CROWDSTRIKE

2025 EUROPEAN THREAT LANDSCAPE REPORT

Sommario

Panoramica introduttiva

L'European Threat Landscape Report 2025 di CrowdStrike offre insight chiave sull'attività informatica osservata e sui relativi sviluppi geopolitici in Europa. Il report riassume le minacce all'Europa provenienti da criminali nation-state, eCrime e hacktivismo, con l'obiettivo di informare gli stakeholder del settore pubblico e privato.

L'Europa si conferma come uno dei principali obiettivi degli avversari eCrime, probabilmente a causa della redditività delle entità con sede nel continente rispetto ad altre regioni, del quadro normativo europeo e delle motivazioni politiche degli attori dell'eCrime. Sebbene la cosiddetta "caccia grossa" (BGH) costituisca una minaccia persistente, le entità basate in Europa devono fare i conti anche con tecniche eCrime in evoluzione, come le campagne basate sul phishing vocale (vishing) e sulle esche CAPTCHA. Gli avversari, siano essi originari dell'Europa o attivi contro obiettivi europei, utilizzano un ecosistema sotterraneo altamente organizzato e resiliente, accessibile tramite forum in lingua inglese e russa nel Web visibile e nel dark Web. Questo ecosistema facilita la collaborazione e ospita servizi che forniscono accesso alle reti, malware pronto all'uso e VaaS (violence-as-a-service).

L'invasione su larga scala dell'Ucraina da parte della Russia a febbraio del 2022 ha provocato un aumento delle intrusioni informatiche mirate contro entità ucraine. Sebbene la maggior parte di queste operazioni sia stata condotta da cybercriminali legati o allineati alla Russia, anche avversari connessi alla Corea del Nord hanno preso di mira organizzazioni ucraine. Al di là delle operazioni legate in maniera specifica ai conflitti, Paesi come Russia, Iran, Corea del Nord, Cina, Turchia, Kazakistan e India continuano ad attaccare entità europee attraverso operazioni informatiche che mirano a raccogliere informazioni strategiche, influenzare l'opinione pubblica attraverso information operations (IO), sottrarre proprietà intellettuale e ottenere guadagni finanziari in modo opportunistico.

Gli eventi geopolitici, inclusi i conflitti in corso tra Russia e Ucraina e tra Israele e Hamas, sono stati i principali fattori scatenanti dell'attività degli hacktivisti a livello globale diretta contro paesi europei. Le azioni più comuni hanno incluso attacchi DDoS, campagne hack-and-leak e deturpazioni di siti Web.

Questo report offre una visione approfondita del panorama delle minacce in Europa, basata sulle analisi condotte da CrowdStrike Intelligence tra gennaio 2024 e settembre 2025. È stato prodotto dal team CrowdStrike Counter Adversary Operations, che integra due gruppi strettamente collegati: CrowdStrike Intelligence e CrowdStrike OverWatch. Il team CrowdStrike Intelligence produce report operativi che identificano nuovi avversari, ne monitorano le attività e tengono sotto controllo l'emergere di nuove minacce informatiche in tempo reale. Sfruttando queste informazioni, il team CrowdStrike OverWatch svolge attività proattive di threat hunting analizzando i dati telemetrici dei clienti, con l'obiettivo di rilevare e contrastare l'attività malevola prima che degeneri.

Poiché il panorama delle minacce informatiche in Europa si evolve senza sosta, le organizzazioni devono tenere alta l'attenzione nei confronti di un ampio numero di avversari, dai gruppi di criminali informatici ai cybercriminali e hacktivisti supportati dagli stati. Attraverso strategie di sicurezza basate sull'intelligence, gli stakeholder regionali possono rafforzare le proprie difese, ridurre i rischi e anticipare le minacce emergenti in uno scenario sempre più complesso.

CONVENZIONI DI DENOMINAZIONE

AVVERSARIO	NATION-STATE O CATEGORIA DI AFFILIAZIONE
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (COREA DEL NORD)
CRANE	ROK (REPUBBLICA DI COREA)
HAWK	SIRIA
JACKAL	HACKTIVISTA
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	REPUBBLICA POPOLARE CINESE
SAIGA	KAZAKISTAN
SPHINX	EGITTO
SPIDER	eCRIME
TIGER	INDIA
WOLF	TURCHIA

Panoramica dell'eCrime

Caccia grossa

Le vittime europee rappresentano quasi il 22% delle entità nominate sui siti dedicati all'esposizione dei dati (DLS) monitorati da CrowdStrike Intelligence, il che rende il continente la seconda area più colpita dopo il Nord America. Secondo i set di dati, le entità europee hanno più del doppio delle probabilità di essere prese di mira rispetto a quelle dell'area Asia-Pacifico e Giappone. Le organizzazioni europee sono obiettivi appetibili per gli avversari BGH, probabilmente a causa dei seguenti fattori:

- **Pressioni legali:** i cybercriminali hanno sfruttato le sanzioni in materia di violazione dei dati previste dal Regolamento generale sulla protezione dei dati (GDPR) dell'UE per fare pressione sulle vittime e convincerle a pagare i riscatti. Diversi cybercriminali hanno minacciato di segnalare le entità per mancata conformità normativa tramite il loro sito dedicato all'esposizione dei dati, in richieste di riscatto o durante trattative.
- **Obiettivi redditizi:** in Europa hanno sede cinque delle dieci aziende più importanti al mondo in termini di valore economico, distribuite tra Francia, Germania, Paesi Bassi, Svizzera e Regno Unito. Poiché gli avversari BGH basano solitamente le loro richieste di riscatto sulle entrate dell'organizzazione colpita, è probabile che considerino le aziende europee come in grado di pagare somme elevate.
- **Motivazioni politiche:** sebbene gli avversari BGH siano mossi principalmente da interessi economici, alcuni hanno espresso posizioni politiche e minacciato di compiere azioni motivate da tali idee. Il gruppo WIZARD SPIDER, ad esempio, ha sostenuto l'invasione dell'Ucraina da parte della Russia nel 2022 e organizzazioni dell'Unione Europea, come Europol, hanno inoltre segnalato che i cybercriminali tradizionali e ibridi[1] stanno collaborando per ottenere vantaggi reciproci.[2]

DAL 1° GENNAIO 2024, I CYBERCRIMINALI BGH HANNO NOMINATO CIRCA 2.100 VITTIME CON SEDE IN EUROPA SU OLTRE 100 SITI DEDICATI ALL'ESPOSIZIONE DEI DATI (DLS) PER RANSOMWARE ED ESTORSIONE DI DATI.

1 I cybercriminali ibridi sono spinti da svariate motivazioni e conducono attività su più fronti: eCrime, nation-state, hacktivismo e information operations.

2 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Secondo le informazioni provenienti dai siti dedicati all'esposizione dei dati, Regno Unito, Germania, Italia, Francia e Spagna sono state le nazioni europee più colpite. Questi Paesi rappresentano le principali economie europee, esclusa la Russia che è assente dal set di dati (vedere la sezione *Divieto di colpire entità in Russia e nell'area CSI* a pagina 12). Tra gennaio 2024 e settembre 2025, i settori più colpiti sono stati quello manifatturiero, dei servizi professionali, della tecnologia, dell'industria, dell'ingegneria e del retail. Le segnalazioni nei siti dedicati all'esposizione dei dati, in cui vengono nominate entità con sede in Europa, sono aumentate di quasi il 13% rispetto all'anno precedente, passando da circa 1.220 a 1.380 (Figura 1).

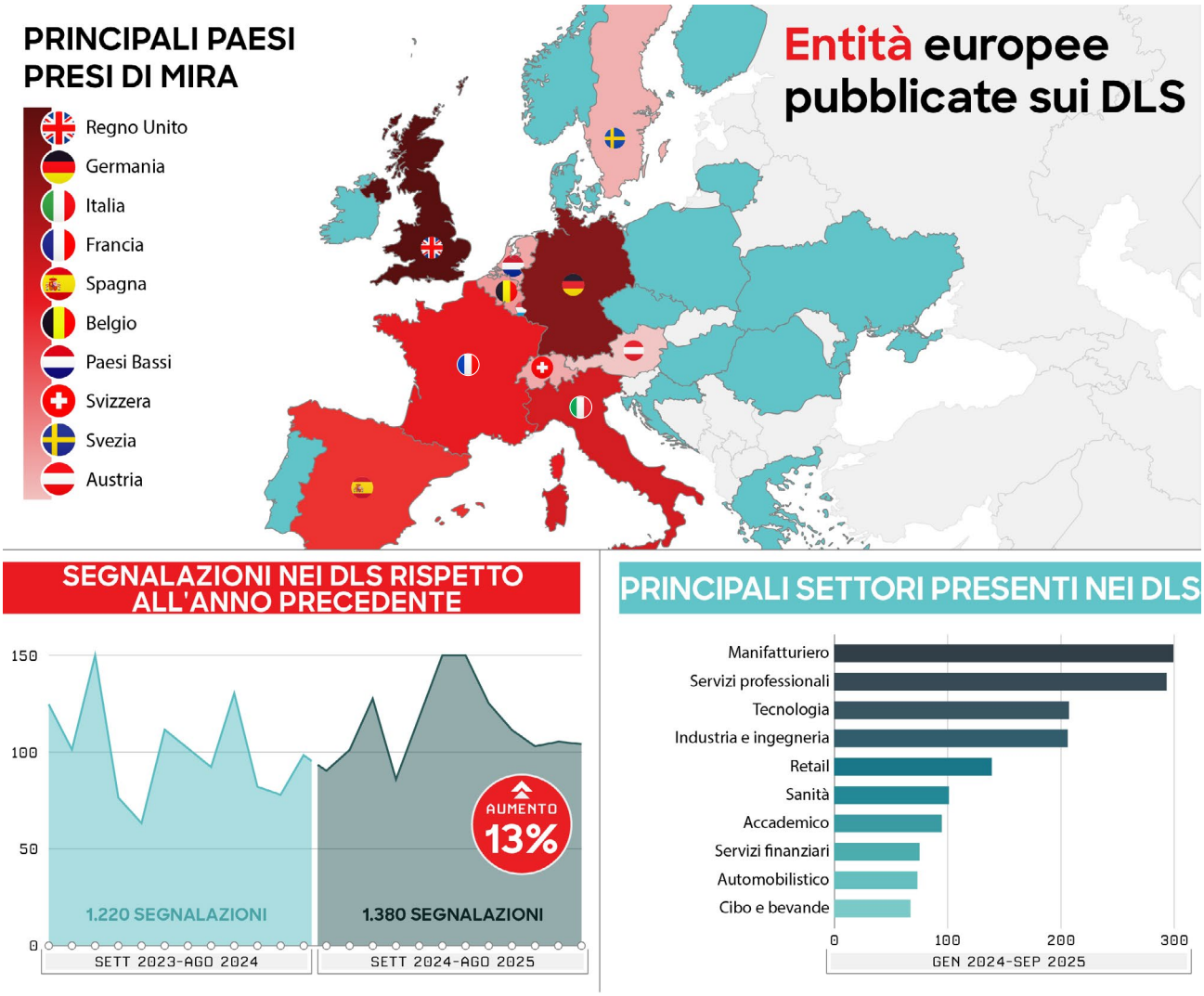


Figura 1. Segnalazioni nei siti dedicati all'esposizione dei dati (DLS) per paese, settore e periodo temporale

Tra queste vittime europee, il 92% è stato nominato su siti dedicati all'esposizione dei dati specializzati in ransomware (come *LockBit di* BITWISE SPIDER); generalmente, gli avversari che si celano dietro questi siti utilizzano una combinazione di ransomware e furto di dati per estorcere denaro alle vittime.
Il restante 8% delle vittime è stato nominato su siti appartenenti ad avversari che ricorrono esclusivamente al furto di dati (come nel caso del sito dedicato all'esposizione dei dati *Clop* di GRACEFUL SPIDER).

Durante il periodo analizzato, i gruppi che hanno colpito il maggior numero di vittime in Europa sono stati: BITWISE SPIDER, PUNK SPIDER, OCULAR SPIDER, TRAVELING SPIDER e BRAIN SPIDER (Figura 2). Tuttavia, sempre durante questo lasso di tempo, diverse operazioni delle forze dell'ordine hanno avuto un impatto significato sulle attività di alcuni di questi avversari.

Ad esempio, i livelli di attività degli affiliati di BITWISE SPIDER sono notevolmente diminuiti in seguito all'operazione di polizia multinazionale Operation Cronos. Un'altra iniziativa multinazionale, Operation Phobos Aetor, ha portato al sequestro del sito dedicato all'esposizione dei dati *8BASE* di BRAIN SPIDER e all'arresto di quattro presunti operatori del ransomware *8BASE.* Inoltre, OCULAR SPIDER ha chiuso il proprio servizio di ransomware as a service (RaaS) *RansomHub* a seguito di conflitti tra gli affiliati di *RansomHub e* l'amministratore del gruppo RaaS *DragonForce.*

Nonostante queste iniziative, avversari particolarmente attivi come PUNK SPIDER, TRAVELING SPIDER e altri cybercriminali ignoti, tra cui affiliati del RaaS *Qilin*, continuano a rappresentare una minaccia significativa per le entità europee.

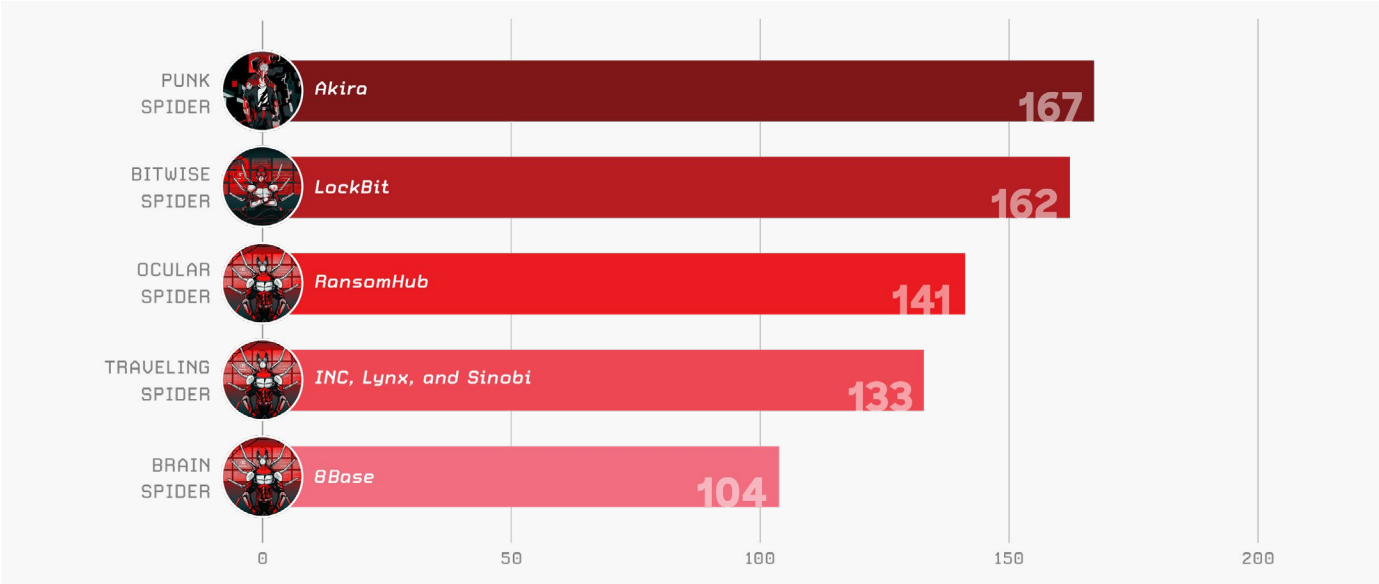


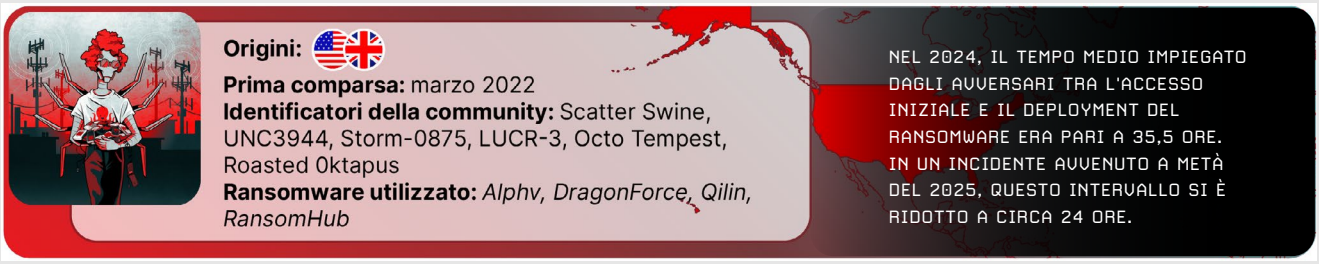
Figura 2. Avversari dominanti di ransomware ed estorsione che operano contro entità europee, gennaio 2024-settembre 2025

Indipendentemente dalla posizione geografica delle vittime, gli avversari BGH tendono a utilizzare le stesse tattiche, tecniche e procedure (TTP). Durante il periodo analizzato, gli attori BGH hanno fatto ampio uso delle seguenti TTP:

- Dumping delle credenziali da database di configurazione di backup e ripristino, che spesso contengono le credenziali utilizzate per accedere all'infrastruttura degli hypervisor
- Crittografia remota dei file, esecuzione di ransomware, spesso da un sistema non gestito[3] ed esecuzione del processo di crittografia dei file al di fuori del sistema preso di mira
- Sfruttamento dell'accesso a sistemi non gestiti per rubare dati e distribuire ransomware
- Distribuzione di ransomware Linux su infrastrutture VMware ESXi

3 Un sistema non gestito è un sistema che non dispone di alcun software di rilevamento e risposta agli endpoint (EDR).

SCATTERED SPIDER prende di mira il settore retail britannico nel 2025



Attivo dal 2022, SCATTERED SPIDER è diventato uno degli avversari eCrime più aggressivi e pericolosi. Il gruppo conduce una serie di attività motivate da interessi economici, tra cui furto di criptovalute, SIM swap ed estorsione. Dal 2023, questo avversario ha preso di mira prevalentemente grandi aziende attraverso campagne di ransomware e furto di dati. Le intrusioni di SCATTERED SPIDER si distinguono per le sofisticate campagne di vishing tramite help desk utilizzati per ottenere l'accesso iniziale, le innovative tecniche di spionaggio cloud conscious ma, soprattutto, per la rapidità.

Sebbene SCATTERED SPIDER colpisca in prevalenza società private del Nord America, ha preso di mira entità in Finlandia, Francia, Germania, Lussemburgo, Svezia e Regno Unito. Dopo un periodo di inattività tra dicembre 2024 e marzo 2025, nell'aprile del 2025 l'avversario ha attaccato numerose aziende del settore retail britannico con l'intento di distribuire il ransomware *DragonForce*.

Nell'aprile del 2025, è stata rilevata una tentata operazione di accesso ravvicinato (close-access). L'azione è stata condotta da un cybercriminale legato all'ecosistema eCrime spesso indicato come "The Com", un ecosistema online prevalentemente in lingua inglese composto da più sottogruppi interconnessi, che avrebbe cercato di reclutare persone disposte a recarsi presso la sede centrale di un'azienda retail del Regno Unito, la quale, secondo quanto emerso, sarebbe stata colpita da un attacco SCATTERED SPIDER. Secondo le istruzioni del cybercriminale, le persone selezionate per l'operazione dovevano procurarsi un laptop Windows usa e getta, recarsi presso la sede centrale dell'azienda nel Regno Unito, connettersi alla rete Wi-Fi in loco e fornire l'accesso remoto al laptop tramite RDP. Non è stato confermato se l'operazione di accesso ravvicinato sia effettivamente avvenuta; tuttavia, il solo fatto che sia stata oggetto di discussione rappresenta un elemento di distinzione tra i cybercriminali occidentali e russi.

A differenza della maggior parte degli avversari BGH più noti, gli operatori di SCATTERED SPIDER hanno sede nei paesi occidentali. CrowdStrike Intelligence ha identificato membri del gruppo sia negli Stati Uniti che nel Regno Unito. A luglio del 2025, la National Crime Agency del Regno Unito ha annunciato l'arresto di quattro persone, di età compresa tra 17 e 20 anni, in relazione ai recenti attacchi contro aziende retail britanniche.[4] A settembre del 2025, due di queste persone sono state nuovamente arrestate e accusate di essere coinvolte in un attacco avvenuto nel 2024 ai danni di Transport for London.[5] Questi soggetti risultano attivi almeno dal 2022 nonostante precedenti arresti, e ciò dimostra quanto sia difficile sconfiggere l'eCrime anche quando i responsabili si trovano all'interno della giurisdizione delle autorità.

