Presentata oggi la nuova edizione del Rapporto Clusit 2020 sulla sicurezza cyber

Clusit: la pandemia spinge il cybercrime

Nei primi sei mesi dell'anno persiste il trend di crescita degli attacchi gravi (+7%): il 14% è a tema Covid-19.
Registrato un aumento in Europa; malware, phishing e social engineering le tecniche più utilizzate. +85% gli attacchi alle infrastrutture critiche, +63% quelli al settore della ricerca.

Faggioli, presidente Clusit: "Fondamentale investire in ricerca e costruire un ecosistema imprese-pubblica amministrazione; necessaria maggiore consapevolezza dei rischi informatici tra i cittadini".

Milano, 10 novembre 2020 – Con **850 attacchi noti analizzati**, circa il 7% in più rispetto allo stesso periodo dello scorso anno, e la crescita costante del cybercrime, causa dell'**83%** degli attacchi, la prima metà del 2020 si guadagna la maglia del "semestre nero" della cybersecurity. È quanto emerge dai dati contenuti nella nuova edizione del Rapporto Clusit 2020, presentata questa mattina in apertura di Security Summit Streaming Edition.

I ricercatori di Clusit, Associazione Italiana per la Sicurezza Informatica, hanno inoltre evidenziato come la pandemia abbia fortemente - e in vario modo - caratterizzato gli attacchi informatici in questi mesi: **il tema "Covid-19"** è infatti stato utilizzato tra febbraio e giugno per perpetrare 119 attacchi gravi, ovvero il **14% degli attacchi complessivamente noti**[1]. In particolare, l'argomento è stato utilizzato a scopo di cybercrime, ovvero per estorcere denaro, nel **72%** dei casi; con finalità di "Espionage" e di "Information Warfare" nel **28%** dei casi.

Oltre ai danni direttamente conseguenti agli attacchi compiuti, gli esperti Clusit evidenziano che il tema Covid-19 ha alimentato anche la diffusione di fake-news, fomentando la confusione sulla pandemia che si è venuta a creare a livello globale soprattutto nei primi mesi.

Gli attacchi a tema Covid-19 sono stati condotti nel 61% dei casi con campagne di "Phishing" e "Social Engineering", anche in associazione a "Malware" (21%), colpendo tipicamente i cosiddetti "bersagli multipli" (64% dei casi): si tratta di attacchi strutturati per danneggiare rapidamente e in parallelo il maggior numero possibile di persone ed organizzazioni. Il 12% degli attacchi a tema

[1] Il Rapporto Clusit è frutto del lavoro di un centinaio di professionisti che operano nell'ambito dell'Associazione per la Sicurezza Informatica in Italia. Viene compilato annualmente e aggiornato a livello semestrale per fornire il quadro più aggiornato ed esaustivo della situazione globale, evidenziando i settori più colpiti, le tipologie e le tecniche d'attacco più frequenti, **sulla base degli attacchi di dominio pubblico** – che rappresentano un campione necessariamente limitato, per quanto ragionevolmente significativo, rispetto al numero degli attacchi informatici gravi effettivamente avvenuti nel periodo in esame. Un buon numero di aggressioni non diventa mai di dominio pubblico, o lo diventa dopo molto tempo.

Covid-19 ha avuto come obiettivo il settore Governativo, Militare e l'Intelligence: sono stati in questo caso prevalentemente attacchi di natura "Espionage". Spiccano infatti tra di essi alcuni casi gravi di "BEC scam" (Business Email Compromise), portati a segno da cyber criminali nelle prime fasi concitate di approvvigionamento dei presidi di sicurezza (per esempio, le mascherine), generando danni considerevoli.

A livello complessivo, nel primo semestre dell'anno gli attacchi - già classificati come "gravi" nell'analisi Clusit - hanno avuto effetti molto importanti o critici nel 53% dei casi, rivelando importanti impatti geopolitici, sociali, economici (diretto e indiretto), di immagine e di costo/opportunità per le vittime.

"*Nella tragedia di questi mesi, sta avvenendo una rivoluzione: il digitale sta trasformando l'organizzazione delle imprese e la vita dei cittadini, e stiamo comprendendo che la sicurezza del digitale è essenziale"*, afferma Gabriele Faggioli, presidente Clusit.

