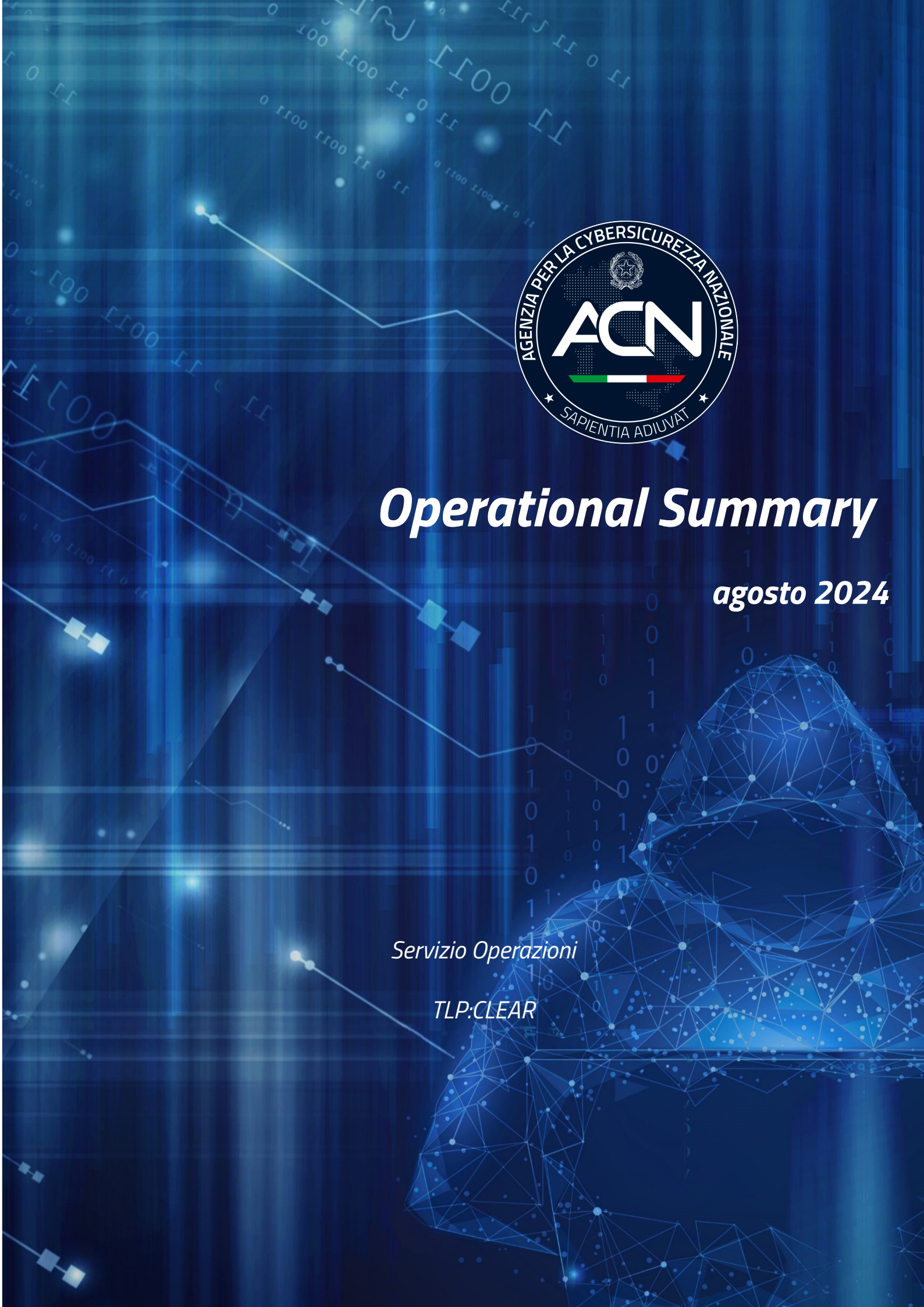

Operational Summary

agosto 2024

Servizio Operazioni

TLP:CLEAR

Operational Summary

Servizio Operazioni

agosto 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 riceve 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 dotano l'Agenzia di un ampio cono di visibilità sullo stato della minaccia cyber a danno del sistema Paese e forniscono, 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 agosto 2024 nonché i 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

Ad agosto 2024 sono stati individuati **122** eventi cyber, in **diminuzione** del 29% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 242 soggetti nazionali**: 193 appartenenti alla constituency[1], i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 122 eventi cyber **41 sono stati classificati quali incidenti**, in **diminuzione** del 52% rispetto a luglio.

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[2], riferita ai successivi 3 mesi.