4 https://www.nationalcrimeagency.gov.uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods

5 https://www.nationalcrimeagency.gov.uk/news/two-charged-for-tfl-cyber-attack

Le tecniche di eCrime più utilizzate

IL VISHING RISCHIA DI DIVENTARE UNA MINACCIA SIGNIFICATIVA

Dal 2024, gli avversari eCrime hanno utilizzato sempre più spesso il vishing per ottenere l'accesso iniziale. Si tratta di una tecnica di social engineering in cui un avversario contatta telefonicamente la vittima per indurla a fornire credenziali o ad agire sul proprio endpoint. Oltre a facilitare le frodi, gli avversari eCrime, tra cui CURLY SPIDER e MUTANT SPIDER, hanno utilizzato il vishing per aprire la strada a gruppi ransomware (vedere la sezione *Initial access broker* a pagina 14). Allo stesso modo, operatori o affiliati di avversari BGH come ROYAL SPIDER, TUNNEL SPIDER e WANDERING SPIDER hanno utilizzato il vishing nelle loro operazioni.

Alla fine del 2024, un utente, molto probabilmente legato a MUTANT SPIDER, ha pubblicato un post sul forum in lingua russa Exploit dichiarando di preferire gli obiettivi nordamericani rispetto a quelli europei, poiché più propensi a pagare riscatti più elevati.

Tuttavia, è probabile che il vishing diventi una minaccia più significativa per le entità con sede in Europa. Questa valutazione è formulata con un grado di fiducia moderato, in base ai recenti episodi di vishing ad alto impatto che hanno colpito entità in Europa (vedere la sezione *SCATTERED SPIDER prende di mira il settore retail britannico nel 2025* a pagina 8) e al fatto che gli avversari eCrime sfruttano in misura sempre crescente madrelingua delle regioni colpite nelle loro campagne di vishing. Ad esempio, il gruppo PLUMP SPIDER ha utilizzato parlanti nativi di portoghese brasiliano per colpire entità con sede in Brasile, mentre una campagna di vishing condotta a febbraio del 2025 ha probabilmente impiegato madrelingua tedeschi per distribuire TeamViewer e *SH RAT* a entità in Germania.

DURANTE IL PERIODO DI RIFERIMENTO, CROWDSTRIKE OVERWATCH E IL TEAM CROWDSTRIKE FALCON® COMPLETE NEXT-GEN MDR HANNO OSSERVATO CIRCA 1.000 INCIDENTI LEGATI AL VISHING A LIVELLO GLOBALE. LA MAGGIOR PARTE DEGLI INCIDENTI HA AVUTO EFFETTI SU ENTITÀ BASATE IN NORD AMERICA, PROBABILMENTE A CAUSA DELL'UBIQUITÀ DELLA LINGUA INGLESE E DEI MAGGIORI FATTURATI DELLE ORGANIZZAZIONI.

I FALSI CAPTCHA RIMANGONO UN METODO DI DISTRIBUZIONE COMUNE

A partire dalla metà del 2024, gli avversari eCrime hanno iniziato ad adottare su larga scala esche CAPTCHA (note anche come *ClickFix*) per distribuire malware. Questa tecnica di social engineering consiste nell'utilizzare pagine che imitano i test di autenticazione CAPTCHA per convincere le vittime a copiare, incollare ed eseguire codice dannoso nella finestra Esegui o nel terminale di Windows.

Le campagne identificate hanno utilizzato e-mail di phishing, pubblicità dannosa (malvertising) e SEO (Search Engine Optimization) poisoning per indirizzare le vittime verso pagine CAPTCHA false. Sebbene le campagne che utilizzano esche CAPTCHA colpiscano in modo indiscriminato, alcuni cybercriminali personalizzano i falsi CAPTCHA in base ai loro obiettivi specifici, come entità del settore dell'ospitalità e dei viaggi.

NEL 2024 E 2025, CROWDSTRIKE HA IDENTIFICATO OLTRE 1.000 INCIDENTI CHE HANNO INTERESSATO CLIENTI CON SEDE IN EUROPA E CHE HANNO COINVOLTO ESCHE CAPTCHA (FIGURA 3).

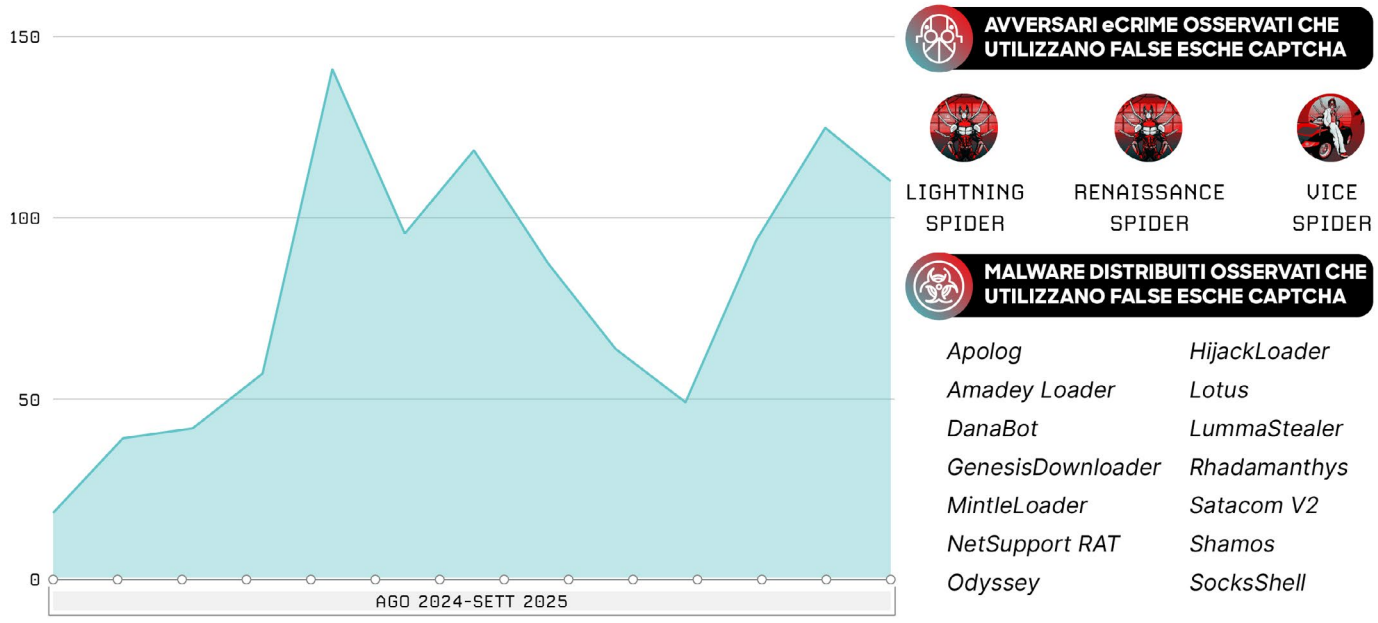


Figura 3. Incidenti correlati alle esche CAPTCHA causati a clienti con sede in Europa

Nei forum di eCrime in lingua russa, come Exploit e XSS, sono stati pubblicizzati diversi strumenti che possono essere utilizzati per creare pagine CAPTCHA false, sia personalizzabili che preconfezionate, per Windows, macOS e Linux (vedere la sezione *Ecosistema sotterraneo* a pagina 11). Le funzionalità pubblicizzate includono offuscamento del codice creato dinamicamente, capacità di bypassare le misure di sicurezza e funzionalità esca (come l'imitazione di piattaforme di gestione delle criptovalute). Questi servizi di eCrime rendono le esche CAPTCHA facilmente accessibili a un'ampia gamma di cybercriminali.

LIGHTNING SPIDER, RENAISSANCE SPIDER e VICE SPIDER hanno da sempre preso di mira entità con sede in Europa e hanno utilizzato esche CAPTCHA nelle loro campagne. Inoltre, cybercriminali non identificati hanno utilizzato esche CAPTCHA per distribuire *Odyssey* di BRASH SPIDER, *Shamos* di COOKIE SPIDER, *Amadey Loader* di HAZARD SPIDER, *Lotus* di LUNAR SPIDER, *DanaBot* di SCULLY SPIDER e *MintleLoader* (noto anche come *MintsLoader, MintLoader)* in campagne contro l'Europa e altre aree geografiche.

Ecosistema sotterraneo

Nonostante le forze dell'ordine, tramite le loro operazioni, occasionalmente sequestrino le infrastrutture e arrestino gli amministratori che gestiscono importanti piattaforme eCrime in Europa, l'ecosistema sotterraneo europeo, in particolare quello di lingua russa, si dimostra particolarmente resiliente. Numerosi forum, marketplace e canali Telegram, attivi da tempo ed emergenti, supportano cybercriminali più o meno sofisticati fungendo da hub per la collaborazione, la condivisione di conoscenze e strumenti e vari servizi che agevolano le attività eCrime.

FORUM DI eCRIME IN LINGUA RUSSA

Da quasi 30 anni, i cybercriminali si riuniscono su forum clandestini in lingua russa. Sebbene questi forum inizialmente fornissero una piattaforma per il carding (ovvero il furto e la vendita dei dati delle carte di credito), l'ecosistema si è rapidamente evoluto fino a includere forum specializzati in vari servizi di eCrime o metodi di monetizzazione.[6]

Il numero crescente di forum di eCrime ha permesso ai cybercriminali di condividere conoscenze su tecniche di spionaggio e strumenti, nonché di pubblicizzare e sviluppare i loro servizi criminali. Alcuni forum, tra cui exploit e XSS (quest'ultimo colpito di recente da diversi arresti e dal sequestro del dominio clearnet), ospitano discussioni generali sull'eCrime; tuttavia, numerosi forum sono specializzati in servizi di eCrime o metodi di monetizzazione specifici, tra cui:

- **Carding:** una delle prime e più frequenti attività di cybercrime nell'ecosistema sotterraneo in lingua russa, il carding continua ad essere discusso su forum generalisti e specializzati (come WWH-Club o lo storico CarderPlanet). I cosiddetti carder (кардеры) vendono i dati delle carte di pagamento ottenuti tramite violazioni di dati o skimming dei bancomat, malware su POS (point-of-sale) e formjacking.[7]
- **Servizi finanziari:** questi forum discutono e offrono servizi per mettere in atto frodi finanziarie, riciclaggio di denaro o conversione in contanti. Il forum DarkMoney, gestito da un operatore di RENAISSANCE SPIDER, è storicamente uno dei principali forum di servizi finanziari, con un fatturato pubblicitario di 200.000 euro al mese.
- **Probiv:** il termine "probiv" (пробив) descrive un servizio molto noto nell'ecosistema sotterraneo in lingua russa in cui gli utenti vendono informazioni personali ottenute da dati trapelati o reclutano insider con accesso a dati specifici. Le autorità russe hanno recentemente intensificato la lotta contro le fughe di dati e i servizi probiv, in parte a causa del loro ruolo nel facilitare il giornalismo investigativo.[8]
- **Ransomware:** in seguito all'attacco *DarkSide di* CARBON SPIDER a maggio del 2021, che è stato ampiamente pubblicizzato, i principali forum di eCrime in lingua russa hanno vietato le discussioni sul ransomware. Di conseguenza, un cybercriminale, probabilmente connesso all'ormai defunto gruppo *Babuk Locker*, ha creato il forum RAMP, che ospita una sezione dedicata ai programmi di affiliazione RaaS.

Questo ecosistema eCrime ospita un'ampia gamma di cybercriminali e servizi, tra cui broker di accesso iniziale e dati, provider di hosting bulletproof, servizi di conversione in contanti e mixer di criptovalute, operatori MaaS (malware-as-a-service), RaaS e spammer. Per gestire le interazioni e creare fiducia tra acquirenti, venditori e altri utenti, i forum di eCrime in lingua russa hanno sviluppato un modello di autogestione che include arbitrato delle controversie, garanti delle transazioni e deposito a garanzia automatizzato, sistemi di reputazione del venditore e livelli utente, funzionalità di deposito[9] e regole del forum applicate da amministratori e moderatori.

---

6 https://www.justice.gov/archives/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison
https://www.own.security/ressources/blog/russian-language-cybercriminal-forums---chapter-i-an-excursion-into-the-core-of-the-underground-ecosystem

7 Nel formjacking (noto anche come Magecart, skimming digitale, sniffing), i cybercriminali iniettano codice Javascript dannoso nei siti Web per sottrarre i dati delle carte di pagamento dei clienti e/o informazioni di identificazione personale (PII) dai front-end dei siti Web.

8 https://meduza.io/en/feature/2025/07/29/too-much-is-slipping-through

9 Spesso, gli amministratori del forum chiedono ai venditori di effettuare un deposito commisurato al valore di ciò che stanno vendendo; ad esempio, un utente che desidera vendere un prodotto per 10.000 USD potrebbe essere tenuto a depositare tale somma in un wallet dedicato del forum.

Divieto di colpire entità in Russia e nell'area CSI

Il divieto di prendere di mira le organizzazioni e i cittadini della Russia e dei paesi della Comunità degli Stati Indipendenti (CSI) è stato a lungo una regola tacita e spesso codificata nell'ecosistema sotterraneo di lingua russa. Sebbene lo scopo di tale divieto sia probabilmente quello di evitare l'intervento delle forze dell'ordine locali, è possibile che sia motivato anche dal patriottismo, come dimostra il fatto che i cybercriminali dell'area CSI preferiscono prendere di mira entità esterne.

Molti operatori MaaS e RaaS di lingua russa vietano a clienti e affiliati di rivolgere i loro attacchi alla Russia e alla Comunità degli Stati Indipendenti (CSI). Ad esempio, in un annuncio pubblicato sul forum XSS, HAZARD SPIDER ha dichiarato che *Amadey Loader* "non è operativo nella Federazione Russa e nei paesi considerati alleati". *Amadey Loader* garantisce l'applicazione del divieto non eseguendo i comandi C2 (command-and-control) nel caso in cui il sistema rilevi gli identificativi di tastiera dei paesi della CSI. Barriere simili per le lingue dell'interfaccia utente sono presenti in *Lumma Stealer*, *Matanbuchus* di DEMON SPIDER e in *Rhadamanthys*.

Sebbene gli attacchi alle entità di queste regioni non siano sempre esplicitamente vietati sui forum di eCrime, i cybercriminali eCrime di lingua russa hanno ostracizzato i criminali informatici che non aderiscono al divieto. A marzo 2024, un utente del forum XSS associato a BRASH SPIDER, sviluppatore dei malware di furto delle informazioni macOS *Doshell Stealer* e *Odyssey*, ha accusato COOKIE SPIDER di aver rivolto attacchi a entità della regione CSI e ha richiesto la sua espulsione dal forum.

FORUM DI eCRIME IN LINGUA INGLESE

I forum di eCrime in lingua inglese si sono affermati come hub critici all'interno del più ampio ecosistema eCrime europeo, fungendo da marketplace e spazi comunitari in cui i cybercriminali scambiano strumenti, dati e competenze. A differenza dei forum in lingua russa che hanno tradizionalmente dominato lo sviluppo di malware sofisticati e il reclutamento di affiliati ransomware, i luoghi di incontro in lingua inglese hanno creato gateway accessibili per cybercriminali europei con diversi livelli di competenze. Forniscono un facile accesso ai dati compromessi, strumenti di uso comune e servizi di riciclaggio di denaro, il tutto supportato da funzionalità che favoriscono la fiducia come il deposito a garanzia e i punteggi di reputazione.

Su forum come BreachForums, gli strumenti base generalmente includono database contenenti dati personali e aziendali compromessi, credenziali di accesso per VPN aziendali e ambienti cloud, strumenti di furto delle informazioni, loader e kit di phishing. I fornitori offrono anche tutorial, elenchi di access broker iniziale e servizi di riciclaggio che consentono ai cybercriminali di monetizzare le loro operazioni. Le transazioni sono in genere condotte utilizzando criptovaluta e molti forum utilizzano servizi di deposito a garanzia per mediare le operazioni, riducendo il rischio di frode in comunità per loro natura inaffidabili.

I leader di BreachForums, l'intervento delle forze dell'ordine

BreachForums si è imposta come piattaforma di riferimento nell'ecosistema dell'eCrime in lingua inglese dopo la chiusura del suo predecessore, RaidForums, da parte delle autorità ad aprile 2022. Dopo che le forze dell'ordine hanno arrestato l'amministratore di RaidForums, Diogo Santos Coelho (noto come Omnipotent) in Portogallo e sequestrato il dominio, il vuoto è stato rapidamente colmato da Pompompurin, un membro rispettato della community di RaidForums, che ha lanciato BreachForums nel marzo 2022.

Pompompurin è stato arrestato nel 2023 e la proprietà del forum è passata a ShinyHunters, a cui sono attribuite numerose operazioni di furti di dati di alto profilo. ShinyHunters ha probabilmente sede in Francia, come confermato dal rinvio a giudizio da parte del Dipartimento di Giustizia (DOJ) statunitense di diversi individui residenti in Francia associati al gruppo nel giugno 2021. La leadership del forum è cambiata più volte finché ad agosto 2024 BUTLER SPIDER (noto anche come *IntelBroker*), con sede nel Regno Unito, è diventato il principale proprietario e amministratore.

BUTLER SPIDER era un membro di spicco del forum e ha rivendicato la responsabilità della vendita e dell'esposizione di dati sensibili del governo statunitense ed europeo. A gennaio 2025, BUTLER SPIDER si è dimesso dal ruolo di amministratore di BreachForums, sostenendo di non avere il tempo necessario per amministrarlo. A febbraio 2025, secondo quanto riferito, le autorità francesi hanno arrestato BUTLER SPIDER. La sua inattività da marzo 2025 ha portato altri membri del forum a speculare sul fatto che l'avversario fosse stato arrestato.

Nell'aprile 2025, il forum è stato disattivato, anche se gli amministratori dell'epoca hanno affermato di aver rimosso intenzionalmente il forum in seguito a un attacco con un exploit zero-day. Nel giugno 2025, l'agenzia francese contro la criminalità informatica ha arrestato quattro individui che operavano con gli pseudonimi di ShinyHunters, Hollow, Noct e Depressed per il ruolo svolto nello sviluppo e nell'amministrazione di BreachForums.

La tumultuosa storia di BreachForums dimostra come singoli cybercriminali possano influenzare in modo significativo l'attività di un forum, richiamando la vigilanza delle forze dell'ordine a livello internazionale.

INITIAL ACCESS BROKER

Gli Initial Access Broker (IAB) sono cybercriminali che ottengono e vendono l'accesso alle reti aziendali su forum e marketplace. Per ottenere l'accesso iniziale, gli IAB utilizzano vari TTP, tra cui l'abuso delle credenziali compromesse, lo sfruttamento delle vulnerabilità e l'utilizzo del social engineering. Le entità basate in Europa sono un bersaglio popolare tra gli IAB e i loro acquirenti. I potenziali acquirenti spesso preferiscono l'accesso a entità statunitensi, seguite da entità di Europa, Canada e Australia.

Gran parte delle entità pubblicizzate ha sede nel Regno Unito, in Spagna, Germania, Italia e Francia e opera nel settore accademico, della vendita al dettaglio, dei servizi professionali, di produzione, industria e ingegneria. Analogamente ad altri servizi di supporto, gli IAB di lingua russa spesso si autoimpongono limitazioni nel pubblicizzare l'accesso alle entità russe e dell'area CSI (Figura 4).

DA GENNAIO 2024, CROWDSTRIKE INTELLIGENCE HA IDENTIFICATO 260 INITIAL ACCESS BROKER (IAB) CHE PUBBLICIZZANO L'ACCESSO A RETI DI OLTRE 1.400 ENTITÀ CON SEDE IN EUROPA.

	REGNO UNITO	SPAGNA	GERMANIA	ITALIA	FRANCIA	PAESI BASSI	BELGIO	SVEZIA	SVIZZERA	PORTOGALLO	AUSTRIA	POLONIA	DANIMARCA	NORVEGIA	REPUBBLICA CECA	ALTRO	TOTALE COMPLESSIVO
Accademico	40	10	23	19	16	14	5	1	1	9	1	7	0	0	1	15	162
Retail	28	25	10	20	12	2	4	5	6	2	2	5	7	2	0	14	135
Servizi professionali	34	10	24	6	13	9	2	6	5	3	5	2	4	3	2	6	133
Manifatturiero	20	9	16	14	3	6	3	3	5	0	4	1	0	2	0	6	92
Industria e ingegneria	19	5	18	16	4	5	7	3	3	0	3	1	0	0	0	5	85
Tecnologia	14	14	7	10	9	5	2	4	1	6	0	1	3	4	0	3	83
Pubblica amministrazione	4	7	3	10	9	1	1	5	0	1	1	0	1	1	0	6	50
Servizi finanziari	13	3	1	7	6	5	0	0	2	1	0	1	1	0	3	7	49
Telecomunicazioni	5	5	4	4	5	2	0	1	0	1	1	1	0	0	1	1	40
Sanità	4	2	4	1	5	8	5	0	1	0	0	1	1	0	1	6	38
Automobilistico	1	3	7	5	1	4	0	2	1	0	0	0	0	1	0	3	27
Energetico	2	1	3	3	3	0	0	0	1	0	0	3	1	1	0	2	20
Media	4	1	1	0	10	0	0	0	1	0	0	0	0	0	1	2	20
Trasporti	1	0	1	2	2	6	0	2	0	0	0	0	0	0	1	3	18
Logistica	6	5	1	1	2	0	0	0	0	0	1	0	1	0	0	0	17
Altro	100	65	38	40	55	14	18	10	15	5	9	4	7	5	5	72	462
Totale complessivo	292	161	160	156	153	80	46	42	41	28	27	27	24	19	15	160	1.431

Figura 4. Entità pubblicizzate dagli IAB, divise per settore e per i principali paesi europei, gennaio 2024-settembre 2025

Sulla base di questo set di dati, i paesi e i settori più pubblicizzati dagli IAB coincidono sostanzialmente con quelli nominati sui DLS di caccia grossa (vedere la sezione *Caccia grossa* a pagina 5). Questo è probabilmente frutto di molteplici fattori, uno dei quali è la stretta collaborazione tra IAB e avversari BGH. Ad esempio, HOOK SPIDER, che ha operato con diversi pseudonimi sui forum di eCrime in lingua russa Exploit, RAMP e XSS, ha molto probabilmente venduto l'accesso a vari avversari BGH (tra cui BITWISE SPIDER e BRAIN SPIDER) ed è storicamente associato a SCATTERED SPIDER.