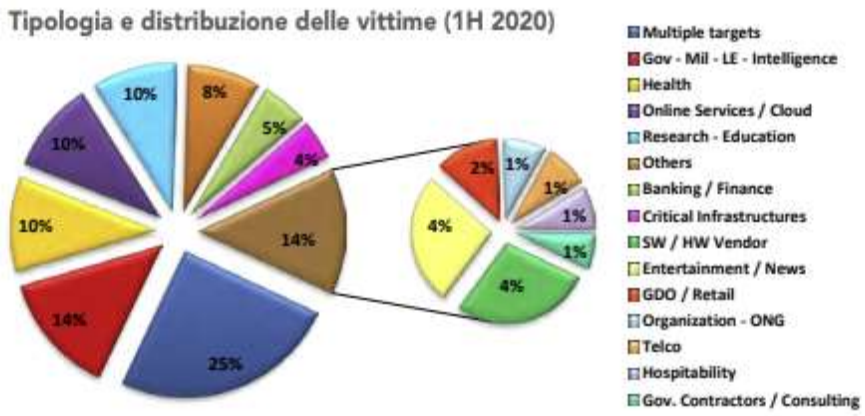
"*Pensiamo che siano tre in particolare i punti da indirizzare nel percorso virtuoso verso la sicurezza informatica: investire in ricerca e innovazione, costituire un ecosistema delle imprese e della pubblica amministrazione in cui gli investimenti risultino adeguati alla minaccia e consapevolizzare maggiormente i cittadini. Lavoriamo in queste direzioni anche con le istituzioni per supportare la continuità in ambito produttivo e dei servizi, in primis quelli sanitari ed educativi del nostro Paese*", conclude Faggioli.

Cyber attacchi nel primo semestre 2020: chi viene colpito e perché.

Nei primi sei mesi del 2020 gli esperti Clusit hanno registrato in prevalenza attacchi verso la categoria "**Multiple Targets**" che, come nel caso specifico degli attacchi a tema Covid-19, risulta la categoria più colpita, in crescita del 26% rispetto allo stesso periodo dello scorso anno.

A crescere maggiormente sono tuttavia gli attacchi verso le categorie "**Critical Infrastructures**" (+85%), "**Gov Contractors**" (+73,3%) e "**Research / Education**" (63%). Sono anche aumentati gli attacchi verso la categoria "**Government**" (+5,6%).

In termini assoluti, il settore "**Government - Military - Intelligence**" è stato il secondo settore nel mirino degli attaccanti (con il 14% degli attacchi), seguono i settori "**Healthcare**" e "**Online Services**" (10% degli attacchi).



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

"*L'analisi degli attacchi nel primo semestre 2020 rende evidente che, oggi come non mai, la nostra civiltà digitale è esposta a rischi importanti e potenzialmente sistemici: nell'emergenza mondiale che stiamo attraversando la cyber security è chiaramente, e in maniera irreversibile, un requisito fondamentale per il benessere di singoli individui, istituzioni ed imprese*", commenta Andrea Zapparoli Manzoni, tra gli autori del Rapporto Clusit.

Le aree geografiche colpite

Il Rapporto Clusit rappresenta su base continentale le vittime dei crimini informatici: nel primo semestre del 2020 rimangono sostanzialmente invariate rispetto allo stesso periodo dell'anno precedente le vittime di area americana (dal 46% al 45%), mentre **crescono gli attacchi verso realtà basate in Europa** (dal 9% al 15%). Rimangono percentualmente quasi invariati quelli rilevati contro organizzazioni asiatiche (dal 10% al 11%).

© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

Le tecniche d'attacco
Nel primo semestre dell'anno gli attaccanti hanno conseguito i loro obiettivi utilizzando **malware** nel 41% dei casi**.** Agli attacchi compiuti con questa tecnica, i ricercatori Clusit sommano gli attacchi compiuti con **Multiple Techniques / APT**, più sofisticati ma quasi sempre basati anche sull'utilizzo di malware, concludendo così che **di fatto il malware arriva a rappresentare il 45% delle tecniche di attacco complessivamente utilizzate**.

Le tecniche di "**Phishing e Social Engineering**", in crescita del 26% rispetto allo stesso periodo dello scorso anno, sono state utilizzate nel 20% dei casi. Oltre il 40% delle campagne condotte con tecniche di Phishing, in particolare tra febbraio e giugno, hanno sfruttato il tema Covid-19, facendo leva su situazioni di incertezza e particolare sensibilità a livello globale ai temi della pandemia, nonché sulla insufficiente consapevolezza individuale.

