# Prospettive e sfide della sicurezza informatica e della Cyber-Security

Claudio Dell'Ali

SE Italia Extreme Networks

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

# ZERO TRUST

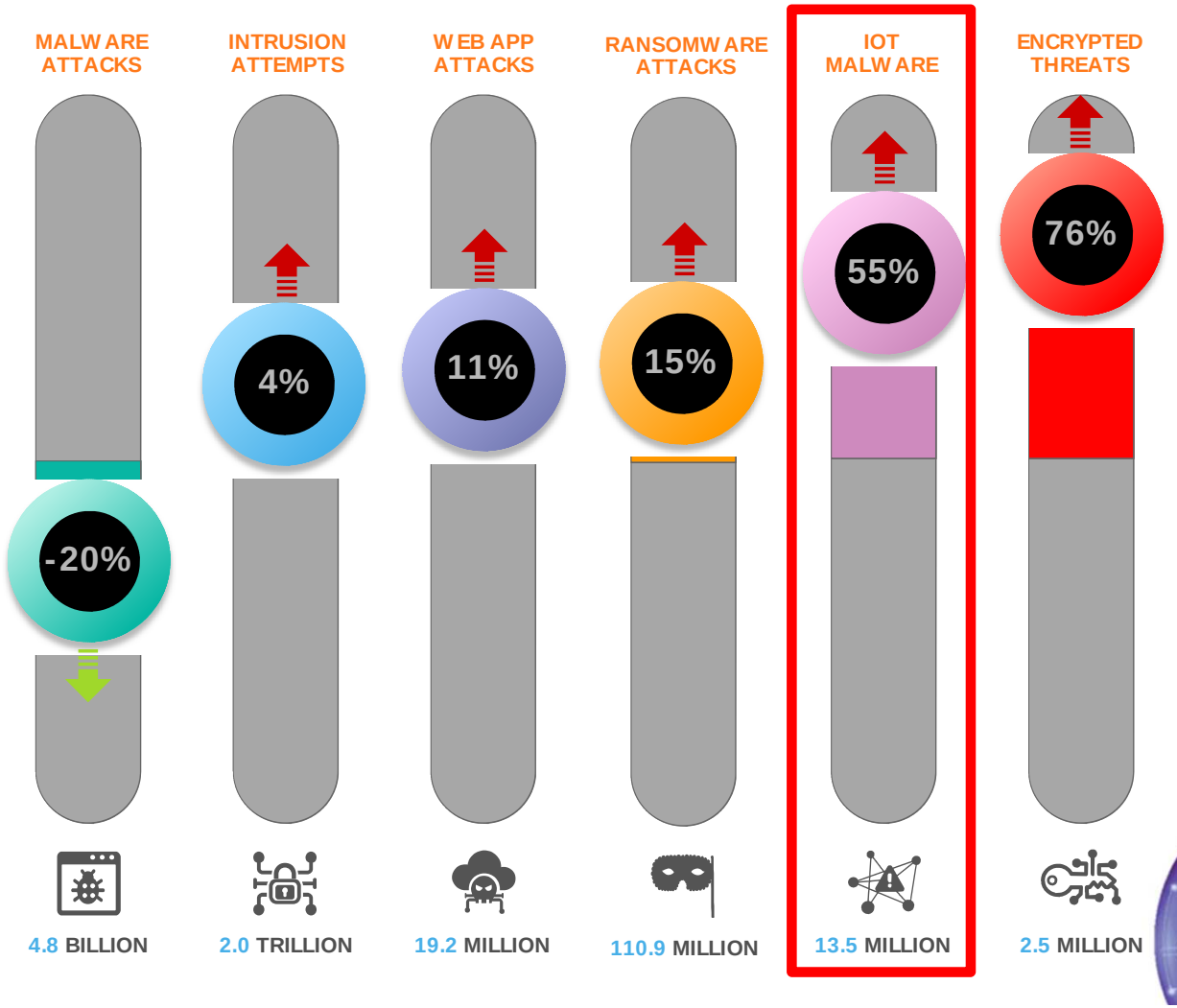
Zero Trust, Zero Trust Network o Zero Trust Architecture fanno riferimento a concetti di sicurezza e modello di minaccia che **non presuppongono più che attori, sistemi o servizi che operano all'interno del perimetro di sicurezza debbano essere automaticamente considerati attendibili** e che invece devono verificare qualsiasi cosa provino a connettersi i suoi sistemi prima di concedere l'accesso. Il termine è stato coniato da un analista della sicurezza presso Forrester Research

Il modello Zero Trust è la risposta alla consapevolezza che l'approccio alla **sicurezza perimetrale da sola non funziona:** molte violazioni dei dati sono avvenute perché gli hacker, una volta superati i firewall aziendali, sono stati in grado di spostarsi attraverso i sistemi interni senza molta resistenza.

