FBI Says US Seized $1.2 Billion Worth of Cryptocurrency Stolen From Binance

Also Thursday, the FBI blamed North Korea for a separate social engineering scheme that officials say resulted in the theft of $400 million worth of cryptocurrency.

The post FBI Says US Seized $1.2 Billion Worth of Cryptocurrency Stolen From Binance appeared first on SecurityWeek.

https://www.securityweek.com/fbi-says-us-seized-1-2-billion-worth-of-cryptocurrency-stolen-from-binance/

Syrian Hacker Gets Prison Time in US After Over a Decade on the Run

A US court sentenced Syrian hacker Ahmad Umar Agha to 42 months for pro-Assad attacks on media, businesses, and government entities.

The post Syrian Hacker Gets Prison Time in US After Over a Decade on the Run appeared first on SecurityWeek.

https://www.securityweek.com/syrian-hacker-gets-prison-time-in-us-after-over-a-decade-on-the-run/

Bulletproof Host Virtualine Loses Its Domain to FBI Seizure

It allowed customers to host hack-for-hire services, supported ransomware and infostealer operators, and accepted crypto payments.

The post Bulletproof Host Virtualine Loses Its Domain to FBI Seizure appeared first on SecurityWeek.

https://www.securityweek.com/bulletproof-host-virtualine-loses-its-domain-to-fbi-seizure/

$2 Million+ Drained From Polymarket Traders in New Supply Chain Attack

Malicious code linked to a website monitoring tool was designed to hijack logged-in Polymarket sessions and siphon user funds.

The post $2 Million+ Drained From Polymarket Traders in New Supply Chain Attack appeared first on SecurityWeek.

https://www.securityweek.com/2-million-drained-from-polymarket-traders-in-new-supply-chain-attack/

CVD, 615-ter e il coraggio di chiedere aiuto

L’Agenzia per la Cybersicurezza Nazionale introduce una procedura per la divulgazione coordinata delle vulnerabilità, ma l’articolo 615-ter del Codice penale resta applicabile. Tra anonimato, obblighi di segnalazione e assenza di un safe harbor legislativo, emergono interrogativi sulla posizione dei ricercatori di sicurezza. Un’analisi del quadro italiano e delle soluzioni adottate negli altri Paesi europei.

CVD e hacker etici: la nuova politica ACN sulle zero day e i limiti delle tutele penali

A pagina 9 della Politica nazionale di divulgazione coordinata delle vulnerabilità (CVD) c’è un riquadro che ogni ricercatore italiano dovrebbe leggere due volte. Dice che le attività di ricerca delle zero day «non devono integrare alcuna fattispecie criminosa», e tra le norme richiamate mette l’accesso abusivo dell’articolo 615-ter del Codice penale. Poi ricorda che il personale del CSIRT Italia è pubblico ufficiale e, se ha notizia di un reato perseguibile d’ufficio, deve informare l’autorità giudiziaria.

La Politica è stata comunicata da ACN il 7 ottobre 2026. Crea una procedura di segnalazione, anche anonima. Non crea nessuna tutela penale. Vediamo cosa dice il testo, cosa dice la legge e cosa fanno gli altri Paesi europei.

CVD: cosa prevede la politica nazionale di divulgazione delle vulnerabilità

Le basi sono europee e nazionali. L’articolo 12 della direttiva NIS2 (UE 2022/2555, pubblicata in Gazzetta ufficiale dell’Unione europea il 27 dicembre 2022) chiede a ogni Stato membro di designare un CSIRT come coordinatore della divulgazione coordinata delle vulnerabilità. L’Italia ha recepito la direttiva con il D.Lgs. 138/2024, in vigore dal 16 ottobre 2024. L’articolo 16 designa il CSIRT Italia e, al comma 4, affida all’autorità NIS l’adozione della politica nazionale. L’articolo 40, comma 5, lettera d), prevede che avvenga «d’intesa con il Ministero della giustizia».

