Newsletter Kaspersky

Giugno 2020

Sommario. ▪ **P.2** COVID-19: quale impatto avrà sulla sicurezza informatica di organizzazioni e individui? ▪ **P.3** Garantire la sicurezza del voto elettronico per sostenere lo sviluppo della e-democracy. ▪ **P.3** Violenza domestica: stalkerware, una minaccia informatica in crescita. ▪ P.4 Infrastrutture critiche e sicurezza informatica: quasi il doppio delle vulnerabilità. ▪ P.4 Prosegue l'attività della Global Transparency Initiative di Kaspersky con il programma "Cyber Capacity Building".

La prima metà del 2020 è stata segnata dalla crisi generata dalla pandemia da coronavirus che ha colpito sia il mondo reale che il cyberspazio. Abbiamo assistito a diversi attacchi rivolti alle organizzazioni sanitarie che hanno lasciato un triste segno, così come a campagne di phishing che hanno approfittato dell'utilizzo massiccio del telelavoro.

Morten Lehn
General Manager
Kaspersky Italia

Questi ultimi accadimenti ci hanno dimostrato come la cyber-immunità possa essere raggiunta solo attraverso un approccio multilaterale e un lavoro di fiducia che coinvolga tutti gli attori della cybersecurity.

A questo proposito Kaspersky ha partecipato a diversi progetti nati in questo periodo difficile ma che siamo convinti che porteranno dei benefici anche per il futuro.
Uno tra questi è il progetto **"Solidarietà Digitale"** promosso dal Ministero per l'Innovazione tecnologica e la Digitalizzazione, con supporto tecnico dell'Agenzia per l'Italia Digitale, per ridurre l'impatto sociale ed economico del Coronavirus grazie a soluzioni e servizi innovativi gratuiti messi a disposizione da molte aziende per supportare privati e imprese.

Oppure l'iniziativa del Miur che ha avviato **Protocollo in Rete**, un progetto per l'innovazione didattica e la tecnologia delle scuole al quale abbiamo aderito anche noi mettendo a disposizione, degli istituti scolastici che hanno aderito al progetto, le nostre soluzioni.

Abbiamo anche realizzato un video con le regole per studiare in sicurezza anche da casa nell'ambito dell'iniziativa **#LaScuolaContinua**, nata in risposta alla call del Ministero dell'Istruzione per la crisi Covid-19, per supportare in modo congiunto le community del sistema scolastico durante l'emergenza scuole chiuse.

Siamo convinti che questa situazione e i progetti nati in questa occasione contribuiranno ad una presa di coscienza sull'importanza della digitalizzazione nel nostro Paese.

Questa edizione della nostra newsletter è anche un'occasione per fare il punto su diverse tendenze in materia di sicurezza informatica, tra cui lo sviluppo di un nuovo preoccupante fenomeno in materia di violenza domestica "digitale" ovvero lo stalkerware. A questo proposito Kaspersky collabora già con diverse associazioni e aziende in tutto il mondo e ci auguriamo presto di poter collaborare anche con dei partner italiani.

Ma si parlerà anche del programma **Global Transparency Initiative di Kaspersky**, il progetto per assicurare la massima trasparenza ai propri clienti e di una delle minacce più pericolose per le infrastrutture critiche, i ransomware.

kaspersky

COVID-19: quale impatto avrà sulla sicurezza informatica di organizzazioni e individui?

3 domande a Giampaolo Dedola, security researcher del Global Research & Analysis Team (GReAT) di Kaspersky.

La pandemia di COVID 19 ha costretto molte persone al telelavoro. Anche adesso che il lockdown è terminato sono in tanti a lavorare ancora da casa. Quali sono i rischi?
Il passaggio di massa improvviso allo smart working che si è verificato all'inizio della pandemia, di persone costrette ad organizzare in tutta fretta una postazione di lavoro all'interno della propria abitazione, ha rappresentato sicuramente un'opportunità unica per i cyber criminali che hanno approfittato dell'urgenza con cui questi trasferimenti sono avvenuti e hanno sfruttato qualsiasi vulnerabilità. Si è parlato tanto, ad esempio, di come abbiano sfruttato sin da subito l'argomento "hot" del momento e dei malware diffusi attraverso file che dovevano sembrare documenti informativi riguardo al virus. Più in generale, una volta che un dispositivo aziendale viene portato al di fuori dell'infrastruttura di rete dell'azienda e, quindi, connesso a nuove reti e al Wi-Fi, i rischi aumentano drasticamente. Ransomware, infezioni da malware e spionaggio aziendale sono tra le minacce che devono essere sempre tenute in considerazione, soprattutto quando si parla di smart working, poiché una rete Wi-Fi non sicura amplifica il rischio di infezione. Inoltre, l'uso di dispositivi personali per scopi lavorativi è una pratica che si verifica con molta più probabilità in condizioni di lavoro da remoto e rappresenta un ulteriore rischio alla sicurezza. Il phishing veicolato attraverso i siti di consumo può facilmente infettare i dispositivi e, in particolare i dispositivi personali che hanno molte più probabilità di avere un software obsoleto con vulnerabilità potenzialmente non aggiornate. Infine, il controllo decentralizzato dell'IT e la difficoltà di tracciare e mettere in sicurezza i dispositivi rendono il sistema di sicurezza molto più vulnerabile.

