

## NUOVO BALZO DI ATTACCHI INFORMATICI IN ITALIA NEI PRIMI MESI DELL'ANNO: IL CYBERCRIME COLPISCE APP, SOCIAL E BANKING ONLINE

*L'Osservatorio Cybersecurity di Exprivia registra nel primo trimestre dell'anno 349 eventi criminali, in continua crescita rispetto al 2020. Calano i crimini informatici a tema Covid. Il furto dei dati è in cima alla classifica dei danni.*

**6 maggio 2021** – Continua a crescere il trend degli attacchi **informatici in Italia** anche nel 2021. Da quanto emerge nel **primo rapporto del 2021 sulle minacce informatiche in Italia** elaborato dall'**Osservatorio Cybersecurity di Exprivia**, nel periodo **gennaio-marzo 2021** si sono registrati **349 eventi**, tra attacchi, incidenti e violazioni della privacy. Si tratta di una crescita del 47% sul trimestre precedente e sette volte di più rispetto ai primi tre mesi del 2020. A un anno dallo scoppio della pandemia che ha portato alla massiccia diffusione dello smart working e al ricorso sempre più frequente a servizi online, il cybercrime continua a colpire spesso utilizzando tecniche poco sofisticate.

Nel primo trimestre del 2021 l'Osservatorio di Exprivia - impegnata nel diffondere la cultura della sicurezza informatica sia nelle aziende che tra privati cittadini – rileva una forte crescita degli **attacchi** (+56% rispetto all'ultimo trimestre del 2020). Nonostante ciò, il numero medio di **incidenti**, ovvero attacchi andati a buon fine, registra una flessione del 18% rispetto al trimestre precedente, rimanendo comunque costante in media rispetto all'intero anno 2020. Un significativo aumento continuano a registrarlo le **violazioni della privacy** attestate dalle multe del Garante, che segnano un +55% rispetto al trimestre precedente.

Secondo l'Osservatorio Exprivia, che prende in considerazione 86 fonti pubbliche, in questi primi mesi del 2021 il Covid-19 non è più la prima tematica utilizzata dagli hacker per colpire le vittime: il primato viene ceduto ai temi che riguardano la sfera del trattamento dei dati personali, sempre più esposti in rete per effetto della 'vita digitale' condotta massivamente da più di un anno. A seguire, sempre tra i temi più sfruttati dai cyber-criminali, il banking on line e la DAD.

*"I primi mesi dell'anno confermano una complessiva crescita dei crimini informatici - afferma **Domenico Raguseo, direttore Cybersecurity Exprivia**. Se da un lato gli attaccanti spendono molto di più per progettare gli attacchi, utilizzando tecniche sempre più sofisticate, dall'altro le vittime denotano una preoccupante mancanza di consapevolezza dei rischi. Il tema va necessariamente affrontato sia in termini di governance della sicurezza che di standard di certificazione, in particolare per quanto riguarda la difesa dei dispositivi industriali e IoT esposti in rete".*

Per la prima volta sul podio dei settori maggiormente colpiti dai cyber-criminali compare quello **Software/Hardware**, con 98 eventi, quasi quintuplicati rispetto allo scorso trimestre. Si tratta di fenomeni che colpiscono **app di messaggistica istantanea, sistemi operativi, piattaforme di videoconferenza, social network e dispositivi** utilizzati sia in ambito industriale che privato. Seguono il settore **Finance** - dagli istituti bancari alle assicurazioni, alle piattaforme di criptovalute - che, con 81 fenomeni segnalati, raddoppia gli eventi rispetto al trimestre 2020, e la **Pubblica Amministrazione** in leggero calo (-6%). Nei primi tre mesi dell'anno, cresce nuovamente l'interesse degli hacker per il settore **Healthcare**, ancora sotto scacco con la terza ondata della pandemia, che aumenta di dieci unità rispetto ai tre mesi conclusivi del 2020. A questo si aggiunge un livello di criticità degli attacchi che va ben oltre il semplice danno economico o la violazione della privacy;



sempre più spesso si è di fronte, infatti, al concreto rischio di una paralisi del sistema colpito (che sia quello di produzione industriale o quello sanitario).

