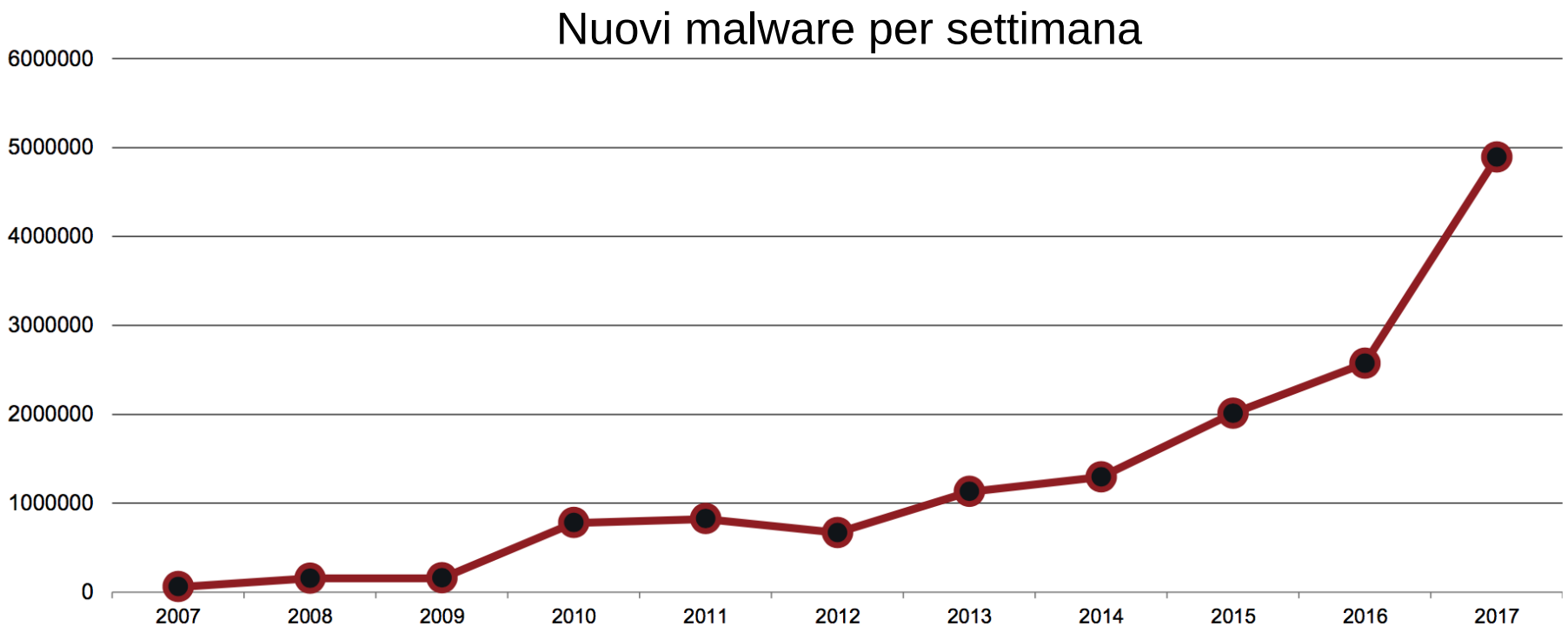
Minacce e Attacchi

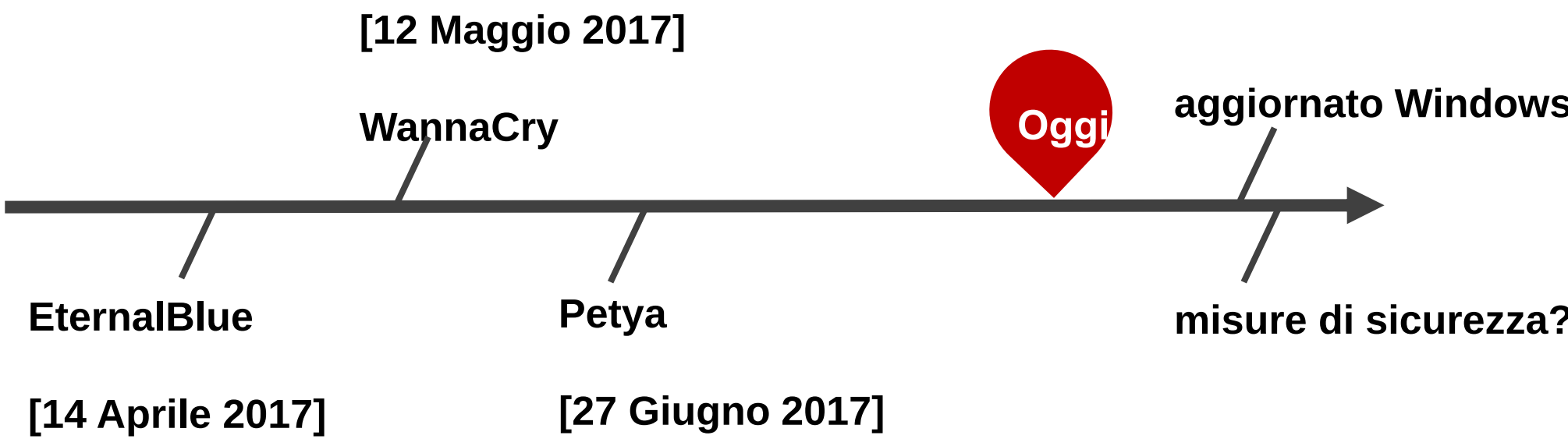
Franco Sivilli
fsivilli@unich.it

I meno famosi... 5.000.000 nuovi malware per settimana



Source: FortiGuard Labs

Cronistoria degli ultimi attacchi globali



Cosa sappiamo di Petya?

Gli attacchi complessi richiedono studi approfonditi che spesso integrano a distanza di tempo nuovi dettagli:

- Petya o ExPetr (varianti NotPetya o Nyetya)
- Classificato inizialmente come RansomWare, si è visto che era un Wiper
- E può essere definito RansomWorm dal punto di vista della diffusione
- Sfrutta gli exploit EternalBlue e EternalRomance,il sistema di aggiornamento di MeDoc (sistema delle tasse Ucraino), oltre al canale mail
- L'infezione si stima essere partita proprio dall'Ucraina
- Per molti non sembra essere "Cyber Crime" ma uno "State-Sponsored cyber attack"
- Per via della tipologia dell'attacco e della situazione geo politica locale
- Bilancio delle vittime stimato: oltre 45.000 computer infetti in 74 paesi.