Una delle principali vulnerabilità delle aziende è rappresentata proprio dai dipendenti. Cosa si può fare per impedire che i dipendenti diventino una porta aperta che dà accesso ai dati sensibili dell'azienda?
È proprio così. Lo scorso anno, il 67% dei furti di credenziali ha avuto successo grazie a errori causati da dipendenti disattenti che si sono lasciati ingannare da truffe di phishing. Il download accidentale di contenuti malevoli da questo tipo di email può portare all'infezione dei dispositivi e anche alla compromissione dei dati aziendali con conseguenze enormi da un punto di vista economico e di reputazione. Tenendo conto di queste statistiche, per costruire un ambiente aziendale più sicuro e mettere i dipendenti nella condizione di lavorare in sicurezza anche da casa, molte organizzazioni dovrebbero inserire tra le loro priorità la questione relativa al rafforzamento e al miglioramento della consapevolezza in materia di sicurezza informatica dei loro dipendenti. Un programma di formazione in grado di migliorare davvero il livello di sicurezza di un'azienda, dovrebbe includere attività di formazione non solo relative alla conoscenza della sicurezza informatica ma anche in grado di agire sul comportamento dei dipendenti. Un dipendente adeguatamente formato seguirà le policy di sicurezza e le migliori pratiche fornendo un contributo importante alla protezione dell'azienda e alla sua reputazione e riducendo drasticamente la possibilità che l'azienda diventi vittima di un attacco informatico a causa di azioni guidate dalla mancanza di consapevolezza dei dipendenti.

Quali accorgimenti deve prendere un dipendente che opera in smart-working e quali le imprese?
Per i dipendenti esistono regole basilari ma molto importanti. Innanzitutto quella di proteggere sempre tutti i dispositivi, compresi quelli mobili, con soluzioni per l'Internet Security affidabili e mantenere sempre aggiornati i vari sistemi operativi e le app in uso. A proposito di app, è molto importante che si utilizzino solo quelle disponibili sugli store ufficiali, come Google Play, App Store, e vale lo stesso per i portali di e-learning e le piattaforme per la comunicazione, è fondamentale utilizzare solo quelle fornite dai datori di lavoro o dalle scuole. Inoltre, è sempre bene ricordare di non cliccare mai su link o allegati ricevuti da persone che non si conoscono o di cui non si può verificare l'identità, né tantomeno rispondere a messaggi indesiderati. Per quanto riguarda le aziende, invece, quello che raccomandiamo è di essere particolarmente vigili in questo momento. Tutte le organizzazioni dovrebbero garantire un accesso sicuro anche da remoto, attraverso soluzioni di sicurezza affidabili e fornendo una VPN, e dovrebbero assicurarsi, attraverso una chiara comunicazione, che i propri dipendenti siano consapevoli dei possibili rischi informatici in cui possono incorrere lavorando da casa.

Garantire la sicurezza del voto elettronico per sostenere lo sviluppo della e-democracy.

Le elezioni online consentono notevoli vantaggi permettendo all'organizzatore di ridurre i costi e all'utente di risparmiare tempo evitando code o ingorghi. Tuttavia, il voto su Internet richiede un investimento significativo per essere implementato in modo ottimale e in completa sicurezza. Per questo motivo è stato spesso difficile giustificare la necessità di introdurre questa opzione.

Tuttavia, l'esigenza di imporre un isolamento sociale degli ultimi mesi ha favorito un utilizzo maggiore dei servizi digitali. C'è un interesse crescente per l'e-voting all'interno degli enti locali e regionali ma soprattutto all'interno di consigli di amministrazione e assemblee generali di imprese, associazioni, sindacati e partiti politici. Siamo convinti che questo è un trend che vedremo crescere e che le misure di autoisolamento a livello globale modificheranno l'atteggiamento nei confronti del voto a distanza.

