Operational Summary

maggio 2024

Servizio Operazioni

TLP:CLEAR

Operational Summary

Servizio Operazioni

maggio 2024

Indice

Elenco delle figure

1 Introduzione

Il presente documento riporta su base mensile alcuni numeri e indicatori derivanti dalle attività operative dell'Agenzia per la Cybersicurezza Nazionale, utili per caratterizzare lo stato della minaccia cyber in Italia.

In particolare, il CSIRT Italia, articolazione tecnico-operativa dell'Agenzia, è hub nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (Perimetro di Sicurezza Nazionale Cibernetica, Direttiva NIS, D.M. Telco) e collaziona altresì informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali ed internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni costituiscono un ampio cono di visibilità di cui l'Agenzia dispone sullo stato della minaccia cyber a danno del sistema Paese e forniscono all'Agenzia, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali.

Tutte le informazioni vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di triage le analizzano e classificano come eventi cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

- **approfondire le informazioni** a disposizione, analizzando i contenuti anche dal punto vista strettamente tecnico, quale lo studio dei malware, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti;
- **se necessario inviare richieste di informazioni** ai soggetti;
- **fornire supporto da remoto o in loco** ai soggetti impattati;
- **inviare comunicazioni** ai soggetti impattati oppure a tutti i soggetti potenzialmente impattati;
- **pubblicare alert o bollettini**.

Nel documento, in Sezione 2, sono riportati gli andamenti di eventi e incidenti registrati dall'ACN, organizzati per tipologia di minacce e settori impattati; in Sezione 3 si riporta un'analisi sulle vulnerabilità scoperte o comunque divenute d'interesse durante maggio 2024 nonché o riferimenti ai principali alert pubblicati dal CSIRT Italia sul sito `www.csirt.gov.it`; infine, la Sezione 4 presenta informazioni sulla diffusione delle varie tipologie di malware in Italia e in Europa nonché un focus sulle rivendicazioni di ransomware e di DDoS.

Il glossario delle definizioni è in Sezione 5.

2 EVENTI E INCIDENTI

A maggio 2024 sono stati individuati **283** eventi cyber, in **aumento** del 148% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 175 soggetti nazionali**: 121 appartenenti alla *constituency*[1], i restanti hanno riguardato cittadini e società private operanti in settori non critici[2].

La Figura 1 mostra l'andamento di eventi e incidenti fino al mese in esame, corredato da una previsione, basata sull'analisi dei dati precedenti[3], riferita ai successivi 3 mesi.

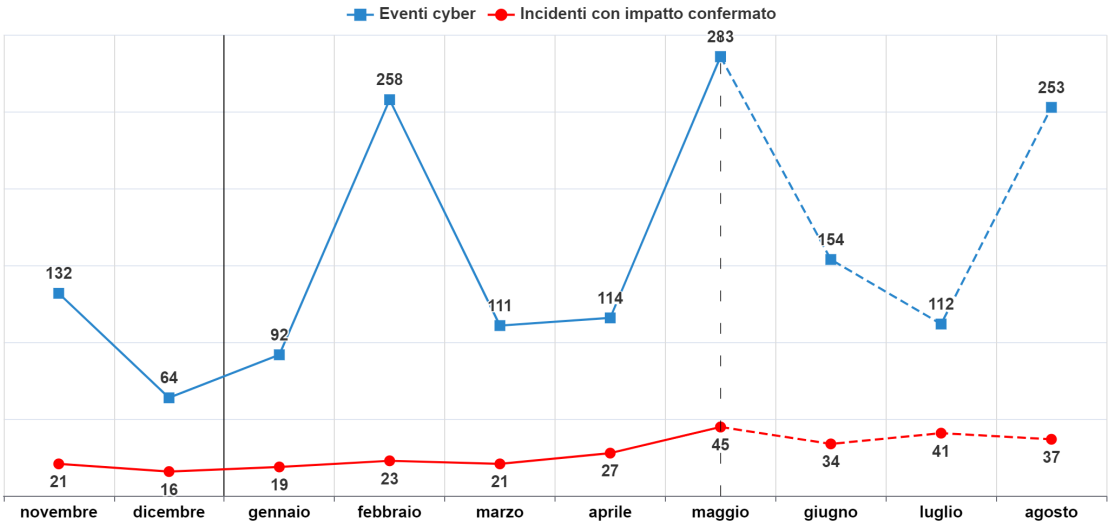

Figura 1: andamento attività reattive e analisi previsionale

2.1 Settori impattati

In Figura 2 si riporta il numero di eventi registrato per settore impattato[4]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico).

[1]La constituency è l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli eventi cibernetici.

[2]Ovvero i soggetti che non operano nei settori NIS, Perimetro, Telco o nella pubblica amministrazione.

[3]La previsione da un'idea generale degli andamenti futuri utilizzando un modello ARIMA (AutoRegressive Integrated Moving Average). È importante sottolineare che la previsione non può essere accurata in quanto il manifestarsi degli eventi dipende da molti fattori, tra i quali quelli di natura geopolitica, la scoperta di nuove vulnerabilità, la capacità degli attaccanti e così via.

[4]Si noti che ognuno dei citati eventi può essere stato associato ad uno o più settori di attività, ad esempio, un evento può avere un impatto su più settori e un soggetto può operare in più settori. Talvolta non è possibile associare un evento ad un settore.

