by Isdi a year ago

Wannageddon

Il messaggio di richiesta di riscatto comparso sugli schermi dei computer infettati

pic.twitter.com/BJuMkHWFcZ

IRIS ROSSI @IRISROSSI · A YEAR AGO

Il 12 maggio 2017 il malware WannaCry, chiamato anche WanaCrypt0r 2.0 è stato responsabile di un'epidemia su larga scala che ha infettato i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo, tra cui Portugal Telecom, Deutsche Bahn, FedEx, Telefónica, Tuenti, Renault, il National Health Service, il Ministero dell'interno russo, l'Università degli Studi di Milano- Bicocca.
Si è trattato di un Worm, di tipologia Ransomware che in esecuzione cripta i file presenti sul computer e chiede un riscatto di alcune centinaia di dollari per decriptarli.

Attacco hacker mondiale: virus "Wannacry" chiede il riscatto, ospedali britannici in tilt. "Usato codice Nsa"

Un "ransomware" lanciato su centomila sistemi in 105 Paesi. Chiede soldi in Bitcoin, incognita l'origine. Pagamenti in corso, rischio truffa.

REPUBBLICA.IT

“WANNACRY, ovvero "voglio piangere". Computer inchiodati ovunque, dalle strutture sanitarie pubbliche inglesi ai computer di FedEx, fino ai server della telco spagnola Telefonica, con una schermata che dice "i tuoi dati saranno perduti per sempre se non paghi un riscatto di 300 dollari".

Un attacco "di proporzioni mai viste", segnalano alcuni esperti di sicurezza su Twitter: si tratterebbe di decine di migliaia di attacchi contemporanei, numero in continua crescita. Il "malware" non ha ancora un'origine nota. Ma secondo alcune ricostruzioni, per lanciarlo sarebbe stato usato EternalBlue, una cyber arma dell'Nsa che è stata trafugata dal gruppo hacker Shadow Brokers.”

di TIZIANO TONIUTTI 12 maggio 2017 Repubblica

Una delle prime fonti a darne notizia è stata la BBC

Massive ransomware infection hits computers in 99 countries

The malware is thought to have been created with tools stolen from the US National Security Agency.

BBC NEWS

Theresa May afferma che i dati dei pazienti non sono stati compromessi

Theresa May: Patients records 'not compromised' in WannaCry cyber attack

Theresa May said the British Government is not aware of any evidence that patient records have been compromised in the massive cyber attack on the NHS.

BREAKINGNEWS.IE

Pirateria informatica: in corso attacco in mezzo mondo. Colpita anche l'Italia

Il ransomware minaccia di rendere inaccessibili i file sul computer. Attaccate centinaia di organizzazioni e aziende, dal Servizio Sanitario Nazionale inglese alla compagnia spagnola Telefonica, fino al governo russo. Gli hacker hanno chiesto un riscatto in Bitcoin

BRUNO RUFFILLI

La mappa delle infezioni

pic.twitter.com/GYloAweGoZ

IRIS ROSSI @IRISROSSI · A YEAR AGO

COME E' AVVENUTO?

"Esistono tante varietà di ransowmare, tante famiglie diverse, più o meno efficaci.Quella responsabile dell'esplosione di ieri si chiama «WannaCry»: esisteva da marzo, e a dire il vero non sembrava fare molti danni. Ciò che l'ha «armata», trasformandola nel panzer dei ransomware, è stato un codice di attacco,battezzato Eternalblue, che era originariamente usato dall'Agenzia nazionale per la sicurezza Usa, la Nsa".

