Rassegna stampa

Centro Studi C.N.I. 23 ottobre 2016

Waypress
media monitoring

RISCHIO SISMICO E IDROGEOLOGICO

SISMA AMATRICE

SICUREZZA INFORMATICA

LA NOVITÀ IN 875 COMUNI

Ora l'allarme terremoto arriva via app

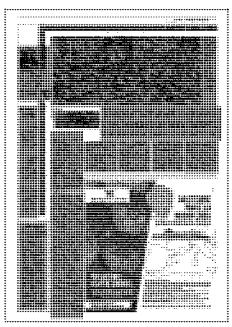
DAVIDE LESSI

Per dirla come Massimo Lopez «una telefonata allunga la vita». E l'idea ricorda proprio lo spot degli Anni 90. Se non fosse che in Italia, dove per Legambiente l'86% dei Comuni è a rischio idrogeologico, di vite se ne potrebbero salvare davvero.

CONTINUA A PAGINA 11


LA STAMPA

La nuova Agenzia delle entrate sconti su cartelle, tasse e multe



L'ITALIA CHE CAMBIA / 2

L'app per terremoti e alluvioni Così i sindaci daranno l'allerta

Inventata da una giovane imprenditrice, è già attiva in 875 Comuni

La storia

DAVIDE LESSI
TORINO

SEGUE DALLA PRIMA PAGINA

Magari anche grazie a questa applicazione. Si chiama «Sindaci in contatto» ed è un sistema di allerta che permette ai primi cittadini di informare in tempo reale la propria comunità sulle eventuali emergenze. «Avevo 19 anni quando ho pensato a un modo per permettere ai sindaci di comunicare attraverso telefonate automatiche», racconta l'estrosa imprenditrice campana Valentina Flaminio. Oggi, 15 anni e tanta tecnologia dopo, l'idea è diventata una app per smartphone che viene promossa dall'Associazione nazionale Comuni italiani (Anci), attraverso la società privata Anci comunicare.

Come funziona

«Sono 2432 i sindaci che ci hanno contattato per chiedere informazioni. Di questi 875 hanno già ricevuto la prima abilitazione gratuita», fa i conti Flaminio. Funziona così: una volta scaricata l'applicazione, il primo cittadino può registrare un messaggio vocale dal suo telefono. Poi schiacciando il pulsante per l'invio immediato parte un sistema di chiamate automatiche ai numeri fissi e mobili registrati nel suo Comune. «I cittadini - spiega la 35enne Flaminio - sentiranno così la voce del sindaco che potrebbe dare l'allerta su un'alluvione o segnalare i posti di primo soccorso in una zona terremotata». Il sistema è possibile grazie all'accesso al database unico delle comunicazioni, in cui tutti i gestori telefonici depositano le utenze registrate che sono a disposizione di enti pubblici e protezione civile.

Il mancato allarme

«Se 20 anni fa ci fosse stata una tecnologia del genere forse sarebbe andata diversamente», dice il sindaco di Sarno Giuseppe Canfora. Ha ancora nella mente le immagini dell'alluvione che colpì la sua comunità nel 1998. Per quella frana che uccise 137 persone la Cassazione ha bollato come «negligente» la condotta dell'allora primo cittadino Gerardo Basile, condannandolo per non aver ordinato l'evacuazione della popolazione nella notte tra il 4 e il 5 maggio. Ma gli esempi, anche più recenti, non mancano: è il caso, tra gli altri, dell'ex sindaco di Olbia, Gianni Giovannelli, ancora sotto processo per «mancata attivazione delle procedure di allarme» nell'alluvione che sconvolse l'isola il 18 novembre 2013 provocando 13 vittime solo nella regione della Gallura.