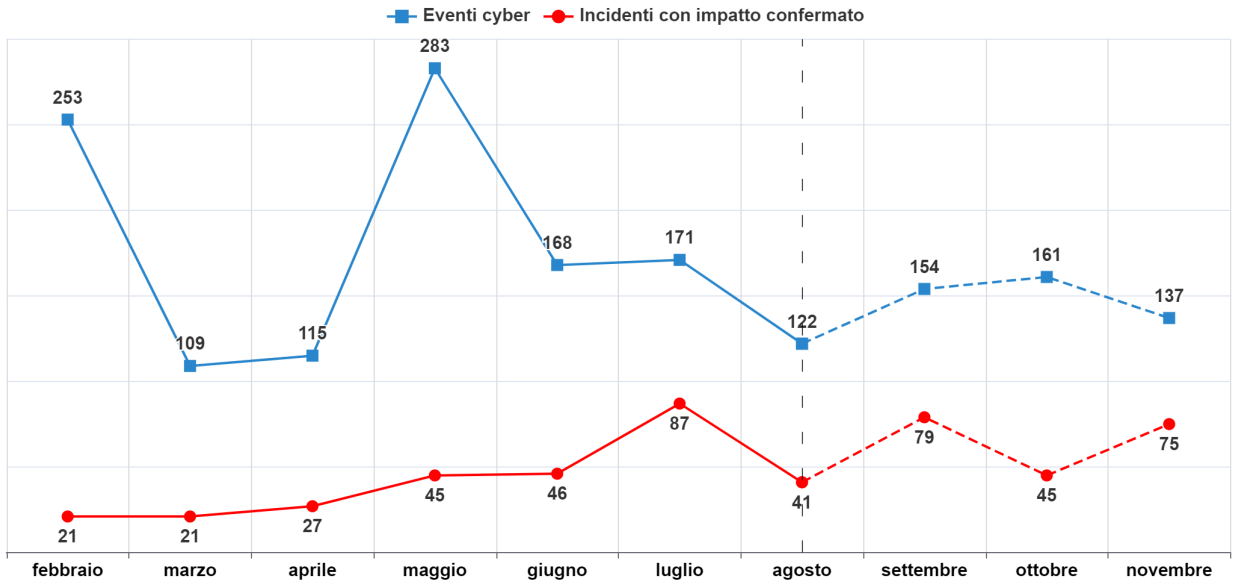

Figura 1: andamento attività reattive e analisi previsionale

[1]La constituency è l'insieme dei soggetti che operano nei settori NIS, Perimetro, Telco o nella Pubblica amministrazione, 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]La previsione dà 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.

2.1 Settori impattati

In Figura 2 si riporta il numero di vittime di eventi per settore impattato[3]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico). L'aumento nel settore Università e ricerca è dovuto al rilevamento di un dataleak, pubblicato su un forum criminale, con impatti su oltre 60 soggetti.

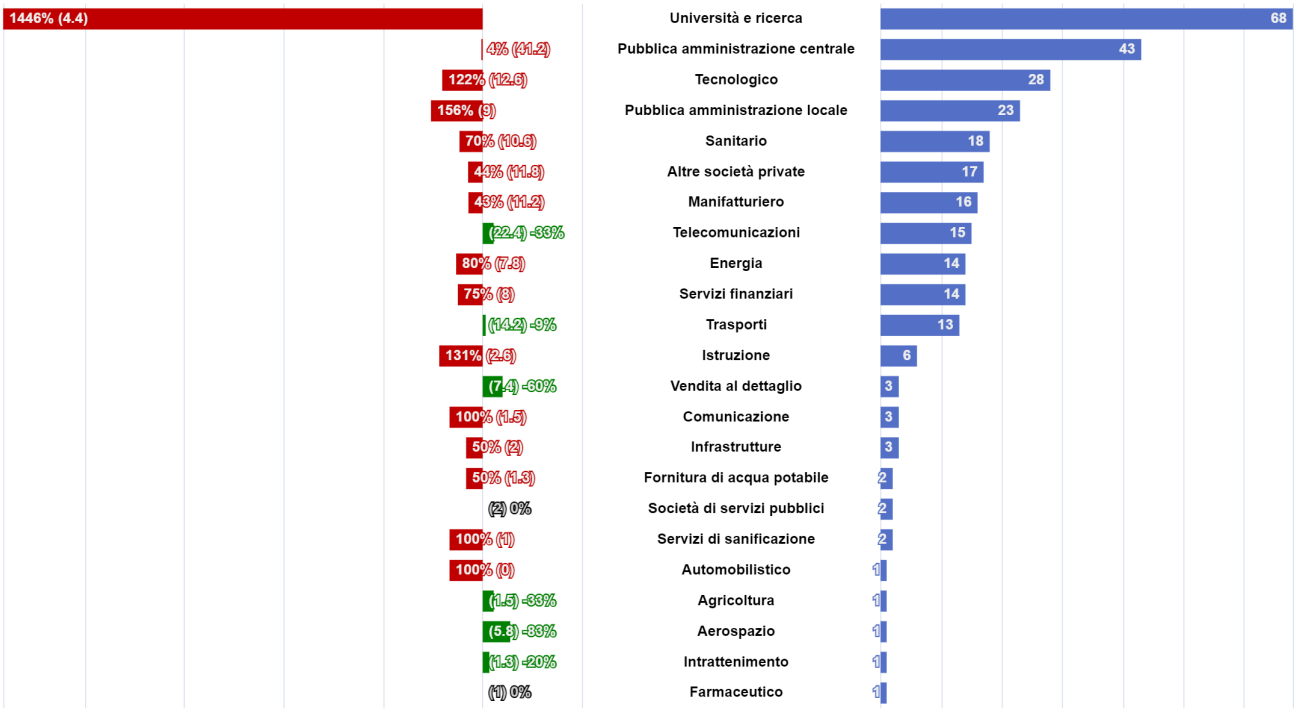

Figura 2: numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente

2.2 Tipologia di minacce negli eventi

In Figura 3 si riporta il numero di minacce rilevate negli eventi[4] e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico).

[3]Si noti che ogni evento può avere più vittime, afferenti ad uno o più settori di attività e che una vittima può operare in più settori. Talvolta non è possibile associare un evento ad una vittima e la vittima ad un settore.

