

# CRYPTOWORM E CONTROLLI ESSENZIALI DI SICUREZZA

CYBERSECURITY SUMMIT - Milano 7 Giugno 2017

Roberto Baldoni  
@robertobaldoni

CYBER INTELLIGENCE  
AND INFORMATION  
SECURITY CENTER



SAPIENZA  
UNIVERSITÀ DI ROMA



**cini**  
**Cybersecurity National Lab**

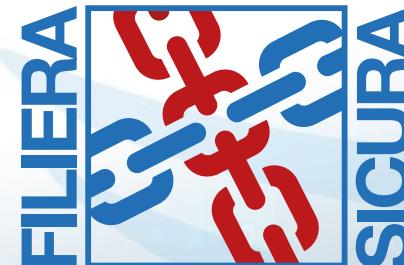


**CIS SAPIENZA**

CYBER INTELLIGENCE AND INFORMATION SECURITY



# Cybersecurity National Lab



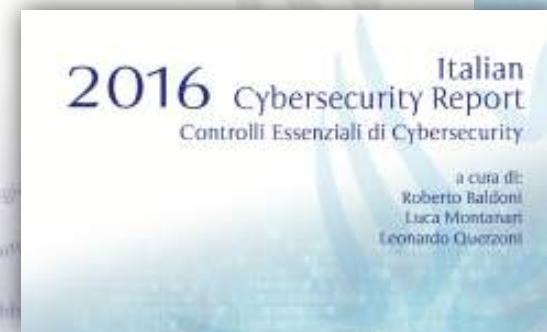
## MASTER OF SCIENCE IN CYBERSECURITY

### OBETTIVI FORMATIVI

La laurea magistrale in Cybersecurity dell'Università di Roma "La Sapienza" è la prima laurea magistrale di questo genere offerta in Italia. Il corso di studio si caratterizza per un'offerta didattica interdisciplinare che raccoglie contributi dell'informatica, dell'ingegneria, della statistica, delle scienze giuridico-economiche e organizzative, insieme a conoscenze specifiche dei principali domini applicativi di protezione contro i cyber-attacchi.

In particolare, la laurea magistrale in Cybersecurity offre le conoscenze professionali, sia dal punto di vista tecnologico sia organizzativo sia normativo, necessarie per definire, supervisionare e coordinare i processi di analisi e governo della sicurezza di sistemi ed informazioni nell'ambito di infrastrutture informatiche complesse, per organizzare la protezione da cyber-attacchi, attuare i processi di gestione degli incidenti informatici, gestire il recupero dei casi di attacco, mettendo con successo, sviluppare attraverso metodologie avanzate di progettazione, infine, per comprendere gli aspetti legali alla sicurezza di sistemi e informazioni all'interno delle politiche aziendali di gestione del rischio.

La forte enfasi su una formazione multidisciplinare sia tecnologica, sia giuridica, sia economica caratterizza l'unicità dei contenuti della laurea magistrale in Cybersecurity, prima in Italia, ad offrire all'interno di un percorso altamente specializzante, corsi indirizzati all'ethical hacking, analisi di malware, digital forensics e security governance.



a cura di:  
Roberto Baldoni  
Luca Montanari  
Leonardo Quarzoni



- Malware analysis
- Malware detection
- Penetration testing
- Vulnerability assessment
- Dependability
- Stream Processing
- Machine Learning for security

- Big Data analysis
- Big Data for Security
- Framework e Standard
- ...





# CRYPTOWORM WANNACRY

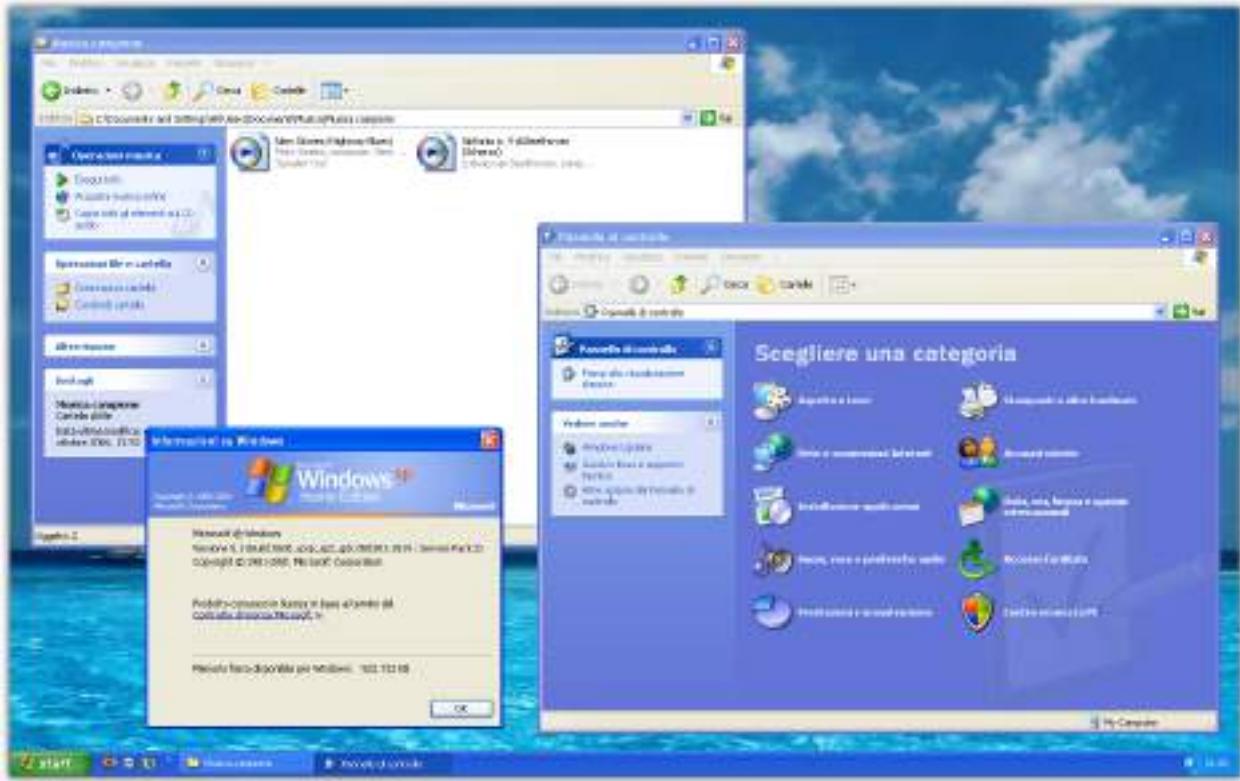
# CryptoWorm “WannaCry”: Cronistoria

- Wannacry ha colpito computer equipaggiati con una versione vulnerabile del protocollo SMB v1 (CVE-2017-0144) di Microsoft Windows
- Una volta infettato un computer automaticamente infetta altri computer vulnerabili tramite la rete indipendentemente dalle azioni degli utenti (worm) e successivamente cifra il contenuto del computer (Cryptolocker)
- Nasconde un meccanismo di kill switch, fortunatamente trovato e messo in opera il 12 maggio
- Durante la sua attività di circa quattro giorni il malware ha :
  - Infettato circa 400.000 macchine rilasciando il cryptolocker
  - Infettato circa 3 milioni di macchine senza rilasciare il cryptolocker grazie al kill switch
  - Stima di circa 10 milioni di host infettati e criptati senza kill switch