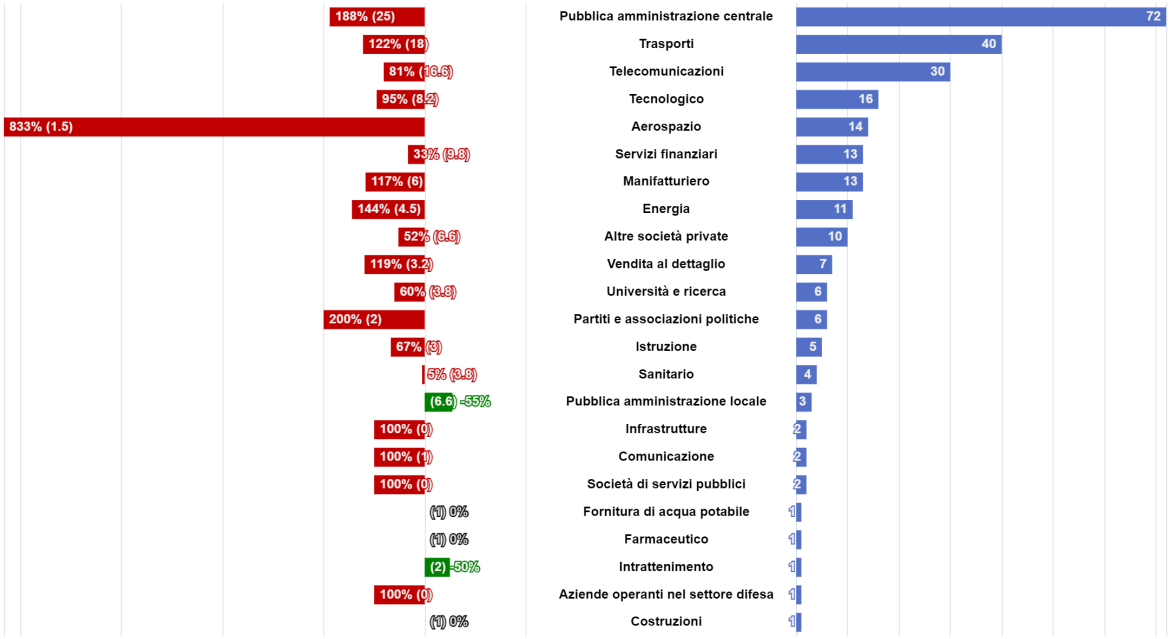

Figura 2: numero di eventi cyber per settore e variazione percentuale rispetto al semestre precedente

2.2 Tipologia di minacce negli eventi

In Figura 3 si riporta il numero di minacce rilevate negli eventi[5] e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico)..

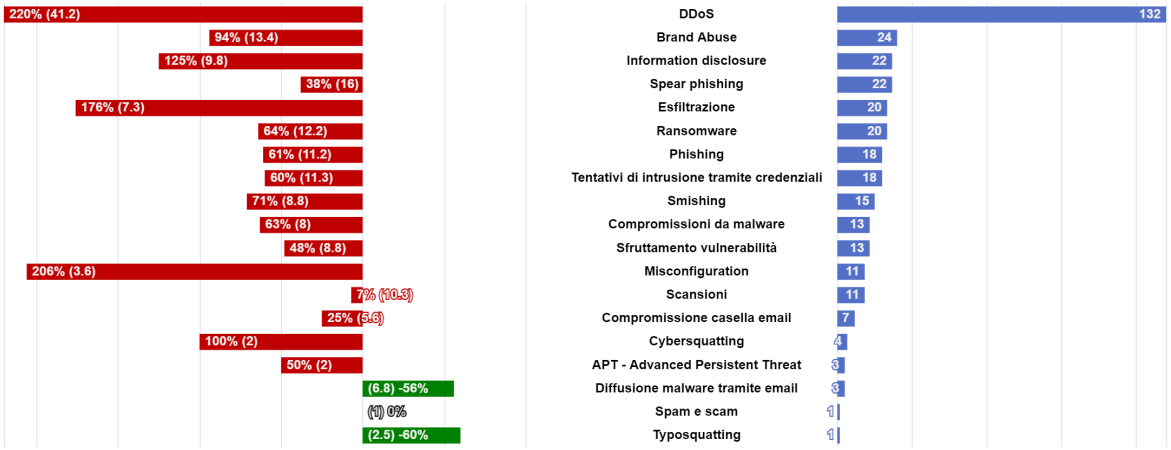

Figura 3: tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente

2.3 Focus constituency

Dei 283 eventi cyber **121** hanno riguardato soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

[5]Si noti che ognuno degli eventi può essere stato associato ad una o più tipologia di minacce.

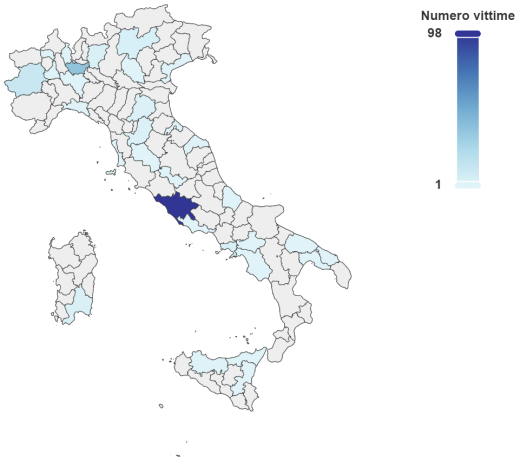

Figura 4: distribuzione geografica delle vittime appartenenti alla constituency

In Figura 5 si riportano i settori di afferenza delle vittime, evidenziando, altresì, la tipologia di minaccia rilevata.

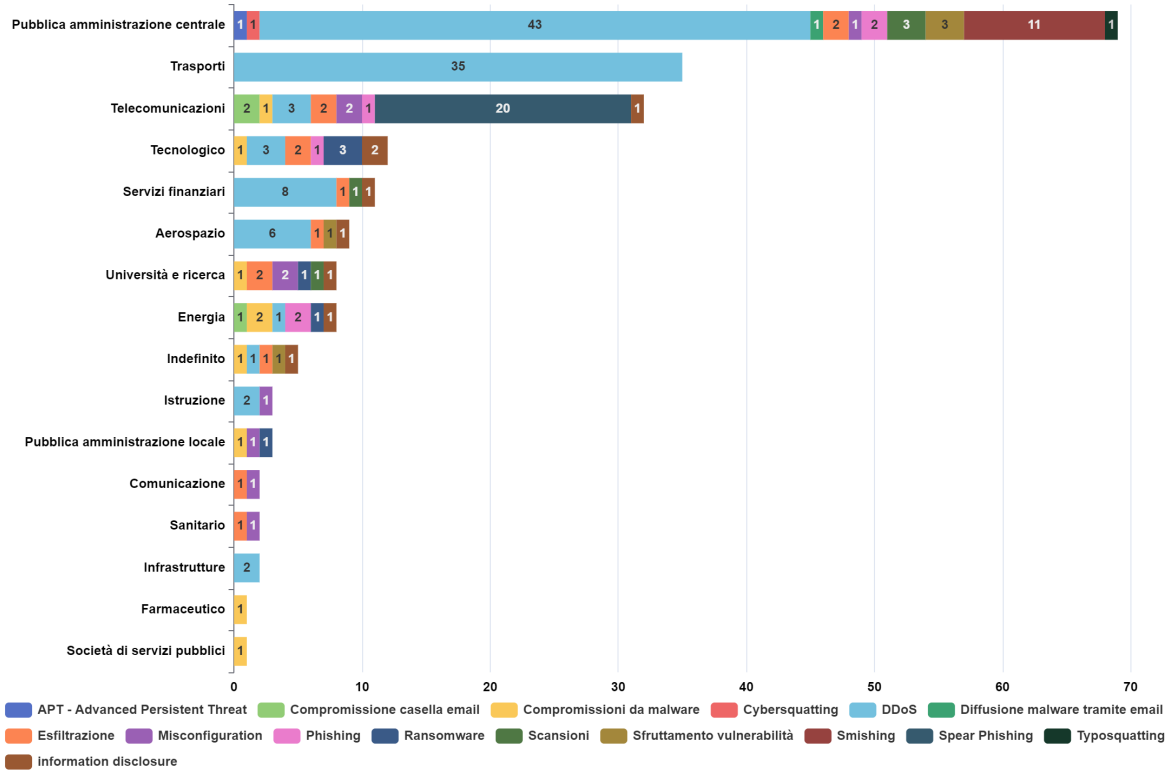

Figura 5: tipologie di minacce con impatto sulla constituency

3 VULNERABILITÀ

A maggio 2024 sono state pubblicate[6] **5.026** nuove CVE, in **aumento** (+**1.355**) rispetto ad aprile. Di queste, **831** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione**(**-196**), e per **14** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (+**4**) rispetto ad aprile.