Secondo il comunicato di ACN, la Politica è stata adottata con determina del Direttore generale Andrea Quacivi. La determina, firmata digitalmente il 6 ottobre 2026, richiama l’intesa del Ministero della giustizia (comunicazione del 31 ottobre 2025) e il parere del Tavolo NIS (riunione del 18 dicembre 2025). Il processo descritto dalla Politica ha tre fasi: segnalazione, validazione e cooperazione, divulgazione. Il CSIRT Italia verifica la segnalazione, contatta il fabbricante e chiede il CVE ID. Il *workaround* va individuato entro 7 giorni solari dalla validazione, la patch entro 90, salvo complessità. Il testo vale solo per le vulnerabilità zero day.

Il segnalante assume degli obblighi. Deve segnalare «non appena ne abbia preso consapevolezza» e non può condividere con terzi, senza autorizzazione del CSIRT, alcun dettaglio, comprese le tecnologie usate per trovare o sfruttare la falla. Il canale indicato è segnalazioni.acn.gov.it. Un portale di segnalazione esisteva già: le FAQ del CSIRT Italia lo descrivono, anche per vulnerabilità non note. La novità è una procedura con fasi e tempi.

CVD e anonimato: quali tutele per gli hacker etici?

Il segnalante può chiedere l'anonimato. A pagina 12 ACN promette di tutelare le informazioni identificative ricavabili dal mezzo di segnalazione, come IP, e-mail e numero di telefono. Aggiunge però che potrà essere tenuta a comunicare le informazioni alle autorità competenti, in particolare se ravvisa una notizia di reato. L'anonimato protegge l'identità durante il processo, non nei confronti dell'autorità giudiziaria.

A mio avviso l'intesa con il Ministero della giustizia, richiamata nella determina, va letta con prudenza. Riguarda l'adozione di un atto amministrativo. In materia penale vale la riserva di legge (articolo 25, secondo comma, della Costituzione), quindi una determina non può introdurre una causa di non punibilità. La Relazione annuale ACN 2025 (riquadro Focus, pagina 16 del documento, 17 del PDF) conferma la lettura: la Politica, elaborata a legislazione vigente, «non reca una disciplina in materia di tutela dei segnalanti delle vulnerabilità sotto i profili della responsabilità civile e penale».

Articolo 615-ter: i rischi penali per gli hacker etici

L'articolo 615-ter punisce chi si introduce abusivamente in un sistema protetto da misure di sicurezza, o vi si mantiene contro la volontà espressa o tacita del titolare. Non richiede un'autorizzazione scritta. L'ipotesi base è a querela. Le ipotesi aggravate si procedono d'ufficio, come già prima della L. 90/2024. Quella legge ha alzato le pene per i sistemi di interesse pubblico (comma 3) a 3-10 anni, e a 4-12 se ricorre anche un'aggravante del comma 2. Il tetto di 12 anni non è automatico.

Sulle intenzioni la giurisprudenza è netta. Le Sezioni Unite Casani (n. 4694/2012) hanno stabilito che per chi è abilitato conta il rispetto delle condizioni poste dal titolare, mentre sono irrilevanti «gli scopi e le finalità» che hanno motivato l'ingresso. Le Sezioni Unite Savarese (n. 41210/2017) riguardano i pubblici ufficiali, e l'estensione ai ricercatori è un'interpretazione. Per chi non ha alcuna abilitazione il problema, a mio avviso, sta ancora più a monte: manca il consenso del titolare.

Esiste un precedente favorevole, ma isolato: il decreto di archiviazione del GIP di Catania del 15 luglio 2019, che ha ricondotto la condotta alla divulgazione responsabile. Non è vincolante. Il valore pratico dell'autorizzazione scritta è una mia valutazione di prudenza: la legge non la richiede, ma senza di essa è difficile provare il consenso.

Safe harbor per gli hacker etici: le proposte legislative in Italia

Il DDL S. 1441 (sen. Basso), comunicato alla Presidenza il 3 aprile 2025, è una delega al Governo sulla strategia contro il ransomware. La lettera q) dell'articolo 1, comma 1, prevede un «safe harbor» per chi segnala in buona fede vulnerabilità informatiche rilevanti. Secondo il fascicolo del Senato risulta assegnato e non ancora esaminato. È un criterio di delega di una riga e parla di chi segnala, non di chi ricerca. Nelle verifiche svolte non ho trovato altre proposte pendenti con una scriminante specifica.