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

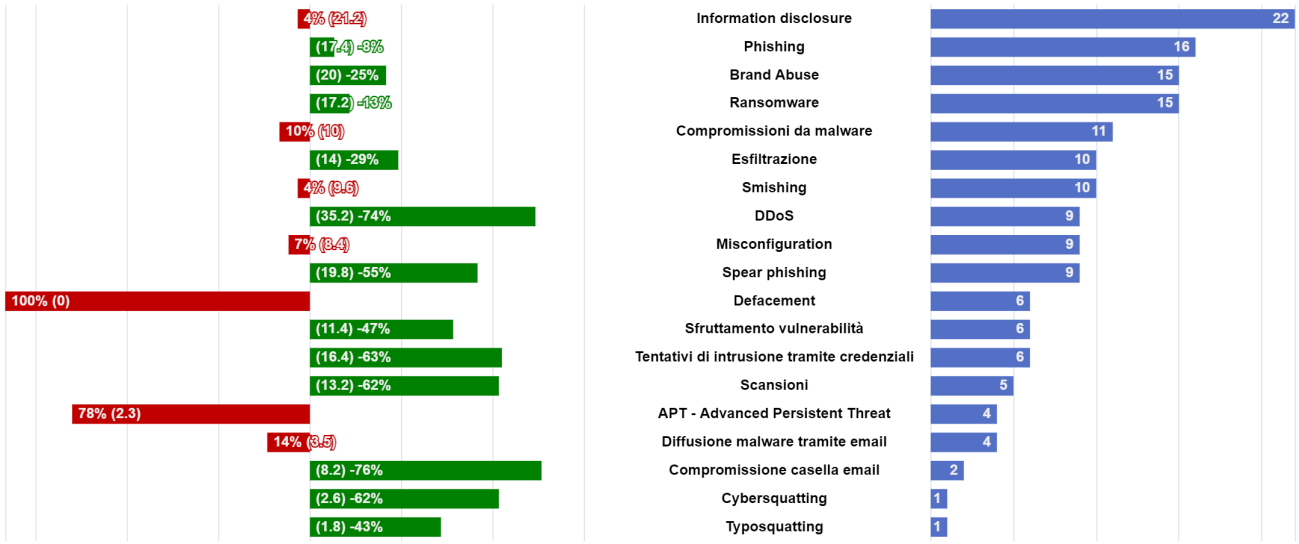

Figura 3: tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente

2.3 Focus constituency

Dei 122 eventi cyber **193** hanno riguardato soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

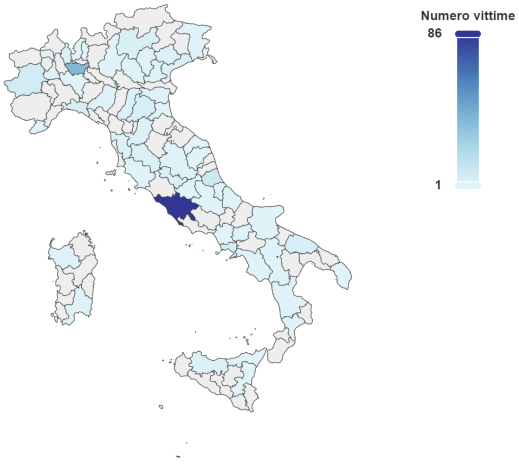

Figura 4: distribuzione geografica delle vittime appartenenti alla constituency

In Figura 5 si riportano i settori di afferenza delle vittime, evidenziando, altresì, la tipologia di minaccia rilevata. Si ricorda che ad un evento possono essere associate più tipologie di minaccia.

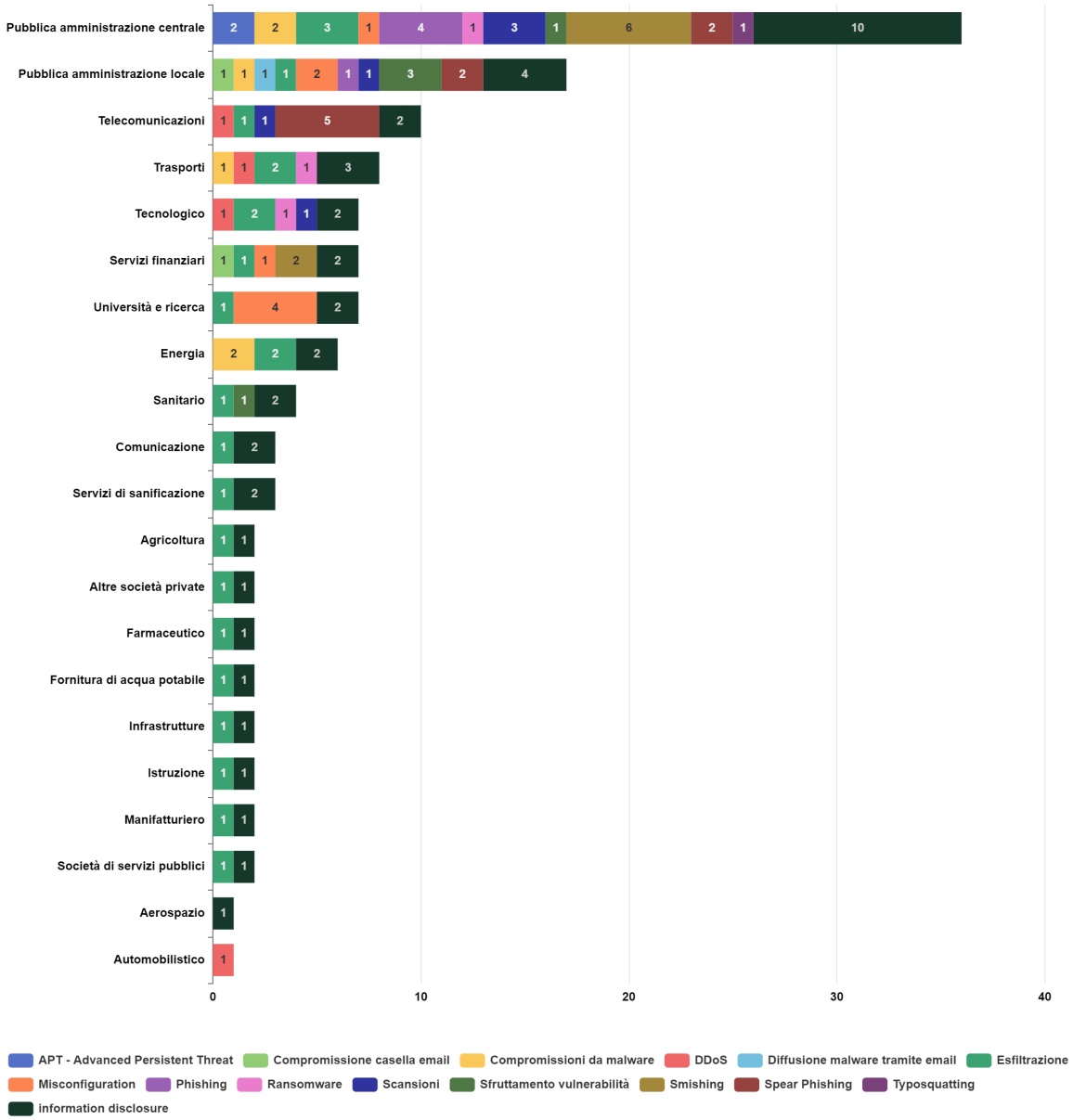

Figura 5: tipologia di minacce con impatto sui settori della constituency

3 VULNERABILITÀ

Ad agosto 2024 sono state pubblicate[5] **2.885** nuove CVE, in **diminuzione** (**−276**) rispetto a luglio. Di queste, **538** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+279**) e per **12** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (**+3**) rispetto a luglio.