MALWARE-AS-A-SERVICE

Il MaaS è un servizio di supporto che offre software dannoso (ad esempio, malware bancario, programmi di furto di informazioni, programmi di crittografia e loader), simile al modello SaaS (Software as a Service) legittimo. Il modello MaaS rende molto più facile per i cybercriminali di eCrime di accedere a strumenti che non avrebbero né il tempo né le risorse per sviluppare.

Gli operatori MaaS offrono i loro strumenti attraverso vari modelli di business, tra cui l'acquisto, il noleggio o pay-per-install, nonché programmi di affiliazione che prevedono la condivisione degli utili tra operatori MaaS e affiliati (Figura 5). Gli operatori MaaS di lingua russa offrono in genere i loro servizi su forum di eCrime (in particolare Exploit), canali Telegram pubblici o privati e, nel caso di LUNAR SPIDER, su segnalazione.

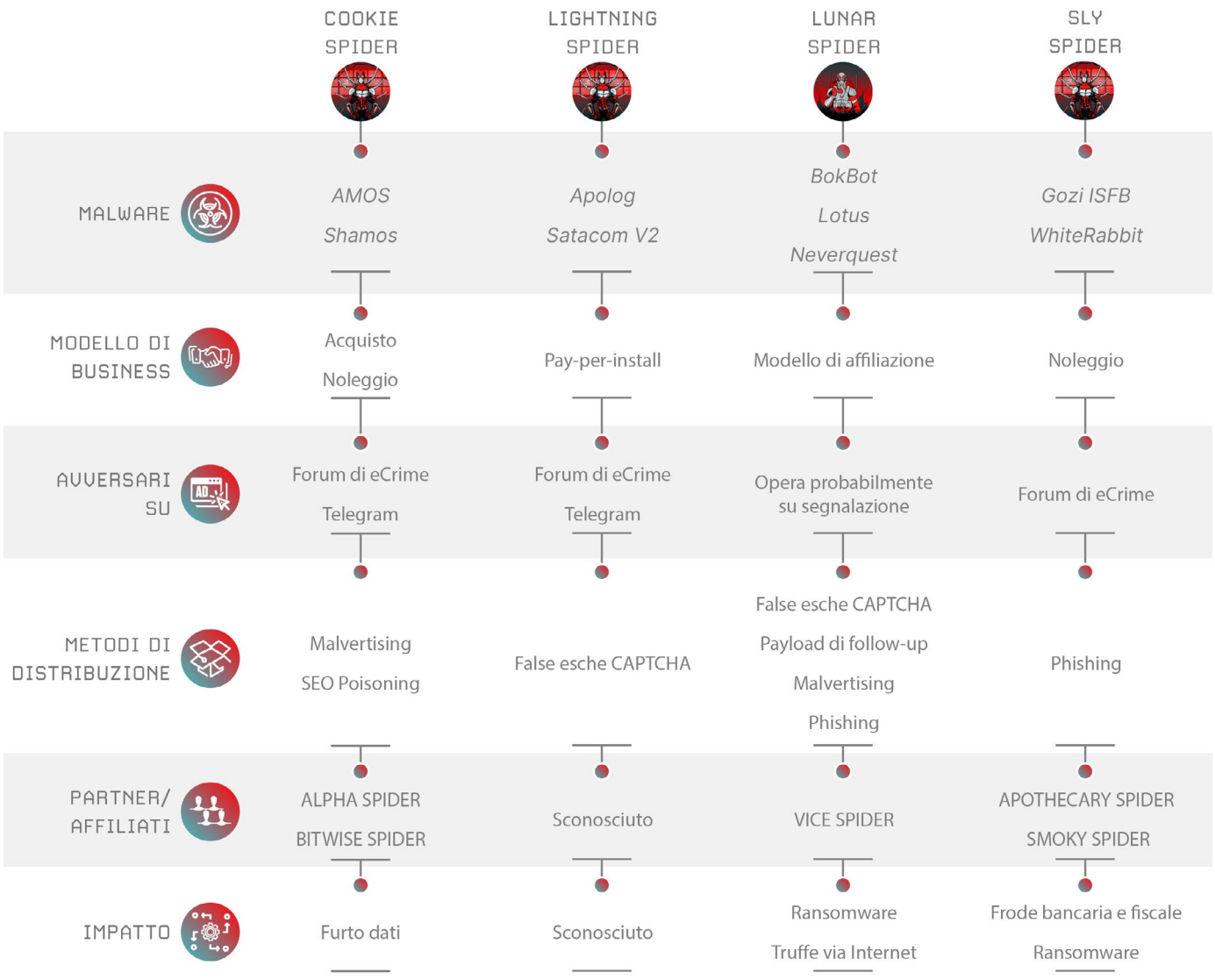


Figura 5. I principali operatori MaaS interessati ai paesi europei

Mentre le operazioni delle forze dell'ordine, come Operation Endgame o il sequestro di XSS di luglio 2025, destabilizzano regolarmente l'ecosistema, gli operatori MaaS rimangono resilienti, in parte a causa della persistenza di membri di lunga data che agiscono quasi impunemente nelle loro giurisdizioni. Tuttavia, Vyacheslav Igorevich Penchukov (alias Tank), un membro di LUNAR SPIDER attivo dal 2009 e inizialmente membro della gang *JabberZeus*, è stato arrestato a Ginevra, in Svizzera, nel 2022 ed estradato negli Stati Uniti agli inizi del 2024.

Oltre a facilitare l'azione di altri cybercriminali, la persistenza e la proliferazione degli operatori MaaS ostacola anche l'attribuzione degli incidenti, poiché offre a molti cybercriminali gli stessi strumenti, che spesso vengono forniti utilizzando TTP simili. Gli avversari nation-state sfruttano questo modello, ad esempio l'avversario legato alla Russia EMBER BEAR, che ha sfruttato *Matanbuchus di DEMON SPIDER*, SmokeLoader di SMOKY SPIDER e *Raccoon Stealer*. A maggio 2025, il Dipartimento di Giustizia degli Stati Uniti ha incriminato 16 membri del Maas *DanaBot* di SCULLY SPIDER, rivelando che il cybercriminale legato alla Russia aveva utilizzato questo servizio criminale per supportare operazioni militari e di spionaggio.[10]

Strumenti di comunicazione, Telegram, Tox e Jabber

Sebbene i servizi di eCrime inseriscano spesso annunci sui loro forum, la comunicazione con i potenziali clienti generalmente avviene tramite Telegram. Mentre le chiusure dei canali sono aumentate dopo l'arresto del CEO di Telegram Pavel Durov ad agosto 2024 e i termini di servizio di Telegram sono stati aggiornati, i cybercriminali di eCrime continuano ampiamente a fare affidamento su Telegram come principale piattaforma di comunicazione. Telegram consente ai servizi di eCrime di comunicare aggiornamenti o interruzioni del servizio, nonché di offrire supporto diretto ai clienti.

Tra gli altri metodi di comunicazione, troviamo Tox e Jabber. I messaggi Tox non sono modificabili, il che impedisce ai clienti di modificare gli accordi dopo l'avvenuta vendita. Inoltre, rispetto ai forum di eCrime e a Telegram, Jabber è meno soggetto a interruzioni grazie alla sua natura decentralizzata e al fatto che i cybercriminali possono gestire i propri server Jabber.

VIOLENCE-AS-A-SERVICE E FURTO DI CRIPTOVALUTA FISICA

Dal 2024, i furti di criptovaluta che coinvolgono attacchi fisici e rapimenti sono aumentati vertiginosamente, in particolare in Europa. A gennaio 2025, un criminale informatico ha rapito e tentato di estorcere il co-fondatore di Ledger, un fornitore di portafogli di criptovaluta molto prolifico in Francia. Sebbene i cybercriminali in questo caso (e in numerosi altri) siano stati arrestati, la minaccia persiste.[11] Tra gennaio e settembre 2025 si sono verificati 17 incidenti simili in Europa, di cui 13 in Francia.[12]

I soggetti coinvolti nel furto fisico di criptovaluta spesso operano all'interno di comunità di eCrime affiliate a "The Com". Molti di questi soggetti hanno precedentemente pubblicizzato strumenti come i bot di intercettazione con password monouso, ovvero strumenti basati su Telegram che consentono ai cybercriminali di automatizzare le chiamate di vishing e che vengono spesso utilizzati per rivolgere l'attacco agli account di scambio di criptovaluta.

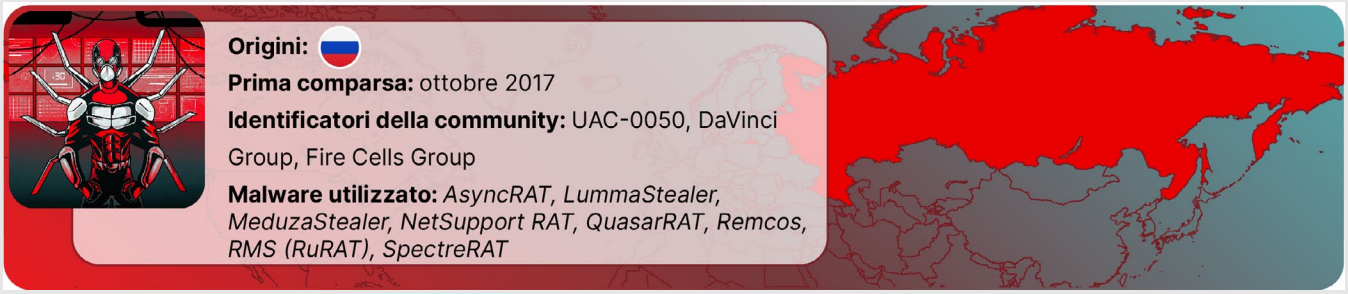
---

10 https://www.crowdstrike.com/en-us/blog/crowdstrike-partners-with-doj-disrupt-danabot-malware-operators/

11 https://www.france24.com/en/france/20250621-france-arrests-five-kidnapping-cryptocurrency-entrepreneur-father

12 https://github.com/jlopp/physical-bitcoin-attacks

RENAISSANCE SPIDER rappresenta una grave minaccia per l'Europa



RENAISSANCE SPIDER è un cybercriminale basato in Russia che ha storicamente condotto vari tipi di attività eCrime, spionaggio informatico e operazioni di manipolazione dell'opinione pubblica e facilitato operazioni di sabotaggio fisico.

- RENAISSANCE SPIDER conduce campagne di phishing ad alto volume principalmente rivolte al settore pubblico e privato dell'Ucraina. Ha condotto attacchi sporadici in tutta Europa, in Germania, Italia, Lituania, Moldavia, Polonia, Svizzera e Regno Unito. L'avversario è probabilmente motivato sia dall'interesse economico che dalla raccolta di intelligence.
- RENAISSANCE SPIDER ha rivolto i suoi attacchi in tutta Europa attraverso e-mail e operazioni di intelligence basate sui social media, utilizzando varie identità, tra cui il falso hacktivista *DaVinci Group* o spacciandosi per veri giornalisti moldavi, utilizzando i loro account e-mail compromessi. Più di recente, ha inviato via e-mail diversi falsi allarmi bomba a varie entità europee, probabilmente con l'obiettivo di indebolire il loro sostegno all'Ucraina.
- Ad agosto 2024, RENAISSANCE SPIDER ha creato il presunto VaaS *Fire Cells Group*, ingaggiando persone per operazioni di sovversione e sabotaggio in Ucraina. Sotto la copertura di *Fire Cells Group*, l'avversario ha condotto operazioni di intelligence, ha offerto pagamenti per l'assassinio di funzionari ucraini e molto probabilmente ha pagato persone per condurre attacchi incendiari contro veicoli militari e infrastrutture civili ucraine.

CrowdStrike Intelligence ritiene che gli operatori di RENAISSANCE SPIDER stiano probabilmente agendo sotto la direzione o in coordinamento con i servizi speciali russi. Questa valutazione è espressa con un livello di fiducia moderato e sulla base delle attività dell'avversario (ad esempio, information operations e sabotaggio) che sono in linea con gli interessi dello stato russo, del probabile arresto di membri del gruppo nel 2021 e di altre accuse di crimine informatico.

Panoramica degli avversari nation-state

I conflitti cinetici, tra cui la guerra in Ucraina e i conflitti in Medio Oriente, sono i principali motori dell'attività informatica in Europa. All'interno di questi contesti, i cybercriminali sponsorizzati da stati impiegano prevalentemente capacità informatiche in ruoli di supporto, ad esempio per ottenere visibilità su entità governative e militari, allo scopo di supportare gli sforzi bellici o di amplificare le operazioni di informazione (e disinformazione). Inoltre, alcuni avversari hanno utilizzato l'accesso alla rete come arma per degradare, interrompere o distruggere l'accesso alle infrastrutture critiche e alle funzioni governative essenziali.

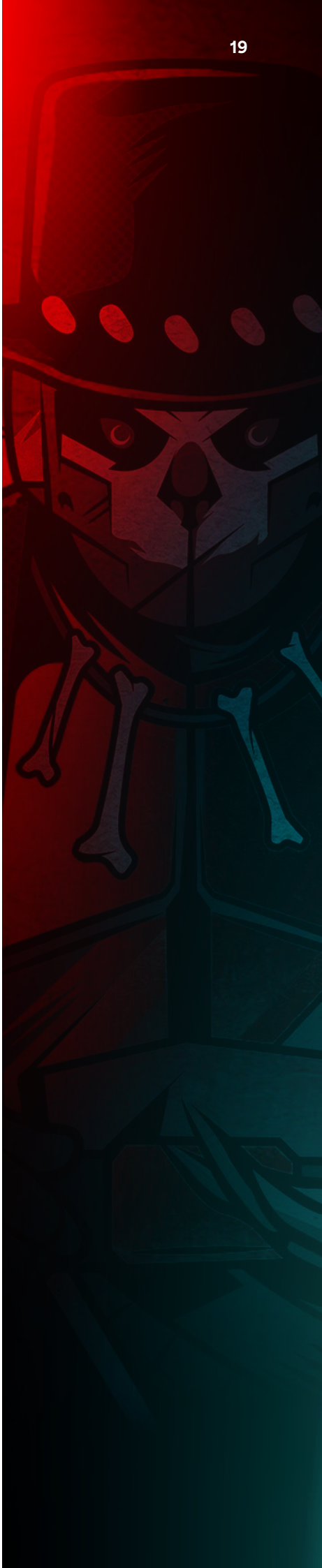
Nel frattempo, persiste l'esistenza di un ampio spettro di attività informatiche sponsorizzate da stati. Queste campagne spaziano dall'intrusione mirata per le attività di spionaggio tradizionale, volte a ottenere informazioni geopolitiche e operative o a facilitare il furto di proprietà intellettuali, fino alle intrusioni opportunistiche a scopo di lucro.

Attività informatica legata ai conflitti

CONFLITTI APPOGGIATI DALLA RUSSIA

L'invasione su vasta scala dell'Ucraina da parte della Russia, avvenuta a febbraio 2022, ha innescato un'ondata di intrusioni informatiche mirate da parte di una varietà di cybercriminali, sia nuovi che affermati. I singoli mandati di intelligence di ciascun avversario formano collettivamente un'ampia campagna di raccolta di informazioni a sostegno di vari obiettivi strategici. Sebbene la maggior parte delle attività di raccolta di intelligence sul conflitto sia condotta dai servizi di intelligence russi (RIS), principalmente dal GRU (noto anche come GU, Direttorato principale dello Stato Maggiore delle Forze Armate della Federazione russa) e dal Servizio di Sicurezza Federale della Federazione russa (FSB), anche le agenzie di intelligence della Corea del Nord sono state coinvolte in operazioni cinetiche e informatiche rivolte all'Ucraina.

Figura 6. Avversari legati alla guerra in Ucraina



Gli avversari legati al GRU conducono attività di raccolta di intelligence e operazioni di disturbo

L'avversario FANCY BEAR gestito dal GRU ha condotto numerose campagne simultanee contro entità militari e governative ucraine. Sebbene per le operazioni di phishing rivolte agli utenti del servizio di webmail ucraino gratuito l'avversario utilizzi dal 2023 il suo toolkit personalizzato di phishing delle credenziali **ukr.net**, nelle sue campagne ha sempre sfruttato *ClickFix*, i file RDP dannosi e le funzionalità dei modelli linguistici open-source.

La raccolta di intelligence di FANCY BEAR si concentra sul sostegno degli obiettivi militari della Russia in Ucraina, a livello strategico, operativo e tattico. L'avversario prende di mira importanti entità nazionali e locali operanti in vari settori, come entità governative, ma anche persone, inclusi i membri che prestano servizi nell'esercito ucraino.

Nel frattempo, VOODOO BEAR, altro avversario gestito dal GRU, si concentra sulle infrastrutture critiche ucraine, conducendo operazioni distruttive contro entità del comparto energetico, delle telecomunicazioni e dei servizi pubblici. Quando non ha distribuito immediatamente il malware wiper, VOODOO BEAR ha probabilmente mantenuto l'accesso per spostarsi lateralmente e compromettere ulteriormente le reti per supportare le sue esigenze di raccolta di intelligence e le operazioni distruttive.

All'inizio del 2025, CrowdStrike OverWatch ha rilevato che VOODOO BEAR sfrutta *POEMGATE* la backdoor di secure shell (SSH) e il logger di credenziali negli ambienti di operatori di telecomunicazioni ucraini. A giugno 2025, l'avversario ha proseguito le operazioni di accesso iniziale, consegnando programmi antivirus falsi contenenti la backdoor *Sumbur* che scarica ed esegue cariche distruttive aggiuntive per favorire la persistenza a lungo termine.

Gli avversari legati all'FSB conducono attività di raccolta di intelligence e operazioni di informazione

Le priorità di attacco dei cybercriminali legati all'FSB russo sono rimaste coerenti dal 2022. PRIMITIVE BEAR continua a condurre campagne di spear phishing ad alto volume contro il governo ucraino e le organizzazioni militari, probabilmente per raccogliere intelligence per supportare gli obiettivi bellici della Russia, come il rafforzamento della sua influenza politica e militare.

GOSSAMER BEAR conduce operazioni di phishing delle credenziali rivolte al governo e alle entità militari ucraine, nonché alle organizzazioni non governative (ONG) del Regno Unito e dell'UE. CrowdStrike Intelligence valuta con moderata sicurezza che le operazioni di phishing delle credenziali condotte da GOSSAMER BEAR probabilmente supportino le operazioni di intelligence per demoralizzare i cittadini ucraini o denigrare e minare la credibilità della governance del Regno Unito e delle istituzioni occidentali.

Altri cluster di attività appoggiati dalla Russia

Almeno dal 2017, il cluster di attività allineato alla Russia RepeatingUmbra colpisce il governo e gli organismi della difesa dell'Ucraina. Nel 2024 e 2025, il cluster ha condotto campagne di phishing delle credenziali e ha utilizzato diverse varianti del suo downloader personalizzato *Pryatki* per distribuire *Cobalt Strike* a bersagli ucraini.

Dal 2022, l'accresciuta necessità di intelligence per supportare le attività belliche della Russia ha determinato la comparsa di nuovi cybercriminali che spesso conducono operazioni ad alto volume ma a bassa sofisticazione contro obiettivi governativi e militari ucraini. Ad esempio, CrudeScientist, un probabile cluster legato alla Russia, attivo almeno da novembre 2023, ha mantenuto un ritmo operativo elevato fino all'inizio del 2025 con tattiche, tecniche e procedure (TTP) ampiamente consistenti e a bassa sofisticazione.

Analogamente, FamishedLibrarian, un altro probabile cluster di attività legato alla Russia, attivo almeno da novembre 2022, si basa su TTP di distribuzione relativamente invariate e continua a commettere errori di sicurezza OPSEC che espongono l'infrastruttura delle sue campagne.