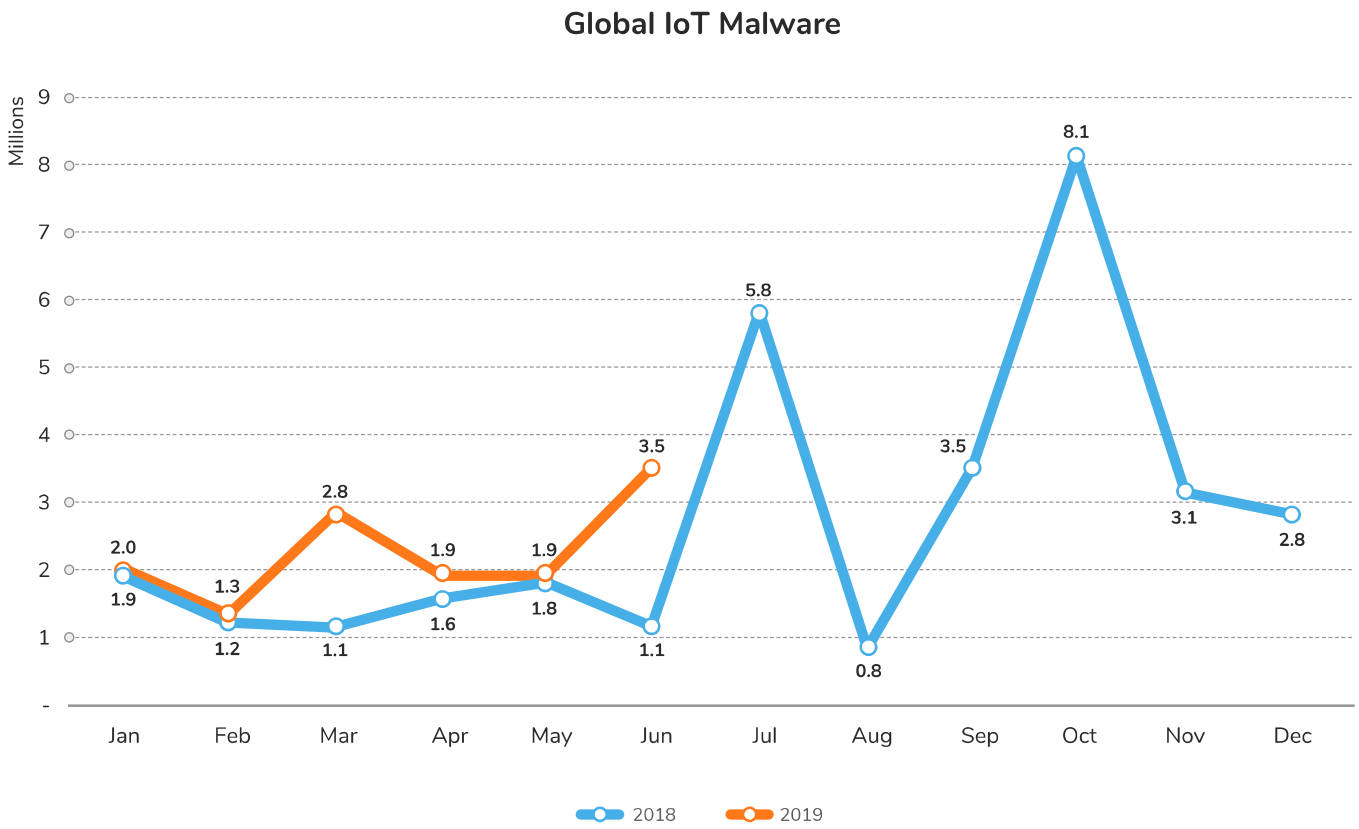
Inoltre, con l'avvento del **Cloud, il perimetro stesso non è più chiaramente definito**, poiché le applicazioni e gli archivi di dati possono essere locali e/o nel Cloud, e devono garantire accesso agli utenti da più dispositivi e posizioni.