"L' exploit sfruttava una vulnerabilità di un software di Microsoft. Sconosciuta ai più, almeno fino a quando, alcune settimane fa, non è stata messa online, a disposizione di chiunque, da un misterioso gruppo di hacker di nome Shadow Brokers. I quali hanno in qualche modo

sottratto una serie di strumenti e di «armi digitali» all'agenzia Usa; e a cominciare dalla scorsa estate hanno iniziato a buttarli online. Dunque, succede che Shadow Brokers si impossessa dell'attacco informatico della Nsa. Lo rilascia online. Qualcuno lo prende, lo usa per potenziare un ransomware mediocre, e inizia una campagna globale e massiva di infezioni. Che propagandosi velocemente dentro le organizzazioni colpite le mette in ginocchio".

da Carola Frediani - su La Stampa - Pubblicato il 13/05/2017 Ultima modifica il 13/05/2017 alleore 07:03

Quel virus diventato letale grazie ai codici della Nsa

WannaCry attivato da strumenti digitali una volta usati dagli 007 Usa. I cybercriminali hanno sfruttato la falla di un software Microsoft

S CAROLA FREDIANI

"L'azienda di Redmond [Microsoft ndr] si è trovata in prima linea nell'emergenza Wannacry, e ha deciso di fornire un aggiornamento per chiuderela falla sfruttata dal malware anche a sistemi Windows non più supportati da anni, come Windows XP.
Ma a distanza di due giorni dall'esplosione di questo ransomware, se n'è uscita anche con una forte dichiarazione politica. "Questo attacco offre ancora un altro esempio del perché sia un problema il fatto che i governi ammassino vulnerabilità", ha commentato sul suo blog il presidente di Microsoft Brad Smith. "È un trend emergente nel 2017. Abbiamo visto le vulnerabilità conservate dalla CIA pubblicate da Wikileaks, e ora questa rubata alla NSA che ha colpito clienti in tutto il mondo (...) Questo attacco rappresenta un collegamento non voluto ma sconcertante tra le due più serie minacce alla cybersicurezza del mondo oggi - azioni di Stati e azioni di organizzazioni criminali".

da Carola Frediani - La Stampa - Pubblicato il 15/05/2015

Quattro cose da sapere ancora su Wannacry

Microsoft accusa i governi; sbuca un secondo interruttore; e le ultime raccomandazioni dall'Europa. Il punto sul virus che imperversa da venerdì

S CAROLA FREDIANI

Ecco puntata di Report sull'argomento

Report - Sorvegliati speciali - 22/05/2017 - video - RaiPlay

Rai RAI · 3 YEARS AGO

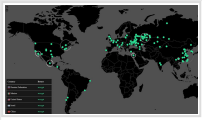
Il legame con l' NSA

pic.twitter.com/t24RLM20n0

IRIS ROSSI @IRISROSSI · A YEAR AGO

Edward Snowden, l'ex tecnico che denunciò un programma di sorveglianza segreto della Nsa, ha puntato il dito contro l'agenzia Usa: «Se la Nsa avesse svelato il difetto sfruttato per attaccare gli ospedali quando lo ha trovato e non quando lo ha perso», ha twittato, «questo poteva essere evitato».

Bruno Ruffili - La StampaPubblicato il 12/05/2017
Ultima modifica il 13/05/2017 alle ore 10:32

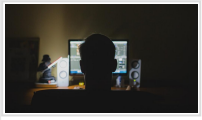


Pirateria informatica: in corso attacco in mezzo mondo. Colpita anche l'Italia

Il ransomware minaccia di rendere inaccessibili i file sul computer. Attaccate centinaia di organizzazioni e aziende, dal Servizio Sanitario Nazionale inglese alla compagnia spagnola Telefonica, fino al governo russo. Gli hacker hanno chiesto un riscatto in Bitcoin

BRUNO RUFFILLI

The Shadows Brokers contro the Equation Group



Shadow Brokers vendono nuovi cyberattacchi Nsa (entro luglio)

Il gruppo che ha rubato le cyberarmi americane muove i suoi soldi e mette in vendita ulteriori vulnerabilità. E c'è chi teme nuove Wannacry per quest'estate

CAROLA FREDIANI

Va anche ricordato il penultimo messaggio pubblicato da *the Shadow Brokers*, dove questi hanno rivendicato il fatto di essere stati «responsabili», per così dire, e di aver aspettato a diffondere l'exploit; hanno specificato che loro non fanno ricatti (come dire: non siamo noi ad aver fatto e diffuso Wannacry); e hanno ribadito di prendersela con avversari sul loro stesso piano. Perché – concetto ribadito in tutte le salse - «riguarda sempre The Shadow Brokers contro The Equation Group».

