09/12/2020

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 819
Utenti unici: 12.467

https://www.cybersecurity360.it/nuove-minacce/cyber-security-i-crimini-aumentano-in-linea-con-la-curva-epidemica-i-consigli-per-difendersi/

Cyber security, i crimini aumentano in linea con la curva epidemica: i consigli per difendersi

Non è un quadro molto confortante quello che riguarda lo stato della sicurezza informatica in Italia, in un anno in cui il paese è sotto scacco della pandemia da Covid-19 mentre in ambito cyber security si assiste ad un aumento dei crimini in linea con la curva pandemica. Ecco i numeri e alcuni utili consigli per difendersi Nel corso del 2020 in Italia, nonostante l'andamento altalenante del cyber crime, si registra un numero crescente di reati informatici che hanno raggiunto un exploit nel mese di giugno e settembre, rispettivamente con 85 e 70 attività malevoli a danno di aziende, pubblica amministrazione e semplici cittadini.L'aumento dei contagi dopo la stagione estiva ha costretto un numero elevato di lavoratori a svolgere le proprie prestazioni in modalità agile e a digitalizzare moltissime attività, dall'industria alla scuola fino ai servizi offerti dai nostri Comuni. Un andamento che sembra marciare parallelo a quello della pandemia di coronavirus. E proprio la COVID-19 continua a essere legata alla maggior parte dei fenomeni segnalati.Secondo il Threat Intelligence Report 3Q2020, elaborato dall'Osservatorio CyberSecurity di Exprivia in Italia, nel periodo luglio-settembre sono stati registrati 148 attacchi, incidenti e violazioni della privacy, rispetto ai 171 eventi del periodo aprile-giugno e ai 49 tra gennaio e marzo. Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi nel 2020 in Italia.Indice degli argomenti I settori più colpitiTecniche di attacco: in testa phishing e social engineeringConsigli pratici per difendersi dalle cyber minacce I settori più colpiti Il settore maggiormente colpito è stato quello della Pubblica Amministrazione con i Comuni tra gli obiettivi più vulnerabili, laddove il blocco di un qualsiasi servizio comunale influisce direttamente sul benessere dei cittadini e si traduce non solo in perdite finanziarie, ma anche in altre conseguenze socialmente impattanti.Nel corso del periodo luglio-settembre sono raddoppiati gli eventi

criminali rispetto al trimestre precedente e precisamente si sono verificati 34 eventi, la metà dei quali nel solo mese di settembre. Nel dettaglio si sono registrati 17 attacchi, 11 incidenti e 6 violazioni della privacy.Un esempio interessante è il caso di MassLogger, il malware che ha sottratto numerose credenziali a utenti della pubblica amministrazione italiana. Un altro caso riguarda una nuova campagna di phishing: false e-mail a tema INPS hanno veicolato malware Urnisf/Gozi in Italia causando una serie di danni notevoli quali: capacità di intercettare traffico di rete, sottrarre credenziali e installare aggiuntivi codici malevoli. Settore PA in Italia 3Q2020.Anche il settore della Finanza è stato duramente colpito dai criminali informatici che, con il 44% in più di attacchi rispetto al trimestre precedente, continua ad essere tra i settori più esposti alle minacce viste le grandi possibilità di profitto, segno anche di una costante specializzazione degli attaccanti in questo ambito.Analizzando i dati del Threat Intelligence Report 3Q2020 si evidenzia, inoltre, che gli istituti bancari rientrano tra le principali vittime dei cybercriminali, che attaccano attraverso false comunicazioni indirizzate ai clienti. Settore Finance in Italia 3Q2020. WHITEPAPER Gestione dei contratti e GDPR: guida all'esternalizzazione di attività dei dati personali Legal Scarica il WhitepaperDall'analisi si evince una forte preoccupazione per gli eventi registrati nel settore industriale. Ben 12 attacchi sono concentrati nei mesi di pieno recupero post COVID-19, ossia tra luglio e settembre, con un aumento del 33% rispetto al trimestre precedente. Le industrie più sensibili a questi attacchi sono quelle in ambito energetico e manifatturiero, soggette il più delle volte a casi di spionaggio industriale.Continua la classifica dei settori più colpiti, con la Sanità che ha riscontrato un aumento degli attacchi nel terzo trimestre pari al 38%; questo settore risulta essere uno dei più attrattivi per il cyber crime poiché tratta informazioni confidenziali e sensibili aventi un alto valore remunerativo nel Dark Web.Concludendo, nel settore Retail sono quasi triplicati gli attacchi rispetto al trimestre precedente durante il periodo estivo, che ha visto un relativo allentamento delle misure per l'emergenza; i criminali sfruttano le scarse competenze tecniche del personale per trarne facili profitti. Tecniche di attacco: in testa phishing e social engineering Alla base di tutti gli attacchi informatici registrati in Italia dall'Osservatorio CyberSecurity di Exprivia ci sono ancora una volta il phishing e il social engineering tra le tecniche di attacco più utilizzate, con ben 62 eventi nel trimestre luglio-settembre.Il phishing, che permette di colpire in maniera particolare utenti distratti o con poca conoscenza delle minacce web, sfrutta un'e-mail o altra comunicazione fraudolenta per attirare la vittima. Il messaggio sembra provenire da un mittente affidabile.Se l'inganno riesce, la vittima viene esortata a fornire