Definizione di Petya da Wikipedia

Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.

Cosa sappiamo di WannaCry?

Gli attacchi complessi richiedono studi approfonditi che spesso integrano a distanza di tempo nuovi dettagli:

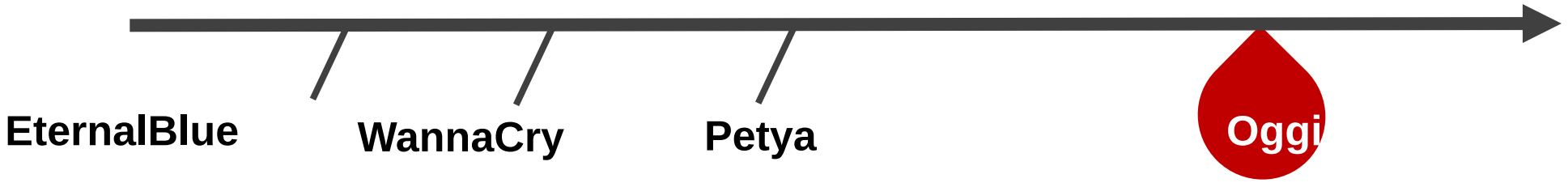
- WannaCry (o WanaCrypt0r 2.0) è un Worm, di tipologia Ransomware
- Il 12 maggio 2017 il malware ha infettato i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo
- WannaCry sfrutta una vulnerabilità di SMB tramite un *exploit* chiamato EternalBlue
- Il malware viene diffuso attraverso finte email e, dopo che viene installato su un computer, comincia a infettare altri sistemi presenti sulla stessa rete
- WannaCry cripta i file bloccandone l'accesso
- A quel punto, in un file denominato @Please_Read_Me@ è presente una richiesta di riscatto, inizialmente di 300 dollari (in bitcoin) ma poi elevati a 600 dollari
- Bilancio delle vittime stimato: oltre 250.000 computer infetti in 150 paesi