UN CLUSTER DI ATTIVITÀ È UN RAGGRUPPAMENTO DI COMPORTAMENTI DANNOSI INTERCONNESSI CHE CONDIVIDONO STRUMENTI, TECNICHE O INFRASTRUTTURE COMUNI E CHE VENGONO MONITORATI DA CROWDSTRIKE QUANDO NON CI SONO ANCORA PROVE SUFFICIENTI PER ATTRIBUIRE L'ATTIVITÀ A UN AVVERSARIO IDENTIFICATO.

Agenti usa e getta reclutati tramite Telegram

Dall'invasione su vasta scala dell'Ucraina da parte della Russia nel febbraio 2022, Mosca ha accresciuto l'impiego di tattiche di guerra ibrida, contro l'Ucraina e i suoi alleati europei, incluso il sabotaggio. Nel 2024 e 2025, in tutta Europa sono stati segnalati numerosi casi di sabotaggio legati alla Russia. Per contro, l'UE ha sanzionato i membri dell'unità GRU 29155 della Russia per le loro attività di destabilizzazione, inclusi gli attacchi informatici.[13]

I servizi speciali russi hanno fanno sempre più affidamento ai cosiddetti agenti usa e getta per condurre operazioni sovversive e di sabotaggio. Gli agenti usa e getta sono agenti operativi reclutati da un servizio di intelligence, spesso per un compito specifico e di basso livello, con la piena consapevolezza che sono sacrificabili. L'impiego di agenti usa e getta garantisce maggiore negabilità credibile, è a basso costo e relativamente a basso rischio, ed è probabilmente utile vista l'espulsione di massa dei diplomatici e dei funzionari dell'intelligence russa da parte dei paesi europei.

Gli agenti usa e getta sono spesso reclutati e coordinati su Telegram, utilizzando intermediari criminali o estremisti, complicando la tracciabilità dell'attacco.[14] Da ottobre 2024, RENAISSANCE SPIDER agisce come intermediario sotto le spoglie del provider VaaS *Fire Cells Group*.

Gli alleati ucraini nel mirino

I cybercriminali appoggiati dalla Russia hanno anche preso di mira organizzazioni europee pubblicamente schierate a sostegno dell'Ucraina. Ad esempio, nel marzo 2022, RepeatingUmbra ha dimostrato un rinnovato interesse per entità tedesche e baltiche, probabilmente per il sostegno che questi paesi hanno fornito in relazione al conflitto. Nel frattempo, tra la fine di marzo e maggio 2022, PRIMITIVE BEAR ha temporaneamente ampliato il raggio degli attacchi, partendo dall'Ucraina per arrivare agli enti governativi in Lettonia, Moldavia e Lituania, probabilmente in risposta al sostegno che questi paesi hanno mostrato pubblicamente per Kiev, subito dopo l'invasione.[15]

Sebbene siano stati presi di mira anche altri governi europei filo ucraini, verosimilmente anche per il loro sostegno all'Ucraina, CrowdStrike Intelligence valuta che queste campagne più ampie siano principalmente motivate da esigenze continuative di raccolta di intelligence (consultare la sezione *Attività appoggiata dalla Russia* a pagina 26).

---

13 https://www.economist.com/graphic-detail/2025/07/22/russian-sabotage-attacks-surged-across-europe-in-2024

14 https://www.tv4.se/artikel/5vLIzItKYKnriPm0uJvd1N/saepo-larmar-vaervar-missbrukare-foer-att-utfoera-sabotage-i-sverige
https://www.abw.gov.pl/pl/informacje/2662,Dzialal-na-rzecz-obcego-wywiadu-przeciwko-RP-21-lipca-br-Kolumbijczyk-uslyszal-z.html
https://dossier.center/gru-guide/

15 https://eng.lsm.lv/article/politics/diplomacy/latvian-officials-immediately-condemn-putins-ukraine-invasion.a445051/
https://web.archive.org/web/20220507122804/https://www.bbc.com/ukrainian/features-61155192
https://www.eurointegration.com.ua/rus/news/2022/04/18/7137985/
https://www.delfi.lt/a/89541661

Attività informatica legata alla Corea del Nord contro l'Ucraina

Nel corso del 2024 e 2025, la Corea del Nord ha rafforzato i suoi legami con la Russia, offrendo sostegno diplomatico, economico e militare durante l'invasione dell'Ucraina. L'alleanza ha raggiunto il suo apice a ottobre 2024, quando la Corea del Nord ha schierato le sue truppe in Russia per sostenere le sue attività belliche contro l'Ucraina. In cambio dell'appoggio militare, la Russia avrebbe fornito alla Corea del Nord attrezzature avanzate per la difesa aerea, missili antiaerei e sistemi bellici elettronici.[16]

Il crescente sostegno militare che la Corea del Nord offre alla Russia coincide con gli attacchi di LABYRINTH CHOLLIMA mirati alle entità militari europee di agosto 2024 e maggio 2025 e con le attività sferrate da VELVET CHOLLIMA contro le entità diplomatiche europee tra marzo e agosto 2025. Queste campagne sono state probabilmente motivate da esigenze di intelligence militare della Corea del Nord, in relazione con la guerra in Ucraina.[17]

Con l'avvio di una nuova fase della loro alleanza, Corea del Nord e Russia hanno promesso di collaborare più strettamente su questioni militari, anche nell'ambito informatico. I leader delle agenzie di intelligence dei due paesi si sono incontrati più volte. Un report di giugno 2025 sostiene che entrambe le parti stiano puntando a un accordo di condivisione dell'intelligence.[18]

Gli avversari con legami alla Russia si concentrano sull'Ucraina

Durante il periodo di riferimento del report, le operazioni legate alla Russia contro l'Europa si sono concentrate quasi esclusivamente sul sostegno degli obiettivi russi, ovvero garantire il controllo della Russia sui territori annessi dell'Ucraina orientale, assicurare la neutralità politica e militare dell'Ucraina nei confronti della NATO e stabilire in Ucraina un governo favorevole alla Russia.

Dal 2022, sono state condotte almeno due operazioni distruttive legate alla Russia, principalmente rivolte a entità o capacità ucraine e che hanno interessato entità al di fuori dell'Ucraina, dimostrando il potenziale impatto su altre entità europee.[19] Un'operazione ha comportato danni collaterali, mentre l'altra ha intenzionalmente preso di mira la Polonia, il cui governo sostiene l'Ucraina.

A meno che il sostegno dell'Occidente all'Ucraina non cambi in modo significativo, incluso un eventuale coinvolgimento diretto delle forze militari occidentali nelle operazioni contro le forze russe, è improbabile che i cybercriminali russi sferrino attacchi distruttivi contro entità non ucraine in Europa. Tuttavia, CrowdStrike Intelligence stima che il governo russo probabilmente è disposto ad accettare il rischio di danni collaterali minori a entità esterne all'Ucraina derivanti da operazioni informatiche rivolte contro obiettivi militari ucraini.

---

16 https://assets.korearisk.com/uploads/2025/05/Unlawful-Military-Cooperation-including-Arms-Transfers-between-North-Korea-and-Russia-MSMT_2025_1-1.pdf

17 https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

18 https://www.dailynk.com/english/n-korea-uses-moscow-security-meeting-to-advance-intelligence-cooperation-with-russia/

19 https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-inukraine-and-poland/

RIPERCUSSIONI DEI CONFLITTI IN MEDIO ORIENTE

I conflitti cinetici in Medio Oriente, in particolare quelli tra Israele e Hamas, sono stati i principali motori delle operazioni informatiche sostenute dall'Iran e dell'hacktivismo filo iraniano contro le organizzazioni europee. Sebbene l'attività informatica iraniana si sia principalmente concentrata su entità basate in Israele, le tese relazioni diplomatiche tra l'Iran e le nazioni europee hanno spinto un limitato numero di cybercriminali legati all'Iran a prendere di mira le entità europee. Gli avversari legati all'Iran hanno condotto varie operazioni nella regione, tra cui attività di spionaggio e di hack-and-leak e campagne distruttive. Poiché le tensioni tra Israele e Iran rimangono alte, gli avversari legati all'Iran continueranno probabilmente a bersagliare Israele e i suoi alleati occidentali coinvolti nel conflitto, con operazioni di impersonificazione e campagne di spear phishing.

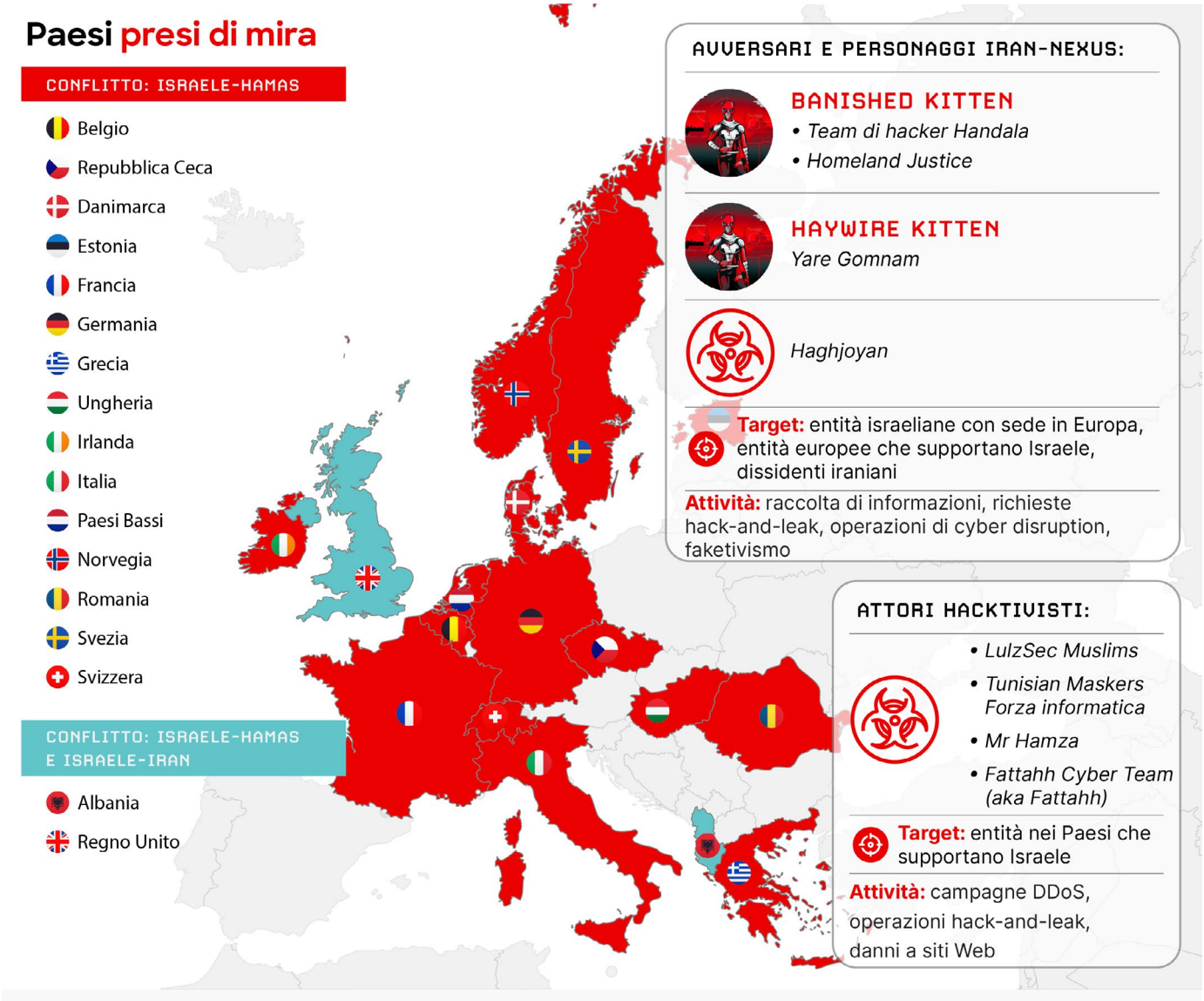


Figura 7. Ripercussioni degli avversari legati all'Iran e degli hacktivisti derivanti dai conflitti in Medio Oriente

Operazioni di raccolta di intelligence

Tra la fine di luglio e la metà di agosto 2025, le campagne di spear phishing, quasi certamente condotte da un cybercriminale legato all'Iran e affiliato al Corpo delle Guardie Rivoluzionarie Islamiche (IRGC), sono state rivolte a un'istituzione accademica basata nel Regno Unito, presumibilmente per raccogliere informazioni. L'avversario ha probabilmente utilizzato messaggi a tema lavorativo per indurre le vittime a scaricare ed eseguire il malware *AlDente*. Questa operazione ha coinciso con l'aumento delle tensioni tra Regno Unito e Iran riguardo ai negoziati sul nucleare e con la decisione di Germania, Francia e Regno Unito (noti collettivamente come E3) di attivare sanzioni con meccanismo "snapback" contro l'Iran alla fine di agosto 2025. Sebbene sia improbabile che l'Iran conduca operazioni palesemente destabilizzanti o distruttive durante i negoziati, è molto probabile che rimanga concentrato sulla raccolta di intelligence, mentre procede il processo di ripristino delle sanzioni.[20]

Operazioni di hack-and-leak

Dal 2024, i gruppi informatici legati all'Iran conducono operazioni di hack-and-leak in modo sempre più incisivo, sotto le spoglie di hacktivisti non autentici (noti anche come faketivisti), prendendo di mira organizzazioni israeliane o di paesi che sostengono pubblicamente Israele. Questa tattica viene impiegata come forma a basso costo di guerra asimmetrica, consentendo all'Iran di vendicarsi, destabilizzare i suoi avversari e influenzare l'opinione pubblica, mantenendo una negabilità credibile ed evitando un conflitto militare convenzionale.

A luglio 2025, due gruppi informatici collegati all'Iran, il gruppo di hacktivisti pro-IRGC *Gomnaman Team* e alcuni membri del team di hacker Handala di BANISHED KITTEN hanno rivendicato la responsabilità delle operazioni di hack-and-leak rivolte contro la testata mediatica dell'opposizione iraniana basata nel Regno Unito. I gruppi hanno rivendicato la divulgazione di informazioni personali di alcuni dipendenti, nonché e-mail e file sensibili. Questa attività è stata presumibilmente condotta in risposta alla cooperazione della testata con le agenzie di intelligence israeliane. Le affermazioni del *team di hacker Handala* e del *Gomnaman Team* di luglio 2025 sono parte di una più vasta campagna IO presumibilmente destinata a controllare le informazioni e a reprimere le attività dei dissidenti al di fuori del territorio iraniano, nonché a minare la fiducia nei media dell'opposizione in un momento politicamente delicato per il regime.

Operazioni di interruzione informatica

A gennaio 2024, *YareGonnam* di HAYWIRE KITTEN (noto anche come *Yare Gomnam Cyber Team*) ha rivendicato la responsabilità di un attacco DDoS contro un'organizzazione del governo olandese e un sito Web in lingua inglese di un'organizzazione collegata alla difesa. *YareGomnam* ha dichiarato che gli attacchi DDoS sono stati sferrati in risposta alla partecipazione dei Paesi Bassi alla coalizione guidata dagli Stati Uniti, responsabile degli scioperi contro i siti militari degli Houthi nello Yemen tenuti a gennaio 2024. Tuttavia, la notizia trapelata a metà gennaio 2024 che annunciava la partecipazione di un ingegnere olandese nel sabotaggio nucleare iraniano del 2007 potrebbe essere stata influenzata dagli obiettivi prioritari del gruppo.

ATTIVITÀ DEGLI HACKTIVISTI LEGATA AI CONFLITTI

Tra gennaio 2024 e settembre 2025, i conflitti globali, inclusi quelli tra Russia e Ucraina, Israele e Hamas e Israele e Iran, ha scatenato un'ondata di attività da parte degli hacktivisti, tra cui attacchi DDoS, operazioni di hack-and-leak, danni a siti Web e attività distruttive. Sebbene questi attacchi siano stati prevalentemente rivolti contro entità all'interno dei paesi o delle regioni attivamente coinvolte nei conflitti, alcuni hanno avuto ripercussioni sulle nazioni europee. Gli attacchi degli hacktivisti sono stati sferrati in risposta al presunto sostegno all'Ucraina o a Israele contro organizzazioni finanziarie, telecomunicazioni, governative, energetiche, logistiche, forze dell'ordine e delle infrastrutture critiche europee.

20 https://www.iranintl.com/en/202507268188

Entità hactiviste	Attività regionali
BOUNTY JACKAL	Tra gennaio 2024 e settembre 2025, l'avversario hacktivista filorusso BOUNTY JACKAL ha condotto quasi quotidianamente diffuse campagne DDoS rivolte a entità europee in risposta al sostegno militare o finanziario fornito all'Ucraina o ai presunti sentimenti russofobi. Quasi certamente, la scelta del bersaglio è in gran parte opportunistica; l'avversario ha utilizzato il suo toolkit di attacco *DDoSia* per coordinare le campagne con la sua rete globale di volontari. Oltre a fornire supporto DDoS tramite i volontari, BOUNTY JACKAL ha collaborato con hacktivisti con vedute simili , tra cui *UserSec*, *Fronte Popolare di liberazione*, *Cyber Army of Russia (CARR)*, *HackNeT* e *Z-Alliance* in molteplici occasioni per sferrare attacchi a entità finanziarie, delle telecomunicazioni, governative, energetiche, logistiche, forze dell'ordine e infrastrutture critiche nonché a un'alleanza militare occidentale. Numerose campagne di BOUNTY JACKAL sono state quasi certamente programmate per coincidere con le elezioni o le proteste in corso in Europa. Questo scenario evidenzia le più ampie motivazioni anti-UE dell'avversario, pur rimanendo in linea con il presunto sostegno dei paesi all'Ucraina, e dimostra il suo desiderio di attirare l'attenzione, sincronizzando gli attacchi con i principali eventi nel territorio di interesse.
Cyber Army of Russia (noto anche come *CARR*)	Nel corso del 2024, gli hacktivisti filorussi del *CARR* hanno rivendicato le numerose campagne DDoS contro entità europee come rappresaglia per il sostegno militare e finanziario occidentale all'Ucraina. Il *CARR* ha anche rivendicato diverse campagne condotte insieme a BOUNTY JACKAL e *Z-Alliance*, tra cui gli attacchi DDoS dell'aprile 2024 contro i siti Web del governo spagnolo e di entità operanti nel comparto energetico e logistico del paese. A settembre e ottobre 2024, il *CARR* ha rivendicato la responsabilità della compromissione del sistema di controllo industriale (ICS) di Polonia, Francia, Stati Uniti e Taiwan. A dicembre 2024, il *CARR* ha eliminato il suo canale Telegram pubblico e ha annunciato che i membri del gruppo avrebbero continuato a condurre attacchi DDoS con lo pseudonimo *Z-Alliance*.
Fattahh Cyber Team (noto anche come *Fattahh*)	A gennaio 2024, il gruppo di hackivisti *Fattahh Cyber Team*, affiliato al Corpo delle Guardie Rivoluzionarie Islamiche (IRGC), ha danneggiato il sito Web di un produttore olandese con messaggi pro-Houthi. Sebbene gli hacktivisti risultino ancora attivi a ottobre 2025, questo incidente rimane finora l'unico caso noto di attacco all'Europa.
LulzSec Muslims	Almeno fino ad agosto 2024, il gruppo di attivisti filo palestinese e filo islamico *LulzSec Muslims* ha rivendicato gli attacchi a numerose entità a livello globale, incluse alcune organizzazioni di paesi dell'Europa occidentale, settentrionale e meridionale, ma nessuna dell'Est Europa a parte l'Ucraina. L'attività ha incluso operazioni di hack-and-leak, attacchi DDoS e danneggiamenti di siti Web di entità con sede in paesi che il gruppo percepisce come sostenitori diretti o indiretti di Israele, nell'ambito dei conflitti con Hamas.
Mr Hamza	A gennaio 2025, l'hacktivista filo islamico *Mr Hamza* ha rivendicato gli attacchi DDoS contro la polizia federale e nazionale, entità di sicurezza e di intelligence, un ministero della difesa e i servizi militari in Belgio, Repubblica Ceca, Danimarca, Estonia, Germania, Ungheria, Irlanda, Italia, Paesi Bassi, Norvegia, Romania, Svezia e Stati Uniti. Questa attività è stata motivata dal presunto sostegno di questi paesi a favore di Israele.
Tunisian Maskers Cyber Force	Da maggio a giugno 2025, il gruppo di hacktivisti filo palestinese *Tunisian Maskers Cyber Force* ha condotto la campagna #Dark_Pulse_V2 contro entità basate in Europa, in risposta al sostegno del Regno Unito a Israele nel conflitto Israele-Hamas. L'hacktivista ha rivendicato gli attacchi DDoS contro entità finanziarie, di servizi professionali, di ospitalità e di vendita al dettaglio con sede nel Regno Unito e ha condiviso i link agli strumenti di monitoraggio di siti Web per dimostrare il successo della campagna. Nell'ambito della campagna, *Tunisian Maskers Cyber Force* ha minacciato di rendere pubbliche le e-mail di un ente governativo non specificato (presumibilmente con sede in Europa) e i dati verosimilmente ottenuti da un entità di servizi professionali colpita in passato. Tuttavia, poiché successivamente gli hacktivisti non hanno menzionato queste minacce né pubblicato i dati sui loro canali social media noti, non sappiamo se abbiano dato seguito alle minacce.
Z-Alliance (noto anche come *Z-Pentest*)	Tra la fine del 2024 e l'inizio del 2025, *Z-Alliance* ha rivendicato la violazione dei sistemi di supervisione e acquisizione dati (SCADA) di almeno sei entità di Stati Uniti, Francia, Germania, Ucraina e Taiwan e la compromissione dei sistemi ICS in Francia, Grecia, Lituania, Italia, Polonia, Spagna e Svezia. Questi compromissioni sono state motivate dai sentimenti filorussi, anti-ucraini e anti-occidentali del gruppo e probabilmente tesi a guadagnare notorietà.