CVD in Europa: le tutele per i ricercatori negli altri Paesi

Il Belgio ha scritto l'esenzione nella legge. Introdotta nel 2022 dalla norma sul whistleblowing, oggi è negli articoli 22 e 23 della legge NIS2 del 26 aprile 2024, in vigore dal 18

ottobre 2024. Secondo il Centre for Cybersecurity Belgium la protezione richiede azioni necessarie e proporzionate, assenza di intento fraudolento, notifica al CCB e al titolare, e nessuna divulgazione pubblica senza il consenso del CCB.

I Paesi Bassi non hanno un'immunità formale. Hanno la guida del Nationaal Cyber Security Centrum, pubblicata nel 2013 e aggiornata nel 2018, e una lettera di politica della Procura del 14 dicembre 2020 che sostituisce quella del 2013. Secondo la sintesi dell'OM, in assenza di una policy la denuncia non basta a trattare l'hacker etico come sospettato.

La Germania ci sta lavorando. Nel novembre 2024 il Ministero della giustizia ha elaborato un Referentenentwurf, una bozza ministeriale e non un disegno di legge, che modificava il § 202a StGB per escludere l'accesso finalizzato a segnalare una vulnerabilità. Il progetto non è stato approvato prima della fine anticipata della legislatura. Il contratto di coalizione CDU/CSU-SPD del 2025 promette certezza giuridica per la ricerca, e il Governo ha ribadito l'impegno in una risposta parlamentare del 16 aprile 2026. Non ho trovato una nuova bozza.

La Francia offre una protezione solo procedurale: l'articolo L2321-4 del Code de la défense disapplica l'obbligo di denuncia dell'articolo 40 del codice di procedura penale nei confronti di chi, in buona fede, trasmette l'informazione alla sola autorità nazionale (l'ANSSI), e tutela la riservatezza della sua identità. È in vigore dal 9 ottobre 2016. Uno studio sul Journal of Cybersecurity del 2026, che esamina anche l'Italia, chiede safe harbour giuridici e tecnici a livello europeo perché le politiche di divulgazione siano «*legally accessible and safe for the researchers*».

Il caso FreeHour: quando l'hacking

etico diventa un procedimento penale

A Malta la mancanza di tutele ha avuto un volto. Secondo MaltaToday, nell'ottobre 2022 tre studenti individuarono una vulnerabilità nell'app FreeHour e scrissero al fondatore, che informò la polizia. Gli arresti sono di novembre 2022. Il docente che aveva riletto la mail fu accusato di concorso. Le cronache riportano che gli studenti chiesero una ricompensa e che uno di loro modificò temporaneamente l'app, poi ripristinata (Newsbook).

L'imputazione formale è arrivata nella prima settimana di marzo 2025. Nella settimana successiva il Cabinet ha raccomandato la grazia, concessa dal presidente il 1° luglio 2025. Il premier Robert Abela, secondo la stampa maltese (Malta Daily), ha riconosciuto la responsabilità dello Stato di aggiornare le leggi alla realtà tecnologica. È una parafrasi giornalistica, non una citazione. A mio avviso il caso mostra che, senza una tutela espressa, la decisione di procedere resta a titolare, procura e giudice.

CVD e segnalazione delle vulnerabilità: cosa fare in pratica

Questo è il mio parere. Chi trova una vulnerabilità senza accedere a sistemi altrui, per esempio analizzando firmware acquistato o software proprio, ha ora un canale con tempi definiti, e il rischio penale è basso. Chi ha già acceduto a un sistema in produzione è nella posizione più delicata: la Politica chiede di segnalare subito, il CSIRT può informare l'autorità giudiziaria e l'anonimato non copre quel passaggio. Il divieto di condividere dettagli con terzi incide anche sul confronto con la *community*.

