La criminalità in rete

Investigazione, diplomazia internazionale e legislazione. Il magistrato Stefano Dambruoso spiega le complesse intersezioni tra sicurezza e geopolitica

pagine 15

Cybersicurezza

L'Agenzia per l'Italia digitale monitora costantemente la diffusione delle minacce informatiche e analizza le vulnerabilità emerse. Il punto di Mario Nobile

pagina 9

REPORT SICUREZZA

UN PAESE MENO VULNERABILE

di **Gaetano Gemiti**

Nunzia Ciardi, vicedirettore generale dell'ACN, Agenzia per la Cybersicurezza Nazionale

Portali della pubblica amministrazione, siti istituzionali, testate giornalistiche, sistemi di trasporto, banche e, in misura crescente, infrastrutture sanitarie e industriali. Su questi obiettivi, ad alta visibilità e valore simbolico, si concentrano le offensive cyber dirette l'anno scorso all'Italia. Al quinto posto mondiale, secondo il Y-Report 2025 di Yarix (Var Group), tra i Paesi colpiti da attacchi di matrice hacktivista. «L'intento principale non è tanto economico- spiega Nunzia Ciardi, vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale- quanto dimostrativo».

>>> segue a pagina 3

ALL'INTERNO

LE GRANDI SFIDE TRA PROTEZIONE FISICA E DIGITALE

Droni, nuovi sistemi di videosorveglianza e controllo accessi integrati con l'Ai, nuovi impianti antincendio ad alta sensibilità, sistemi wireless per rilevazione fumi e gas, piattaforme per il controllo remoto e la gestione predittiva della manutenzione e del monitoraggio. I trend e gli sviluppi innovativi in tutti i comparti della security & fire- videosorveglianza, antincendio, controllo accessi, sicurezza passiva- saranno al centro della nuova edizione di Sicurezza, che si terrà dal 19 al 21 novembre a Fiera Milano. Cresce la manifestazione, rafforzando il suo posizionamento globale. Aumentano, infatti, la superficie espositiva (+18 per cento rispetto al 2023) e gli espositori esteri, che rappresentano oggi il 32 per cento del totale. A inizio ottobre, erano già 340 le aziende confermate, provenienti da 26 Paesi, con importanti ritorni da parte di brand assenti da alcune edizioni e nuovi ingressi di rilievo: non mancheranno i principali produttori europei- Francia, Germania, Regno Unito e Spagna- e la Cina, peso massimo a livello mondiale. Grazie a ICE-Agenzia, gli espositori incontreranno in appuntamenti one to one più di 100 top hosted buyer provenienti da 32 Paesi, con le maggiori delegazioni da Medio Oriente e Nord Africa, interessanti bacini di sbocco per le tecnologie in mostra, in particolare da Egitto, Tunisia, Emirati Arabi Uniti e Qatar. Questi numeri testimoniano la vitalità del settore, ma soprattutto la capacità della manifestazione di intercettare le evoluzioni del mercato e i suoi protagonisti.

LE GRANDI SFIDE DELLA SICUREZZA

Sicurezza 2025 proporrà un nuovo format verticalizzato su tre giornate tematiche, pensato per rispondere alle esigenze dei diversi segmenti del comparto. Una impostazione che fa della fiera una piattaforma di riferimento per il confronto e l'aggiornamento professionale. Tra i contenuti, spiccano la digitalizzazione, la cybersecurity, l'uso crescente dell'intelligenza artificiale, l'integrazione tra tecnologie e la personalizzazione delle soluzioni: le aziende non offrono più solo prodotti, ma si propongono come partner consulenziali, che - ascoltate le esigenze dei clienti - progettano impianti "su misura" e modulabili. Il 19 novembre aprirà il Cyber Day con incontri ed eventi focalizzati sulla crescente convergenza di minacce fisiche e digitali, il ruolo strategico e trasversale della cybersecurity, le strategie operative per proteggere la catena del valore dell'intera supply chain e l'impatto sul mercato- e sulle aziende - delle nuove direttive europee NIS 2 e CER. Il 20 novembre sarà, invece, la volta del Security Day. Un primo focus approfondirà l'applicazione di tecnologie in situazioni ad alto rischio in settori come trasporti, finanza, grandi eventi, beni culturali. Stiamo parlando di soluzioni integrate per videosorveglianza, controllo accessi, antintrusione, Ai comportamentale e interoperabilità dei sistemi. Uno spazio sarà dedicato al settore bancario e al retail, con focus su modelli innovativi come Bank-in-Shop e Cash BAI, che uniscono sicurezza fisica e digitale per la gestione del contante.