# CYBERATTACK TRENDS

Nel 2019, a livello globale, gli addetti ai lavori hanno registrato un decremento degli attacchi basati su ‘’Malware’’ ma una crescita costante di altri tipi di pericolose Cyber Minacce come ad esempio i Malware specifici per il mondo delle IOT Device



# I MALWARE PROLIFERANO NEL MONDO IOT




Solo considerando la prima metà del 2019, gli addetti ai lavori hanno già registrato ben 13,5 milioni di attacchi verso le Device IoT, che superano i primi due trimestri del 2018 ben del 54,6%

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

# WANNACRY & FIGLI MINACCE CONTINUE

| Ransomware Volume YTD | | | |
|---|---|---|---|
| | *1H 2018* | *1H 2019* | *Change* |
| **U.K.** | **2.2M** | **6.4M** | **+195%** |
| **Global** | **96.6M** | **110.9M** | **+15%** |
| **U.S.** | **52.5M** | **41.7M** | **-21%** |
| **India** | **1.0M** | **382K** | **-62%** |
| **Germany** | **5.4M** | **1.6M** | **-71%** |

Circa 110.9 milioni di Attacchi Ransomware sono stati registrati solo nella prima metà del 2019!

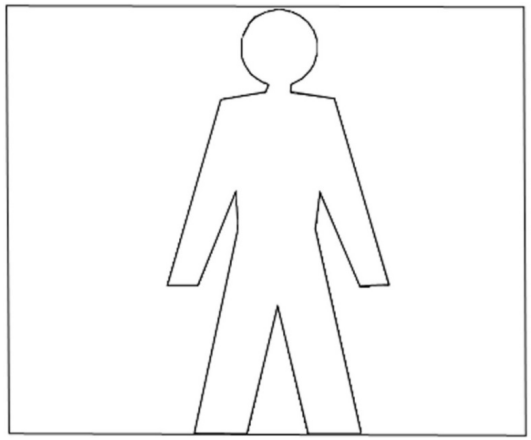
Il fatto è che la premiata ditta ''Wannacry e Figli'' continua a finanziare le azioni criminose dei cattivoni di Internet con un incremento Globale pari al 15% anno su anno

# RaaS: WANNACRY AS-A-SERVICE

Questa tabella evidenza come a livello Globale i Cybercriminali stanno inondando la rete di nuove e sempre più sofisticate tipologie di attacchi come il Ransomware-As-A-Service (RaaS) e gli Open-Source Malware Kits

| 2018 | | | 1H 2019 | | |
|---|---|---|---|---|---|
| **FAMILY** | **VOLUME** | **TYPE** | **FAMILY** | **VOLUME** | **TYPE** |
| Cerber | 101.6 Million | RaaS | *Cerber* | 39.5 Million | RaaS |
| BadRabbit | 7.8 Million | Custom | *Gandcrab* | 4.0 Million | RaaS |
| Dharma | 7.34 Million | Custom | *HiddenTear* | 4.0 Million | Open Source |
| LockyCrypt | 6.1 Million | Custom | *CryptoJoker* | 2.4 Million | Open Source |
| CryptoJoker | 5.6 Million | Open Source | *Locky* | 1.8 Million | Custom |
| Locky | 2.4 Million | Custom | *Dharma* | 1.5 Million | Custom |
| Petya | 1.9 Million | Custom | | | |

# RICORDIAMOCI CHE:



L'essere umano, oltre che rappresentare il bersaglio, è anche il vettore inconsapevole degli attacchi informatici.

Molti attacchi informatici utilizzano infatti tecniche di Social Engineering e numerosi Cyber Criminali adottano metodi sempre più complessi per bypassare il ''Firewall Umano'', con l'obiettivo di convincere un individuo, specificamente selezionato, ad eseguire un'azione che provoca un'infezione o la divulgazione di informazioni preziose. L'attaccante crea qualcosa di plausibile, di verosimile, partendo dall'analisi comportamentale dell'individuo che interagirà con i Sistemi Informatici sfruttando la psicologia umana.