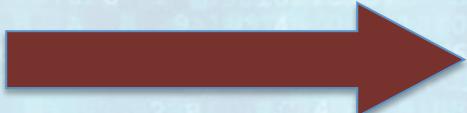
# Dettagli sul worm

WannaCry Usa due Exploit, entrambi attribuiti all'Equation Group dell'NSA:

- EternalBlue: permette di eseguire codice arbitrario ricevuto da remoto sulla macchina vulnerabile (cioè con a bordo SMBv1 – Server Message Block).
- DoublePulsar è una backdoor (implant tool) eseguita attraverso EternalBlue che gira in kernel mode. Ha solo tre comandi, ping, kill, and exec. L'ultimo dei tre permette di caricare il Cryptolocker.



End of Support  
Windows XP  
Feb 2014



Windows XP  
including SMB  
25 Oct 2001

mag.1 934256

100

itemisage = BM-NBv8hFp5VwBykgbirVLndZIEFCY8ht8  
2p-bots = o1u40K0cMoFEa707dsE1zFMwW2o7sDw-td3x9gVz4h4t50rlJ7U6GUhr5GZoWaQ9f2friY58z1h0JMVFn1Lp

quation Group Cyber Weapons Auction - Invitation

!! Attention government sponsors of cyber warfare and those who profit from it !!!!

Microsoft Security Bulletin MS17-010 - Critical  
SMB Server (4013389)

# Microsoft Security Bulletin MS16-035

# End of Support Windows XP Feb 2014

# Microsoft patch for SMB

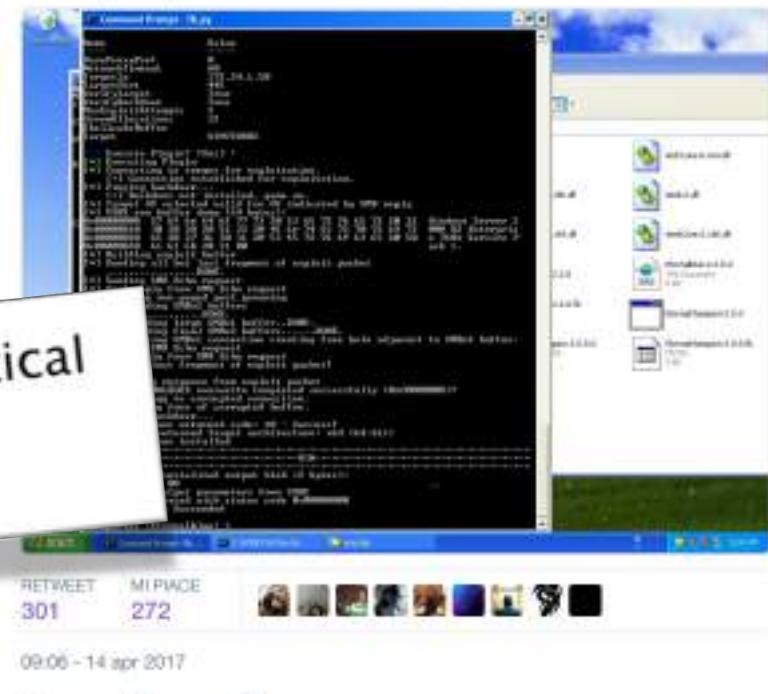
## 14 March 2017

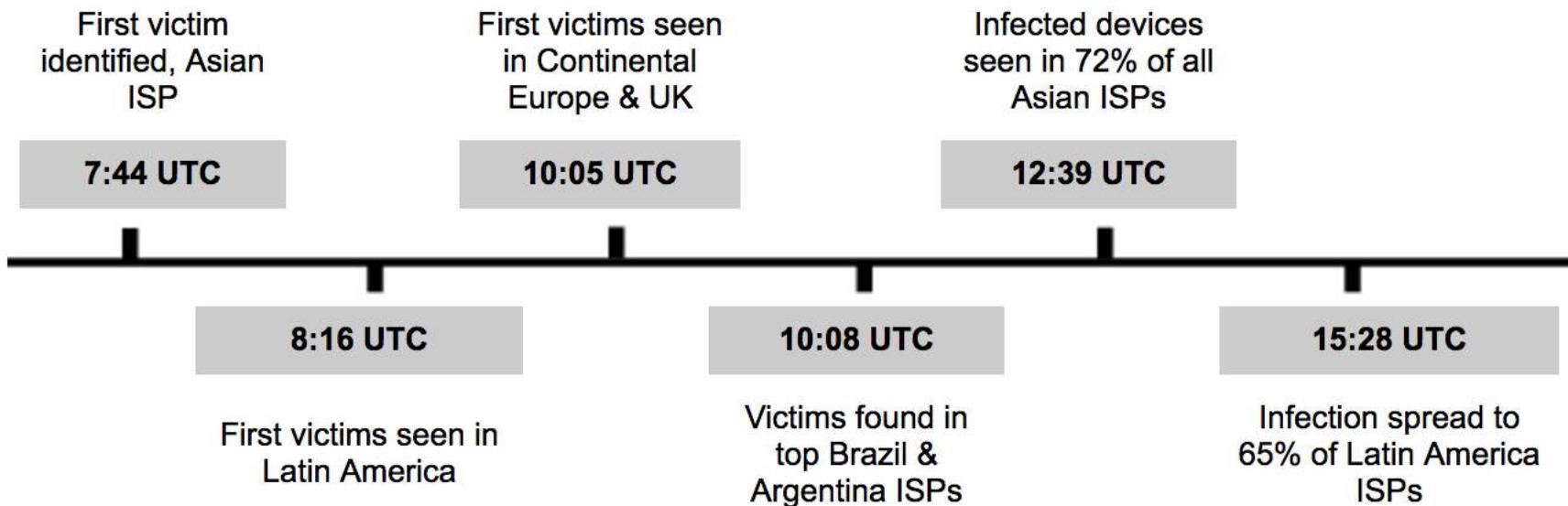
# Windows XP including SMB 25 Oct 2001

# Shadow Brokers 1st dump August 2016

# Shadow Brokers 4th dump 14 April 2017

ETERNALBLUE -here is a 0day exploit successfully getting RCE on Windows 2008 SP1 (x64) via SMBv2 #0day from FUZZBUNCH

