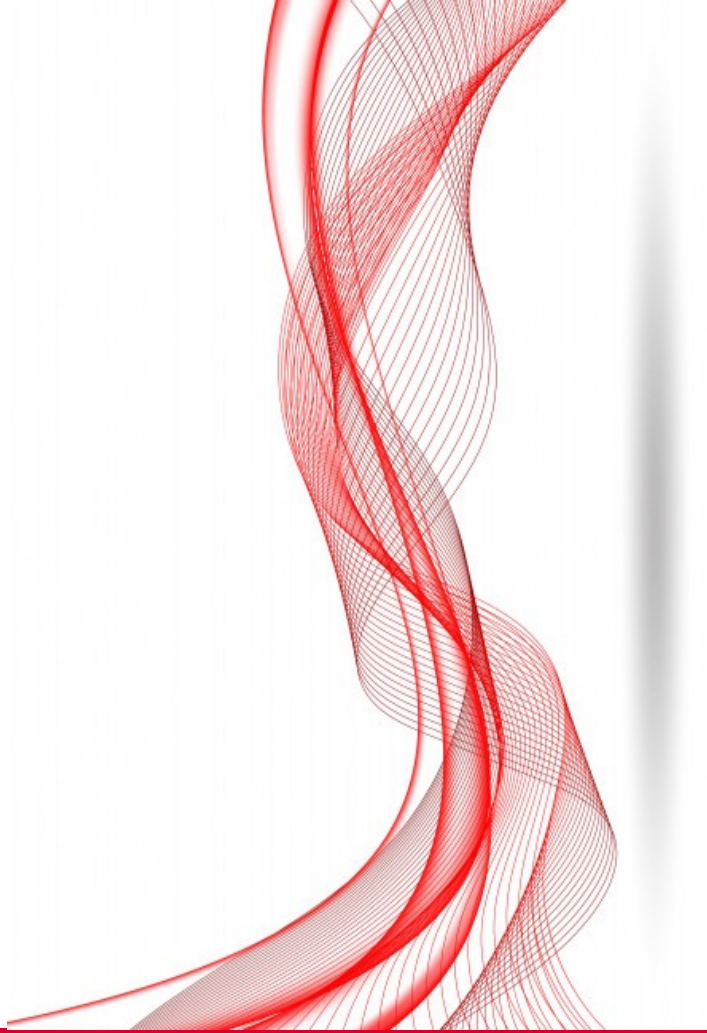
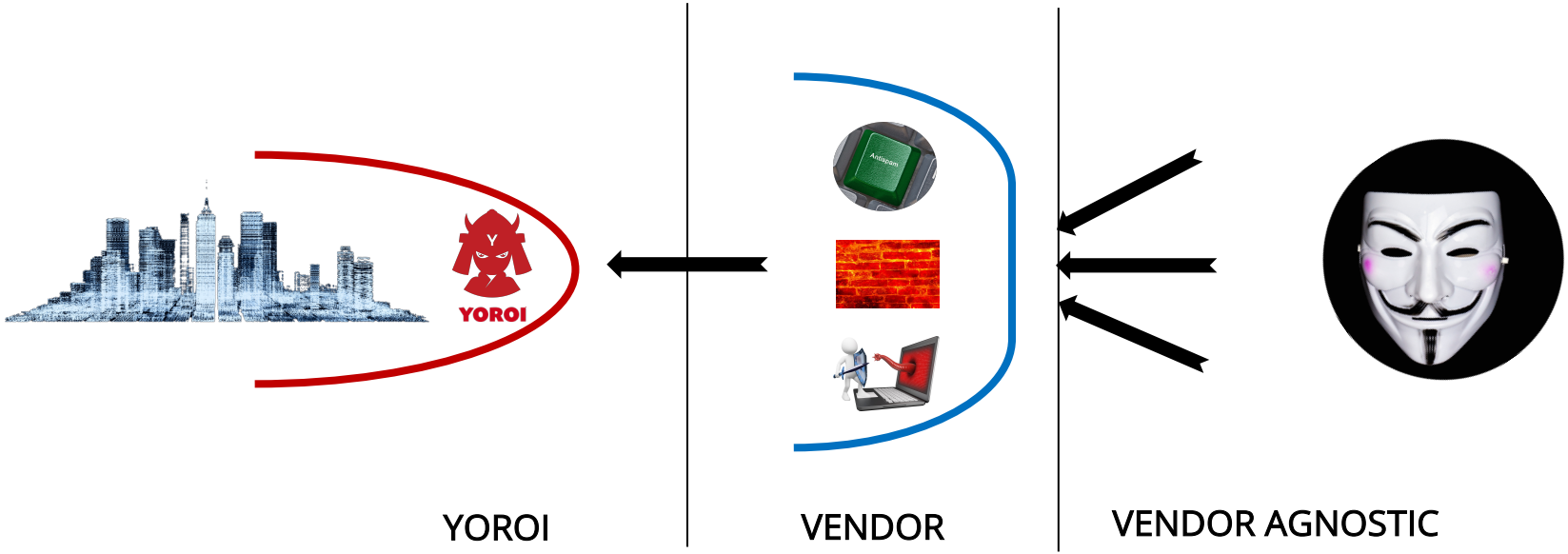
Cybersecurity Annual Report 2022