«Proprio partendo dall'esperienza della Sardegna abbiamo deciso di sviluppare questa app», spiega Valentino Flamino, titolare di Enterprise Contact, azienda basata a Napoli. E spiega: «Allora avevamo solo una piattaforma chiamata PowerTalk ma a Olbia non poté essere utilizzata perché l'accesso a internet da rete fissa era precluso». Adesso, invece, viaggiando anche sulle reti della telefonia mobile il problema dovrebbe essere evitato. Ma c'è di più: l'app propone anche la possibilità di inviare delle notifiche sui principali social network (Facebook e Twitter) agli utenti che si sono geolocalizzati, cioè registrati in un determinata posizione».

«Nei momenti di panico c'è l'esigenza di raggiungere tutti i cittadini in tempi molto rapidi», spiega il sindaco di Chiavenna Luca Della Bitta. Lui, che è anche presidente della commissione Innovazione dell'Anci, ha avuto modo di conoscere l'app all'ultima assemblea nazionale. «È uno strumento importante che può aiutare a creare un clima di maggior dialogo tra le amministrazioni, sempre più digitali, e i cittadini, anche in situazioni di emergenza», conclude Della Bitta.

La mia idea? Creare un modo semplice per far comunicare gli enti pubblici con la cittadinanza

Valentina Flaminio
Titolare dell'azienda Enterprise Contact

Ad Amatrice
Una piattaforma per i soccorsi

«Durante il terremoto ad Amatrice i volontari della Protezione civile hanno usato la nostra app per coordinare la distribuzione delle merci per i primi soccorsi». Valter Basinelli parte da un episodio per raccontare l'app sviluppata da VJ Technology. Si chiama WhereApp e permette di ricevere, con un messaggio simile a un sms, tutti gli aggiornamenti su un fatto, inviati dagli enti di soccorso che si sono registrati al servizio, come la Croce Rossa e la Protezione civile. «Non solo: anche il cittadino può segnalare un'emergenza fino a un chilometro di distanza», conclude Basinelli. [D. L.]

Un Paese sempre a rischio

86
per cento
Le aree interessate dal dissesto idrogeologico coprono 6663 dei 7720 Comuni italiani (l'86%)

156
per cento
L'aumento del consumo di suolo dal '56. La popolazione è cresciuta "solo"del 24%

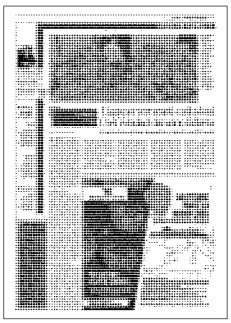
499.511
frane
Sono quelle censite nel nostro Paese: è un'area pari al 7% del territorio nazionale

Tra i detriti
Gli effetti dell'alluvione del 18 novembre 2013 in un negozio di Olbia, in Sardegna Per «mancato allarme» è ancora imputato l'ex sindaco Gianni Giovannelli Anche a partire da questa esperienza è nata l'idea della app "Sindaci in contatto"

Ad Amatrice

Una piattaforma per i soccorsi

«Durante il terremoto ad Amatrice i volontari della Protezione civile hanno usato la nostra app per coordinare la distribuzione delle merci per i primi soccorsi». Valter Basinelli parte da un episodio per raccontare l'app sviluppata da VJ Technology. Si chiama WhereApp e permette di ricevere, con un messaggio simile a un sms, tutti gli aggiornamenti su un fatto, inviati dagli enti di soccorso che si sono registrati al servizio, come la Croce Rossa e la Protezione civile. «Non solo: anche il cittadino può segnalare un'emergenza fino a un chilometro di distanza», conclude Basinelli. [D. L.]