informazioni riservate, spesso su un sito web truffa e, in alcuni casi, la macchina della vittima viene infettata da un malware.Ad esempio, si rischia di subire un attacco phishing nel concedere agli attaccanti informazioni sulla carta di credito o altri dati personali, incappando in un ricatto in denaro.Altre volte le e-mail di phishing vengono inviate al fine di ottenere le credenziali di accesso ai sistemi aziendali dei dipendenti o altre informazioni utili a sferrare un attacco più sofisticato, come ad esempio minacce avanzate persistenti (APT) contro un'azienda specifica.Per comprendere l'impatto di questa tecnica è utile effettuare un'attenta analisi relativa alla "severity" degli eventi. A tal proposito come Osservatorio CyberSecurity abbiamo ritenuto di suddivide gli attacchi in tre fasce per valutarne la gravità: gli attacchi con impatto "medio" sono i più diffusi, ben 52 rispetto ai 10 con impatto "alto". I target Finance, Sanità, Education e Industria sono caratterizzati da attacchi aventi un impatto per la maggior parte di livello "alto". Consigli pratici per difendersi dalle cyber minacce I risultati emersi nel terzo trimestre del 2020 ci portano a insistere sulla consapevolezza di un aumento degli attacchi informatici a tema COVID-19, ecco perché la conoscenza e la formazione sulla sicurezza sono, ancor più, le migliori armi che si hanno a disposizione per ridurre il rischio sia dei singoli utenti che dei lavoratori in remote working di incorrere in truffe.È necessario a tutti livelli investire in cultura digitale, in misure proattive che accrescano la consapevolezza e le competenze per riconoscere un crimine e, soprattutto, per fare in modo che non si verifichi. Bisogna imparare a conoscere il mondo digitale e a comprendere cosa è un bene e cosa è un male.Il rischio di poter essere vittime di cyber crime, mai come in questo periodo, è reale, ma molto dipende dai nostri comportamenti. Un meccanismo di controllo del comportamento umano, ad esempio, è la tecnologia UBA (User Behavior Analytics) che sfrutta tecniche di machine learning atte a identificare attività anomale. Ancora una volta le più diffuse tecniche di attacco fanno leva sulle debolezze dell'utente umano, spesso anello debole della catena di sicurezza informatica.Consideriamo, ad ogni modo, che per assicurare business continuity è fondamentale sviluppare un programma di sicurezza dinamico, capace di adattarsi ai cambiamenti; si sente spesso parlare, infatti, di cyber resilienza, in quanto la velocità con cui si trasforma questo settore rende impossibile definire un unico piano di difesa che difenda il proprio perimetro di esposizione.Inoltre, è necessario ormai dotarsi di strumenti di threat intelligence che consentono di possedere informazioni riguardo le motivazioni degli attaccanti, le tecniche di attacco e via dicendo. Questi strumenti possono aiutare le organizzazioni a identificare in maniera più rapida le minacce informatiche e, allo stesso tempo,

educare al meglio i propri dipendenti per ridurre al minimo i danni causati dagli attacchi stessi. WHITEPAPER Come è cambiato in Italia il quadro normativo dei pagamenti digitali verso la PA? Scarica il Whitepaper@RIPRODUZIONE RISERVATA