Lo strumento più solido resta il consenso documentato del

titolare, con un contratto di pentest o un *bug bounty* con regole di ingaggio. Le clausole di *safe harbor* dei programmi privati vincolano le parti, non il pubblico ministero. Aziende e PA, dal canto loro, possono pubblicare una *Vulnerability Disclosure Policy* con l'impegno a non sporgere querela contro i ricercatori in buona fede. Funziona per l'ipotesi base del 615-ter, che è a querela, non per le aggravate.

Il mio commento

Quasi quattro anni dopo la direttiva e due dopo l'entrata in vigore del decreto, l'Italia ha il suo canale CVD. Va riconosciuto, ed è un passo utile. Ma guardate come è scritto. La Politica chiede di segnalare «non appena» si ha consapevolezza della vulnerabilità, vieta di parlarne con terzi e avverte che l'accesso abusivo è reato.

A chi ha trovato una zero day entrando dove non doveva dice di farsi avanti. Nello stesso riquadro ricorda che chi riceve la segnalazione è un pubblico ufficiale con obbligo di informare i magistrati. La Giustizia ha dato l'intesa a ottobre 2025 e il Tavolo NIS ha espresso il parere a dicembre. Alla firma, a ottobre 2026, il testo non contiene una riga di tutela.

Il Belgio ha scritto l'esenzione nella legge, con condizioni precise. L'Italia ha scritto un avviso e lo ha chiamato politica. Un ricercatore in buona fede esce da questa lettura con una certezza sola: segnalare conviene a tutti, tranne a lui. Si può discutere se sia un difetto di progettazione o il compromesso obbligato da un codice penale che non cambia. Ma finché il 615-ter resta com'è, la domanda di ogni hacker etico non è se segnalare. È come ha trovato quello che segnala, e se può dimostrarlo.

https://www.ictsecuritymagazine.com/articoli/cvd-hacker-etici-615-ter/

Microsoft Disrupts Chinese-Language Phishing Market Behind 1B+ Messages

Backed by a federal court order, Microsoft and Health-ISAC seized domains powering YAM Store, CoGUI, and Iron Man.

The post Microsoft Disrupts Chinese-Language Phishing Market Behind 1B+ Messages appeared first on SecurityWeek.

https://www.securityweek.com/microsoft-disrupts-chinese-language-phishing-market-behind-1b-messages/

US Arrests Two in Crackdown on North Korean IT Worker Laptop Farms

Investigators stormed 40 locations in Texas and seized 187 laptops used by North Korean IT workers to hide their location.

The post US Arrests Two in Crackdown on North Korean IT Worker Laptop Farms appeared first on SecurityWeek.

https://www.securityweek.com/us-arrests-two-in-crackdown-on-north-korean-it-worker-laptop-farms/

Cyberattack Prompts Grocery Giant Ahold Delhaize to Disconnect Systems

The company says it took some of its systems offline to contain a security issue within its network.

The post Cyberattack Prompts Grocery Giant Ahold Delhaize to Disconnect Systems appeared first on SecurityWeek.

https://www.securityweek.com/cyberattack-prompts-ahold-delhaize-to-disconnect-systems/

Insider Cyber Extortion Plot Against Industrial Firm Lands Engineer in Prison

The former core infrastructure engineer deleted admin accounts, reset hundreds of passwords, and demanded 20 bitcoin to spare the company’s servers.

The post Insider Cyber Extortion Plot Against Industrial Firm Lands Engineer in Prison appeared first on SecurityWeek.

https://www.securityweek.com/insider-cyber-extortion-plot-against-industrial-firm-lands-engineer-in-prison/

Google Domains Impacted by Recent ccTLD Hijacks

Hackers hijacked the .gh, .sl, and .as ccTLDs and obtained HTTPS certificates for several Google domains.

The post Google Domains Impacted by Recent ccTLD Hijacks appeared first on SecurityWeek.

https://www.securityweek.com/google-domains-impacted-by-recent-cctld-domain-hijacks/