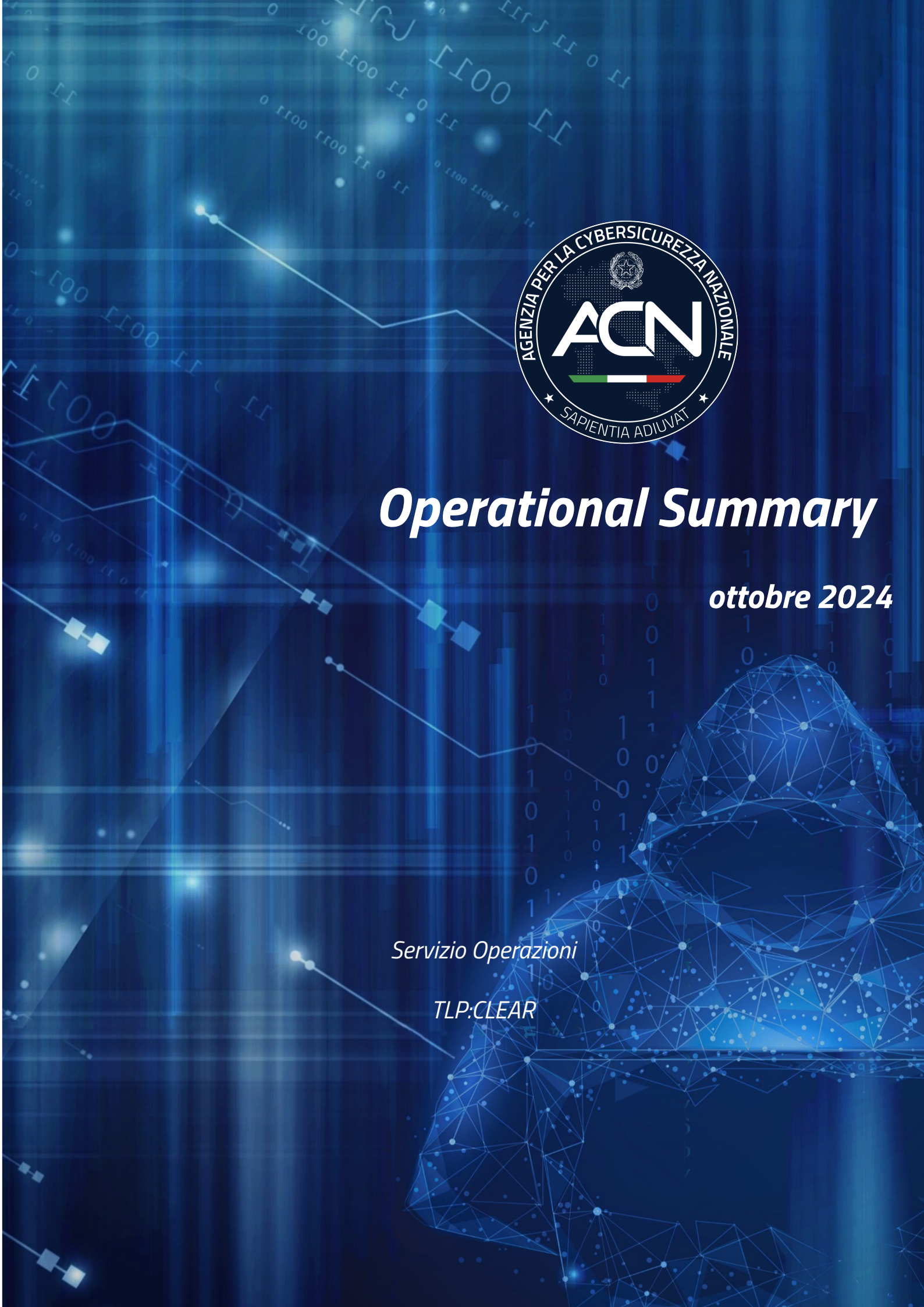

Operational Summary

ottobre 2024

Servizio Operazioni

TLP:CLEAR

Operational Summary

Servizio Operazioni

ottobre 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, Legge 28 giugno 2024, n. 90, Direttiva NIS, Legge 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 ottobre 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

A ottobre 2024 sono stati individuati **150** eventi cyber, in **aumento** del 18% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 147 soggetti nazionali**: 107 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 150 eventi cyber **73 sono stati classificati quali incidenti**, in **aumento** del 128% rispetto a settembre.

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[1], riferita ai successivi 3 mesi.

