ARRIVANO GLI 007 DI NAPOLI

L'italiana Innovery controlla in segreto le difese digitali delle aziende. Come al cinema ma è legale

di **ALESSIO LANA**

La telecamera da film
Grazie al diametro di pochi millimetri, la telecamera endoscopica si insinua ovunque offrendo immagini in HD anche sullo schermo dello smartphone. Le più economiche costano una decina di euro

Il ladro arriva al caveau della banca, copre la telecamera di sicurezza con una fotografia e scappa con il bottino. Abbiamo visto (e letto) innumerevoli volte una scena del genere, fatto spallucce e pensato che fosse solo fiction. E invece c'è chi lo fa davvero. E legalmente. Innovery è una delle poche realtà italiane specializzate in infiltrazione fisica delle aziende, una miscela di spy story e tecnologia con un pizzico di *Ocean's Eleven* e una spruzzatina di Arsenio Lupin.

Nata a Napoli vent'anni fa ma con filiali sparse in Italia, Messico e Spagna, l'impresa viene assoldata dalle aziende per mettere alla prova le loro difese fisiche e digitali. Per un prezzo che può andare da diecimila euro a ben oltre i centomila, un imprenditore può chiedere di penetrare la propria sede fino allo studio dell'amministratore delegato (l'hanno fatto davvero, con tanto di foto sulla poltrona dirigenziale), di compromettere il caveau di una banca o rubare dati sensibili dalla rete aziendale.

Volendo operano anche attacchi digitali ma sono quelli fisici ad apparire più affascinanti. L'operazione parte come nei migliori film di spionaggio. Definita la richiesta del committente, il dipartimento «red team» (vocabolo militare che indica una squadra offensiva) si mette all'opera: studia un piano di penetrazione e poi mette in campo le «spie».

Il primo passo, infatti, prevede ricognizioni fisiche intorno all'obiettivo per vedere se ci sono guardie di sicurezza o telecamere di sorveglianza, quali sono gli accessi del personale, i loro orari di ingresso e di uscita, quand'è la finestra della pausa pranzo. «Questa fase dura diversi giorni e ci alterniamo per evitare che si vedano sempre le stesse facce», racconta il coordinatore del red team, Andrea Bruschi. I dipendenti sono spesso l'anello debole della sicurezza aziendale. Un badge poggiato sul tavolo del ristorante in pausa pranzo per esempio può essere clonato da un Rfid spoofer, un lettore tascabile che la spia cela in una borsa o nello zaino. Questa si avvicina al tesserino e lo copia, magari scegliendone uno con privilegi d'accesso elevati. «In genere sul badge è scritto il nominativo e LinkedIn è fondamentale per identificare le figure chiave dell'azienda», prosegue Bruschi. I dipendenti sono anche coloro che scelgono password semplicissime per entrare nei sistemi digitali e non mancano i casi in cui queste erano scritte direttamente sui Pc magari con foglietti gialli ben evidenti a chiunque passi di lì.

Tra gli altri strumenti di questi 007 ci sono tanti altri oggetti che siamo abituati a vedere solo nei film (e pensavamo funzionassero solo lì). Bruschi mostra degli insospettabili occhiali con microcamera, una telecamera endoscopica (quella flessibile che si infiltra in spazi minuscoli), un rilevatore di cimici che sembra venuto dallo spazio (emette una luce rossa intermittente per scovare le microcamere e rileva anche i trasmettitori Gps). Ecco poi una minuscola chiavetta Usb. In realtà è un microcomputer che simula il comportamento della tastiera: non appena connesso a un Pc permette di impartirgli comandi da remoto come se si fosse fisicamente lì a battere sui tasti.

Perché non dimentichiamoci che l'attività del red team è sempre sotto copertura. Generalmente solo gli amministratori delegati committenti sanno dell'azione in corso e tutti gli altri sono all'oscuro. Ecco quindi che c'è chi si traveste da tecnico della stampante per entrare nell'impresa e usare il cavo di rete del macchinario per connettervi il proprio computer e rubare dati. Oppure chi si camuffa da addetto alle pulizie. In caso si venga scoperti c'è una lettera di manleva che tiene al riparo le «spie» da conseguenze legali (e fisiche) mentre esperti legali redigono dettagliati documenti per tutelare la privacy dei lavoratori e la fedina penale delle «spie».