LA STAMPA

CHI SONO I PIRATI DELLA CYBERGUERRA

GIANNI RIOTTA

Una mamma sistema il monitor per controllare la nanna del bambino, un ragazzo accende il videoregistratore, un signore monta immagini alla videocamera. Intenti alla vita quotidiana digitale, sono ignari che i loro gadget sono infiltrati da pirati, e pian pian collegati in un «botnet», rete di terminali «schiavi» di un «botmaster». Quando il botmaster ritiene di avere un esercito di robot con sufficiente potenza lancia l'attacco, magari via il sistema di malware Mirai, da poco reso pubblico da un sito hacker https://goo.gl/Ub7CkL . I lillipuziani web, uniti, paralizzano il Domain-Name System, Dns, le reti gigantesche che regolano l'accesso ai siti, in un blitz chiamato in cybersecurity «Denial of service», rifiuto di servizio, Ddos. Quando vi collegate a un sito, www.lastampa.it , www.riotta.it i server traducono la richiesta in cifre, indirizzo Ip, per smistarla. Venerdì la rete, compresi giornali e social media, è stata paralizzata da un raid Ddos, grazie a «internet delle cose», gli elettrodomestici collegati al web, senza parole chiave o sicurezza alcuna. I pirati li hanno infiltrati sereni, prima vittima Dyn, compagnia che provvede accesso a siti sulla costa atlantica. «Il web non funziona e il tostapane è in ostaggio» scherza Matt Tait, influente esperto di sicurezza che twitta da @pwnallthethings e Jeff Jarmoc rincara «Siamo passati dalla rete che doveva resistere a un attacco atomico, alla rete vittima del tostapane».

Quando il Pentagono, nel 1969, realizzò Arpanet, prototipo del web, voleva infatti creare una trincea elettronica segreta capace di sopravvivere alla guerra termonucleare con l'Urss. Oggi un paio di ragazzi e un buon sistema di computer e molta malizia possono passarvi da casa, allineare un paio di chip e partecipare alla paralisi del mondo contemporaneo.

Chi c'era dietro l'assedio di venerdì? L'attacco è legato all'irruzione nei computer della portaerei Usa che incrociava nei mari rivendicati dalla Cina? L'arresto, in quelle ore, dell'hacker russo Yevgeniy Aleksandrovich Nikulin a Praga (gli americani lo incriminano come pirata e rischia 30 anni di carcere, i russi ne chiedono la liberazione immediata) è un caso?

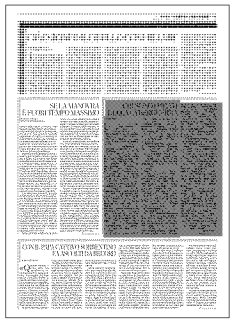
Dopo che Hillary Clinton ha indicato senza reticenze il presidente russo Vladimir Putin come fonte delle rivelazioni Wikileaks, molti sospettano della rete legata a Julian Assange, accusato in patria di stupro e rifugiato all'ambasciata dell'Ecuador a Londra. Gli attacchi di Assange al partito democratico, e la convergenza tra Wikileaks e Cremlino pro Donald Trump aumentano gli indizi e, poche ore dopo il Ddos, Wikileaks rivendica via twitter: «Il signor Assange è vivo e Wikileaks attiva. Chiediamo ai nostri amici di non bloccare più il web Usa. Abbiamo fatto vedere chi siamo».

Non tutti abboccano alla provocazione. Henry Farrell, docente alla George Washington University, osserva: «Dietro il raid possono non esserci Stati, governi, Wikileaks, perché la rivelazione del protocollo Mirai permette a tantissimi un'operazione analoga». Potrebbero essere dilettanti, quelli che cinema e giornali immaginano come studenti fuoricorso con la felpa alzata, chiusi in un garage. Forse. Ma, come dimostrano Wikileaks e la reazione dell'Ecuador che, dopo anni di sostegno, ha chiuso l'accesso al web al rifugiato Assange per le troppe scorribande contro Clinton, nel buio della rete Deep, segreta, non ci sono confini. Il teenager brufoloso di oggi è l'hacker pagato di domani, dopodomani al soldo di una spia che lo usa, ma non lo incontrerà mai.

Bruce Schneier, informatico che lavora sulla sicurezza strategica, parla di «probing», sondaggi: «Cina e Russia conoscono bene la debolezza della rete, la si può infiltrare con facilità con un Ddos, e allora lanciano assaggi, affondi, per capire fino a che punto spingersi». Per esempio, la scorsa estate, il blogger Bruce Krebs ha visto il suo sito alluvionato da un Ddos tragico, in protesta contro qualcosa che aveva scritto. Tali sono stati i danni che Akamai, che ospitava il blog di Krebs, l'ha buttato fuori senza complimenti. Ecco la nuova censura, di Stato, di business, di pirati, basta colpire un sito sgradito con un Ddos e lo si lascia orfano, senza che nessuno voglia rilanciarlo online.

A Mosca Putin se la ride, e a chi gli chiede se è lui a scatenare la cyberguerra obietta «Vi interrogate su chi c'è dietro, e non guardate le manipolazioni alla democrazia che rivela», le malefatte di Hillary Clinton. Per capire dunque chi siano i pirati di venerdì, rivoltate il ragionamento di Putin: non cercate «la mano», partite dal tostapane di casa, dal pirata da cantina che lo invade, passate ai centri strategici che ne raccolgono i dati, via leaks, e infine ragionate sull'apparato strategico e militare che li usa. La Seconda Guerra Fredda si combatterà così, in questa trincea digitale.

Facebook riotta.it



«Spiare WhatsApp e Telegram è un gioco da ragazzi»

Una società milanese trova e denuncia una falla nel sistema: abbiamo assistito alla prova

di **Gianfranco Giardina**

L'annuncio è tale da far tremare i polsi: violare un account WhatsApp o Telegram sarebbe un gioco da ragazzi. La vulnerabilità, portata alla luce da InTheCyber, società milanese specializzata nella sicurezza offensiva e difensiva informatica, si concretizza grazie alla facilità di accesso indebito delle segreterie telefoniche di alcuni gestori e alle procedure di autenticazione dei sistemi di messaggistica, incautamente basati su messaggi telefonici vocali. La semplice procedura necessaria per la violazione è stata mostrata in anteprima al *Corriere della Sera* e verrà presentata domani, durante la settima Conferenza sulla Cyber Warfare a Milano.

Si tratta di una falla di sicurezza importante (secondo i tecnici di InTheCyber riguarderebbe a diverso titolo circa 32 milioni di Sim italiane), anche in considerazione del fatto che per sfruttarla non serve alcun basista all'interno delle telco (gli operatori di telecomunicazione), nessuna apparecchiatura sofisticata e bastano competenze tecniche minime.

Malintenzionati o anche solo curiosi possono di fatto avere libero accesso al testo integrale delle chat di Telegram o ai gruppi di WhastApp, conoscendo solo il numero di telefono della vittima e niente più. Il problema, secondo i tecnici di InTheCyber, al momento è fortemente sottovalutato: «WhatsApp, da noi informata della vulnerabilità, si è detta semplicemente "non interessata al problema" perché, secondo la società, la responsabilità sarebbe delle telco. Telegram invece non ha risposto alla nostra segnalazione, come anche i gestori telefonici che abbiamo contattato». Una situazione che contrasta con la scritta che campeggia sul sito di WhatsApp: «La privacy e la sicurezza sono nel nostro Dna».

«Questa vulnerabilità può essere chiusa facilmente con la collaborazione delle telco e dei fornitori di servizi — ci spiega Paolo Lezzi, Ceo e fondatore di InTheCyber — ma è solo la dimostrazione dello stato non ottimale in cui versa la sicurezza dei sistemi informatici e digitali». La diffusione sempre più capillare dell'Internet degli Oggetti e della iper-connessione richiede una maggiore consapevolezza da parte degli utenti «ma soprattutto ci vorrebbero — prosegue Lezzi — obblighi e responsabilità chiare per chi progetta e gestisce i prodotti e i servizi connessi, sia a livello pubblico che privato».

Spesso si pensa che gli effetti di un attacco restino confinati alla sfera digitale e che possano comportare, come massimo rischio, la cancellazione dei dati; ma le conseguenze di un atteggiamento disattento sul fronte della cyber sicurezza possono finire per riguardare anche la sfera fisica. «Una vulnerabilità banale come questa da noi dimostrata può mettere a repentaglio la sicurezza delle persone, a cascata anche quella dell'ente o azienda per cui lavorano e, in caso di utilizzi estremamente malevoli, del Paese intero».

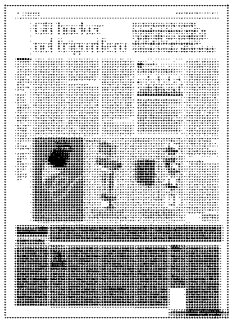
La notizia arriva nel giorno in cui il ministro dell'Interno Alfano ha comunicato che dall'inizio dell'anno sono stati censiti 626 cyber attacchi alle strutture critiche italiane. Qualcosa di più di un campanello di allarme.

32 milioni di Sim
La falla di sicurezza riguarderebbe a diverso titolo circa 32 milioni di Sim italiane

Il test

● Domani alla conferenza sulla Cyber Warfare a Milano la prova pubblica sulla vulnerabilità delle app di messaggistica istantanea condotta dalla società InTheCyber (sopra l'ad Paolo Lezzi)

> Questa vulnerabilità può essere chiusa facilmente se le aziende collaborano
>
> **Paolo Lezzi**
> Ad InTheCyber



CORRIERE DELLA SERA

Gli hacker nel frigorifero

Il cyber attacco che venerdì ha paralizzato Internet negli Usa è partito dalle case «intelligenti» dei cittadini (a loro insaputa) Wikileaks rivendica, allarme globale

L'attacco è arrivato da videoregistratori, frigoriferi, telecamere di sicurezza, router e sistemi per il controllo dei neonati. Quella che sembra la trama di un film di fantascienza, neanche dei più raffinati, è invece il racconto degli esperti sull'attacco informatico che ha bloccato il Web americano per tutta la giornata di venerdì. Un cyber-attacco che bloccando i server della Dyn, azienda del New Hampshire che svolge il compito di indirizzare il traffico Web, di fatto ha reso inaccessibili a milioni di utenti centinaia di siti. Da quelli di giornali come New *York Times* e *Financial Times*, a quelli di servizi a dir poco popolari: Twitter, Netflix, Spotify, AirBnb e molti altri. Alla base, come esercito, ci sarebbe l'Internet of Things, i miliardi di oggetti comuni collegati al Web.

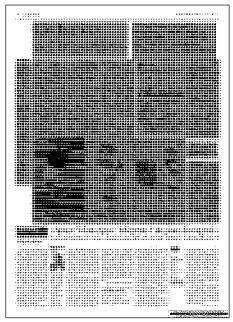
I generali che hanno condotto l'offensiva sono ancora oggetto di indagine: si parla di hacker russi o cinesi, di «vandali della Rete», ma anche di seguaci di Julian Assange, come lasciava intendere ieri un tweet di Wikileaks: «Chiediamo a tutti i sostenitori di smettere di attaccare i siti internet Usa». Una sorta di rivendicazione indiretta. In ogni caso negli Usa, alla vigilia delle elezioni, l'allarme è molto alto.

Cosa è successo

I server della Dyn gestiscono parte del «Domain Name System» della rete americana, ossia si occupano di tradurre in numeri comprensibili ai computer quegli indirizzi che digitiamo nei browser, come «Corriere.it». Dalle ore 7 del mattino locali sono iniziati i primi problemi che, in diverse ondate, hanno portato al blackout parziale della Rete americana, che da una costa si è spostato sull'altra. Secondo quanto emerso nella tarda serata di venerdì, l'attacco di tipo Ddos — Distributed Denial of Service — sarebbe partito da migliaia di oggetti «smart», che dalle case di cittadini all'oscuro hanno intasato i server dell'azienda di «false richieste» al punto di zittirli del tutto. Si tratta di oggetti sempre più diffusi — secondo gli analisti di Gartner oggi se ne contano 7 miliardi nel mondo, nel 2020 saranno quasi 30 — e rappresentano forse il più grande problema di sicurezza informatica del momento, perché vulnerabili ad attacchi esterni. Quanto successo poche ore fa negli Stati Uniti sarebbe stato causato da dispositivi resi «zombie», ovvero pilotati a distanza, da un software «cattivo» chiamato «Mirai», una sorta di virus che negli ultimi tempi avrebbe infettato centinaia di migliaia di registratori digitali, telecamere, sensori di vario genere e altri oggetti connessi ala Rete.

I sospetti

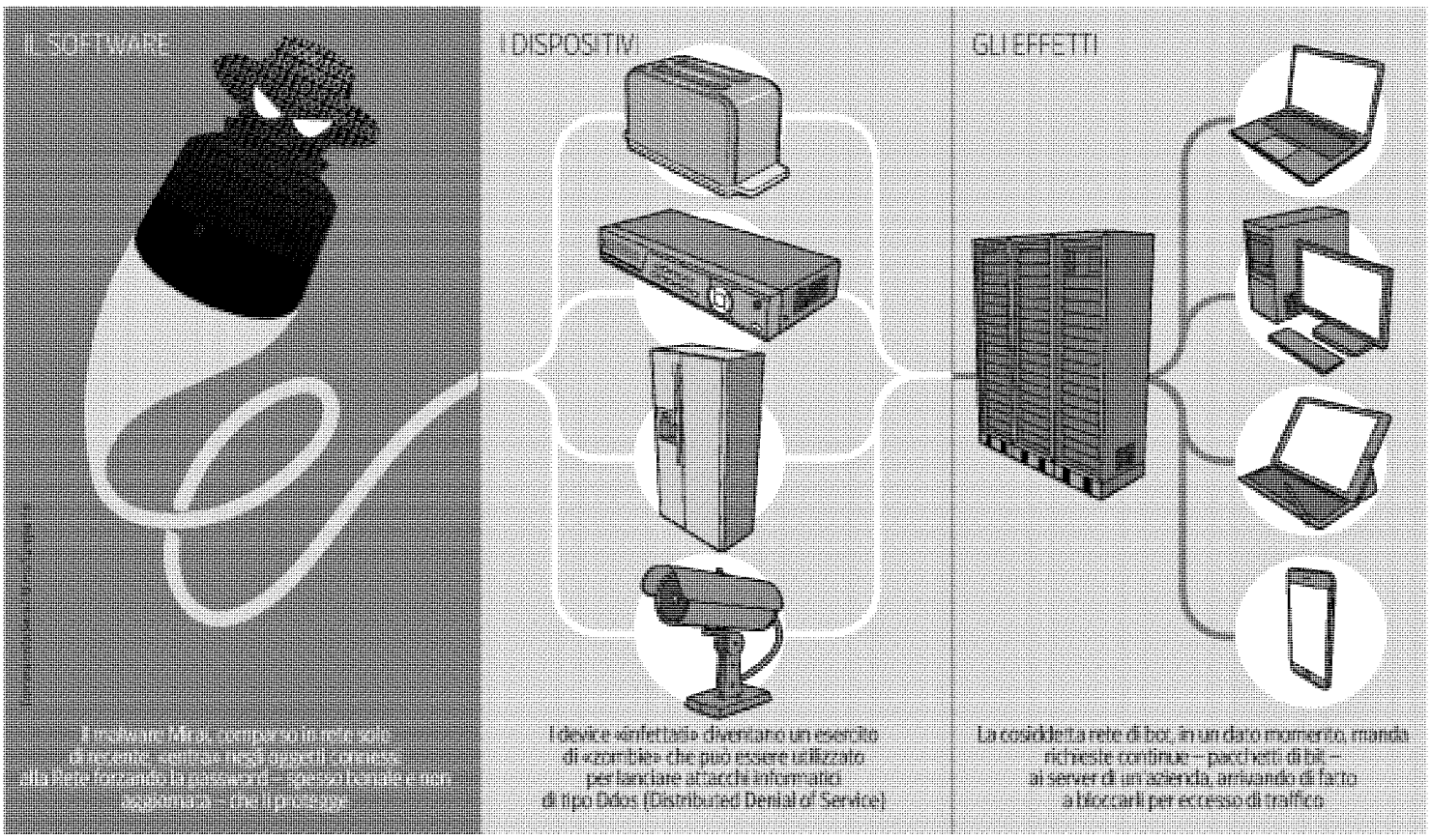
Queste tipologie di attacchi condotti attraverso «smart devices», secondo il colosso americano della Rete Verisign, sono aumentati del 75% negli ultimi mesi rispetto all'anno precedente. Diventando sempre più massici e sofisticati. Secondo il blogger Bruce Schneier, un esperto di sicurezza citato tra gli altri dal *New York Times*, sembra che dietro ci sia una specie di disegno, come se qualcuno stesse mettendo alla prova le difese delle aziende che gestiscono pezzi del traffico di Internet. Potrebbe trattarsi di Paesi «nemici» come Russia e Cina, con cui gli Usa avrebbero già da tempo ingaggiato una guerra informatica neanche troppo sotterranea — il vicepresidente Biden, a inizio mese, aveva avvertito della capacità americana di rispondere alle cyber provocazioni —, oppure di gruppi di hacker più o meno isolati. L'*Associated Press* racconta della rivendicazione via Twitter da parte di un collettivo «ombra» New World Hackers: avrebbero scatenato «zombie» capaci di generare traffico fasullo sui server della Dyn per 1,2 Terabit al secondo.



