *nemico*

- Difficoltà degli attacchi: da medio-alta ad altissima
  - 2010: *Stuxnet*
  - 2020: *SolarWinds*
- Conoscenze tecniche
- Mezzi finanziari
- Tempo e persone
- Strumenti tecnici, in particolare quelli in possesso delle vittime.

Conoscenze tecniche

- Non sono mai state un problema
- Gli hacker nascono in ambiente informatico
- Socializzazione e associativismo
  - Chaos Computer Club
  - Associazioni spontanee
  - L'underground del *Dark Web*

Mezzi finanziari

- Stima del «fatturato» complessivo del cyber crime
  - 2017: $1.5tn – il PIL della Russia
  - 2021: $6tn – il terzo PIL del mondo

- Non è un singolo gruppo, è una miriade di costellazioni

- Le risorse non mancano per:
  - Formazione
  - Acquisizione sistemi da studiare e neutralizzare
  - Ulteriori sviluppi

Tempo e persone

- Ampia disponibilità di personale, sia full- che part-time

- Skill largamente diffusi
  - Conoscenza informatica di base e tecniche di rete
  - Sviluppo software in diversi linguaggi
  - Sistemi operativi più diffusi: Windows, Linux, ESX etc.

- Formazione su nuovi metodi e tecniche

Strumenti tecnici

- Kit di attacco
- Sistemi di comando e controllo
- Gli strumenti di difesa delle vittime
  - Per imparare come funzionano, e neutralizzarli

Il *nemico* ha più risorse di noi

- E le sa sfruttare molto bene
- Non abbiamo speranza di batterlo sul suo terreno
- …Ci dobbiamo arrendere?

Agenda

1. Trent'anni di cybersecurity: siamo più al sicuro?
2. La cronaca recente: SolarWinds
3. L'infrastruttura tipica di cybersecurity di una media azienda
4. Non è più un problema: è una GUERRA
5. Gli obiettivi e le strategie del *nemico*
6. Le risorse del *nemico*
7. La cybersecurity non basta più. Strategie e piano di azione

TÒRIA
SECURE SYSTEMS

A che punto è la guerra?

- Pochi credono davvero che siamo in guerra
  - Continuano ad affrontare la situazione come un problema tecnico
  - E come se gli aggressori di oggi fossero ancora i ragazzini di ieri
- Non esiste una soluzione tecnica quando il problema non è tecnico
- La «corsa agli armamenti» della cybersecurity ne è la prova

La situazione delle singole aziende

Viel gelernt

Von den Kunden habe Offix in der schwierigen Zeit eine enorme Solidarität erfahren, sagt Geschäftsleitungsmitglied Sandra Hurter. Anstatt abzuspringen, hätten sie weiterhin bestellt und damit das Unternehmen am Leben gehalten. Der Zusammenhalt der Mitarbeitenden gegen den äusseren Feind sei beeindruckend gewesen. Offix hat nach eigener Einschätzung viel aus dem Cyber-Angriff gelernt. «Wir dachten, unsere IT-Sicherheit sei in einem Topzustand», kommentiert Kelterborn. Diese Einschätzung sei falsch gewesen. Inzwischen plant das Unternehmen, sich selber anzugreifen, um Schwachstellen zu erkennen.

«Pensavamo che la nostra sicurezza IT fosse in perfette condizioni»

(NZZ, luglio 2019)

TÒRIA
SECURE SYSTEMS

La situazione delle singole aziende

- «Noi abbiamo la super-protezione»
- «Abbiamo fatto investimenti importanti, la nostra cybersecurity è allo stato dell'arte»
- «A noi non può succedere nulla»

Una mentalità inadeguata

- Affrontare il cybercrime come un qualsiasi altro problema tecnico
- Pensare di poter risolvere aumentando gli investimenti
  - O perfezionando gli strumenti
- L'inganno della «security awareness»

Un qualsiasi problema tecnico

- Nei primi anni '90 c'erano i virus
  - Erano i virus il problema? NO! erano *gli autori* dei virus
- All'inizio del nuovo secolo ci siamo accorti degli hacker che «entravano nelle reti»
  - Erano le reti il problema? NO! erano *gli hacker*
- Nell'ultimo decennio siamo stati invasi dai ransomware
  - Il problema sono i ransomware? NO! sono *gli autori* che incassano il riscatto

Investimenti e strumenti

- L’esperienza di 30 anni
  - Investimenti in crescita esponenziale
  - Attacchi in crescita esponenziale

- Strumenti tecnici contro la creatività umana
  - Era chiaro già trent’anni fa

La «Security Awareness»

- Cyber-attacchi causati da errore umano: 98%
- Problema umano, soluzione umana: formare le persone
- Idea giusta ma applicazione sbagliata
- Quello che i fornitori di awareness non dicono

TÒRIA
SECURE SYSTEMS

Oltre la «Security Awareness»

- Dalla teoria alla pratica: *cambiare i comportamenti*
- Il *nemico* fa affidamento sui comportamenti sbagliati delle sue vittime
- La sola *consapevolezza* non garantisce che al momento del pericolo le persone faranno le scelte giuste
- I comportamenti si cambiano solo con un addestramento progettato nei minimi dettagli

Cybersecurity e comportamenti

- La cybersecurity *non è* superata
- È superata l'idea che la cybersecurity *da sola* possa eliminare il problema
- Cybersecurity «giusta» + comportamenti «giusti» = STRATEGIA

La vera vulnerabilità del nemico

- Ricordiamo Sun Tzu: conoscere sé stessi e conoscere il nemico
- *«Il 98% degli attacchi riusciti sfrutta un errore umano»*
- Eliminare del tutto l'errore non è possibile
  - Si può ridurre con una strategia adeguata e con un radicale cambiamento nei comportamenti

Quattro fasi per la difesa dell'azienda

1. **Assessment**
   Un quadro chiaro della situazione: dove sono i pericoli

2. **Strategia**
   Stabilire obiettivi precisi, tempi e metriche

3. **Addestramento**
   Un programma dettagliato, finalizzato al cambiamento dei comportamenti

4. **Azione**
   Un piano di attività annuali, mensili, settimanali.
   Sotto la guida di un «generale» esperto

TÒRIA
SECURE SYSTEMS

Una strategia che funziona

1. Fondamenta solide
   Quali sono gli *asset* da proteggere

2. Conoscere rischi e minacce

3. Piano strategico
   Quadro, obiettivi, maturità attuale, timeline

4. Capacità di esecuzione del piano

TÒRIA
SECURE SYSTEMS

TÒRIA
SECURE SYSTEMS

Stefano Toria
CEO

stefano@toriasecuresystems.com
+41 79 308 83 12

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Grazie per l’attenzione