L'OMBRA DELLE SPIE

Il caso più avvincente però è quello della banca (impossibile saperne il nome, qui tutto è segreto). L'obiettivo era testare il sistema d'allarme del caveau e, come moderni Diabolik, Bruschi e colleghi si sono messi all'opera. I committenti gli hanno permesso di arrivare fino alla grande porta spessa un metro e mezzo: meglio non infiltrarsi di nascosto in un edificio del genere. Era controllata da una centrale d'allarme che andava manomessa. Come fare? Per prima cosa i membri del red team si sono fatti campo libero «confondendo» la videocamera puntata sul caveau. Si sono nascosti nel suo angolo cieco, hanno scattato una foto della stanza vuota, l'hanno stampata e l'hanno messa davanti all'obiettivo con un elastico. Spoiler: ha funzionato. «Erano videocamere a bassa risoluzione e solo un sorvegliante molto attento si sarebbe accorto della differenza», ricorda Bruschi. Poi, grazie al post su Facebook di un installatore, hanno riconosciuto il modello del sistema di sorveglianza (non c'è davvero limite agli strumenti d'infiltrazione), scaricato i manuali e scoperto che questo lanciava allarmi alle guardie tramite sms inviati su rete 2G. Proprio come dei cellulari. A questo punto hanno creato una finta cella telefonica, il sistema si è agganciato ad essa e il gioco è fatto. Ogni allarme veniva ora inviato a Bruschi e soci che, se fossero stati dei ladri, avrebbero avuto via libera per operare sul caveau. Ma lavorando dalla parte dei «buoni» si sono limitati a scattarsi un selfie di fronte a quella grande porta. Missione compiuta.

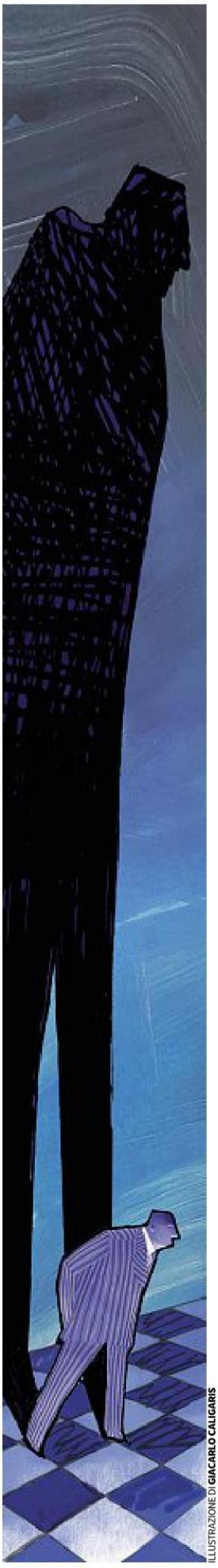

ILLUSTRAZIONE DI GIACARLO CALIGARIS

LOG

GLI RFID SPOOFER CLONANO I BADGE

Realizzabile in casa e venduto anche online per una decina di euro, l'Rfid Spoofer può clonare i badge a distanza. La spia cela il dispositivo in uno zaino o in tasca, si avvicina al tesserino e, grazie a un'antenna, ne carpisce il segnale e quindi il numero identificativo. A questo punto trascrive i dati su una tessera vuota creandone una copia.

GLI OCCHIALI PER REGISTRARE

Sembrano usciti dai giornalini degli anni '70 ma gli occhiali dotati di una o più microcamere sono una realtà. Acquistabili online per qualche decina di euro, possono scattare foto e registrare video in HD, salvarli in memoria o inviarli a un computer remoto. Anche Ray-Ban ne ha realizzato un modello insieme a Meta.

ANCHE I SOCIAL SONO UN'ARMA

Un'efficace intrusione fisica richiede di individuare bene il proprio obiettivo e così LinkedIn diventa una fonte insostituibile. Il social delle imprese e dei professionisti permette di studiare l'organigramma di un'azienda, conoscere il ruolo di quasi tutti i dipendenti (se iscritti) e presumere quindi i loro privilegi di accesso fisici o digitali.