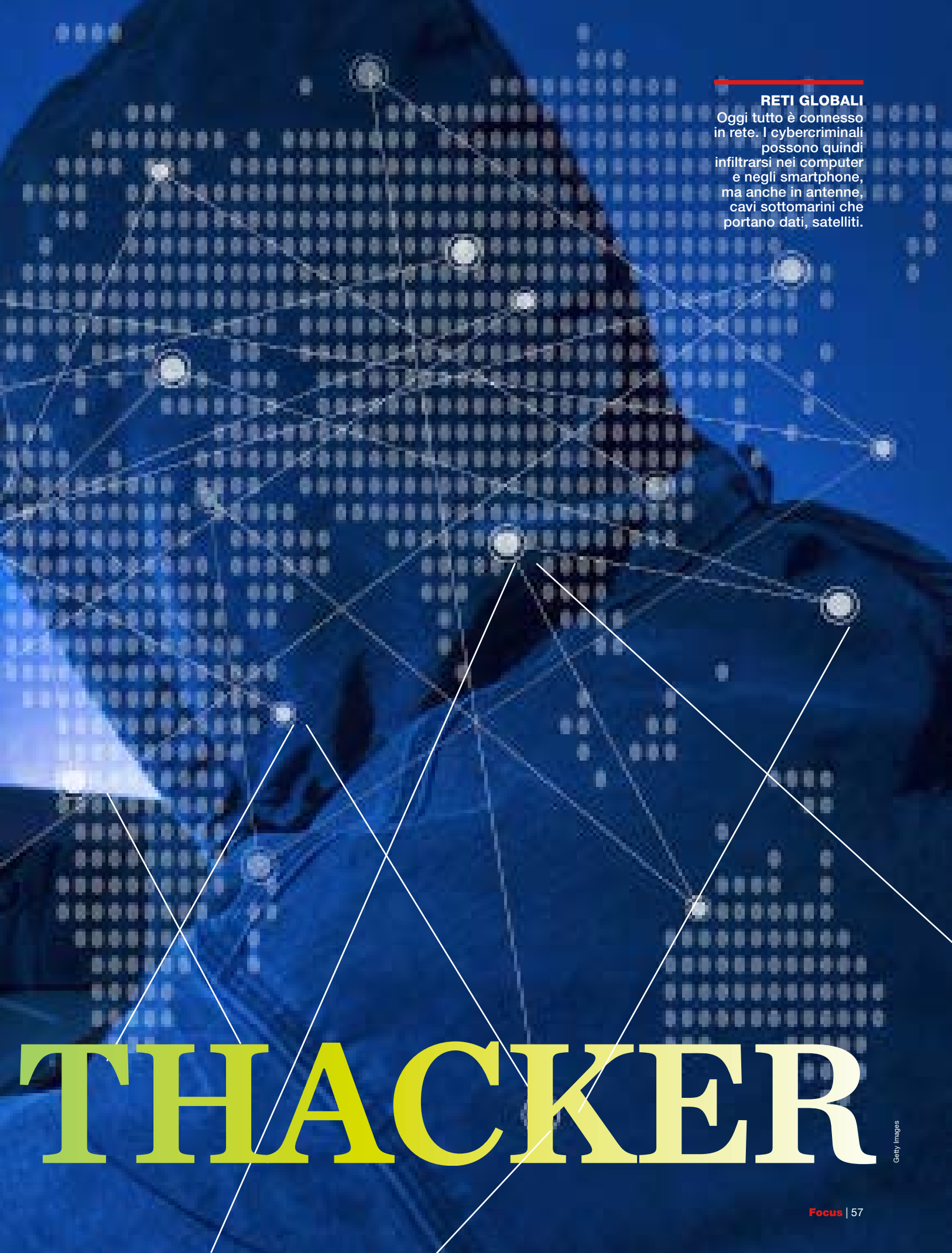
Cronaca di una giornata nel Global Security Operation Centre di Leonardo, dove si contrastano i **cyber criminali**. Ogni secondo si intercettano e setacciano 115mila azioni sospette.

di Marco Consoli

CONTRAT



RETI GLOBALI
Oggi tutto è connesso in rete. I cybercriminali possono quindi infiltrarsi nei computer e negli smartphone, ma anche in antenne, cavi sottomarini che portano dati, satelliti.