E i soldi?

Se le ipotesi sulla loro identità restano aleatorie, molti stanno seguendo i (pochi) soldi arrivati sull'indirizzo bitcoin diffuso da The Shadow Brokers. Per la prima volta, ieri, questi sono stati mossi: da quell'unico indirizzo i bitcoin hanno cominciato a spostarsi su più indirizzi, frammentandosi in cifre minori (qui da dove sono partiti). Potrebbe essere l'inizio di ulteriori scomposizioni (in corso mentre scriviamo) che portino poi a un mixer, un servizio di lavatrice, che serve ad offuscare la tracciabilità dei bitcoin rimescolandoli con altri. «Ci sono vari metodi di funzionamento dei mixer: alcuni consistono anche semplicemente nel depositare il tutto dentro un indirizzo, cioè, tutti gli utenti depositano dentro ad un solo indirizzo», commenta a La Stampa Franco Cimatti, presidente della Bitcoin Foundation in Italia. «Poi i bitcoin escono in quantità diverse, in tempi diversi, cosi non si sa di chi siano. Il mixing però funziona per piccole cifre, e se non sei uno ricercato dai servizi segreti».

Carola Frediani - La Stampa - Pubblicato il 30/05/2017 Ultima modifica il 30/05/2017 alle ore 15:58

Ricercatore 22enne blocca l'attacco

Wannacry, hacker blocca "per caso" l'attacco informatico mondiale

Ha registrato il dominio che i pirati informatici hanno inserito nel malware come sistema di autodistruzione, fermandone così la diffusione a macchia

REPUBBLICA.IT

"ROMA - Eroe per caso dei tempi moderni. Un ricercatore di sicurezza informatica ha accidentalmente trovato il modo di bloccare la diffusione a macchia d'olio di Wannacry: l'attacco informatico che ieri ha colpito organizzazioni e aziende di diversi paesi del mondo, compresa l'Italia. Su Twitter è conosciuto come @malwaretechblog e grazie all'aiuto di DarienHuss, un 'collega' che lavora per la compagnia di sicurezza californiana Proofpoint, ha trovato e attivato una sorta di pulsante di autodistruzione contenuto all'interno del virus".

di ROSITA RIJTANO - La Repubblica - 13 maggio 2017

Quando si diffonde la notizia del nuovo virus @malwaretechblog e grazie all'aiuto di DarienHuss, un 'collega' che lavora per la compagnia di sicurezza californiana Proofpoint, ha trovato e attivato una sorta di pulsante di autodistruzione contenuto all'interno del virus".

In un tweet commenta così l'impresa...

"Così oggi posso aggiungere 'ha accidentalmente fermato un cyberattacco mondiale' al mio curriculum", ha scritto l'hacker sulla piattaforma di Jack Dorsey.

A fine giugno si diffonde anche l'infezione Petya - not Petya

@malwaretechblog (il ricercatore 22enne) si prepara alla sua lunga notte per tentare di bloccare anche questo attacco ….ordinando la pizza…

My Cyber Attack Survival Pack has arrived Pizza guy recognized me off the news and asked if I was investingating the new attack :') pic.twitter.com/wwrjZOXtqQ

MALWARETECH @MALWARETECHBLOG · A YEAR AGO

10 cose da sapere dell'infezione NotPetya, e perché è più insidiosa di Wannacry

Come attacca e si diffonde? Che sistemi può colpire? Che differenze ci sono con Wannacry? Che fare? Ecco quello che sappiamo finora

S CAROLA FREDIANI

NotPetya, cosa significa che hanno hackerato Chernobyl

A causa del ransomware Petya è andata fuori uso una parte dei sistemi di monitoraggio delle radiazioni. I sistemi informatici vitali per la gestione dell impianto (e per prevenire fughe radioattive) sono rimasti inviolati

W GIANLUCA DOTTI

Crypto - PEC: la campagna di estorsioni tutta italiana

"Mentre nel mondo furoreggiava Wannacry - il virus del riscatto che dal 12 maggio in poi ha colpito circa trecentomila vittime in 150 Paesi - in Italia si consumava in pochi giorni una campagna di estorsioni digitali decisamente più piccola ma piuttosto interessante. Per come è nata e apparentemente morta. Perché potenzialmente molto efficace e dannosa, anche se si è poi bloccata subito. E perché potrebbe essere stata interamente messa in piedi da italiani".

"Solitamente però queste campagne sono gestite da criminali di altri Paesi anche attraverso sistemi con cui affittano l'infrastruttura ad altri e usando traduttori automatici. Col risultato che le mail-esca inviate - ma anche gli allegati e le istruzioni fornite - oltre ad avere un italiano zoppicante, presentano spesso delle incongruenze. Insomma sono poco credibili".

In questo caso invece ndr...[...]«Le mail portatrici erano fatte bene, in un buon italiano», commenta a La Stampa Enrico Tonello di Tg Soft. «Quella relativa al dissesto stradale era in linea con il target di riferimento, cioè i Comuni cui era indirizzata. Che sono abbastanza abituati a ricevere simili mail».

Questo ha permesso di far cadere nella trappola molte più persone ed enti rispetto alle campagne portate avanti dall'estero - ndr -

Crypto-PEC, la prima campagna di estorsioni digitali tutta made in Italy?

Poco prima di Wannacry, veniva diffuso un virus del riscatto veicolato da mail molto credibili. Ma poi qualcosa è andato storto

CAROLA FREDIANI

Crypto-PEC, la prima campagna di estorsioni digitali tutta made in Italy - Carola Frediani - Pubblicato il 18/05/2017 - Ultima modifica il 18/05/2017 alle ore 12:43 (sotto il link)

Il sistema di protezione in Italia

Il nostro sistema di protezione è partito solo tre anni fa, in ritardo rispetto all'Europa....

La barriere fragili dell'Italia anti hacker

Pochi uomini e disarmati contro la minaccia delle cyber incursioni: il nostro sistema di protezione è parito solo tre anni fa, in ritardo rispetto all'Europa, ma il governo dopo il varo si è dimenticato di finanziarlo. Così siamo ancora all'anno zero e le gelosie tra militari e civili vanificano il coordinamento.

DI GIANLUCA DI FEO

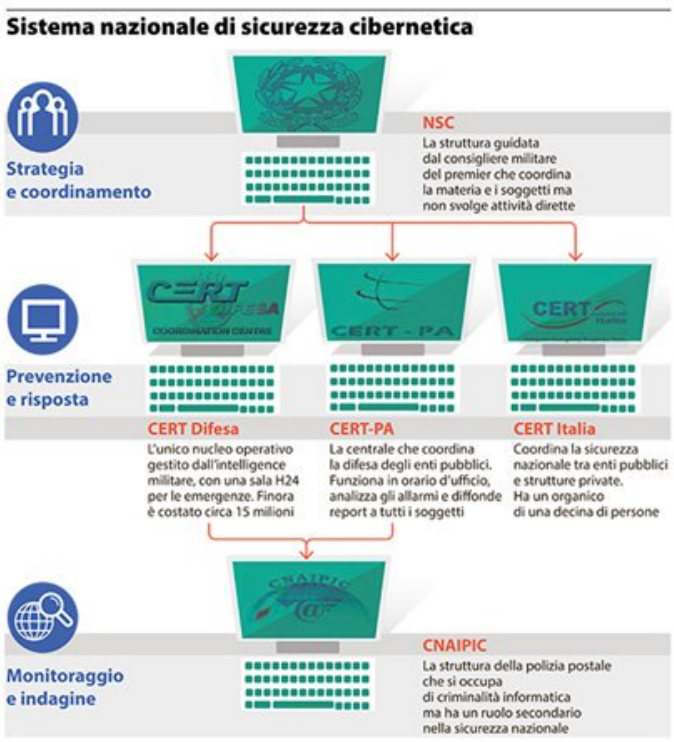
"Le tre fortezze che hanno il compito di proteggere l'Italia dalle grandi incursioni digitali […] si chiamano Cert, Computer emergency response team: sono le centrali operative incaricate di scoprire gli assalti e sincronizzare la risposta. La più importante, un po' enfaticamente battezzata 'Cert Italia', dovrebbe coordinare tutte le realtà pubbliche e private in un unico scudo online ma ha un organico di "una decina di persone". Il 'Cert Pubblica Amministrazione' invece è la barriera degli enti statali o locali che però funziona "in orario d'ufficio, anche se pure il sabato o la domenica si trova qualcuno che rispondeal telefono" […]
Infine c'è il Cert Difesa, il più dotato e reattivo seppur costruito con un investimento complessivo di 15-20 milioni […]