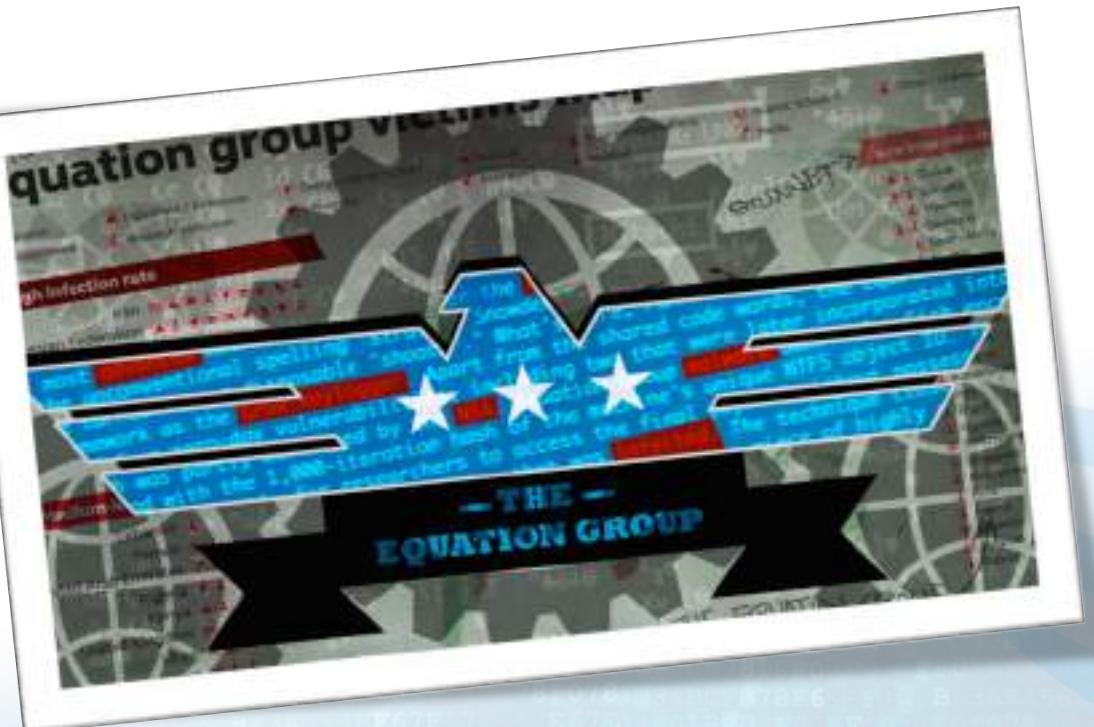




# OSSERVAZIONI



# Fino a 15 anni di vulnerabilità



Microsoft  
patch for  
SMB  
14 March 2017

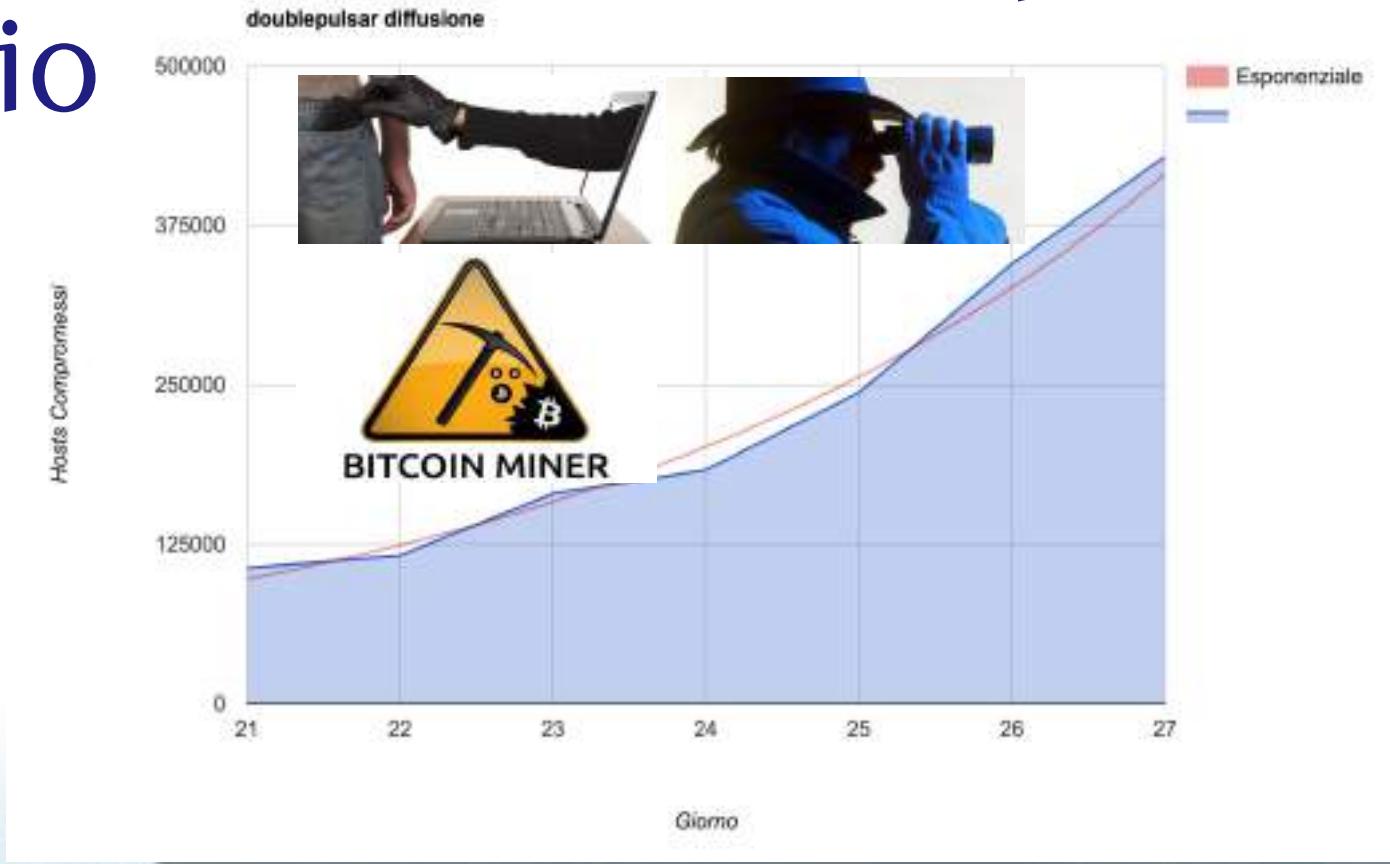
Potential use of EternalBlue by Equation Group