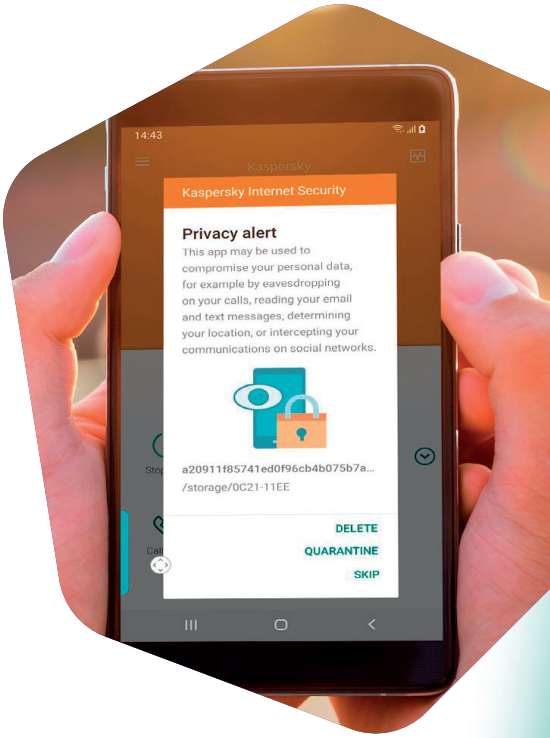
Kaspersky contribuisce a questa transizione offrendo una nuova piattaforma di e-voting basata sulla sicurezza informatica. Il progetto Polys (www.polys.me) consiste in un sistema di voto online chiavi in mano basato sulla tecnologia blockchain e su un'architettura decentralizzata su più nodi che può essere gestita nel cloud di un cloud provider fidato o on-premise sull'infrastruttura del promotore del voto. Le ultime innovazioni di Kaspersky: una macchina per il voto sicura e urne collegate alla blockchain! La nostra missione è chiara: garantire l'integrità e l'inviolabilità del voto elettronico.

Violenza domestica: stalkerware, una minaccia informatica in crescita

I programmi noti come **stalkerware** sono software di tracciamento che permettono di seguire la vita privata di una persona accedendo ai suoi dati personali: messaggi, fotografie, account social, geolocalizzazione e registrazioni audio o video della vittima (in alcuni casi in tempo reale). Si tratta di un tipo di spyware commerciale considerato legale, ma che di fatto può portare a casi di violenza domestica "digitale" in quanto può essere usato per monitorare in segreto le attività sul dispositivo del proprio partner.

L'utilizzo di questi software si è **diffuso notevolmente anche in Italia**.
Secondo il report The State of Stakerware 2019 di Kaspersky, nei primi otto mesi del 2019, in Italia il numero degli utenti unici oggetto di almeno un tentativo di intrusione con stalkerware ammonta a 1.031, aggiudicandosi il 6° posto tra i Paesi più colpiti dopo Russia, India, Brasile, Stati Uniti e Germania. Guardando allo stesso periodo dell'anno precedente, in Italia, è stato registrato un aumento del numero di intrusioni con stalkerware del 93%. Inoltre, il panorama delle minacce che riguarda gli stalkerware si è ampliato. Kaspersky ha scoperto 380 varianti di stalkerware in the wild nel 2019 - il 31% in più rispetto all'anno precedente. Kaspersky ha quindi deciso di mettersi in prima linea per quanto riguarda la protezione delle vittime di stalkerware. Non solo è stata la prima nel settore ad avere aggiornato il suo prodotto consentendo agli utenti di Kaspersky Internet Security for Android di ricevere un Privacy Alert, una nuova funzionalità che avvisa l'utente nel caso in cui i suoi dati privati siano monitorati a sua insaputa da terzi, ma nel 2019, Kaspersky e altre nove organizzazioni che operano sia nel settore della sicurezza IT che in gruppi di difesa e organizzazioni non profit, hanno lanciato un'iniziativa globale per proteggere gli utenti contro lo stalking e la violenza domestica la **Coalition Against Stalkerware.**

COALITION AGAINST STALKERWARE



In Italia è stato registrato un aumento del numero di intrusioni con stalkerware del