Roma, 9 Marzo 2022

I dati YOROI

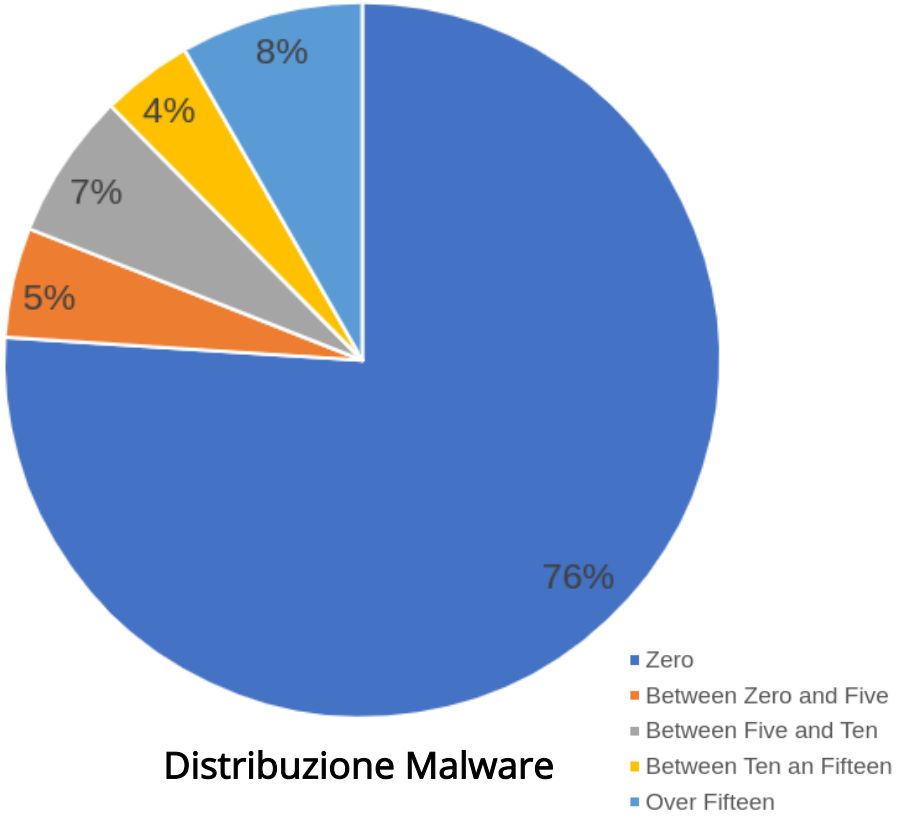


Il valore dei dati sta DOVE vengono rilevati.
I dati utilizzati non appartengono solo all'open source intelligence (OSINT) o alle rilevazioni di reti esterne, ma piuttosto a incidenti reali che sono stati gestiti da analisti umani, che Yoroi raccoglie OLTRE tutti i confini perimetrali davanti ai quali gli altri report si fermano.