EternalBlue

EternalBlue è il nome di un exploit che si ritiene sia stato scritto dalla **National Security Agency** (NSA). Il mondo informatico è venuto a conoscenza dell'esistenza di questo exploit dopo che il gruppo di hacker chiamato **The Shadow Brokers** lo ha illegalmente diffuso il 14 aprile 2017

Questa vulnerabilità è oggi elencata come la numero CVE-2017-0144 nel catalogo Common Vulnerabilities and Exposures (CVE)

Il servizio di aggiornamento standard per Windows consente di risolvere questo problema attraverso la **patch di sicurezza rilasciata da Microsoft in data 14 marzo 2017 e chiamata MS17-010**



Cifre stimate

Petya – 8.000$

è stato estratto un solo indirizzo di pagamento dove fino al tardo pomeriggio sono state compiute 18 transazioni per un totale di 1,8 bitcoin, meno di 4 mila euro. Con altri 10 o 12 pagamenti in coda. Poi è successa una cosa strana. Raccolti ottomila dollari l'indirizzo mail al quale scrivere è stato chiuso.

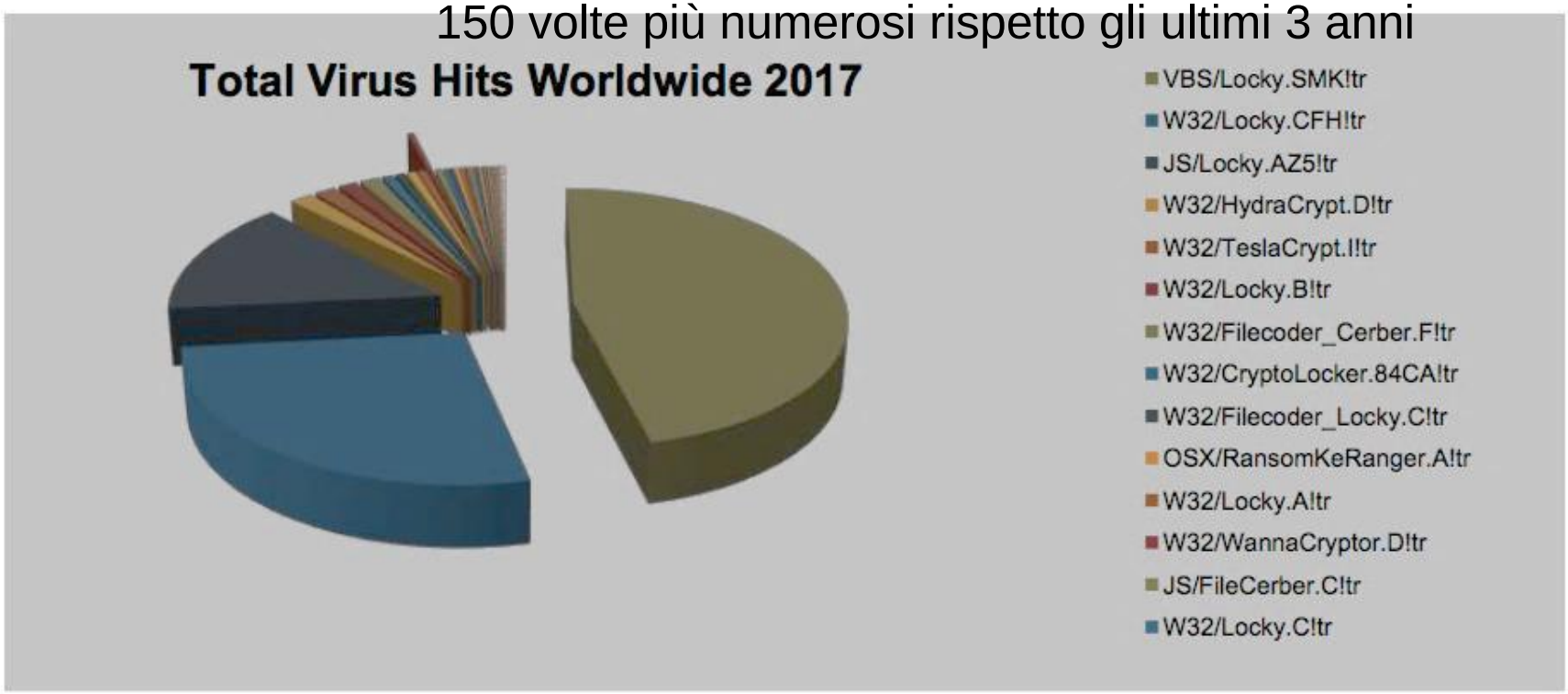
WannaCry – Meno di 100.000$

Calcolo più complesso ma stimato al di sotto dei 100.000$

http://www.repubblica.it/tecnologia/sicurezza/2017/06/27/news/i_segreti_del_virus_petya_due_minacce_note_in_un_nuova_combinazione_micidiale_-169300022/

Top Ransomware 2017

150 volte più numerosi rispetto gli ultimi 3 anni



Sistemi più comunemente utilizzati come vettore di attacco – Adobe, MS Office, siti web, Worm-like