THACKER

Getty Images

La disperata richiesta d'aiuto arriva alle quattro e trentacinque del mattino. Un gruppo di hacker malevoli ha bloccato una grande azienda manifatturiera: le macchine, collegate alla rete, non funzionano più e i criminali chiedono un riscatto per far ripartire la produzione. Prima che il blocco provochi ingenti danni economici, il team di esperti informatici inviato per risolvere il problema individua la causa: un dipendente dell'amministrazione ha ricevuto via email una fattura, e per leggere il file ha attivato involontariamente un programma nascosto che ha scaricato sul suo pc un software in grado di "infettare" la rete aziendale. Mentre i soccorritori attraverso copie di **backup** (*v. riquadro nell'ultima pagina*) riavviano l'impianto, l'investigazione identifica come evitare il ripetersi di situazioni simili: formare gli impiegati e stabilire accessi limitati a pochissime persone ai sistemi critici.

MILIONI DI MINACCE ALL'ANNO

Questa è solo una delle crisi affrontate dal Global Security Operation Centre (Soc) di Leonardo, che dal 2014 opera notte e giorno a Chieti per difendere istituzioni, aziende private e infrastrutture strategiche: 7.000 reti e 100.000 utenti cyber in 130 Paesi del mondo. «Qui monitoriamo e analizziamo ogni anno 4,7 milioni di minacce», spiega Aldo Sebastiani, responsabile del Soc di Leonardo, dove siamo venuti per capire come si garantisce la sicurezza del cyberspazio.

Per comprendere cosa vuol dire questo termine, abbiamo chiesto aiuto a Luigi Martino, tra i massimi esperti in Italia e professore di cybersecurity dell'Università di Firenze con numerose esperienze all'estero: «Si pensa che il cyberspazio sia limitato al suo livello logico-sintattico cioè a Internet, ma ne è solo una sua parte, perché bisogna considerare anche le infrastrutture fisiche come antenne, satelliti, cavi sottomarini, router, oltre allo spettro elettromagnetico, perché anche il wifi o la rete 5G della telefonia possono essere usati per veicolare le informazioni». In tutta la rete, «esiste un livello sociale, fatto da persone che utilizzando varie identità interagiscono con le macchine». E dato che ormai da anni individui, aziende, nazioni hanno affidato alla rete tutte le informazioni di ogni aspetto della vita del genere umano, quei dati hanno acquisito un valore tale da far gola a esperti in grado di penetrare nei sistemi informatici privati. «Gli attaccanti possono sottrarre dati per conto di governi», spiega Sebastiani, «tentare di ottenere un riscatto, come con i cosiddetti attacchi **ransomware**, o in alcuni casi agire da hacktivist, cioè attivisti, magari per contrastare Stati dittatoriali o aziende che attuano pratiche illegali».

ATTACCHI IN AUMENTO

Il recente rapporto del Clusit, l'Associazione Italiana per la Sicurezza Informatica, ha registrato nel primo semestre dello scorso anno 1.141 attacchi gravi a livello globale (+8,4% rispetto al primo semestre 2021). Il 78,4% sono azioni di cybercrimine, il 13,5% di spionaggio e sabotaggio, il 5% ha carattere bellico, il 3,1% è attivismo. 190 attacchi al mese possono sembrare pochi, ma le conseguenze sono spesso disastrose: «Basti ricordare nel

Getty Images

SU TUTTI I FRONTI
Le antenne per le telecomunicazioni sono un possibile obiettivo per gli hacker. A destra, una pompa a secco in Virginia (Usa) dopo un attacco informatico al colosso del gas Colonial Pipeline verificatosi nel maggio del 2021.

AFP via Getty Images

SALA OPERATIVA
Qui e a destra, due immagini del Global Security Operation Centre di Leonardo, a Chieti. La struttura monitora oltre 7.000 reti in 130 Paesi del mondo.

IL FATTORE UMANO

Se la tecnologia protegge dagli attacchi malevoli, spesso a essere fallace è il fattore umano: basta un clic sbagliato per trovarsi il pc o l'infrastruttura tecnologica di un'intera società invasa da malware. È per questo che Leonardo ha creato la Cyber & Security Academy, un polo di eccellenza per la formazione del personale, oltre che per il costante aggiornamento degli stessi addetti interni alla sicurezza. Il cuore di questo centro è costituito da due piattaforme, chiamate Cyber Range e Cyber Trainer, che simulano scenari operativi di minaccia e crisi attuati su gemelli digitali (i cosiddetti digital twin) di migliaia di nodi e centinaia di reti, sistemi e applicazioni da proteggere, e sfruttano come strumento didattico i principi della gamification, che consente di affrontare operazioni complesse utilizzando dinamiche di gioco a squadre a team multipli con decine di utenti per squadra.