Windows XP  
including SMB  
25 Oct 2001

Shadow Brokers  
Exfiltration  
Oct 2013

End of Support  
Windows XP  
Feb 2014

# Cosa è successo dal 14 Aprile all'11 Maggio



Use of EthernalBlue by any cybercriminal

Shadow Brokers  
Dump  
14 April 2017

21 April-27  
April

Wannacry  
spreading  
12 May 2017

<https://blog.binaryedge.io/2017/04/21/doublepulsar/>

# Cosa è successo dal 14 Aprile all'11 Maggio

jennamagius commented on 28 Apr • edited

EternalBlue is fairly straightforward to reproduce, the only trick is that it involves opening 21 different connections. I've been able to install DoublePulsar without using the NSA tools by directly replaying the captured attack.

Files to reproduce this are:

<https://gist.github.com/jennamagius/301cead69d87719819d56fbde0d81238>

<https://gist.github.com/jennamagius/ca036fca317b3aeb33f55495e2a45ea7>

That's proven to work fairly consistently on freshly booted Server 08 R2 boxes. I think all it needs to work on non-freshly-booted ones is monkey patching in the correct "User ID" and "Tree ID" values out of the Session Setup AndX and Tree Connect AndX responses into all the later packets in connection 1.

Shadow  
Brokers Leak  
14 April 2017

Replaying  
the attack  
28 April

Wannacry  
spreading  
12 May 2017

# Cosa è successo dal 14 Aprile all'11 Maggio

Tempo di sviluppo malware attraverso:

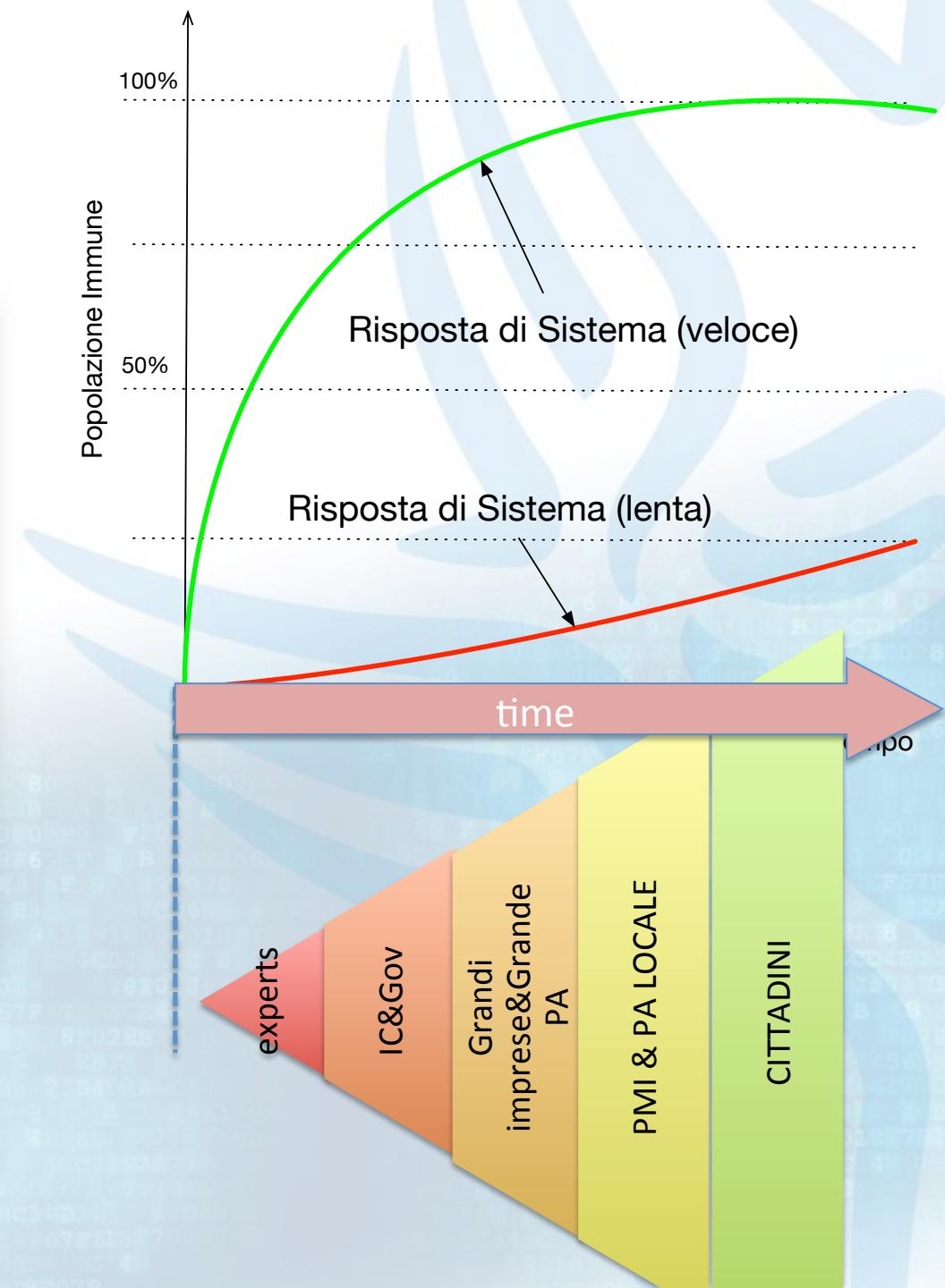
- exploit “weaponized” a partire da 2 giorni
- se la vulnerabilità non è “weaponized” abbiamo qualche giorno in più’ dipende dalla complessità della costruzione dell’exploit