University network fault, IoT flaws

NEWS

Hackers used flaws in IoT devices to take down university network

By **Rene Millman** - February 13, 2017

Baby monitor attack

NEWS ANALYSIS

Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny

This is the third time news has circulated about some jerk hijacking a wireless Foscam camera/baby monitor and made his virtual intrusion known by talking. Please change the default password!

MORE LIKE THIS

Hacker strikes again: Creep hijacks baby monitor to scream at infant and...

2 more wireless baby monitors hacked: Hackers remotely spied on babies and...

Eerie music coming from wireless baby cam; is it a haunting? No, it's a hacker

VIDEO

Tim Cook speaks cybersecurity at Stanford

Russian hackers, SCADA attack

Security

48

Irked train hackers talk derailment flaws, drop SCADA password list

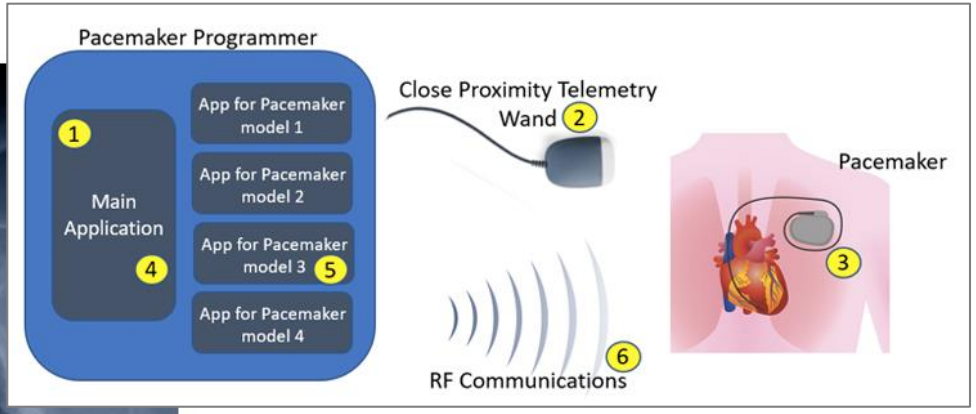
Maybe now they'll fix it.

4 Jan 2016 at 07:30, Darren Pauli

Pacemakers, Pay or die scenario

Over 8,600 Vulnerabilities Found in Pacemakers

Monday, June 05, 2017 Swati Khandelwal



It uses more than 300 third-party libraries, 174 of which are known to have over 8,600 vulnerabilities.

"*If you want to keep living, Pay a ransom, or die.*" This could happen, as researchers have found thousands of vulnerabilities in Pacemakers that hackers could exploit.

Defacement Comune.Roma.it

Attacco hacker al sito del Comune di Roma: «Islam non è terrorismo»

