Comando
telefono 091 814 67 42 e-mail stampa@polca.ti.ch
url www.polizia.ti.ch

Repubblica e Cantone Ticino
Polizia cantonale
6501 Bellinzona

Comunicato stampa

Con la pandemia raggiri informatici ancor più sotto la lente

Bellinzona, 08.04.2020

Gli autori di reati legati alla cybercriminalità hanno sfruttato la pandemia per tentare di ottenere ancor più guadagni illeciti, traendo giovamento dal confinamento delle persone tra le quattro mura di casa. Le truffe, legate in particolare alla compravendita di materiale sanitario e prodotti igienici, nonché l'acquisizione illecita di dati personali attraverso applicativi dedicati al telelavoro sono solo alcuni esempi di come il settore si sia adattato celermente al nuovo scenario. Sempre in auge anche le truffe denominate Business Email Compromise (BEC) e gli attacchi ransomware.

Le attività svolte dalla Sezione Analisi Tracce Informatiche (SATI) sono in costante aumento e questo va di pari passo con l'incremento generalizzato dei dispositivi informatici e di comunicazione nella nostra società. Fenomeno ancor più accentuatosi nel periodo pandemico.

Nel corso dell'anno la Sezione è stata attiva in 38 inchieste su casi specifici che presentavano componenti tecnico informatiche particolari. Ha inoltre svolto 55 perquisizioni in supporto ad altri servizi, ha effettuato 1'253 analisi informatico forensi a favore delle indagini condotte da altre unità della Polizia giudiziaria e della Gendarmeria, ha elaborato 37 analisi criminali operative, ha collaborato in 23 ricerche d'urgenza e ha evaso 517 richieste e-mail giunte da utenti o da altre autorità. In quest'ambito ransomware e BEC hanno richiesto particolare attenzione. I BEC prevedono, attraverso le tecniche di social engineering, l'accesso illecito a una casella di posta elettronica (solitamente aziendale) e la conseguente scoperta di una relazione finanziaria. I truffatori, spacciandosi quindi per il creditore, comunicano alla controparte delle false coordinate bancarie, sulle quali eseguire il trasferimento fraudolento di denaro. In quest'ambito lo scorso anno la Sezione Analisi Tracce Informatiche (SATI) della Polizia cantonale ha indagato su 19 casi, dai quali è emerso un danno economico pari a circa 3'300'000 franchi.

Attraverso un attacco **ransomware** i criminali riescono invece a criptare i dati contenuti nei dispositivi, così da poter chiedere un riscatto in cambio della chiave di decifratura. Gli autori, attraverso varie tecniche, selezionano in maniera sempre più mirata gli obiettivi, prediligendo grandi aziende (fenomeno conosciuto come *whaling*), al fine d'incrementare i propri profitti grazie all'estorsione d'ingenti somme di denaro.

Questi fenomeni hanno, di fatto, un comun denominatore, la difficoltà sempre maggiore nell'identificare gli autori e nel perseguirli poiché sfruttano l'anonimato legato al fatto di agire in rete. La prevenzione riveste quindi estrema importanza e la popolazione ha la possibilità di

informarsi consultando i siti della Polizia cantonale www.polizia.ti.ch , del gruppo cantonale Cyber Sicuro www.cybersicuro.ch e della Prevenzione svizzera della criminalità (PSC) https://www.skppsc.ch/it/temi/internet/. Per quanto riguarda invece le segnalazioni è attivo il Centro nazionale per la cibersicurezza (NCSC) all'indirizzo https://www.ncsc.admin.ch/ncsc/it/home.html.

Ancora in aumento le richieste provenienti da forze dell'ordine estere che, sulla base della convenzione sulla criminalità informatica, richiedono la conservazione dei dati presenti su server di società ubicate in Ticino. Il 2020 ha inoltre visto altre due particolari attività d'interesse: l'analisi criminale operativa, dettata dalla grande mole di dati, nel contesto di un'inchiesta per titolo di truffa e l'implementazione del nuovo gestionale in dotazione al **Tracciamento Contatti COVID-19** dal mese di dicembre.

Per interviste: capitano Orlando Gnosca (stampa@polca.ti.ch)