Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
STREAMING EDITION

ASTREA Advanced Security, Training Research, Events Agency

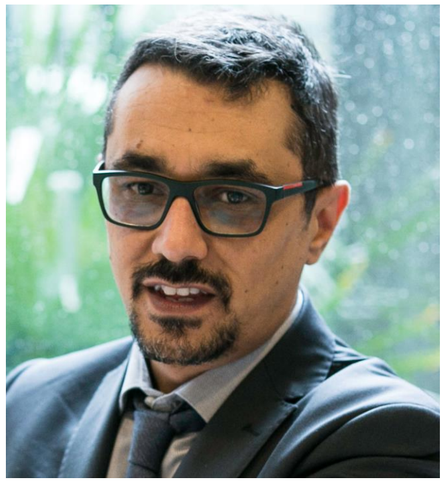
Sessione
Gli attacchi Phishing e Ransomware perdurano negli anni: cosa e' mancato per contrastarli?

Luca Bechelli, Comitato Scientifico, CLUSIT

Giampaolo Parravicini , Security Solutions Specialist, HP Italy

9 novembre 2022 orario 15.00-16.00

Luca Bechelli

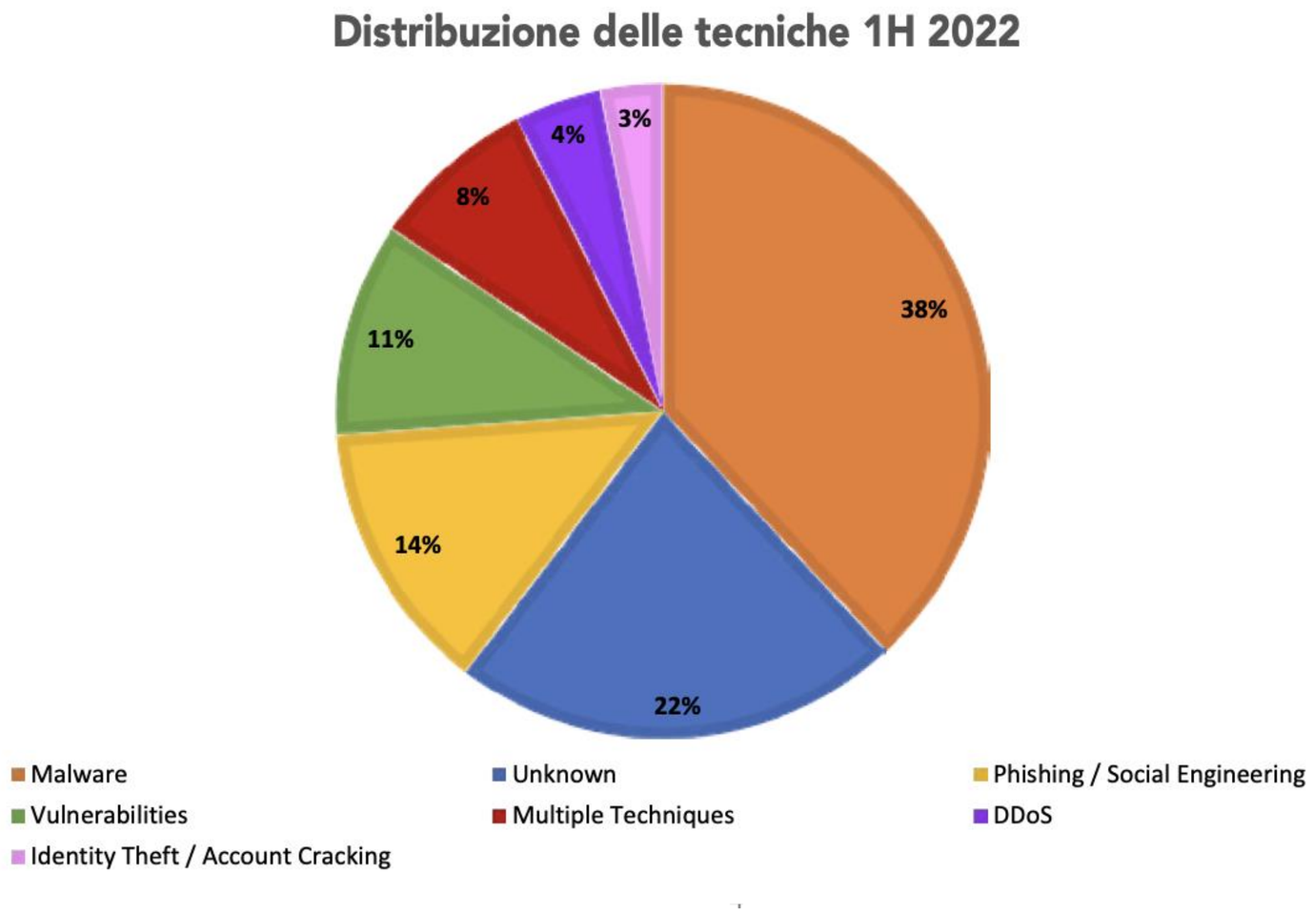


COMITATO SCIENTIFICO CLUSIT
PARTNER @P4I – GRUPPO DIGITAL360

Giampaolo Parravicini

SECURITY SOLUTIONS SPECIALIST
HP ITALY

Malware e Phishing al primo posto



Malware e Phishing al primo posto

Tecniche di attacco	2018	2019	2020	2021	1H 21	1H 22	2021 su 2020	TREND