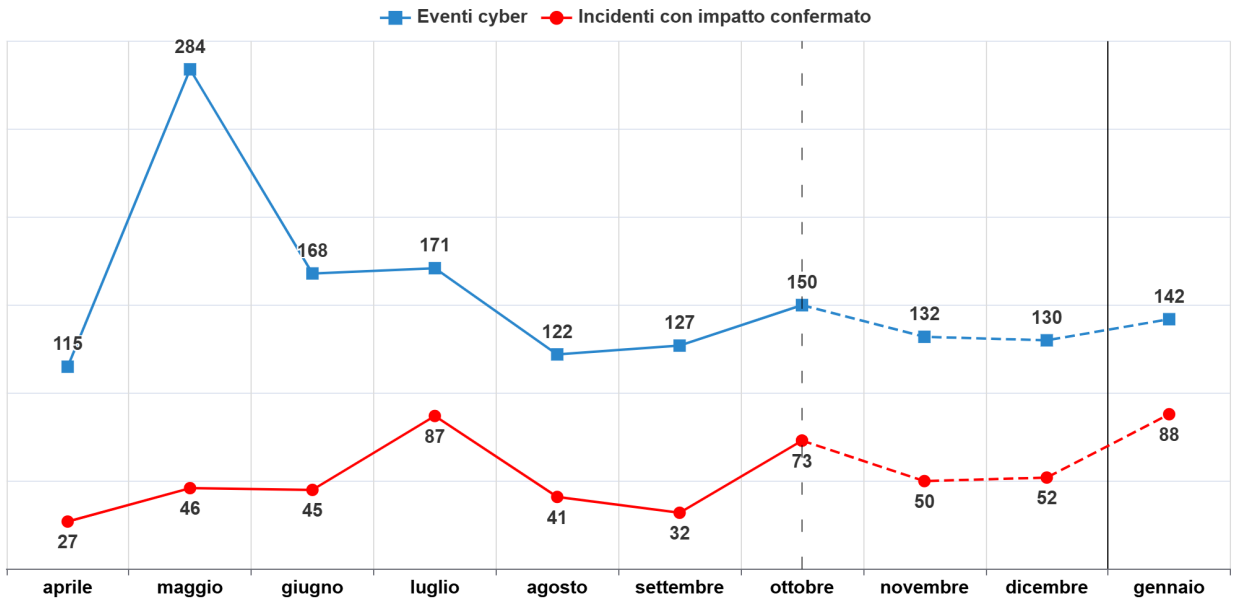

Figura 1: andamento attività reattive e analisi previsionale

[1]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[2]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico).

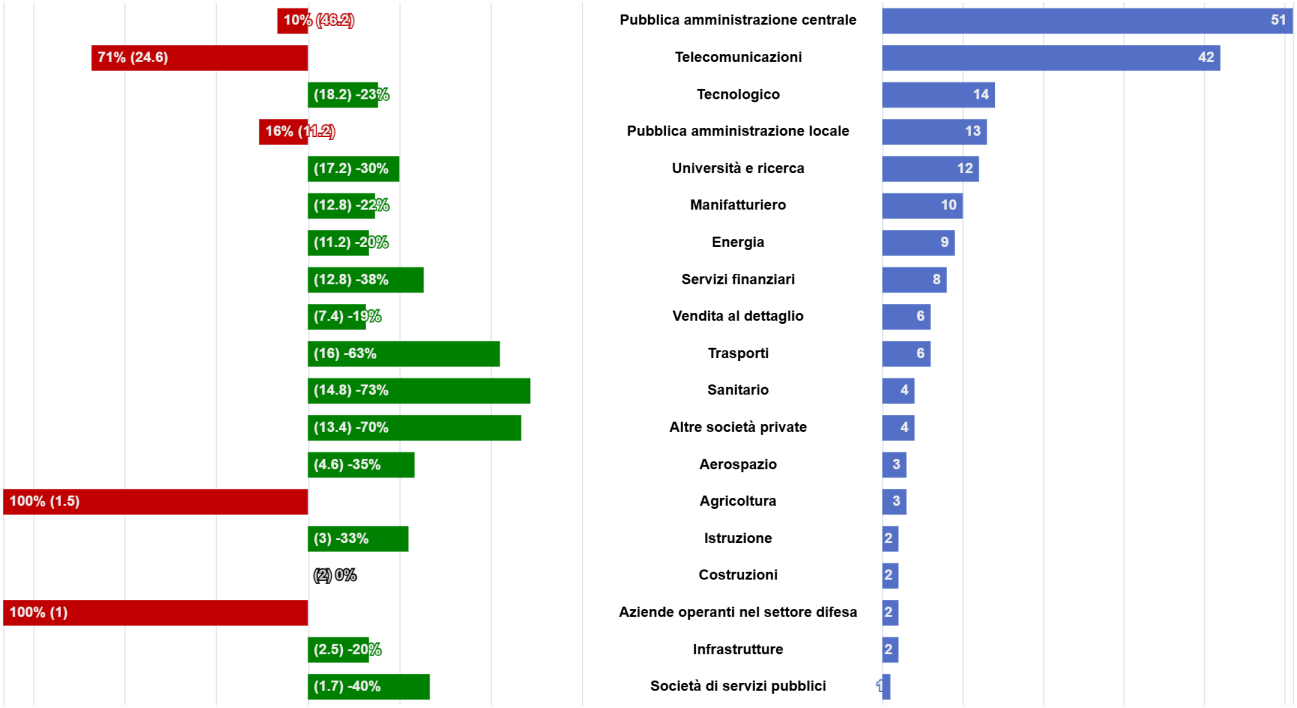

Figura 2: numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente

2.2 Tipologia di minacce negli eventi

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

[2]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.