Viste le tante implicazioni, oltre agli informatici ci sono criminologi, psicologi ed esperti di **geopolitica**

2021 il caso del ransomware che ha mandato in tilt il sistema sanitario e l'hub nazionale dei vaccini Covid della regione Lazio», dice Martino, «oppure l'attacco simile che ha tenuto in scacco per cinque giorni il colosso americano dei gasdotti e oleodotti Colonial Pipeline».

«I danni possono essere non solo economici», precisa Sebastiani. «L'anno scorso, in Florida, alcuni hacker hanno tentato di aumentare il livello di idrossido di sodio (solitamente usato per bilanciare il pH dell'acqua, *ndr*) nell'acquedotto di Oldsmar, minacciando di avvelenarne i cittadini. Il problema è che una volta per sabotare un impianto bisognava andare di persona, ma la costante digitalizzazione dei sistemi fisici, che li rende più efficienti, li espone anche alla minaccia cyber».

LE DIVERSE FASI DELLA PROTEZIONE

Per questo, in tutto il mondo strutture come il Soc di Leonardo operano per contrastare queste azioni: «Analizziamo 115mila eventi al secondo», spiega Sebastiani, «grazie all'utilizzo di tecnologie come il SIEM, un correlatore di eventi automatici che evidenzia anomalie, per esempio ripetuti tentativi di accesso a un sistema informatico da un luogo geografico inusuale (un po' come quando Google ci avverte che qualcuno ha avuto accesso alla nostra email da Chicago e noi siamo a Milano, *ndr*), attivando in alcuni casi la supervisione di un essere umano».

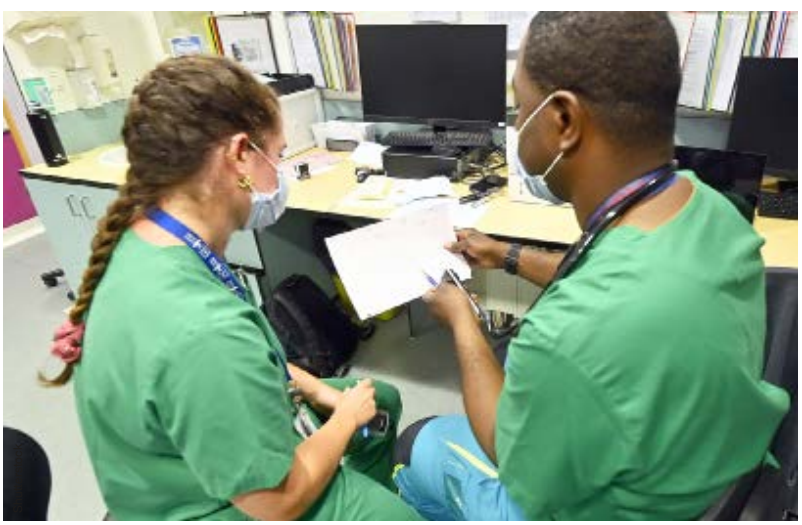
Per capire come funziona il Soc, siamo venuti nella sala operativa dove, di fronte a enormi **videowall,** gli esperti lavorano alle varie fasi del processo di sicurezza: nella prima fase, chiamata Identify, da remoto si mappano la rete e le infrastrutture fisiche del soggetto da difendere, verificando che siano tutti funzionanti, poi in quella di Protect si opera per aumentare la sicurezza dei firewall, le barriere di protezione della rete stessa; nella fase di Detect poi vengono evidenziate potenziali minacce, per esempio quando un server non risponde e potrebbe essere sotto attacco oppure si è collegato a un sito in cui si trovano programmi malevoli: se i software del Soc reputano che non è un falso allarme, il problema è seguito da un analista. Se è confermata l'offensiva cyber, l'incidente viene gestito nelle fasi di Respond & Recovery: qui bisogna caratterizzare il tipo di attacco, capire da dove è entrato, quanto a fondo è penetrato nella rete, se sono stati sottratti dati, bloccati sistemi, e così via. A seconda della gravità della situazione, e se la rete di chi è sotto attacco è conosciuta o meno da Leonardo, il problema si può risolvere da remoto o richiedere l'invio di un team in loco. A questo punto nella cosiddetta "War Room" si cerca di arginare e porre fine all'attacco il prima possibile, ripristinando funzionalità e infrastrutture, gestendo la crisi verso investitori e media e ricostruendo l'evento criminoso per attuare pratiche di difesa più efficaci e, a volte, permettere indagini di polizia. ▶

