YARIX
a vargroup company

YSOC SECURITY REPORT

2020 H2 – 2021 H1

YARIX
a vargroup company

Sommario

Introduzione

Il documento restituisce un'elaborazione dei dati ricevuti e analizzati dal SOC di Yarix nel periodo luglio 2020 - giugno 2021

Chi siamo: Yarix, la Divisione Digital Security di Var Group

Parte di **Var Group**, in qualità di società a capo della divisione dedicata alla sicurezza digitale, Yarix esprime una leadership riconosciuta nel comparto della cybersecurity, avendo orientato la propria missione allo sviluppo di soluzioni specifiche per imprese ed enti governativi, aziende sanitarie, scuole e università. È stata la prima azienda privata in Italia ammessa al FIRST, la rete di protezione globale che riunisce player come Nasa, Apple e Google con l'obiettivo di contrastare le minacce emergenti.

Il SOC

Yarix dispone di uno dei più evoluti Cognitive Security Operation Center (C SOC) in Italia: una cyber control room dotata di misure di sicurezza fisica e biometrica di ultima generazione, basata su forme computazionali predittive e cognitive. Attivo 24 ore su 24 – grazie al presidio di un team di 30 esperti di sicurezza informatica – permette alle aziende di accedere a servizi di security, business continuity e disaster recovery, in modo da rispondere efficacemente alla rapida evoluzione delle minacce e dei rischi. Se la protezione del patrimonio tecnologico, informativo e intellettuale di ogni organizzazione è diventata una necessità improrogabile, il SOC rappresenta lo strumento più potente per contrastare le minacce cyber, attraverso avanzate funzionalità di intelligence e un approccio olistico alla sicurezza. L'efficacia del SOC è stata potenziata nel tempo, grazie all'integrazione di strumenti di Intelligenza Artificiale – per effettuare analisi predittive – e di soluzioni di **Cyber Threat Intelligence** applicate a dati open source e fonti eterogenee, per prevedere in anticipo potenziali attacchi informatici. L'approccio è multidisciplinare e multilivello: la sinergia tra competenze security e skill in ambito legale ed economico, amplifica la capacità di rispondere alla sfida della cybercriminalità, anche nella sua dimensione normativa e socio-economica.

I team YCTI e YIR

Il Cyber Threat Intelligence Team di Yarix (YCTI) è formato da analisti specializzati che, grazie a particolari skill ed esperienza maturati in questo settore, interpretano le informazioni disponibili nella rete – Clear, Dark e Deep Web – per prevenire e contrastare minacce quali cybercrime, hacktivism, operazioni pianificate per la sottrazione di dati o il blocco dell'operatività aziendale. Sono in grado di muoversi nel dark web con profili sotto copertura, infiltrandosi in black market e forum dove vengono scambiati e distribuiti malware, exploit e altri strumenti di attacco così da interagire direttamente con i Threat Actor.
Il team YIR affronta e risolve tutti gli aspetti delle violazioni informatiche, dall'indagine alla gestione delle crisi, fornendo una risposta efficace agli incidenti di sicurezza. Gestisce le

azioni di contenimento, analizzando e utilizzando le informazioni disponibili per determinare l'ambito e la gravità delle minacce, al fine di avviare le azioni necessarie a interromperle e neutralizzarle. Dal momento dell'ingaggio, il nostro YIR supporta gli operatori di sicurezza che presidiano l'infrastruttura sotto attacco, fornendo consulenza in ogni fase del processo di risposta: rilevamento, contenimento, eradicazione e gestione della crisi.

Il Report

Lo scopo di questo documento è tracciare una panoramica sul contesto delle cyber minacce che hanno investito il nostro Paese ed effettuare una valutazione sui trend e le azioni di mitigazione necessarie a ridurne gli impatti. Il report si riferisce al periodo luglio 2020 – giugno 2021 e rappresenta un documento dinamico, aggiornato su base annuale in modo da costruire una serie storica di dati raffrontabili.

Il Metodo

Il documento restituisce una elaborazione dei dati ricevuti e analizzati dal SOC di Yarix nel periodo di riferimento. Le informazioni provengono dal panel specifico delle aziende monitorate dal SOC e corrispondenti alla base dei clienti di Yarix, nella quale trovano espressione, in maniera trasversale, i diversi settori dell'economia nazionale. Le imprese rappresentate nel panel analizzato occupano, in media, oltre il migliaio di addetti e sviluppano fatturati superiori ai 50 milioni di euro. I dati sono stati normalizzati statisticamente e resi omogenei in modo da poter essere utilizzati come output quantitativo fondato e utile a supportare considerazioni qualitative. Tutti i dati raccolti sono stati automaticamente anonimizzati e aggregati per finalità di privacy, rimuovendo qualsiasi collegamento tra le informazioni raccolte e le imprese coinvolte.

Il report è suddiviso in due sezioni:

// SEZIONE QUANTITATIVA
Riporta il numero degli eventi di sicurezza registrati dal SOC, evidenziando quanti siano evoluti in veri e propri attacchi da gestire e quali siano stati i comparti più colpiti. A queste domande, il report risponde attraverso dati raccolti ed elaborati dagli analisti Yarix, a partire da un panel rappresentativo dei diversi settori economici italiani e che nello specifico comprende i comparti:

- Finanziario
- Assicurativo
- Fashion
- Automotive
- Trasporti
- Industriale/siderurgico
- Food and beverage
- IT System Integrator
- Infrastrutture Critiche
- Gaming
- Sanitario

// SEZIONE QUALITATIVA
Analizza in maniera oggettiva e informata i dati raccolti nella precedente sezione, per identificare indici di andamento e anomalie.
Nella sezione conclusiva vengono identificati i principali trend del periodo analizzato e le relative contromisure volte alla mitigazione delle problematiche rilevate.
Viene inoltre fatto un approfondimento sugli attacchi informatici che caratterizzano in modo significativo l'attuale panorama nazionale e internazionale della cyber security.

1. Dati analizzati

I dati analizzati in questo report relativo alla seconda parte del 2020 e inizio del 2021 sono relativi a circa 57 mila eventi di sicurezza

I dati analizzati in questo report sono relativi ai circa **57 mila eventi di sicurezza** rilevati dai sistemi di monitoraggio messi in opera dal SOC di Yarix.
Gli analisti di Yarix hanno successivamente analizzato questa base di dati, integrandola e correlandola con ulteriori informazioni di **Threat Intelligence**, derivanti da fonti interne e da collaborazioni con istituzioni, enti e altre aziende. Non da ultimo, il presente documento di analisi tiene conto delle notizie provenienti dal circuito **FIRST** (Forum for Incident Response and Security Teams), la comunità internazionale più estesa e autorevole per la prevenzione e la gestione congiunta di incidenti di sicurezza.

2. Analisi quantitativa

L'analisi quantitativa dei dati è stata eseguita analizzando il campione secondo diverse aggregazioni

L'analisi quantitativa dei dati è stata eseguita analizzando il campione secondo diverse aggregazioni e, in alcuni casi, ha richiesto l'introduzione di metodologie di rimozione di bias statistici, dovuti alla presenza di un maggior numero di aziende o di aziende di dimensioni maggiori in uno specifico settore piuttosto che in un altro.

2.1 Eventi e incidenti di sicurezza

La differenza tra evento e incidente di sicurezza è sottile e, talvolta, porta a generare confusione e fraintendimenti relativamente ai dati in analisi. Per completezza riportiamo nel seguito le definizioni che abbiamo utilizzato per i due termini, che saranno valide per tutto il prosieguo del report.

// Evento di sicurezza
Un evento di sicurezza informatica è un'occorrenza identificata dello stato di un sistema, di un servizio o di una rete informatica, che indica una possibile violazione dei livelli di sicurezza informatica definiti, oppure una situazione sconosciuta che può essere rilevante per la sicurezza del patrimonio informativo e degli asset aziendali.

// Incidente di sicurezza
Evento, o una catena di eventi, conseguente ad un'azione, intenzionale o accidentale, svolta nell'ambito del Sistema Informatico controllato, che può causare la perdita di riservatezza, integrità o disponibilità dei dati aziendali e dei servizi erogati dagli asset informatici protetti, nonché l'utilizzo di asset al fine di commettere illeciti o arrecare danni verso terzi, in violazione a disposizioni aziendali e/o legislative.

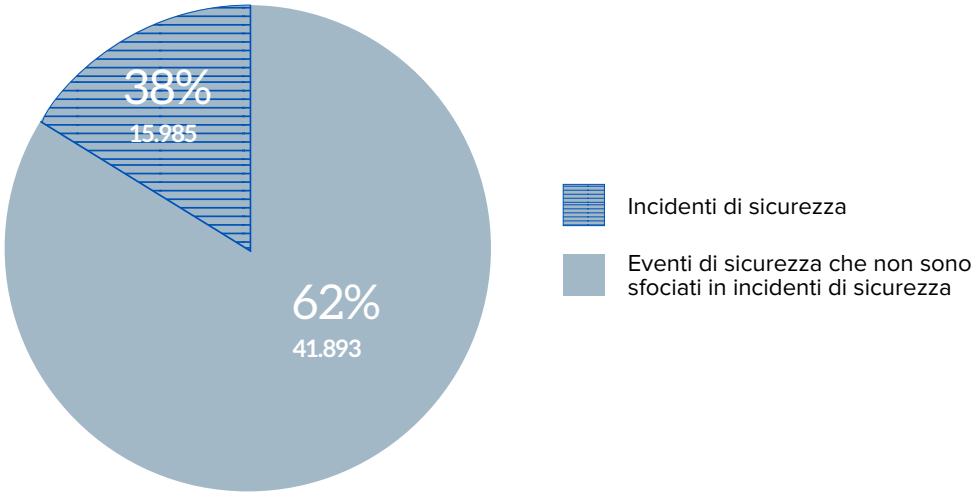
A titolo esemplificativo e non esaustivo, gli eventi di sicurezza analizzati consistono in:

- eventi riconducibili a codici malevoli/malware;
- sfruttamento di vulnerabilità note;
- presenza di sistemi collegati a Botnet;
- esfiltrazione di dati;
- intrusioni;
- compromissione di sistemi e/o applicazione e/o servizi;
- attacchi DoS/DDoS;
- modifica o cancellazione non autorizzata di dati;
- invio di mail di phishing;
- comunicazione con IP, domini, URL riconducibili ad attività malevole.

Gli eventi analizzati **in totale sono 57.878**, di cui **15.985** si sono **evoluti in incidenti di sicurezza**, di diversa criticità (*fig. 1*).

Figura 1

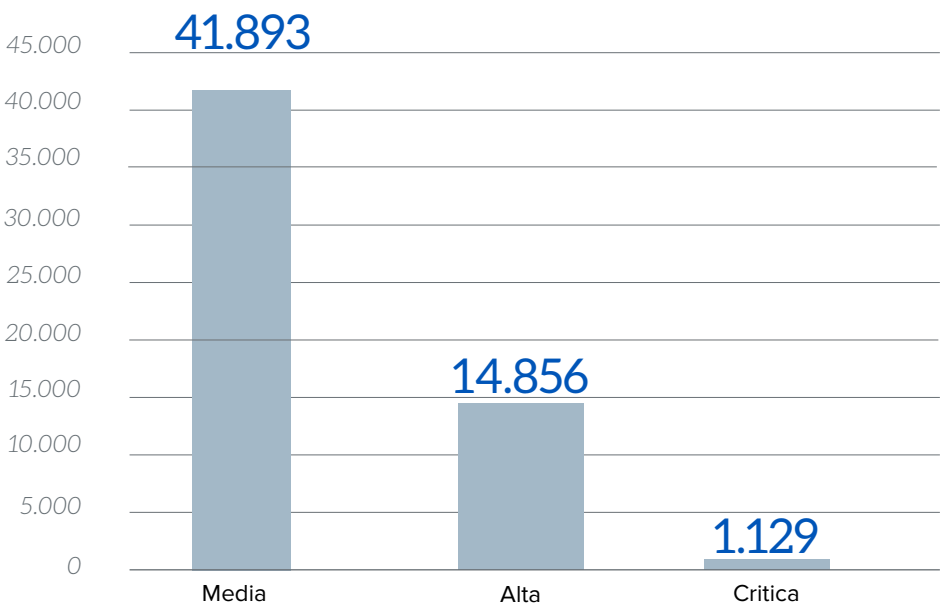
Eventi totali analizzati



La criticità degli eventi e degli incidenti viene calcolata sulla base delle indicazioni contenute nel manuale operativo dei singoli clienti del servizio, e definita secondo le metriche e le procedure concordate, basate su **standard nazionali e internazionali**. Questa classificazione permette di allineare le tipologie e le criticità degli incidenti rilevati per i singoli clienti nella seguente infografica (*fig. 2*).

Figura 2

Eventi suddivisi per gravità



Per gli eventi di **gravità "critica"** (*fig. 2*) è stato validato il passaggio a incidente di sicurezza e in questi casi alle attività di analisi sono seguite anche **attività di Emergency Response** compiute dal **team YIR** di Yarix. Il team ha supportato il cliente nella gestione dell'incidente, nella risoluzione e nella successiva analisi post-incidente, al fine di rilevare l'origine della compromissione o dell'attacco, i possibili danni collaterali e attività persistenti messe in campo dall'attaccante.

Le attività di Emergency Response consistono nel supporto al cliente nella gestione dell'incidente di sicurezza. Il suo scopo è l'identificazione, l'analisi e la classificazione, secondo priorità, degli eventi di sicurezza e la definizione delle procedure da adottare in risposta alla conferma di avvenuto incident, fino al ripristino della normale operatività, salvaguardando la possibilità di effettuare un'analisi forense dettagliata successiva. Garantisce inoltre un miglioramento dei controlli, grazie alla lesson learned, prevenendo o comunque limitando le conseguenze in caso di ripetersi dello stesso accadimento.

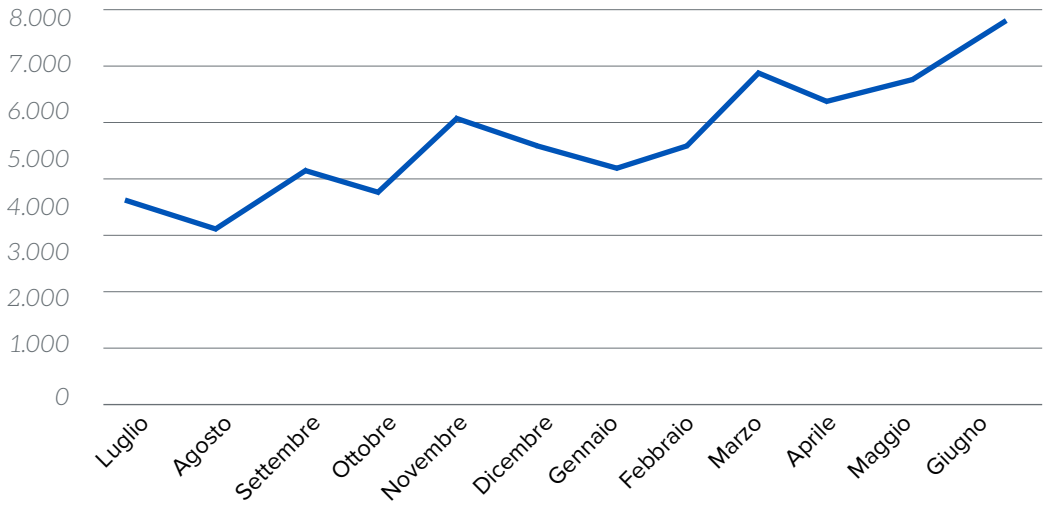
In particolare, a fronte di una segnalazione di Incidente Informatico, vengono eseguite una serie di azioni:
• **Assistere** i soggetti coinvolti nella gestione degli incidenti di sicurezza
• **Rispondere** alle segnalazioni di incidenti, avvertendo i soggetti coinvolti e seguendone gli sviluppi
• **Diffondere** informazioni sulle vulnerabilità più comuni e sugli strumenti di sicurezza da adottare
• **Assistere** i soggetti coinvolti nella realizzazione di misure preventive ritenute necessarie per la riduzione a livelli accettabili del rischio di incidenti
• **Emanare** direttive sui requisiti minimi di sicurezza per le macchine con accesso alla rete, verificandone il rispetto
• **Gestire** corsi di aggiornamento tecnico, a tutti i livelli, e in particolare per gli utenti finali
• **Mantenere aggiornati** allo stato dell'arte gli strumenti e le metodologie per la sicurezza

• **Testare** metodologie/strumenti esistenti e svilupparne di nuovi per esigenze specifiche.

Il trend degli eventi complessivi analizzati gestiti durante il primo semestre del 2021 ha visto un costante rialzo in linea con i primi mesi del 2020. (fig.3)

Figura 3

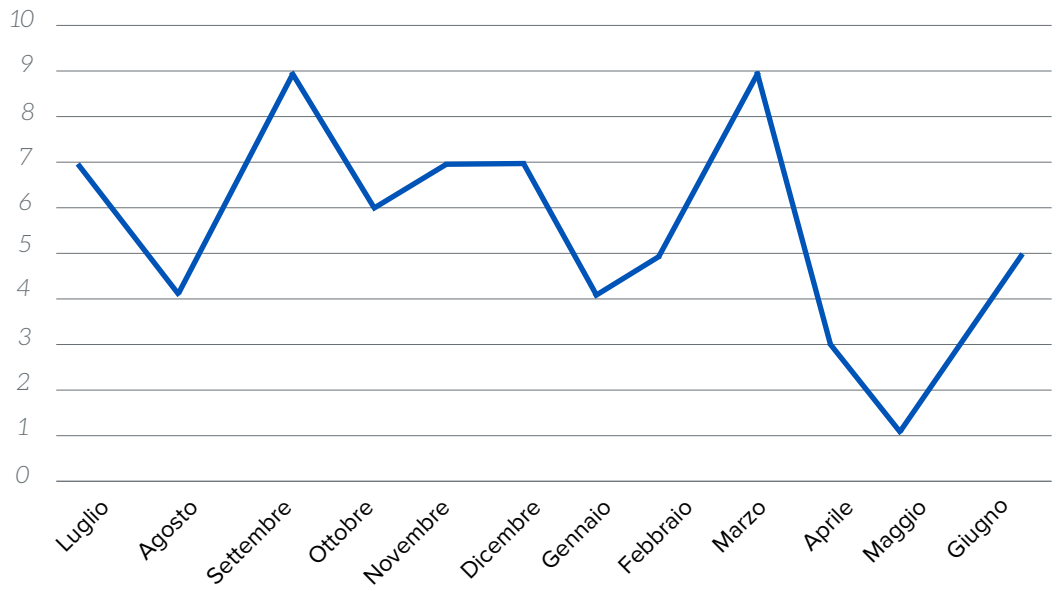
Distribuzione temporale degli eventi nel 2020 H2 - 2021 H1



Il trend degli eventi complessivi analizzati gestiti durante il primo semestre del 2021 ha visto un costante rialzo in linea con i primi mesi del 2020. Per quanto riguarda gli eventi di gravità critica, invece, si è registrato un andamento pressoché costante, con una media di cinque eventi al mese (fig. 4).

Figura 4

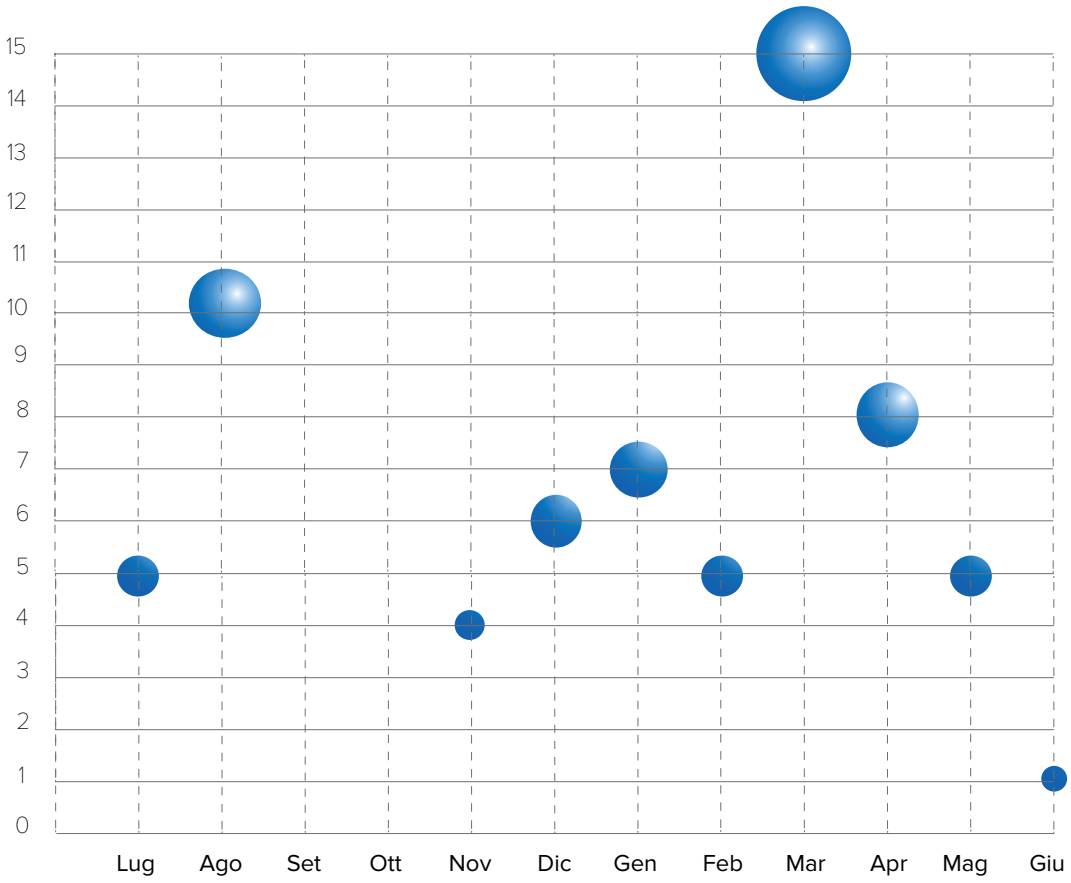
Distribuzione temporale degli eventi di gravità critica nel 2020 H2 - 2021 H1



Un trend diverso è invece quello relativo agli **attacchi informatici gestiti dal team di YIR**. A differenza degli incidenti critici gestiti dal SOC, dove l'attività proattiva ha permesso la gestione dell'incidente senza impatti particolarmente dannosi per l'infrastruttura monitorata, gli incidenti gestiti dal team YIR coinvolgono sempre realtà che si trovano al di fuori del perimetro di monitoraggio del Security Operation Center di Yarix e che sono state, parzialmente o totalmente, compromesse da un attacco informatico (*fig. 5*).

Figura 5

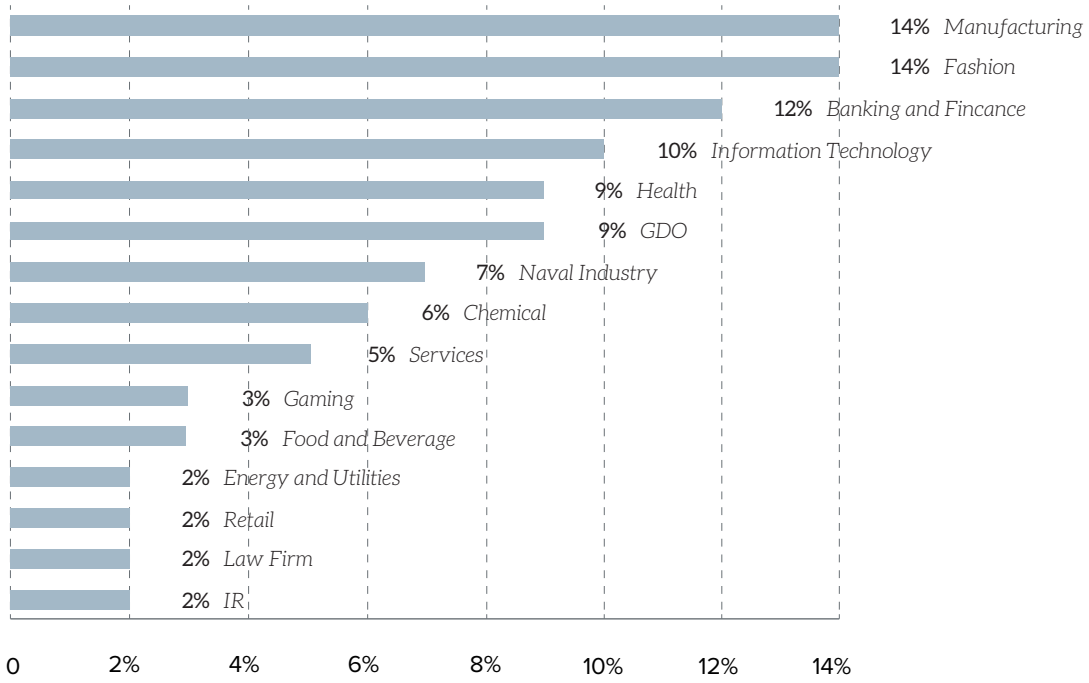
Distribuzione temporale degli eventi gestiti dal team IR nel 2020 H2 - 2021 H1



In seguito, l'analisi si è concentrata sulla tipologia di settore industriale impattato, tenendo presente che tale categorizzazione viene fortemente condizionata dal campione preso in esame che, come anticipato, è identificato dai clienti che usufruiscono del servizio SOC di Yarix. Per tale motivo sono state fatte delle considerazioni di tipo statistico che verranno descritte nella sezione successiva (*fig. 6*).

Figura 6

Eventi di sicurezza suddivisi per settore industriale



Nel periodo analizzato il settore più colpito è quello del **Manufacturing** (14%) e **Fashion**, (14%), seguito da **Banking and Finance** (12%) **Information Technology** (10%). Di particolare interesse è anche l'aumento significativo registrato dal settore **Health** (9%).

2.1.1 Cyber Threat Intelligence

Il team YCTI (Yarix – Cyber Threat Intelligence) ha riportato un totale di **423 eventi** significativi, di cui:

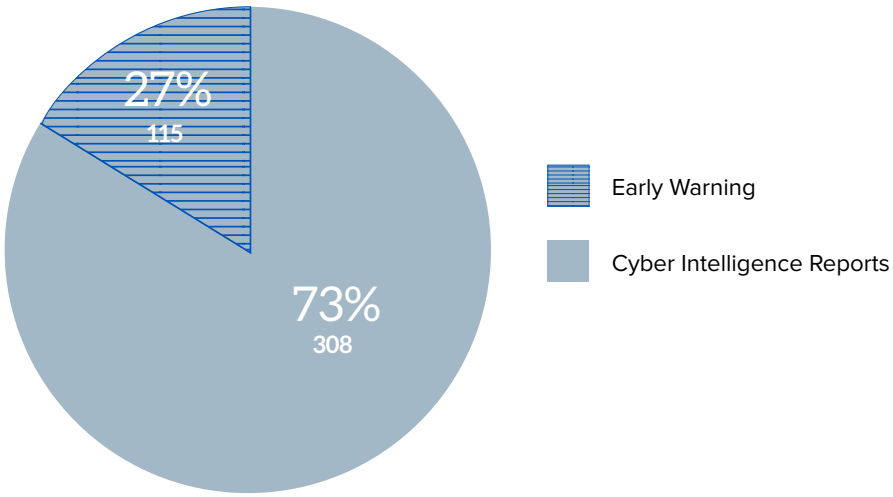
- 308 eventi di Cyber Intelligence e Data Leakage
- 115 eventi di Early Warning

A titolo esemplificativo e non esaustivo, gli eventi CTI analizzati consistono in:

- eventi riconducibili a vendita di credenziali / accessi compromessi su Deep Web / Dark Web
- eventi su vulnerabilità critiche e vulnerabilità 0-day attivamente sfruttate dai TA (Threat Actor)
- eventi riconducibili a data breach, data leak o vendita di informazioni e dati confidenziali su Deep Web / Dark Web.
- eventi di impatto importante o critico emersi a seguito di attività OSINT / HUMINT.

Figura 7

Eventi totali analizzati



Per ogni evento CTI (423), il team YCTI ha fornito un report di segnalazione specifico, supportando il cliente nella gestione dell'incidente, fornendo le evidenze raccolte, suggerendo le corrette contromisure e le azioni di mitigazione/remediation.
Durante il periodo di riferimento sono stati identificati dagli analisti del team YCTI circa **163 mila host compromessi da malware**, dai quali sono state rubate ed esfiltrate **oltre 9 milioni di credenziali.**

Di seguito è riportata la distribuzione temporale degli eventi significativi gestiti dal team YCTI , nel quale si evidenzia un trend di picco negli ultimi mesi dell'anno a seguito di un aumento di data breach.

Figura 8
Distribuzione temporale degli eventi gestiti dal team YCTI nel 2020 H2 - 2021 H1

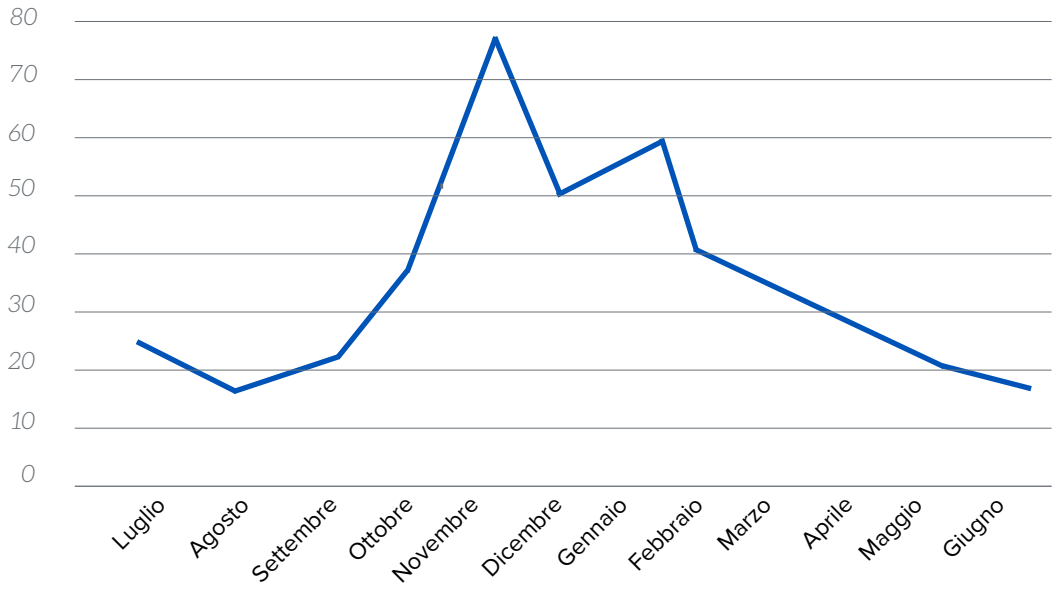
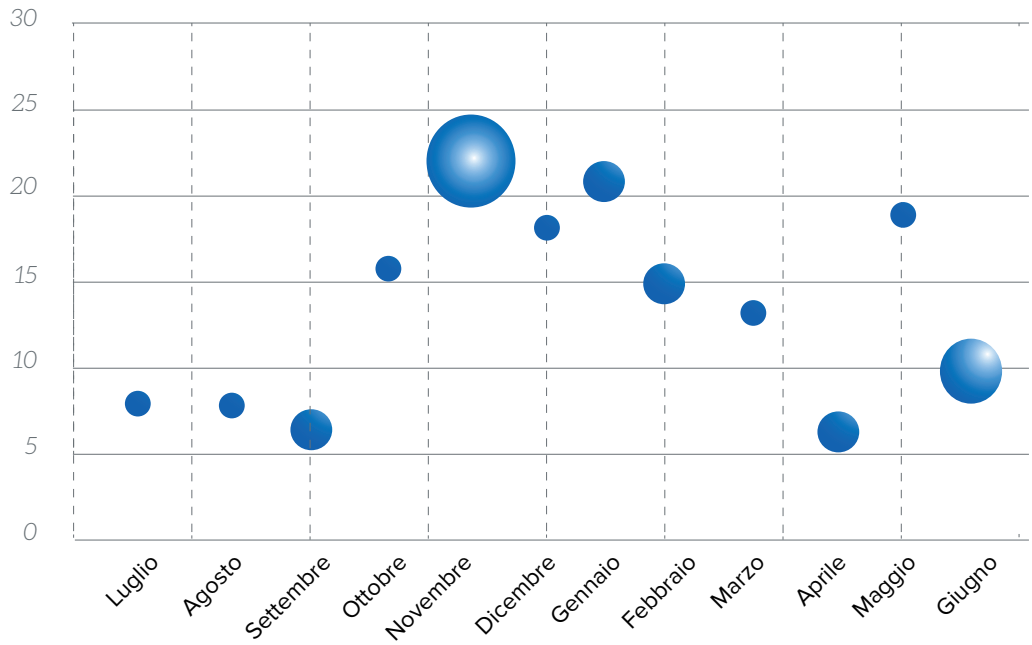


Figura 9
Distribuzione temporale dei data breach analizzati e gestiti dal team YCTI nel 2020 H2 - 2021 H1



3. Analisi qualitativa

Quadro analitico degli attacchi identificati dal SOC di Yarix, sulla base del metodo illustrato

Le informazioni presenti in questa sezione tracciano il quadro analitico degli **attacchi identificati dal SOC di Yarix**, sulla base del metodo illustrato in premessa.

3.1 Trend dei dati analizzati

I temi evidenziati dai dati raccolti dal SOC durante il secondo semestre del 2020 e il primo semestre del 2021 sono riportati di seguito:

// TREND 1 - Compromissione di utenze
Nel periodo osservato si evidenzia un trend di attacco che prevede l'utilizzo sempre più frequente di utenze compromesse da parte degli attaccanti, con un notevole aumento della difficoltà per gli analisti di sicurezza nell'individuazione dell'attività malevola. Infatti, gli attori malevoli utilizzano spesso credenziali valide di utenti autorizzati per eseguire il primo accesso all'infrastruttura target, diminuendo al minimo le attività di ricognizione che possono essere utili ai processi di rilevazione eseguite dal team SOC. Tali credenziali sono spesso ottenute tramite attacchi phishing eseguiti verso i dipendenti aziendali o tramite compravendite delle stesse su canali underground del dark web.

// TREND 2 - Sfruttamento di vulnerabilità note
Durante il periodo di osservazione di questo report, e specialmente nel primo semestre dell'anno in corso, si sono sviluppate vere e proprie campagne di sfruttamento di vulnerabilità note che permettevano agli attaccanti di avere accesso in modo relativamente semplice al perimetro aziendale. Alcuni esempi, tra i più eclatanti, sono i seguenti:

- **CVE 2020-12271**: SQL Injection su firewall Sophos
- **CVE-2018-13379**: Leak di credenziali su firewall Fortigate
- **CVE-2021-26855**: vulnerabilità Proxylogon su server Exchange

Queste vulnerabilità sono state utlizzate massivamente da parte di gruppi di attaccanti (Threat Actor) per ottenere credenziali valide per accessi remoti all'infrastruttura o per posizionare strumenti di accesso remoto da utilizzare in un secondo momento per portare a termine la loro attività malevola.
Ne è un esempio lampante il numero di incidenti avvenuti a marzo 2021, legati all'ultima CVE elencata.

// TREND 3 - Il valore dell'intelligence
Nel mondo del cybercrime si evidenzia un trend in costante aumento relativo al furto di credenziali e alla messa in vendita di informazioni confidenziali.
La maggior parte degli attacchi ha l'obiettivo di esfiltrare le informazioni sensibili e confidenziali per rivenderle nel Dark Web e nei canali underground specializzati nella compravendita

di informazioni. E' sempre più importante monitorare attivamente l'esposizione della propria organizzazione sui canali underground specializzati in cybercrime, per individuare la messa in vendita di credenziali compromesse o il furto di dati avvenuto in modo silente.

Nel periodo di riferimento, il team YCTI ha notificato in modo preventivo a oltre 100 organizzazioni italiane eventi di intelligence relativi ad attacchi imminenti verso l'organizzazione vittima del furto di dati o della compromissione di credenziali amministrative, in seguito messe in vendita nel mercato del cybercrime, pronte a essere opportunamente utilizzate da attori ransomware.

4. Focus: Dalla vendita all'attacco

Trend in aumento relativo alla vendita di accessi di tipo corporate sul Dark Web / Deep Web

Nel mondo del cybercrime si evidenzia un costante trend in aumento relativo alla vendita di accessi di tipo corporate sul Dark Web / Deep Web.
Le principali tipologie di accesso osservate da parte del team YCTI sul Dark Web / Deep web sono le seguenti:

- Accessi VPN
- Accessi RDP / RDPWEB
- Accessi a infrastrutture compromesse da vulnerabilità critiche (Citrix, Microsoft Exchange, Fortigate, Vmware, Pulse Secure, F5 Big-IP)

Si osservano principalmente due metodologie di vendite differenti da parte dei threat actor:

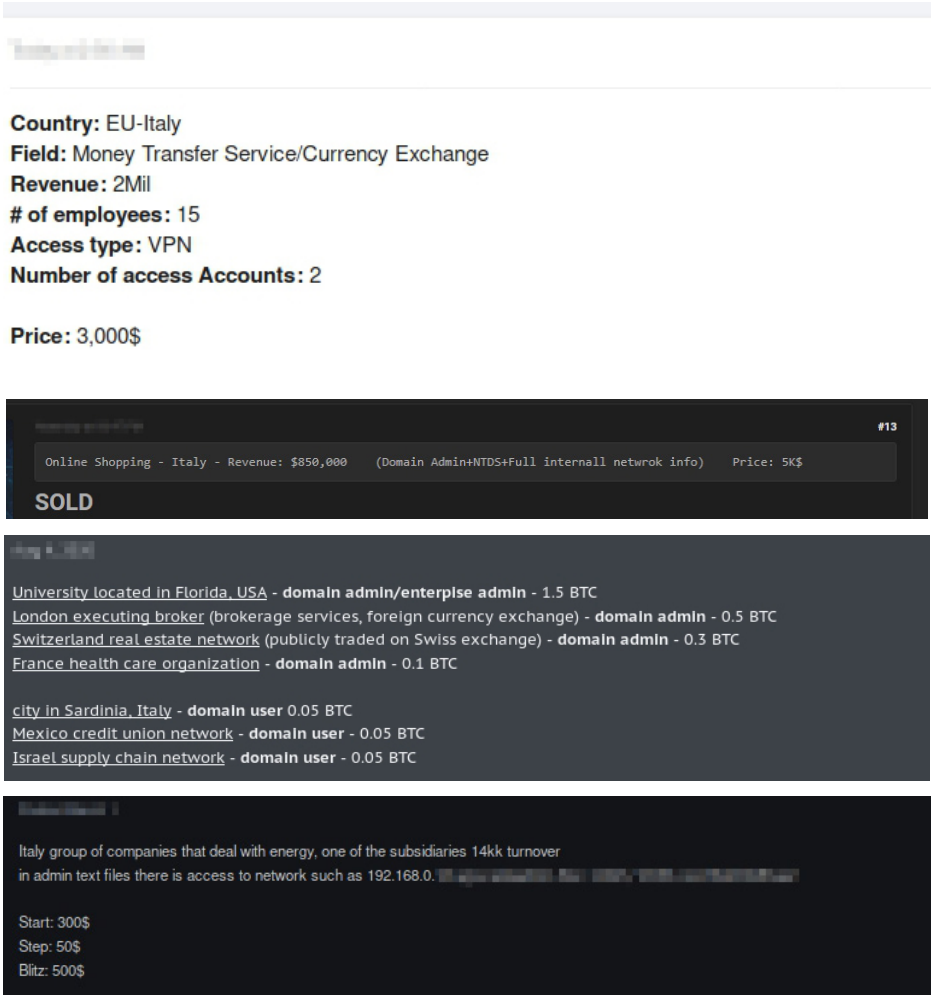
- vendita semplice
- vendita con attività di compromissione già avviata

Le due metodologie di vendita si differenziano, oltre che per il costo, anche per le informazioni fornite dal threat actor o access broker.
Nel primo caso, il threat actor **effettua la vendita** della credenziale compromessa senza svolgere nessuna ulteriore attività limitandosi quindi a fornire le credenziali valide per l'acceso all'interno dell'azienda target.
Nel secondo caso, il threat actor **fornisce un accesso completo** all'azienda vittima: questo signfiica che potenzialmente può fornire uno o più accessi con privilegi amministrativi (local admin, domain admin etc..) o fornire una backdoor con privilegi amministrativi all'interno dell'infrastruttura dell'azienda vittima.

Per quanto riguarda questa seconda metodologia più completa, il threat actor, per fornire informazioni aggiuntive nella vendita, svolge i seguenti step all'interno dell'infrastruttura vittima:

- Attività di ricognizione (reconnaissance)
- Privilege escalation
- Lateral movement

Di seguito alcuni esempi di aste/vendite che hanno coinvolto target italiani:



5. Focus: Supply Chain Attack

Nel panorama dei cyber attacchi ha preso piede una nuova tipologia di compromissione

Nel corso del 2021 nel panorama dei cyber attacchi ha preso piede una nuova tipologia di compromissione, definita dallo sfruttamento di canali di accesso privilegiati all'infrastruttura target dell'attacco: quelli della Supply Chain. Questa tipologia di attacchi prevede dunque una compromissione che avviene in almeno due fasi: una prima fase di compromissione del "fornitore" e una seconda fase di compromissione dell'anello successivo della catena di fornitura (questo può essere l'utilizzatore finale o un fornitore intermedio).
Il motivo per cui questa tipologia di attacchi rappresenta un rischio elevatissimo per le infrastrutture target è che sfrutta una componente insita nella maggior parte dei rapporti di fornitura, cioè il trust che c'è tra fornitore e utilizzatore del servizio. Il trust può essere presente sia sotto forma di rapporto contrattuale, sia basato su una fiducia insita nel servizio o nel software stesso, dettata dal brand del fornitore o da rapporti di fiducia personali con il fornitore medesimo.

Quando viene declinato nell'ambito degli attacchi informatici, l'attacco alla Supply Chain è essenzialmente di due tipologie:

1. **Compromissione di un fornitore di servizi**
2. **Compromissione di un software**

Nel primo scenario, la compromissione avviene primariamente su una società di fornitura di servizi informatici, la quale ha per sua natura e per esigenze lavorative accessi privilegiati alle infrastrutture informatiche dei loro clienti (o almeno a quella porzione sulla quale erogano i servizi di assistenza). Tali accessi vengono utilizzati come una sorta di testa di ponte per poi procedere con la seconda fase dell'attacco, seguendo le metodologie standard descritte anche nelle versioni precedenti di questo report. Il vantaggio di un attaccante è che, compromettendo una singola organizzazione, si trova a disposizione un certo numero di accessi validi alle aziende clienti di quella realtà, potendo massimizzare il profitto con attacchi mirati ed orchestrati verso queste ultime. A questo spesso si aggiunge un ulteriore e ormai "classico" secondo ricatto, cioè quello dovuto all'esfiltrazione di dati e al danno reputazionale legato alla pubblicazione di informazioni relative a contratti, clienti e know how aziendale.

Nel secondo scenario, la compromissione sfrutta la presenza di software largamente diffuso all'interno delle realtà aziendali con la finalità di poter utilizzare questi ultimi come vettori del payload malevolo dell'attaccante. In questo caso il trust è implicito nella presenza del software stesso e non sono rare le situazioni in cui tali software siano oggetto di whitelist sui sistemi di protezione dell'endpoint, al fine di consentirne il corretto funzionamento.

Il caso più eclatante, avvenuto nel mese di luglio 2021, riguarda la compromissione del software per la gestione degli endpoint Kaseya[1] : il giorno 2 luglio (il venerdì precedente al weekend della festa d'indipendenza negli USA) è stato registrato un attacco su scala globale assegnato al noto gruppo di cyber criminali REvil. L'attacco ha portato alla cifratura simultanea di un numero di aziende che si aggira tra le 800 e le 1500 unità, causando disservizi in tutto il mondo, Italia compresa.
Vista la sua portata, questo attacco ha coinvolto anche enti governativi e leader di stati come USA e Russia, per identificare una soluzione comune alla situazione di compromissione diffusa. Questo ha portato, il 23 luglio, al rilascio di una chiave di decifratura universale, che ha permesso alle aziende colpite di recuperare i dati che erano stati cifrati durante l'attacco.

6. Conclusioni

Il periodo di osservazione relativo al secondo semestre del 2020 e al primo semestre del 2021 disegnano una situazione di crescita complessiva per quanto riguarda gli attacchi rivolti verso le realtà oggetto di analisi

Le evidenze fornite dal report per il periodo di osservazione relativo al secondo semestre del 2020 e al primo semestre del 2021, disegnano una situazione di crescita complessiva per quanto riguarda gli attacchi rivolti verso le realtà oggetto di analisi, sia per l'ambito dei clienti SOC che per le realtà che subiscono incidenti informatici, in quanto non dispongono di un presidio di sicurezza continuativo.

Un secondo elemento significativo che emerge dai dati analizzati, riguarda la diffusione degli attacchi informatici in modo pressoché uniforme sui diversi settori industriali, con la mancanza di un settore che rappresenti un target preferito rispetto ad altri per gli attacchi registrati dal SOC; questo è riconducibile a una modalità di approccio tenuta dai gruppi di attori malevoli che hanno posticipato la fase di studio del target in un momento successivo alla compromissione. Infatti, mentre in precedenza la fase di raccolta informazioni era da considerarsi come propedeutica all'attacco, ad oggi si rileva che queste attività vengono svolte quando il primo accesso al perimetro aziendale è già avvenuto. In questo modo gli attaccanti possono massimizzare i profitti, tarando effort e richieste di riscatto sulla reale dimensione dell'azienda.

Da questo si evince che nessuna realtà può considerarsi esente dai rischi derivanti da un attacco informatico, poiché anche le realtà più piccole possono essere soggette ad attività malevole che possono comportare importanti disservizi.

Altro tema importante evidenziato dal presente report è relativo alla vendita di credenziali, sempre più frequente su mercati underground e che rappresenta un rischio potenzialmente molto elevato per le aziende oggetto dell'attacco ma, allo stesso tempo, un'opportunità per le stesse di anticipare tali problematiche attivando un monitoraggio continuo tramite servizi di Cyber Threat Intelligence sulle comunicazioni che

[1] https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack

avvengono tra potenziali acquirenti e i possessori delle credenziali.

In conclusione, gli attacchi di tipo Supply Chain rappresentano un rischio molto elevato per le aziende, poiché sfruttano un canale di compromissione che è di per sé considerato come trusted. Tuttavia, come per tutte le tipologie di attacchi, esistono delle contromisure che possono essere applicate per ridurre questo rischio. Tra queste si possono annoverare la corretta gestione dei privilegi degli utenti e delle applicazioni, una segregazione opportuna della rete aziendale interna e un adeguato monitoraggio di sicurezza per identificare il prima possibile eventuali compromissioni del perimetro aziendale.


YARIX
a vargroup company