In aggiunta oggi i Cyber Criminali sono mossi e invogliati da grandi e facili guadagni.

L'Uomo è l'Anello Debole

!

# PERCHE' HANNO SUCCESSO

Offrono al Cyber Criminale un **modo semplice e sicuro per guadagnare**:

- non vi è trasferimento illegale di fondi dagli account delle vittime
- non ci sono intermediari
- da parte dei cyber criminali non è richiesta nessuna azione

Fanno leva **accusando le vittime**:

- spesso accusano gli utenti di aver fatto qualcosa di illegale e/o sconcio (potrebbe essere vero…)
- sollevano dubbi relativi a download di materiale pornografico
- vengono citati articoli del codice penale

Il Malware meno discreti impongono la visione di **immagini "imbarazzanti"**:

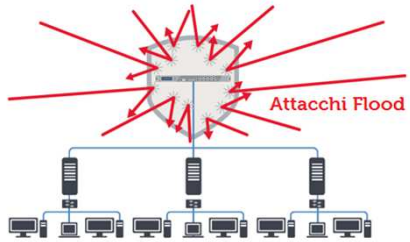
- immagini pornografiche o accuse di illegalità
- L'utente imbarazzato è scoraggiato a denunciare il problema

Millantano potenziali perdite catastrofiche di documenti personali/aziendali:

# COSA CI DICONO I DATI

Questi dati ci indicano chiaramente quali sfide si dovranno accogliere e vincere!

- Malware & Ransomware sempre più sofisticati e cifrati
- IOT: Internet of Threats
- File Threats: le minacce nascoste nei file più utilizzati
- Nuove modalità d'intrusione
- Minacce dal mondo dei Bitcoin
- Attacchi alle Applicazioni WEB






# CYBER ATTACK: FBI & POSTAL POLICE POINT

FBI, Italian Postal Police and other national and international bodies, do not approve the payment of a ransom in response to a ransomware attack

THE FBI FEDERAL BUREAU OF INVESTIGATION

FBI CYBER DIVISION

polizia delle comunicazioni

## What to do?

*Prevention* is the key!

# COSA FARE IN CONCRETO

## La Sicurezza è un Processo che parte dalle specifiche Esigenze

Fare Sicurezza non è solo un Hardware o un Software: è un vero e proprio **Processo**!

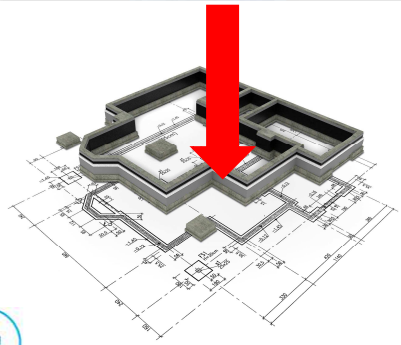
Per garantire la Sicurezza di un Infrastruttura occorre effettuare un percorso:

- **Fare Training**: agli utenti dei sistemi ed agli addetti ai lavori
- **Fare Maintenance di tutta l'infrastruttura**: System Patches, Software Update e Device Upgrade
- **Utilizzare Sistemi di Network Visibility**: Che cosa viene eseguito nella mia rete in Real Time? Come è utilizzata la mia infrastruttura?
- **Effettuare un costante Management**: Device management, avere un inventario delle Device aggiornato, utilizzare sistemi di allarmistica basati su Eventi importanti in base all'infrastruttura
- **Implementare Politiche di Access Control**: sulla rete cablata o senza fili Device ed Utenti devono autenticarsi