3.1 Distribuzione delle vulnerabilità sui vendor

In Figura 6 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor.

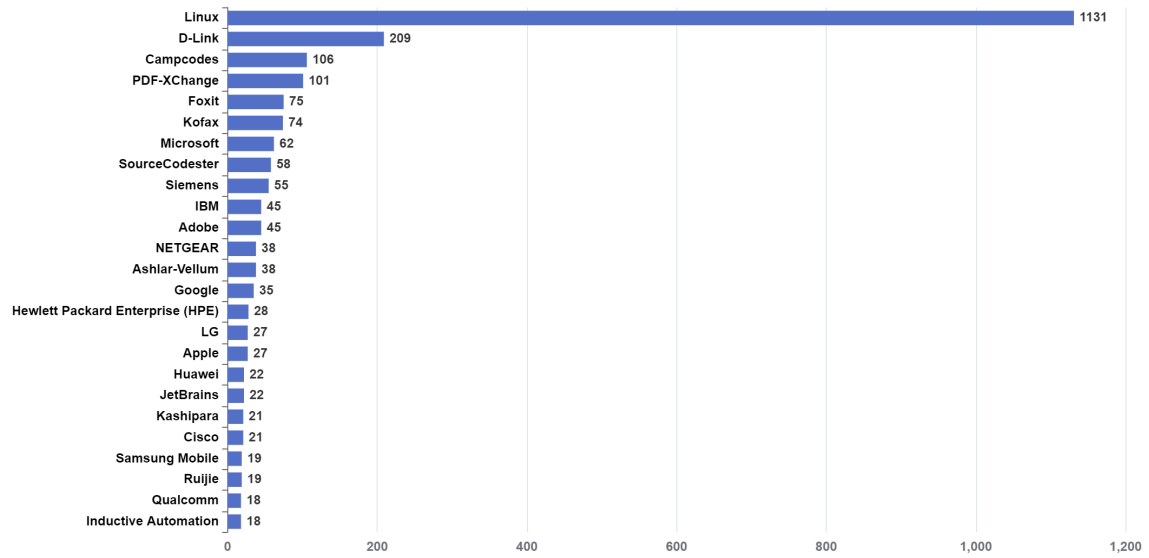

Figura 6: top 25 produttori affetti da vulnerabilità nel mese

In Figura 7 è riportato, invece, il numero delle vulnerabilità rilevate distribuite tra i principali prodotti.

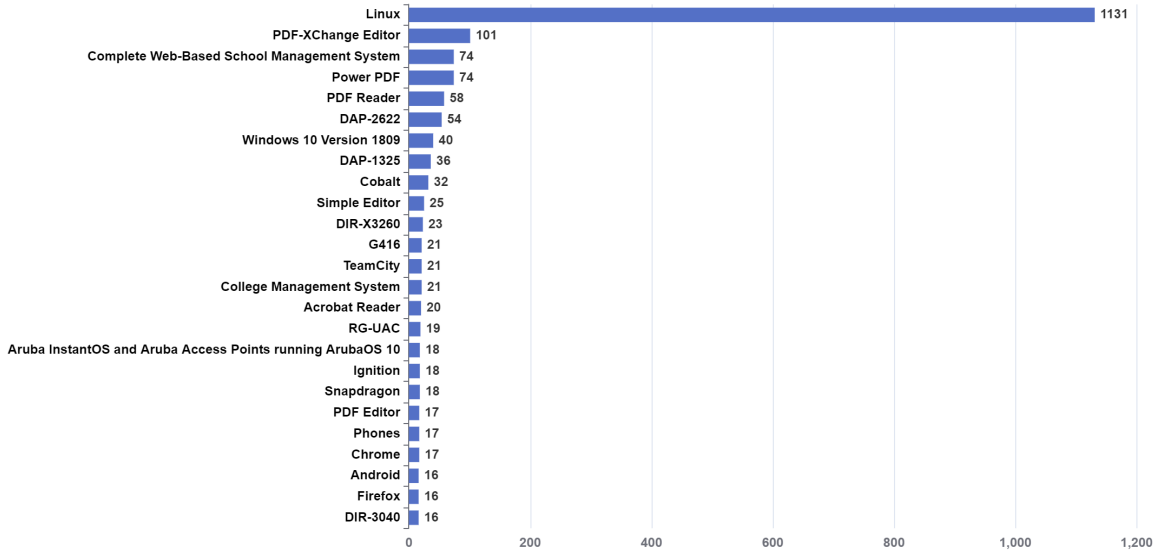

Figura 7: top 25 prodotti affetti da vulnerabilità nel mese

[6]Dati del National Vulnerability Database `https://nvd.nist.gov/vuln` del NIST. Il database completo delle CVE è pubblicamente accessibile `https://cve.mitre.org/`.

3.2 CWE nel mese

In Figura 8 sono riportate le 5 tipologie di vulnerabilità (Common weakness enumeration – CWE) più rilevate.