Malware	601	737	775	850	454	433	-4.6%	↗
Unknown	429	309	372	433	230	253	10.0%	↗
Vulnerabilities	143	158	200	320	164	120	-26.8%	↓
Phishing / Social Engineering	170	291	299	203	94	154	63.8%	↑
Multiple Techniques	64	57	86	103	48	93	93.8%	↑
Identity Theft / Account Cracking	67	71	90	76	31	35	12.9%	↗
Web Attack	43	21	18	33	20	4	-80.0%	↓
DDoS	37	23	34	31	12	49	308.3%	↑
TOTAL	**1.554**	**1.667**	**1.874**	**2.049**	**1.053**	**1.141**		

La conferma sul territorio

Fonte: Sole24Ore

La conferma sul territorio

Truffe e frodi informatiche

Milano

POSIZIONE

7

DENUNCE/100.000 ABIT.

568,3

TOT. DENUNCE

18.641,0

Fonte: Sole24Ore

Uno sguardo agli ultimi anni

Anatomia di un attacco ransomware

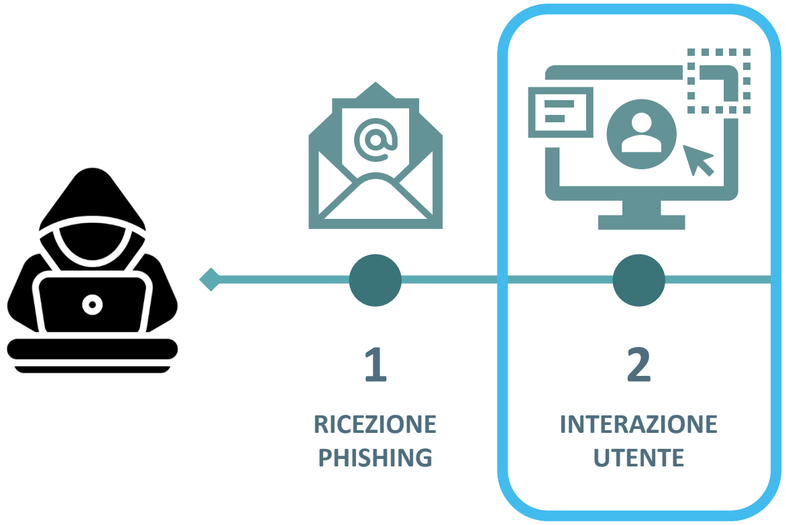
Flusso semplificato degli eventi (1 di 2)