>>> segue a pagina 6

GOLFARELLI EDITORE
INTERNATIONAL GROUP

Colophon

Direttore onorario
Raffaele Costa

Direttore responsabile
Marco Zanzi
direzione@golfarellieditore.it

Redazione
Lucrezia Antinori, Tiziana Bongiovanni, Silvia Brundu, Eugenia Campo di Costa, Cinzia Calogero, Anna Di Leo, Alessandro Gazzo, Cristiana Golfarelli, Simona Langone, Leonardo Lo Gozzo, Michelangelo Marazzita, Guia Montefamelio, Marcello Moratti, Michelangelo Podestà, Desna Ruscica, Debora Stampone, Giuseppe Tatarella

Relazioni internazionali
Magdi Jebreal

Hanno collaborato
Ginevra Cavalieri, Gaetano Gemiti, Bianca Raimondi, Guido Anselmi, Angelo Maria Ratti, Fiorella Calò, Francesca Druidi, Francesco Scopelliti, Lorenzo Fumagalli, Gaia Santi, Maria Pia Telese

Sede
Tel. 051 228807 - Piazza Cavour 2
40124 - Bologna - www.golfarellieditore.it

Relazioni pubbliche
Via del Pozzetto, 1/5 - Roma

Tiratura complessiva: 60.000 copie

Supplemento a Dossier-Registrazione Tribunale di Bologna n. 7578/05 del 22/09/2005

>> continua dalla prima pagina

Un Paese meno vulnerabile

Autenticazione multi-fattore, crittografia dei dati in transito e a riposo, backup isolati. Sono alcune delle precauzioni consigliate da Nunzia Ciardi per rendere i nostri ecosistemi infrastrutturali meno vulnerabili ai cyber-attacchi

Portali della pubblica amministrazione, siti istituzionali, testate giornalistiche, sistemi di trasporto, banche e, in misura crescente, infrastrutture sanitarie e industriali. Su questi obiettivi, ad alta visibilità e valore simbolico, si concentrano le offensive cyber dirette l'anno scorso all'Italia. Al quinto posto mondiale, secondo il Y-Report 2025 di Yarix (Var Group), tra i Paesi colpiti da attacchi di matrice hacktivista. «L'intento principale non è tanto economico- spiega Nunzia Ciardi, vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale- quanto dimostrativo: ottenere attenzione mediatica, diffondere messaggi ideologici o destabilizzare la fiducia dei cittadini nelle istituzioni».

Quali punti deboli sfruttano per raggiungere tale scopo?

«I gruppi hacktivisti utilizzano tecniche relativamente semplici ma ad alto impatto comunicativo, come attacchi DDoS e defacement, spesso coordinati con campagne di disinformazione. Sfruttano debolezze strutturali diffuse- servizi esposti, sistemi non aggiornati, credenziali deboli e catene di fornitura non protette- che ampliano la superficie d'attacco agli ecosistemi digitali più complessi e interconnessi».

Tra i più vulnerabili agli attacchi informatici c'è quello sanitario. Perché i dati relativi alla nostra salute fanno così gola ai cyber criminali?

«I dati sanitari rappresentano una delle informazioni più preziose nel dark web: sono completi, difficilmente modificabili e collegano identità, patologie e informazioni finanziarie. Per i criminali valgono decine di volte più delle carte di credito perché consentono furti d'identità, estorsioni e sofisticate truffe assicurative. Inoltre, gli ospedali e le Asl si trovano a gestire sistemi informatici stratificati nel tempo e spesso basati su tecnologie obsolete. In questi contesti, la continuità operativa non è solo una questione di efficienza organizzativa, ma può incidere direttamente sulla salute e sulla vita stessa dei pazienti. È quindi comprensibile che, in molte circostanze, la priorità venga data alla funzionalità e alla disponibilità dei sistemi, anche se purtroppo ciò può penalizzare la sicurezza informatica».

Attraverso quali strumenti si possono tutelare?

«Servono strategie di sicurezza mirate, in grado di coniugare efficacemente la protezione informatica con le garanzie di continuità operativa. Bisogna investire nella resilienza digitale: aggiornamento e segmentazione delle reti, autenticazione multi-fattore, crittografia dei dati in transito e a riposo, backup isolati, formazione del personale e soprattutto monitoraggio continuo, per rilevare precocemente anomalie e contenere l'impatto di eventuali violazioni».

L'impiego avanzato dell'intelligenza artificiale è cruciale per la difesa cibernetica. Che aiuto può dare e, per contro, a quali nuovi pericoli presta il fianco?

«L'la consente oggi di analizzare enormi quantità di dati in tempo reale, individuare pattern anomali e riconoscere minacce ancora sconosciute con una rapidità impossibile per l'uomo. Supporta le attività di threat hunting, risposta automatizzata e protezione predittiva, migliorando la resilienza complessiva dei sistemi. Tuttavia, l'la è anche un'arma a doppio taglio: gli stessi algoritmi possono essere manipolati, avvelenati nei dati di addestramento o sfruttati per generare attacchi più sofisticati e difficili da attribuire. Inoltre, la crescente dipendenza da modelli e piattaforme non sempre sviluppati o controllati a livello nazionale espone a nuovi rischi di vulnerabilità sistemica, di sovranità tecnologica e di affidabilità delle decisioni automatizzate».

Avete siglato un accordo con ASI per rafforzare la cybersicurezza nel settore spaziale e aerospaziale. In che iniziative congiunte di tradurrà?

«L'accordo è una tappa importante nella strategia italiana che mira a proteggere l'intera catena spaziale italiana, dalla progettazione fino all'operatività orbitale. Le iniziative congiunte prevedono, tra l'altro, programmi di formazione specializzata e training per il personale tecnico delle infrastrutture spaziali; scambio informativo e intelligence condivisa sulle minacce emergenti; campagne coordinate di sensibilizzazione e comunicazione per l'ecosistema spaziale nazionale; e lo sviluppo e diffusione di best practice, in particolare in ambito crittografia avanzata e metodologie di sicurezza come lo Zero Trust e soluzioni post-quantum».

Nunzia Ciardi, vicedirettore generale dell'ACN, Agenzia per la Cybersicurezza Nazionale

Costruire e rendere accessibile una cultura della sicurezza informatica è un presupposto fondamentale per rafforzarla. Cosa avete in corso e in serbo come ACN per raggiungere questo obiettivo?

«Oggi la tecnologia permea ogni gesto quotidiano, ma la coscienza dei rischi e dei comportamenti corretti non ancora. La vera resilienza di un Paese, invece, nasce proprio da una cyber-hygiene diffusa e quotidiana che diventi abitudine e non eccezione. Come ACN, lavoriamo per far sì che la sicurezza informatica non sia percepita come un obbligo tecnico o un adempimento burocratico, ma come un valore culturale condiviso, parte integrante dell'identità digitale del Paese. Promuoviamo programmi di sensibilizzazione, percorsi formativi e collaborazioni con scuole, università, enti pubblici, imprese e organizzazioni della società civile, affinché la conoscenza e la responsabilità digitale diventino strumenti di cittadinanza attiva».

• GG

«BISOGNA INVESTIRE NELLA RESILIENZA DIGITALE: AGGIORNAMENTO E SEGMENTAZIONE DELLE RETI, AUTENTICAZIONE MULTI-FATTORE, CRITTOGRAFIA DEI DATI IN TRANSITO E A RIPOSO, BACKUP ISOLATI, FORMAZIONE DEL PERSONALE E SOPRATTUTTO MONITORAGGIO CONTINUO, PER RILEVARE PRECOCEMENTE ANOMALIE E CONTENERE L'IMPATTO DI EVENTUALI VIOLAZIONI»

MIBA, una piattaforma internazionale unica

«Mettiamo in relazione edilizia, impiantistica, sicurezza e mobilità verticale, creando un ecosistema unico dove innovazione e sostenibilità si rafforzano a vicenda». Paola Sarco commenta l'edizione 2025 di MIBA, dove non manca la security

Punto di riferimento europeo per il settore security & fire, Sicurezza- che come sappiamo si terrà dal 19 al 21 novembre a Fiera Milano- si inserisce all'interno di MIBA- Milan International Building Alliance, il format che riunisce, in un unico ecosistema, quattro manifestazioni leader nei rispettivi ambiti, che rappresentano l'intera filiera del costruito. Sicurezza si affianca, infatti, a GEE- Global Elevator Exhibition, MADE Expo, Smart Building Expo, che raccontano l'evoluzione di edifici e città, attraverso materiali, tecnologie, soluzioni e impianti all'avanguardia. I numeri sono significativi: più di 1.250 aziende da 38 Paesi, otto padiglioni, oltre 100 eventi e una importante rappresentatività estera pari al 28 per cento del totale. «MIBA è il frutto di un percorso di crescita che ha unito mercati e manifestazioni un tempo separati, creando un sistema capace di trasformare innovazione tecnologica e know-how professionale in opportunità concrete di business», spiega Paola Sarco, amministratore delegato di Made Eventi e Head of Building & Industry Exhibitions di Fiera Milano. «Con una offerta di oltre 1.250 aziende, sempre più rappresentativa e internazionale, MIBA offre una piattaforma unica dove numeri, progetti e idee si traducono in soluzioni reali per la riqualificazione e la costruzione sostenibile degli edifici».

Perché l'integrazione è la chiave vincente per affrontare la sfida della sostenibilità e guidare la transizione ecologica e digitale del patrimonio edilizio e urbano del nostro Paese?

«L'integrazione è la chiave per affrontare in modo concreto la transizione ecologica e digitale. Con MIBA mettiamo in relazione edilizia, impiantistica, sicurezza e mobilità verticale, creando un ecosistema unico dove innovazione e sostenibilità si rafforzano a vicenda. Solo una visione condivisa tra questi ambiti può generare edifici e città davvero intelligenti, efficienti e sostenibili».

Sono quattro le grandi sfide comuni: sostenibilità, digitalizzazione, sicurezza e applicazione dell'intelligenza artificiale. Come le quattro fiere affrontano queste istanze?

«Dalle quattro manifestazioni emerge una direzione condivisa: costruire un ambiente edificato più efficiente, sicuro e intelligente. L'innovazione si traduce in materiali sostenibili, edifici connessi, sistemi predittivi di manutenzione e soluzioni basate sull'intelligenza artificiale. È una trasformazione profonda che unisce digitale e sostenibilità, rendendo l'edilizia protagonista della transizione ecologica».

Come descriverebbe, in termini di potenzialità e criticità, l'evoluzione di edifici e città?

«Edifici e città stanno diventando organismi dinamici, capaci di dialogare con chi li abita e con l'ambiente circostante. La grande potenzialità è la possibilità di coniugare tecnologia e sostenibilità per migliorare la qualità della vita. La criticità, invece, sta nel saper governare questa trasformazione con competenze, visione e responsabilità condivisa».

Realizzato dal Politecnico di Milano, partner scientifico dell'evento, il Terzo Osservatorio MIBA propone una analisi relativa al triennio 2025-2027 sulle prospettive di sviluppo del comparto edilizio derivanti dal New European Bauhaus (NEB) della Ue e dai suoi principi cardine: sostenibilità, bellezza, inclusività. Quale dovrebbe essere l'impatto sull'edilizia sostenibile in Italia e sulle quattro fiere del Miba? Come verrebbero attivati gli investimenti NEB-oriented?

«Il New European Bauhaus rappresenta un'opportunità straordinaria per ridefinire il modo in cui pensiamo e realizziamo gli spazi del vivere. Non si tratta solo di un progetto estetico o ambientale, ma di una visione integrata che unisce sostenibilità, bellezza e inclusività. L'Osservatorio MIBA, realizzato con il Politecnico di Milano, stima che nel triennio 2025-2027 i progetti NEB-oriented possano mobilitare oltre 20 miliardi di euro in Europa, di cui 2,5 miliardi in Italia, con un effetto moltiplicatore molto significativo sull'intera filiera del costruito. Per le quattro manifestazioni di MIBA, questo scenario si traduce in una spinta reale verso l'edilizia sostenibile, la digitalizzazione dei processi e l'integrazione tra tecnologie e sicurezza. È un percorso che mette al centro la qualità dell'abitare e la rigenerazione urbana, trasformando l'innovazione in valore per i territori. Gli investimenti NEB-oriented, se ben indirizzati, potranno accelerare il rinnovo del patrimonio edilizio italiano, favorendo soluzioni architettoniche più efficienti, accessibili e rispettose dell'ambiente. In una parola: una nuova cultura del costruire, europea e condivisa».• **Francesca Druidi**

Paola Sarco, ad Made Eventi e Head of Building & Industry Exhibitions di Fiera Milano

LE OPPORTUNITÀ DEL NEB

In base al Terzo Osservatorio MIBA del Politecnico di Milano, il settore della security, al centro della proposta di SICUREZZA, rappresenta una componente trasversale dei progetti NEB. La spinta verso edifici intelligenti e sostenibili implica l'integrazione di soluzioni di sicurezza avanzate: sistemi IoT di rilevazione precoce incendi, compartimentazioni intelligenti, sensori ambientali, sorveglianza passiva e tecnologie Cpted (Crime Prevention Through Environmental Design). Con una quota stimata del 5,5 per cento sul valore complessivo dei finanziamenti NEB, il giro d'affari annuale europeo per la sicurezza di circa 1,2 miliardi di euro nel periodo 2025-2027. In questo caso il valore atteso per l'Italia è pari a circa 150 milioni di euro.

Le frontiere della protezione fisica e digitale

Una struttura tematica verticale, il focus sui giovani e tre parole chiave: integrazione, cyber-resilienza e customizzazione. Sicurezza si conferma un laboratorio dell'innovazione in ambito security & fire

Droni, nuovi sistemi di videosorveglianza e controllo accessi integrati con l'Ai, nuovi impianti antincendio ad alta sensibilità, sistemi wireless per rilevazione fumi e gas, piattaforme per il controllo remoto e la gestione predittiva della manutenzione e del monitoraggio. I trend e gli sviluppi innovativi in tutti i comparti della security & fire- videosorveglianza, antincendio, controllo accessi, sicurezza passiva- saranno al centro della nuova edizione di Sicurezza, che si terrà dal 19 al 21 novembre a Fiera Milano. Cresce la manifestazione, rafforzando il suo posizionamento globale. Aumentano, infatti, la superficie espositiva (+18 per cento rispetto al 2023) e gli espositori esteri, che rappresentano oggi il 32 per cento del totale. A inizio ottobre, erano già 340 le aziende confermate, provenienti da 26 Paesi, con importanti ritorni da parte di brand assenti da alcune edizioni e nuovi ingressi di rilievo: non mancheranno i principali produttori europei-Francia, Germania, Regno Unito e Spagna-e la Cina, peso massimo a livello mondiale. Grazie a ICE- Agenzia, gli espositori incontreranno in appuntamenti one to one più di 100 top hosted buyer provenienti da 32 Paesi, con le maggiori delegazioni da Medio Oriente e Nord Africa, interessanti bacini di sbocco per le tecnologie in mostra, in particolare da Egitto, Tunisia, Emirati Arabi Uniti e Qatar. Questi numeri testimoniano la vitalità del settore, ma soprattutto la capacità della manifestazione di intercettare le evoluzioni del mercato e i suoi protagonisti.

LE GRANDI SFIDE DELLA SICUREZZA

Sicurezza 2025 proporrà un nuovo format verticalizzato su tre giornate tematiche, pensato per rispondere alle esigenze dei diversi segmenti del comparto. Una impostazione che fa della fiera una piattaforma di riferimento per il confronto e l'aggiornamento professionale. Tra i contenuti, spiccano la digitalizzazione, la cybersecurity, l'uso crescente dell'intelligenza artificiale, l'integrazione tra tecnologie e la personalizzazione delle soluzioni: le aziende non offrono più solo prodotti, ma si propongono come partner consulenziali, che - ascoltate le esigenze dei clienti - progettano impianti "su misura" e modulabili. Il 19 novembre aprirà il Cyber Day con incontri ed eventi focalizzati sulla crescente convergenza di minacce fisiche e digitali, il ruolo strategico e trasversale della cybersecurity, le strategie operative per proteggere la catena del valore dell'intera supply chain e l'impatto sul mercato- e sulle aziende - delle nuove direttive europee NIS 2 e CER. Il 20 novembre sarà, invece, la volta del Security Day. Un primo focus approfondirà l'applicazione di tecnologie in situazioni ad alto rischio in settori come trasporti, finanza, grandi eventi, beni culturali. Stiamo parlando di soluzioni integrate per videosorveglianza, controllo accessi, antintrusione, Ai comportamentale e interoperabilità dei sistemi. Uno spazio sarà dedicato al settore bancario e al retail, con focus su modelli innovativi come Bank-in-Shop e Cash BAI, che uniscono sicurezza fisica e digitale per la gestione del contante. Altro focus sarà il modello di sicurezza usato per i grandi eventi internazionali, come i prossimi Giochi olimpici invernali di Milano Cortina 2026. Verranno analizzate anche le figure professionali emergenti richieste dal mercato, come i Travel Security Manager o i Cultural Security Manager, capaci di coniugare competenze tecnologiche, organizzative e normative nei loro specifici settori.

IL 21 NOVEMBRE SARÀ IL JOB IN SECURITY DAY, UNA GIORNATA DEDICATA ALL'INCONTRO TRA SCUOLE, ITS E AZIENDE DEL SETTORE SICUREZZA PER RIDURRE LA DISTANZA TRA FORMAZIONE E LAVORO, RISPONDENDO ALL'ESIGENZA DELLE IMPRESE DI PERSONALE ADEGUATAMENTE PREPARATO