13

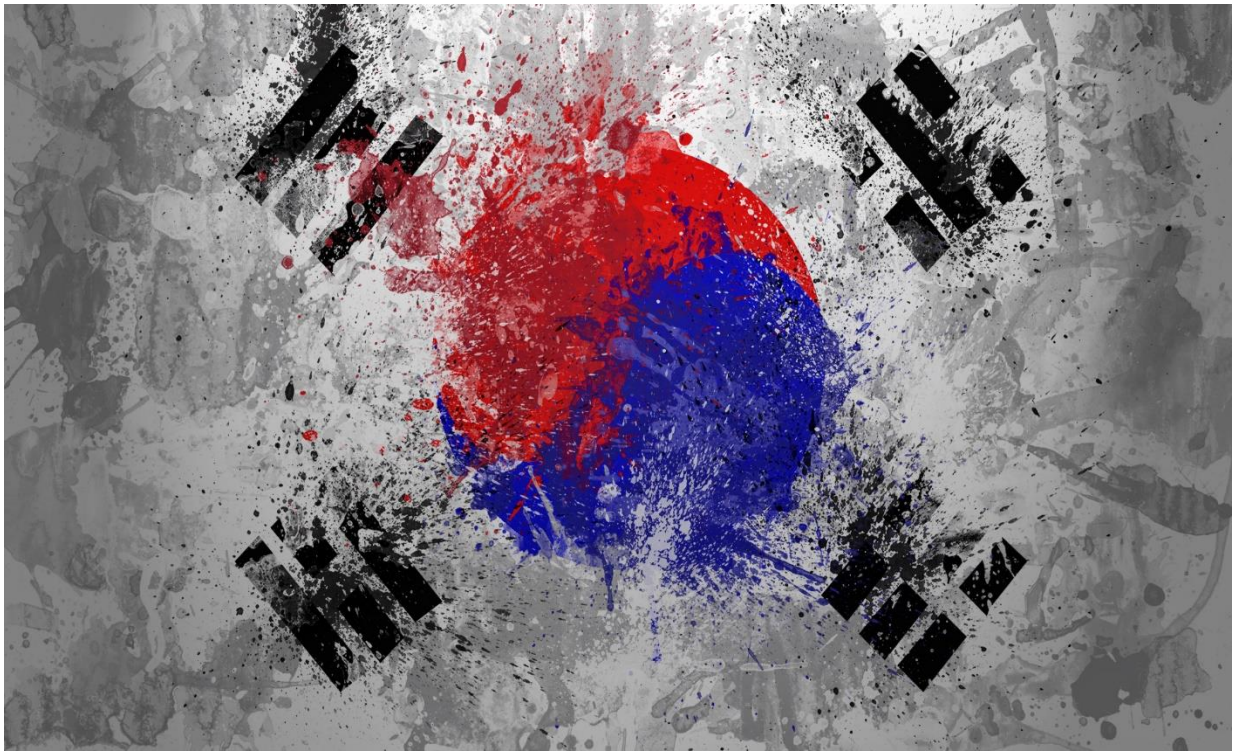
Attacco hacker al portale del Comune di Roma. A quanto apprende l'agenzia Dire, stamattina presto pirati informatici hanno danneggiato le pagine dedicate agli open data che adesso risultano oscurate. Il ripristino del servizio è previsto per la tarda mattinata.

NBC, Drive by download

Alcune pagine della NBC risultano compromesse. Le pagine colpite sono state utilizzate per effettuare un attacco ai visitatori (decine di migliaia) senza la necessità di ulteriori azioni rispetto la semplice navigazione.

South Korea, Time Bomb attacks

Formattati 32.000 computer appartenenti alle banche Shinhan Bank e Nonghyup Bank e alle emittenti TV KBS, MBC, YTN.



Stuxnet [2010]

Stuxnet, Israele e Usa dietro al virus "Creato da noi, ci è sfuggito di mano"

Il codice era stato sviluppato per contrastare il programma nucleare iraniano. Ma una modifica non perfettamente programmata introdotta dal governo di Tel Aviv ha reso il worm in grado di replicarsi su macchine esterne alle centrali. Il ruolo chiave di Obama nell'operazione denominata "Giochi olimpici", iniziata nell'era Bush