93%

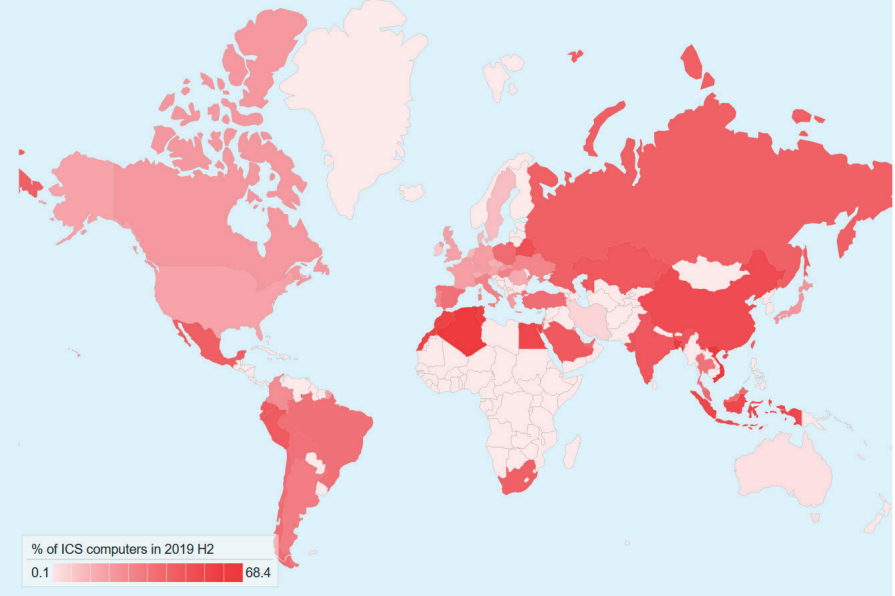
Kaspersky ha scoperto

380 varianti di stalkerware in the wild nel 2019 - il 31% in più rispetto all'anno precedente.

Infrastrutture critiche e sicurezza informatica: quasi il doppio delle vulnerabilità

Una nuova ricerca dell'ICS CERT di Kaspersky sulle minacce ai sistemi di controllo industriali (ICS) ha rilevato 103 nuove vulnerabilità nel 2019 che potrebbero essere sfruttate da attacchi informatici, quasi il doppio rispetto alle 61 segnalate nel 2018. Alla fine del primo trimestre del 2020, 33 di queste risultano ancora non corrette dai produttori.

La minaccia è reale: nel 2019 sono stati bloccati oggetti malevoli su quasi un sistema ICS su due (46,4%). Tra i sistemi presi di mira abbiamo rilevato software di automazione, sistemi di controllo industriale e sistemi IoT. È stato interessante notare come anche le minacce che potremmo definire generiche si rivolgano a sistemi industriali specializzati. I ransomware, ad esempio, come il famoso Wannacry o GandCrab, è stato bloccato sull'1% dei sistemi ICS protetti da Kaspersky. Si tratta di una minaccia molto pericolosa in particolare nel Sud-Est asiatico e nel Nord Europa.



Il settore energetico è tra i più colpiti a livello mondiale: il 36,6% dei sistemi ICS del settore energetico è stato colpito da almeno un attacco, e il 36,3% nel settore Oil&Gas. Altre infrastrutture critiche e servizi essenziali come il trattamento delle acque, la sanità e la lavorazione degli alimenti sono in cima alla lista in termini di maggior numero di vulnerabilità individuate. Questi trend confermano l'importanza di regolari controlli di sicurezza e di un monitoraggio attivo (threat intelligence) per la protezione contro i criminali informatici tradizionali e le minacce avanzate persistenti.

Per saperne di più:

https://ics-cert.kaspersky.com/

Prosegue l'attività della Global Transparency Initiative di Kaspersky con il programma Cyber Capacity Building"

Proseguono le attività a sostegno della **Global Transparency Initiative (GTI)** di Kaspersky, il progetto di Kaspersky per assicurare ai propri clienti la massima "trasparenza" e la possibilità di verificare i propri prodotti.

Nell'ambito di questa iniziativa Kaspersky aveva già mosso dei passi molto importanti tra cui: il trasferimento dei dati degli utenti europei a Zurigo, l'apertura dei Transparency Center in diversi Paesi nel mondo per consentire la revisione del codice sorgente, aver superato con successo l'audit Service Organization Control for Service Organizations (SOC 2) Type 1 condotto da una delle società di revisione Big Four e aver ottenuto la certificazione ISO27001. Sempre perseguendo lo stesso obiettivo di trasparenza Kaspersky ha deciso di offrire il proprio aiuto sviluppando un programma specifico, il "Cyber Capacity Building Program".
Si tratta di un percorso di formazione dedicato proprio a sviluppare capacità relative alla valutazione della sicurezza dei prodotti e delle soluzioni di cybersecurity in uso. Disponibile in versione online e offline, il programma è stato progettato per aiutare le aziende, le organizzazioni governative e il mondo accademico in generale a sviluppare strumenti pratici e conoscenze utili per poter fare una valutazione dello status della propria sicurezza.

La partecipazione al programma pilota sarà gratuita e verrà lanciata per la prima volta nel terzo trimestre del 2020 per le organizzazioni governative e il mondo accademico. Più tardi, sempre nel corso dell'anno, la formazione verrà resa disponibile anche per le realtà aziendali. Le organizzazioni interessate possono ricevere maggiori informazioni visitando la sezione dedicata sul sito di Kaspersky.

Proven.
Transparent.
Independent.

@KasperskyLabIT @kasperskylabitalia Kaspersky-lab-italia

Kaspersky Italia,
Piazza Sigmund Freud, 1 – 20154
Milan Italy | www.kaspersky.it