APPROCCIO TRADIZIONALE

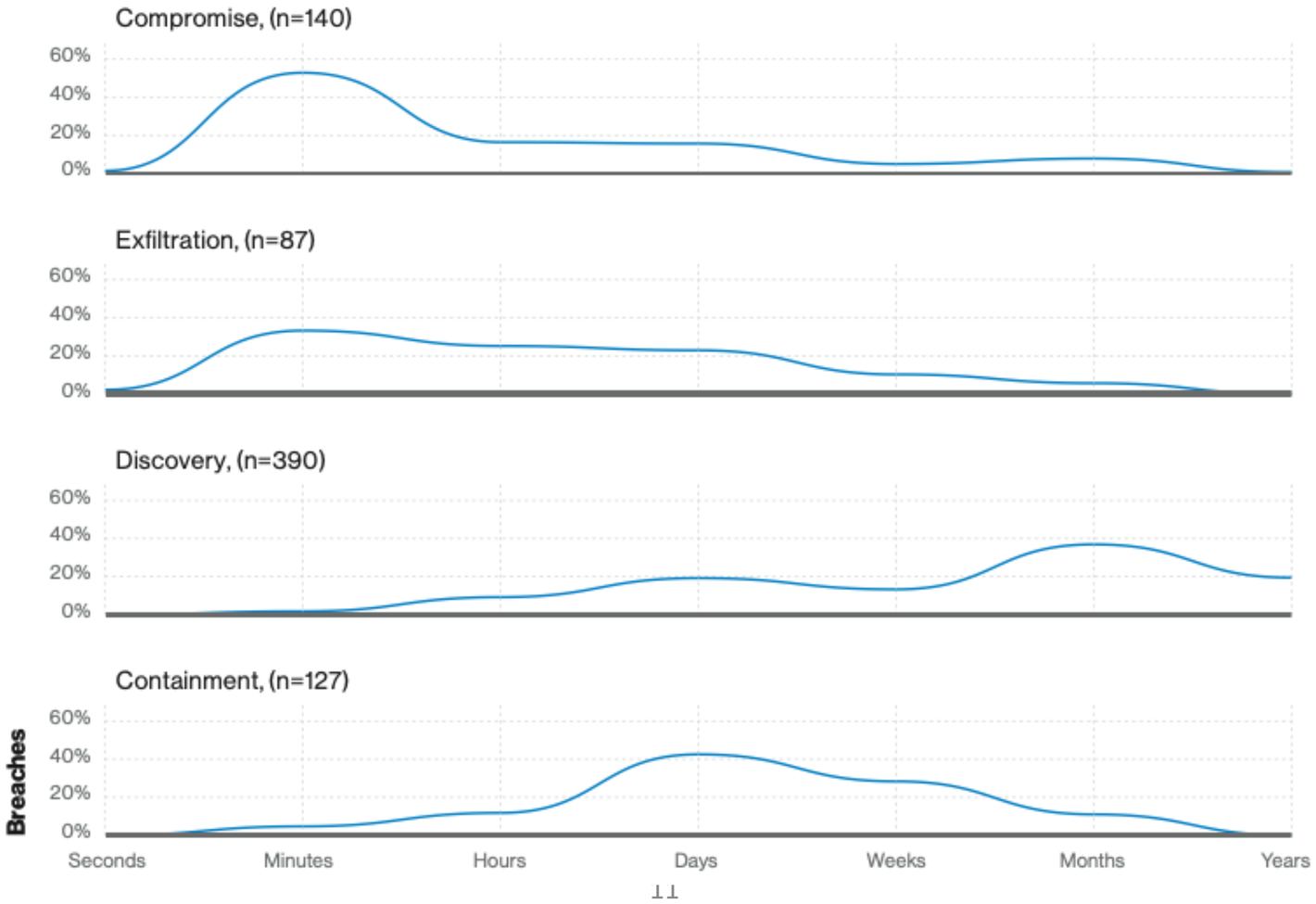
Anatomia di un attacco ransomware

Flusso semplificato degli eventi (2 di 2)