RIFLETTORI SULLA FORMAZIONE

Il 21 novembre sarà, infine, il Job in Security Day, una giornata dedicata all'incontro tra scuole, Its e aziende del settore sicurezza per ridurre la distanza tra formazione e lavoro, rispondendo all'esigenza delle imprese di personale adeguatamente preparato. Il Progetto EDU guarda a questa necessità con attività mirate: presentazioni aziendali, colloqui brevi, workshop e spazi di dialogo tra studenti, docenti e imprese. Tutti gli eventi formativi della manifestazione si terranno all'interno della Cyber & Security Arena, lo spazio polifunzionale in cui si alterneranno talk, casi studio, dimostrazioni e tavole rotonde con la partecipazione di esperti, aziende leader, enti pubblici e associazioni di categoria. A completare l'offerta formativa, i Security Talk organizzati dalle associazioni di categoria, con focus su normative, trend e scenari evolutivi, e i podcast di Assiv che offriranno approfondimenti su tecnologie, formazione, sinergie pubblico-privato e innovazione nel comparto della vigilanza privata.

• **FD**

Proteggersi dai Ransomware

TG Soft Cyber Security Specialist protegge le Pmi, e non solo, dagli attacchi informatici anche zero day

TG Soft dal 1992 sviluppa il software antivirus VirIT per Ms-DOS che con l'avvento del Windows® trova la sua evoluzione dal 1998 nella suite Vir.IT eXplorer PRO AntiVirus – AntiSpyware – AntiMalware e dal 2012 anche AntiRansomware.

I test internazionali a cui è sottoposta la suite Vir.IT eXplorer PRO

Negli anni Vir.IT eXplorer PRO è riuscito ad ottenere non solamente riconoscimenti a livello nazionale ma anche, e soprattutto, a superare test internazionali che ne hanno valutato l'efficacia e l'efficienza, tra i quali:
OPSWAT® (San Francisco US), dal 2012 è stato inserito nella piattaforma Multimotore MetaDefender MAX in qualità di partner tecnologico con certificazioni progressive: BRONZE (2012); SILVER (2016); GOLD (2020-06); PLATINUM (2020-09);
VB100® Virus Bulletin (London GB) dal 2016 ha ottenuto oltre 40 certificazioni, raggiungendo il Grado A nel luglio 2025;
ICSALabs (International Computer Security Association, divisione indipendente di Verizon®), Vir.IT eXplorer PRO ottiene il premio "5-Year Excellence in Testing Security Award Winner for 2021", in quanto ha superato con continuità dal 2016-10 i test "Certified Anti Virus Desktop/Server", aumentando l'elevato standard di qualità delle proprie tecnologie.

Le partnership tecnologiche internazionali del motore di scansione della suite Vir.IT eXplorer PRO

La prima collaborazione internazionale è nata nel 2012 con OPSWAT® che ha riconosciuto il motore di scansione di Vir.IT eXplorer partner tecnologico della piattaforma multimotore MetaScan prima e Meta Defender MAX poi.
Dal 2019 il motore di Vir.IT eXplorer PRO viene testato periodicamente per essere riconosciuto dal centro sicurezza di Windows® (MVI Microsoft Virus Initiative).
Nel 2021 ottiene il riconoscimento come partner tecnologico in Virus TOTAL, entrando come unico motore di scansione proprietario totalmente sviluppato in Italia.
Grazie all'attività di ricerca & sviluppo coordinate dall'ingegnere Gianfranco Tonello, in rappresentanza di TG Soft, è stato accreditato come membro di Wild List organizzazione che si è occupata per decenni di catalogare i virus/malware realmente circolanti a livello mondiale.

Enrico e Gianfranco Tonello di TG Soft

Gli attacchi Ransomware, un flagello che può essere evitato grazie al giusto approccio tecnologico