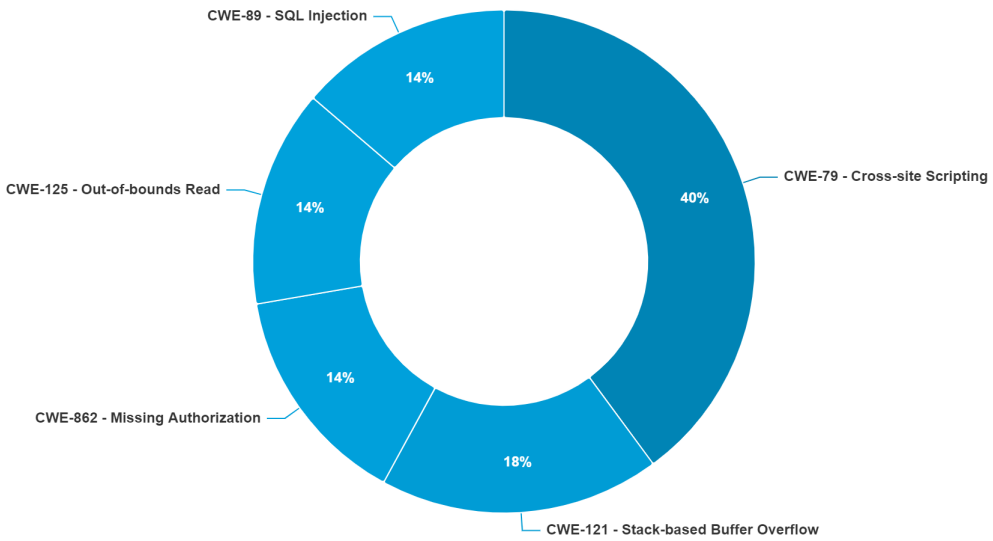

Figura 8: top 5 CWE nel mese

3.3 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **53**. Oltre al consueto aggiornamento mensile di Microsoft (link all'alert sul sito web), che ha risolto un totale di 61 nuove vulnerabilità (3 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Checkpoint**: è stato rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-24919 – già sanata dal vendor – che interessa le soluzioni Checkpoint Security Gateways con le funzionalità Remote Access VPN (IPSec) o Mobile Access blade abilitate. Tale vulnerabilità consentirebbe ad un attacante remoto di sottrarre informazioni sensibili e di ottenere l'accesso agli account target (stima di impatto sistemico **78,07/100**). Link all'alert del 29/05/2024.

- **Atlassian**: disponibile in rete Proof of Concept (PoC) per la vulnerabilità CVE-2024-21683 – già sanata dal vendor – presente in Atlassian Confluence Data Center and Server. Tale vulnerabilità consentirebbe l'esecuzione di codice da remoto sui dispositivi interessati (stima di impatto sistemico **77,3/100**). Link all'alert del 23/05/2024.

- **Linux**: è stato rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-1086 – già sanata dal vendor – che interessa la componente nftextunderscore tables del kernel Linux. Tale vulnerabilità consentirebbe ad un utente malevolo remoto la possibilità di elevare i propri privilegi sui dispositivi target (stima di impatto sistemico **76,66/100**). Link all'alert del 31/05/2024.

- **Fluent Bit**: disponibili in rete Proof of Concept (PoC) per la vulnerabilità CVE-2024-4323 presente in Fluent Bit, sistema open source multi-piattaforma di elaborazione e invio dei log. Tale vulnerabilità potrebbe esporre il servizio al rischio di compromissione, divulgazione di informazioni o all'esecuzione di codice remoto (stima di impatto sistemico **72,56/100**). Link all'alert del 22/05/2024.

- **Ivanti**: disponibile in rete Proof of Concept (PoC) per la vulnerabilità CVE-2024-22026 – già sanata dal vendor – presente in Ivanti EPMM, software per la gestione dei dispositivi mobili, precedentemente noto come MobileIron Core. Tale vulnerabilità consentirebbe ad un attaccante di elevare i propri privilegi ed eseguire codice arbitrario sui sistemi target (stima di impatto sistemico **70,76/100**). Link all'alert del 17/05/2024.

All'indirizzo https://www.csirt.gov.it/contenuti è possibile accedere a tutti gli altri alert pubblicati.

3.4 Vulnerabilità sfruttabili da remoto

Di seguito si riporta l'elenco delle vulnerabilità particolarmente gravi che possono essere sfruttate da attaccanti remoti, oggetto di alert a maggio 2024.

- **Checkpoint Security Gateways** (CVE-2024-24919): tale vulnerabilità permetterebbe ad un attaccante remoto di accedere ad informazioni sensibili e ottenere così le credenziali di accesso al servizio VPN di determinati account. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;

- **SAP** (CVE-2024-33006): tale vulnerabilità permetterebbe ad un attaccante non autenticato di effettuare l'upload di file malevoli sul server vulnerabile che, una volta acceduti dalla vittima, possono portare alla compromissione dell'intero sistema. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;

- **Zabbix** (CVE-2024-22120): tale vulnerabilità, di tipo SQL injection, permette la potenziale esecuzione di comandi arbitrari sull'endpoint vulnerabile. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;

- **Tinyproxy** (CVE-2023-49606): attraverso questa vulnerabilità, di tipo Use After Free, un attaccante remoto non autenticato potrebbe eseguire codice arbitrario sul dispositivo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;

4 ANALISI DELLA MINACCIA

In questa sezione si riportano gli andamenti dei dati sul monitoraggio di malware e delle rivendicazioni di ransomware e DDoS (in Italia ed UE).

4.1 Malware

In Figura 9 è riportato l'andamento della diffusione in Italia delle diverse tipologie di malware, mentre in Figura 10 è riportata la diffusione delle tipologie nel mese di maggio 2024.

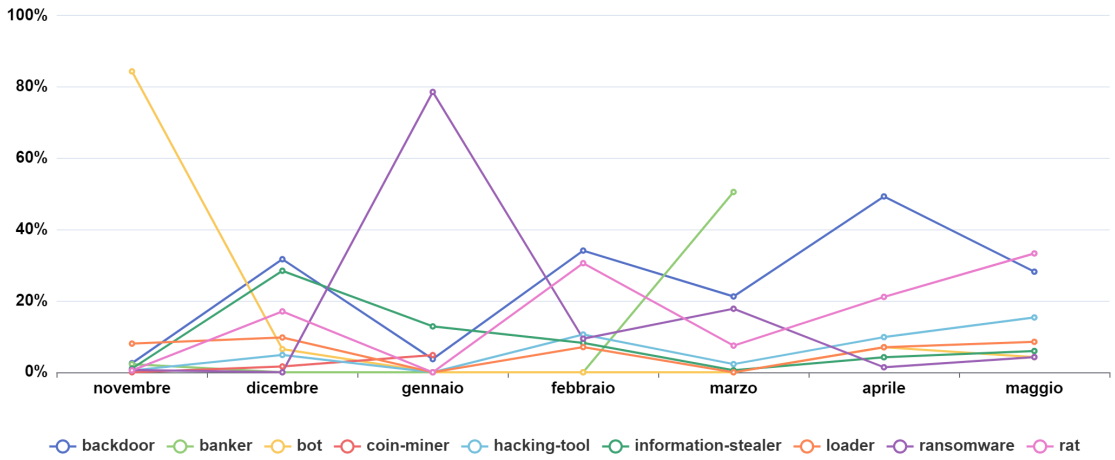

Figura 9: andamento semestrale della diffusione della tipologia di malware in Italia

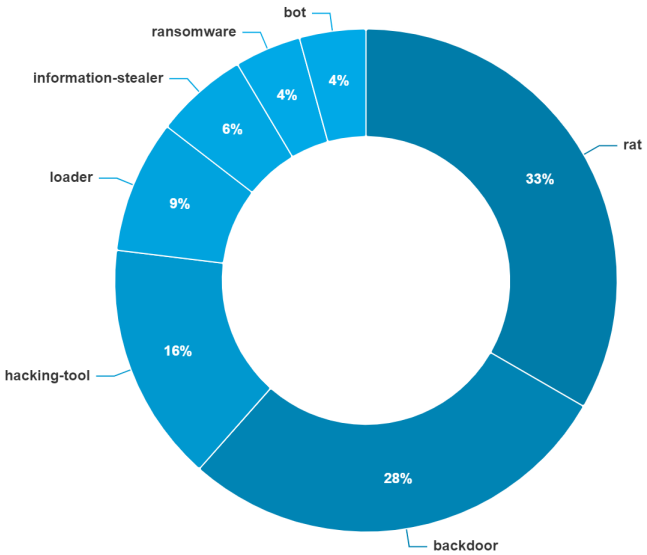

Figura 10: tipologie malware più diffuse in Italia a maggio 2024

In Figura 11 e Figura 12 le stesse informazioni sono riportate in ambito UE.