di TIZIANO TONIUTTI

Lo leggo dopo

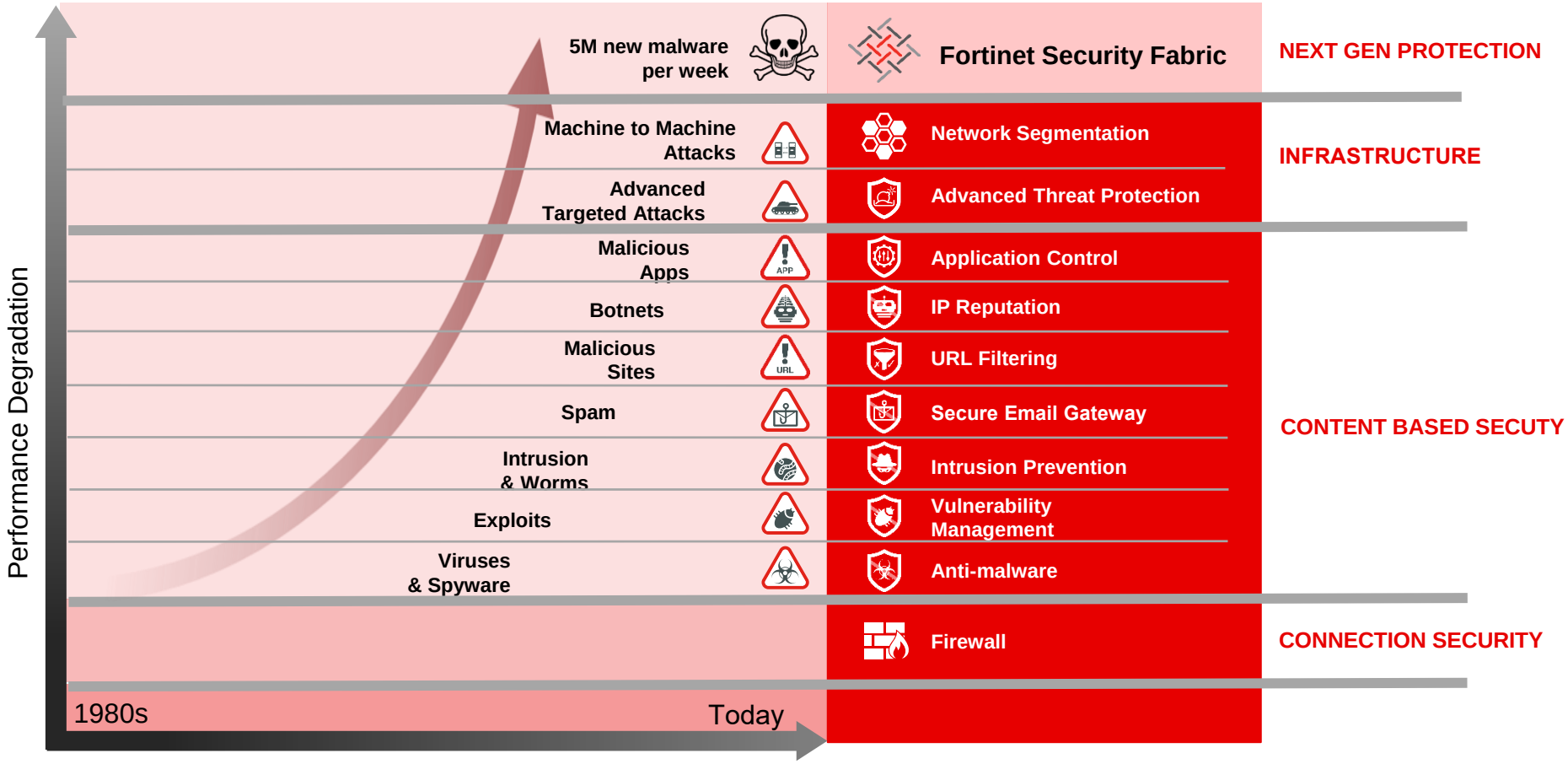
(reuters)

UN CLASSICO SCENARIO di spie e paesi in guerra, anche se soltanto nei circuiti informatici, quello che vede Usa, Israele e Iran nell'*affaire* del virus Stuxnet, una delle più potenti cyber-armi mai sviluppate, ora consegnata alla storia. L'operazione di sviluppo e diffusione del worm denominata "Giochi olimpici" è iniziata sotto l'amministrazione di George Bush Junior e poi proseguita, in maniera più incisiva, sotto la presidenza Obama. E' il New York Times ad alzare il velo su questa cyberguerra lanciata dagli Usa, che arriva alle cronache dopo 18 mesi di interviste con fonti americane, europee e israeliane coinvolte nel programma, come pure con esperti del settore estranei all'operazione.

APPROFONDIMENTI

ARTICOLO

Per fermare le nuove minacce occorre una cooperazione tra prodotti



Fine

fsivilli@unich.it