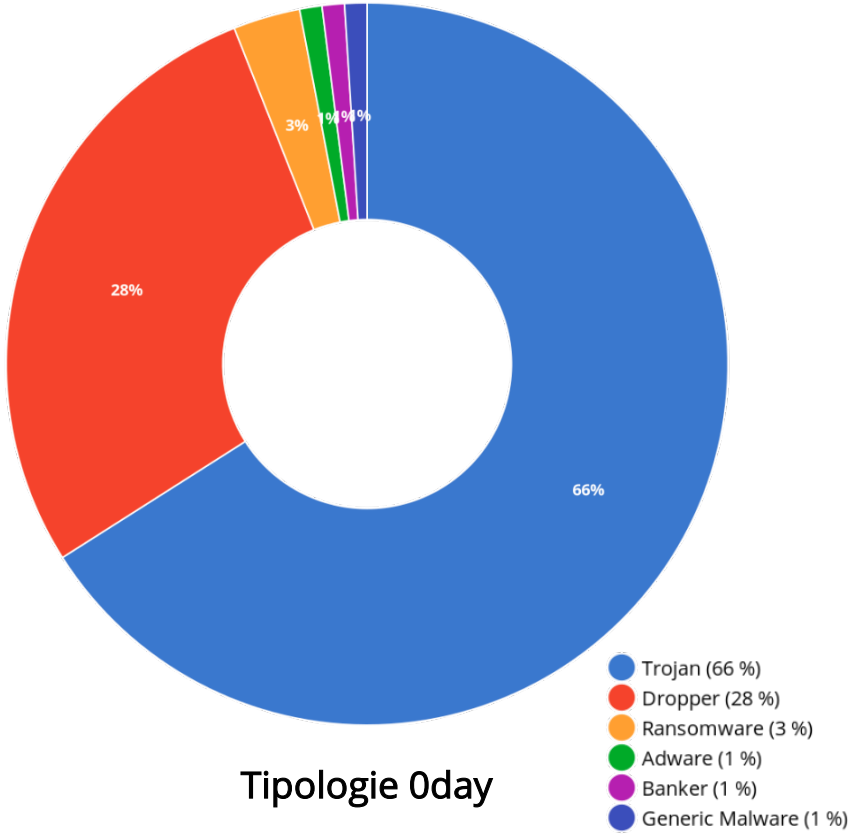


MALWARE
Malicious Unwanted Software

Malware 0day

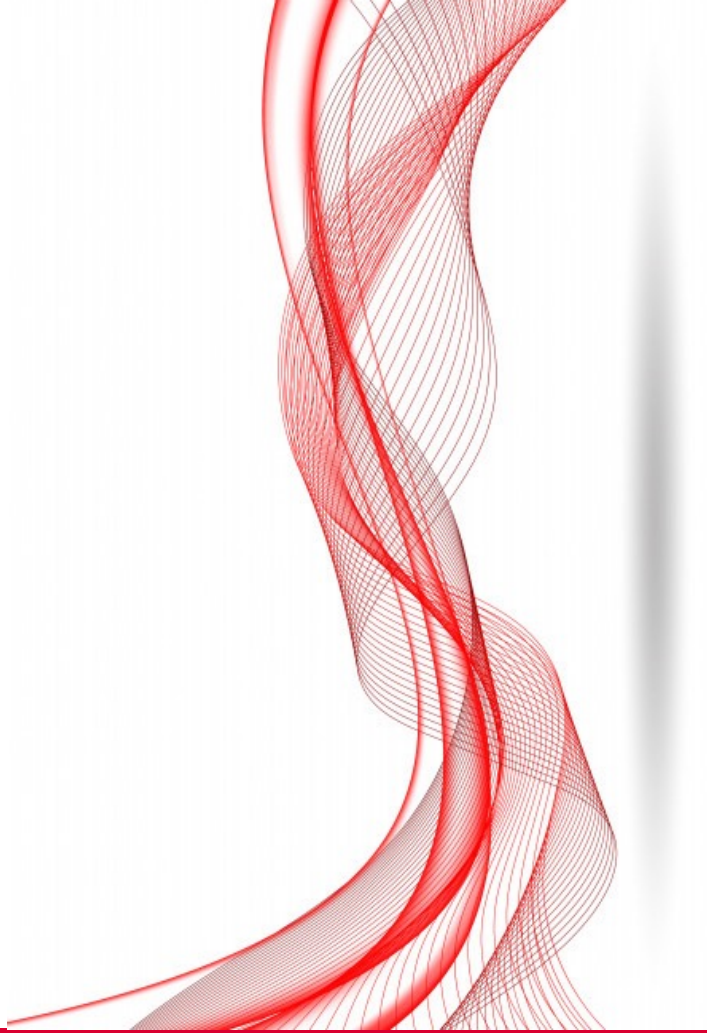


Distribuzione Malware

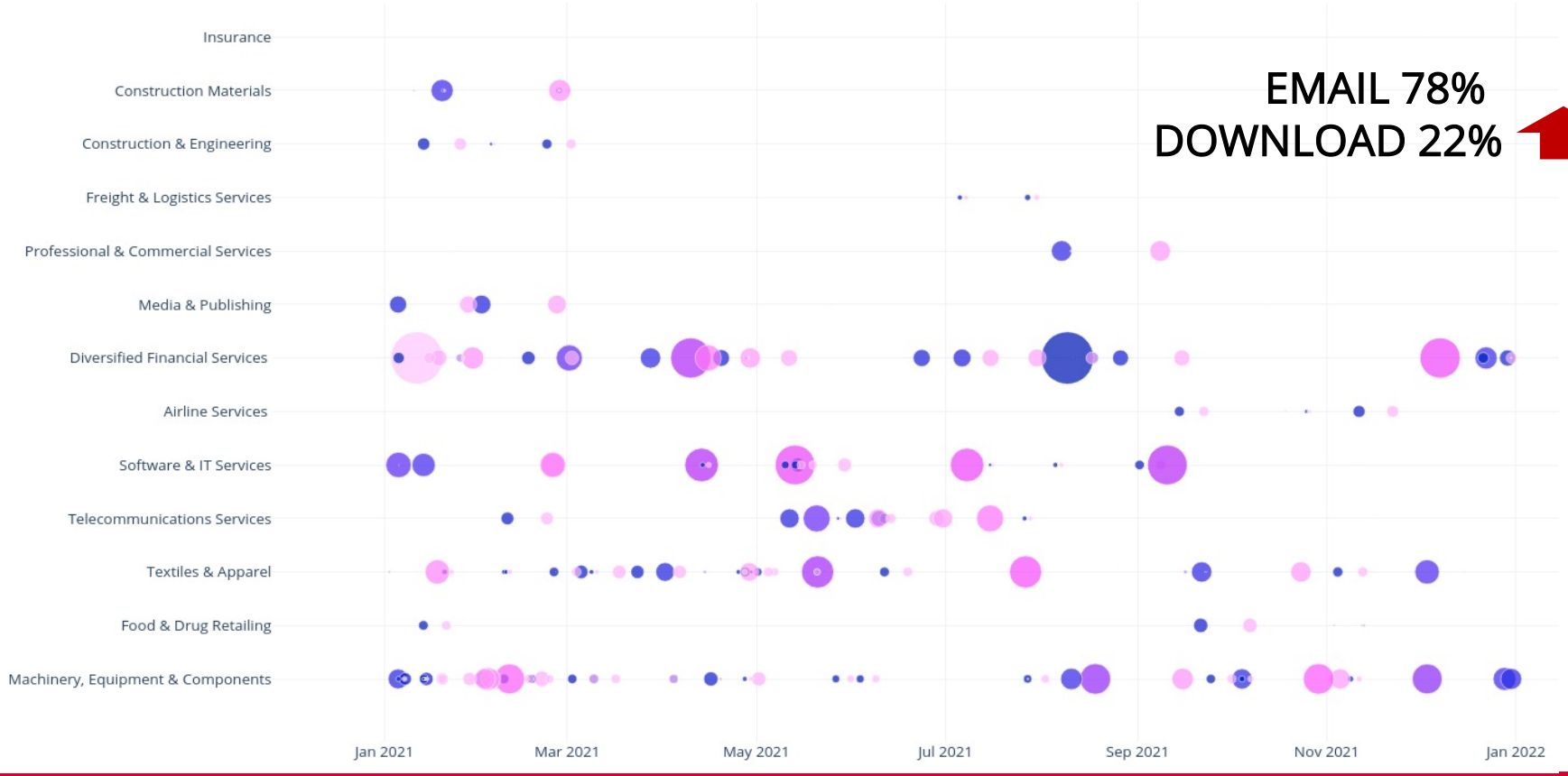


Tipologie 0day

Principali settori colpiti

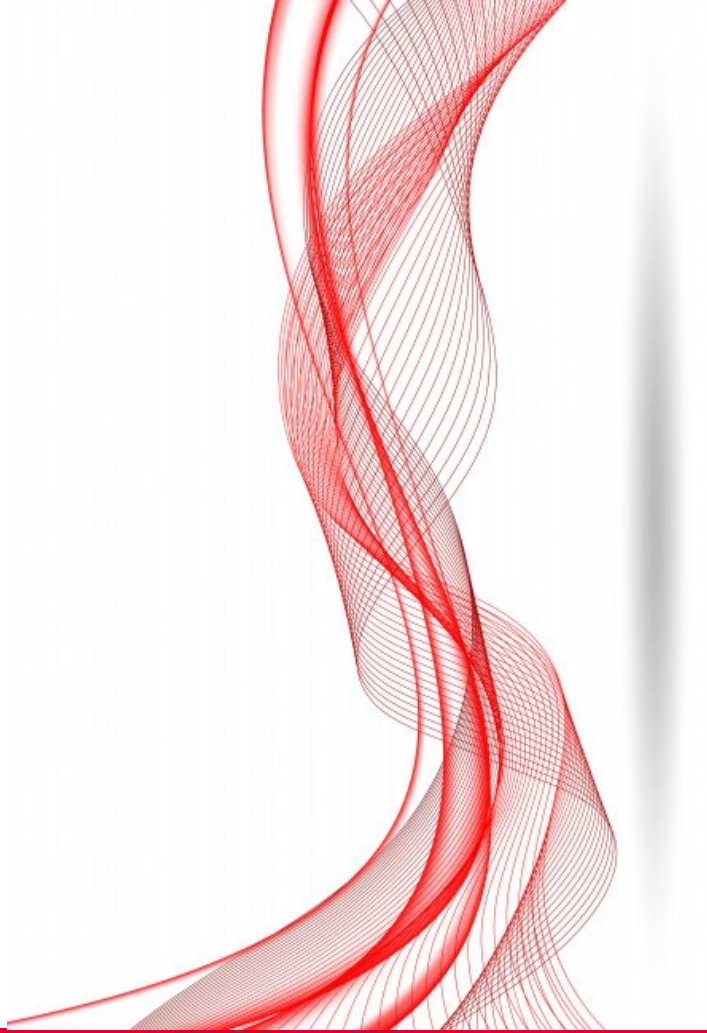


Distribuzione degli attacchi su verticali di settore



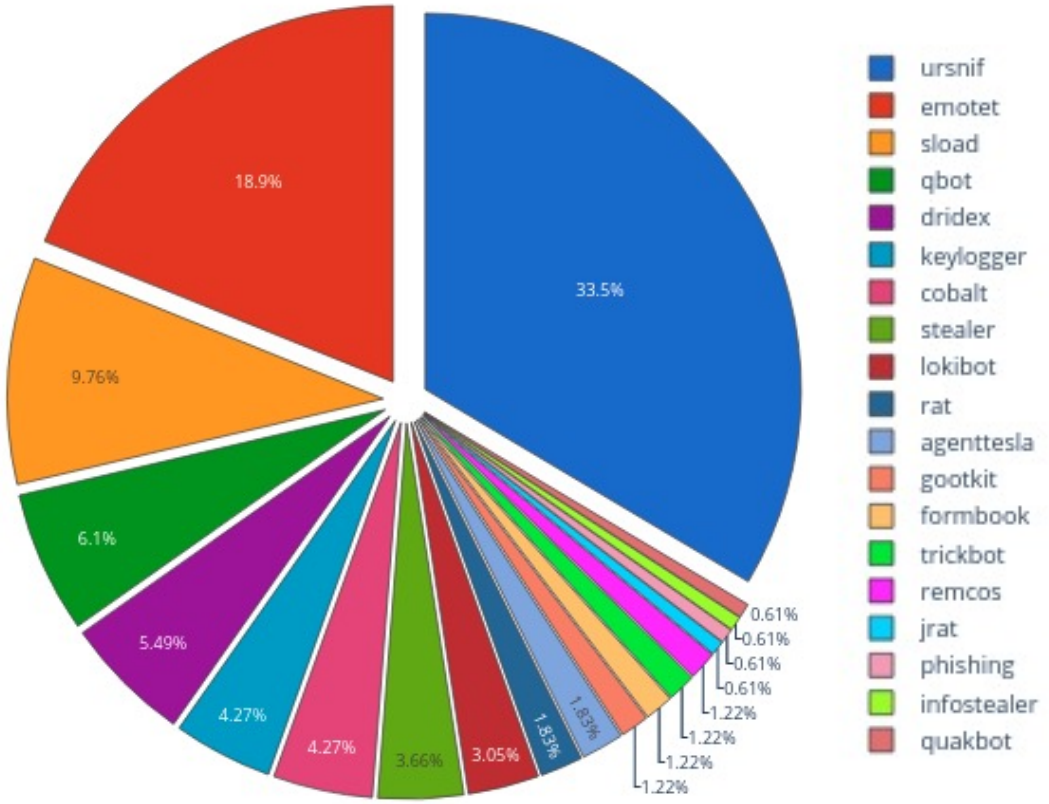
EMAIL 78%
DOWNLOAD 22%

Il contesto italiano



Distribuzione degli attacchi su verticali di settore

- Anche quest'anno la maggioranza di Malware presenti nelle organizzazioni sono Trojan Bancari
- Ursnif si conferma come primaria minaccia all'interno del panorama cibernetico italiano. Campagne di phishing che vengono attivate da social engineering per poi proseguire su fogli di calcolo per utilizzare payload sviluppati in PowerShell e macro XML
- Emotet, seconda minaccia classificata, segue un pattern discreto, con tempi di stop più o meno lunghi, prima di ripartire con costanza