Tabella 1. Attività degli hacktivisti contro bersagli europei

I conflitti in corso e quelli emergenti continueranno molto probabilmente a motivare l'attività degli hacktivisti, sia all'interno delle aree di conflitto che a livello globale, poiché essi cercano di vendicarsi del supporto, di diffondere le loro ideologie o di sfruttare la copertura mediatica per attirare l'attenzione. Questa valutazione altamente affidabile è stata condotta sulla base delle attività degli hacktivisti in risposta ai conflitti globali in corso da almeno il 2022.

Attività informatica nation-state non legata ai conflitti

Sebbene i principali conflitti abbiano alterato gli obiettivi prioritari e il ritmo operativo di alcuni avversari nation-state, le motivazioni delle attività di spionaggio informatico rimangono costanti. La persistente domanda di intelligence da parte degli avversari nation-state, per informare la policy nazionale, supportare le imprese pubbliche o finanziare i regimi autocratici, garantisce la persistenza di una serie di operazioni informatiche.

ATTIVITÀ APPOGGIATA DALLA RUSSIA

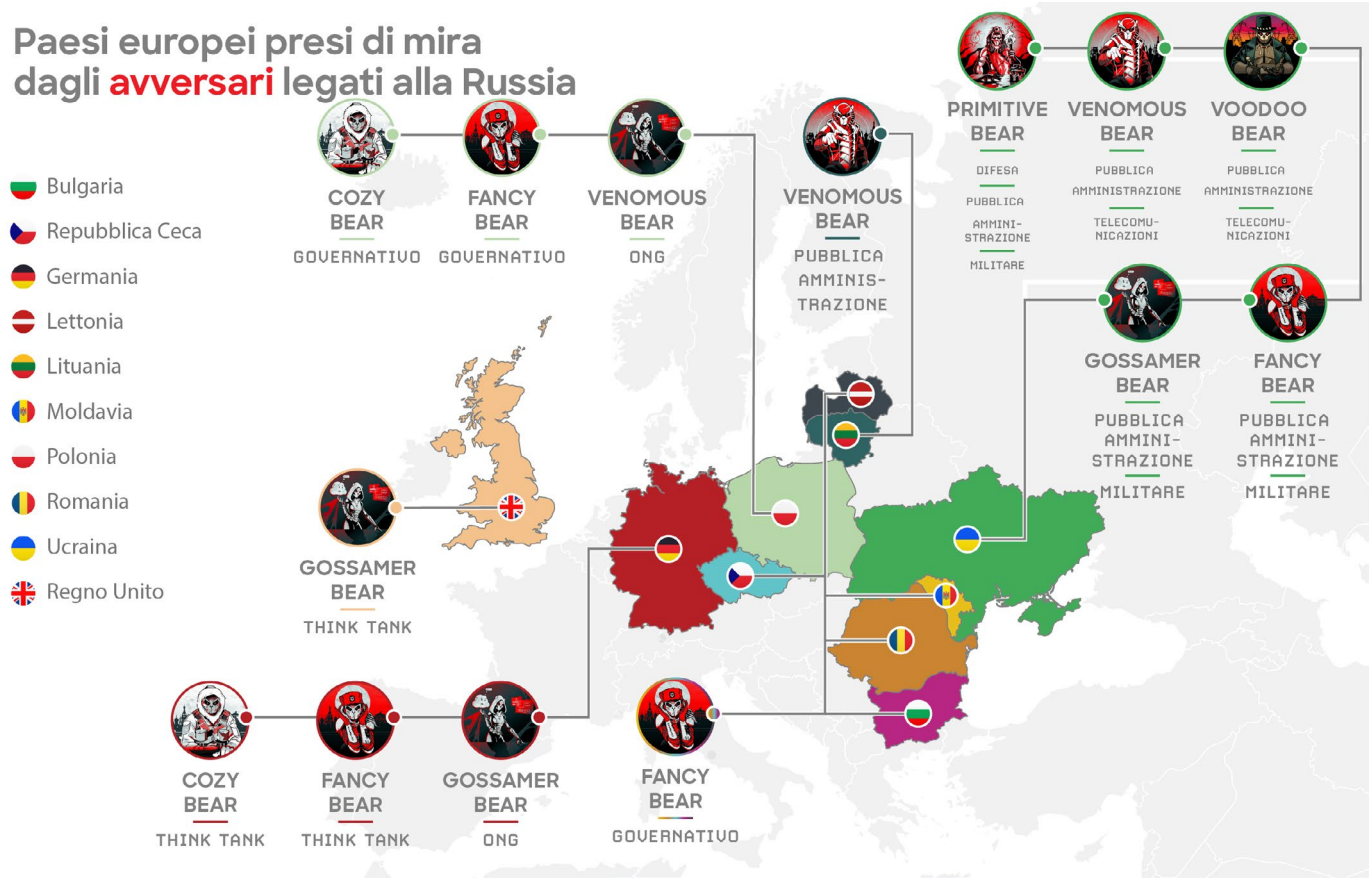
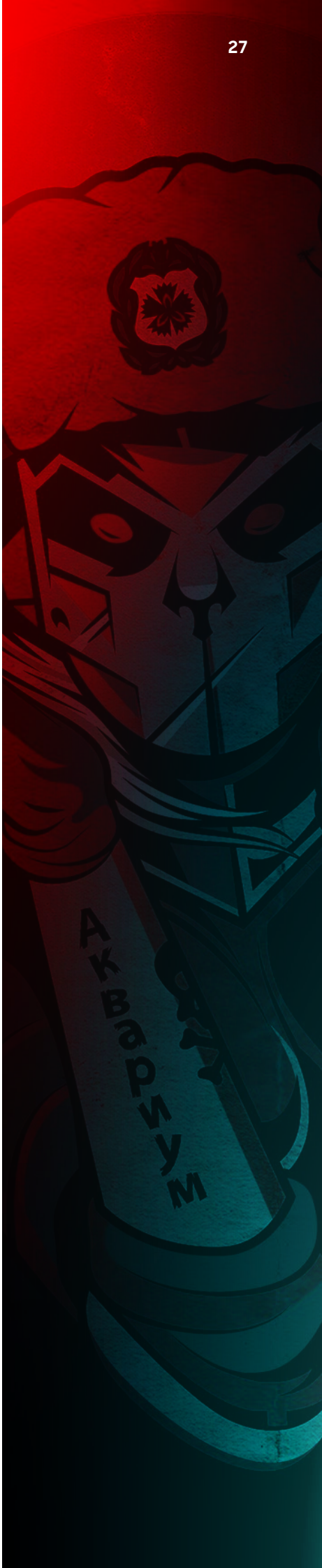


Figura 8. Avversari legati alla Russia interessati ai paesi europei

Sebbene gran parte degli avversari e dei cybercriminali nation-state legati alla Russia si concentri sull'Ucraina, l'obiettivo strategico di colpire altri stati europei, in particolare i paesi membri della NATO, rimane una priorità.

I modelli di raccolta di intelligence impiegati dagli avversari legati alla Russia tra i vari settori sono in linea con gli obiettivi politici e militari che la Russia ha definito riguardo all'Europa. Per sostenere ulteriormente le attività belliche della Russia in Ucraina, questi avversari raccolgono informazioni strategiche, operative e tattiche, consentendo alla Russia di tracciare gli aiuti militari a favore dell'Ucraina. Colpire queste entità probabilmente agevola anche la Russia nel raccogliere informazioni politiche per strumentalizzare le spaccature interne che minano il sostegno all'Ucraina da parte dell'Europa e fratturano la coesione della NATO e dell'UE.



Le operazioni informatiche dei cybercriminali appoggiate dalle Russia e condotte per colpire le organizzazioni dei paesi europei non appartenenti alla NATO, probabilmente perseguono obiettivi strategici distinti. Per le organizzazioni dei paesi allineati all'Occidente, queste intrusioni probabilmente mirano in primis a raccogliere informazioni e monitorare i rapporti con l'UE e la NATO. Per i paesi che cercano attivamente di integrarsi con queste istituzioni, i cybercriminali probabilmente intendono monitorare e potenzialmente ostacolarne l'ingresso e riaffermare la sfera di influenza della Russia sulla regione.

Queste operazioni mostrano come la Russia integri le sue attività di raccolta di intelligence con quelle di influenza, concentrandosi sulle attività della NATO, sui rapporti energetici e sullo sviluppo di policy. La persistenza dei cybercriminali e l'alto volume di campagne indicano che la Russia sta destinando risorse di alto livello a queste attività e sta dando priorità alla raccolta di intelligence e alle operazioni di influenza in Europa.

Settore governativo europeo nel mirino

Fancy Bear, avversario operato dal GRU, ha mantenuto un ritmo operativo molto elevato nei confronti degli enti governativi europei. Per tutto il 2024, l'avversario ha sfruttato le vulnerabilità e condotto campagne di malware probabilmente mirate agli enti governativi di nazioni europee tra cui Polonia, Moldavia, Repubblica Ceca, Bulgaria e Lettonia. Nel corso del 2025, FANCY BEAR continua a sfruttare le vulnerabilità nei client di webmail come Zimbra, Roundcube e MDaemon per acquisire i dati di autenticazione, reindirizzare ed esfiltrare le e-mail.

Molto probabilmente, FANCY BEAR ha preso di mira entità governative della Repubblica Ceca mediante esche di collaborazione con la NATO e ha sfruttato le vulnerabilità NTLM contro le organizzazioni governative della Romania, evidenziando i suoi persistenti obiettivi di raccolta di intelligence. Gli Stati membri della NATO e i paesi che hanno stabilito partnership formali e accordi di cooperazione con la NATO rimarranno un obiettivo primario a lungo termine per le future operazioni di FANCY BEAR.

Da ottobre 2020, l'avversario COZY BEAR, operato dal Servizio di Intelligence Estera della Federazione Russa (SVR), ha continuato a portare avanti la sua campagna DiplomaticOrbiter rivolta ai Ministeri degli Affari Esteri europei per raccogliere informazioni, in linea con gli obiettivi diplomatici e strategici dell'SVR. L'avversario ha ripreso le operazioni a gennaio 2025 e molto probabilmente ha utilizzato e-mail di spear phishing per consegnare il suo nuovo downloader personalizzato *BoomTwins*. A ottobre 2024, COZY BEAR ha presumibilmente cercato di colpire le organizzazioni governative europee durante una campagna mirata su ampia scala. L'avversario ha distribuito file RDP dannosi e ha registrato più di 180 domini che riproducono quelli di ministeri della difesa, forze armate e think tank.

Tra il 2023 e il 2025, VENOMOUS BEAR ha distribuito il suo impianto *CoreTech* e *Kazuar RAT* in campagne rivolte a più organizzazioni governative dell'Est Europa, incluse quelle dell'Ucraina. Dall'invasione su vasta scala della Russia, CrowdStrike Intelligence ha osservato solo un'attività Venomous Bear limitata, rivolta contro i paesi dell'Est Europa, inclusa l'Ucraina. Tuttavia, CrowdStrike Intelligence valuta con moderata sicurezza che Venomous Bear abbia preso e continuerà a prendere

di mira le organizzazioni governative dell'Est Europa, presumibilmente per esigenze ordinarie di raccolta di intelligence che l'avversario ha definito insieme alle sue capacità di raccolta prima di febbraio 2022.

Per tutto il 2024 e il 2025, il cluster di attività RepeatingUmbra appoggiato dalla Russia ha preso di mira persone e organizzazioni dell'Est Europa, utilizzando campagne di phishing delle credenziali e malware. Il cluster di attività ha condotto massicce operazioni di phishing delle credenziali contro persone ed enti pubblici polacchi, lituani, lettoni e ucraini, nonché persone di lingua russa.

Inoltre, RepeatingUmbra ha continuato a utilizzare documenti dannosi per consegnare diversi loader, tra cui *Pryatki*, riuscendo a distribuire il beacon *Cobalt Strike* in entità dell'Est Europa. Molto probabilmente, RepeatingUmbra continua a raccogliere informazioni sulle attività IO, come la compromissione degli account dei social media dei politici e il riciclaggio di dati rubati attraverso gruppi di hacktivisti, al fine di destabilizzare i paesi dell'Est Europa.

Ad agosto e settembre 2025, un probabile cybercriminale di eCrime legato alla Russia ha condotto alcune campagne di phishing su WhatsApp rivolte a organizzazioni e persone della Moldavia, tra cui un probabile membro delle forze armate nazionali. Il cybercriminale ha abusato delle funzionalità di collegamento dei dispositivi per accedere agli account WhatsApp delle vittime. A settembre 2025, secondo quanto riferito, il cybercriminale ha utilizzato l'applicazione di messaggistica Signal per distribuire un link che collegava a un sito Web dannoso, falsificando una petizione legittima a sostegno di un manifesto economico moldavo. Il sito Web invitava le vittime ad accedere a WhatsApp per "prevenire frodi elettorali".

Sempre a settembre 2025, un altro probabile cybercriminale legato alla Russia ha sfruttato a suo favore i server di Zimbra Collaboration compromessi per raccogliere e-mail. Il cybercriminale ha indicato che il suo ambito di applicazione comprende organizzazioni governative, no-profit, politiche e logistiche situate in Europa, in particolare in Moldavia. CrowdStrike Intelligence ritiene che il cybercriminale non identificato stia probabilmente raccogliendo informazioni per conto dell'FSB.

Settore della difesa europeo nel mirino

A ottobre 2024, COZY BEAR ha sfruttato lo spoofing di domini, utilizzando domini registrati almeno dall'agosto 2024, per colpire un'organizzazione internazionale di difesa, nonché governi entità governative e private di Europa e Nord America. Inoltre, a luglio 2025, le sanzioni del governo del Regno Unito contro gli operatori dell'unità GRU 26165 affermano che il gruppo aveva avuto accesso alle telecamere IP private installate a ridosso di strutture militari, porti, valichi di frontiera e altre infrastrutture di trasporto in diversi paesi europei, tra cui la Moldavia. Questo evidenzia le ampie esigenze di raccolta di intelligence della Russia riguardanti obiettivi militari e infrastrutture di importanza critica.

Il settore energetico europeo utilizzato nei contenuti esca

In una campagna di aprile 2024, FANCY BEAR aveva utilizzato esche sul tema dell'energia rinnovabile, probabile segno che l'energia è una priorità importante per la raccolta dei servizi di intelligence russi (RIS), a causa delle pesanti sanzioni sull'industria petrolifera e del gas della Russia. FANCY BEAR ha utilizzato un sottodominio che ospitava un documento esca che falsificava il "profilo energetico" dell'Austria pubblicato da un'organizzazione intergovernativa del settore energetico.

A dicembre 2023, l'Austria importava il 98% del suo gas dalla Russia.[21] A febbraio 2024, il Ministero dell'Energia austriaco annunciava che il Paese stava cercando di terminare il contratto di importazione con Gazprom. Sebbene l'esatto campo d'azione della campagna rimanga sconosciuto, la presenza di un'esca indica che FANCY BEAR stava potenzialmente prendendo di mira le organizzazioni energetiche europee. L'operazione dimostra le esigenze di intelligence a lungo termine della Russia riguardo ai rapporti energetici e allo sviluppo di policy in Europa.

Settore think tank europeo nel mirino

Tra la fine del 2023 e il secondo trimestre del 2024, il gruppo GOSSAMER BEAR, controllato dall'FSB, ha condotto campagne di phishing delle credenziali contro organizzazioni think tank del Regno Unito, specializzate in affari internazionali, difesa e sicurezza. L'avversario ha probabilmente utilizzato i dati come arma in successive operazioni di influenza hack-and-leak. Come parte delle sue operazioni raccolta di intelligence, anche FANCY BEAR ha sfruttato le vulnerabilità NTLM contro un ente governativo rumeno e probabilmente contro un'organizzazione think tank tedesca. Nel frattempo, la campagna DiplomaticOrbiter di COZY BEAR ha preso di mira i think tank occidentali come parte della sua raccolta di intelligence ordinaria.

DURANTE LA SUA CAMPAGNA DI PHISHING CONDOTTA A OTTOBRE 2024, COZY BEAR HA REGISTRATO PIÙ DI 180 DOMINI CHE FALSIFICAVANO ENTITÀ THINK TANK E ORGANIZZAZIONI DELLA DIFESA. L'ATTIVITÀ DIMOSTRA LA PROBABILE PRIORITÀ CHE L'AVVERSARIO ASSEGNA AL MONITORAGGIO DI ENTITÀ GOVERNATIVE, TECNOLOGICHE, DELLA DIFESA E NO-PROFIT OCCIDENTALI, CONSIDERATE DI ALTO VALORE PER LA RACCOLTA DI INTELLIGENCE STRATEGICA.

Media e organizzazioni ONG europee nel mirino

GOSSAMER BEAR ha rivolto i suoi attacchi contro i media e le ONG europee coducendo utilizzando campagne di hack-and-leak e utilizzando documenti rubati come arma per le operazioni IO. Da gennaio ad agosto 2025, GOSSAMER BEAR ha continuato a condurre operazioni di phishing delle credenziali, probabilmente rivolte a think tank, dissidenti e ONG in Europa e Africa. In linea con l'attenzione storica dell'avversario per le "organizzazioni indesiderabili",[22] nel 2025, GOSSAMER BEAR ha rivolto i suoi attacchi ad almeno una ONG che promuove le relazioni con la società civile della Germania e dei paesi dell'Est Europa.

Dopo l'inizio del conflitto tra Israele e Hamas ad ottobre 2023, GOSSAMER BEAR ha registrato diversi domini che falsificano un'entità delle forze dell'ordine europee per acquisire credenziali di Microsoft Outlook di persone associate. All'inizio di febbraio 2024, GOSSAMER BEAR ha registrato domini che si spacciano per un'organizzazione europea di addestramento militare focalizzata sull'Africa, in linea con il crescente interesse strategico di Mosca per l'Africa. La Russia si sta posizionando come valida alternativa ai partner occidentali dell'Africa, mentre l'esercito dell'UE e degli Stati Uniti riducono la loro presenza nel continente. La raccolta di intelligence e le campagne IO di GOSSAMER BEAR spesso prevedono operazioni di hack-and-leak che sfruttano i documenti rubati a enti governativi, media, think tank e ONG a scopo offensivo.

A gennaio 2024, VENOMOUS BEAR ha preso di mira una ONG polacca con una nuova backdoor chiamata *dcmd*. Questa attività è in linea con le esigenze di raccolta di intelligence a lungo termine dell'avversario e con l'aumento delle entità polacche come bersagli, presumibilmente per il fatto che la Polonia accoglie rifugiati dell'Ucraina e fornisce aiuti al paese.

---

21 https://www.reuters.com/markets/europe/austria-seeking-end-russian-gas-import-contract-energy-minister-says-2024-02-12/

22 La Russia considera "indesiderabili" quelle organizzazioni che percepisce come una minaccia straniera per gli interessi dello stato russo, impedendo loro di condurre affari all'interno della Russia.