CON ISOLAMENTO DEI CONTENUTI



L’importanza della tecnologia



Nuovi tipi di malware

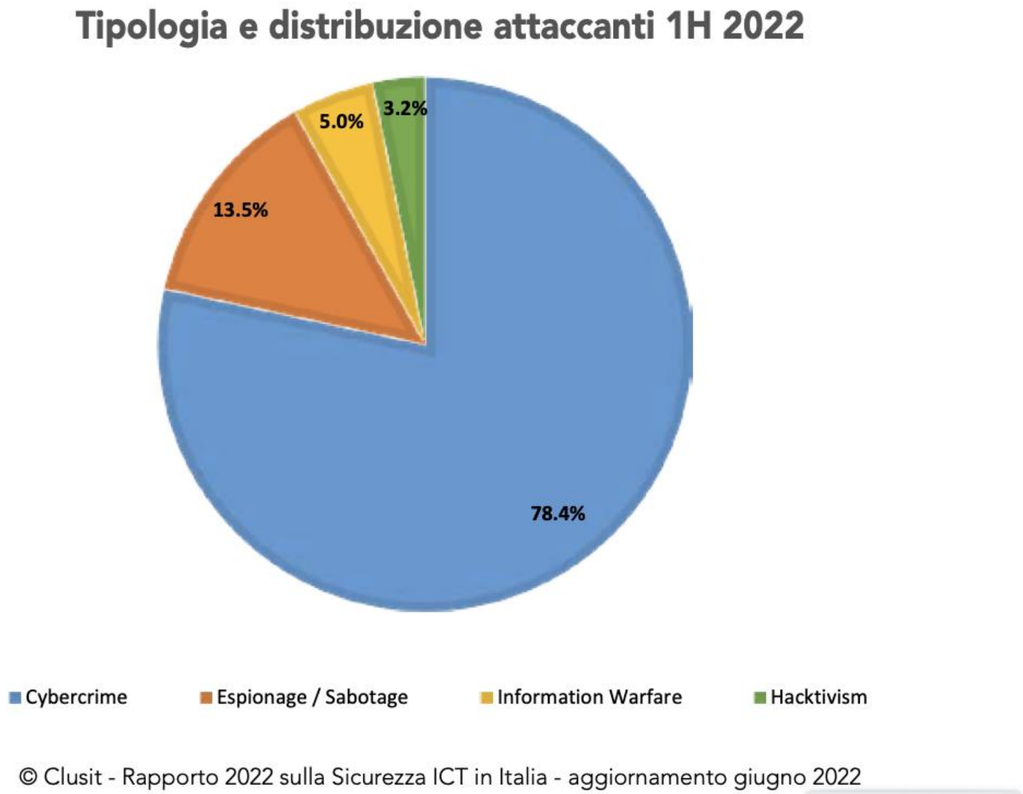
Per garantirsi di rimanere nel dispositivo della vittima il più a lungo possibile, gli attaccanti sfruttano ora nuovi tipi di agenti malevoli capaci di infettare il BIOS / UEFI dei PC.

LOJAX e **MOSAIC REGRESSOR** sono esempi concreti di come queste forme d'attacco siano estremamente efficaci.

SOFTWARE & HARDWARE PER INNALZARE LE DIFESE

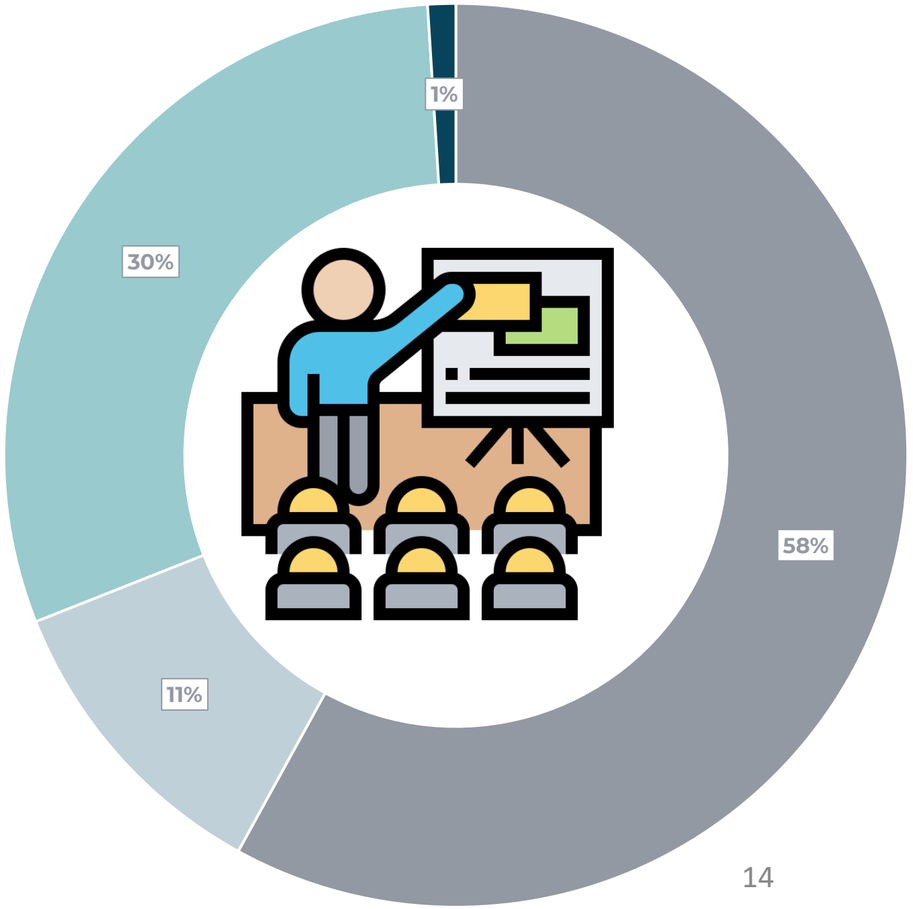
Quando l'attacco agisce a basso livello, hardware e software devono essere in grado di cooperare per scongiurare l'infezione