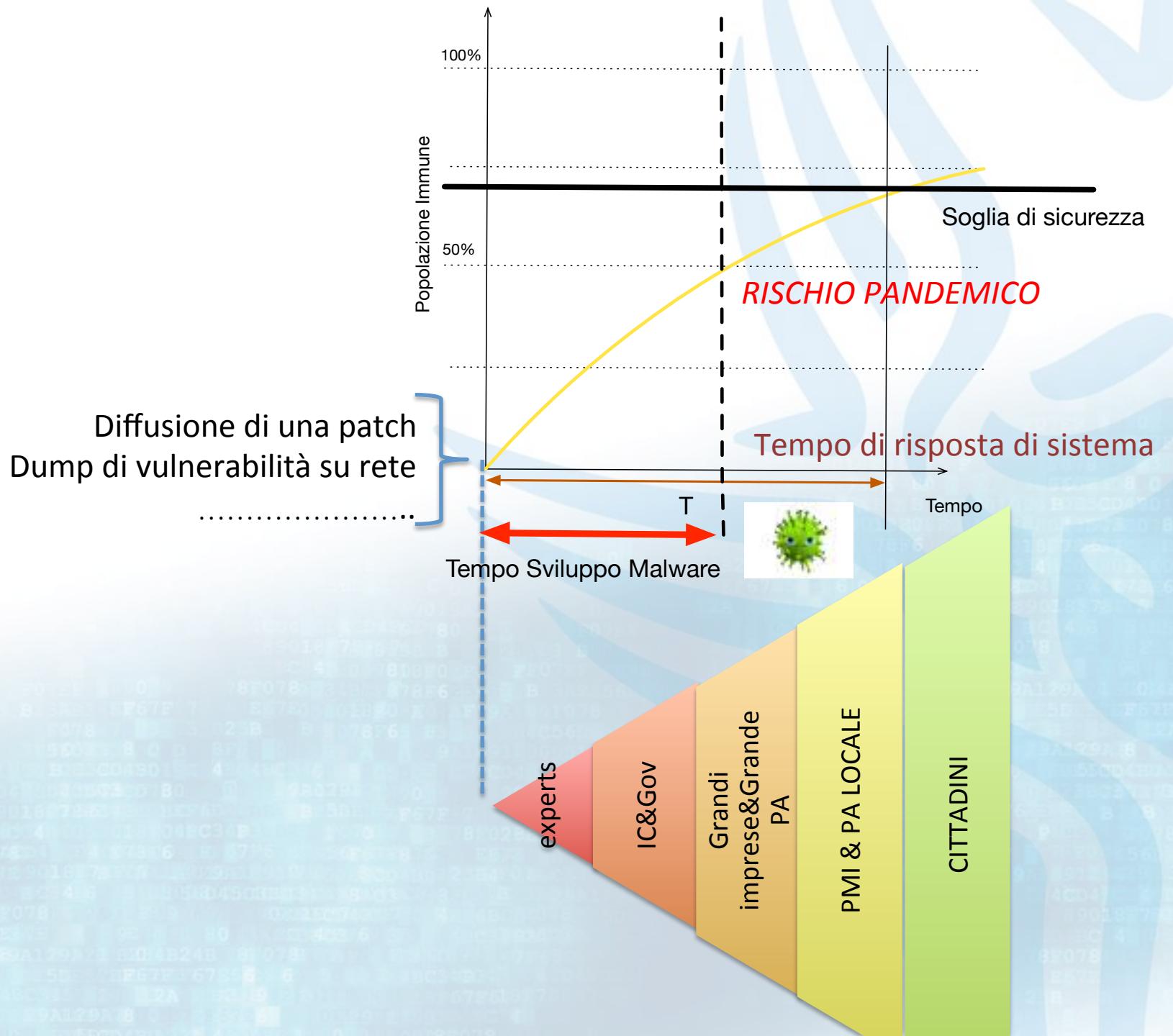
# Risposta di sistema paese



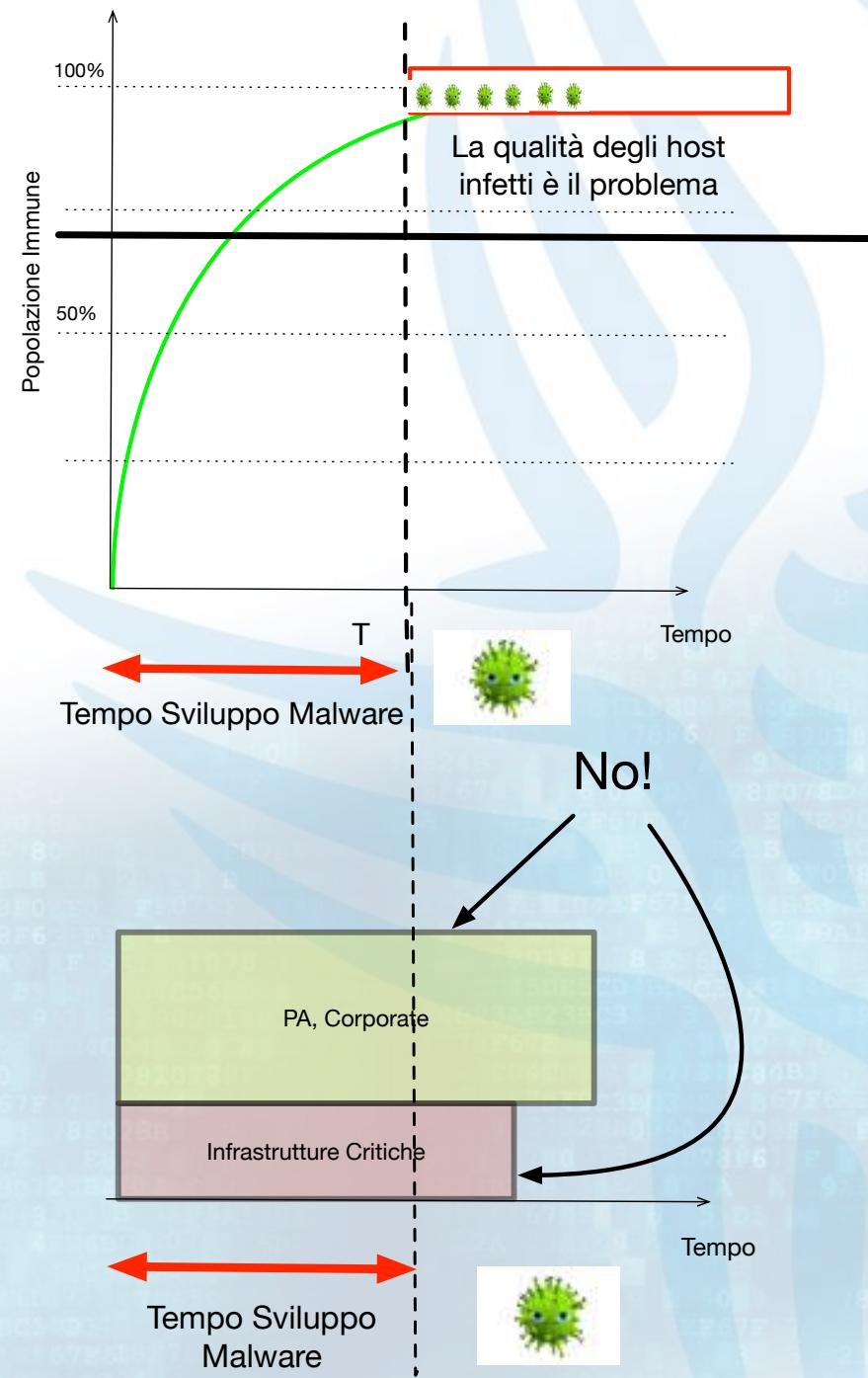
Revisionato 31/5/2017



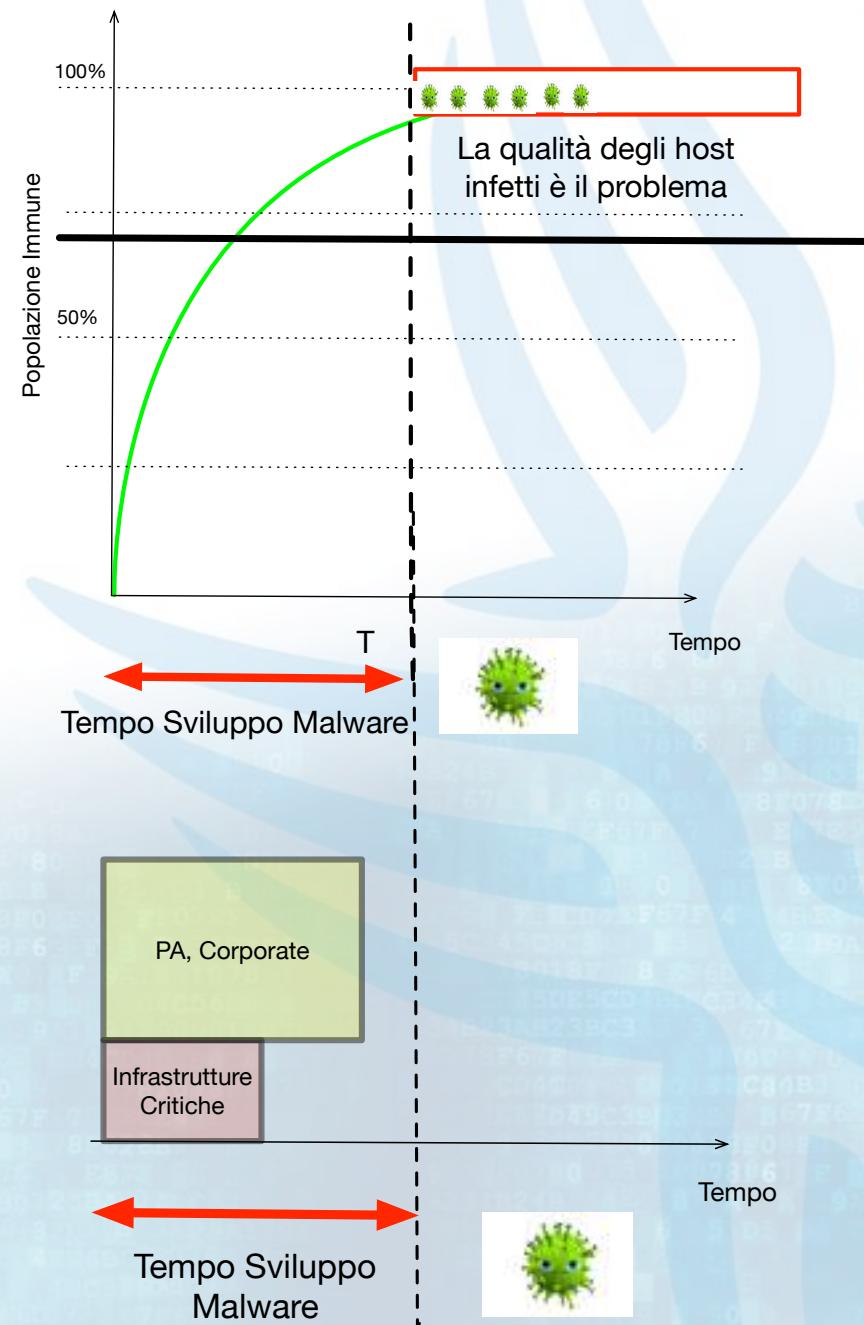
# Risposta di sistema paese



# Risposta di sistema paese



# Risposta di sistema paese



# The close future

Although what the June dump would contain is not clear at the moment, the Shadow Brokers' last announcement claimed that the upcoming data dump would include:

- Exploits for operating systems, including Windows 10.
- Exploits for web browsers, routers, and smartphones.
- Compromised data from banks and Swift providers.
- Stolen network information from Russian, Chinese, Iranian, and North Korean nuclear missile programs.



Shadow  
Brokers  
First dump  
August 2016

Shadow Brokers  
4th dump  
14 April 2017

Wannacry  
spreading  
12 May 2017

Shadow Brokers  
New dump  
30 June 2017

# The close future

Although what the June dump would contain is not clear at the moment, the Shadow Brokers' last announced dump was in June 2017. The new data dump would include:

Shadow Brokers  
5th dump  
30 June 2017

New spreadings in  
july-august 2017???

- Stolen network programs.