È in aumento l'utilizzo di vulnerabilità "**0-day**" (+16,7%), per quanto il dato - notano gli esperti Clusit - sia ricavato da incidenti di dominio pubblico e sia quindi probabilmente sottostimato. Ritornano a crescere in modo significativo gli attacchi basati su tecniche di "**Account Hacking/Cracking**" (+24,2%).

In complesso, gli esperti Clusit rilevano che le **tecniche di attacco meno sofisticate**, quali SQLi, DDoS, Vulnerabilità note, Account cracking, Phishing e Malware "semplice") **rappresentano il 76% del totale**, e la tendenza non mostra inversioni rispetto ai semestri precedenti: questo significa che gli attaccanti possono ancora realizzare attacchi gravi di successo contro le loro vittime con relativa semplicità e a costi molto bassi.

La nuova edizione del Rapporto Clusit 2020 presentata oggi nel corso di Security Summit Streaming Edition include inoltre l'analisi degli attacchi in Italia nel periodo gennaio-giugno 2020 svolta da **Fastweb** sulla base dei dati rilevati dal Fastweb Security Operations Center (SOC); le segnalazioni della **Polizia Postale e delle Comunicazioni** e del **CERT PA**.
È inoltre presente uno studio sullo stato della cybersecurity nel sud d'Italia, realizzato da ricercatori dell'**Università degli Studi di Bari e di Exprivia/Italtel**, un capitolo dedicato al settore finanziario "Elementi sul Cyber-crime nel settore finanziario in Europa", a cura di **IBM**, cui si aggiungono i contributi del **CERTFin** e del **CERT di Banca d'Italia**.

Il nuovo Rapporto Clusit comprende inoltre uno "**Speciale Pandemia**" relativo all'impatto del Covid-19 sulla sicurezza delle informazioni, a cui ha contribuito anche il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della **Guardia di Finanza**.

Seguono uno studio realizzato dall'Osservatorio Cybersecurity & Data Protection della **School of Management del Politecnico di Milano** sulla gestione dell'OT Security e un'analisi del mercato italiano della sicurezza IT, realizzata da **IDC Italia**.
Èparticolarmente ricca la sezione di approfondimento su tematiche specifiche "**Focus On**":

- "L'impatto dei deepfake sulla sicurezza delle organizzazioni economiche", di
- "Business Continuity & Resilienza, leve fondamentali per una società sempre più globalizzata e digitalizzata", Federica Bertoni
- "Mobile App italiane: una lente di ingrandimento sul loro stato di salute e sulle vulnerabilità più diffuse", Maria Rita Livelli,
- Sicurezza nel settore sanitario – Perché gli ospedali sono così violabili", a cura di CryptoNet Labs.
- "Tendenze IT che avranno un impatto sui professionisti italiani nel 2020", a cura di Netwrix.
- "Email security: i trend rilevati in Italia nel corso del 2019", a cura di Libraesva.

Security Summit è organizzato da:

Clusit - Associazione Italiana per la Sicurezza Informatica - i cui soci rappresentano oltre 500 aziende e organizzazioni. Clusit collabora, a livello nazionale, con diversi Ministeri, Authority e Istituzioni, con la Polizia Postale e con altri organismi di controllo. Inoltre, svolge un'intensa attività di supporto e di scambio con le Confederazioni Industriali, con numerose Università e Centri di Ricerca e con Associazioni Professionali e dei Consumatori. In ambito internazionale, Clusit partecipa a molte iniziative in collaborazione con i CERT, i CLUSI, la Commissione Europea, ITU (International Telecommunication Union), UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale) e sostiene attivamente le attività di ENISA (European Union Agency for Network and Information Security). Ulteriori informazioni sulle attività del Clusit sono disponibili sul sito www.clusit.it

Astrea, Agenzia di Comunicazione e Marketing, specializzata nell'organizzazione di eventi business nel mondo della tecnologia, e in particolare della Sicurezza Informatica. Con sede operativa a Milano, Astrea mette le competenze dei propri professionisti a disposizione delle organizzazioni per sviluppare soluzioni creative ed innovative volte a incrementare visibilità e ad acquisire autorevolezza sui mercati di riferimento. www.astrea.pro

Per ulteriori informazioni si prega di contattare:

Daniela Sarti
Ufficio Stampa Security Summit | Clusit
press@securitysummit.it - dsarti@clusit.it
Tel. 335 459432