3.1 Distribuzione delle vulnerabilità sui vendor

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

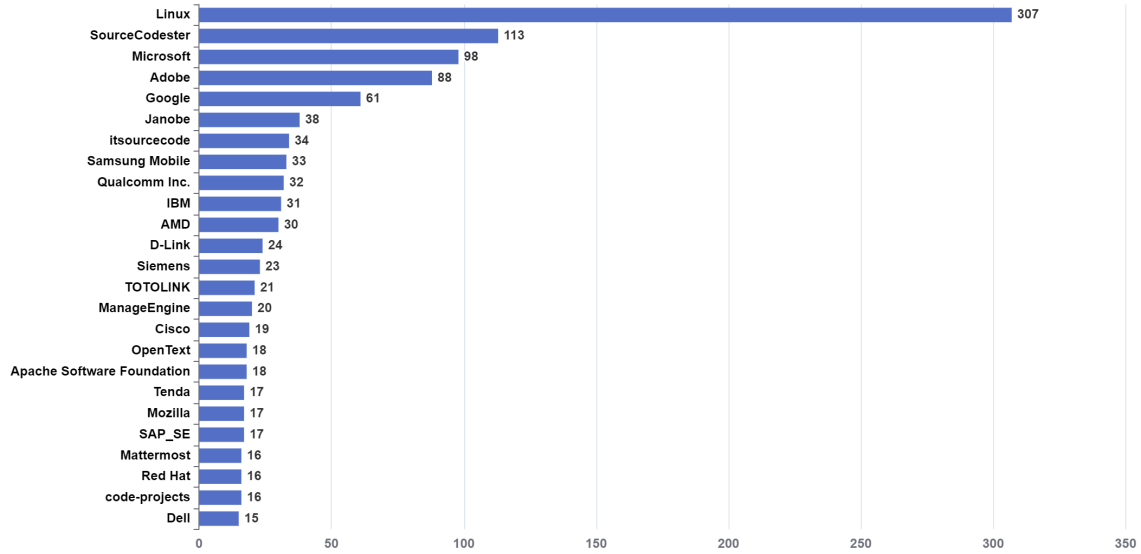

Figura 6: top 25 produttori affetti da vulnerabilità nel mese

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

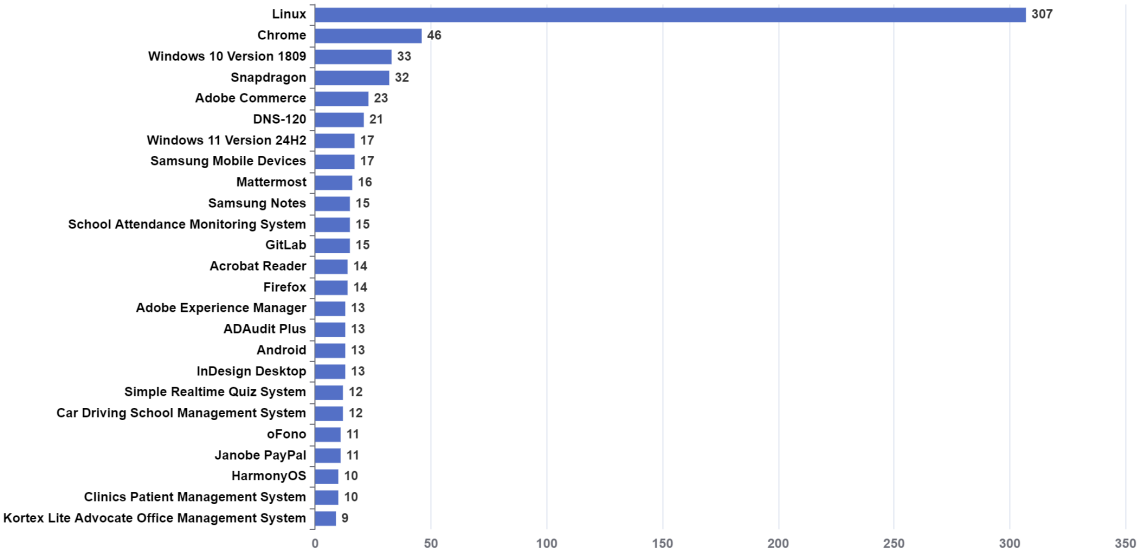

Figura 7: top 25 prodotti affetti da vulnerabilità nel mese

[5]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 weakness (Common Weakness Enumeration – CWE) più rilevate.

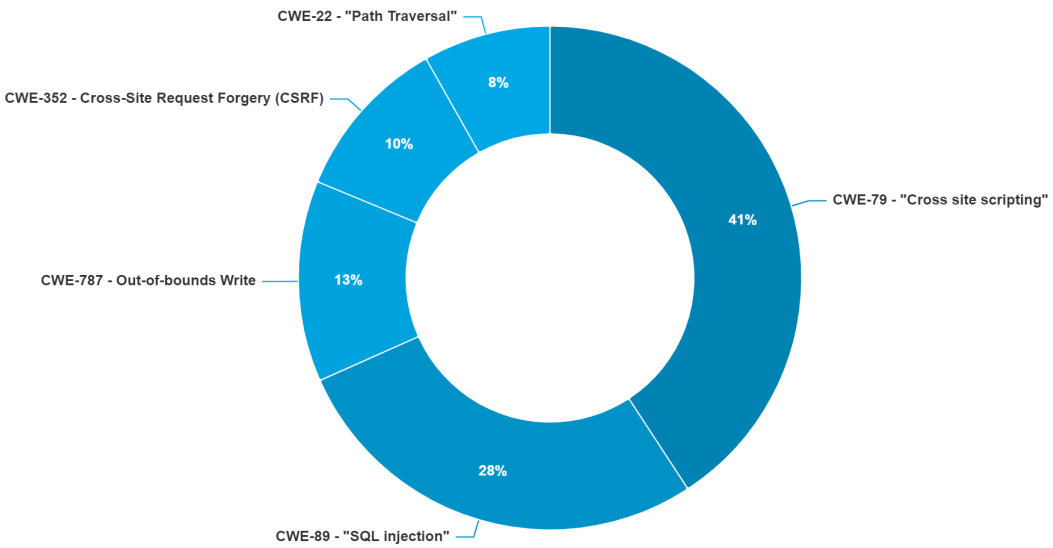

Figura 8: top 5 CWE nel mese

3.3 Vulnerabilità con maggior probabilità di sfruttamento

Di seguito il dettaglio delle 3 vulnerabilità che potrebbero subire il maggior incremento nel trend di exploitation, ottenuto monitorando l'Exploit Prediction Scoring System (EPSS)[6] fornito dal FIRST nel mese in esame.

Tabella 1: CVE-2024-38856

Vendor	Apache Software Foundation
Prodotti e versioni vulnerabili	OFBiz, versioni fino alla 18.12.14
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo sul server.
Data di rilascio CVE	05/08/2024 modificata il 28/08/2024
CVSS score 3.x	9.8 CRITICAL
EPSS max score	0.93

[6] `https://www.first.org/epss/` fornisce un'indicazione della probabilità che una vulnerabilità venga sfruttata, è un valore aggiornato quotidianamente dal FIRST.

Tabella 2: CVE-2018-0824

Vendor	Microsoft Corporation
Prodotti e versioni vulnerabili	Microsoft COM for Windows, tutte le versioni di Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo.
Data di rilascio CVE	09/05/2018 modificata il 08/08/2024
CVSS score 3.x	8.8 HIGH
EPSS max score	0.73

Tabella 3: CVE-2024-38112

Vendor	Microsoft Corporation	
Prodotti e versioni vulnerabili	**Prodotto**	**Build Number**
	Windows 10 Version 1809 for 32-bit Systems	10.0.17763.6054
	Windows Server 2019	10.0.17763.6054
	Windows 11 Version 22H2 for x64-based Systems	10.0.22621.3880
	Windows 10 Version 21H2 for x64-based Systems	10.0.19044.4651
	Windows Server 2022	10.0.20348.2582
	Windows 11 version 21H2 for x64-based Systems	10.0.22000.3079
	Windows 11 version 21H2 for ARM64-based Systems	10.0.22000.3079
	Windows Server 2019 (Server Core installation)	10.0.17763.6054
	Windows Server 2022, 23H2 Edition (Server Core installation)	10.0.25398.1009
	Windows Server 2022 (Server Core installation)	10.0.20348.2582
	Windows 10 Version 21H2 for ARM64-based Systems	10.0.19044.4651
	Windows Server 2012 R2 (Server Core installation)	6.3.9600.22074
	Windows 10 Version 22H2 for 32-bit Systems	10.0.19045.4651
	Windows 11 Version 23H2 for ARM64-based Systems	10.0.22631.3880
	Windows Server 2012 R2	6.3.9600.22074
	Windows 10 Version 22H2 for ARM64-based Systems	10.0.19045.4651
	Windows 10 Version 1809 for x64-based Systems	10.0.17763.6054

	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	6.0.6003.22769
	Windows Server 2008 for x64-based Systems Service Pack 2	6.0.6003.22769
	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	6.0.6003.22769
	Windows Server 2008 for 32-bit Systems Service Pack 2	6.0.6003.22769
	Windows 10 Version 1809 for ARM64-based Systems	10.0.17763.6054
	Windows Server 2016 (Server Core installation)	10.0.14393.7159
	Windows 10 Version 21H2 for 32-bit Systems	10.0.19044.4651
	Windows Server 2016	10.0.14393.7159
	Windows 10 Version 1607 for x64-based Systems	10.0.14393.7159
	Windows 10 Version 1607 for 32-bit Systems	10.0.14393.7159
	Windows 10 for x64-based Systems	10.0.10240.20710
	Windows 11 Version 22H2 for ARM64-based Systems	10.0.22621.3880
	Windows 10 for 32-bit Systems	10.0.10240.20710
	Windows 11 Version 23H2 for x64-based Systems	10.0.22631.3880
	Windows 10 Version 22H2 for x64-based Systems	10.0.19045.4651
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette ad un attaccante di eseguire codice malevolo.	
Data di rilascio CVE	09/07/2024 modificata il 14/08/2024	
CVSS score 3.x	7.5 HIGH	
EPSS max score	0.97	

3.4 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Ad agosto 2024 gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **43**. Oltre al consueto aggiornamento mensile di Microsoft (link all'alert sul sito web), che ha risolto un totale di 85 nuove vulnerabilità (10 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Solarwinds**: risolte due vulnerabilità, con gravità "critica", nel prodotto Web Help Desk di SolarWinds. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato l'esecuzione di codice arbitrario e la lettura/modifica di file sui dispositivi target (stima di impatto sistemico **79,23/100**). Link all'alert del 14/08/2024;
- **Ivanti**: Ivanti rilascia aggiornamenti di sicurezza che risolvono 8 vulnerabilità, di cui una con gravità "critica" e 7 con gravità "alta", nei prodotti Ivanti Neurons for ITSM, Ivanti Avalanche e Ivanti Virtual Traffic Manager (stima di impatto sistemico **79,23/100**). Link all'alert del 14/08/2024;
- **Apache**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-32113 – già sanata dal vendor – che interessa Apache OFBiz, suite open source per la gestione aziendale. Tale vulnerabilità, di tipo "Path Traversal", potrebbe permettere ad un utente malevolo la possibilità di eseguire comandi arbitrari sui sistemi target (stima di impatto sistemico **68,07/100**). Link all'alert del 05/08/2024;
- **Moodle**: rilevate 16 nuove vulnerabilità in Moodle, nota piattaforma open source tipicamente utilizzata per l'erogazione di corsi in modalità e-learning, di cui 1 con gravità "critica" e 7 con gravità "alta" (stima di impatto sistemico **66,41/100**). Link all'alert del 22/08/2024.

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

3.5 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 agosto 2024

- **OpenSSH** (CVE-2024-6387): tale vulnerabilità permetterebbe ad un attaccante non autenticato di eseguire da remoto codice arbitrario sul dispositivo coi privilegi di root e senza alcuna interazione utente. Ciò sarebbe possibile per mezzo di un'erronea gestione di una race condition da parte di *sshd*, sfruttabile da eventuali attaccanti utilizzando un gran numero di tentativi di login falliti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
- **GeoServer** (CVE-2024-36401): tale vulnerabilità – di tipo Code Injection – permetterebbe ad un attaccante non autenticato di eseguire da remoto codice arbitrario sui server vulnerabili. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
- **Cisco NX-OS** (CVE-2024-20399): tale vulnerabilità permetterebbe ad un utente malevolo, in possesso di credenziali amministrative valide sull'apparato ed autenticato, la possibilità di eseguire comandi arbitrari come utente root sul sistema operativo del dispositivo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
- **GitLab** (CVE-2024-5655): la vulnerabilità, di tipo Improper Access Control, potrebbe permettere ad un utente malevolo di attivare una pipeline come un altro utente in determinate circostanze. Ciò potrebbe permettere l'esecuzione di azioni non autorizzate sul sistema e potenzialmente di compromettere la confidenzialità e l'integrità dei dati su di esso memorizzati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **CitrixNetScaler ADC** e **NetScaler Gateway** (CVE-2023-6548): contrariamente a quanto noto in precedenza, tale vulnerabilità - di tipo Code Injection - permetterebbe a un attaccante non autenticato di eseguire da remoto codice arbitrario attraverso l'interfaccia di management dell'apparato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;

- **Telerik Report Server** (CVE-2024-4358): tale vulnerabilità - di tipo Authentication Bypass - permetterebbe a un eventuale attaccante non autenticato di ottenere l'accesso alle funzionalità di Telerik Report Server, laddove questo sia ospitato su un installazione Microsoft IIS, eludendone i meccanismi autenticazione.

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 agosto 2024.

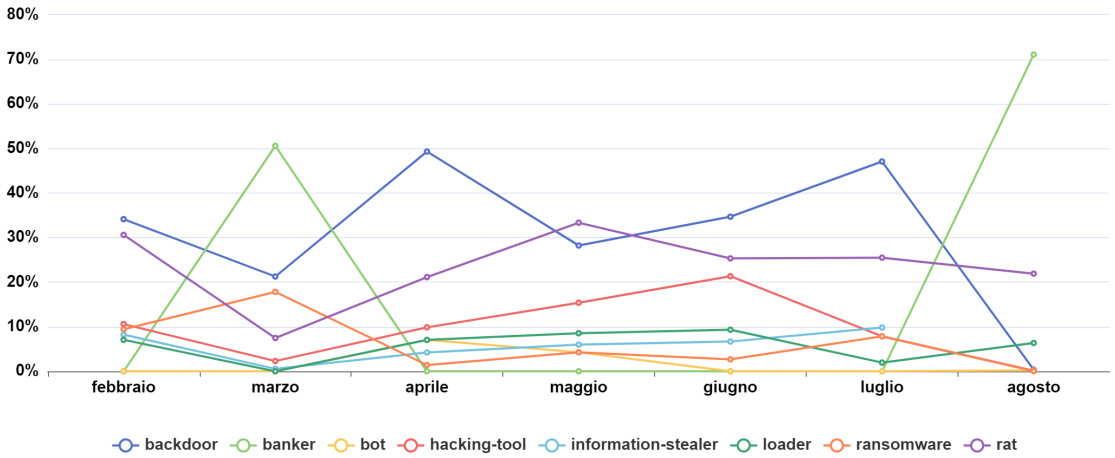

Figura 9: andamento semestrale della diffusione della tipologia di malware in Italia

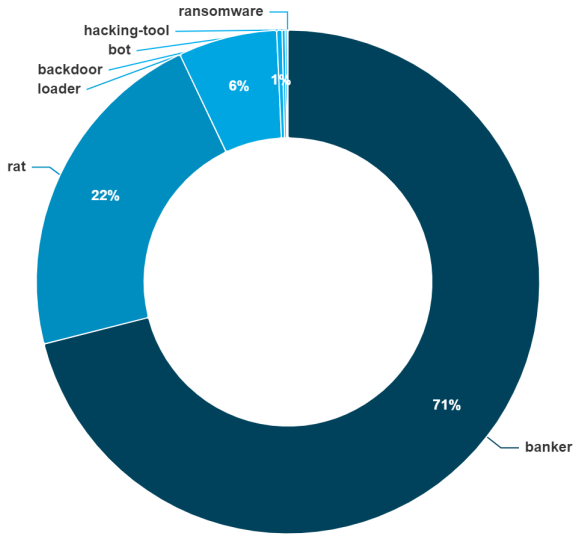

Figura 10: tipologie malware più diffuse in Italia nel mese di agosto 2024

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

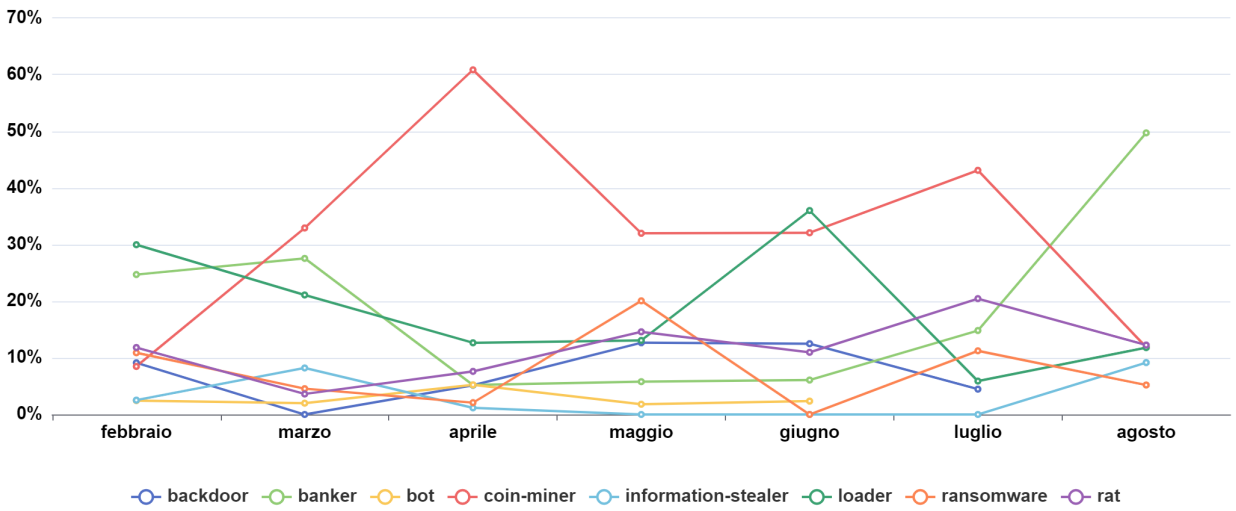

Figura 11: andamento semestrale della diffusione della tipologia di malware in UE

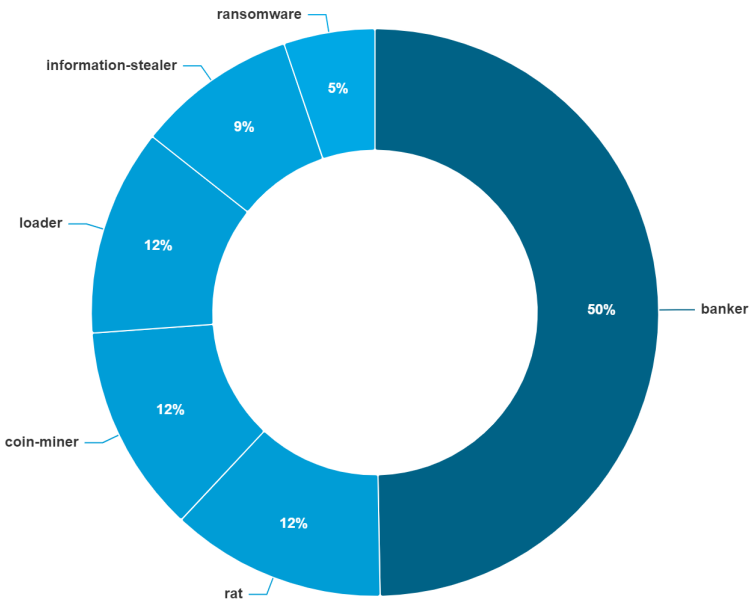

Figura 12: tipologie di malware più diffuse in Europa nel mese

4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel mese di agosto 2024 ha permesso di individuare **14** rivendicazioni di attacchi Ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **HuntersInternational** e **CiphBit**. Il grafico in Figura 13 mostra l'andamento delle rivendicazioni nell'anno in corso.

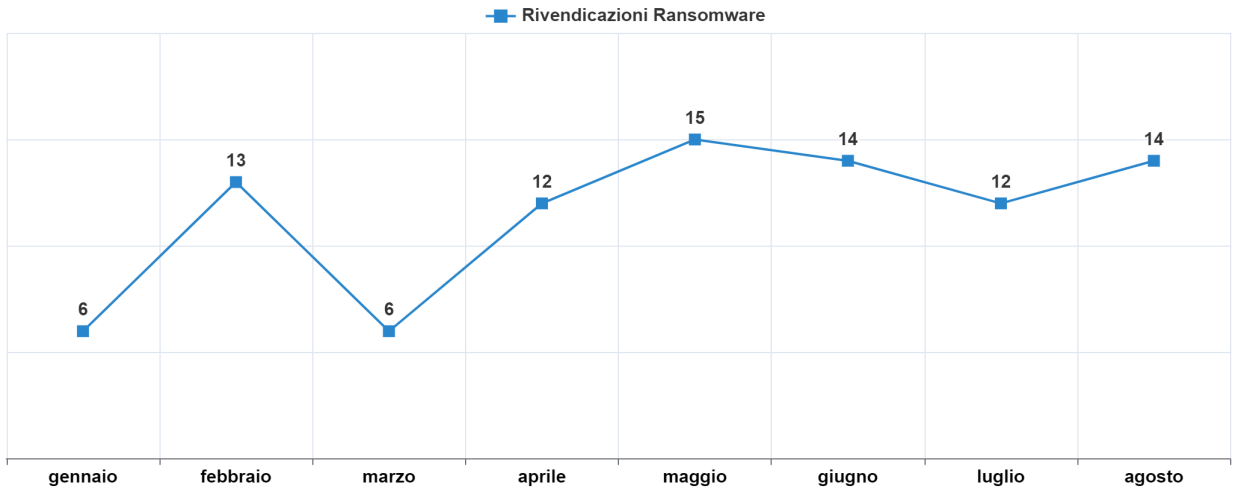

Figura 13: andamento delle rivendicazioni Ransomware

Il grafico in Figura 14 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

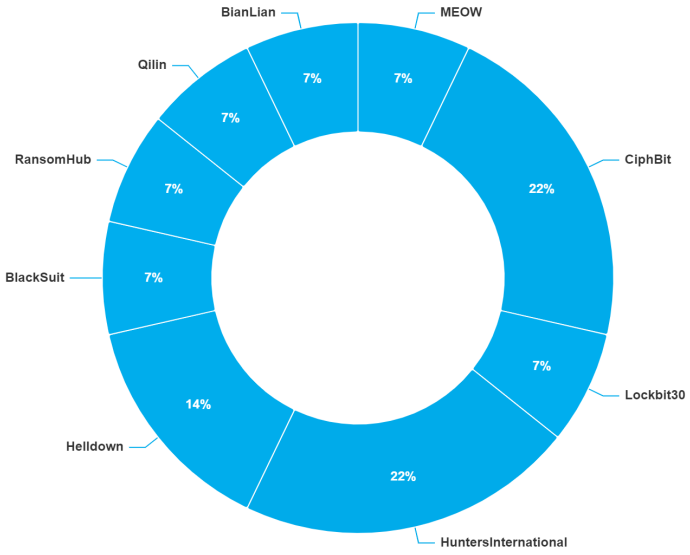

Figura 14: distribuzione percentuale dei gruppi autori delle rivendicazioni

4.3 Rivendicazioni DDoS

Ad agosto 2024 sono state individuate[7] **4** rivendicazioni di attacchi DDoS in danno di soggetti italiani. I gruppi più attivi sono stati **NoName057(16)** e **hack_n3t**. Il grafico in Figura 15 mostra l'andamento delle rivendicazioni DDoS dell'anno in corso.

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

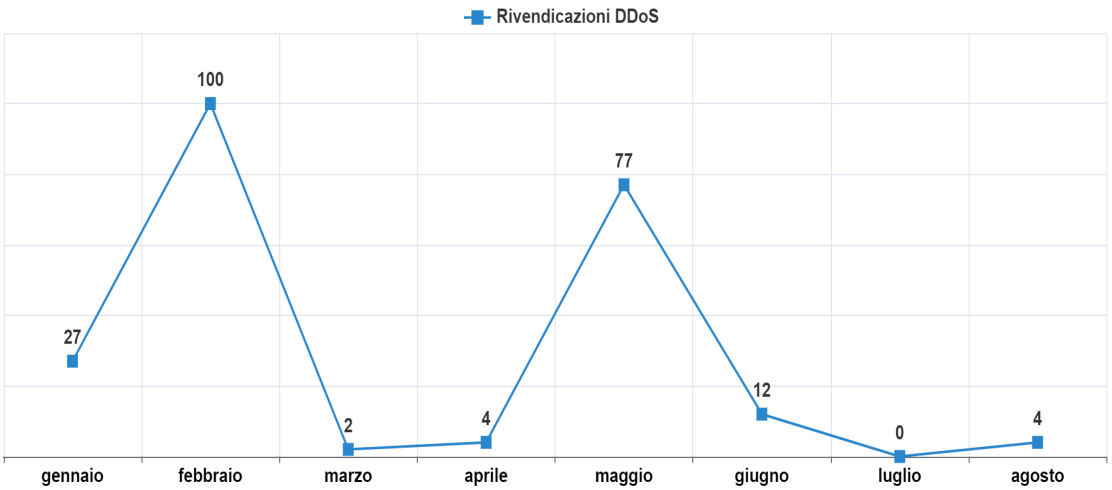

Figura 15: andamento delle rivendicazioni DDoS

Il grafico in Figura 16 mostra i gruppi più attivi in termini di rivendicazioni.

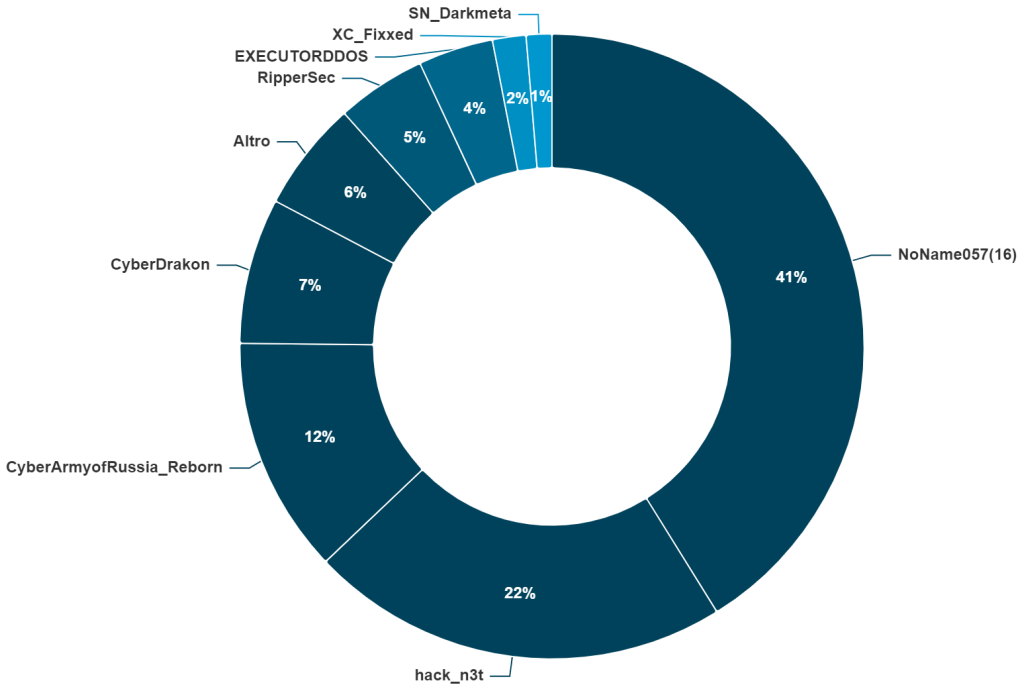

Figura 16: distribuzione percentuale dei gruppi autori delle rivendicazioni

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. Sono oggetto di monitoraggio i servizi e gli asset di soggetti appartenenti al TIER 4 e TIER 3.

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 - DDoS) 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, lo 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 sulla disponibilità, confidenzialità o integrità delle informazioni.

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