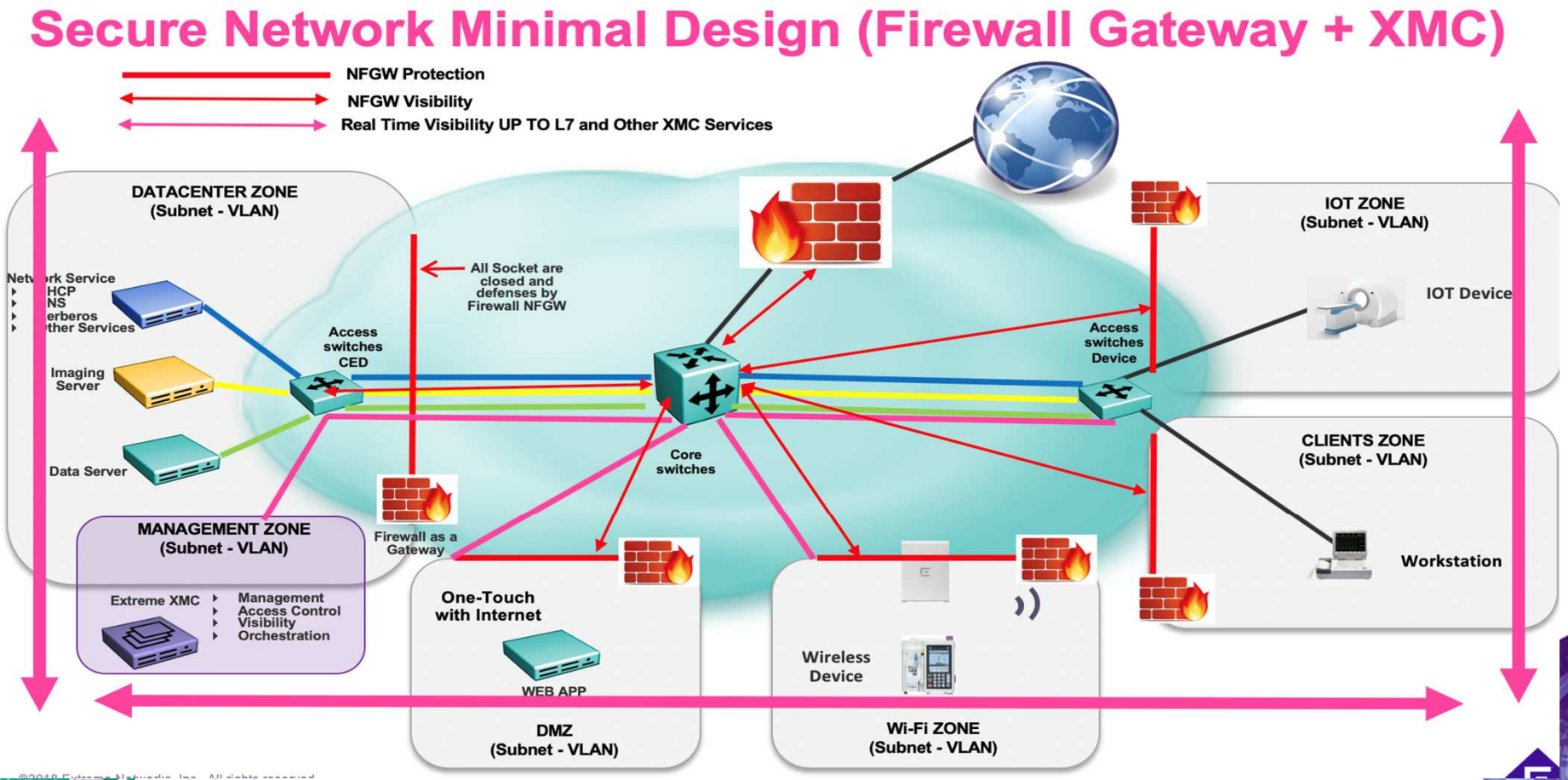
# ARCHITETTURE SICURE DALLE FONDAMENTA

## Questi dati ci indicano chiaramente quali sfide si dovranno accogliere e vincere!

- Mettere in sicurezza l'infrastruttura e la rete dalle Fondamenta:
  - Non solo sicurezza perimetrale e quindi Firewall
  - Segmentazione: una Zona circoscritta è più facile da difendere e da tenere sotto controllo
  - Applicare Sicurezza all'EDGE: **NAC** e Controllo Accessi
  - Accendere la luce: **Visibilità** del traffico EST-OVEST, INTRAVLAN & nello stesso dominio di Broadcast
  - Sistemi di monitoraggio e Automazione (**Orchestration**)
  - Sicurezza sulle Applicazioni
- IOT Security Layer per qualunque rete
- Analizzate il traffico Cifrato
- Trasmettere Dati Sensibili in modalità cifrata anche nella LAN (**IPSEC**)
- SandBoxing




# ESEMPIO CONCRETO



# GRAZIE

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA
A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO