Swascan
TINEXTA GROUP

Ransomware:
Trend e analisi nel Q2 2022

INDICE

EXECUTIVE SUMMARY

Come ipotizzato nel report pubblicato da Swascan che analizzava l'attività ransomware nei mesi di gennaio-marzo 2022, il Ransomware si è confermato essere la minaccia per eccellenza nel panorama della sicurezza informatica a livello globale anche nel Q2 dello stesso anno.

Il secondo trimestre del 2022 dimostra infatti come le gang ransomware siano rimaste il "nemico numero uno" nel panorama delle minacce e abbiano continuato nelle loro attività, nonostante la pressione nei loro confronti da parte delle forze dell'ordine sia aumentata. A tal proposito, un caso particolare è rappresentato dalla gang Conti, che sarà analizzata successivamente.

In questo contesto il SOC di Swascan ha intrapreso un'analisi del profilo delle vittime finite nel mirino delle gang di Criminal Hacker. In particolare sono stati raccolti, attraverso specifiche ricerche OSINT & CLOSINT, i dati che riguardano le vittime delle 15 gang Ransomware più attive nel secondo trimestre del 2022, ovvero le seguenti:

LockBit 2.0	ALPHV/ BlackCat	BlackBasta	Conti	ViceSociety
IndustrialSpy	Quantum	Hive	Karakurt	AvosLocker
KelvinSecurity	Lorenz	Stormous	CLOP	Blackbyte

L'approccio metodologico utilizzato è stato il seguente:

1. Identificazione dei siti Darkweb delle relative gang Ransomware;
2. Individuazione delle aziende vittime che sono state pubblicate sui portali Darkweb;
3. Clusterizzazione delle informazioni relativamente alle vittime in termini di:

- Area geografica
- Settore merceologico
- Fatturato e dipendenti

IL CONTESTO

A livello globale, è possibile osservare come nel secondo trimestre del 2022 il numero di vittime pubblicate raggiunga i **707 casi**, con un **incremento del 36.9%** rispetto al Q2 2021 dove se ne contavano 517. Si tratta di **un aumento del 30%** rispetto alla stessa attività individuata nel primo trimestre 2022 (544 casi).

Se, come abbiamo anticipato nel report relativo al Q1 2022, l'attività ransomware risulta in calo rispetto all'ultimo trimestre dell'anno precedente, confrontando invece il Q2 2021 con Q2 2022, possiamo notare come nel trimestre di quest'anno il livello di attività sembri essere in aumento rispetto all'anno precedente.


Swascan
TINEXTA GROUP
Q2 2022
Q2 2021
Total
Ransomware
groups
31
Total
Ransomware
groups
29
Most
impacted
region
United States
Most
impacted
region
United States
Total
Countries
Impacted
62
Total
Countries
Impacted
60
Most
Impacted
Industry
Services
Most
Impacted
Industry
Manufacturing

Come è possibile notare nelle tabelle di cui sopra, **gli Stati Uniti** hanno continuato ad essere il paese maggiormente preso di mira negli attacchi ransomware: il 39% delle organizzazioni colpite, infatti, sono geolocalizzate in questo paese. **L'Italia** scende al **quarto posto**, rispetto al terzo posto riscontrato nel primo trimestre del 2022.

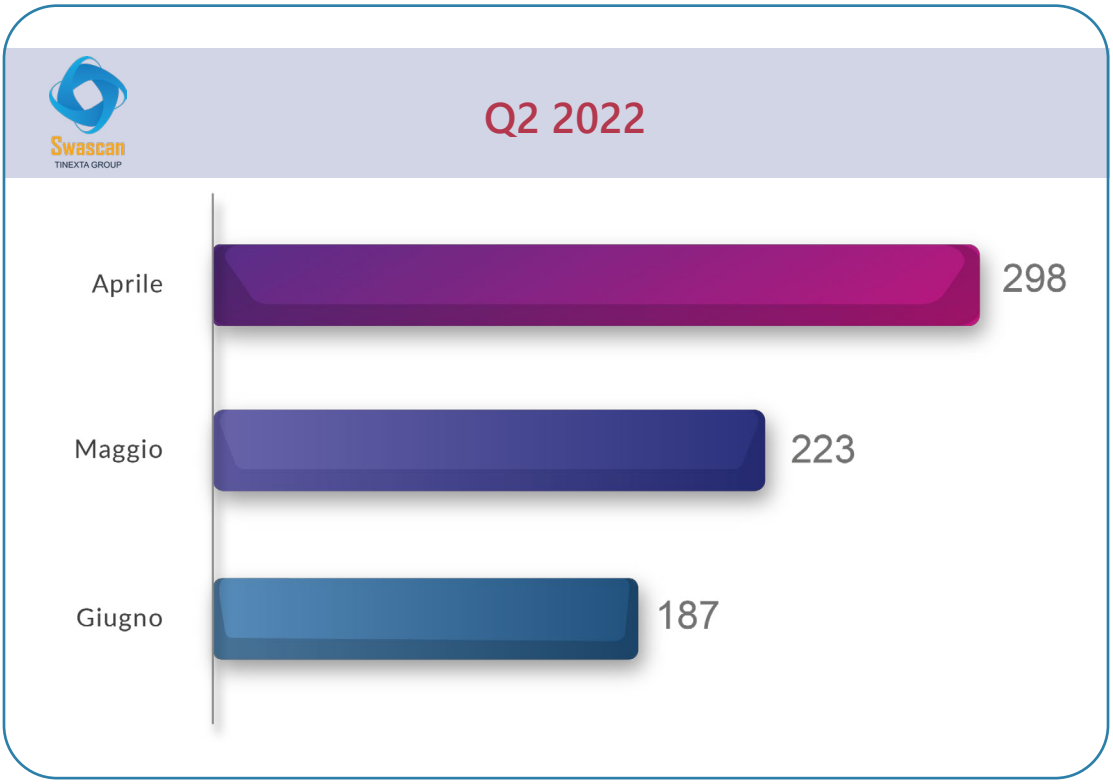
Focalizzandoci sul Q2 2022, si riscontrano:

1. +66% di vittime dall'inizio dell'anno, passando da 112 vittime nel mese di gennaio a 187 nel mese di giugno.

2. Diminuzione di vittime in Italia rispetto al Q1 2022, con un -17,5% di vittime, mentre passa al primo posto la Germania come paese europeo più colpito (+26.4% di vittime) .

3. Picco di attacchi ad aprile corrispondente, dunque, ad una crescita nel Q2 2022, seguito da un decremento di attacchi fino a giugno 2022.

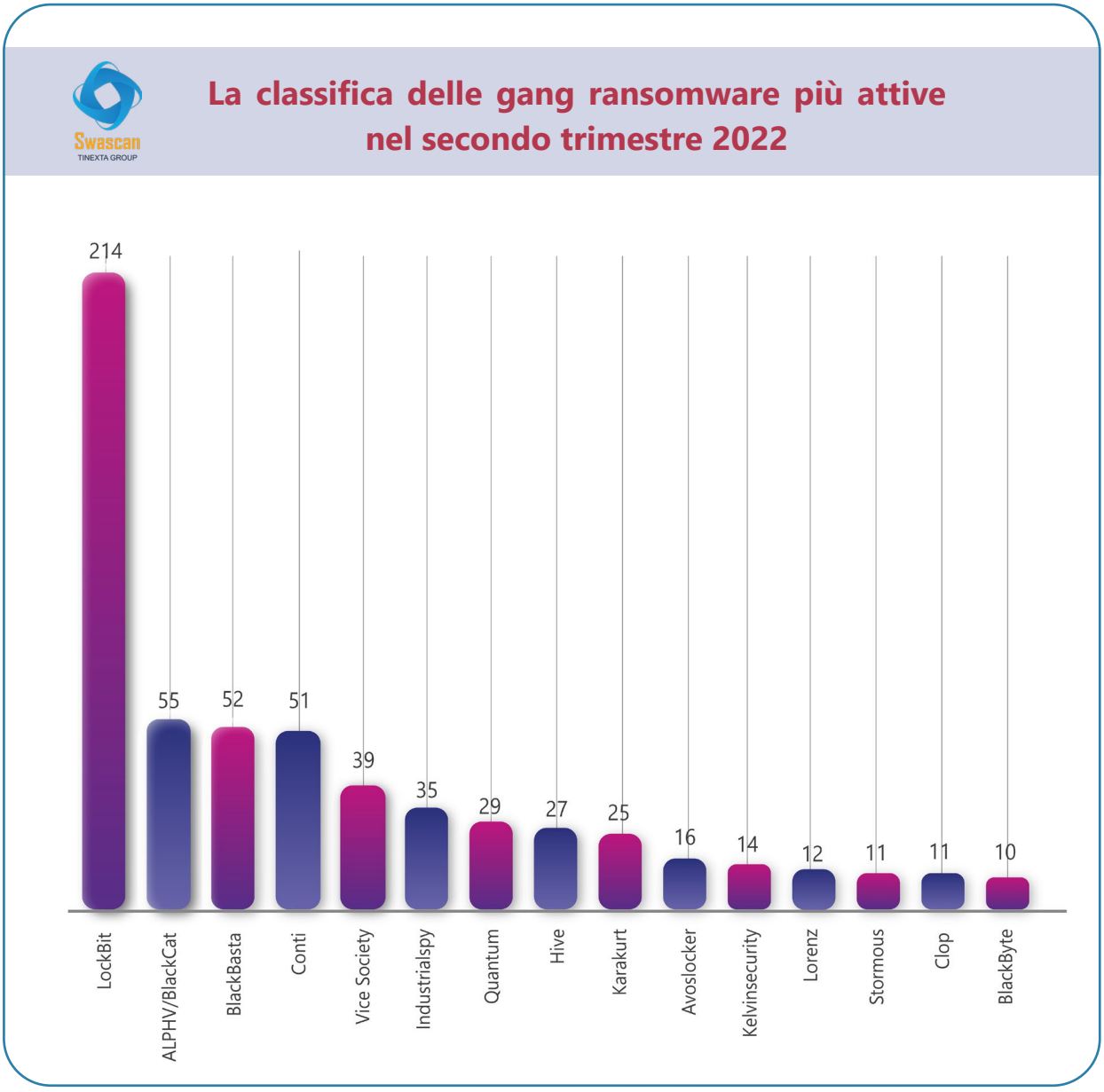
4. Lieve diminuzione di vittime anche negli Stati Uniti (-4%), ma nel totale continua ad essere il paese più colpito.



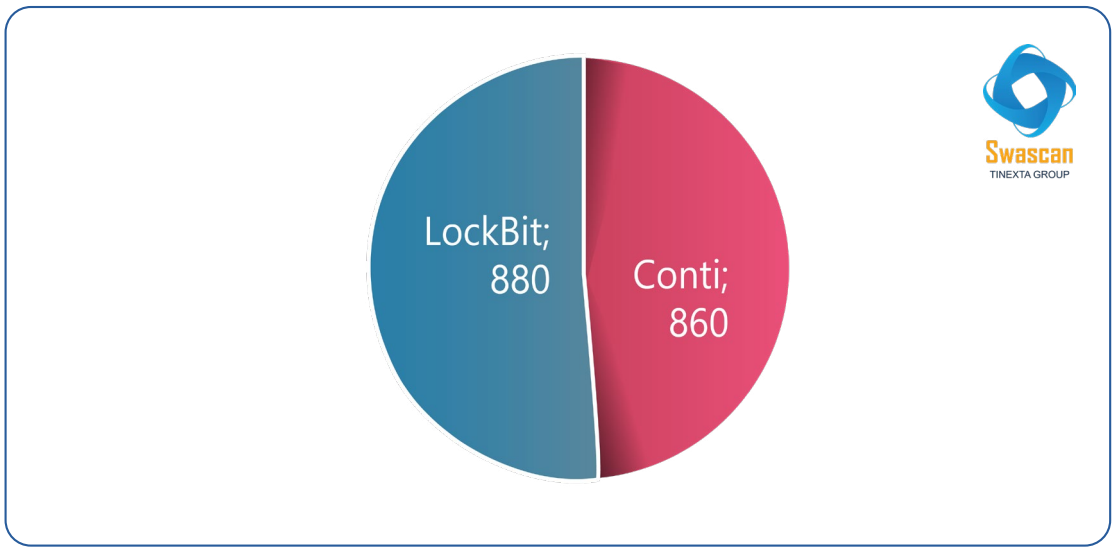
LE GANG RANSOMWARE PIÙ PROLIFICHE

Volendo dare uno sguardo alle gang ransomware più attive nel secondo trimestre 2022, notiamo come la gang LockBit spicchi per numero di attacchi.

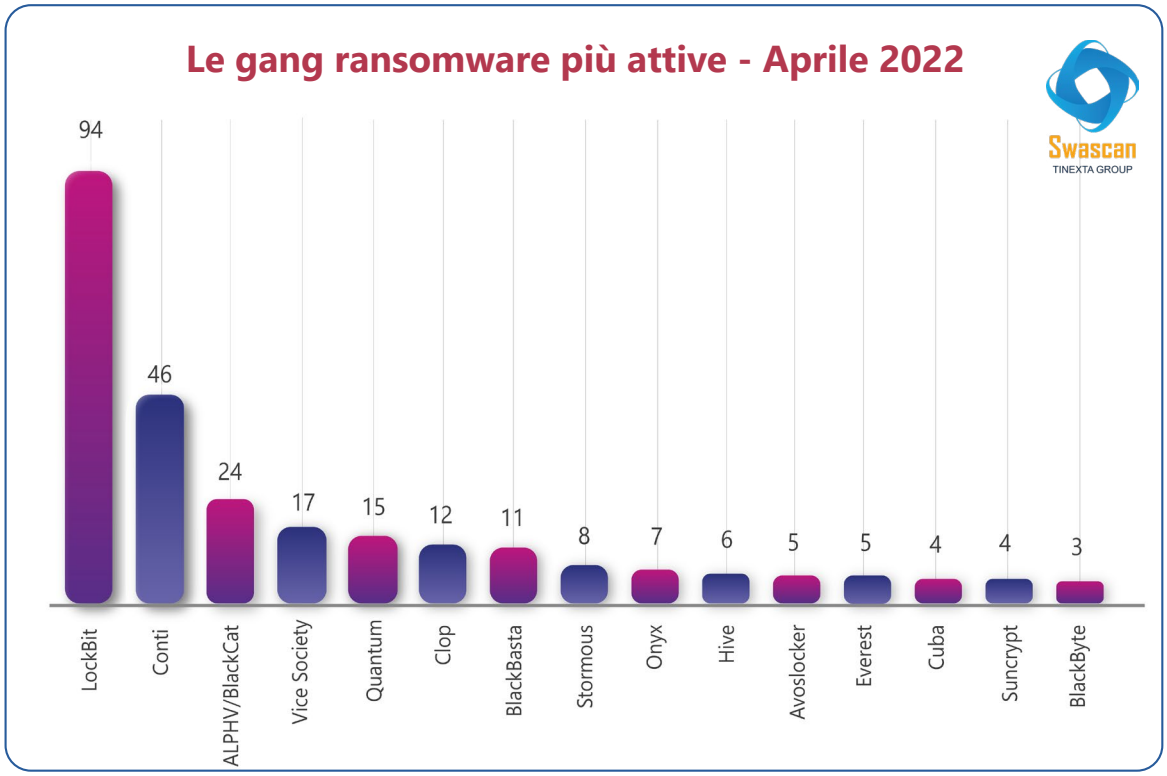
Di seguito la classifica delle gang ransomware più attive nel **secondo trimestre 2022:**



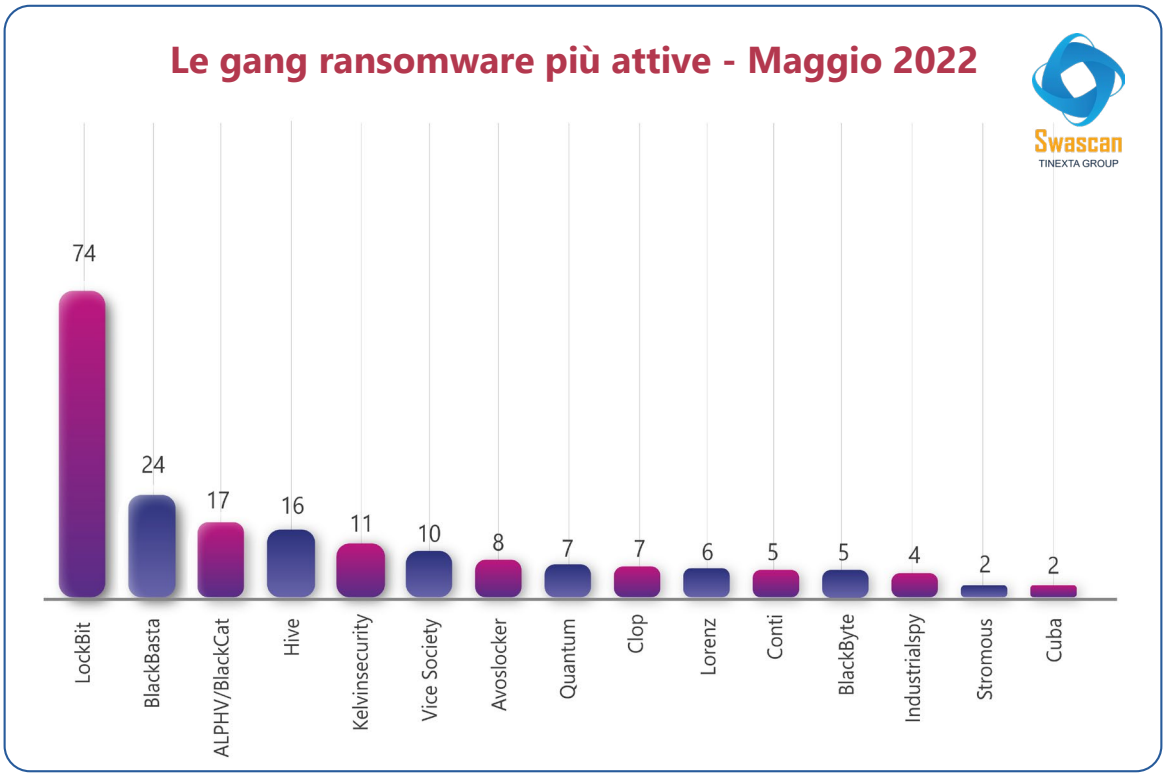
Come si evince dal grafico, il 30.2% di tutti gli attacchi ransomware del secondo trimestre del 2022 sono da attribuirsi alla gang LockBit, che supera definitivamente la gang Conti: analizzando il totale degli attacchi dall'inizio delle attività di entrambe le gang ed arrivando fino a giugno 2022 è possibile notare come LockBit raggiunga un totale di 880 attacchi contro gli 860 totali di Conti:



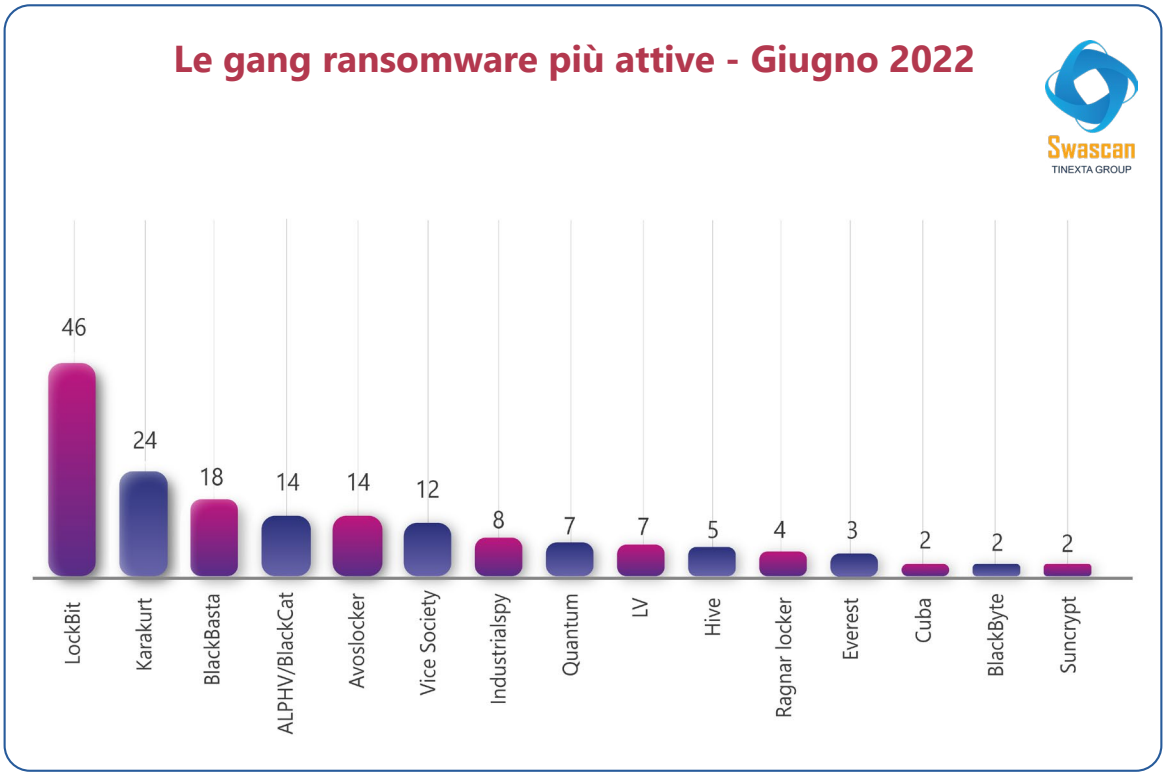
Di seguito riportiamo l'analisi relativa ad ogni singolo mese del Q2 2022. Per il solo mese di aprile 2022, queste le gang ransomware più attive:



Per il mese di maggio 2022, queste le gang ransomware più attive:

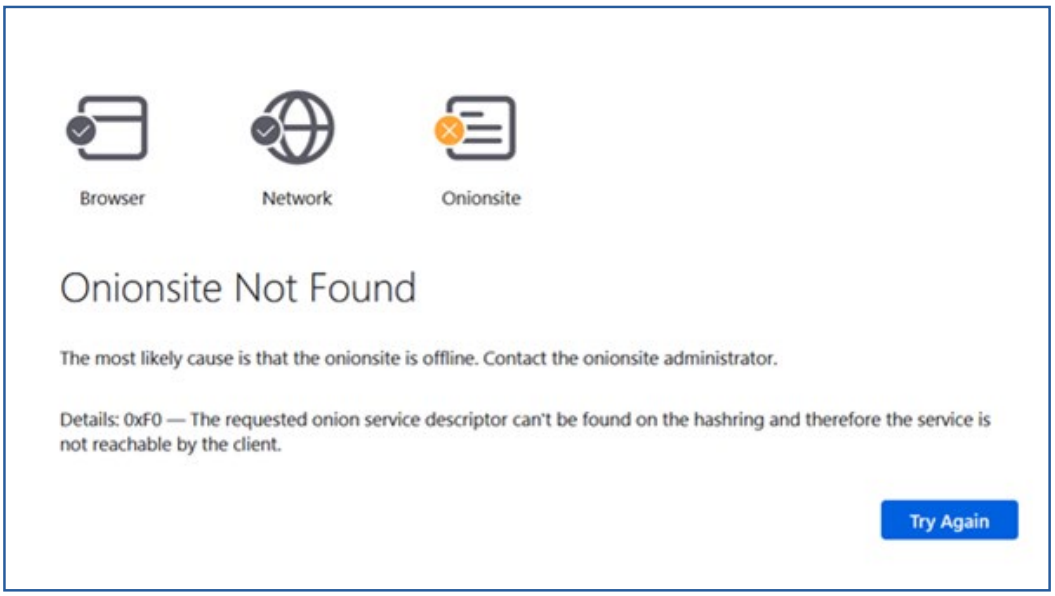


Per il mese di giugno 2022, queste le gang ransomware più attive:



LA GANG CONTI INTERROMPE LE ATTIVITÀ

Ciò che più salta all'occhio nell'analisi di giugno 2022 è l'assenza della famigerata banda di ransomware Conti, che sembra aver ufficialmente chiuso la propria attività, interrompendo il funzionamento dell'infrastruttura utilizzata per la gestione degli attacchi **ransomware:** tuttavia, sembrerebbe che il gruppo abbia infatti di unirsi ad altre gang esistenti "celle" indipendenti, che avranno compiti differenti. Questo tipo di **riorganizzazione interna** è già avvenuta per altri noti gruppi ed è probabilmente dovuta alla necessità di eludere le attenzioni delle forze dell'ordine.



Il gruppo **Conti** è responsabile di numerosi attacchi, tra cui quelli recenti contro i governi dell'Ucraina e della Costa Rica. Le forze dell'ordine cercano di trovare gli organizzatori degli attacchi e gli esecutori materiali (Conti è un **ransomware-as-a-service**), offrendo anche ricompense in denaro. Forse per questo motivo, i cybercriminali hanno deciso di mettere offline l'infrastruttura e di chiudere i siti utilizzati per la pubblicazione dei dati rubati e la negoziazione del riscatto. Quello contro la Costa Rica è quindi l'ultimo attacco effettuato come Conti.

Se da un lato la gang Conti interrompe le attività, dall'altro LockBit lancia la terza versione del suo servizio, LockBit 3.0, introducendo opzioni di pagamento in criptovaluta Zcash, nuove tattiche di estorsione e il primo programma di ricompense di bug ransomware in cambio di segnalazioni di bug valide.

L'ASCESA DI LOCKBIT 3.0

"Invitiamo tutti i ricercatori sulla sicurezza, gli hacker etici e non etici del pianeta a partecipare al nostro programma di ricompense dei bug", secondo la pagina di ricompense dei bug di LockBit 3.0. "L'importo della remunerazione varia da $ 1000 a $ 1 milione".

Tuttavia, il programma di ricompense dei bug dell'operazione non si limita alla ricerca di vulnerabilità con il servizio. Comprende anche quanto segue:

- **Bug siti Web:** trovare i punti deboli del sito Web, comprese le injection MySQL e le vulnerabilità XSS, ottenere una shell sul server del sito Web.

- **Doxing:** in cambio dell'identificazione del gestore del programma di affiliazione, LockBit offre 1 milione di dollari in criptovaluta.

- **Locker Bugs:** eventuali errori durante la crittografia da parte del malware che portano a file danneggiati o alla possibilità di decrittografare i file senza ottenere un decryptor.

- **dee:** LockBit paga per idee o suggerimenti che li aiuterebbero a migliorare il loro funzionamento.

- **TOX Messenger:** ricerca delle vulnerabilità di TOX messenger, comprese quelle che faciliterebbero l'intercettazione delle comunicazioni, l'esecuzione di malware o il rilevamento degli indirizzi IP.

- **Tor Network:** trovare vulnerabilità che espongano l'indirizzo IP del server che ospita il sito Web sul dominio onion, ottenere l'accesso come root ai server o scaricare il database del sito Web.

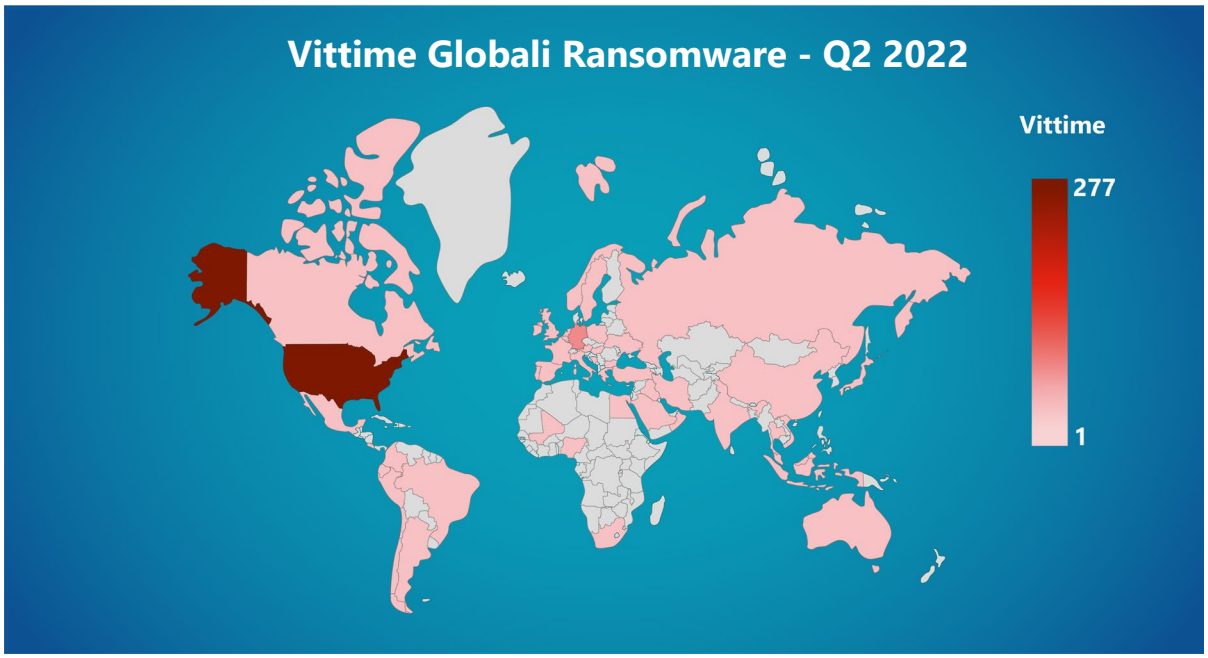
Risultano rinnovate anche la sezione "contatti" e "affiliati", mentre viene introdotta una nuova sezione relativa all'acquisto di Bitcoin ed ulteriori modalità di monetizzazione:

- **Estendi il "countdown":** la vittima può pagare per estendere il countdown per la pubblicazione dei dati;
- **Distruggi tutte le informazioni:** la vittima può pagare per distruggere tutte le informazioni esfiltrate dalla sua organizzazione;
- **Scarica i dati in qualsiasi momento:** la vittima può pagare per ottenere l'accesso al download esclusivo di tutti i dati esfiltrati dell'azienda.

La gang opera come una vera e propria azienda, dove uno dei punti fondamentali è la reputazione: si tratta pertanto di un'operazione di marketing a costo zero con una vista verso l'esterno, creando in tal modo reputazione verso i possibili affiliati e terrorismo verso le possibili vittime, ed optando per una modalità di hiring e business development attraendo così insiders che segnaleranno criticità.

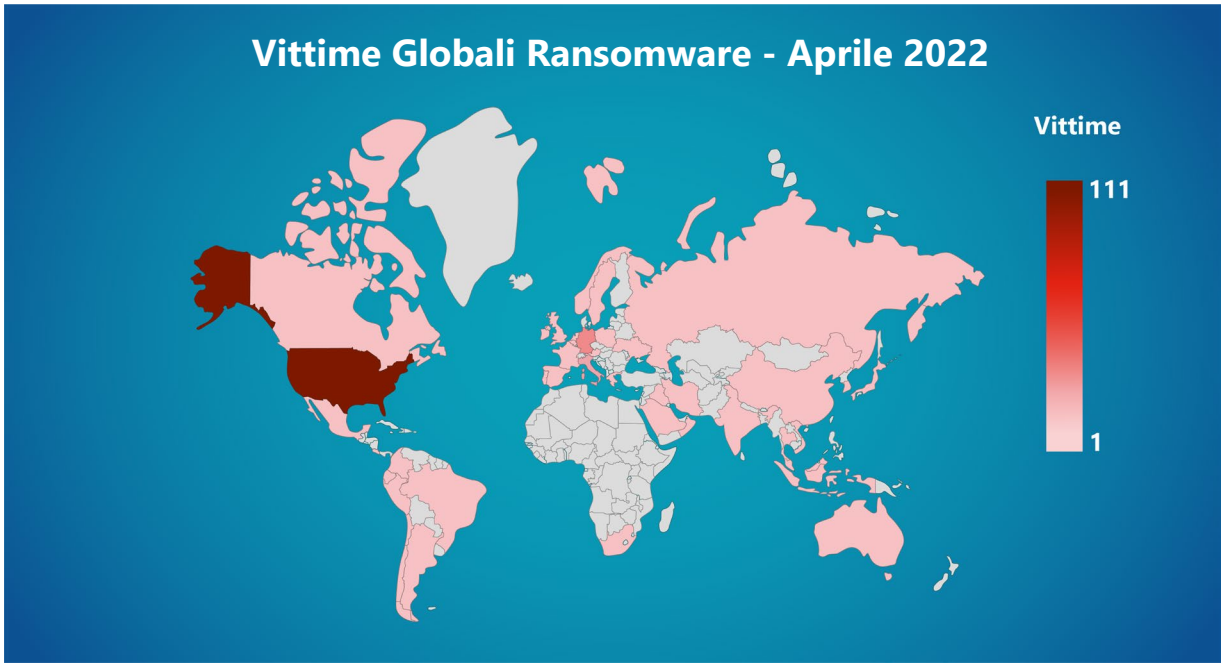
DISTRIBUZIONE GEOGRAFICA DELLE VITTIME

Nel corso delle analisi è stato possibile riscontrare come la maggior parte delle gang sia risultata attiva negli **Stati Uniti**, con un **totale di 277 vittime**, mentre **in Italia** si contano un totale di **33 vittime.**
Nelle mappe di seguito, la distribuzione geografica degli attacchi ransomware nel secondo trimestre 2022.



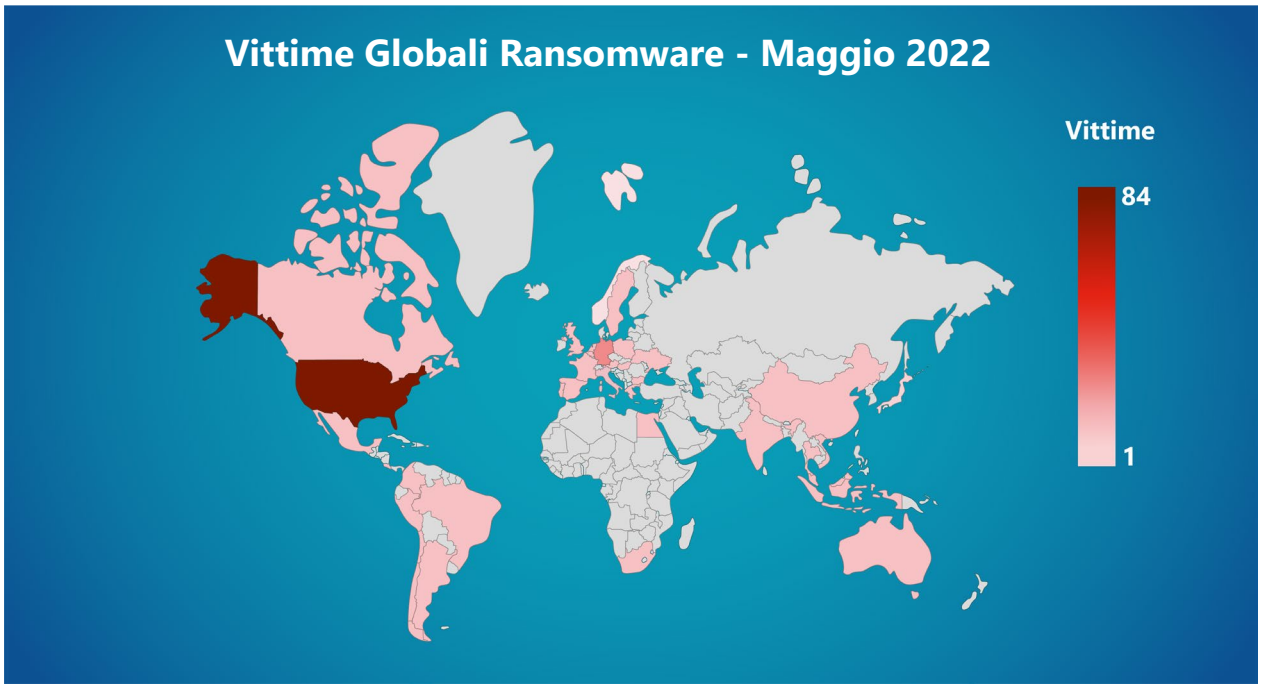
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – Q2 2022
United States	277
Germany	43
Canada	37
Italy	33
United Kingdom	32
France	28
Spain	17
India	15

Nel dettaglio, **gli Stati Uniti** mantengono il loro primato anche nel mese di aprile, con un totale di **111 vittime**. Nello stesso mese, in **Italia** se ne contano **18**.



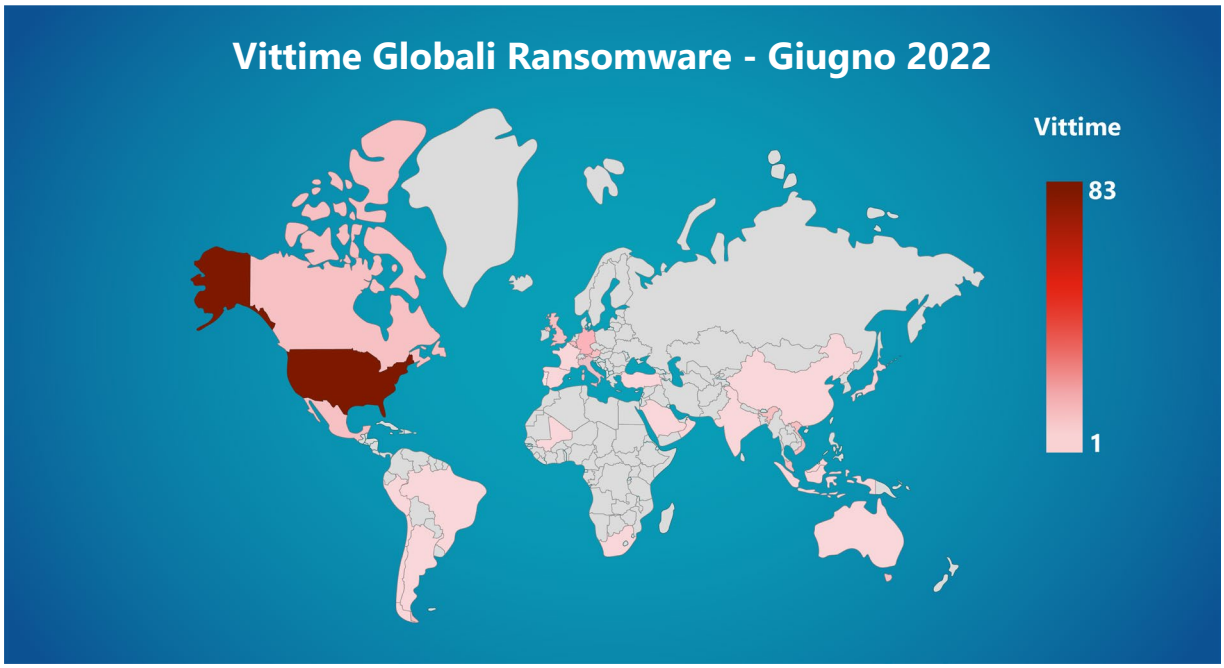
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – Aprile 2022
United States	111
Germany	20
Italy	18
Canada	16
France	12
United Kingdom	11
India	9
Spain	9

Stesso di scorso per il mese di maggio, in cui **gli Stati Uniti** contano un totale di **84** vittime. Nello stesso mese, in **Italia** se ne contano **6**.



PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – Aprile 2022
United States	84
Germany	14
Canada	12
United Kingdom	11
Taiwan	7
France	6
Italy	6
Mexico	6

Anche a giugno 2022 il più alto numero di vittime è riscontrato negli **Stati Uniti** (**83**). Nello stesso mese, in **Italia** se ne contano **9**.

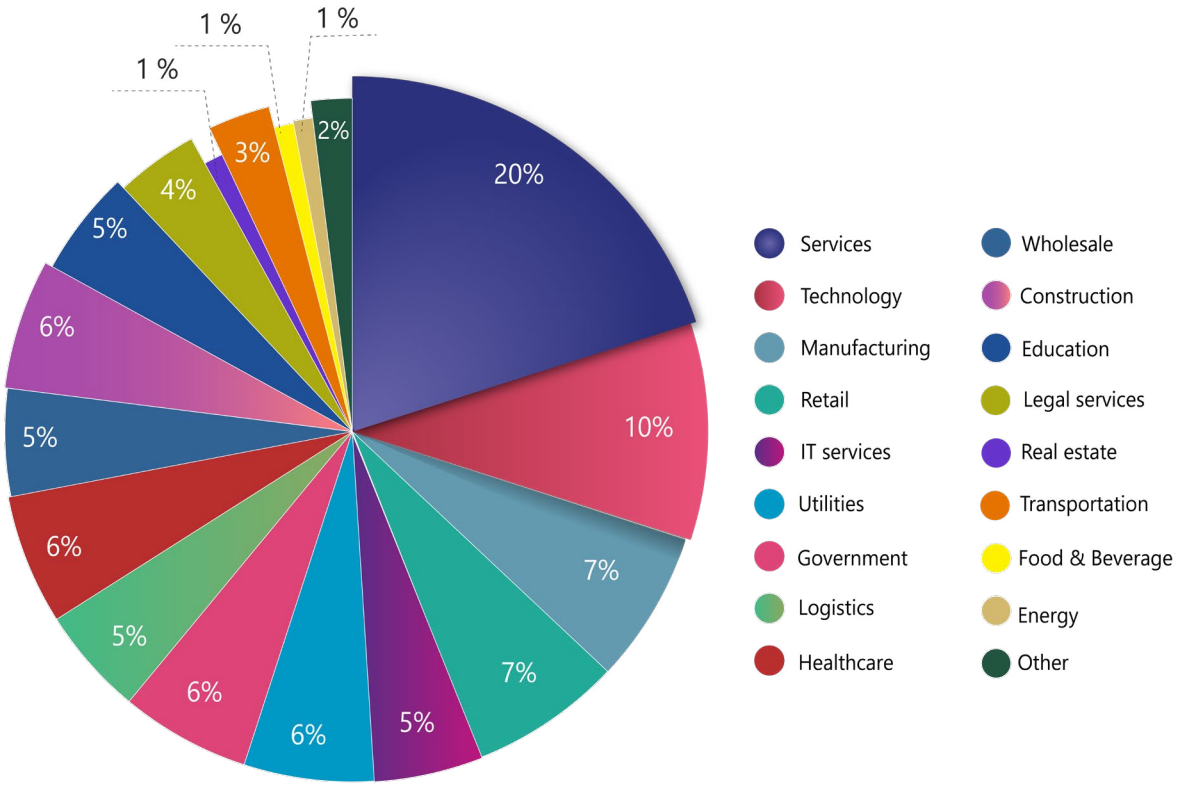


PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – Aprile 2022
United States	83
Canada	10
United Kingdom	10
France	9
Germany	9
Italy	9
Austria	5
Indonesia	4

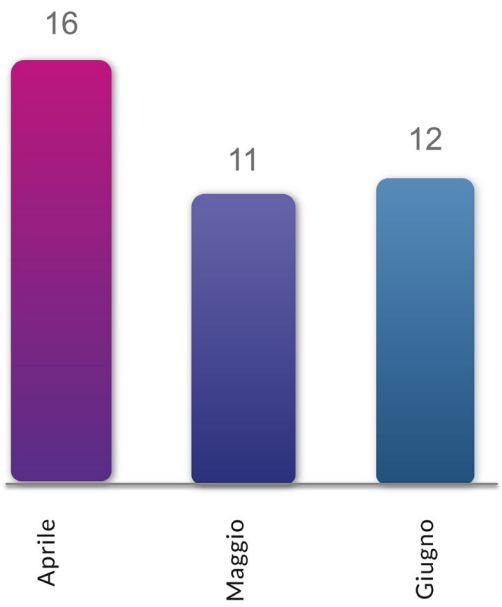
I SETTORI PRESI DI MIRA

Di seguito riportiamo un'analisi dei settori e delle infrastrutture critiche colpite nel Q2 2022. In particolare, si evidenzia un lieve calo nel numero di attacchi ransomware rivolti ad infrastrutture critiche nel mese di maggio.

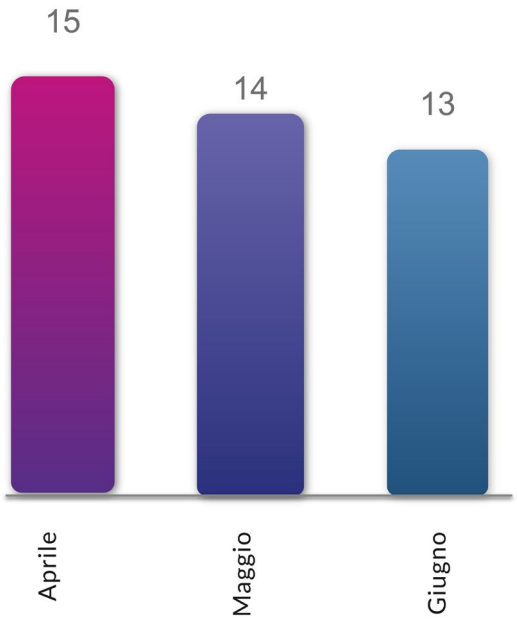
ATTACCHI PER SETTORE IN PERCENTUALE



ATTACCHI RANSOMWARE A STRUTTURE SANITARIE



ATTACCHI RANSOMWARE AD AMMINISTRAZIONI STATALI E COMUNALI



CLUSTER FATTURATO E DIPENDENTI AZIENDE VITTIME PUBBLICATE

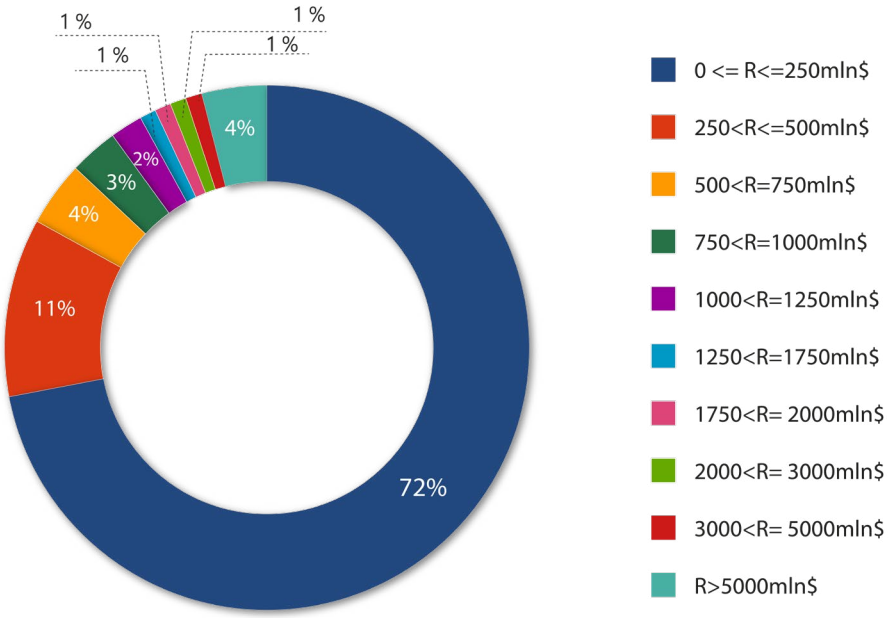
Secondo le statistiche, larga parte delle vittime colpite da ransomware sono le aziende medio piccole. I criminal hacker hanno intensificato le loro ricerche e tecniche, introducendo tecnologie di attacco sempre più mirate e sofisticate. Siamo abituati a leggere sui giornali le notizie di attacchi informatici ai danni di grandi aziende: Regione Lazio, Amazon, Microsoft… informazioni che fanno certamente notizia e che attraggono un gran numero di utenti.
Tuttavia, come avevamo già dimostrato nell'analisi del Q1 2022, se da un lato le aziende di grandi dimensioni possiedono una maggiore disponibilità economica, sono anche le stesse che implementano soluzioni di sicurezza informatica strutturate.

Le PMI, al contrario, sono quasi del tutto estranee al problema, spesso mancano del tutto di soluzioni cybersecurity, motivo per cui sono spesso i soggetti più vulnerabili.

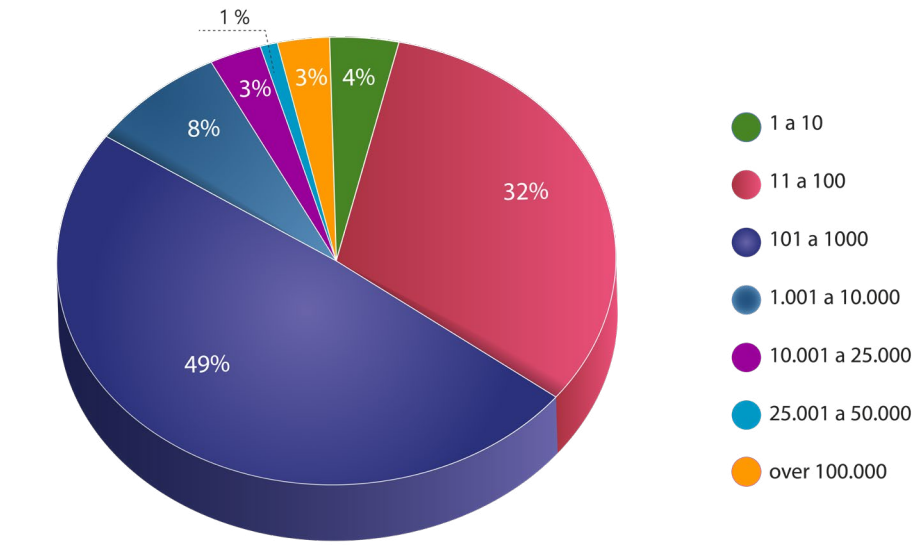
La riprova è nei due grafici riportati di seguito.

L'analisi è stata condotta scegliendo a campione 10 aziende vittime per ognuna delle 10 gang ransomware che si sono distinte nel periodo intercorso tra aprile e giugno 2022, per un totale di **100 aziende analizzate**. I dati sono poi stati aggregati in base al fatturato e al numero di dipendenti delle vittime:

SPACCATO AZIENDE COLPITE IN BASE A FATTURATO



NUMERO DIPENDENTI AZIENDE COLPITE



L'analisi ha confermato quanto mostrato già nel primo trimestre 2022, ossia come le aziende di piccole dimensioni siano più facilmente suscettibili al pagamento del riscatto (che naturalmente sarà proporzionato al fatturato del target).

Riportiamo di seguito una tabella riassuntiva confrontando il Q1 vs Q2 2022:

	Q1 2022	Q2 2022	Q2/Q1 (in %)
Total victims	544	707	+ 29.9%
Total Ransomware groups	35	31	-11.4%
LockBit victims	220	214	-2.7%
Conti Victims	120	51	-57.5%
Most impacted region	United States	United States	
Total Countries Impacted	83	62	-25.3%
5 most impacted countries	United States, United Kingdom, Italy, Germany, Canada	United States, Germany, Canada, Italy, United Kingdom	
Most Impacted Industry	Manufacturing	Services	
PMI impacted	78%	85%	+8.9%

CONCLUSIONI

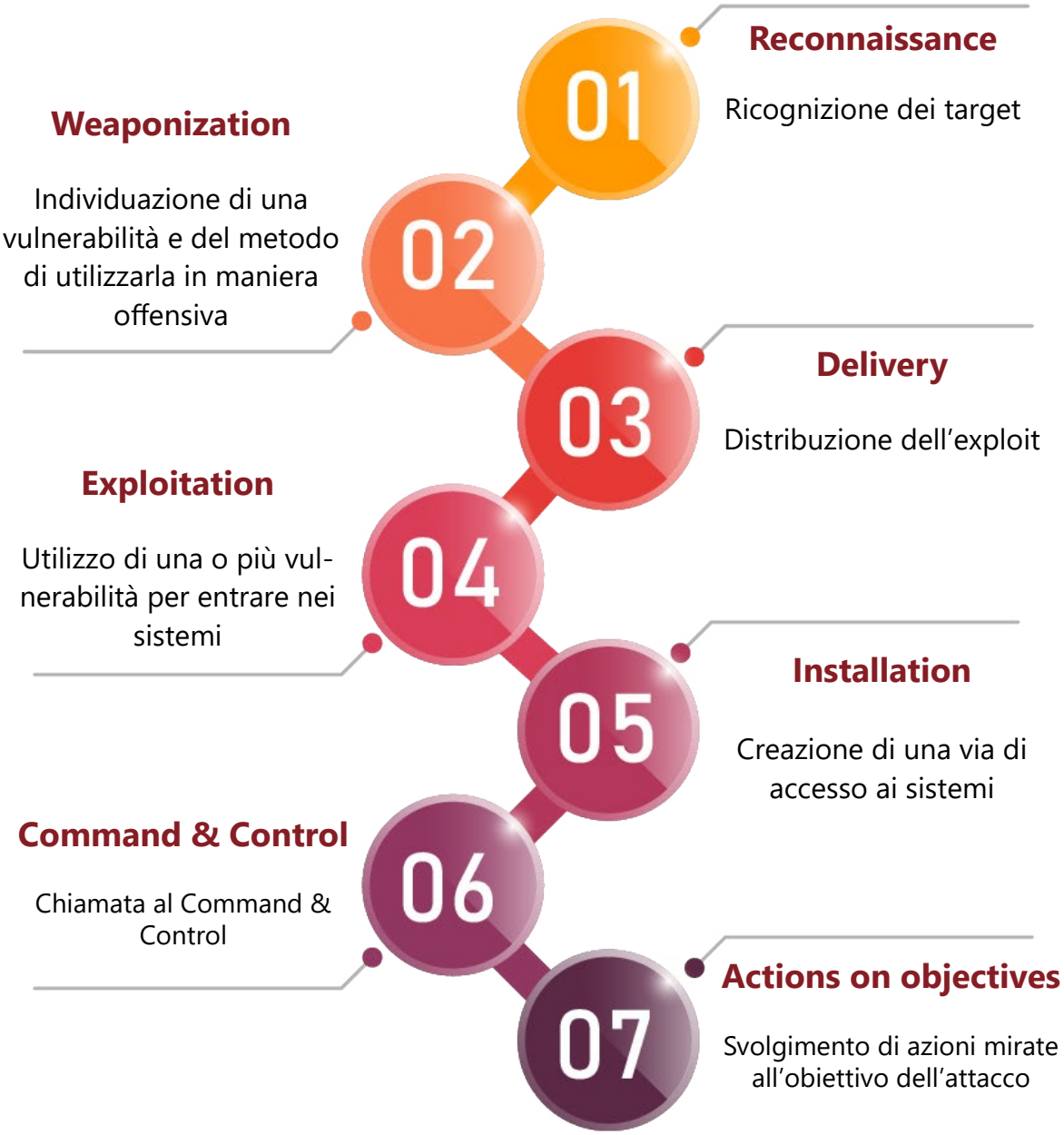
Nel secondo trimestre 2022 si è osservato un significativo aumento degli attacchi ransomware, principalmente a causa di un picco di attività da parte di uno dei gruppi più prolifici, LockBit, che raggiunge una media di 6.6 vittime al giorno, superando definitivamente la gang Conti.

Il mese di aprile 2022 è stato caratterizzato dall'emergere di tre nuove gang ransomware: Onyx, Mindware, e Black Basta, così come il ritorno sgradito di Revil, uno dei gruppi più pericolosi al mondo. A maggio 2022 Conti risulta ancora attivo, ma la sua attività risulta significativamente ridotta rispetto ai mesi precedenti (con soli 5 attacchi), fino ad arrivare all'effettiva scomparsa nel mese di giungo. Sembrerebbe tuttavia che alcuni leader della gang Conti abbiano sottoscritto accordi con altre gang per continuare la loro attività: una riorganizzazione interna già avvenuta da parte di altri noti gruppi, probabilmente dovuta alla necessità di eludere le attenzioni delle forze dell'ordine.

L'industria dei servizi risulta il settore più colpito e gli Stati Uniti il paese più attaccato: qui, infatti, il numero di attacchi continua a crescere in modo esponenziale, distaccandosi da tutti gli altri paesi per numero di vittime. Tuttavia, il trend risulta in crescita anche nell'Europa occidentale, dove al primo posto si posiziona la Germania, mentre scende al quarto posto l'Italia.

Infine, in riferimento al cluster fatturato delle aziende vittime, il 72% delle aziende con dati pubblicati analizzati hanno un fatturato che non supera i 250 milioni di dollari: pertanto, come anticipato nel report precedente, se l'anno scorso si riscontrava un aumento degli attacchi ransomware contro le organizzazioni "più grandi", nel 2022 notiamo un incremento degli attacchi verso le Piccole Medie Imprese.

COME OPERA IL RANSOMWARE: CYBER KILL CHAIN



COME DIFENDERSI DAL RANSOMWARE: IL CYBER SECURITY FRAMEWORK

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno solidificati e rispettati i tre canoni di:

- **Sicurezza Predittiva**
- **Sicurezza Preventiva**
- **Sicurezza Proattiva**

Swascan
TINEXTA GROUP

Sicurezza Predittiva

1. Identifica le minacce aziendali fuori dal perimetro aziendale operando a livello di web, Darkweb e Deepweb
2. Ricerca eventuali minacce emergenti
3. Effettua attività di Early Warning
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di attenzione alla Sicurezza Proattiva

Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale
2. Contrasta e blocca gli attacchi informatici
3. Gestisce i Cyber Incident
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di investigazione alla Sicurezza Predittiva

Sicurezza Preventiva

1. Verifica e misura il Rischio Cyber
2. Definisce i piani di remediation
3. Indica il Rischio esposto al Layer di Sicurezza Proattiva
4. Fornisce le aree di Investigazione alla Sicurezza Predittiva

Sicurezza Predittiva

Domain Threat Intelligence: La Domain Threat Intelligence ricerca le informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed email compromesse. Il servizio non effettua alcun test sul target. Opera unicamente sulle informazioni disponibili sul web, Darkweb e deepweb. Raccoglie, analizza e clusterizza le informazioni disponibili a livello OSINT (Open Source Intelligence) e Closint (Close Source Intelligence) presenti su database, forum, chat, newsgroup.
Nello specifico, in base al dominio-target di analisi, identifica:

- Potenziali Vulnerabilità
- Dettagli delle Vulnerabilità in termini di CVE, impatti e severity
- Impatti GDPR (CIA)
- Numero dei Sottodomini
- Numero Potenziali e-mail compromesse (vengono solo conteggiate e non raccolte o trattate)
- Numero delle Source delle e-mail compromesse
- Typosquatting

Cyber Threat Intelligence: È il servizio evoluto di Threat Intelligence di Swascan. Effettua una attività di ricerca, analisi e raccolta delle informazioni presenti a livello web, Darkweb e Deepweb relativamente al dominio/target di analisi.
Nello specifico:

- Data Leaks: credenziali/source/data
- Identifica Forum/Chat ...
- Botnet relative a dispositive di Clienti, Fornitori e dipendenti
- Botnet con credenziali e relative url di login page
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Early Warning Threat Intelligence: È il servizio di Early warning che segnala giornalmente le evidenze che vengono identificate e raccolte nel Darkweb e deep web relativamente al target di analisi.
Nello specifico:

- Data Leaks
- Scraping data
- Phishing data
- Botnet

Sicurezza Preventiva

Tecnologico

Vulnerability Assessment: Esegue la scansione di siti e applicazioni web per identificare e analizzare i modo proattivo le vulnerabilità di sicurezza.

Penetration Test: Le attività di Penetration Test sono svolte da Penetration Tester certificati e in linea con gli standard internazionali OWASP, PTES e OSSTMM.

Human Risk

Phishing/Smishing attack Simulation: Permette alle aziende di prevenire i danni dovuti ad attacchi di phishing/smishing attraverso delle vere e proprie simulazioni di attacco. È infatti possibile, attraverso un'interfaccia web inviare vere e proprie campagne di phishing/ smishing simulate che generano delle insostituibili occasioni di apprendimento per i dipendenti. I dipendenti, infatti, grazie a questi attacchi simulati riusciranno, in futuro, ad individuare una vera e-mail di phishing o un messaggio di smishing e ad evitarla. Un'insostituibile attività di formazione e awareness dei tuoi dipendenti tramite vere e proprie simulazioni di attacco phishing/smishing .

Awareness: Corsi di formazione dedicati di Cybersecurity in aula o tramite Webinar. Attività di Awareness per il personale tecnico, per i dipendenti e per i Top Manager.

Processo – Compliance

ISO27001: ISO/IEC 27001:2013 (ISO 27001) è lo standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano). Dal momento che l'informazione è un bene che aggiunge valore all'organizzazione, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

ICT Security Assessment: L'ICT Security Assessment è una metodologia proprietaria di Swascan che permette alle aziende di verificare e misurare il proprio livello di rischio cyber e di valutare l'efficacia delle misure di sicurezza adottate. Il servizio fornisce le indicazioni e le azioni correttive da adottare a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo.

Sicurezza Proattiva

SOCaaS: La progettazione, la messa in esercizio e il mantenimento di un Security Operation Center può essere costoso e complesso. Il servizio **SOC as a Service** Swascan è la soluzione più efficace, efficiente, coerente e sostenibile per i contesti aziendali. Il Soc as a service con il suo servizio di Monitoring & Early Warning permette di **identificare**, **rilevare, analizzare** e segnalare gli attacchi cyber prima che possano trasformarsi in una minaccia concreta per l'azienda.
Un team dedicato nell'attività di **Monitoring & Early Warning** reattivo delle minacce informatiche sulle reti locali, ambienti cloud, applicazioni ed endpoint aziendali. Il nostro team di Security Analyst monitora i dati e le risorse ovunque risiedano all'interno dell'azienda. Indipendentemente dal fatto che le risorse siano archiviate nel cloud, in locale o in entrambi. L'attività di monitoring e segnalazione permette di agire solo quando viene identificata una minaccia reale.

Incident Response Management: è un insieme di risorse e procedure organizzate e strutturate per garantire la corretta reaction e gestione degli incidenti informatici. In caso di incidente informatico, Data Breach, DDoS, attacco Ransomware e/o relativo Data Recovery è necessario affrontare e rispondere con un approccio strutturato, predisposto e organizzato per affrontare in maniera efficace ed efficiente la violazione della sicurezza e per ridurre gli impatti a livello di Business Continuity aziendale. L'obiettivo dell'Incident Response è quello di:

- Gestire l'incidente;
- Limitare i danni diretti e indiretti;
- Ridurre tempi e costi di ripristino.

ABOUT US

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence,** oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di idetità digitale e sicurezza digitale.

Analysis by:

Martina Fonzo

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI