Sicurezza. I ricercatori di Trend Micro hanno "inventato" una fabbrica del settore industria 4.0 per studiare come operano i criminali informatici. In sei mesi sono stati lanciati 39 attacchi, di cui 12 mirati

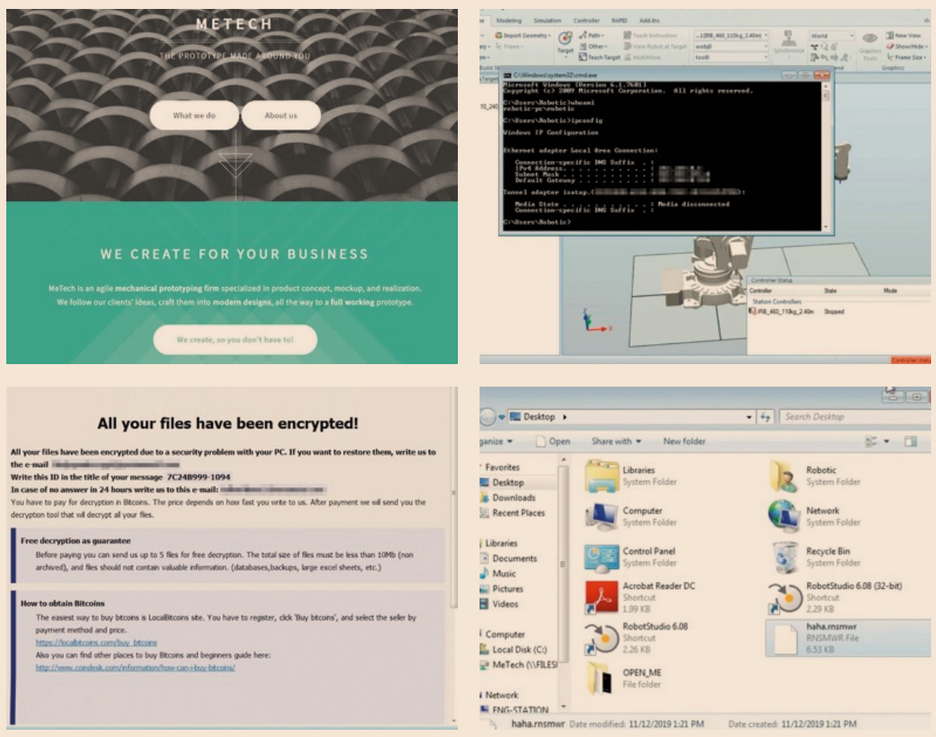
Aziende esche contro gli hacker

Luca Tremolada

Metech è una piccola azienda manifatturiera statunitense, una boutique tecnologica che progetta e produce prototipi avanzati per il settore militare, dell'automotive e aerospaziale. Pochi dipendenti (quattro) e grandi clienti. Ma la caratteristica che rende davvero unica Metech, è che non esiste. L'hanno inventata a tavolino i ricercatori dell'azienda di sicurezza informatica Trend Micro per studiare gli attacchi dei cybercriminali. In gergo viene definita "honeypot" (vaso di miele per gli orsi), è una azienda fittizia il cui scopo è quello di capire e vedere come avvengono questi attacchi "dall'interno".

«Volevamo un sistema industriale reale attrattivo - spiega al Sole 24 Ore Federico Maggi, il ricercatore Trend Micro che ha lavorato al report "Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats"- per questo non ci siamo limitati a creare il sito, ma ci siamo immaginati l'azienda intorno, appunto per aumentarne la credibilità». Dal nome dell'azienda che non doveva esistere al numero di telefono con tanto di segreteria telefonica,messaggi pre-registrati e foto con bio dei dipendenti. Nonché l'uso di veri controlli logici programmabili (PLCs), interfacce uomo-macchina (HMIs) , componenti robotici, workstation per la programmazione della produzione e file server.

La scelta come settore dell'industria 4.0 non è casuale. Le industrie manifatturiere sono in media equipaggiate con macchine vecchie di vent'anni, non possono permettersi interruzioni nella catena di montaggio e rispetto ad altri settori sono per questo più vulnerabili.



Ecco Metech. Partendo da sinistra e scendendo in senso orario: l'home page di Metech, l'azienda-esca creata da Trend Micro, le prime tracce di violazione per studiare le vulnerabilità, l'attacco ramsonware, fino al messaggio lasciato dall'hacker buono

Per essere precisi sono partiti il 6 di maggio. Un mese e mezzo dopo arriva il primo malware. Appartenente alla famiglia dei cryptominer è un software che sfrutta la potenza dei computer dell'azienda bersaglio per l'attività di "mining" cioè di creazione e validazione delle criptovalute. Per avere una indicazione di contesto il numero dei malware totali che ha colpito l'Italia nel 2019 è stato di 17.120.526, deva ai sistemi It.

«Proprio per questo - spiega - abbiamo anche finto di essere stati attaccati da qualcuno in precedenza, facendo girare alcuni nostri dati "sensibili" in determinati forum per adescare l'interesse dei criminali informatici.

L'esperimento è durato sei mesi, duranti i quali Maggi e i suoi colleghi hanno risposto alle mail e "registrato" tutto quello che accel'Italia è settima al mondo.

Dopo ogni aggressione le macchine venivano ripulite in modo da segnalare agli aggressori che c'era una forma di controllo e difesa dei sistemi It. Intorno ad agosto dopo altri malware arrivano le prime operazioni di detection, aggressori che violano i server ma non mettono in pratica azioni distruttive. Si limitano a guardare, non toccare nulla e uscire. Di solito questo tipo di azioni precedono le fasi di un attacco. Attacco che immancabilmente arriva un mese dopo, ai primi di settembre. La forma è quello del ramsonware, una azione di "sequestro" dei sistemi informativi che mette sotto scacco tutte i computer dell'azienda chiedendo in cambio il pagamento di un "pizzo" sotto forma di Bitcoin. «Rispetto ad aziende reali noi eravamo avvantaggiati - commenta il ricercatore - per ritornare in possesso dei nostri computer ci è bastato riavviare e ripulire tutto, non abbiamo perso dati e neppure soldi».

Sono seguiti altri due attacchi ramsonware. C'è stato anche, mi racconta, un hacker "buono" che è entrato e ci ha lasciato un messaggio per avvertirci sulla debolezza delle nostre difese. Solo verso la fine della breve vita di questa azienda, sono arrivati gli attacchi veri, quelli distruttivi che hanno acceso e spento la catena di montaggio e i singoli macchinari. Tirando le somme in sei mesi si sono verificati 12 attacchi mirati e 26 a basso rischio.

«Quello che abbiamo imparato - commenta - è qualcosa di più sulla psicologia dell'hacker cattivo, diciamo. Gli aggressori cercano la monetizzazione di breve periodo, diciamo. Per loro fare un attacco distruttivo vuole dire bruciare un bersaglio che genera reddito». E poi c'è un aspetto di intelligence più inquietante. Mettendo il logo di una azienda più grande e famoso, i ricercatori di Trend Micro sono stati contattati da istituzioni governative attive nella sicurezza informatica che li hanno avvertiti della loro vulnerabilità. Se il camuffamento ha funzionato con loro - chiosa Federico Maggi - vuole dire che non solo i buoni ma anche i cattivi possono essere ingannati».

© RIPRODUZIONE RISERVATA

17,1 MILIONI DI MALWARE. Il numero dei malware totali che ha colpito l'Italia nel 2019 è stato di 17.120.526, l'Italia è settima al mondo. È quanto emerge dal nuovo report di Trend Micro che verrà diffuso

OLTREFRONTIERA

INNOVAZIONE

Un miliardo di utenti Windows 10 valgono 5 miliardi di smartphone?

A cinque anni dal debutto Microsoft ha raggiunto l'obiettivo che si era prefissata: un miliardo di utenti nel mondo stanno usando Windows 10 il suo sistema operativo. Se consideriamo Windows 7, sono 1,5 gli utenti dei sistemi di Redmond. Il numero sembra alto ma è specchio dei tempi. Oggi si stima che oltre 5 miliardi di persone dispongano di dispositivi mobili e oltre la metà di queste connessioni sono smartphone. A differenza del mondo pc la crescita della tecnologia mobile fino ad oggi non è stata uguale, né tra le nazioni né all'interno degli stessi confini. Il discrimine è e resta l'acceso a internet sia via rete mobile che da rete fissa. E poi va considerato l'acceraleratore proprio del mondo delle applicazioni. In questi anni gli App store per dispositivi mobili hanno saputo generare un ecosistema per quanto caotico, coerente sotto il profilo degli incentivi. L'innovazione non si è spostata ma si è distribuita, più velocemente.

—**L.Tre.**

© RIPRODUZIONE RISERVATA

FINTECH

Amazon accelera come piattaforma per servizi finanziari

Le trattative sono già in fase avanzata e il progetto potrebbe partire a breve, già a marzo. Goldman Sachs è ormai vicina a un accordo con Amazon per offrire i propri prestiti destinati alle piccole e medie imprese, un target che al momento è fuori dalla sua portata. Il colosso di Wall Street punta quindi sempre più su Big tech - l'anno scorso ha siglato una partnership con Apple per la carta di credito della Mela - per fare breccia in Main Street, l'economia reale e aziendale. Parallelamente il supermercato online globale punta a estendere i suoi servizi in ambito finanziario, presentandosi sempre più come piattaforma di servizi di terze parti. A dir la verità la stessa Amazon ha già una divisione Lending, attiva nei prestiti alle aziende che vendono i loro prodotti sulla piattaforma, di cui ha già tutti gli elementi per determinarne l'affidabilità creditizia: a fine 2019 Amazon ha iscritto a bilancio prestiti in essere con piccole imprese per 863 milioni di dollari. Ma le partnership con il mondo bancario permetteranno di ampliare la propria presenza nel settore senza doversi adeguare alla regolamentazione connessa all'attività creditizia. Intanto in Europa Bbva starebbe pensando di sfruttare la piattaforma di Amazon come canale di distribuzione per tutti i suoi prodotti, soprattutto in ambito consumer.

—**P.Sol.**

© RIPRODUZIONE RISERVATA

I numeri. I dati di Moige, Polizia Postale, Telefono Azzurro

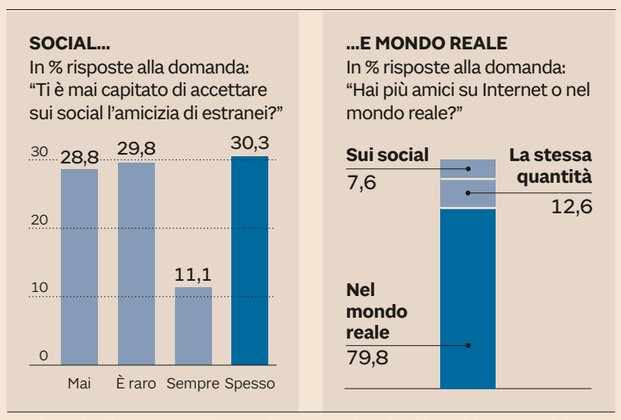
Cyberbullismo senza freni, crescono i reati verso i minori