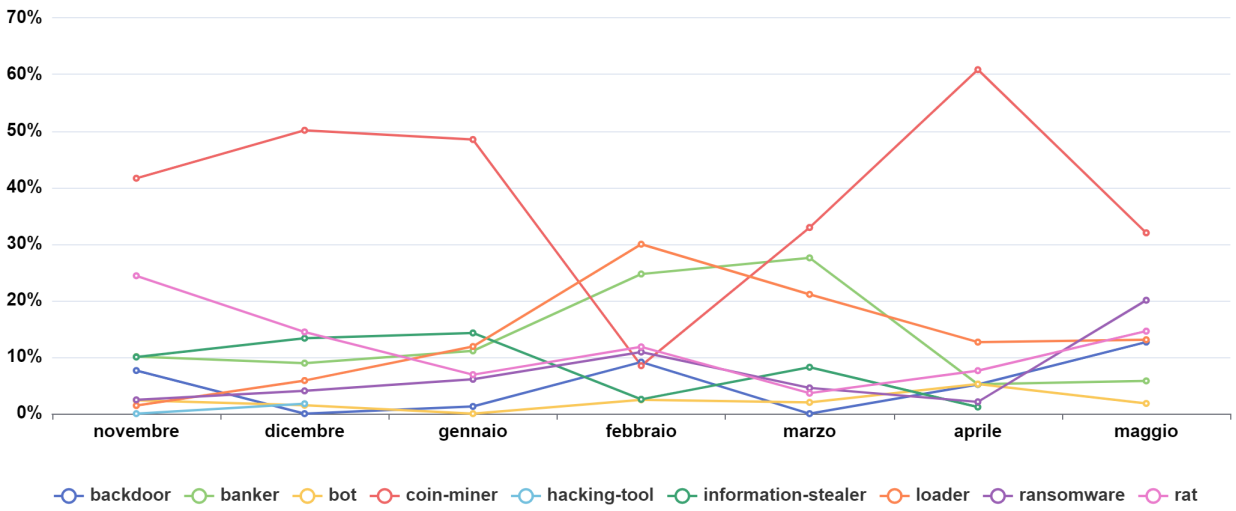

Figura 11: andamento semestrale della diffusione della tipologia di malware in UE

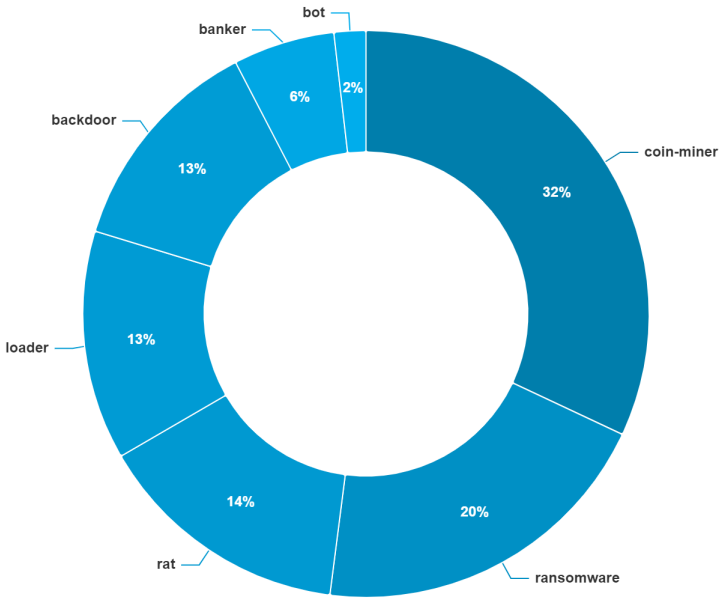

Figura 12: tipologie di malware più diffuse in Europa nel mese

4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel mese di maggio 2024 mostra che l'Italia è stato il **nono paese al mondo** per numero di rivendicazioni e il **quarto in UE**. Nel mese precedente era il sesto al mondo e il secondo in UE[7]. I gruppi più attivi sono stati **Blackbasta** e **Lockbit**. Il grafico in Figura 13 mostra il numero di rivendicazioni ransomware per Paese (top 10).

[7]I dati rilevati si riferiscono solo gli eventi pubblicamente disponibili

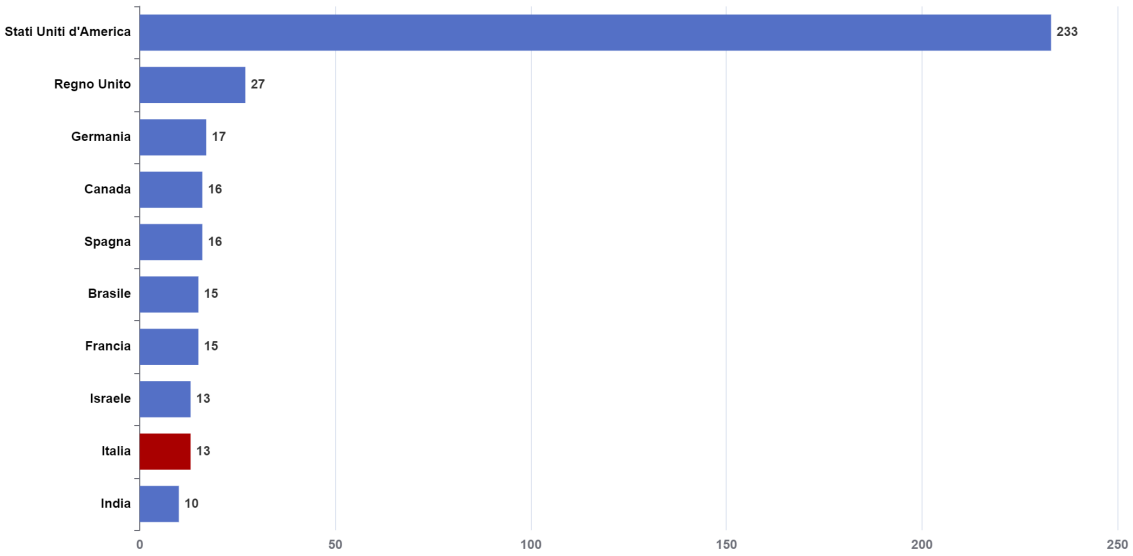

Figura 13: numero di rivendicazioni ransomware per Paese (top 10)

La cartina in Figura 14 mostra la distribuzione geografica delle rivendicazioni.