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

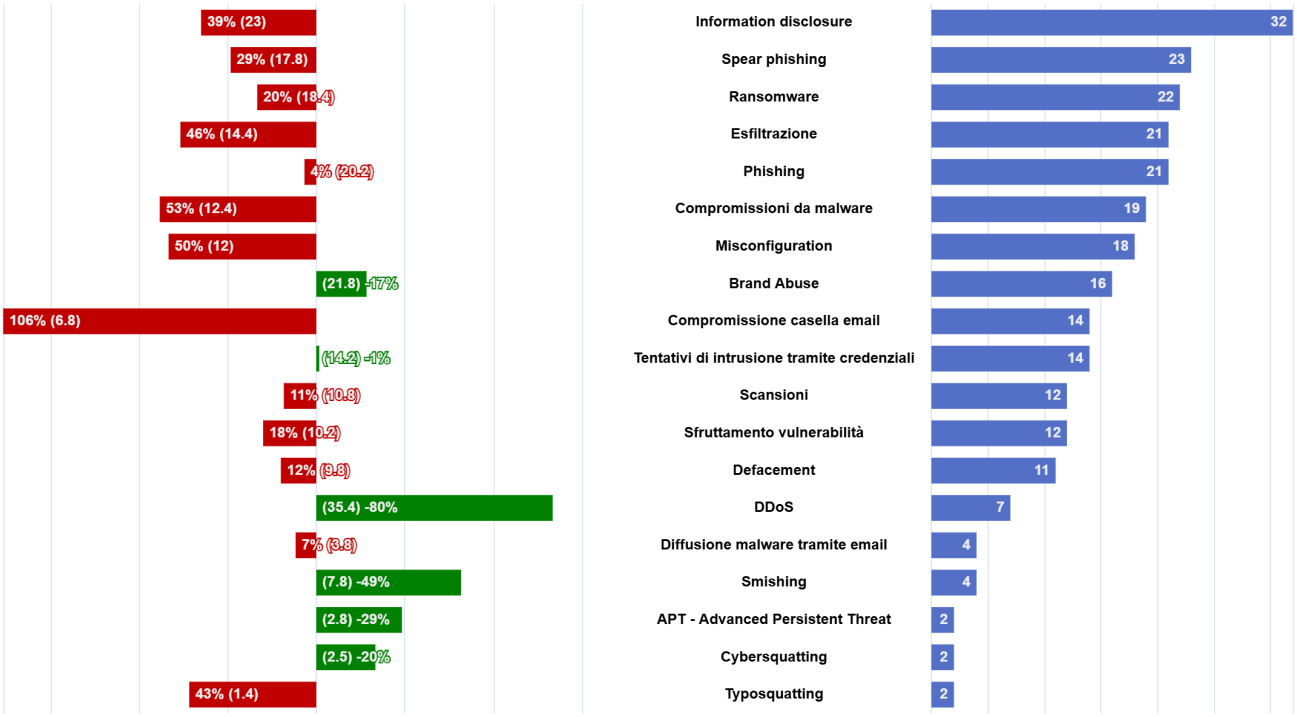

Figura 3: tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente

2.3 Focus constituency

I 150 eventi cyber hanno interessato **107** soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

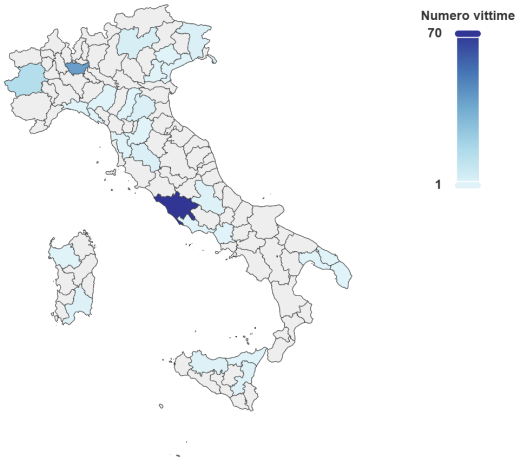

Figura 4: distribuzione geografica delle vittime appartenenti alla constituency

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.

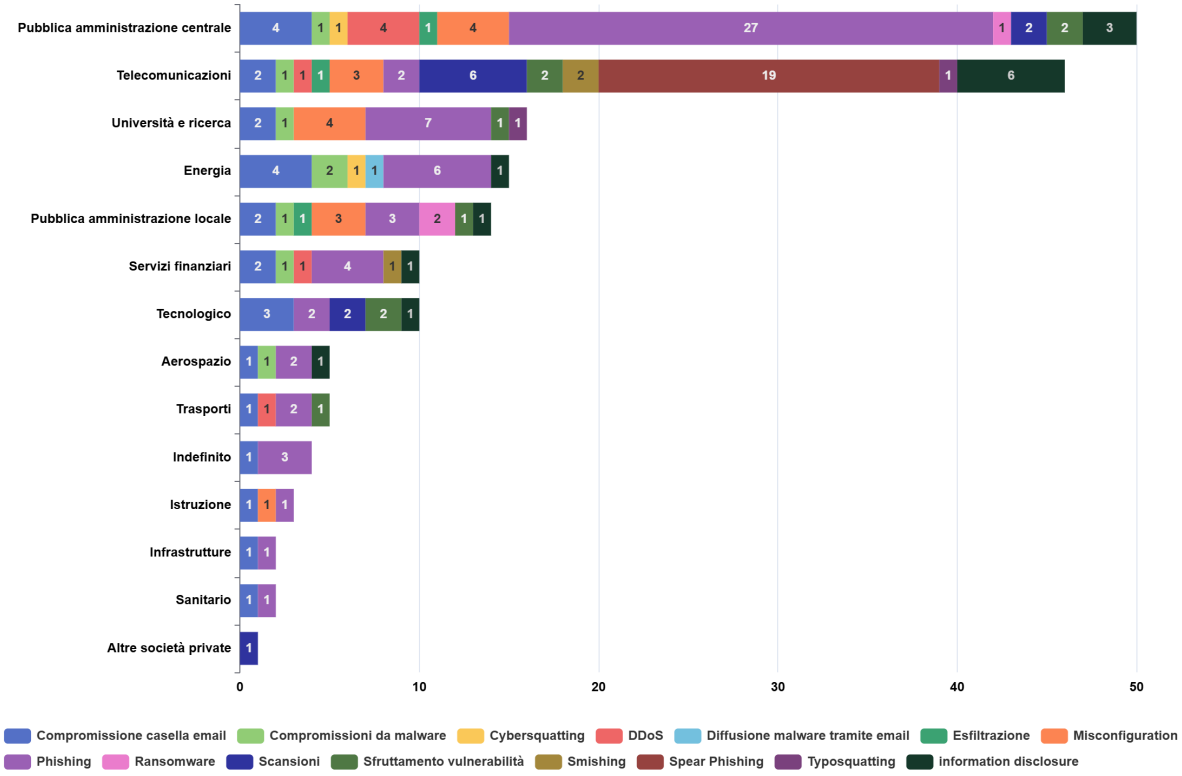

Figura 5: tipologia di minacce con impatto sui settori della constituency

3 VULNERABILITÀ

A ottobre 2024 sono state pubblicate[4] **3.543** nuove CVE, in **aumento** (+**1.005**) rispetto a settembre. Di queste, **338** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (+**24**) e per **14** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (+**6**) rispetto a settembre.