Chiara Di Cristofaro

Se ne parla, si fa formazione nelle scuole, ma ancora non basta. Il cyberbullismo e più in generale i reati contro i minori realizzati online risultano in aumento. Ma soprattutto, le ricerche mostrano che c'è ancora un gap di conoscenze e informazioni corrette che non riguarda solo i minori. Alla vigilia della Giornata nazionale contro il bullismo e Cyberbullismo (il 7 febbraio) e del Safer Internet Day (l'11 febbraio) la Polizia Postale registra un aumento del 18% dei casi trattati che vedono vittima un minorenne (da 389 a 460 nel 2019), di cui 52 casi di bambini di età inferiore ai 9 anni. La fascia di età più "colpita" è quella 14/17 anni (309 vittime), mentre 99 vittime hanno tra 10 e 13 anni. Raddoppiano i casi di detenzione e diffusione di materiale pedopornografico. L'aumento può essere letto anche come un segnale positivo: proprio con la formazione e le campagne di sensibilizzazione le vittime sono spinte a denunciare di più. «È innegabile però la presenza di un sommerso, legato al sentimento di vergogna della vittima che vive la sua condizione come una colpa da tenere segreta», spiega Fabiola Silvestri, che dirige il compartimento della Polizia Postale di Piemonte e Valle d'Aosta. Troppo spesso i ragazzi non denunciano "perché si isolano e non sono in grado di capire che stanno subendo veri e propri reati", spiega Silvestri. «Certo – dice - il bullismo è da sempre esistito ma il cyberbullismo è più pericoloso, perché il mezzo amplifica la potenzialità offensiva della condotta. L'essere connessi 24 su 24 fa sì che non si possa mai sfuggire al proprio aguzzino».

I numeri della Polizia Postale saranno presentati oggi in un incontro a Roma che dà il via alla nuova campagna del Moige – Movimento Italiano Genitori, che coinvolgerà 250 scuole in Italia. Proprio la formazione può

Amicizie online, reali e gli estranei



Nota: il questionario è stato somministrato online ad un campione di 2.778 bambini e adolescenti di scuola elementare, media e superiore con età compresa tra i 5 e i 22 anni. Fonte: Polizia di Stato e Moige

fare la differenza, perché una cultura adeguata non è ancora stata assimilata dalle nuove generazioni. Tra i dati di un'ampia ricerca realizzata dal Moige su 2.500 bambini e ragazzi, alcuni numeri saltano all'occhio: il 71% ha accettato l'amicizia di un estraneo sui social; il 21% ha incontrato personalmente estranei conosciuti on line; il 19% ha dato il numero di telefono a un estraneo; l'8% ha scambiato foto personali con un estraneo. Comportamenti ad altissimo rischio, che non dovrebbero esistere in una generazione per la quale la distinzione tra vita reale e virtuale non ha alcun senso e in cui il tempo trascorso in rete e l'utilizzo del web in ogni ambito della propria vita implicherebbero una conoscenza del mezzo ben superiore.

E questo vale non solo per i ragazzi, ma anche per i genitori: secondo un'indagine realizzata da DoxaKids per Telefono Azzurro, più della metà dei genitori non è pienamente consapevole dei rischi e delle opportunità dei social, il 44% condivide online contenuti riguardanti i figli mentre il 30% non crede di avere sufficienti competenze su pericoli e opportunità del digitale. Ma il ruolo centrale per rompere il silenzio delle vittime, è proprio quello degli adulti: «Serve una rete di cui deve far parte anche la scuola, di adulti responsabili capaci di trasmettere un senso di sicurezza, di protezione, di accoglienza», spiega ancora Silvestri. Sono proprio i ragazzi a raccontare le difficoltà degli adulti: Davide Dal Maso, giovane professore in un istituto superiore, ha fondato una no profit, Movimento etico digitale, che ha formato lo scorso anno 17mila ragazzi e 4mila genitori all'uso consapevole del web. «I dati del nostro Osservatorio –dice - raccontano della difficoltà degli adulti di impartire regole precise ed esplicite per vivere serenamente il web in famiglia, forse per il distacco e la sfiducia con cui molti di loro hanno sempre visto il digitale. Ma è sempre più necessario costruire un ponte tra genitori analogici e figli digitali per arrivare ad un sano equilibrio tra vita on-line e off-line».

© RIPRODUZIONE RISERVATA