Il maggior danno causato dai criminali rimane **il furto dei dati**, con il 70% dei casi tra gennaio e marzo, mentre **la sottrazione di denaro**, comunque in aumento del 40%, occupa la seconda posizione. Al terzo posto, le **violazioni dei dati personali**, in calo del 10% circa rispetto all'ultimo trimestre del 2020. Un forte segnale di crescita si rileva, infine, nelle pratiche che rendono un portale non disponibile, il cosiddetto **defacement**, che registra un +40% in confronto al trimestre ottobre-dicembre 2020.

Tra le tecniche più sfruttate dai cyber-criminali continua a primeggiare il **phishing-social engineering con circa il 60% dei casi** - quasi il doppio rispetto all'ultimo quarto del 2020 - che colpisce in maniera particolare utenti distratti o con poca conoscenza delle modalità di adescamento tramite e-mail o social network. Seguono i **malware**, che hanno l'obiettivo di sottrarre informazioni sensibili, principalmente mediante lo spionaggio delle attività bancarie degli utenti. Sul terzo gradino del podio anche le tecniche con cui gli attaccanti sfruttano vulnerabilità già conosciute (**known vulnerabilities**).

Diminuisce nel primo trimestre dell'anno il numero dei dispositivi esposti in rete: dai quasi 8 milioni del precedente trimestre, si passa ai circa 7,25 milioni nei primi tre mesi del 2021. Nello specifico, i dispositivi IoT diminuiscono dell'8% rispetto all'ultimo trimestre 2020, così come i dispositivi senza protocolli sicuri di autenticazione (il 7% in meno rispetto alla fine del 2020) e quelli industriali (-10%). Tra questi ultimi, però, il rapporto evidenzia in controtendenza una crescita dei PLC (controllore logico programmabile), dispositivi usati nell'automazione industriale, ancora poco protetti.

*“Nonostante la complessiva diminuzione, resta alto il numero dei dispositivi in Italia connessi a Internet e molti risultano senza protezione o protocolli di autenticazione - commenta Raguseo. Se pensiamo ad esempio che molti di questi potrebbero essere funzionali a erogare un servizio essenziale, il loro malfunzionamento potrebbe avere conseguenze importanti, soprattutto nel caso di sistemi sanitari o di software clinici”.*

Oltre al report, sul sito di Exprivia [www.exprivia.it](http://www.exprivia.it) è presente anche l'elenco dei **corsi** organizzati per la formazione nell'ambito della sicurezza e della gestione dei rischi a livello informatico.



## **Exprivia**

Exprivia è a capo di un gruppo internazionale specializzato in Information and Communication Technology in grado di indirizzare i driver di cambiamento del business dei propri clienti grazie alle tecnologie digitali.

Con un consolidato know-how e una lunga esperienza data dalla presenza costante sul mercato, il gruppo dispone di un team di esperti specializzati nei diversi ambiti tecnologici e di dominio, dal Capital Market, Credit & Risk Management all'IT Governance, dal BPO alla CyberSecurity, dai Big Data al Cloud, dall'IoT al Mobile, dal networking alla collaborazione aziendale sino al mondo SAP. Il gruppo affianca i propri clienti nei settori Banking&Finance, Telco&Media, Energy&Utilities, Aerospace&Defence, Manufacturing&Distribution, Healthcare e Public Sector. L'offerta comprende soluzioni composte da prodotti propri e di terzi, servizi di ingegneria e consulenza.

Oggi il gruppo conta circa 2.400 professionisti distribuiti in 7 paesi nel mondo.

Exprivia S.p.A. è quotata in Borsa Italiana nel mercato MTA (XPR).

La società è soggetta alla direzione e coordinamento di Abaco Innovazione S.p.A.

[www.exprivia.it](http://www.exprivia.it)

## **Contatti**

### **Exprivia SpA**

#### **Investor Relations**

Gianni Sebastiano

[gianni.sebastiano@exprivia.it](mailto:gianni.sebastiano@exprivia.it)

T. + 39 0803382070 - F. +39 0803382077

### **Ufficio Stampa**

#### **Sec Mediterranea**

T. +39 0805289670

Teresa Marmo

[marmo@segrp.com](mailto:marmo@segrp.com)

Cell. +39 3356718211

Gianluigi Conese

[conese@segrp.com](mailto:conese@segrp.com)

Cell. +39 3357846403

#### **Sec and Partners**

T. +39 063222712

Martina Trecca

[trecca@segrp.com](mailto:trecca@segrp.com)

Cell. +39 3339611304

Andrea Lijoi

[lijoi@segrp.com](mailto:lijoi@segrp.com)

Cell. +39 3292605000