Shadow  
Brokers  
First dump  
August 2016

Shadow Brokers  
4th dump  
14 April 2017

Wannacry  
spreading  
12 May 2017

Shadow Brokers  
New dump  
30 June 2017



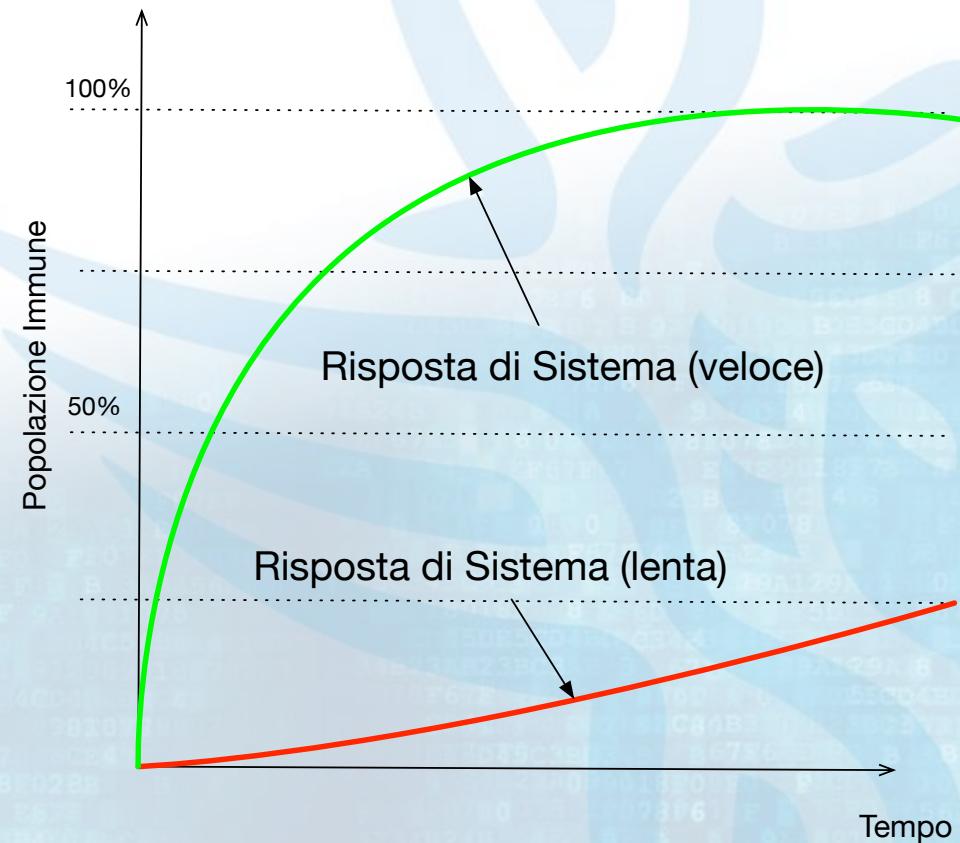
How can we prevent such future epidemics? This incident highlights the need to see cyber security as a public health issue just as much as one for law enforcement or intelligence agencies. It is a challenge to be solved by the entire ecosystem working to make itself more resilient and immune to future attacks — much as society works together to fight mutating influenza-virus outbreaks by using prevention, vaccination and basic hygiene.

**FINANCIAL TIMES**



# CONTROLLI ESSENZIALI DI CYBERSECURITY

# Come migliorare la risposta di sistema



Revisionato 31/5/2017

# Come migliorare la risposta di sistema



Revisionato 31/5/2017

- Indirizzo operativo 1 – Potenziamento delle capacità di *intelligence*, di polizia e di difesa civile e militare .....
- Indirizzo operativo 2 – Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati .....
- Indirizzo operativo 3 – Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento .....
- Indirizzo operativo 4 – Cooperazione internazionale ed esercitazioni .....
- Indirizzo operativo 5 – Operatività delle strutture nazionali, di *incident prevention, response e remediation* .....
- Indirizzo operativo 6 – Interventi legislativi e *compliance* con obblighi internazionali .....
- Indirizzo operativo 7 – *Compliance a standard e protocolli* di sicurezza .....
- Indirizzo operativo 8 – Supporto allo sviluppo industriale e tecnologico .....
- Indirizzo operativo 9 – Comunicazione strategica e operativa .....
- Indirizzo operativo 10 – Risorse .....
- Indirizzo operativo 11 – Implementazione di un sistema di *cyber risk management* nazionale .....

ma (veloce)

enta)

Tempo

# Come migliorare la risposta di sistema



## Indirizzo operativo 1 – Potenziamento delle capacità di *intelligence*, di polizia e di difesa civile e militare

### 7.1 Standardizzazione e compliance

- a. Aggiornare il quadro nazionale di riferimento agli *standard* e alle *best practices* secondo le normative ratificate NATO e UE, ed internazionali
- b. Identificare e aggiornare le misure minime di sicurezza da implementare sulle reti e i sistemi della PA e delle infrastrutture critiche
- c. Adottare *standard* di riferimento, *best practices* e requisiti minimi per la sicurezza delle reti e dei sistemi (tra cui quelli indicati in 7.1.a e 7.1.b)
- d. Costituire un sistema per l'accreditamento e l'auditing degli Enti responsabili dell'emissione di certificati digitali per l'autenticazione e per le altre certificazioni di sicurezza informatica

## Indirizzo operativo 10 – Risorse

## Indirizzo operativo 11 – Implementazione di un sistema di *cyber risk management* nazionale

Revisionato 31/5/2017

ione  
ello

culta  
to

onali,

e

illi

ale

operativa

na (veloce)

enta)

Tempo

# Controlli Essenziali sono parte dello stesso processo del Framework Nazionale



Strumento che permette di "iniziare" a parlare la lingua del Framework Nazionale dedicato a uno specifico target d'imprese



# Imprese target

## Le imprese che non hanno sufficienti risorse per adottare il Framework Nazionale

### Razionale:

- Possibilità di danni verso terzi in servizi/prodotti
- Esposizione su internet
- Dati sensibili, personali, know how nei dispositivi

#### 1.2 Imprese target del documento

5

##### Definizione delle imprese target

Il presente documento si rivolge alle organizzazioni, indipendentemente dalla loro dimensione, che non hanno struttura interna che si occupa di cybersecurity e per le quali valga almeno una delle seguenti frazioni:

- L'azienda possiede proprietà intellettuale/know how che deve rimanere riservato e memorizzata su dispositivi informatici o informazioni (disegni industriali, piani di sviluppo di prodotti, informazioni relative a processi e dinamiche interne, anche all'interno di messaggi email o di testi, business plan, prototipi software/hardware)?
- L'azienda ha clienti ai quali fornisce servizi o prodotti e tali prodotti o servizi potrebbero risentire in qualche disponibilità, nel caso in cui i sistemi dell'azienda fossero resi indisponibili oppure fossero controllati in maniera malevola da attaccanti?
- I prodotti (hardware/software/servizi) dell'organizzazione potrebbero essere installati in ambienti sensibili (es. IoT) oppure eventuali manipolazioni dei prodotti potrebbero causare danni a terzi?
- L'organizzazione ha una presenza su internet e offre servizi via web (es. fa business online, shop online, ecc.)?
- L'organizzazione è in possesso di dati personali relativi a dipendenti e/o clienti?
- L'azienda ha stipulato accordi di riservatezza (NDA) con clienti/fornitori?
- L'azienda gestisce sistemi ICS (es. SCADA)?
- L'azienda gestisce dati sensibili per conto di altre imprese (clienti o fornitori)?

Se l'organizzazione è parte del target, dovrebbe implementare i Controlli Essenziali presenti in questo volume.