ATTIVITÀ LEGATA ALL'IRAN

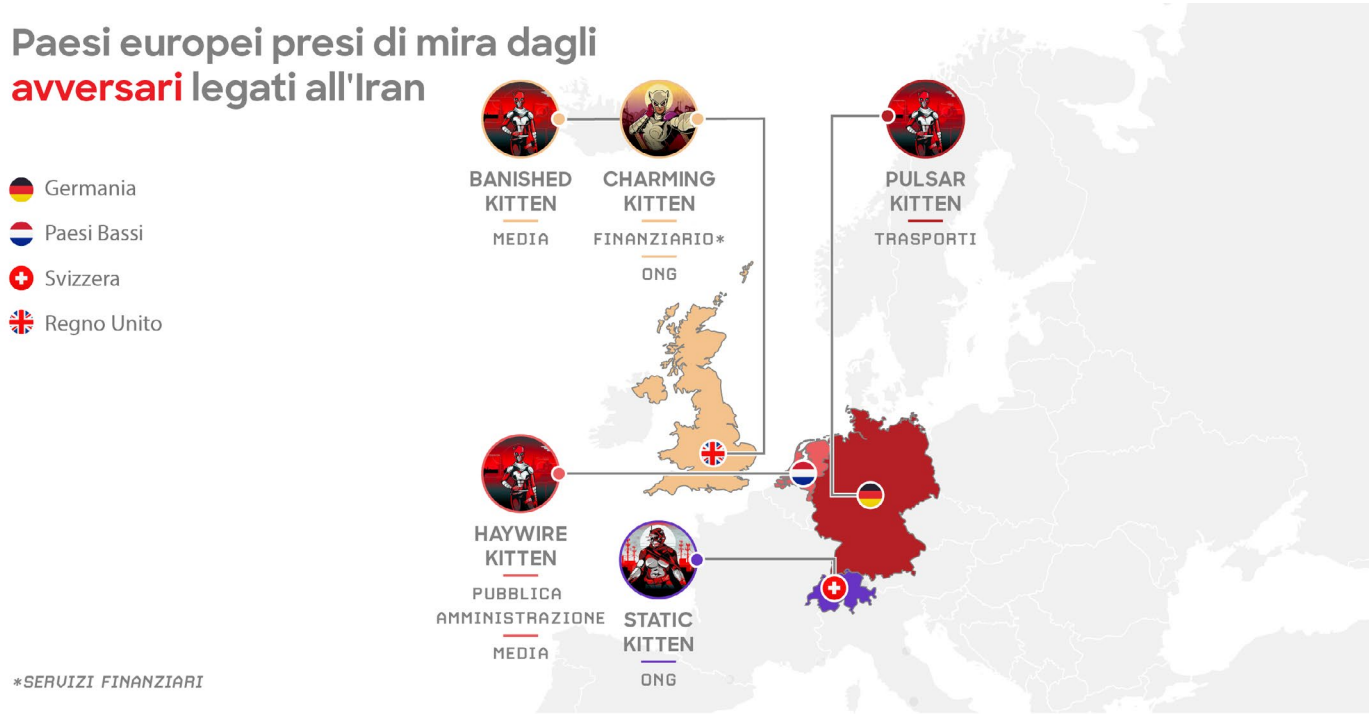


Figura 9. Avversari legati all'Iran interessati ai paesi europei

Gli avversari legati all'Iran hanno concentrato i loro attacchi principalmente su Israele, sui suoi alleati e su altri obiettivi in Medio Oriente a causa delle continue tensioni regionali. Tuttavia, hanno anche continuato a raccogliere intelligence da obiettivi europei, in particolare da quelli che si oppongono agli interessi dello Stato dell'Iran. Anche se l'Iran probabilmente si asterrà dall'intraprendere attività informatiche offensive di tipo distruttivo o destabilizzante durante i suoi continui tentativi di riprendere i negoziati sul nucleare, i cybercriminali legati all'Iran rappresentano una minaccia ancora maggiore per le nazioni europee.

Alla fine di agosto 2025, l'E3 ha avviato il processo di sanzioni con meccanismo "snapback" contro l'Iran.[23] Con ogni probabilità, l'Iran non considera l'attività di raccolta di intelligence come un'attività informatica apertamente offensiva, quindi l'avvio del processo di sanzioni spingerà probabilmente gli avversari legati all'Iran a rivolgersi ai paesi E3 per raccogliere informazioni.

Settore governativo europeo nel mirino

Gli avversari legati all'Iran hanno costantemente preso di mira le entità governative europee, in particolare quelle che si oppongono agli interessi dello Stato dell'Iran. Probabilmente a partire da gennaio fino a marzo 2025, un cybercriminale non attribuito legato all'Iran ha condotto una campagna di spear phishing contro un importante rappresentante del Parlamento europeo tedesco che guida alcune operazioni a sostegno dei gruppi di opposizione iraniani.

Per la campagna, ha sfruttato le chiamate vocali e tecniche sofisticate di social engineering, con lo staff del politico tedesco che avrebbe ricevuto messaggi e telefonate da criminali informatici sconosciuti che si spacciavano per un contatto legittimo associato a un think tank basato negli Stati Uniti. Alla fine, i cybercriminali hanno compromesso i sistemi e installato il software dannoso su un laptop dell'ufficio del politico. Sebbene siano riusciti a compromettere i sistemi della vittima, le misure di sicurezza del Parlamento europeo avrebbero impedito qualsiasi furto di dati sensibili.

Il politico tedesco è stato probabilmente scelto come bersaglio per la sua posizione politica e per la vicinanza professionale ai dissidenti iraniani.

23 https://www.iranintl.com/en/202507268188

Settore dei servizi finanziari europeo nel mirino

A maggio 2024, CHARMING KITTEN ha condotto campagne di phishing contro organizzazioni finanziarie basate nel Regno Unito, con l'obiettivo di raccogliere informazioni. L'avversario ha adattato le sue operazioni utilizzando infrastrutture falsificate, social engineering specifico per la vittima e siti Web che falsificano entità legittime. Ha inoltre sistematicamente abusato di servizi legittimi come Microsoft OneDrive per distribuire il malware personalizzato.

Settore dei trasporti europeo nel mirino

A metà luglio 2025, PULSAR KITTEN ha probabilmente condotto un'operazione di spear phishing contro la filiale tedesca di un'azienda di trasporti con sede negli Stati Uniti. L'avversario ha utilizzato offerte di lavoro in ambito aeronautico per distribuire il suo sofisticato malware *SilkySand* tramite il servizio legittimo di condivisione dei file ONLYOFFICE. L'avversario ha condotto l'operazione in un contesto di crescenti tensioni tra Iran e Germania, in particolare a seguito di dichiarazioni controverse sul conflitto tra Israele e Iran e delle minacce europee di nuove sanzioni. L'operazione aveva sia finalità politiche sia di raccolta di intelligence e favoriva gli interessi del controspionaggio iraniano in Europa occidentale. PULSAR KITTEN aveva precedentemente falsificato i siti Web di alcune case automobilistiche tedesche, ma non è stato mai osservato che mirasse a organizzazioni di trasporto.

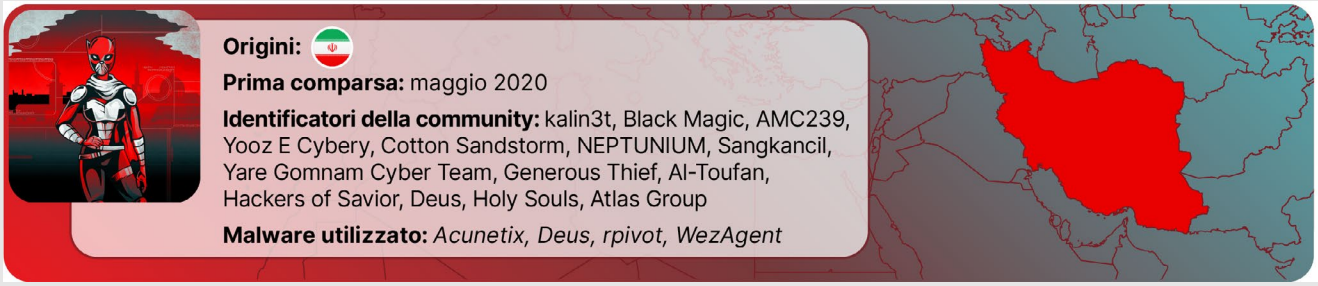
Gli avversari legati all'Iran affiliati all'IRGC, inclusi PULSAR KITTEN, IMPERIAL KITTEN, un cybercriminale non attribuito legato all'Iran e HAYWIRE KITTEN, hanno probabilmente simulato o preso di mira entità con sede in Germania dall'inizio e fino alla metà del 2025.

Settore delle ONG europeo nel mirino

Ad agosto 2025, STATIC KITTEN ha condotto una campagna di raccolta di intelligence rivolta alla filiale del Sud-Est asiatico di una ONG con sede in Svizzera. L'avversario ha probabilmente ottenuto l'accesso iniziale mediante la compromissione del server Web; tuttavia, l'ONG non lo ha confermato.

Una volta stabilito il punto d'appoggio, STATIC KITTEN ha utilizzato un account di servizio compromesso per muoversi lateralmente attraverso la rete. Utilizzando l'accesso con privilegi elevati, l'avversario ha invocato PowerShell per scaricare una carica distruttiva dannosa da un indirizzo IP da lui controllato. Infine, ha tentato di scrivere gli hive di registro sul disco e raccogliere le credenziali, quasi certamente per preparare l'esfiltrazione.

La probabile campagna di phishing di HAYWIRE KITTEN prende di mira l'Europa



A partire da almeno dicembre 2024 e fino a luglio 2025, HAYWIRE KITTEN ha probabilmente condotto una campagna di phishing su larga scala a tema Microsoft rivolta a organizzazioni occidentali di vari settori. La sua attività si è concentrata su entità tecnologiche, di energia rinnovabile, manifatturiere e dell'ospitalità. Alcune prove suggeriscono che l'avversario abbia preso di mira organizzazioni in Francia, Germania, Spagna, Svizzera e Stati Uniti. Il gruppo ha distribuito pagine di raccolta delle credenziali a tema Microsoft e ha probabilmente utilizzato e-mail di spear phishing con allegati PDF come esca per richiedere il preventivo per uno spazio per eventi che ospita varie fiere e conferenze in Germania.

L'obiettivo di HAYWIRE KITTEN di colpire entità tecnologiche, di energia rinnovabile e ospitalità rispecchia gli interessi strategici dell'Iran e segue i modelli storici rivolti contro l'Occidente. L'avversario ha probabilmente condotto questa attività per raccogliere informazioni.

L'attività è inoltre coerente con il modello di HAYWIRE KITTEN di colpire le entità occidentali e mette in evidenza la sua capacità di sviluppare domini infrastrutturali. CrowdStrike Intelligence ritiene che HAYWIRE KITTEN presumibilmente controlli l'infrastruttura associata a questa campagna di phishing a tema Microsoft; tuttavia, non è chiaro se l'infrastruttura sia stata resa operativa e implementata con successo.

ATTIVITÀ LEGATA ALLA CINA

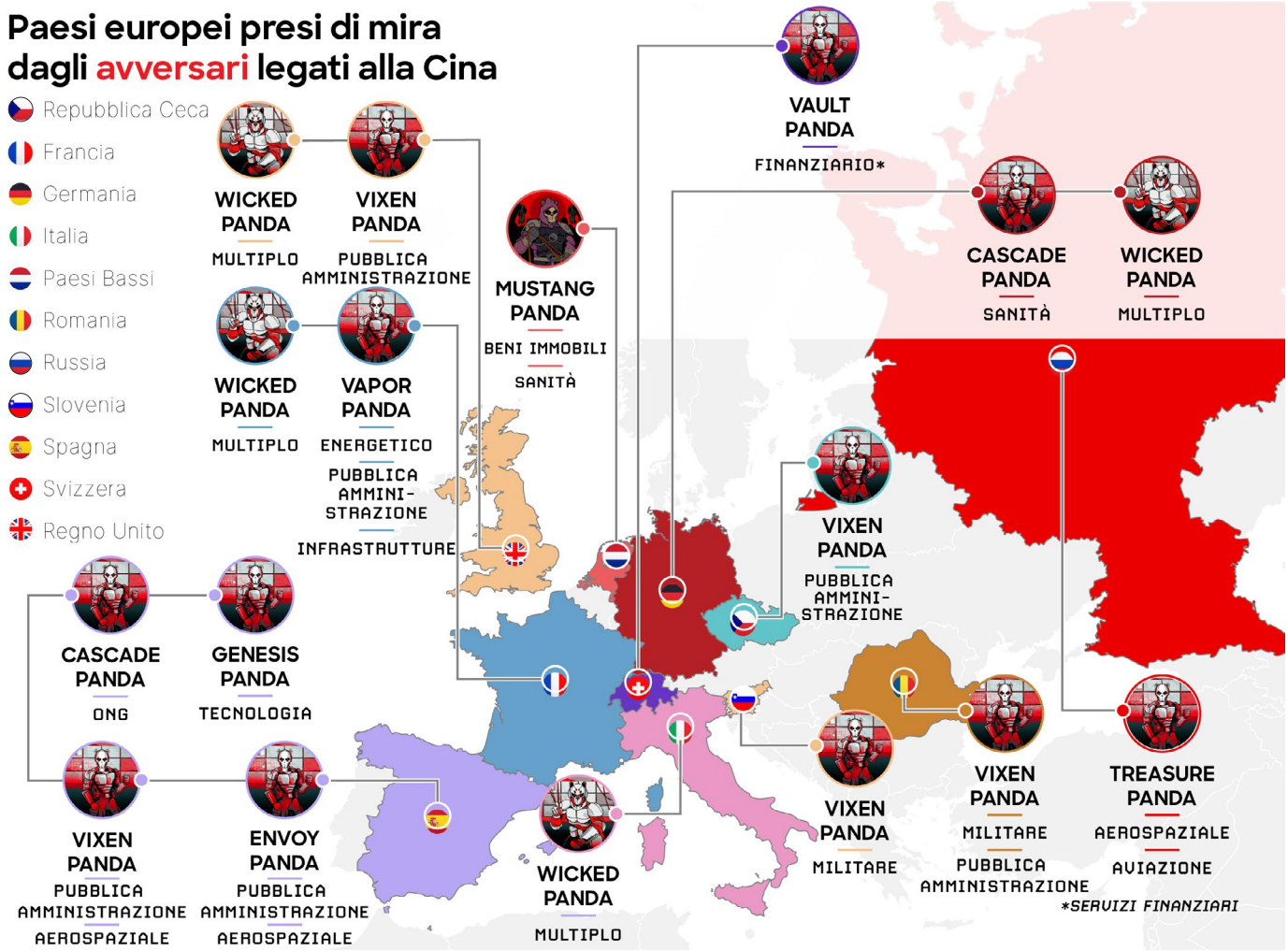


Figure 10. Paesi europei presi di mira da avversari legati alla Cina

L'UE, uno dei maggiori partner commerciali e destinazione di investimenti della Cina, svolge un ruolo chiave nelle aspirazioni del paese asiatico di migliorare l'integrazione con la regione, attraverso il commercio in Asia centrale e nell'Est Europa. Nella sua attività informatica rivolta all'Europa, la Cina è rimasta costantemente concentrata sulla probabile raccolta di informazioni utili per alimentare l'impegno politico ed economico di Pechino nei riguardi della regione. Pechino mira anche a sostenere le priorità strategiche del governo in un periodo attualmente turbolento per le relazioni UE-USA per quanto riguarda le questioni commerciali e di difesa. I cybercriminali legati alla Cina continuano a rivolgere gli attacchi contro entità governative, di difesa, industriali e aerospaziali europee.

Le operazioni dei cybercriminali contro l'Europa probabilmente mirano a sostenere le priorità strategiche della Cina, come il potenziamento dell'economia e l'abbattimento delle interferenze straniere. La Cina mira anche a raggiungere l'autosufficienza in aree scientifiche e tecnologiche strategiche, considerato che il suo accesso alle tecnologie avanzate prodotte al di fuori del paese è sempre più limitato.

Il settore della sanità e delle biotecnologie europeo come obiettivo

Molti avversari legati alla Cina continuano a prendere di mira in modo persistente il settore sanitario e biotecnologico, uno dei bersagli più allettante in Europa. Ad aprile 2024, CASCADE PANDA ha tentato di distribuire il malware *WinDealer* in un'organizzazione biotecnologica tedesca operante in Cina, a riprova della continua attenzione dell'avversario per le entità con una presenza transfrontaliera.

Le operazioni di MUSTANG PANDA hanno avuto ripercussioni su diverse organizzazioni sanitarie per tutto il 2023 e 2024. Queste operazioni distribuiscono malware modulari tramite USB, tra cui lo strumento di infezione *LubanBall*, i loader *Tangram* e *Foregram* e lo strumento di accesso remoto *LingerRAT.* Le capacità dell'avversario hanno continuato a evolvere e ad agosto 2024 MUSTANG PANDA ha distribuito *LubanBall* in un'organizzazione sanitaria basata nei Paesi Bassi.

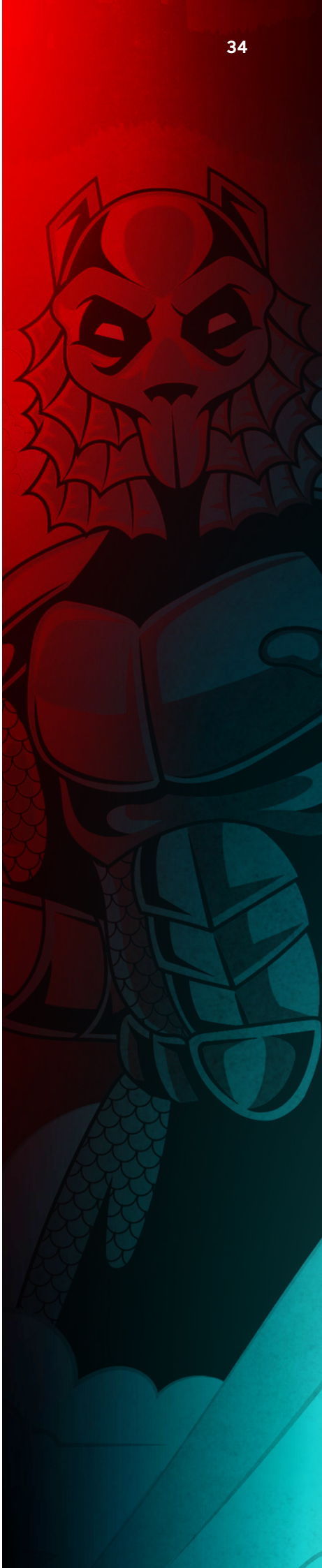
Probabilmente, i cybercriminali legati alla Cina prendono di mira questo settore per raccogliere informazioni, ottenere informazioni personali e rubare proprietà intellettuali che riguardano la ricerca e lo sviluppo di vaccini e tecnologie biomediche. Questo modello di attacco è in linea con l'interesse strategico della Cina di progredire le sue capacità biotecnologiche e comprendere le innovazioni mediche dell'Occidente, fondamentali per la sicurezza sanitaria nazionale.

Settore governativo e della difesa europeo nel mirino

Durante il periodo di riferimento, VIXEN PANDA si è dimostrata la minaccia più prolifica per le entità governative e della difesa europee. Dall'inizio del 2024 all'inizio del 2025, VIXEN PANDA è stato impegnato in operazioni sistematiche di scansione, tramite una rete di dispositivi ORB, tracciata come ORB02, che dimostrano la persistenza e la portata operativa dell'avversario.

Le attività condotte da VIXEN PANDA nella seconda metà del 2024 sono passate da attività estensive di ricognizione contro centinaia di dispositivi di sicurezza della rete in vari paesi europei a tentativi di exploit rivolti a dispositivi perimetrali di entità governative e della difesa in Slovenia, Romania, Repubblica Ceca e istituzioni dell'UE. La scelta di colpire le operazioni europee di un'agenzia del governo statunitense nel febbraio 2025 indica che VIXEN PANDA sta mantenendo il ritmo operativo e si sta concentrando su obiettivi governativi e di difesa di alto valore.

Tra settembre 2024 e marzo 2025, le osservazioni dei dati telemetrici di una rete di terze parti indicano che TREASURE PANDA ha probabilmente preso di mira le entità aerospaziali e della difesa della Russia, impegnate nello sviluppo di sistemi radar militari. L'ampio campo di applicazione dell'avversario si è esteso all'Est Europa, probabilmente a seguito dell'invasione dell'Ucraina da parte della Russia del 2022.



Nel gennaio 2024, un criminale informatico non attribuito legato alla Cina ha colpito un ente governativo italiano per eseguire attività hands-on-keyboard che includevano attività di ricognizione, dumping della memoria LSASS e il deployment dell'impianto *PlugX*. Questa attività si è verificata poco dopo che l'Italia si è formalmente ritirata dalla Belt and Road Initiative cinese a dicembre 2023, suggerendo potenziali motivazioni di ritorsione o di raccolta di intelligence.

La scelta di colpire diverse istituzioni dell'UE e dei paesi allineati alla NATO riflette probabilmente la priorità di Pechino di monitorare il coordinamento della difesa e lo sviluppo di policy in Europa. La Cina considera il governo europeo e le sue entità di difesa come fonti strategiche per comprendere le dinamiche delle alleanze occidentali, le capacità di difesa e i processi di sviluppo di policy. Gli avversari legati alla Cina continuano inoltre a bersagliare i paesi europei non allineati alla politica occidentale. Questi avversari hanno rivolto gli attacchi a entità russe, in linea con la missione geografica delle unità del Northern Theater Command dell'Esercito Popolare di Liberazione (PLA), con il probabile intento di raccogliere informazioni riguardanti la sicurezza e la difesa nazionale.