3.1 Distribuzione delle vulnerabilità sui vendor

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

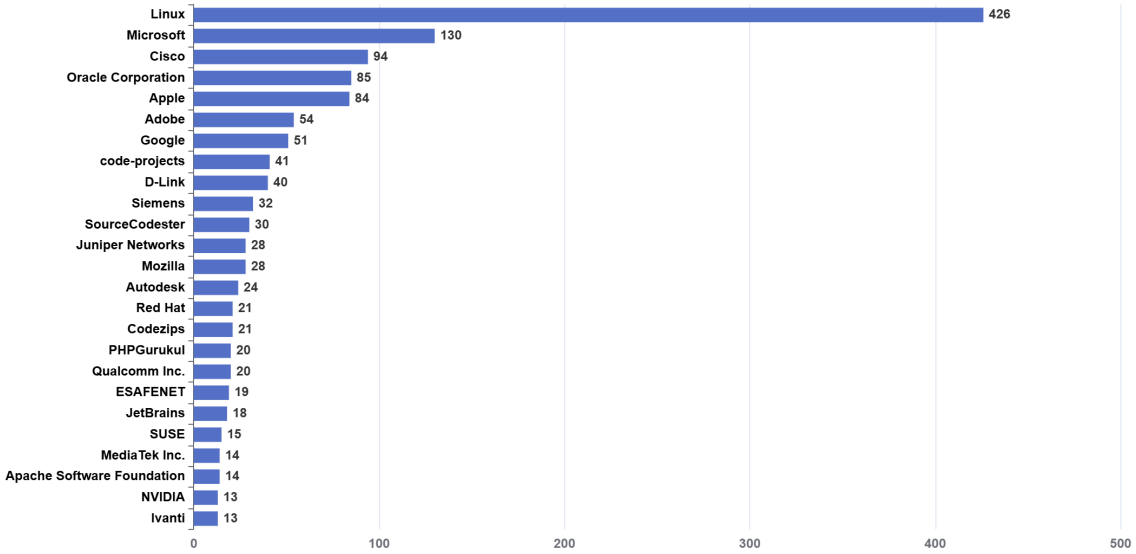

Figura 6: top 25 produttori affetti da vulnerabilità nel mese

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

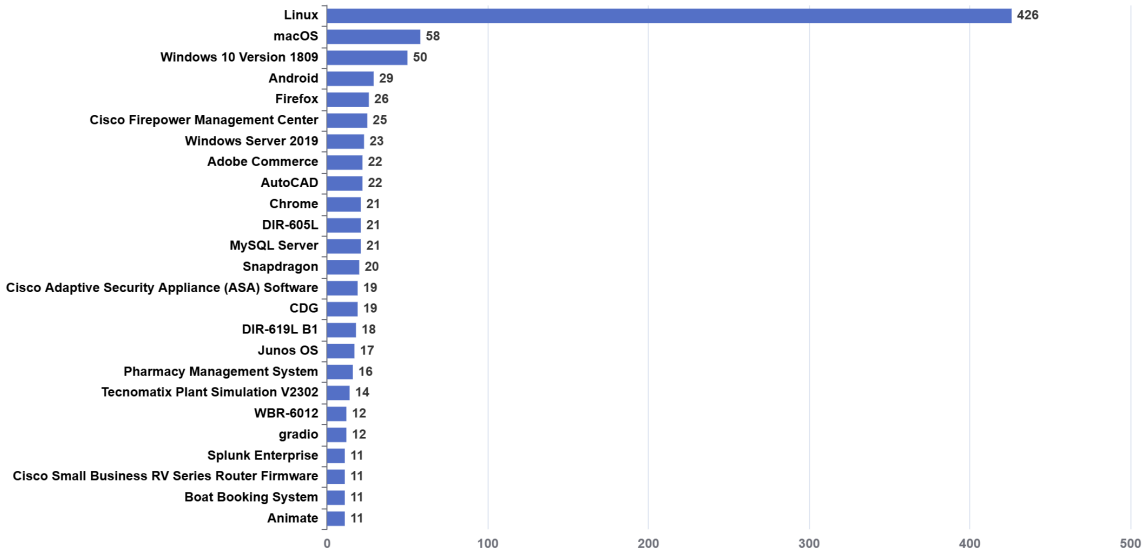

Figura 7: top 25 prodotti affetti da vulnerabilità nel mese

[4]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.