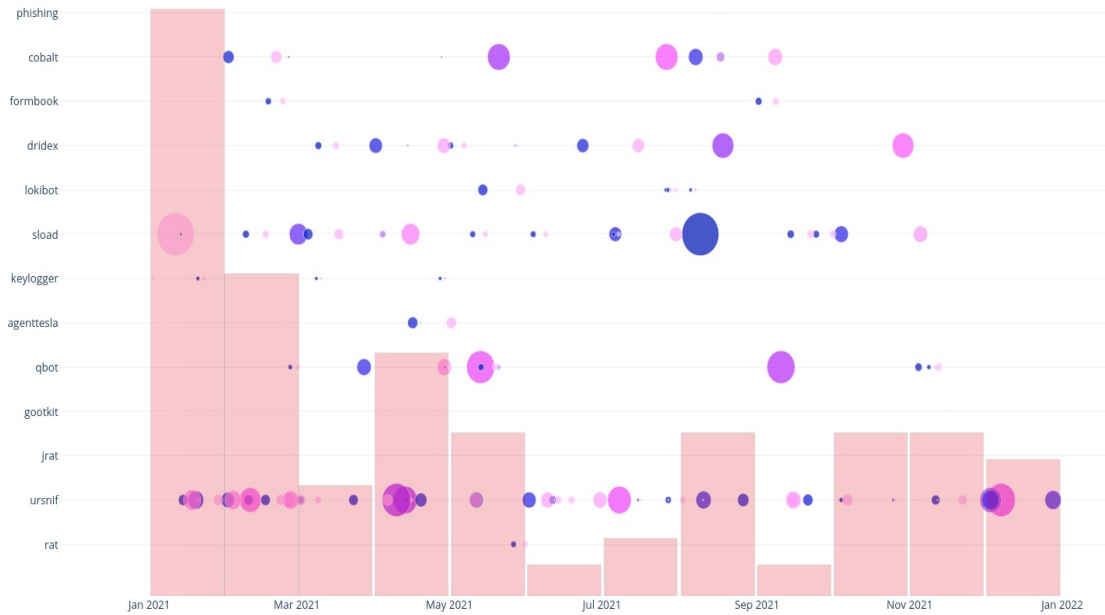


Campagne malware in Italia

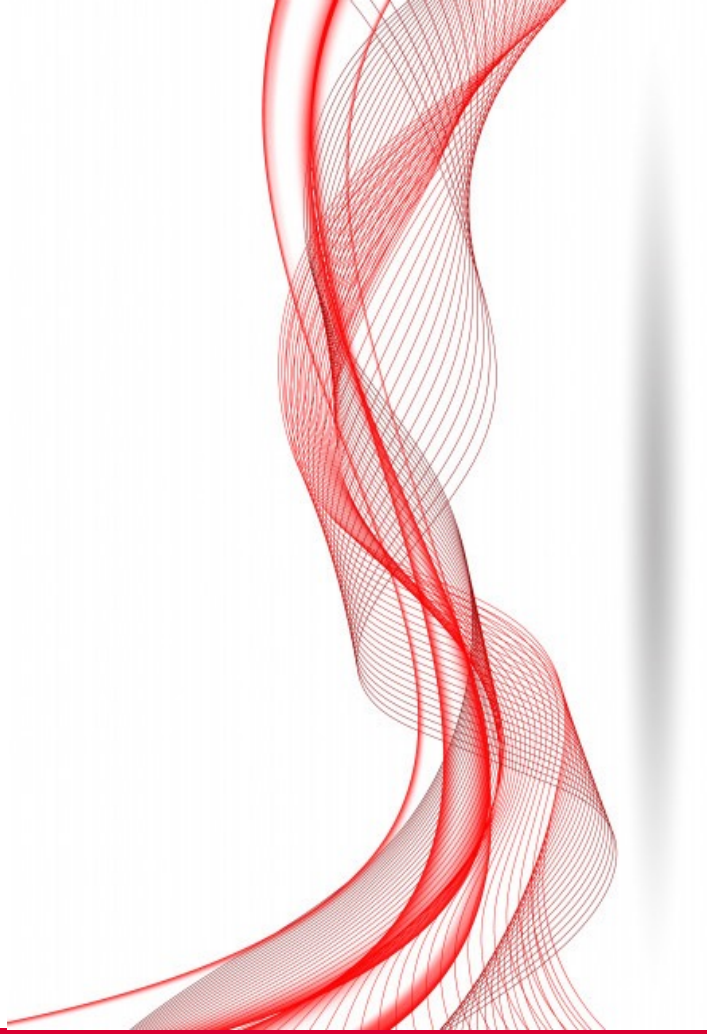
- sLoad è una dei pochi malware che sfrutta le comunicazioni PEC per infettare le postazioni di lavoro sensibili: questo è un ottimo mezzo per sfruttare la social engineering

- Una nuova posizione di rilievo è quella di QBot. Crea una botnet che può scaricare anche backdoor molto usate come Trickbot e CobaltStrike.

- Trickbot e Cobalstrike sono ad oggi gli strumenti numero uno di criminali informatici per le operazioni di Red Team e di intrusione più sofisticata

