CYBERSECURITY NELL'INDUSTRIA 4.0

Campobasso, 18 Luglio 2017

Claudio Telmon

Consulente

Membro del Comitato Tecnico Scientifico e del Comitato Direttivo di Clusit

ctelmon@clusit.it

SICURAMENTE
WWW.CLUSIT.IT

Associazione “no profit” con sede presso
l’Università degli Studi di Milano
Dipartimento di Informatica

2000-2017: 17 anni dedicati alla sicurezza

Malware-as-a-service

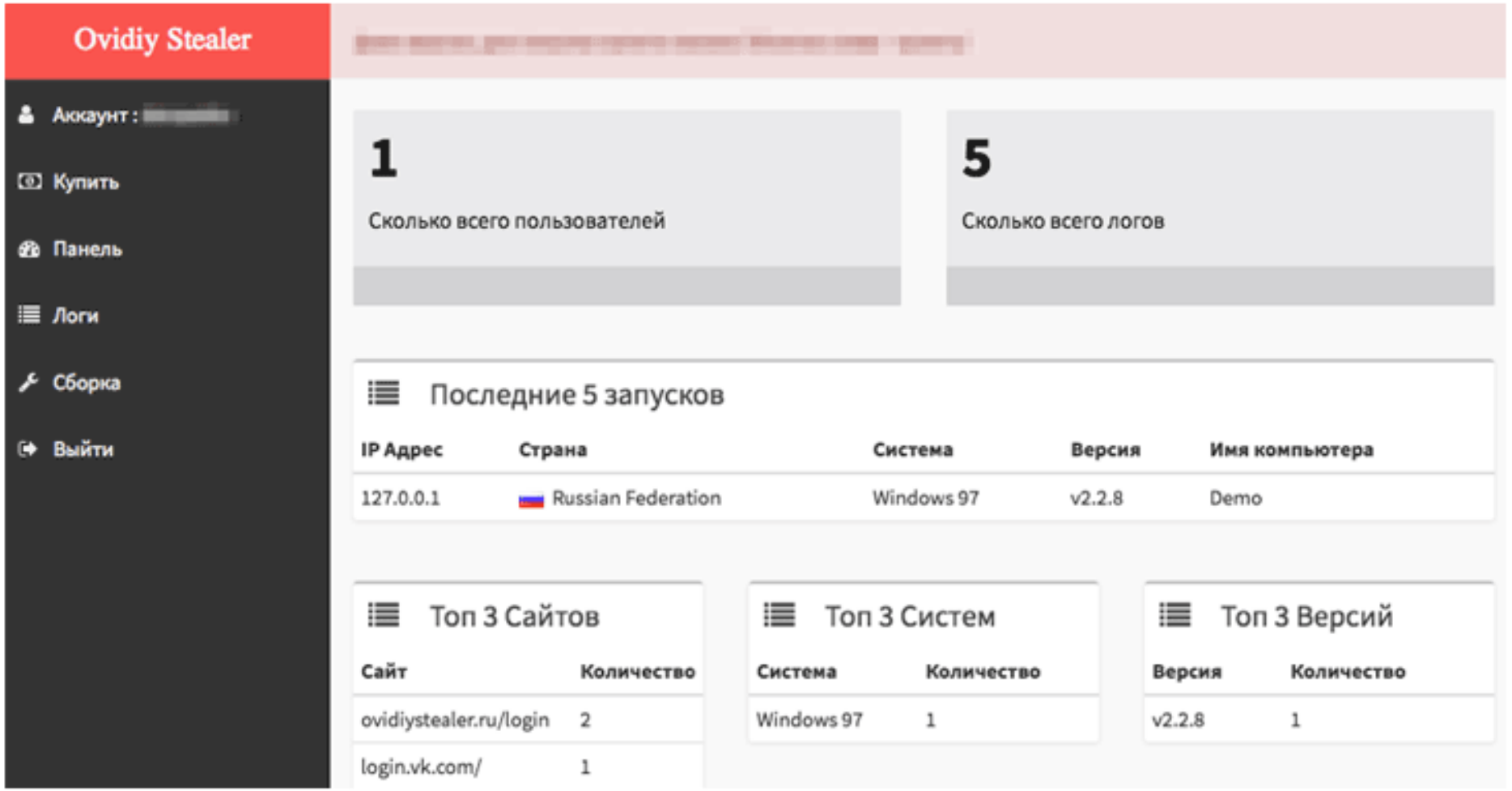
Two New Platforms Found Offering Cybercrime-as-a-Service to 'Wannabe Hackers'

Friday, July 14, 2017 Swati Khandelwal

Fonte: The Hacker News

Password-stealing maleware «di qualità» a buon prezzo

Ovidiy Stealer — $7 Password-Stealing Malware For Everyone

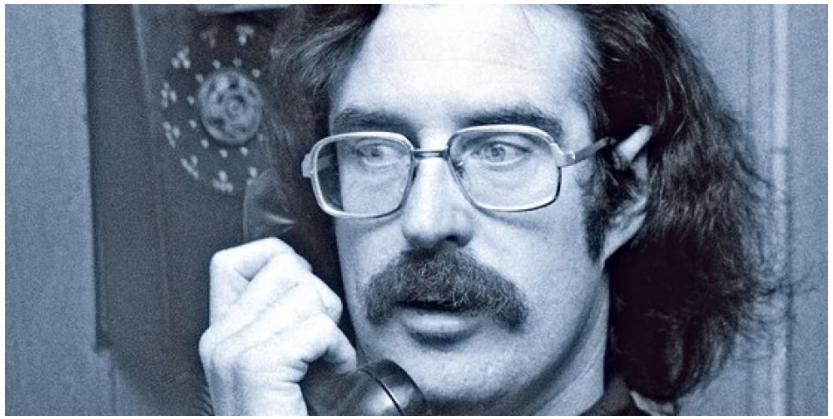


Personalizzato, efficace, cifrato per renderlo difficile da individuare dagli antivirus
La funzione principale è rubare password dai browser.
Ma è solo uno fra i tanti

Fonte: The Hacker News

Sono cambiati gli «hacker»?

John Thomas Draper, «Captain Crunch»
Costruttore della prima «blue box» negli anni '60



"I do it for one reason and one reason only.
I'm learning about a system.
The phone company is a System.
A computer is a System, do you understand?
If I do what I do, it is only to explore a system.

Computers, systems, that's my bag.
The phone company is nothing but a computer"

Attacker
CyberCrime
CyberCrime
CyberCrime
CyberCrime
CyberCrime
CyberCrime
CyberCrime

Gennady Kapkanov


Vi voglio spaventare?

Il rischio è il mio mestiere…

Il fatto che qualcuno possa rubare merci, mezzi e prodotti non è un buon motivo per non far uscire i camion…

La sicurezza è come i freni dell'auto: la loro funzione è rallentarti, ma il loro scopo è permetterti di andare veloce

Rischio di sicurezza delle informazioni: perimetro

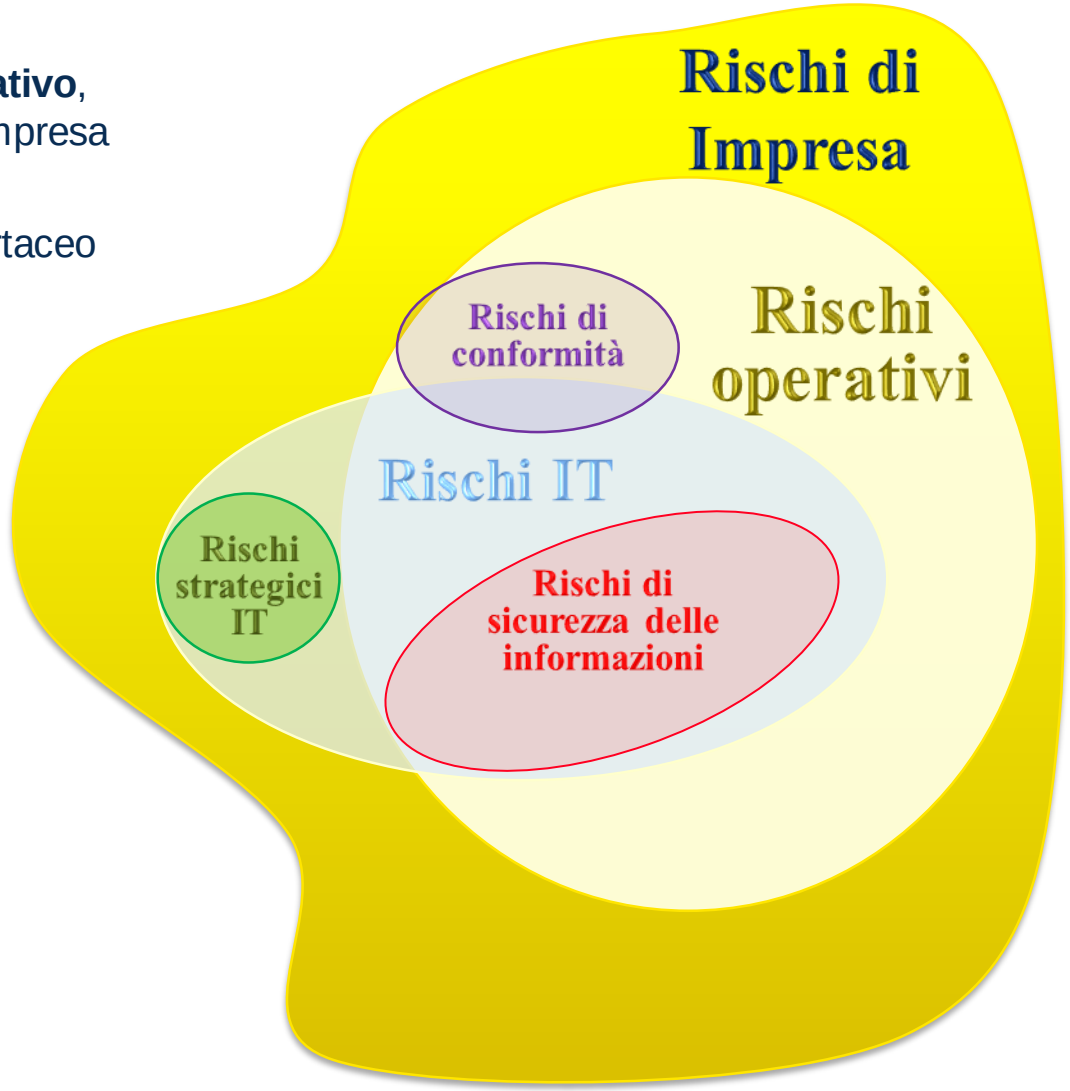
Il **rischio IT** è principalmente, ma non solo, un **rischio operativo**, quindi una componente del più ampio quadro dei Rischi di Impresa

Il **rischio di sicurezza delle informazioni** è un rischio IT e comprende i rischi legati ad es. le informazioni in formato cartaceo

Il rischio IT comprende alcuni **rischi strategici** (ad es. inefficacia del sistema informativo nel supportare l'evoluzione delle esigenze di business, obsolescenza dei sistemi…)

I rischi IT comprendono anche alcuni **rischi di (non) conformità** legati:

- a requisiti normativi sui sistemi IT e sulla loro gestione (es. normativa sul trattamento dei dati personali) che prevedono specifici adempimenti IT
- a inefficacia del sistema IT di supportare il sistema di controllo interno



Cos'è il rischio?

- "effetto dell'incertezza sugli obiettivi" (ISO 31000)
- Più semplicemente, funzione dell'**impatto** di un evento negative e della **probabilità** che l'evento si realizzi
- E il rischio di sicurezza IT?
  - L'impatto è **sui processi di business**, non sui sistemi informativi
  - La probabilità è quella che un incidente di sicurezza si verifichi…

Che domande deve porsi l'imprenditore?

- Quale sarebbe l'**impatto** se un certo processo (es. magazzino) si fermasse per uno o due giorni?
- Quale sarebbe l'**impatto** se certe informazioni (es. ricette) venissero diffuse o andassero a un concorrente?
- Quale sarebbe l'**impatto** se altre informazioni (es. storico degli ordini) andassero perdute?
- Qual è la **probabilità** che succeda per un incidente al sistema informativo?
  - E solo qui, si gira verso il responsabile del sistema informativo…

Wanna cry?

Cerca:

HARDWARE UPGRADE
il sito italiano sulla tecnologia

HOME | HARDWARE | MOBILE | VIDEOGIOCHI | FOTOGRAFIA | SOFTWARE | PRO | AUTO

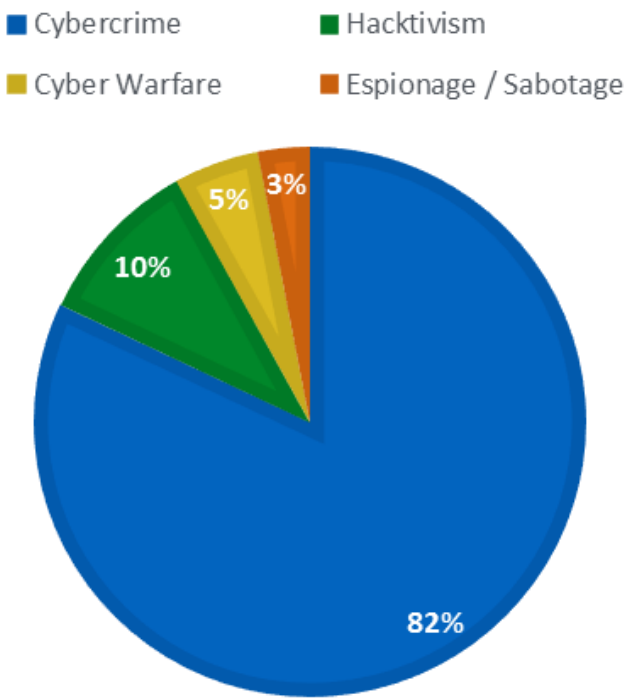
Microsoft rilascia un nuovo aggiornamento per Windows XP contro il ransomware WannaCry

L'azienda di Redmond continua ad aggiornare Windows XP dopo l'importante attacco hacker avvenuto a livello mondiale. Seppure il sistema operativo non fosse più supportato, Microsoft, sta lavorando per non mettere in pericolo gli utenti che ancora lo utilizzano.

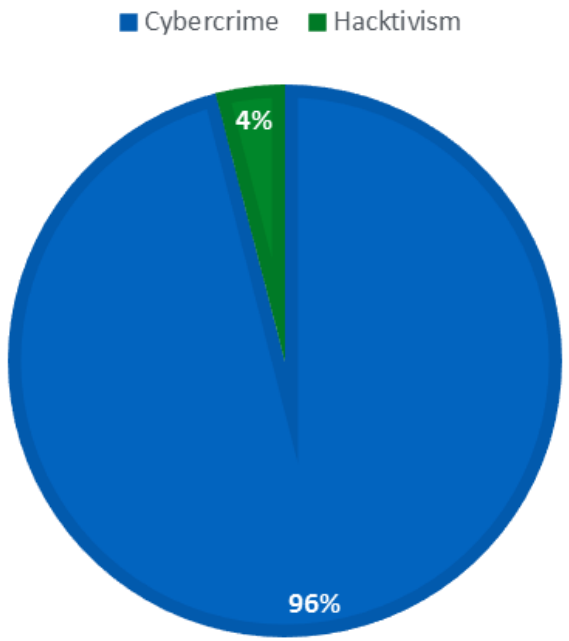
di Bruno Mucciarelli pubblicata il **23 Maggio 2017**, alle **14:31** nel canale SICUREZZA

Tipo e distribuzione degli attaccanti… ci interessa?

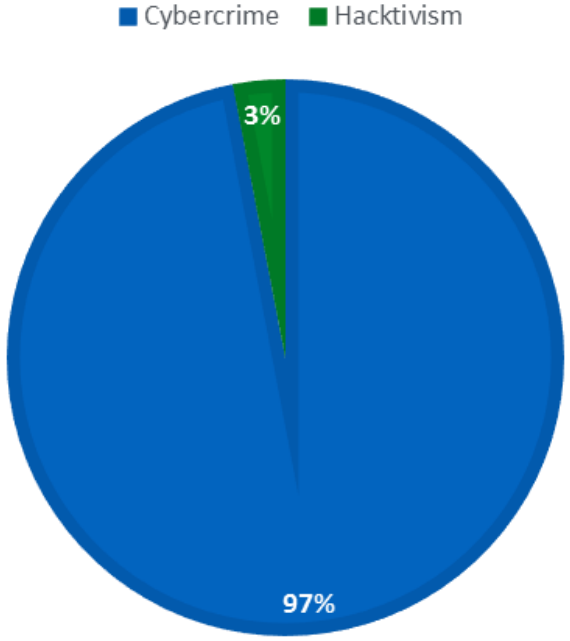
Banking



Healthcare



GDO

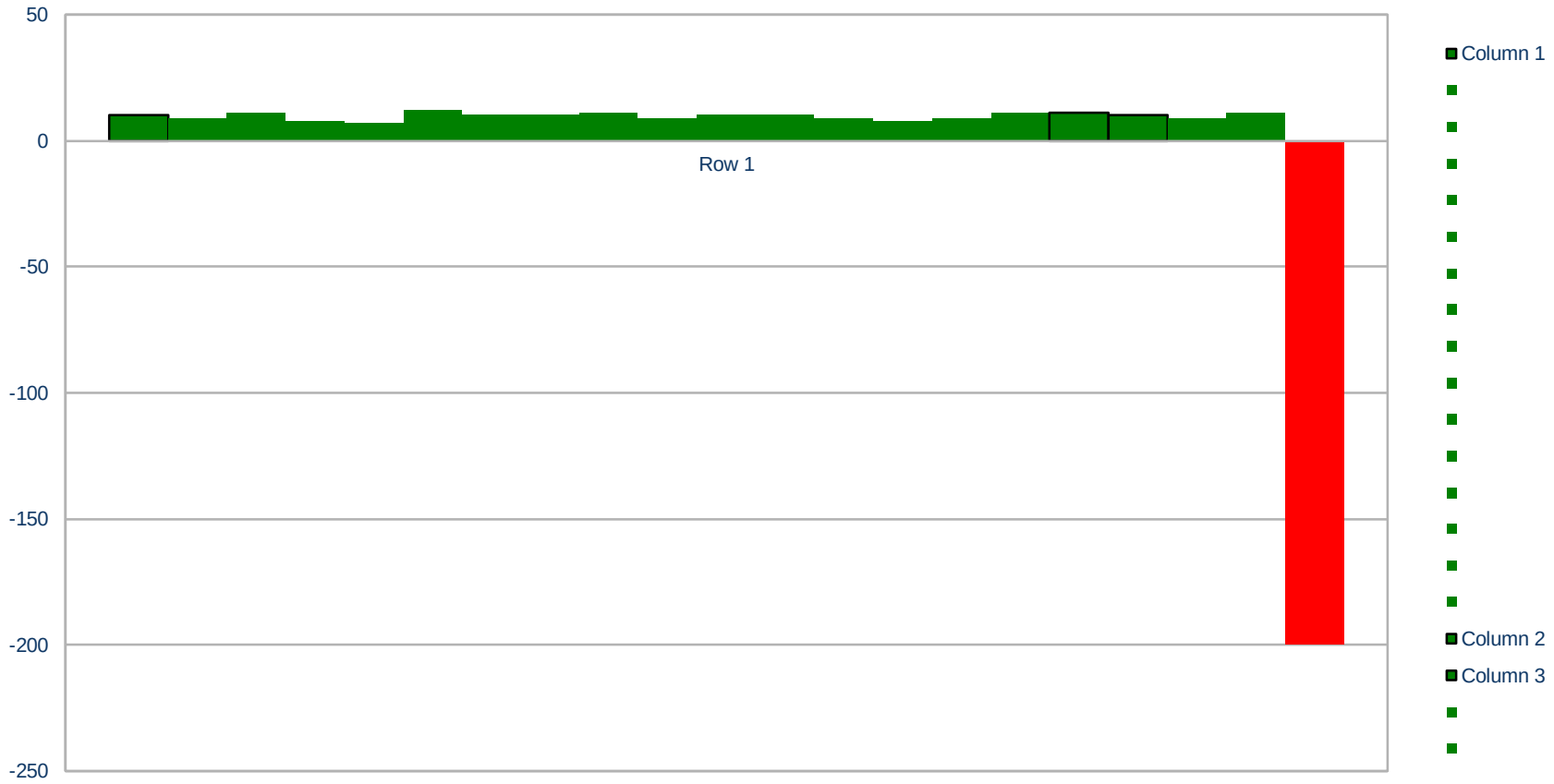


2016

Il paradosso del tacchino

- Per 1000 giorni, un tacchino viene accudito e ingrassato
- Può convincersi che continuerà così all'infinito, e costruire modelli matematici che lo “dimostrano”
- Al 1001-esimo giorno, avviene un unico evento che smentisce tutte le sue previsioni

Il paradosso del tacchino



Cosa ha sbagliato il tacchino?

- Lui non conosce (epistemologicamente) il fenomeno, osserva solo un campione
- Nel campione prevale una parte del fenomeno, e il tacchino ne deduce che sia tutto lì
- A posteriori (abbiamo più conoscenza non solo più informazioni) è facile giustificare quello che è successo
- È facile illudersi che l'approccio del tacchino fosse giusto e che mancasse solo qualche dato: ma l'errore è stata l'impostazione

Statistica e gestione del rischio

- Quanto ci aiutano gli eventi passati nel valutare i rischi futuri?
- Il modello non è nei dati, i dati vengono interpretati in base alla nostra conoscenza del fenomeno

- Le tecnologie dell'informazione evolvono troppo rapidamente per basarci sul passato

Dobbiamo guardarci intorno e cercare di capire cosa ci riserva il futuro

Sistemi aperti = sistemi più vulnerabili

- In una logica di gestione del rischio, è una conseguenza accettabile a fronte dei benefici attesi
  - L'obiettivo è gestire il rischio, non evitarlo
- Cosa possiamo fare per ridurlo?
- Quale rischio consideriamo tollerabile?