di GIANLUCA DI FEO - 16 gennaio 2017 - Le Inchieste di Repubblica e l'Espresso

News - Agid CERT-PA

Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate per contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

CERT-PA



pic.twitter.com/3UAaf1D6Lb

IRIS ROSSI @IRISROSSI · A YEAR AGO

Diritti civili

Quando l'hacker è lo Stato

Gli strumenti, i metodi e le regole (che non ci sono): come funziona la "pirateria" di governo?

ANDREA DANIELE SIGNORELLI

"A suscitare i timori maggiori tra i sostenitori dei diritti civili, però, è il rischio che le forze dell'ordine eccedano nella sorveglianza nei confronti dei loro stessi cittadini, utilizzando strumenti come l'IMSICatcher, un "acchiappa-sim" che consente di localizzare e pedinare i telefonini presi di mira e di ottenere i preziosi metadata, senza bisogno di intervenire direttamente sul dispositivo oggetto della sorveglianza. Apparecchio sempre più utilizzato dall'intelligence, pone però numerose questioni in termini di privacy, trattandosi di uno strumento di sorveglianza elettronica "a strascico"(che si può acquistare sul web) che acquisisce informazioni sensibili in maniera indiscriminata. I modelli più evoluti di IMSI Catcher, peraltro, consentono di intercettare le comunicazioni, leggere gli SMS e – almeno stando a quanto si sente nel documentario Spy Merchants di Al Jazeera UK – anche di inviare SMS o email fingendo di essere un contatto presente nella rubrica del telefono preso di mira".

Andrea Daniele Signorelli 12.06.2017 | - Le Macchine Volanti

Il mercato dei dati personali alimentato dai virus del riscatto

Gli hacker raccolgono centinaia di migliaia di informazionisu pazienti e interventi chirurgici e minacciano di divulgarli

CAROLA FREDIANI

"In questo campo, il rischio informatico più urgente e concreto resta quello dei ransomware, i virus del riscatto. Costituiscono infatti la minaccia principale per i dati sanitari, secondo un recente rapporto del colosso tecnologico Ntt."
[…]"Più in generale, per chi fa attacchi ed estorsioni, le strutture sanitarie sono prede ghiotte essenzialmente per tre ragioni: spesso i sistemi informatici non sono all'altezza; il loro funzionamento non tollera interruzioni; i dati conservati sono molto sensibili."

Carola Frediani
Pubblicato il 30/06/2017
Ultima modifica il 08/07/2017 alle ore 02:31

I cyberattacchi nella Sanità: costi elevati e poca sicurezza

Uno studio dimostra che ogni italiano paga 134 euro per i danniNelle Asl e negli ospedali mancano tecnici per proteggere i dati

PAOLO RUSSO

"Il nuovo regolamento europeo sulla privacy che entrerà in vigore a maggio del prossimo anno darà una mano, prevedendo la figura di un responsabile protezione dati."

Paolo Russo La stampa
Pubblicato il 30/06/2017
Ultima modifica il 08/07/2017 alle ore 02:31