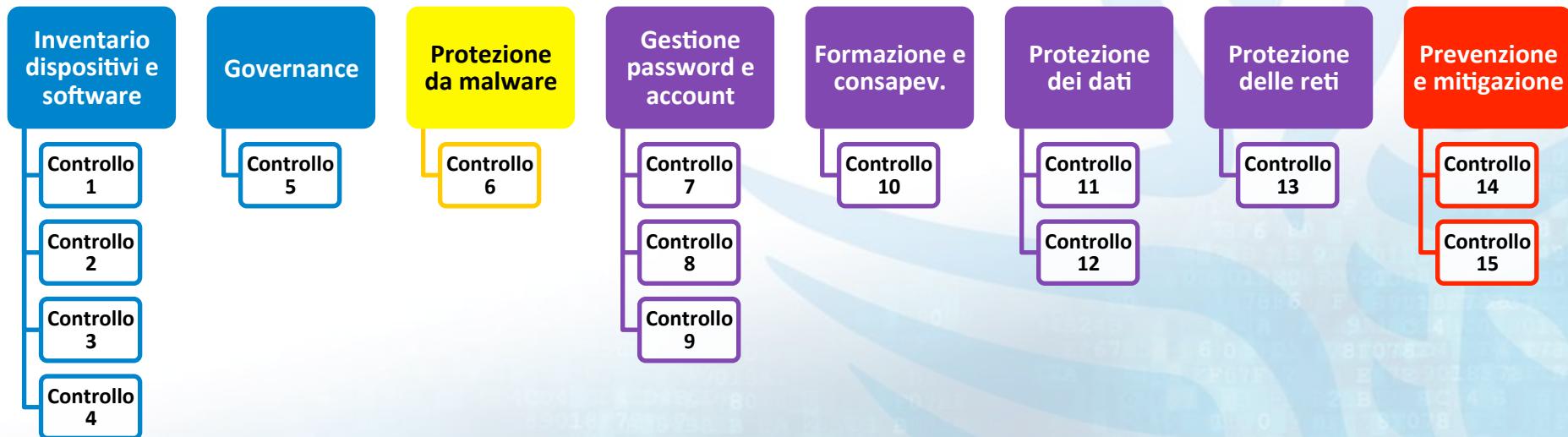
# Imprese target

Se l'organizzazione è parte del target dovrebbe implementare tutti i Controlli Essenziali di Cybersecurity

# Definizione di controllo essenziale

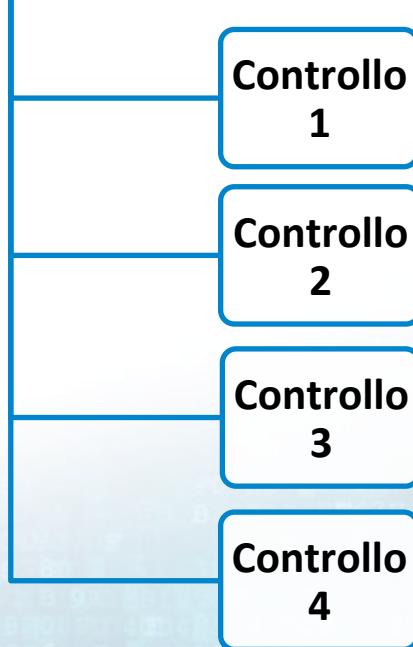
Pratica di cybersecurity che, se  
ignorata, causa un aumento  
inaccettabile del rischio

# I 15 Controlli Essenziali di Cybersecurity



# I 15 Controlli Essenziali di Cybersecurity

## Inventario dispositivi e software



Creare inventari di sistemi, dispositivi, software, servizi

Minimizzare l'esposizione sui social/servizi da terzi

Creare inventari di informazioni, dati e sistemi critici

Nominare un referente per la cybersecurity

# I 15 Controlli Essenziali di Cybersecurity

## Governance

### Controllo 5

Identificare e rispettare le leggi e i regolamenti relativi alla cybersecurity

# I 15 Controlli Essenziali di Cybersecurity

## Protezione da Malware

### Controllo 6

Utilizzare e mantenere aggiornato software antimalware su tutti i dispositivi che lo consentono

# I 15 Controlli Essenziali di Cybersecurity

## Gestione password e account

### Controllo 7

Utilizzare password lunghe e diverse per ogni account, dismissione vecchi account, autenticazione forte

### Controllo 8

Effettuare l'accesso ai sistemi usando utenze personali, non condivise con altri

### Controllo 9

Applicare il principio del privilegio minimo di accesso alle risorse

# I 15 Controlli Essenziali di Cybersecurity

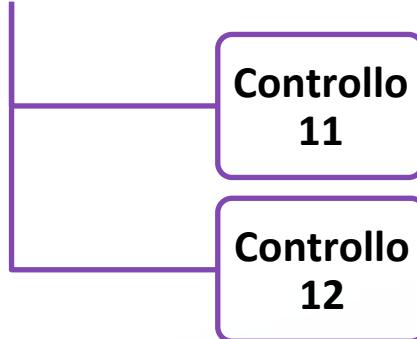
Formazione e consapevolezza

Controllo  
**10**

Eseguire adeguata formazione per tutto il personale, coordinata dai vertici aziendali

# I 15 Controlli Essenziali di Cybersecurity

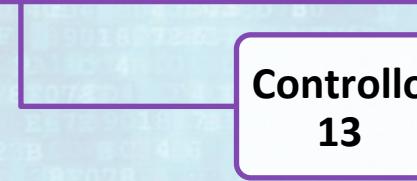
## Protezione dei dati



Effettuare la configurazione iniziale dei dispositivi  
Tramite esperti

Definire procedure di backup dei dati critici

## Protezione delle reti



Utilizzare dispositivi di protezione delle reti

# I 15 Controlli Essenziali di Cybersecurity

## Prevenzione e mitigazione

**Controllo 14**

In caso di incedente informare i responsabili. Il ripristino viene curato da personale esperto

**Controllo 15**

Eseguire gli aggiornamenti software/firmware e dismettere hardware e software non più supportato

# Conclusioni

- Migliorare la risposta di un paese a ondate di attacchi sempre piu' pervasivi prevede un piano di azione complesso su molteplici linee di indirizzo
- I controlli essenziali di sicurezza possono essere una base per una certificazione leggera rispetto alle organizzazioni per migliorare la sicurezza della supply chain di grandi aziende

# GRAZIE



[www.cybersecurityframework.it/csr2016](http://www.cybersecurityframework.it/csr2016)



@CIS\_Sapienza  
@CyberSecNatLab