Beni strumentali il cui funzionamento è controllato da sistemi computerizzati

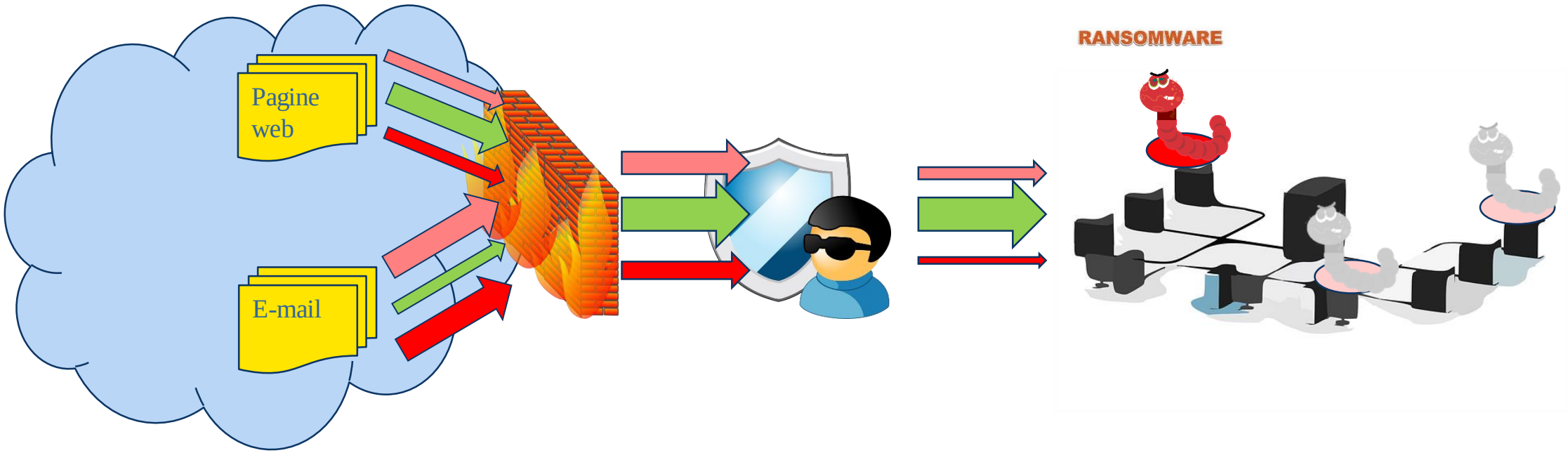
Tutte le macchine sopra citate devono essere dotate delle seguenti caratteristiche:

- ✓ controllo per mezzo di CNC (Computer Numerical Control) e/o PLC (Programmable Logic Controller);
- ✓ interconnessione ai sistemi informatici di fabbrica con caricamento da remoto di istruzioni e/o part program;
- ✓ integrazione automatizzata con il sistema logistico della fabbrica o con la rete di fornitura e/o con altre macchine del ciclo produttivo;
- ✓ interfaccia tra uomo e macchina semplici e intuitive;
- ✓ rispondenza ai più recenti parametri di sicurezza, salute e igiene del lavoro.

Inoltre tutte le macchine sopra citate devono essere dotate di almeno due tra le seguenti caratteristiche per renderle assimilabili o integrabili a sistemi cyberfisici:

- sistemi di telemanutenzione e/o telediagnosi e/o controllo in remoto;
- monitoraggio continuo delle condizioni di lavoro e dei parametri di processo mediante opportuni set di sensori e adattività alle derive di processo;

Solo ransomware?



Sicurezza dall'inizio

- La sicurezza deve essere parte di sistemi e processi fin dalle prime fasi di progettazione
  - Solo così può essere:

    Efficace

    Meno onerosa

    Di minore impatto sull'operatività

- Il monitoraggio degli eventi è un tema fondamentale nelle normative recenti
- La gestione e il contenimento degli incidenti sono un aspetto fondamentale per gestire il "quando e non se"

Internet Of (Broken) Things

CERT nazionale Italia

COMPUTER EMERGENCY RESPONSE TEAM

MINISTERO DELLO SVILUPPO ECONOMICO

Link Utili FAQ Glossario

Home Chi siamo News Bollettini Documenti Contatti

Ricerca: mirai

Home » News » Attacchi DDoS da una botnet di telecamere a circuito chiuso

MINACCE

ATTACCHI DDOS DA UNA BOTNET DI TELECAMERE A CIRCUITO CHIUSO

Sicurezza: capire i rischi per l'azienda

- È importante capire quali sono le minacce e gli impatti specifici per i processi della nostra azienda
  - Il tema riguarda i vertici aziendali e i process owner

La sicurezza non è un problema dell'IT!!!

- A livello di sistema, è importante intervenire sulla supply chain, in modo da evitare che i prodotti utilizzati comprendano vulnerabilità e backdoor in grado di vanificare gli sforzi delle nostre azienda


15
MPH
Grazie!
Claudio Telmon
ctelmon@clusit.it