Tra un riconoscimento e l'altro della suite Vir.IT eXplorer PRO, il team di ricerca e sviluppo ha dovuto, suo malgrado, confrontarsi con tante nuove tipologie di minacce, tra cui la più insidiosa e pericolosa è il Ransomware cioè quel Malware che è in grado di cifrare i dati degli utenti e richiedere un riscatto in denaro (generalmente in Crypto Valute, BitCoin ma non solo) per la loro decifratura, questo lo ha portato a cercare un sistema progressivamente sempre più efficace ed efficiente per proteggere da questi attacchi estremamente insidiosi.
Vir.IT Backup è un sistema di backup specificatamente progettato per resistere agli attacchi Ransomware. Il team di ricerca e sviluppo che realizza la suite Vir.IT eXplorer PRO, nel 2013 ha iniziato a sviluppare un sistema di backup in grado di proteggere i file di dati dell'utente dalla cifratura. Si tratta di Vir.IT Backup che è stato integrato nella suite Vir.IT eXplorer PRO e presentato a vari eventi fieristici a partire dal 2014-04. Le tecnologie che stanno alla base di Vir.IT Backup permettono di proteggere i volumi di backup dei file di dati dell'utilizzatore da qualsiasi attacco di cifratura e/o cancellazione.

Oltre il "semplice" ripristino dei dati dai volumi di backup

Il team di ingegneri e ricercatori di TG Soft ha analizzato in modo sempre più accurato alcune delle principali famiglie di Ransomware per individuarne i comportamenti comuni e provare a costruire un algoritmo in grado di riconoscere i processi di cifratura in atto e quindi bloccarli evitando che possano criptare i file di dati, tutto ciò nel più breve tempo possibile dall'individuazione di un processo di sospetta cifratura in atto.
Si è riusciti a stabilizzare un sistema di riconoscimento di un processo di cifratura / attacco Ransomware nell'intorno dei primi 100 millisecondi e salvaguardare la maggior parte dei file dalla cifratura. Dagli ultimi test effettuati su attacchi Ransomware reali presenti in natura, mediamente, vengono salvati non meno del 99,87 per cento dei file di dati ove sia presente la suite Vir.IT eXplorer PRO.

Servizi di cyber security avanzati per la protezione degli Endpoint

TG Soft dal 2023 ha sviluppato un sistema di monitoraggio degli EndPoint, attraverso una piattaforma in Cloud che permette di monitorare comodamente da un unico panello web tutti gli Endpoint ove è installato Vir.IT eXplorer PRO, denominato CLOUD Console.
Con Vir.IT CLOUD Console + EDR (Endpoint Detection & Response) sono inoltre disponibili una serie di informazioni sulle anomalie dei processi e quant'altro che permettono di rilevare situazioni sospette e intervenire per prevenire attacchi informatici di varia natura.
Inoltre rendiamo disponibile un servizio di supporto SOC remotizzato, da parte di un Team di ingegneri, analisti e ricercatori di Virus & Malware informatici, che vi affiancherà nella protezione della vostra rete IT.
Potersi avvalere di un'azienda italiana i cui fondatori dal 1990 analizzano virus & malware, con una consolidata esperienza oramai da 35 anni è un plus da non sottovalutare poiché l'esperienza non si costruisce dall'oggi al domani. •BG

RECUPERARE I FILE CIFRATI NELLA FASE INIZIALE DELL'ATTACCO

Per i file che dovessero essere stati cifrati nella fase iniziale dell'attacco, cioè quello 0,13 per cento, sono state integrate delle tecnologie di recupero/ripristino che possono arrivare a recuperare quei pochi file cifrati nella fase iniziale dell'attacco, fino al 100 per cento. Si tratta di un sistema automatico di recupero così da poter decifrare i file dopo la conclusione dell'attacco.
Backup On-The-Fly è un sistema, anch'esso automatico, che permette di recuperare/ripristinare le tipologie di file più comuni e farne il ripristino senza perdere nessuna modifica effettuata fino al momento dell'attacco Ransomware di cifratura. Ultimo, ma non ultimo, permette di andare a recuperare i file di dati cifrati nella fase iniziale dell'attacco dai "volumi" protetti da Vir.IT Backup. Tutte queste tecnologie sono integrate nelle suite Vir.IT eXplorer PRO AntiVirus + AntiSpyware + AntiMalware + AntiRansomware basato su tecnologie euristico-comportamentali.