Settore manifatturiero europeo nel mirino

VERTIGO PANDA ha fissato il suo obiettivo sul settore manifatturiero europeo, utilizzando tecniche di exploit basate su USB. A febbraio 2024, VERTIGO PANDA ha preso di mira le operazioni di un'entità manifatturiera dell'Est Europa con sede in Vietnam, utilizzando un'unità USB infetta contenente componenti dannosi, tra cui l'impianto di signature *InstituteX* dell'avversario. Data la natura persistente della distribuzione di malware tramite supporti rimovibili, CrowdStrike Intelligence non è in grado di determinare se questi campioni rappresentino nuovi tentativi di VERTIGO PANDA di distribuire *InstituteX* o di reinfezioni ripetute.

Settore dei servizi finanziari europei nel mirino

Le entità di servizi finanziari devono affrontare i tentativi mirati di raccolta di intelligence, con VAULT PANDA che conduce attività di ricognizione rivolte a istituzioni finanziarie svizzere, come nel caso avvenuto a gennaio 2024. L'avversario ha utilizzato *Acunetix* per il riconoscimento iniziale e identificare le vulnerabilità sfruttabili.

Ad agosto 2024, WICKED PANDA ha condotto una campagna di phishing su larga scala rivolta a entità assicurative di vari paesi europei, tra cui Regno Unito, Francia, Italia e Germania. L'avversario ha utilizzato le e-mail compromesse delle autorità tributarie per distribuire il malware *Voldemort*.

Gli avversari legati alla Cina sembrano prendere di mira le istituzioni finanziarie per la raccolta di intelligence e il furto di informazioni personali. I dati raccolti probabilmente risultano utili per valutare gli asset monetari e facilitare le successive attività di intelligence. Questo suggerisce che la Cina ha interesse nel comprendere le capacità finanziarie dell'Europa e potenzialmente identificare gli obiettivi per future operazioni di spionaggio economico.

Settore accademico europeo nel mirino

Nell'ambito di campagne multisettoriali più ampie, le istituzioni accademiche e le organizzazioni di ricerca devono far fronte ad attacchi sistematici, con VIXEN PANDA che ad aprile 2024 ha condotto ricognizioni contro entità accademiche e istituti di ricerca dell'UE. Anche WICKED PANDA ha puntato l'obiettivo sulle istituzioni accademiche europee, conducendo, ad agosto 2024, una campagna di phishing che ha colpito più di 70 obiettivi a livello globale. Gli attacchi contro gli istituti di ricerca dell'UE e gli enti governativi e militari dimostrano che la Cina riconosce il ruolo fondamentale che il mondo accademico svolge nel progresso tecnologico e nelle capacità di difesa europee.

Settore tecnologico europeo nel mirino

A giugno e luglio 2025, CrowdStrike OverWatch e CrowdStrike Services hanno risposto all'attività di intrusione di GENESIS PANDA rivolta a un'azienda tecnologica con sede in Spagna. L'avversario ha probabilmente ottenuto l'accesso iniziale compromettendo un'istanza di Microsoft SQL Server. Durante l'intrusione, GENESIS PANDA ha eseguito attività di ricognizione basilari, ha tentato di muoversi lateralmente tramite Windows Remote Shell e ha scaricato diversi impianti e strumenti, tra cui *Sliver* e *Cobalt Strike*, da infrastrutture note controllate dall'avversario.

Durante il periodo di riferimento, l'attività legata alla Cina rivolta alle organizzazioni tecnologiche con sede in Europa è stata bassa; tuttavia, gli avversari connessi alla Cina hanno costantemente preso di mira le entità tecnologiche più di qualsiasi altro settore, a livello mondiale. Le organizzazioni tecnologiche sono regolarmente prese di mira per soddisfare le tradizionali esigenze di raccolta di intelligence e spionaggio industriale dell'avversario, evidenziando come lo spionaggio informatico sia parte integrante degli sforzi della Cina per la raccolta di intelligence. Dato che gli avversari legati alla Cina hanno storicamente e pesantemente preso di mira le entità tecnologiche di tutto il mondo, anche il settore tecnologico europeo è probabilmente un obiettivo ad alta priorità per il paese asiatico.

Settore delle ONG e delle organizzazioni no-profit europeo nel mirino

A giugno 2024, CASCADE PANDA ha distribuito con successo il malware *WinDealer* negli uffici di un'organizzazione no-profit dell'Europa occidentale basati in Cina. L'attacco dimostra l'interesse che la Cina ripone nel monitorare le ONG internazionali che operano nel territorio cinese e suggerisce potenziali preoccupazioni riguardo alle operazioni di influenza condotte da paesi stranieri o alle attività di raccolta di intelligence mediante le organizzazioni no-profit.

ATTIVITÀ LEGATE ALLA COREA DEL NORD

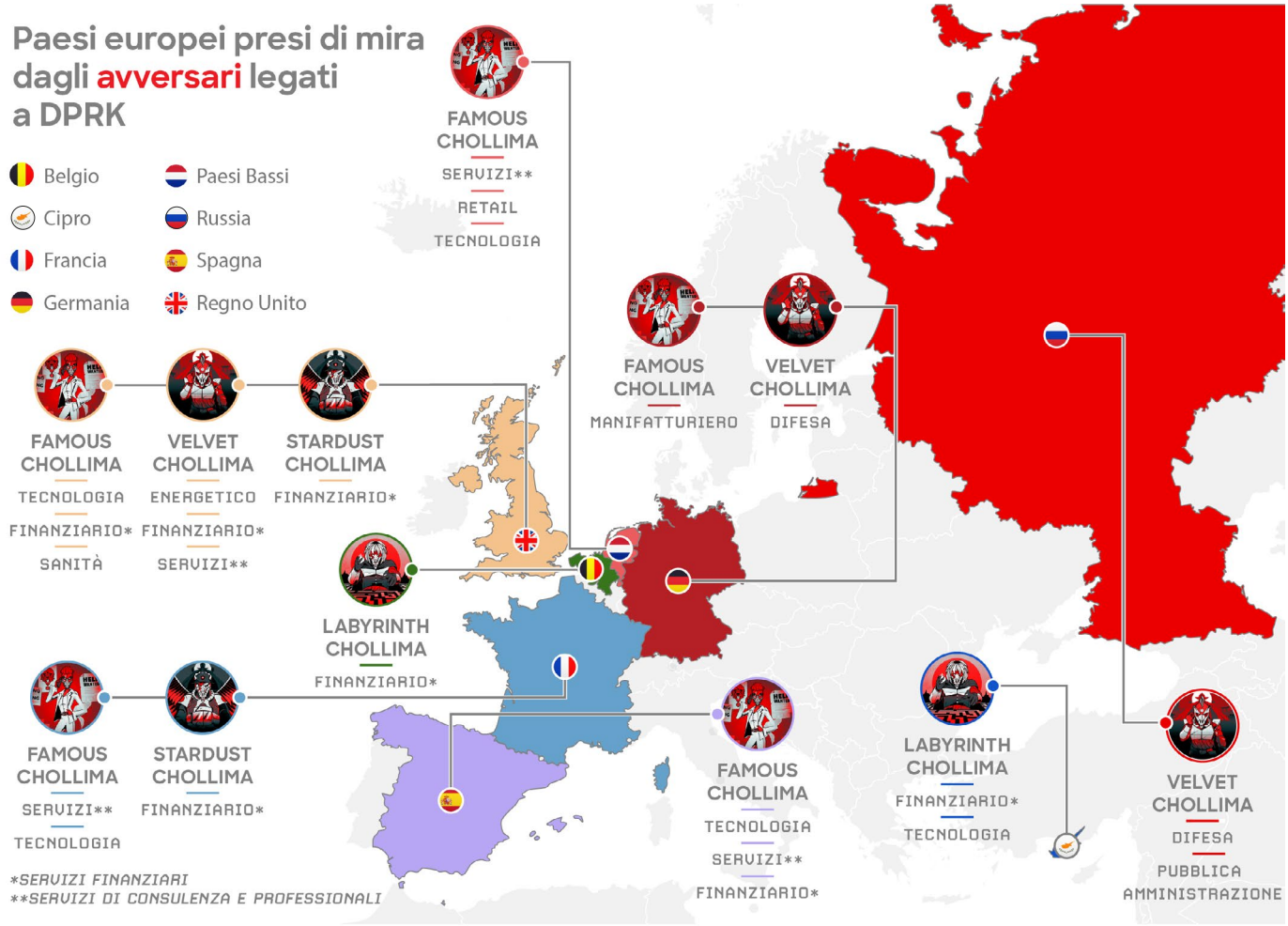


Figura 11. Avversari legati alla Corea del Nord interessati ai paesi europei

La Corea del Nord ha storicamente posto entità europee nel mirino, riconoscendo lo status di hub economico, diplomatico e militare della regione e la sua forte influenza sulle problematiche della penisola coreana. Gli avversari legati alla Corea del Nord sono motivati dalla raccolta di intelligence riguardante l'ambito di policy, tematiche militari e generazione di moneta virtuale e hanno preso di mira vari governi europei e organizzazioni della difesa, servizi finanziari e di consulenza. Queste attività sono in linea con le priorità della Corea del Nord di ottenere armi nucleari e tecnologia militare avanzata e di rafforzare la propria influenza nelle regioni del nord-est asiatico.

Settore della difesa europeo nel mirino

Da almeno aprile 2024, gli avversari VELVET CHOLLIMA e LABYRINTH CHOLLIMA legati alla Corea del Nord hanno posto nel mirino le entità della difesa europee per rubare le proprietà intellettuali e/o soddisfare le esigenze di intelligence militare. Questa attività presumibilmente supporta la tecnologia militare della Corea del Nord e consente al paese di ottenere informazioni tattiche sui sistemi di armamento europei che le forze militari ucraine potrebbero utilizzare contro i soldati della Corea del Nord coinvolti nel conflitto in alleanza con la Russia.

Inoltre, diversi paesi europei contribuiscono fornendo forze militari e materiale al Comando delle Nazioni Unite di stanza nella Repubblica di Corea. Il Comando delle Nazioni Unite è un organismo multilaterale fondato nel 1950 per contrastare l'aggressione nordcoreana nei confronti del sud del territorio, durante la Guerra di Corea. La Guerra di Corea si è conclusa con un armistizio ma i belligeranti sono rimasti in uno stato di guerra legale, rendendo le organizzazioni militari e di difesa europee un bersaglio attraente per le operazioni di spionaggio informatico della Corea del Nord.

Tra maggio 2024 e almeno settembre 2024, VELVET CHOLLIMA ha probabilmente preso di mira i dipendenti di un'azienda manifatturiera tedesca, operante nel settore della difesa, mediante una campagna di phishing delle credenziali che distribuiva il malware proprietario *HTTPSpy*. Colpire le aziende manifatturiere del comparto della difesa per raccogliere proprietà intellettuali o l'intelligence militare è in linea con gli obiettivi e le motivazioni ormai note di VELVET CHOLLIMA.

Ad agosto 2024, LABYRINTH CHOLLIMA si è spacciato per responsabile delle assunzioni per invitare un dipendente di un'azienda europea operante nel comparto della difesa a scaricare un file ZIP dannoso a tema lavorativo, ospitato su un servizio di condivisione di file sul cloud. L'azienda, che opera in aree di grande interesse per il regime nordcoreano (ad esempio, satelliti e ricognizione aerea) è un bersaglio in linea con le esigenze di intelligence della Corea del Nord.[24] Successivamente, a maggio 2025, l'avversario ha rivolto i suoi attacchi a un'altra entità europea del comparto della difesa, utilizzando sempre un file ZIP a tema lavorativo, distribuito tramite WhatsApp.

Servizi finanziari europei nel mirino

Le istituzioni finanziarie e le aziende di tecnologia finanziaria (fintech) europee sono obiettivi di alto valore per le operazioni della Corea del Nord con moventi economici, poiché in Europa sono presenti molte entità finanziarie e fintech ben sviluppate. Molte giurisdizioni europee hanno anche allentato le normative finanziarie, il che potrebbe contribuire a dare la percezione di livelli di sicurezza più bassi o di riluttanza a voler segnalare incidenti di sicurezza informatica. Entrambi gli scenari probabilmente aumentano l'interesse degli avversari legati alla Corea del Nord per queste entità.

Tra gennaio e giugno 2025, STARDUST CHOLLIMA, che detiene il mandato esclusivo di generazione di valuta virtuale, ha puntano il mirino su entità finanziarie e di criptovaluta europee. In diversi incidenti, l'avversario ha sfruttato esche di phishing a tema di videoconferenza camuffate come opportunità di venture capital. Tramite le esche ha indotto le vittime a scaricare ed eseguire la carica distruttiva di AppleScript che apparentemente risolvono problemi di accesso o di audio nelle alle riunioni. Le campagne di STARDUST CHOLLIMA sono molto probabilmente motivate dal bisogno della Corea del Nord di asset digitali e di eludere le sanzioni internazionali.

Nel terzo trimestre 2024, LABYRINTH CHOLLIMA si è spacciato per un reclutatore di teste su LinkedIn per invitare il dipendente di un'azienda fintech con sede in Europa occidentale a partecipare a uno spazio di lavoro Slack per conto della falsa azienda. La vittima ha scaricato un progetto Python trojanizzato contenente *SnakeBaker* che si presentava come un test di valutazione delle competenze. Dopo che la vittima ha eseguito il progetto, LABYRINTH CHOLLIMA ha ottenuto la chiave di accesso all'ambiente cloud, ha condotto una ricognizione, si è spostato lateralmente e ha infine trasferito illecitamente i fondi di criptovaluta.

24 https://kcnawatch.org/newstream/1610155111-665078257/on-report-made-by-supreme-leader-kim-jong-un-at-8th-congress-of-wpk/

Settore energetico europeo nel mirino

Tra aprile e ottobre 2024, VELVET CHOLLIMA ha falsificato alcune entità energetiche del Regno Unito e numerose organizzazioni di Stati Uniti e Giappone. Non è chiaro se VELVET CHOLLIMA si rivolgesse specificamente al settore energetico o se stesse tentando di compromettere l'accesso di un individuo ai siti Web pubblici. Nel primo caso, i dati raccolti potrebbero supportare le esigenze di intelligence a lungo termine della Corea del Nord sulla tecnologia energetica. Inoltre, la tecnologia energetica nucleare è intrinsecamente a doppio uso e la Corea del Nord potrebbe presumibilmente utilizzare qualsiasi informazione rubata per sostenere il suo programma nucleare militare.

Tuttavia, questa attività è un'anomalia per VELVET CHOLLIMA. Gli avversari della Corea del Nord non rappresentano attualmente una minaccia significativa per le società energetiche europee.

Settore dei servizi professionali europeo nel mirino

Nella stessa campagna condotta da aprile a ottobre 2024, VELVET CHOLLIMA ha anche preso di mira alcune entità di servizi professionali del Regno Unito, utilizzando domini falsificati. Questa attività probabilmente supporta gli obiettivi generali di raccolta di intelligence dell'avversario riguardo alle posizioni delle policy occidentali e all'accesso a entità che influenzano i processi decisionali diplomatici ed economici.

FAMOUS CHOLLIMA

Durante il periodo di riferimento, FAMOUS CHOLLIMA ha utilizzato malware e minacce interne per colpire le entità con sede in Europa per attività opportunistiche e indipendenti dal settore. Le operazioni di FAMOUS CHOLLIMA sembrano avere un movente economico, perché le sue attività prevedono costanti furti di criptovaluta o frodi con carta di credito di poco valore oppure versamenti di stipendi illeciti. FAMOUS CHOLLIMA utilizza esche a tema lavorativo per indurre le vittime a scaricare cariche distruttive dannose ospitate su GitHub e Bitbucket. L'avversario adesca le vittime invitandole a visitare infrastrutture dannose proposte come piattaforme per colloqui di lavoro virtuali o per la valutazione delle competenze.

Anche alcuni soggetti europei hanno contribuito a facilitare le operazioni di minaccia interna di FAMOUS CHOLLIMA. A maggio 2024, il Dipartimento di Giustizia degli Stati Uniti ha incriminato e coordinato l'arresto di un cittadino ucraino per aver gestito un servizio che amministrava tre aziende di laptop farming e venduto profili su popolari siti Web per freelance, consentendo agli operatori di FAMOUS CHOLLIMA di falsificare la propria identità.

Inoltre, CrowdStrike Intelligence ha identificato un'azienda di laptop farming con sede in Polonia e utilizzata dall'avversario a giugno 2025. Il Dipartimento di Giustizia degli Stati Uniti ha sanzionato un cittadino russo per aver lavorato con un funzionario del consolato della Corea del Nord basato in Russia, per facilitare i pagamenti a favore di un'entità che impiega lavoratori IT della Corea del Nord in Russia e nel Laos.

A settembre 2024, l'Office of Financial Sanctions Implementation (OFSI) del Regno Unito ha emesso un avviso che descrive le prime operazioni note di FAMOUS CHOLLIMA rivolte al Regno Unito. Da allora, CrowdStrike Intelligence ha osservato diverse minacce rivolte a entità con sede in Europa.

ATTIVITÀ DEL RESTO DEL MONDO

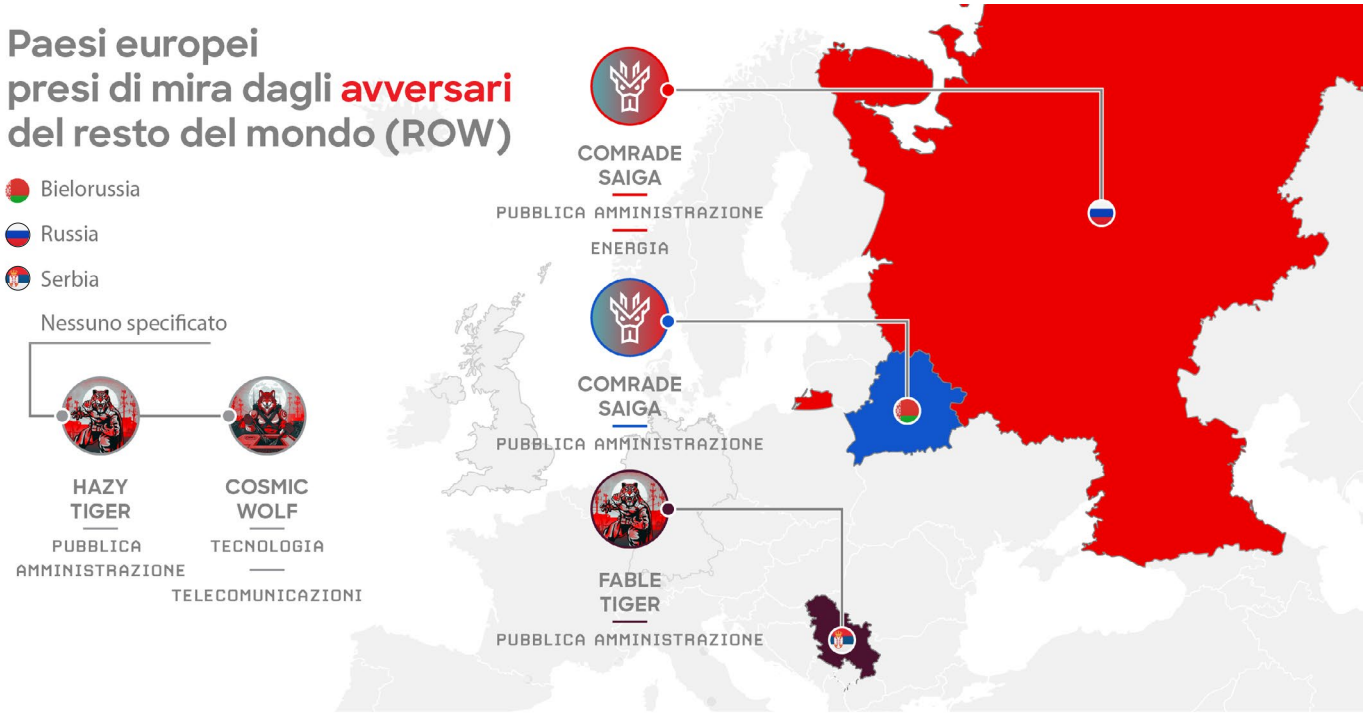


Figure 12. Paesi europei presi di mira da avversari ROW

Tra gennaio 2024 e settembre 2025, CrowdStrike Intelligence ha osservato alcuni casi di avversari del resto del mondo (ROW) che hanno colpito entità europee. Tuttavia, due avversari, COSMIC WOLF e COMRADE SAIGA, si confermano come minacce rilevanti per settori specifici in base alla loro attività storica, al tipo di bersaglio e alle motivazioni.

Avversari legati alla Turchia

Nonostante l'attività minima osservata dall'inizio del 2024, l'avversario COSMIC WOLF legato alla Turchia rimane una minaccia rilevante per le entità europee, in particolare per le entità tecnologiche e delle telecomunicazioni. A dicembre 2023, COSMIC WOLF ha distribuito l'impianto Linux *Torchlight* e utilizzato tecniche living-off-the-land in un'azienda tecnologica basata in Europa. Sebbene il metodo di accesso iniziale dell'avversario sia sconosciuto, CrowdStrike Intelligence indica che COSMIC WOLF ha ottenuto una chiave SSH privata per un server dell'ambiente di destinazione.