Shutterstock/Christopher Halloran

I TERMINI TECNICI

1 Backup: copia di sicurezza di un sistema di archiviazione di dati.
2 Ransomware: software malevolo che chiede un riscatto per far funzionare le infrastrutture aziendali.
3 Videowall: enorme display video su cui sono disponibili varie informazioni.
4 Cavallo di Troia: software malevolo nascosto in un altro che sembra utile e innocuo.
5 Quantum computing: disciplina che si occupa dei computer quantistici, molto più veloci perché basati sulle proprietà quantistiche della materia.
6 Malware: software malevolo, in generale.
7 Gamification: utilizzo di meccaniche tipiche del gioco per rendere più divertente e semplice la spiegazione di sistemi complessi.

ATTACCHI AI SERVIZI
Sopra: nel 2022, anche i siti web di 14 aeroporti statunitensi sono stati attaccati. Così come un ospedale belga (a destra).



«Individuare i responsabili, nascosti da tecniche di anonimizzazione, è molto difficile», spiega Martino, «ed è per questo che ormai all'attribuzione tecnica si è sostituita quella strategica, che individua quale gruppo può essere il più interessato a compiere un determinato attacco».

ATTENZIONE AI SOFTWARE DIFFUSI

A margine e in via preliminare rispetto a queste attività si svolge quella importantissima di Cyber Threat Intelligence: «Si raccolgono informazioni pubbliche o private degli attacchi e si analizzano dal punto di vista dello scenario», dice Sebastiani. Il team di esperti di Leonardo scandaglia nella rete circa 40 milioni di elementi unici al mese, per capire possibili minacce per i soggetti protetti. «Per esempio è molto più redditizio per i criminali sfruttare la falla di un software utilizzato da migliaia di aziende, come un server commerciale di posta elettronica, e usarlo come **cavallo di Troia** per inserire software malevoli nelle aziende stesse, piuttosto che penetrare nei sistemi informatici uno alla volta», spiega Sebastiani. Questa attività si ricollega a quella di analisi del rischio, che non riguarda solo l'eventuale fragilità della rete di un'azienda o di un'istituzione, ma valuta anche quanto un particolare dominio (energetico, governativo, militare, relativo ai trasporti ecc.) può essere più esposto in base agli eventi politici, come il recente conflitto tra Russia e Ucraina. Per questo, tra i 165 esperti al lavoro nel Soc di Leonardo, non si trovano solo laureati in discipline scientifiche, ma anche esperti di geopolitica, criminologia, psicologia.

PROSPETTIVE FUTURE

Se il cyberspazio è già un ambiente così complesso e alla mercé di possibili attacchi che riguardano i governi del mondo ma anche tutti noi, quali sono le maggiori criticità e cosa accadrà in futuro? «Di sicuro l'avvento del **quantum computing**, che

I computer quantistici potranno mettere in crisi la **crittografia** su cui si basa la cybersecurity

permetterà capacità di calcolo oggi inimmaginabili, metterà in crisi i sistemi di crittografia odierni su cui si basa la cybersicurezza e obbligherà a proteggersi con sistemi adeguati», afferma Martino. «Il cyberspazio oggi non è più solo uno spazio per la democratizzazione delle informazioni, detenute ormai da attori privati, ma è un ambiente piegato alle dinamiche politico-militari. In questa chiave, l'utilizzo sempre maggiore dell'Intelligenza Artificiale permetterà risposte più veloci agli attacchi, ma nel contesto militare porrà il problema di stabilire se una reazione che può provocare un'escalation possa essere presa da un software o debba essere presa dagli esseri umani. Di recente, infine, abbiamo visto un assaggio del nuovo scenario bellico, con l'intersezione tra cyberspazio e spazio extra atmosferico: la Russia prima di invadere l'Ucraina ha accecato i sistemi di Viasat, che funge da provider dei sistemi satellitari ucraini. Questo ci annuncia quale sarà il nuovo campo di battaglia: lo spazio e i relativi asset, ovvero i satelliti e tutti i sistemi di controllo a terra». Tutte sfide per cui il Global Security Operation Centre di Leonardo si sta preparando.