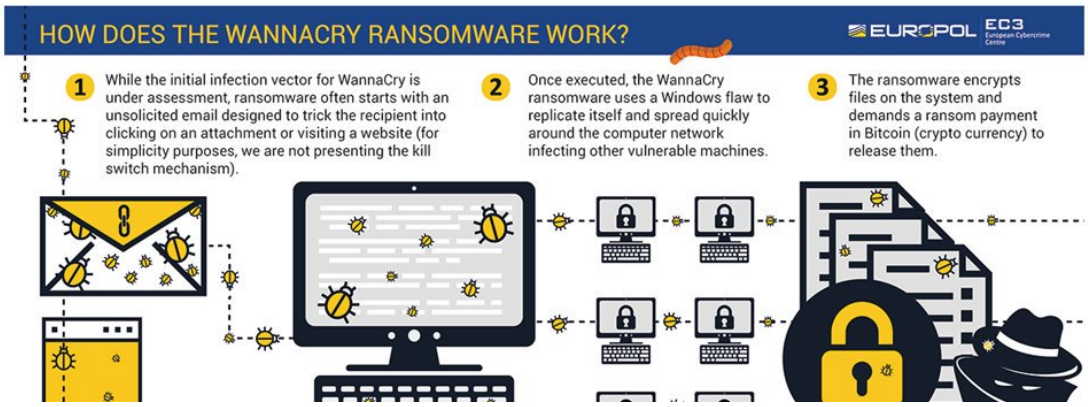
pic.twitter.com/LCwso64J8b

IRIS ROSSI @IRISROSSI · A YEAR AGO

Intanto nuovi attacchi si profilano all'orizzonte ...e Europol pubblica il vademecum e una campagna ad hoc

Wannacry Ransomware

EUROPOL



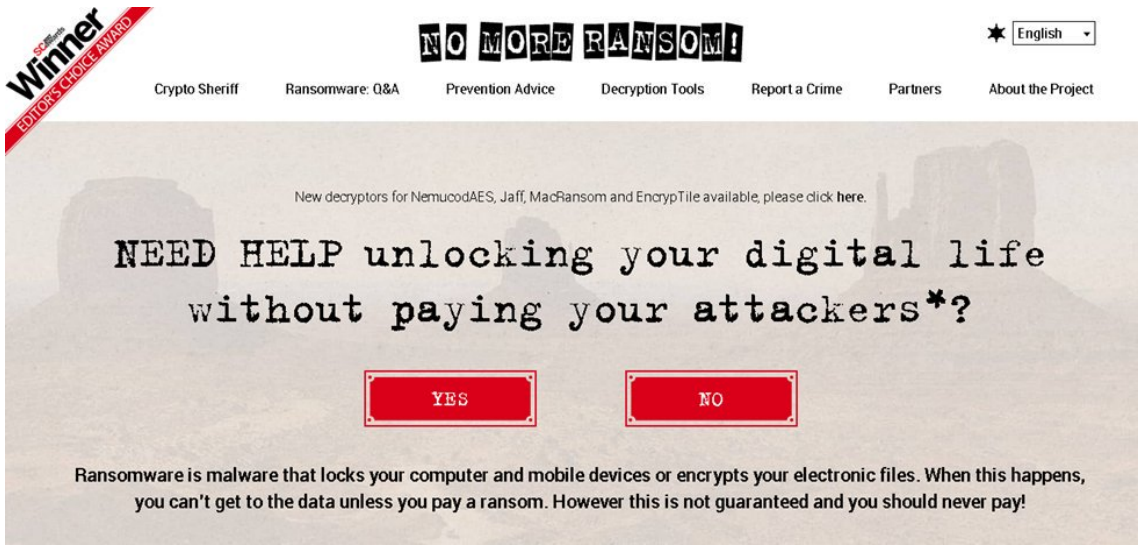
pic.twitter.com/MNfVsY8mQp

IRIS ROSSI @IRISROSSI · A YEAR AGO

The No More Ransom Project

Good news

NOMORERANSOM



pic.twitter.com/sgfUmLKZe8

IRIS ROSSI @IRISROSSI · A YEAR AGO

Diritti civili, diritti digitali - Omaggio a Stefano Rodotà

Stefano Rodotà: Soro (garante privacy), "l'Italia deve a lui quasi tutto del diritto fondamentale alla protezione dei dati personali" | AgenSIR

"La morte di Stefano Rodotà - proprio nel ventennale della legge sulla privacy da lui fortemente voluta - è una perdita incolmabile, in particolare per l'Autorità che egli per primo ha presieduto e per la quale continua a rappresentare un punto di riferimento insostituibile".

SIR AGENSIR - SERVIZIO INFORMAZIONE RELIGIOSA