cyber-criminali sempre avanti: c’è qualcosa che possiamo fare per recuperare terreno?



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Lavorare sulle competenze



- Esiste un piano di formazione strutturato che coinvolge tutte le risorse aziendali
- Esiste un piano di formazione strutturato riservato al personale più a rischio
- Non esiste un piano di formazione strutturato, ma iniziative una tantum
- Non sono previste attività di formazione

Campione: 132 grandi organizzazioni

OSSERVATORI.NET digital innovation

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

L’importanza dei dati

Incrementare la visibilità di quanto succede durante l’attacco permette di non essere colti impreparati

---

Per aumentare le possibilità di successo, gli attaccanti non si limitano a sferrare un singolo attacco, ma adottano molteplici tecniche offensive perpetrate nel tempo.

Essere in grado di analizzare nel dettaglio quello che gli agenti malevoli adottati svolgono durante la loro azione, consente di mettere in atto in maniera preventiva le iniziative opportune per vanificare l’effetto degli attacchi successive.

Approccio Zero Trust

Un prezioso alleato nella protezione dei dati, se sfruttato appieno

User focused

L'applicazione o il repository di dati non dovrebbero fidarsi dell’utente o del suo dispositivo per impostazione predefinita.

- Chi è l’utente?
- Qual’è il suo ruolo?
- Dove si trova in questo momento?
- È autorizzato a interagire con quel contenuto?

Approccio Zero Trust

Un prezioso alleato nella protezione dei dati, se sfruttato appieno

User focused

L'applicazione o il repository di dati non dovrebbero fidarsi dell'utente o del suo dispositivo per impostazione predefinita.

- Chi è l'utente?
- Qual'è il suo ruolo?
- Dove si trova in questo momento?
- È autorizzato a interagire con quel contenuto?

Content focused

L'utente non dovrebbe fidarsi di un file, di un'applicazione o di un sito web per impostazione predefinita.

- Che tipo di contenuto è?
- Come mi aspetto che si comporti?
- Da dove proviene?
- Serve che acceda ai dati del mio dispositivo?

Q&A

HP ENDPOINT SECURITY CONTROLLER

UNIQUE HARDWARE ENABLES RESILIENT DEVICES

Protection starts at the lowest level of the PC

- Hardware-enforced technology only on HP PCs
- ESC always running, even when the system is powered off
- Hardware Root of Trust: protection, detection & recovery
- Physically isolated

Protection continues during runtime

- Ongoing monitoring for health of HP's security system
- HP Wolf Security cryptographic functions secured by hardware

Endpoint Isolation – Advanced Protection Technology

Endpoint software that virtualizes individual tasks

Each high-risk task is isolated inside a “micro-virtual machine”

- Email attachments
- Office documents
- Browsing
- USB drive files

Micro-virtual machine destroyed when task completes, eliminating any malware that may have been present

TI ASPETTIAMO AL NOSTRO VIRTUAL DESK!