Il voto online

Se è troppo presto per poter trarre conclusioni, non lo è per preoccuparsi in vista del voto per le Presidenziali del 8 novembre. Sono infatti 31 gli Stati americani che permettono il voto online per i militari e i civili che si trovano Oltreoceano, con in più l'Alaska. Secondo l'Election Assistance Commission, un'agenzia indipendente creata nel 2002 per agevolare la partecipazione degli americani alle elezioni, un attacco Ddos potrebbe fortemente influire sul voto elettronico. Arrivando a determinare, per esempio, l'esito del ballottaggio negli «swing states», gli stati più in bilico tra Clinton e Trump.

Federico Cella
@VitaDigitale



La vicenda

● Un attacco hacker su larga scala ha colpito gli Usa venerdì bloccando centinaia di siti, compresi quelli di grandi giornali e di big della Rete

● Il tipo di attacco sferrato è il DDoS: con l'invio di una valanga di dati spazzatura, si crea un sovraccarico che impedisce agli utenti di accedere al sito

● Il bersaglio: i server della Dyn, azienda che indirizza il traffico Web. Bloccandoli gli hacker hanno reso inaccessibili centinaia di siti

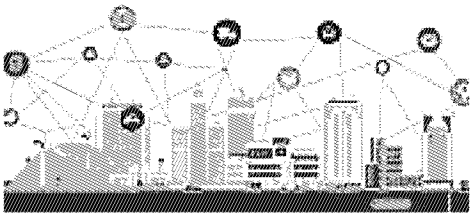
● L'attacco è partito da migliaia di oggetti «intelligenti» connessi al Web come frigo e telecamere infettati da virus

«Mirai» in azione

Il nome del virus che di recente avrebbe infettato un'infinità di oggetti connessi al Web

La parola

INTERNET OF THINGS



Questa espressione, alla lettera «Internet degli oggetti», designa l'insieme di oggetti e dispositivi connessi al Web: elettrodomestici come frigoriferi e videoregistratori, ma anche sensori per il controllo dei neonati o del fitness, radio, automobili, impianti di climatizzazione, telecamere. Insomma qualunque dispositivo elettronico equipaggiato con un software che gli permetta di scambiare dati con altri oggetti connessi. Oggetti «smart», intelligenti, ma vulnerabili ad attacchi esterni: rappresentano al momento il più grande problema di sicurezza informatica