Figura 14: distribuzione geografica delle rivendicazioni ransomware a livello mondiale (top 10)

Il grafico in Figura 15 mostra il numero di rivendicazioni ransomware per Paese dell'UE (top 10).

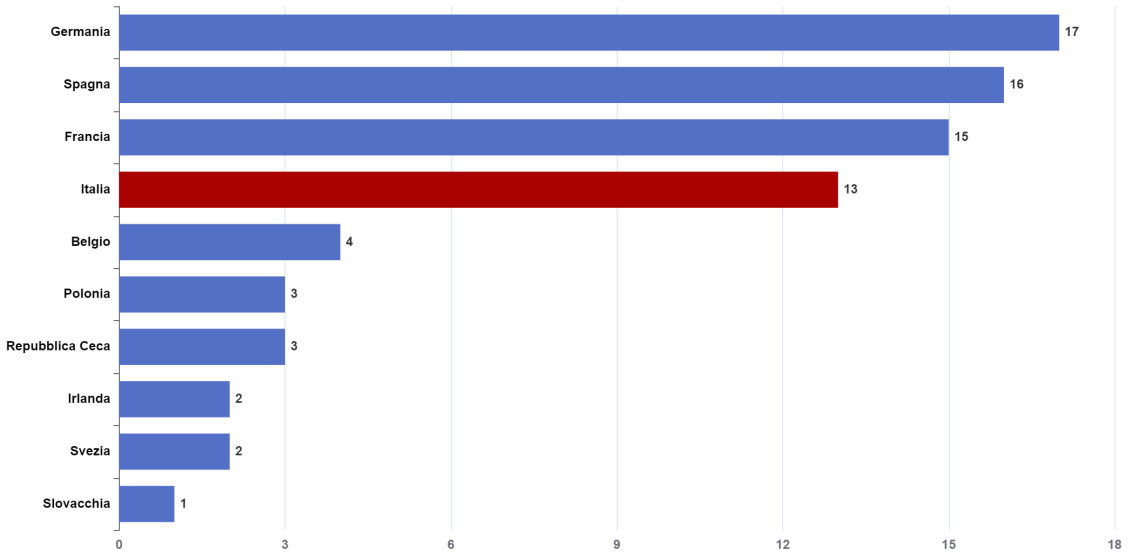

Figura 15: numero di rivendicazioni ransomware per Paese dell'UE

La cartina in Figura 16 mostra, invece, la distribuzione geografica delle rivendicazioni.

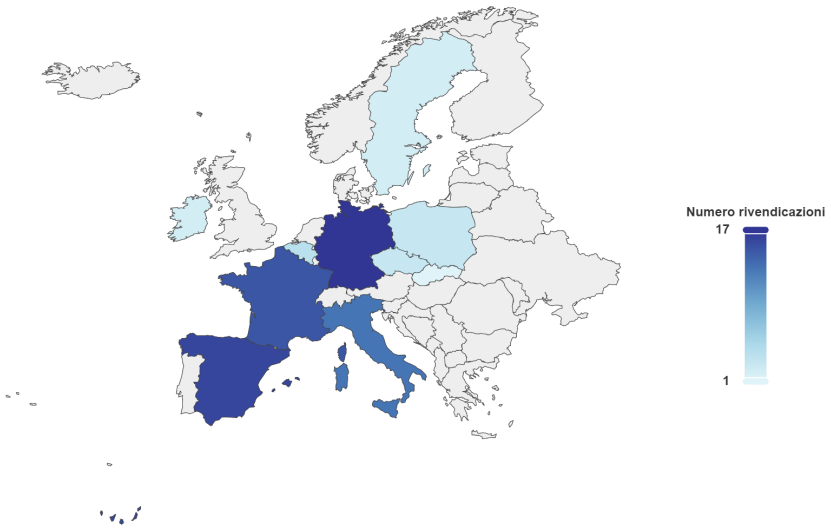

Figura 16: distribuzione geografica degli eventi ransomware in ambito UE

Il grafico in Figura 17 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

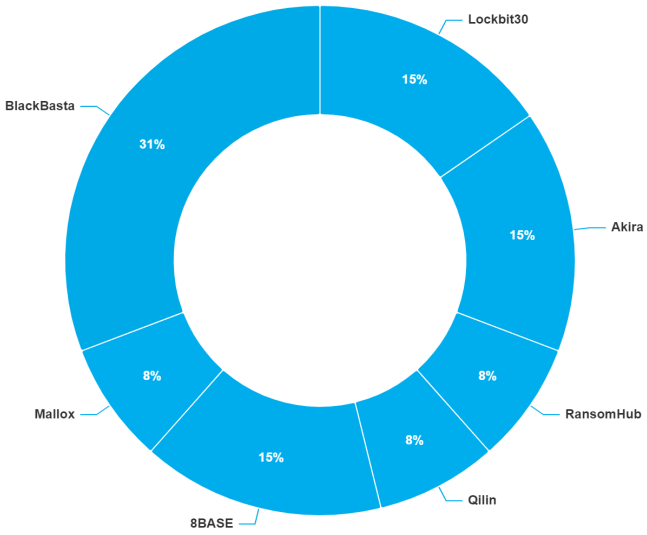

Figura 17: distribuzione percentuale dei gruppi autori delle rivendicazioni

4.3 Rivendicazioni DDoS

Il monitoraggio delle rivendicazioni DDoS nel mese di maggio 2024[8] mostra che l'Italia è stato il **quarto paese al mondo** per numero di rivendicazioni e il **primo in UE**. I gruppi più attivi sono stati **NoName057(16)** e **CyberArmyofRussia**. Il grafico in Figura 18 mostra il numero di rivendicazioni di attacchi DDoS per Paese (top 10).