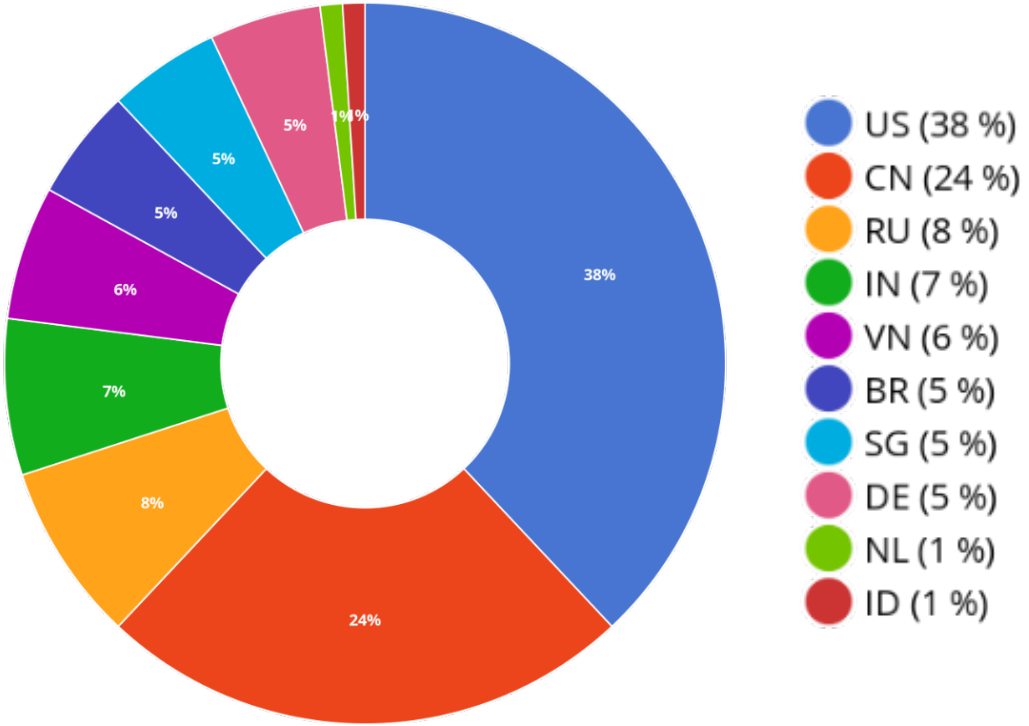


Botnet
e attacchi opportunistici

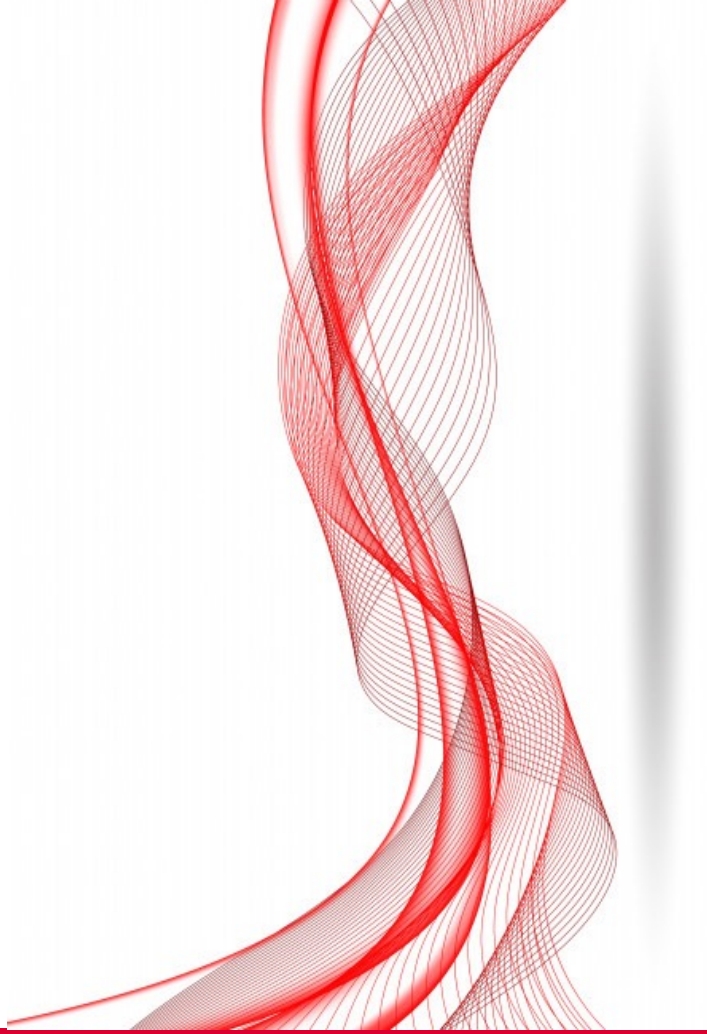


Distribuzione geografica degli attacchi

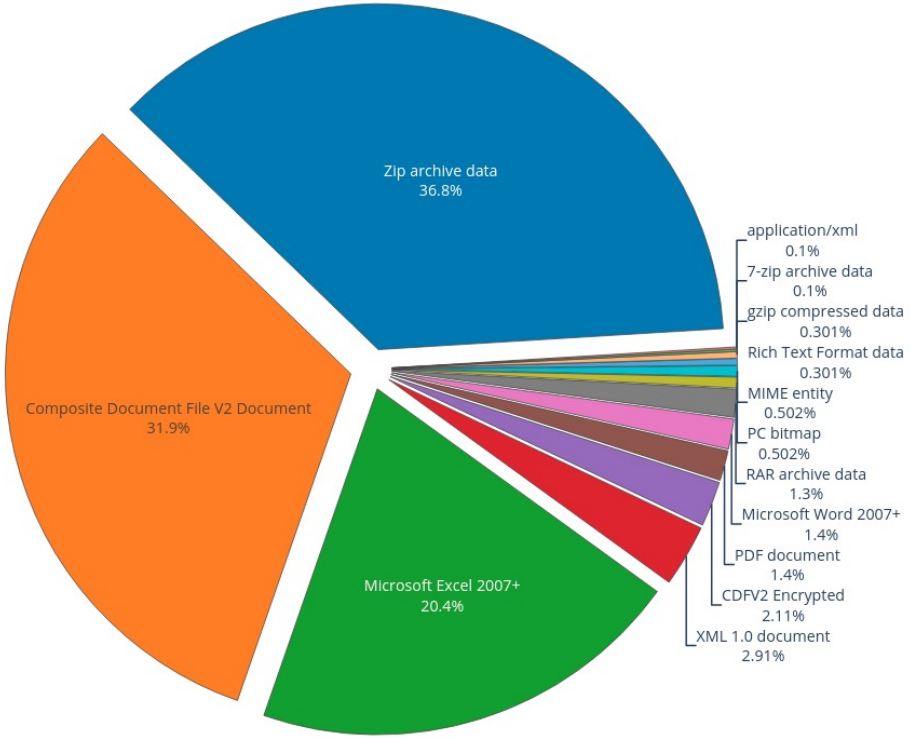
- Yoroi raccoglie la sfida di proteggere i propri clienti mediante la reputazione degli indirizzi e delle sorgenti da cui potrebbero provenire degli attacchi.
- La Top 3 delle infrastrutture malevole prevedono strumenti appositi per l'offuscamento dell'IP
- Diventa importante una strategia di reputazione IP geofenced, che deve considerare i paesi con cui esistono relazioni commerciali

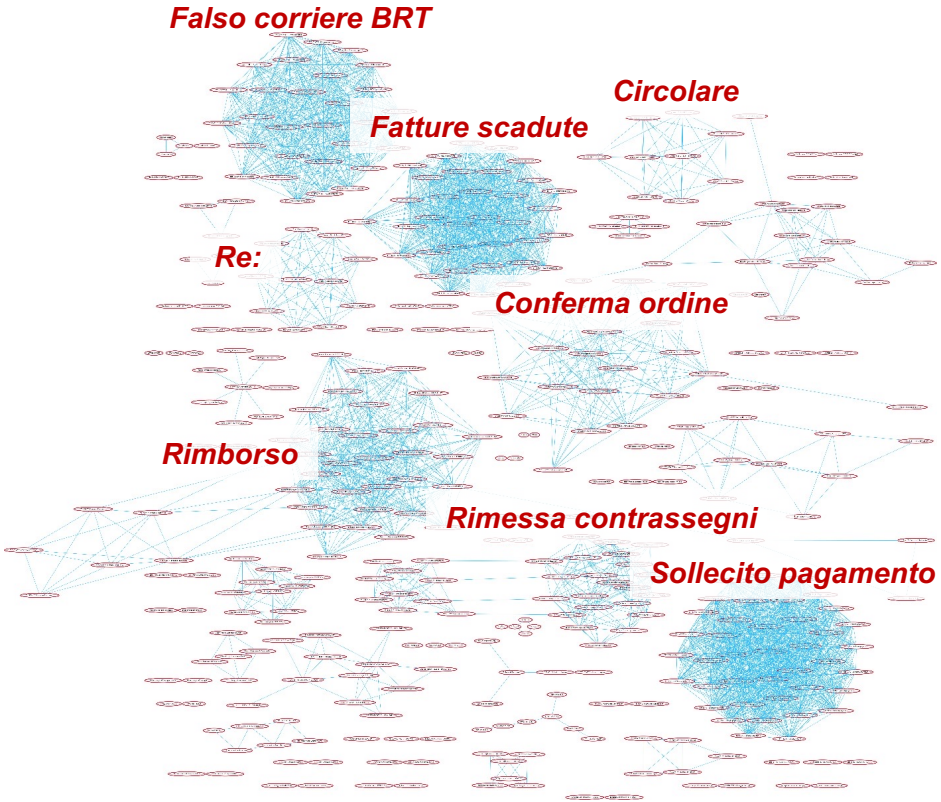


SPACIAL FOCUS
Minacce dalle email

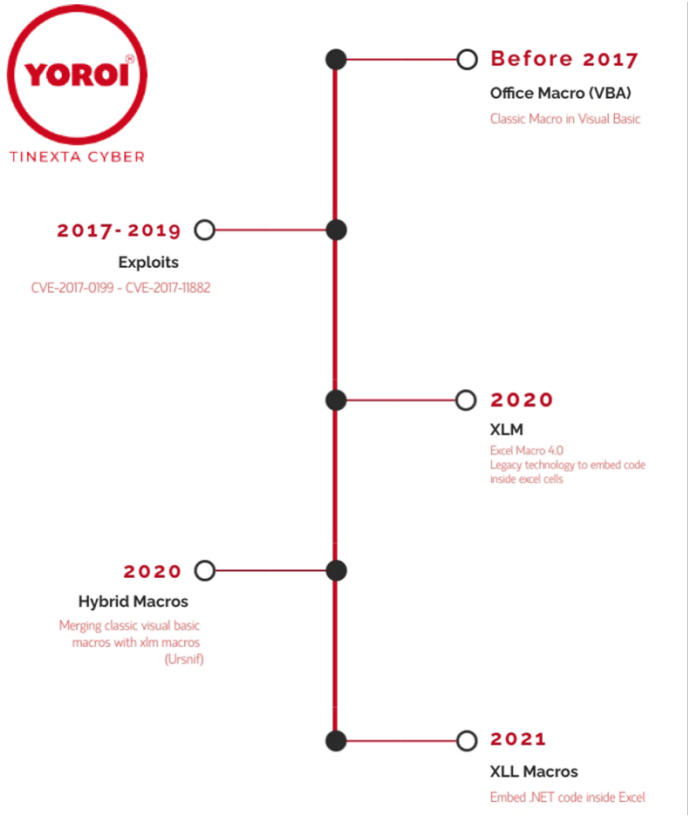


Le campagne email

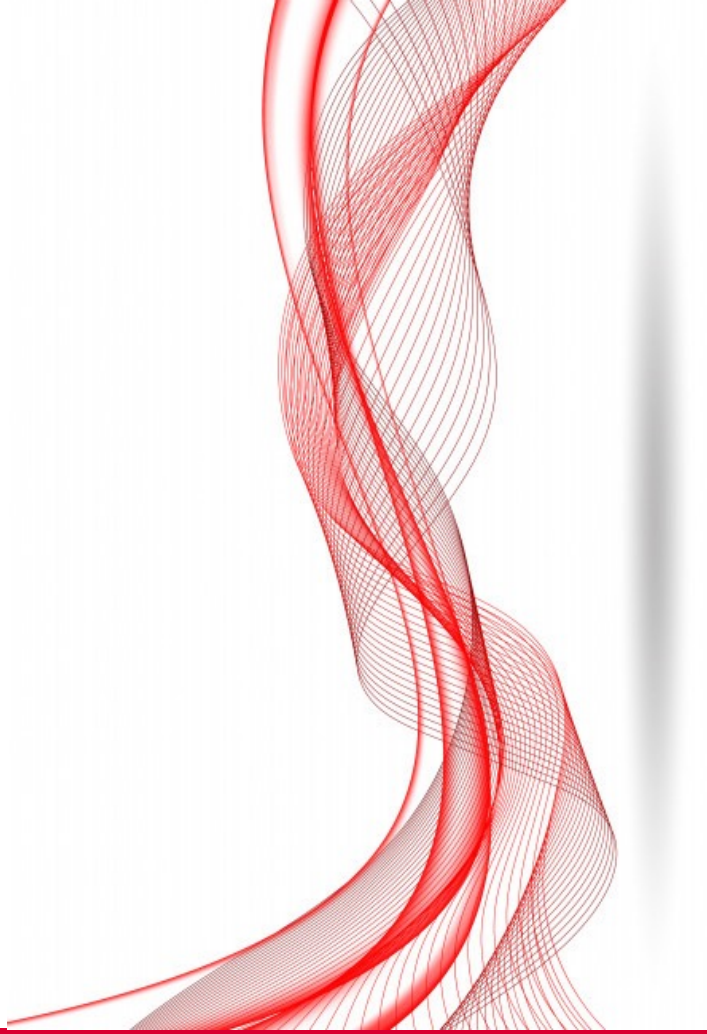




L'evoluzione delle minacce che sfruttano Office

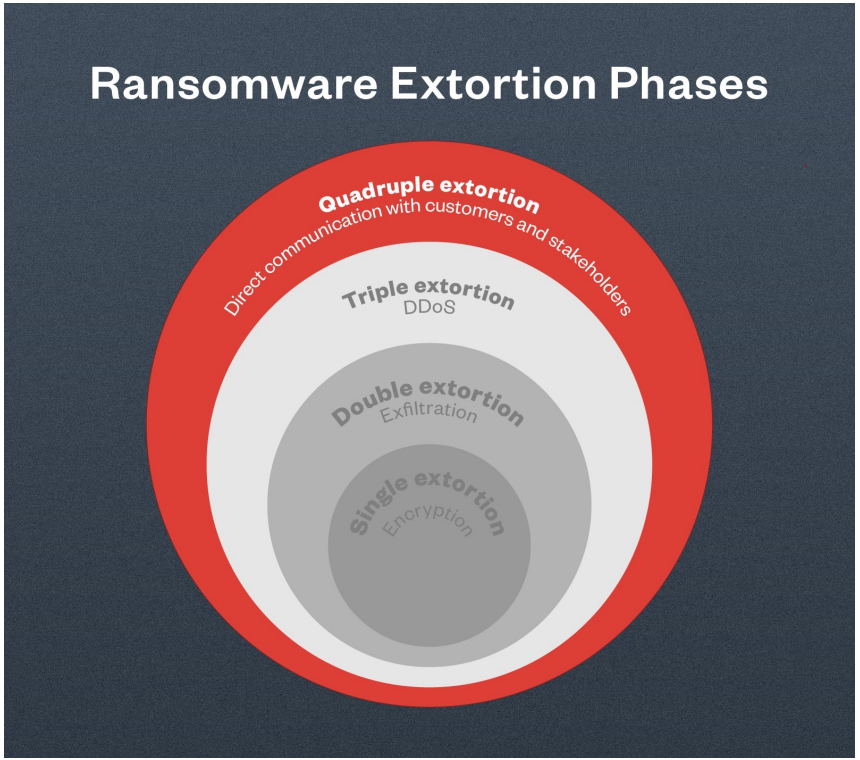


I Ransomware



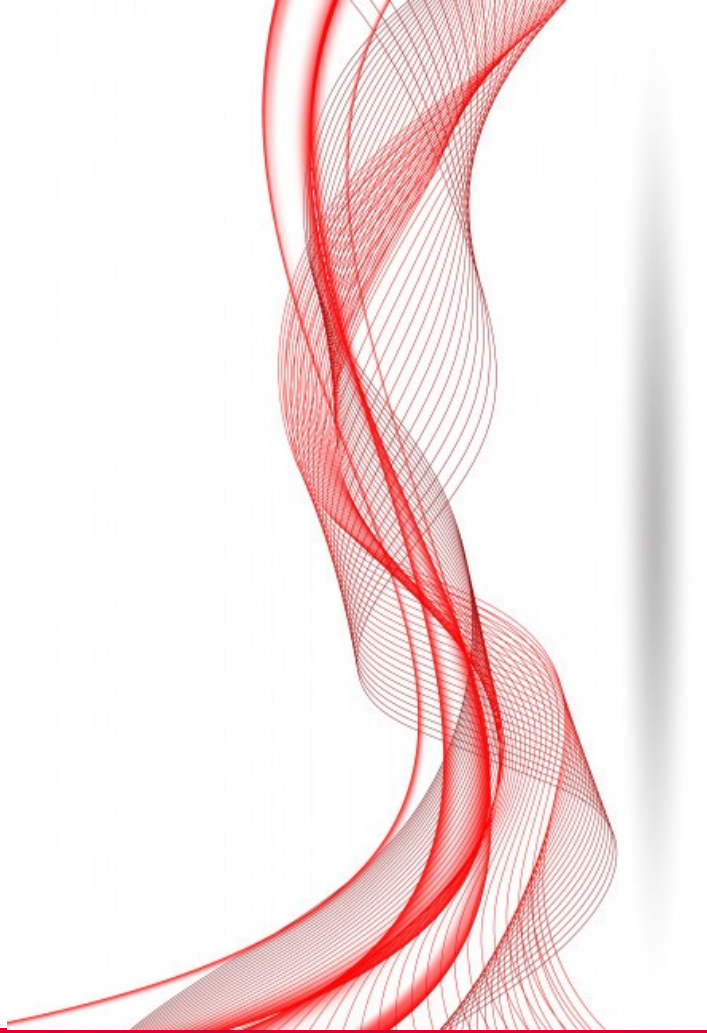
Quadruple extortion Ransomware

Fonte: Ransomware.org



Fonte: Trend Micro Research

La Supply Chain



Principali attacchi al perimetro

- Fortinet FortiGate
- Pulse Connect Secure
- SonicWall
- Palo Alto
- Citrix ADC / NetScaler
- F5 BIG-IP
- Exchange Server
- VMWare vCenter
- Log4j

Yoroi Cyber Exposure Index

Come si calcola Il Cyber Exposure Index

Lo Yoroi Cyber Exposure Index analizza l'esposizione aziendale senza alcuna azione attiva sull'organizzazione indicizzata, su tre diverse dimensioni.

Servizi esposti $S = \sum_{i\ in\ hosts} n_{si}$

$n_{si}\ numero\ dei\ servizi\ dell'host\ i-esimo$

Vulnerabilità $V = \sum_{i\ in\ services} \max_j v_{nji},$

v_{nji} *score della vulnerabilità accessibile da rete* $j-esima$ *nel servizio* $i-esim$

Data Leakage

$$L = \sum_{i\ in\ leaks} M e^{\frac{-(T-T_0)}{\tau}} v_{nji}$$

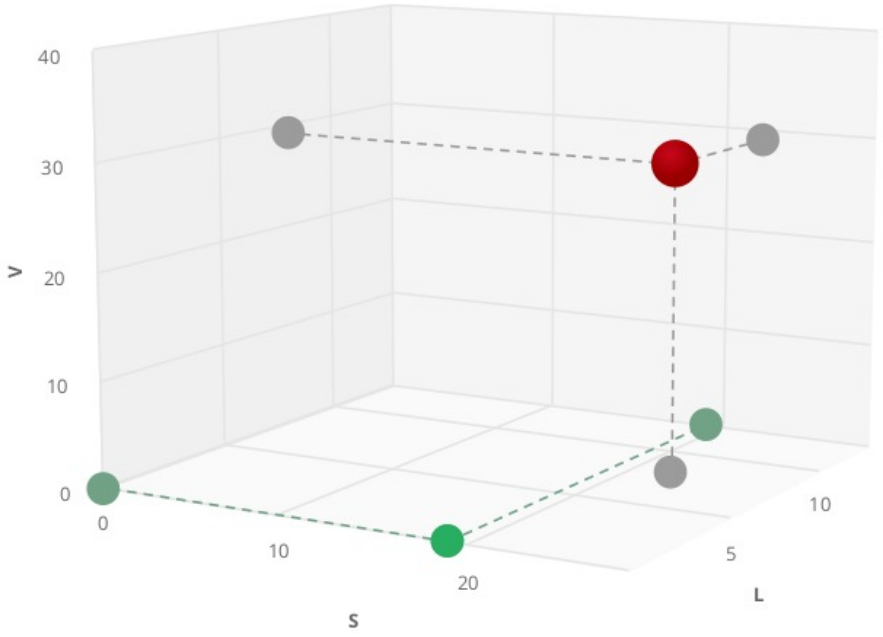
con

$$M = \begin{cases} 100, & se\ presente\ password\ in\ chiaro \\ 65, & se\ presente\ una\ password\ protetta \\ 30, & se\ non\ è\ presente\ una\ password \end{cases}$$

$T_0 =$ *data stimata del leak*

$\tau = 1\ mese,$ *periodo di decadimento*

CEI – un esempio

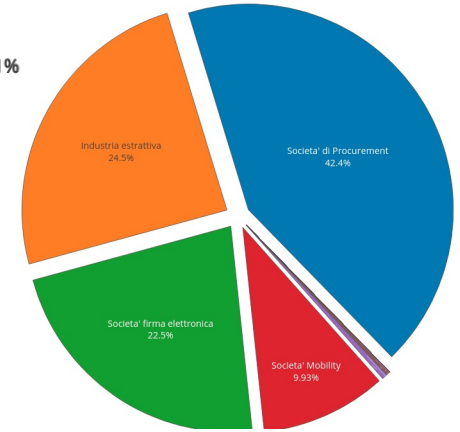


		Benchmark
Numero di **S**ervizi esposti	22	19
Score delle **V**ulnerabilità	29	0
Indice di data **L**eakage	8	0

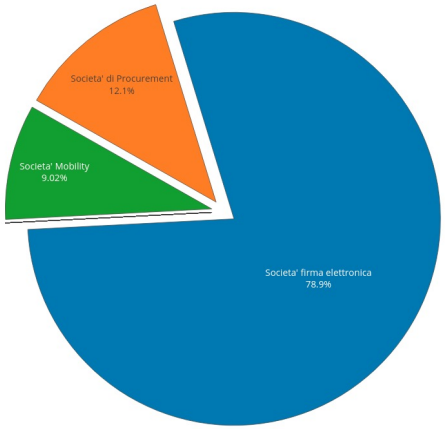
The **RED** dot represent the company's exposure index, the **GREEN** one is the benchmark.

Abbiamo calcolato il CEI per l'Italia

Esposizione settore merceologico – Azienda Large



Data Leak per settore merceologico



Vulnerabilità per settore merceologico

YOROI®

TINEXTA CYBER

YOROI®

TINEXTA CYBER

La presenza Yoroi nel mondo dei Social Media e nella Blogosfera

LinkedIN Twitter Youtube Blog Yoroi Blog M. Ramilli





Yoroi® è un marchio registrato


Registrazione N°: 016792947