Sulla base delle attività condotte da COSMIC WOLF dal 2022, l'avversario si concentra probabilmente sulle entità tecnologiche e delle telecomunicazioni europee. La compromissione di queste entità probabilmente consente a COSMIC WOLF di mirare a entità a valle più direttamente rilevanti per le esigenze di intelligence della Turchia, come i gruppi minoritari e i dissidenti politici turchi.

Avversari legati al Kazakistan

Nel periodo di riferimento gennaio 2024 e settembre 2025, non è stato osservato che l'avversario COMPRADE SAIGA legato al Kazakistan abbia preso di mira entità europee. Tuttavia, l'avversario è una minaccia rilevante per i Ministeri degli Affari Esteri europei, in particolare per quelli che dispongono di ambasciate in Kazakistan. Al di fuori della Russia, COMRADE SAIGA punta il mirino prevalentemente contro le entità governative ed energetiche associate o operanti nella regione della CSI.

Tra gli enti governativi, COMRADE SAIGA prende più comunemente di mira i Ministeri degli Affari Esteri, quasi certamente per raccogliere informazioni su questioni diplomatiche rilevanti per il Kazakistan e per la regione della CSI. Alla fine di gennaio 2023, COMRADE SAIGA ha probabilmente colpito un'ambasciata europea ad Astana, nel Kazakistan, utilizzando un'e-mail di phishing contenente un allegato dannoso. L'attenzione dell'avversario per i Ministeri degli Affari Esteri, non osservata nei confronti di entità europee dal 2023, molto probabilmente indica che COMRADE SAIGA mira a raccogliere informazioni sugli sforzi diplomatici del Kazakistan.

Avversari legati all'India

Da gennaio 2024 a settembre 2025, gli avversari legati all'India hanno condotto una sola operazione contro entità europee. A novembre 2024, HAZY TIGER ha preso di mira alcune entità diplomatiche cinesi, inclusi i rappresentanti di una missione commerciale europea, probabilmente utilizzando e-mail di spear phishing contenenti file di connettori di ricerca collegati a directory WebDAV dannose. HAZY TIGER probabilmente continuava a condurre le sue attività di raccolta di intelligence sulle relazioni diplomatiche cinesi piuttosto che prendere specificamente di mira la missione commerciale.

Alla fine del 2023, FABLE TIGER ha probabilmente mirato a un ente governativo serbo utilizzando un sito Web di raccolta delle credenziali che falsificava la pagina di accesso alla webmail dell'organizzazione. Generalmente, FABLE TIGER prende di mira entità dell'Asia meridionale e CrowdStrike Intelligence non è attualmente in grado di valutare la motivazione dell'avversario per questa attività.

L'attività legata all'India rimarrà molto probabilmente sporadica o marginale nel corso del prossimo anno. Questa valutazione è espressa con elevata certezza sulla base della predominante attenzione che gli avversari legati all'India ripongono sui bersagli dell'Asia meridionale e il Sud-Est asiatico, con un'attività minima rivolta a entità europee.

Panoramica dell'hacktivismo e degli attori non legati agli stati

Tra gennaio 2024 e settembre 2025, CrowdStrike Intelligence ha identificato numerosi gruppi di hacktivisti che hanno rivendicato attacchi ai sistemi di controllo industriale (ICS) in tutta Europa, sia in risposta a conflitti geopolitici, sia nell'ambito di iniziative non direttamente legate a situazioni di conflitto. Il gruppo di hacktivisti filorussi *Z-Alliance* ha sferrato gran parte di questi attacchi contro paesi percepiti come ostili nei confronti della Russia. Il crescente interesse degli hacktivisti nei confronti degli ICS probabilmente deriva dal potenziale impatto e dalla conseguente attenzione dei media.

Durante il periodo di riferimento, le forze dell'ordine internazionali, incluse le autorità europee, sono riuscite a smantellare l'infrastruttura di diversi gruppi hacktivisti e ad arrestare numerosi membri. Questa attività di contrasto è in linea con i più ampi obiettivi europei di lotta alla criminalità informatica, tra cui il programma della Piattaforma Multidisciplinare Europea contro le Minacce Criminali (EMPACT) come priorità assoluta per il 2022-2025.[25]

25 https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

Sistemi di controllo industriale nel mirino

Tra gennaio 2024 e settembre 2025, numerosi gruppi di hacktivisti hanno rivendicato di aver preso di mira ICS, sistemi SCADA, dispositivi IoT (Internet of Things) e tecnologie operative (OT) in tutta Europa. La presunta attività consisteva principalmente in manipolazione delle impostazioni dei dispositivi, deturpazioni, attacchi DDoS contro sistemi esterni e furto di credenziali.

Gli hacktivisti hanno affermato che i motivi politici erano il principale motore trainante per la scelta dei sistemi ICS come bersaglio, con *Z-Alliance* responsabile del maggior volume di denunce durante questo periodo. Secondo quanto riferito, nei suoi attacchi, il gruppo ha utilizzato strumenti disponibili pubblicamente come Shodan e RealVNC Viewer.

Anche altri gruppo di hactivisti, tra cui *APT Iran*, *Cyber Av3ngers*, *Infrastructure Destruction Squad (IDS)*, *GhostSec*, *Golden Falcon Team*, *Maxious Greyhat*, *Russian Partisan* e *Laneh | Dark*, hanno dichiarato di aver preso di mira i dispositivi durante questo periodo. Sebbene la loro presunta attività si sia concentrata su entità non europee, queste affermazioni hanno evidenziato il crescente interesse degli hacktivisti per i dispositivi ICS.

Nei prossimi 12 mesi, i gruppi di hacktivisti continueranno probabilmente a dimostrare interesse per i sistemi ICS a livello globale. Tuttavia, la maggior parte di loro probabilmente dimostrerà capacità tecniche limitate e si affiderà a rivendicazioni esagerate o a malware pubblicamente disponibili progettati per i dispositivi ICS. Queste valutazioni sono espresse con moderata fiducia, sulla base dell'osservato aumento di attività rivendicate da hacktivisti contro questo tipo di dispositivi e sistemi durante il periodo di riferimento e tenendo conto del desiderio di attenzione degli hacktivisti.

Reazione degli hacktivisti alle operazioni delle forze dell'ordine europee

Tra gennaio 2024 e settembre 2025, le forze dell'ordine europee hanno condotto numerose operazioni contro gruppi di hacktivisti, con centinaia di arresti e importanti sequestri di infrastrutture in vari paesi. Gli hacktivisti hanno risposto a queste operazioni con campagne di ritorsione rivolte alle entità dei paesi bersaglio, adeguamenti alla sicurezza operativa e messaggi strategici sui social media, per ridurre al minimo l'impatto dell'attività delle forze dell'ordine.

Durante questo periodo, BOUNTY JACKAL è stato sotto il mirino delle forze dell'ordine. A luglio 2024, le autorità spagnole hanno arrestato i membri di Bounty JACKAL. Questi arresti hanno spinto l'avversario a implementare nuove procedure di sicurezza operativa a lanciare attacchi DDoS coordinati contro i siti Web spagnoli.

Analogamente, dopo che l'operazione Eastwood guidata da Europol ha smantellato l'infrastruttura di BOUNTY JACKAL nel luglio 2025, l'avversario ha rapidamente avviato l'operazione Time of Retribution. L'avversario ha preso di mira i paesi partecipanti all'operazione Eastwood con attacchi DDoS, danneggiamenti ai siti Web e dichiarata compromissione delle infrastrutture, dichiarando che l'impatto che l'operazione Europol ha avuto sul gruppo è stato limitato.

Mentre le forze dell'ordine globali continuano a prendere di mira il crimine informatico, gli hacktivisti continueranno probabilmente a rispondere con campagne di ritorsione, cambiamenti operativi e post sui social media.

Conclusioni

Nel prossimo futuro, gli avversari eCrime continueranno quasi certamente a dare priorità alle entità basate in Europa, per motivazioni finanziarie. Le pratiche di estorsione di dati e il ransomware rimarranno molto probabilmente la minaccia eCrime più critica per l'Europa, dato il forte impatto delle intrusioni portate a termine con successo e la preferenza costante degli avversari BGH nella scelta della regione come bersaglio.

Sebbene il potenziale impatto delle intrusioni andate a buon fine rimanga elevato, gli avversari eCrime beneficiano di tecniche di accesso iniziale e di distribuzione del malware storiche e in evoluzione, come dimostrato dall'improvvisa e ampia adozione del vishing e di esche CAPTCHA. La popolarità dell'IA probabilmente favorirà ulteriormente questa evoluzione.

Dal 2024, le operazioni delle forze dell'ordine internazionali hanno generato effetti sulle attività degli avversari eCrime, sui forum (ad esempio, BreachForums e XSS) e sui servizi di abilitazione. Tuttavia, gli ecosistemi sotterranei in lingua inglese e russa sono resilienti, poiché sono decentralizzati e coinvolgono cybercriminali che agiscono impunemente in paesi che sembrano offrire loro protezione.

Pertanto, i cybercriminali di eCrime basati in Europa e diretti contro l'Europa stessa continueranno a beneficiare di un ecosistema che consente di operare ai cybercriminali con livelli diversi di sofisticazione e che abbassa le barriere di ingresso per l'eCrime. Dato l'anonimato dell'ecosistema e la natura indiscriminata dei servizi abilitanti, anche le minacce non eCrime (tra cui il cybercriminale ibrido RENAISSANCE SPIDER e EMBER BEAR legato alla Russia) beneficiano di queste reti.

Gli avversari legati agli stati quasi certamente continueranno a raccogliere informazioni per plasmare la policy nazionale e decidere il livello di impegno da rivolgere alle entità europee. Gli stati avversari sono altamente motivati a prendere di mira le entità europee, probabilmente perché esse offrono informazioni politiche, economiche e tecnologiche redditizie, sfruttabili per promuovere interessi strategici.

Gli sviluppi geopolitici possono modificare rapidamente il bisogno di intelligence e la portata operativa di un avversario. Per paesi come la Russia e l'Iran, le capacità informatiche sono fondamentali per rispondere ai conflitti percepiti come una minaccia alla loro sovranità. Entrambi i paesi conducono una gamma completa di operazioni, dallo spionaggio passivo e le campagne di ricognizione alle campagne distruttive di hack-and-leak mascherate da hacktivismo, fino agli attacchi dichiaratamente distruttivi. Queste operazioni prevedono una negabilità plausibile, ostacolano gli sforzi di attribuzione e riducono i costi finanziari e umani, consentendo agli stati di affermare la propria forza e influenzare oltre le capacità convenzionali.

Altri cybercriminali legati agli stati puntano alle entità europee per motivazioni economiche e finanziarie. Gli avversari legati alla Cina commettono furti di proprietà intellettuale per rafforzare il loro vantaggio competitivo a livello internazionale ed evitare costose attività interne di ricerca e sviluppo. Oltre alle attività di raccolta di intelligence, gli avversari della Corea del Nord spesso conducono attività opportunistiche volte a generare ricavi (come il furto di criptovaluta) per finanziare il regime del paese.

I conflitti globali continueranno probabilmente a motivare le attività che gli hacktivisti condurranno contro le entità europee nei prossimi 12 mesi. Per massimizzare il loro impatto pubblico, alcuni gruppi di hacktivisti probabilmente rivendicheranno di mirare agli OT strategici, inclusi i sistemi ICS e SCADA, in tutta Europa e nel mondo. Mentre le forze dell'ordine globali intensificano le operazioni di contrasto al crimine informatico, gli hacktivisti probabilmente continueranno a rispondere con campagne di ritorsione, cambiamenti operativi e attività coordinate sui social media.

Raccomandazioni

1 Adottare l'IA agentica per scalare le operazioni di sicurezza

Mentre i cybercriminali adottano l'intelligenza artificiale per colpire più velocemente, scalare le operazioni ed eludere i rilevamenti, per non rimanere indietro i responsabili della difesa devono affrontare una pressione sempre maggiore. I team di sicurezza sono già sovraccarichi, alle prese con un numero crescente di allarmi, combattono con la mancanza di competenze e corrono per rispondere rapidamente. Per colmare queste lacune sempre più ampie, i team di sicurezza devono rendere operativa l'IA agentica, ovvero agenti specializzati in grado di ragionare, adattarsi e agire all'interno di barriere e policy organizzative. L'IA agentica consente di applicare il ragionamento di esperti e la velocità della macchina per accelerare i risultati e automatizzare il lavoro. Queste funzionalità possono scalare le operazioni basate sull'intelligence, applicando la threat intelligence e le competenze emergenti per valutare gli avvisi, condurre indagini ed eseguire azioni di risposta. Eliminando le attività ripetitive e dispendiose in termini di tempo, l'IA agentica consente agli analisti umani di concentrarsi su attività di threat hunting proattivo e su indagini basate su ipotesi, aumentando l'impatto strategico e l'efficienza operativa.

2 Proteggere l'intero ecosistema delle identità

Gli avversari prendono sempre più di mira le identità attraverso il furto di credenziali, eludendo l'autenticazione a più fattori e utilizzando il social engineering, spostandosi lateralmente tra ambienti on-premise, cloud e SaaS sfruttando i rapporti di fiducia. Questo consente loro di fingersi utenti legittimi, scalare i privilegi ed eludere i rilevamenti.

Per impedire gli accessi non autorizzati, le organizzazioni devono adottare soluzioni di autenticazione a più fattori a prova di phishing, come le chiavi di sicurezza hardware. È essenziale disporre di solide policy per identità e accessi, tra cui l'accesso just-in-time, le revisioni periodiche degli account e i controlli di accesso condizionale. Gli strumenti di rilevamento delle minacce all'identità devono monitorare i comportamenti negli endpoint e negli ambienti on-premise, cloud e SaaS per segnalare casi di privilege escalation, accessi non autorizzati e creazione di account backdoor. Integrando questi strumenti con la piattaforma Extended Detection and Response (XDR), è possibile ottenere una visibilità completa e una difesa unificata contro gli avversari.

Le organizzazioni devono inoltre educare gli utenti a riconoscere i tentativi di vishing e phishing, assicurando un monitoraggio proattivo per rilevare e rispondere alle minacce basate sull'identità.

3 Eliminare le lacune nella visibilità cross-domain

L'uso crescente di tecniche hands-on-keyboard e di strumenti legittimi da parte degli avversari rende più difficile il rilevamento e la risposta. A differenza del malware tradizionale, questi metodi consentono agli aggressori di aggirare le misure di sicurezza legacy, eseguendo comandi e utilizzando software legittimi per imitare le normali operazioni.

Per contrastare il problema, le organizzazioni devono modernizzare le loro strategie di rilevamento e risposta. Le soluzioni come Next-Gen SIEM per la gestione degli eventi e delle informazioni forniscono una visibilità unificata su endpoint, reti, ambienti cloud e sistemi di identità, consentendo agli analisti di creare correlazioni tra comportamenti sospetti e identificare l'intero percorso di attacco. Le attività di triage e indagine basate sull'IA agentica possono estendere queste funzionalità, analizzando autonomamente i segnali dei vari domini per portare alla luce informazioni altamente attendibili e dare priorità alle minacce reali.

I processi di threat hunting proattivo e di threat intelligence migliorano ulteriormente la capacità di rilevamento, identificando potenziali pattern di attacco e fornendo approfondimenti su tattiche, tecniche e procedure degli avversari. Grazie all'intelligence in tempo reale, le organizzazioni possono rimanere informate sulle minacce emergenti, anticipare gli attacchi e dare priorità alle attività essenziali per la sicurezza.

4 Difendere il cloud come infrastruttura fondamentale

Gli avversari che sfruttano il cloud approfittano di errori di configurazione, credenziali rubate e strumenti di gestione del cloud per infiltrarsi nei sistemi, spostarsi lateralmente e mantenere l'accesso permanente per condurre attività malevole come il furto di dati e il deployment di ransomware.

Le CNAPP (piattaforme per la protezione delle applicazioni cloud native) con funzionalità CDR (cloud detection and response) sono fondamentali per contrastare tali minacce. Queste soluzioni forniscono una visione unificata della postura di sicurezza del cloud, aiutando a rilevare, assegnare priorità e correggere rapidamente errori di configurazione, vulnerabilità e minacce degli avversari. Inoltre, l'applicazione di rigorosi controlli di accesso, come le policy condizionali e l'accesso basato sui ruoli, riduce l'esposizione ai sistemi critici e garantisce il monitoraggio continuo delle anomalie, inclusi gli accessi da posizioni impreviste.

Inoltre, effettuare audit regolari è essenziale ai fini della sicurezza. Gli strumenti automatizzati possono rivelare impostazioni di archiviazione eccessivamente permissive, API esposte e vulnerabilità prive di patch. L'esecuzione di revisioni frequenti degli ambienti cloud permette ai team di intervenire tempestivamente su autorizzazioni inutilizzate e configurazioni obsolete.

5 Assegnare la priorità alle vulnerabilità mediante un approccio incentrato sull'avversario

Gli avversari sfruttano sempre più le vulnerabilità diffuse pubblicamente e ricorrono al chaining degli exploit che, grazie alla combinazione di più vulnerabilità, garantisce maggiore rapidità di accesso, escalation dei privilegi ed elusione delle difese.
Questi attacchi in più fasi spesso fanno affidamento su risorse pubbliche come gli exploit proof-of-concept e i blog tecnici, consentendo agli avversari di creare cariche distruttive efficaci e difficili da rilevare.

Per contrastare queste minacce, le organizzazioni devono dare massima importanza all'applicazione regolare di patch o all'aggiornamento dei sistemi critici, in particolare dei servizi online presi di mira più di frequente come i server web e i gateway VPN. Il monitoraggio dei segnali impercettibili di chaining degli exploit, come arresti anomali imprevisti o tentativi di privilege escalation, può essere d'aiuto per rilevare gli attacchi prima del loro progredire.

Strumenti come CrowdStrike Falcon® Exposure Management, creati con funzionalità di assegnazione delle priorità con IA nativa, consentono ai team di ridurre il rumore e concentrarsi sulle vulnerabilità più importanti, in particolare quelle che interessano i sistemi critici e ad alto rischio. Grazie ad approcci proattivi alla sicurezza, in grado di rilevare le esposizioni sull'intera superficie di attacco, e all'uso dell'automazione, le organizzazioni sono in grado di mitigare le minacce sofisticate e limitare le opportunità degli avversari.

6 Conoscere l'avversario e tenersi sempre pronti

Quando un attacco informatico si svolge in pochi minuti, o addirittura secondi, essere preparati può essere determinante per riuscire a contenerlo. Un approccio basato sull'intelligence consente ai team di sicurezza di andare oltre la difesa reattiva, permettendo loro di identificare l'avversario, il modo in cui opera e i suoi obiettivi. Con la threat intelligence, la profilazione dell'avversario e l'analisi dell'attività di spionaggio, i team di sicurezza possono dare priorità alle risorse, adattare le difese e andare attivamente in cerca delle minacce per scovarle sul nascere. La threat intelligence di CrowdStrike non si limita a individuare le minacce note, ma anticipa le attività di spionaggio nuove ed emergenti, consentendo ai responsabili della difesa di stare sempre un passo avanti. Integrando perfettamente l'intelligence nei flussi di lavoro di sicurezza, le organizzazioni possono accelerare i tempi di risposta, bloccare gli avversari e trasformare l'intelligence in azione.

Sebbene la tecnologia sia fondamentale per rilevare e bloccare le intrusioni, l'utente finale rimane un anello cruciale della catena per fermare le compromissioni. Le organizzazioni devono adottare programmi di sensibilizzazione degli utenti per contrastare le continue minacce di phishing e le tecniche di social engineering correlate. Per quanto riguarda i team di sicurezza, la pratica li rende perfetti. Occorre promuovere un ambiente che esegua regolarmente simulazioni di attacco ed esercitazioni red team/blue team per identificare le lacune ed eliminare i punti deboli nelle proprie strategie e risposte di sicurezza informatica.

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della sicurezza informatica, ha ridefinito la sicurezza moderna con la piattaforma cloud native più avanzata al mondo per la protezione delle aree di rischio aziendale critiche: endpoint e workload su cloud, identità e dati.

Grazie alla tecnologia CrowdStrike Security Cloud e all'intelligenza artificiale di eccellenza, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, la threat intelligence, le tecniche di spionaggio degli avversari in evoluzione e la telemetria arricchita a livello aziendale per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'élite e analisi prioritaria delle vulnerabilità.

Costruita appositamente nel cloud con un'architettura basata su un unico lightweight agent, la piattaforma Falcon offre deployment rapido e scalabile, protezione e prestazioni superiori, complessità ridotta e time-to-value immediato.

CrowdStrike: We stop breaches.

Ulteriori informazioni: www.crowdstrike.com

Seguici: Blog | X | LinkedIn | Facebook | Instagram YouTube

Inizia oggi stesso la prova gratuita: www.crowdstrike.com/free-trial-guide/