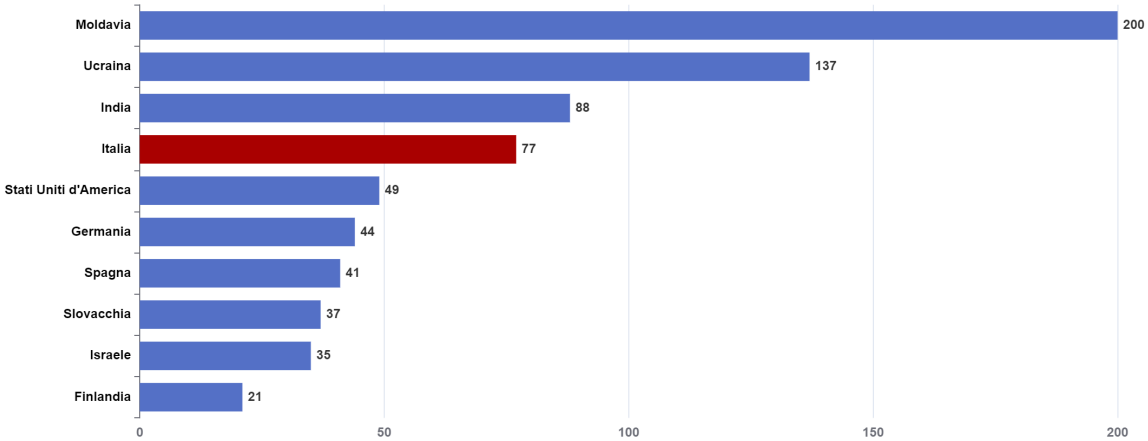

Figura 18: numero di rivendicazioni DDoS per Paese (top 10)

La cartina in Figura 19 mostra la distribuzione geografica delle rivendicazioni.

[8] I dati rappresentano solo gli eventi pubblicamente rivendicati.

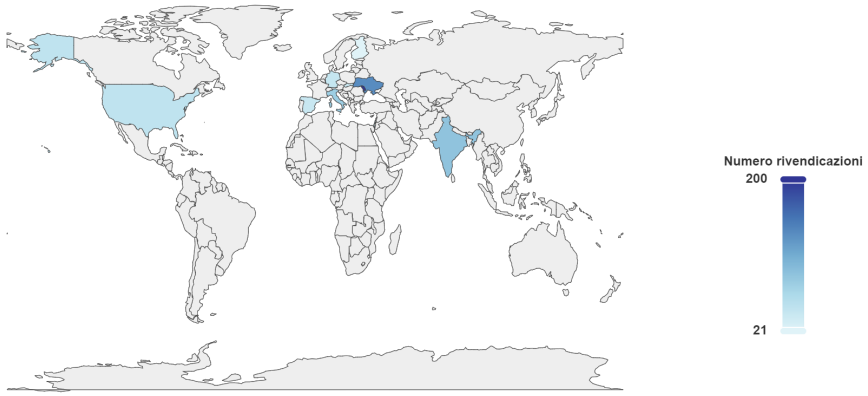

Figura 19: distribuzione geografica delle rivendicazioni DDoS a livello mondiale (top 10)

Il grafico in Figura 20 mostra il numero di rivendicazioni DDoS per Paese dell'UE (top 10).

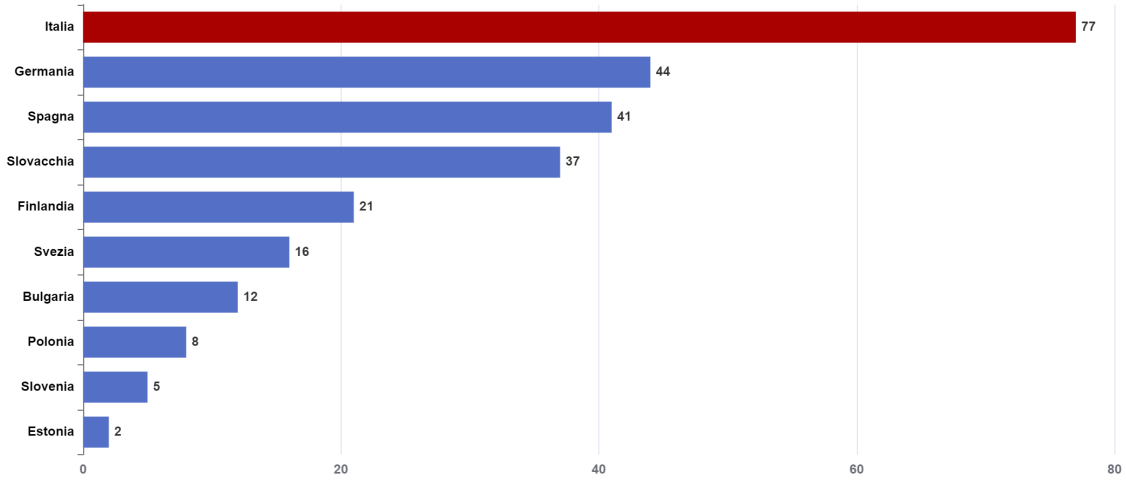

Figura 20: numero di rivendicazioni DDoS per Paese dell'UE

La cartina in Figura 21 mostra, invece, la distribuzione geografica delle rivendicazioni.

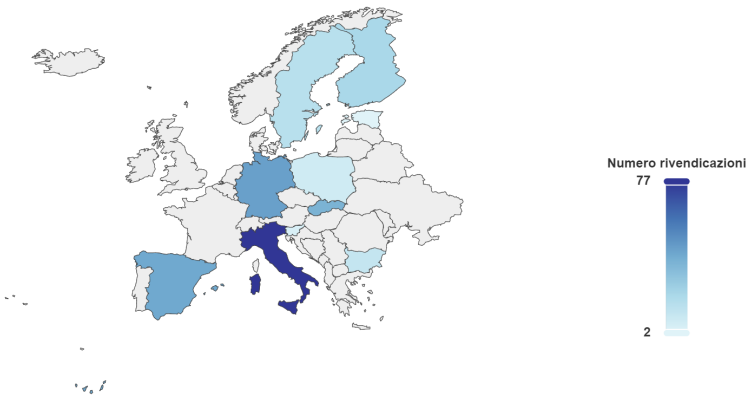

Figura 21: distribuzione geografica degli eventi DDoS in ambito UE

Il grafico in Figura 22 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

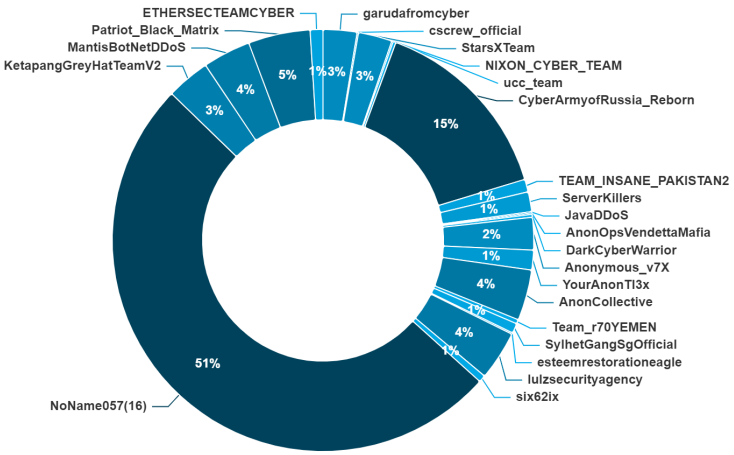

Figura 22: distribuzione percentuale dei gruppi autori delle rivendicazioni

5 GLOSSARIO

Asset a rischio: Sistemi o servizi esposti su Internet da soggetti italiani, rilevati dalle attività di monitoraggio proattivo e per i quali vengono inviate specifiche comunicazioni.