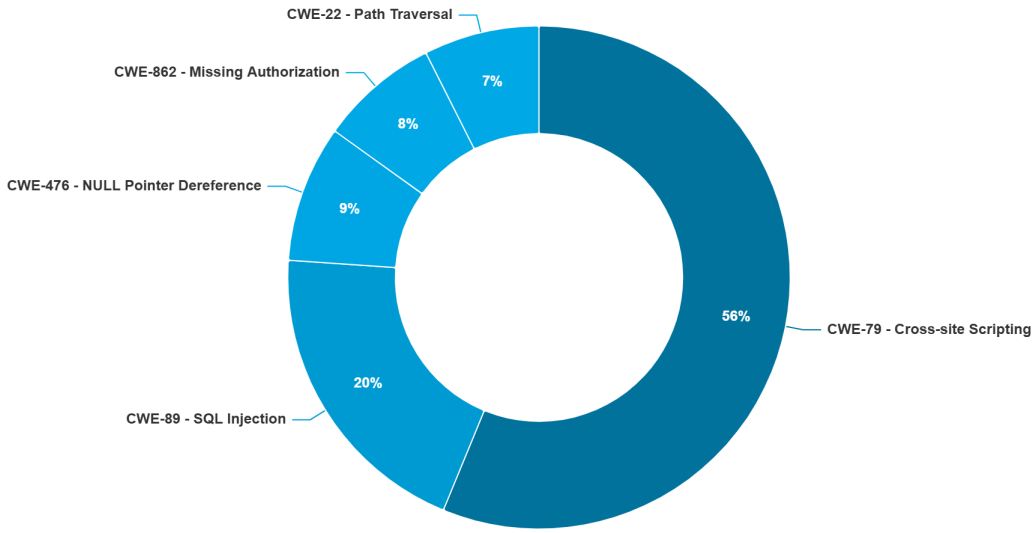

Figura 8: top 5 CWE nel mese

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)[5] fornito dal FIRST nel mese in esame.

Tabella 1: CVE-2024-40711

Vendor	Veeam
Prodotti e versioni vulnerabili	Veeam backup & replication versioni dalla 12.0.0.1420 alla 12.1.2.172
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette ad un attaccante eseguire codice malevolo
Data di rilascio CVE	07/09/2024 modificata il 18/10/2024
CVSS score 3.x	9.8 CRITICAL
EPSS max score	0.967

[5] `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-2024-45519

Vendor	Zimbra
Prodotti e versioni vulnerabili	Collaboration versioni prima della 8.8.15 Patch 46, della 9.0.0 Patch 41, della 10.0.9 e della 10.1.1
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire comandi sul server
Data di rilascio CVE	02/10/2024 modificata il 23/10/2024
CVSS score 3.x	9.8 CRITICAL
EPSS max score	0.95

Tabella 3: CVE-2023-45249

Vendor	Acronis
Prodotti e versioni vulnerabili	Acronis Cyber Infrastructure (ACI) version prima della build 5.0.1-61, della build 5.1.1-71, della build 5.2.1-69, della build 5.3.1-53 e della build 5.4.4-132
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità è possibile a causa dell'utilizzo di password di default e permette ad un attaccante eseguire codice malevolo sul server
Data di rilascio CVE	24/07/2024 modificata il 30/07/2024
CVSS score 3.x	9.8 CRITICAL
EPSS max score	0.88

3.4 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **55**. Oltre al consueto aggiornamento mensile di Microsoft (link all'alert sul sito web), che ha risolto un totale di 120 nuove vulnerabilità (5 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Palo Alto Networks**: rilasciati aggiornamenti di sicurezza per risolvere molteplici vulnerabilità. In particolare, per 5 di tali vulnerabilità – che interessano la soluzione Network Expedition - risulterebbe disponibile un Proof of Concept (PoC) che potrebbe permettere lo sfruttamento concatenato delle stesse al fine di prendere il controllo degli account di amministrazione dei prodotti firewall (stima di impatto sistemico **79,35/100**). Link all'alert del 10/10/2024;
- **Fortinet**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-47575 – già sanata dal vendor – che interessa i prodotti FortiManager e FortiAnalyzer. Tale vulnerabilità può consentire a un utente malintenzionato remoto non autenticato l'esecuzione di codice arbitrario (stima di impatto sistemico **79,23/100**). Link all'alert del 24/10/2024;
- **Mozilla**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-9680 – già sanata dal vendor – che interessa i noti prodotti: Firefox e Thunderbird. Tale vulnerabilità, di tipo "Use-After-Free", che interessa la componente timeline delle animazioni di tali prodotti (stima di impatto sistemico **79,23/100**). Link all'alert del 10/10/2024;
- **Samsung**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-44068 – già sanata dal vendor – che interessa i processori Exynos, una serie di "system-on-a-chip (SoC)" prodotti e sviluppati da Samsung, in uso in dispositivi mobili (stima di impatto sistemico **77,05/100**). Link all'alert del 25/10/2024;
- **Ivanti**: rilasciati aggiornamenti di sicurezza che risolvono 11 vulnerabilità, di cui una con gravità "critica" e 9 con gravità "alta", nei prodotti EPMM (Core), CSA (Cloud Services Appliance), Velocity License Server, Avalanche, Connect Secure e Policy Secure (stima di impatto sistemico **75,89/100**). Link all'alert del 08/10/2024.

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

3.5 Comunicazioni dirette

Sono state diramate un totale di **338** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **715** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

Zimbra (CVE-2024-45519): tale vulnerabilità, relativa al servizio postjournal, potrebbe consentire ad un attaccante non autenticato di eseguire da remoto comandi sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
CUPS (CVE-2024-47176): tale vulnerabilità - laddove combinata con altre vulnerabilità come la CVE-2024-47076, CVE-2024-47175 o CVE-2024-47177 - permetterebbe a un eventuale attaccante non autenticato di eseguire da remoto codice arbitrario sulle macchine affette in determinate condizioni. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
Ivanti (CVE-2024-9381, CVE-2024-9380, CVE-2024-9379): queste vulnerabilità permetterebbero ad un utente malintenzionato autenticato con privilegi di amministratore di eseguire: istruzioni SQL e codice arbitrario bypassando i meccanismi di sicurezza. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;

Fortinet FortiManager (CVE-2024-47575): tale vulnerabilità - di tipo Missing Authentication for Critical Function - permetterebbe a eventuali attaccanti di eseguire codice e comandi arbitrari sui sistemi affetti attraverso l'invio di richieste appositamente predisposte. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
CyberPanel (CVE-2024-51567, CVE-2024-51568 e CVE-2024-51378): tali vulnerabilità permetterebbero ad un eventuale attaccante remoto di eseguire codice e comandi arbitrari bypassando i meccanismi di autenticazione in essere sui dispositivi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
SolarWinds Serv-U (CVE-2024-45711): tale vulnerabilità, di tipo Path Traversal, permetterebbe a un attaccante autenticato di eseguire codice arbitrario tramite l'abuso di variabili d'ambiente, indipendentemente dai privilegi forniti a quel determinato utente. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia;
Fortinet FortiOS (CVE-2024-23113): tale vulnerabilità permetterebbe a un eventuale attaccante non autenticato di eseguire da remoto codice o comandi non autorizzati tramite l'invio di richieste specificamente predisposte. 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 ottobre 2024.

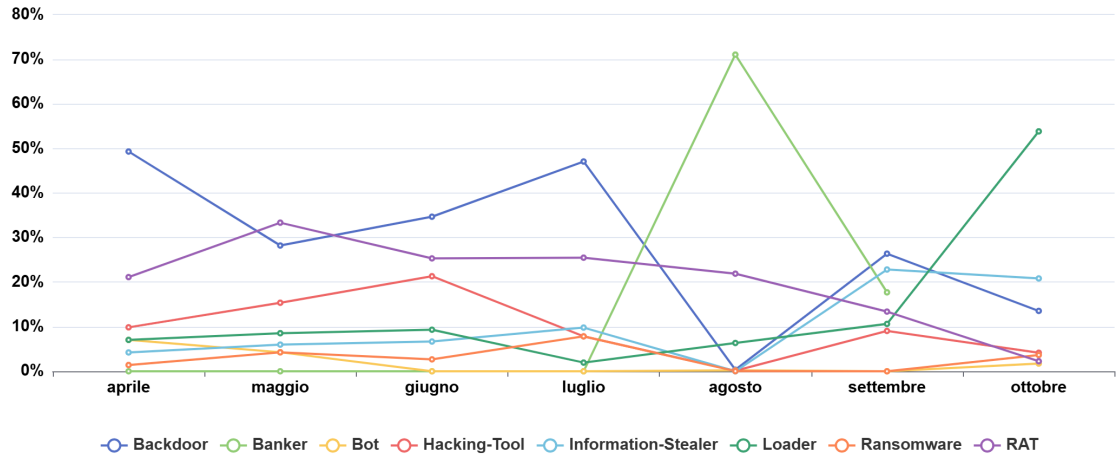

Figura 9: andamento semestrale della diffusione della tipologia di malware in Italia

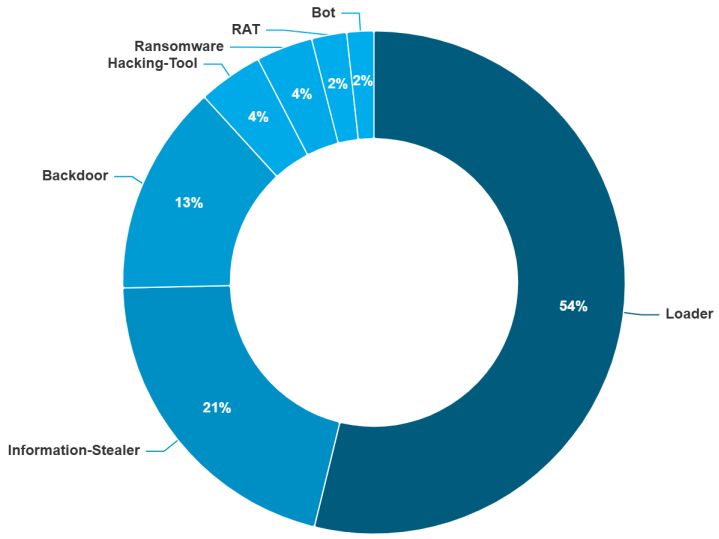

Figura 10: tipologie malware più diffuse in Italia nel mese di ottobre 2024

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

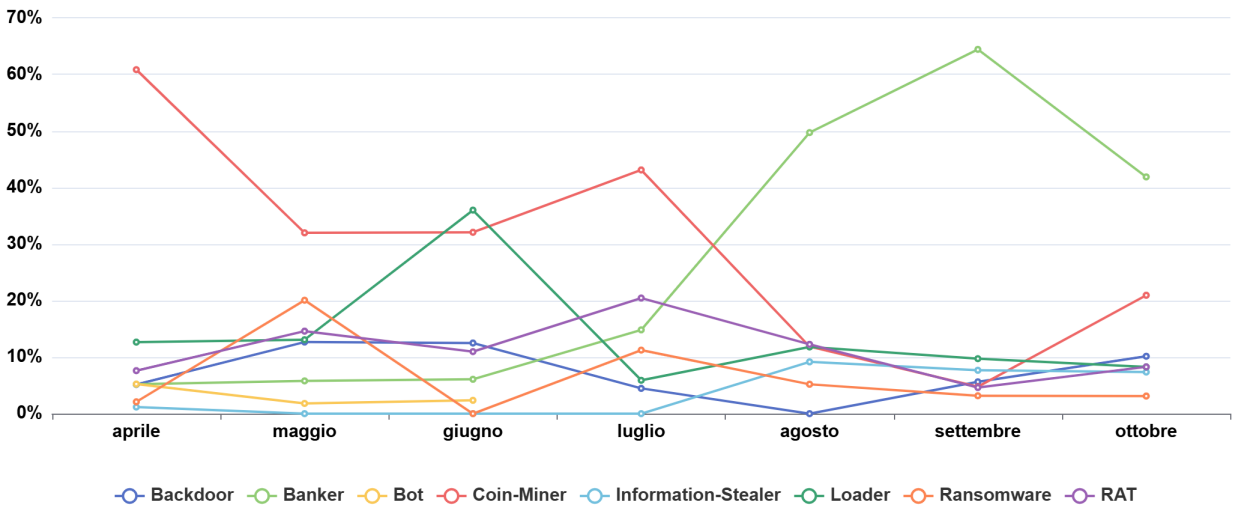

Figura 11: andamento semestrale della diffusione della tipologia di malware in UE

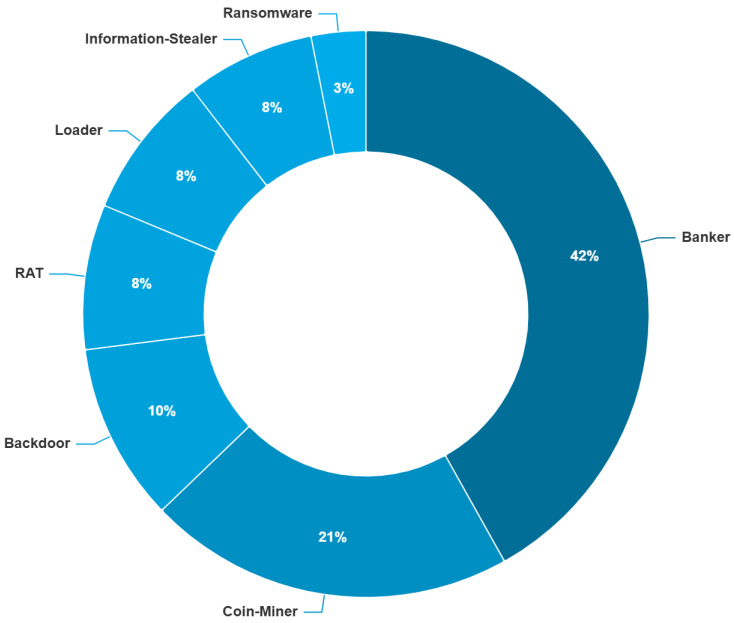

Figura 12: tipologie di malware più diffuse in Europa nel mese

4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel mese di ottobre 2024 ha permesso di individuare **12** rivendicazioni di attacchi Ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **Sarcoma Group** e **Interlock**. Il grafico in Figura 13 mostra l'andamento delle rivendicazioni nell'anno in corso.

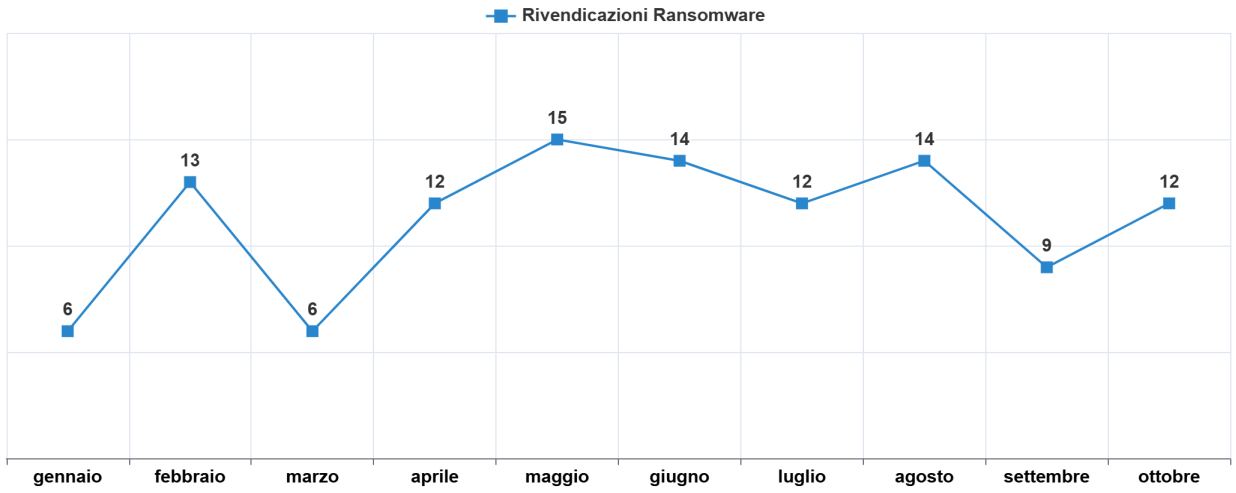

Figura 13: andamento delle rivendicazioni Ransomware

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

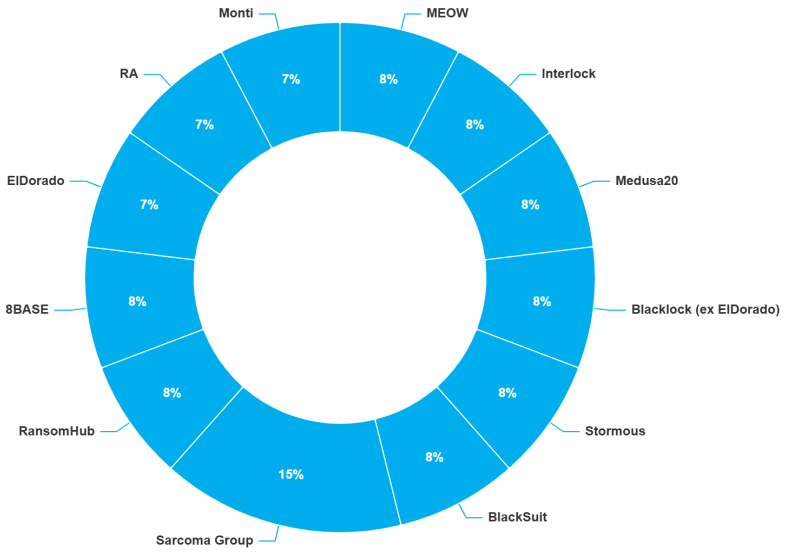

Figura 14: distribuzione percentuale dei gruppi autori delle rivendicazioni

4.3 Rivendicazioni DDoS

A ottobre 2024 non sono state individuate[6] rivendicazioni di attacchi DDoS in danno di soggetti italiani. I gruppi più attivi su scala globale sono stati **NoName057(16)** e **CyberArmyofRussia_Reborn**. Il grafico in Figura 15 mostra l'andamento delle rivendicazioni DDoS dell'anno in corso.

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

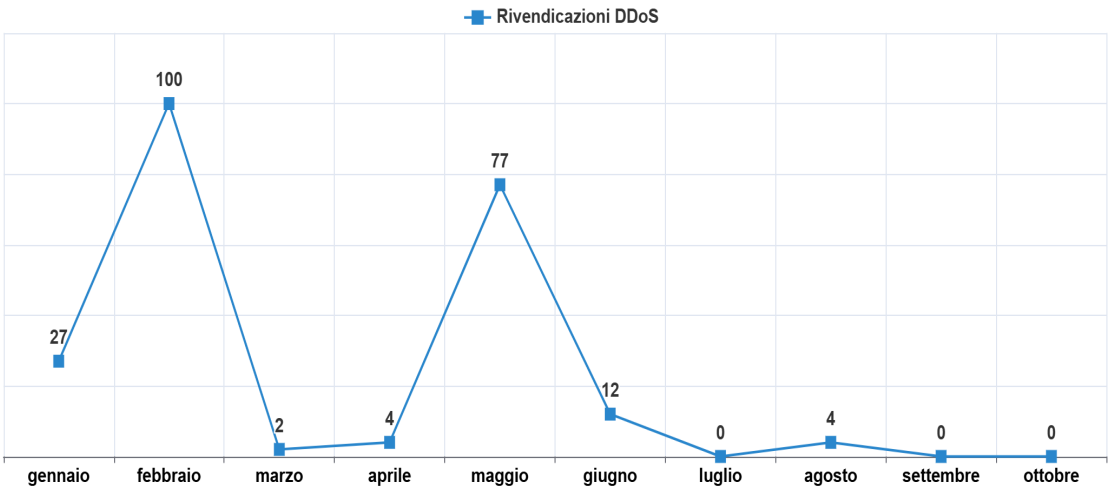

Figura 15: andamento delle rivendicazioni DDoS

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

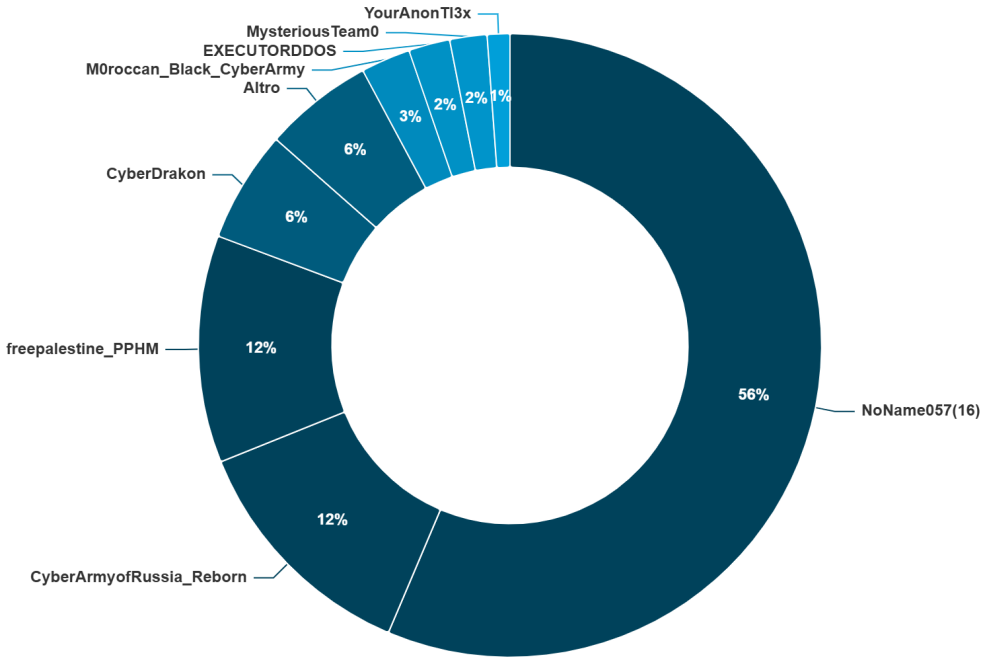

Figura 16: distribuzione percentuale dei gruppi autori delle rivendicazioni

5 GLOSSARIO

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.

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.

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.

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.