Attività proattive: Le attività proattive comprendono tutte quelle volte a monitorare, su base continuativa, i servizi e gli asset esposti su internet dai soggetti della constituency, al fine di rilevare vulnerabilità cui gli stessi potrebbero essere potenzialmente esposti.

Attività reattive: Le attività reattive comprendono tutte quelle avviate a partire da segnalazioni o altre comunicazioni ricevute dal CSIRT Italia oppure intraprese a seguito della scoperta di compromissioni e nuove vulnerabilità da parte delle attività di monitoraggio.

Brand abuse: Con il termine Brand abuse si intende l'utilizzo non autorizzato o illecito di un marchio o di un logo che viene sfruttato in ambito cyber per scopi fraudolenti. Ad esempio, i cyber criminali creano siti web o inviano e-mail che utilizzano il marchio o il logo di un'organizzazione per ingannare e indurre le vittime a consegnare informazioni sensibili o commettere errori.

Comunicazione inviata: Alert, anche massivi, inviati a Pubbliche Amministrazioni e operatori privati potenzialmente interessati da eventi cyber.

Comunicazione ricevuta: e-mail ricevute dal CSIRT Italia relative ad informazioni contenenti profili di natura cyber anche generiche, sottoposte a valutazione preliminare per determinare l'apertura di case o meno.

Constituency: La constituency è l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli eventi cibernetici. La stessa è organizzata per livelli di criticità, validi sia per la pubblica amministrazione che per i privati.

Denial of Service (DoS): Con l'acronimo DoS (Denial of Service) si indica un tipo di attacco che mira a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. Nella versione distribuita (Distributed DoS) l'attacco proviene da un gran numero di dispositivi ed è diretto verso un target. Le botnet sono uno strumento per condurre un attacco DDoS.

Dispositivi o servizi esposti incautamente: Dispositivi e servizi che generalmente non dovrebbero essere esposti pubblicamente su Internet quali ad esempio servizi Remote Desktop Protocol (RDP) o Internet of Things (IoT).

Dispositivi o Servizi obsoleti o vulnerabili: Dispositivi e servizi che presentano vulnerabilità note o che usano versioni di software non più supportate o End of Life (EoL).

Dispositivi o servizi con misconfigurazioni: Dispositivi e servizi che presentano delle configurazioni non in linea con le best practice del settore o errate, che pertanto potrebbero comprometterne la sicurezza.

Exploit: Termine che si riferisce ad un mezzo informatico (in genere software) impiegato per lo sfruttamento di vulnerabilità di un sistema ICT al fine di accedervi abusivamente o porre in essere azioni malevole.

Evento cyber: Un avvenimento con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti. Qualora fosse confermato l'impatto, l'evento cyber viene considerato incidente.

Incidente: Evento cyber con impatto confermato.

Malware: Con il termine malware si indica un qualsiasi software o firmware destinato ad eseguire un processo non autorizzato che ha un impatto negativo sulla riservatezza, integrità o disponibilità di un sistema.

Phishing: Con il termine phishing si indica una tecnica impiegata per cercare di acquisire informazioni riservate di persone o organizzazioni, come password, numeri di carta di credito o dati bancari, attraverso una sollecitazione proditoria della vittima attuata tramite e-mail, sito web o social media.

Portale di collaboration: Portale riservato ai membri della constituency del CSIRT Italia e costituisce lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati.

Portale pubblico: Sito web del CSIRT Italia accessibile all'intera comunità.

Ransomware: Il ransomware è un malware in cui l'attaccante cifra i dati di un'organizzazione al fine di ottenere il pagamento di un riscatto. Il ransomware può causare seri danni alle organizzazioni in termini di perdita dei dati, di interruzione delle attività, di esposizione di informazioni riservate, con un impatto economico, organizzativo e reputazionale rilevante per le vittime.

Ransom notes: Con il termine ransom notes si indicano i messaggi o le note che i cybercriminali inseriscono nei file delle vittime dopo averli cifrati. Queste note possono contenere la richiesta di un riscatto e le istruzioni per effettuare il pagamento (vedi anche ransomware).

Richieste di informazioni: Richieste effettuate dal CSIRT Italia al soggetto potenzialmente impattato da un evento cyber per acquisire ulteriori elementi, come ad esempio la conferma di una possibile compromissione (e la conseguente classificazione dell'evento cyber quale incidente).

Segnalazione: Comunicazioni previste per legge per i soggetti appartenenti al Perimetro di Sicurezza Nazionale Cibernetica, per gli Operatori di Servizi Essenziali e Fornitori di Servizi Digitali (Direttiva NIS), e per gli operatori di comunicazione (D.M. Telco). Le Segnalazioni vengono trattate direttamente come eventi cyber.

Smishing: Lo smishing è una forma di phishing che utilizza i telefoni cellulari come vettore di attacco. Il criminale compie l'attacco con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito. Lo smishing viene attuato attraverso l'invio di SMS (Short Message Service), da cui il nome "SMiShing".

Spear phishing: Campagne di phishing mirate a specifici utenti, spesso con contenuti personalizzati in base alle vittime ed attuate anche tramite i social network.

Traffic Light Protocol: Protocollo utilizzato per lo scambio di informazioni al fine di garantire la diffusione delle stesse in modo controllato.

Triage: Fase in cui gli operatori analizzano le segnalazioni, le comunicazioni ricevute e ogni possibile evento cyber di cui lo CSIRT Italia viene a conoscenza, anche a seguito di attività di monitoraggio proattivo, al fine di identificare i potenziali impatti e classificare quindi l'informazione come evento cyber e proseguire o meno con le ulteriori fasi di trattazione.

Vulnerabilità (sfruttamento di): Lo sfruttamento delle vulnerabilità comprende quegli attacchi attuati attraverso l'utilizzo degli errori e difetti involontariamente presenti nel software. I cyber criminali possono sfruttare vulnerabilità già note nella comunità ma non ancora "sanate" dalle vittime, oppure vulnerabilità di tipo "0-day", tipicamente scoperte dagli attaccanti e non ancora note al produttore del software, per le quali quindi non esiste ancora un rimedio.

LaTeX