YARIX
a varonis company

YSOC SECURITY REPORT

H2 2019

YARIX
a vargroup company

Sommario

Introduzione

Il documento restituisce una elaborazione dei dati ricevuti e analizzati dal SOC di Yarix nel periodo luglio-dicembre 2019

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

Parte di **Var Group**, in qualità di 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: un bunker informatico dotato di misure di sicurezza fisica e biometrica di ultima generazione, basato su forme computazionali predittive e cognitive. Attivo 24 ore su 24 – grazie al presidio di un team di 27 esperti di sicurezza informatica – permette alle aziende di accedere a servizi di security, business continuity e disaster recovery in modo da rispondere efficacemente all'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 di 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.

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-dicembre 2019** e rappresenta un documento dinamico che sarà aggiornato su base semestrale 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**
Riporterà 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 risponderà 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**
Analizzerà in maniera oggettiva e informata i dati raccolti nella precedente sezione, per identificare indici di andamento e anomalie.

Nella **sezione conclusiva** verranno identificati i principali trend del periodo analizzato e le relative contromisure volte alla mitigazione delle problematiche rilevate.

Sarà inoltre riportato un **caso reale** riguardante un **attacco informatico verso una delle più importanti aziende di produzione italiane**, in seguito al quale il team di Yarix ha fornito supporto per il contenimento dell'incidente.

1. Dati analizzati

I dati analizzati in questo report sono relativi a circa 19 mila eventi di sicurezza

I dati analizzati in questo report sono relativi ai **circa 19 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 e l'introduzione di metodologie di rimozione di bias statistici

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.

2.1 Eventi e incidenti di sicurezza

La differenza tra evento ed 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 proseguo 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 catena di eventi, conseguente a 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.

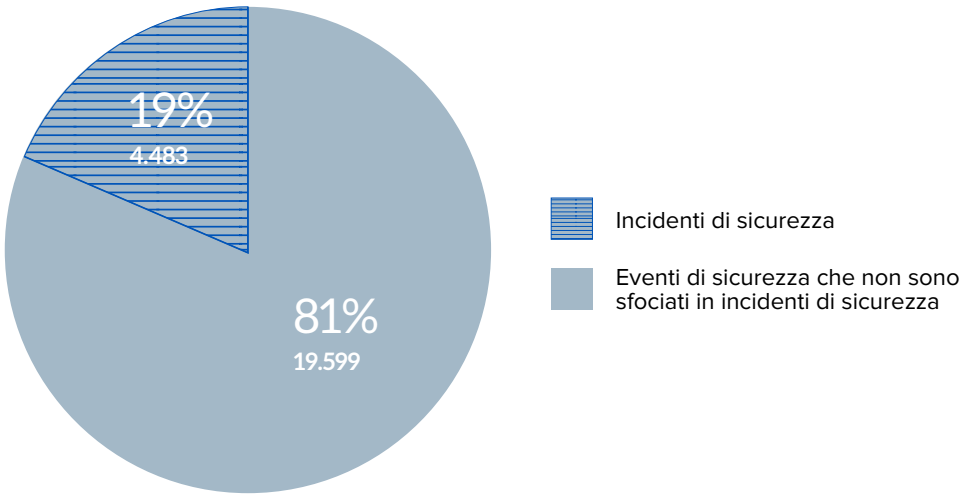
A titolo esemplificativo e non esaustivo, gli eventi di sicurezza analizzati consistono in:

- 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 e-mail di phishing
- Comunicazione con IP, domini, URL riconducibili ad attività malevole.

Gli eventi analizzati **in totale sono 19.599**, di cui **4.483 si sono evoluti in incidenti di sicurezza**, di diversa criticità *(fig.1)*.

Figura 1

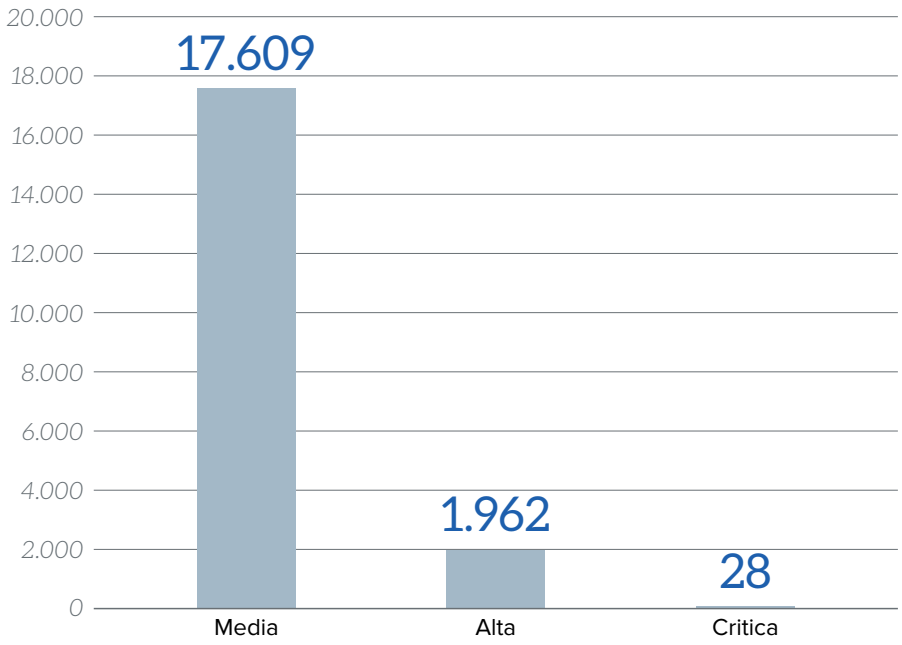
Eventi totali analizzati



La criticità degli eventi 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 *(fig.2)*.

Figura 2

Eventi suddivisi per gravità



Per gli **eventi di gravità "critica"** è stato validato il passaggio ad incidente di sicurezza e in questi casi alle attività di analisi sono seguite anche **attività di Emergency Response** compiute dal YCERT 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 cui 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, in particolare per gli utenti finali;

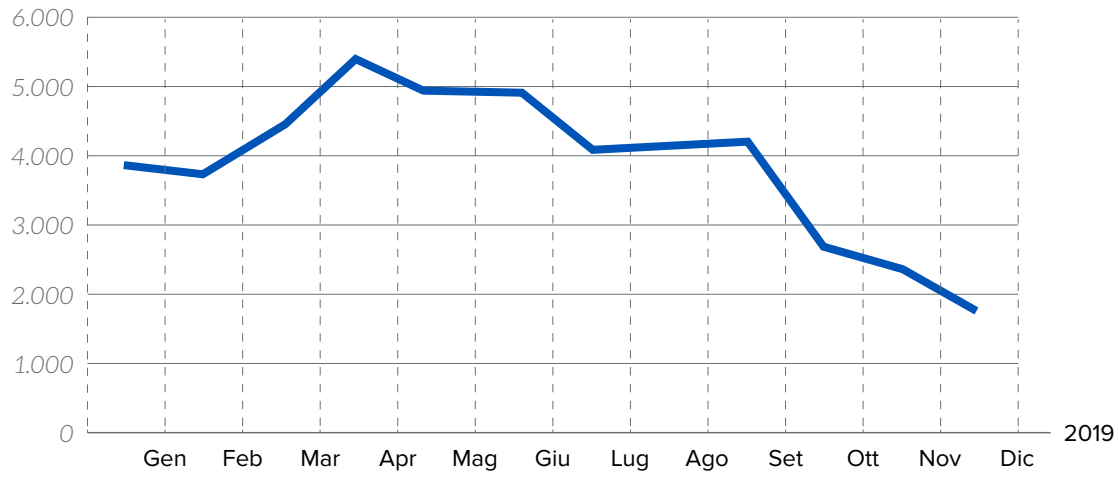
• **Mantenere aggiornati** allo stato dell'arte gli strumenti e le metodologie per la sicurezza;

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

Il trend degli eventi gestiti da parte del SOC ha subito un aumento significativo nei mesi di marzo e aprile, come già intravisto nel report relativo al primo trimestre *(fig.3)*.

Figura 3

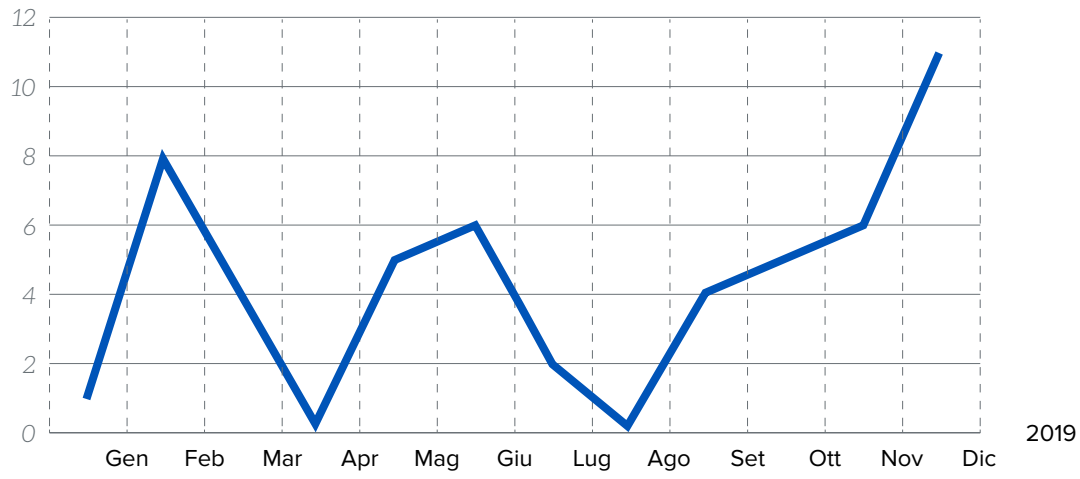
Distribuzione temporale degli eventi



Il trend degli eventi complessivi analizzati gestiti durante il 2019 ha visto una sostanziale diminuzione nell'arco dell'ultimo quadrimestre. Tuttavia, come si evince dal grafico successivo, la diminuzione complessiva è stata accompagnata da un **aumento costante degli incidenti di sicurezza di gravità critica**. Per tali eventi rilevati dal SOC è stato necessario l'ingaggio del team YCERT che si è occupato delle attività di Incident Response, andando a mitigare sul nascere eventi che altresì avrebbero potuto comportare un danno ingente alle aziende oggetto degli attacchi *(fig.4)*.

Figura 4

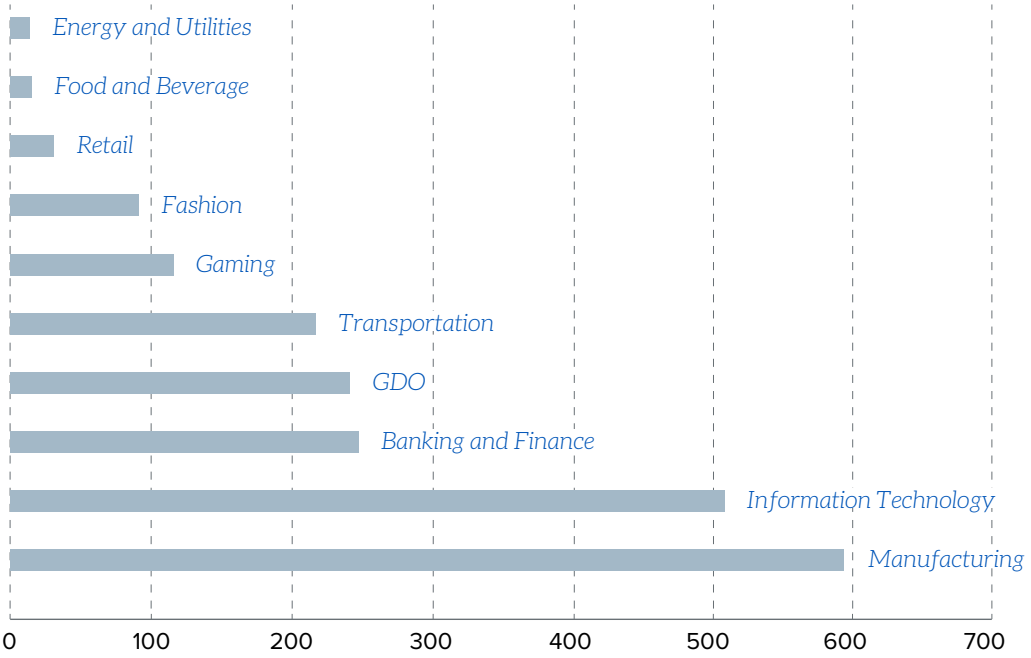
Distribuzione temporale degli eventi critici



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.5)*.

Figura 5

Eventi di sicurezza suddivisi per settore industriale



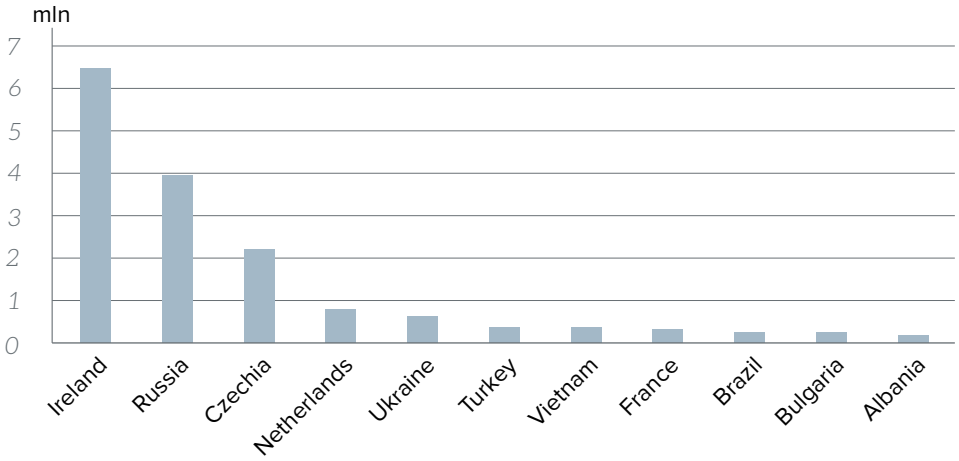
Come evidenziato nei precedenti periodi temporali oggetto di analisi, il settore **Manufacturing** rimane il **più colpito** dagli attacchi, seguito dal settore **IT** e da quello **Banking and Finance**. Da sottolineare, all'interno di questo report, il considerevole aumento del settore **Gaming, aumentato del 50% rispetto al semestre precedente**.

2.2 Threat Intelligence

Grazie alla rete di honeypot diffusa su varie aree geografiche del territorio mondiale, le informazioni raccolte dal perimetro di clienti del SOC vengono arricchite con informazioni di contesto relative ad indicatori di compromissione (IOC) e scenari di rischio aggiuntivi, derivanti dall'analisi eseguita sugli artefatti rilasciati dagli attaccanti. Riportiamo nel seguito le indicazioni relative alla geolocalizzazione degli attacchi *(fig.6)*.

Figura 6

Geolocalizzazione delle minacce



I dati raccolti nel secondo semestre del 2019 hanno evidenziato una **riduzione complessiva del numero di eventi raccolti dalla honeypot**. Tale diminuzione complessiva è dovuta alla drastica riduzione negli ultimi due mesi dell'anno degli eventi provenienti dalla botnet irlandese, che aveva contribuito maggiormente nei mesi precedenti all'aumento delle attività malevole raccolte.

La maggior parte delle infezioni rilevate in questo contesto continua a sfruttare, come nei mesi precedenti, servizi esposti (in questo caso volutamente, ma nei contesti aziendali potrebbe non essere così). I **maggiori servizi colpiti sono SSH, RDP e SMB**, sui quali vengono sfruttate vulnerabilità note o attacchi di tipo bruteforce per ottenere accesso al sistema.

A maggior ragione, nel periodo attuale, va prestata particolare **attenzione a questo tipo di servizi**: infatti l'emergenza sanitaria in atto sta rendendo necessaria l'adozione dello **smart working**. L'esposizione di servizi aziendali, necessaria per consentire tale modalità lavorativa, deve essere fatta prendendo gli opportuni accorgimenti *(link)*.

L'impossibilità per gli utenti di operare presso la normale sede operativa ha reso necessaria l'adozione di procedure e di metodologie di connessione remota alle risorse aziendali. Se in molte realtà questo avveniva già con regolarità prima del problema legato a COVID-19, in altre aziende l'utilizzo delle connessioni remote è un tema completamente nuovo e mai affrontato. Proprio per questo motivo, e per il fatto che l'attivazione si è resa necessaria un un lasso di tempo molto ridotto, si corre il rischio di intraprendere azioni che possono risultare in falle nel sistema di sicurezza aziendale. L'esposizione di servizi interni, l'utilizzo di dispositivi personali per il collegamento alla rete aziendale o l'utilizzo di sistemi non aggiornati sono solo alcuni dei problemi che ci si può dover trovare ad affrontare in questa situazione di emergenza.

2.3 Attacco alle realtà del gaming

Nel periodo tra ottobre e novembre 2019, è stato registrato un **trend di attacchi** rivolti a uno specifico settore industriale, quello del **gaming online**, ossia le aziende che offrono piattaforme di gioco online (slot, poker, scommesse, etc) con eventi che possono raggiungere montepremi di centinaia di migliaia di euro.

In particolare, si sono evidenziati attacchi di tipo DDoS verso importanti realtà afferenti al mondo del gaming, sia italiane che estere.
La peculiarità dell'attacco è data dal fatto che, oltre all'attività standard di DDoS, volta a rendere indisponibile i servizi esposti del cliente, gli attaccanti hanno sfruttato una misconfigurazione di alcuni provider di connettività per compiere un attacco di tipo spoofing.

Gli attaccanti hanno costruito dei pacchetti ad hoc, nei quali hanno sostituito il loro indirizzo IP reale con un indirizzo IP afferente a una delle società di gaming target dell'attacco. Tali richieste venivano dunque indirizzate verso IP casuali su servizi esposti ben noti (come ad esempio servizi web). A questo punto chi riceveva tali richieste, che talvolta erano in numero tale da causare anche un disservizio, vedeva come origine l'IP camuffato dall'attaccante e non quello reale.

Questo tipo di attività, pur non provocando un disservizio diretto alle aziende target dell'attacco, ha creato un duplice danno.

Il primo è quello relativo all'**abbassamento della reputazione degli indirizzi IP pubblici** afferenti all'azienda che, a causa delle massive attività di scansione, sono stati registrati nelle principali blacklist.

Il secondo è dovuto al fatto che molte realtà che hanno ricevuto la scansione dagli IP camuffati, hanno inserito delle regole di blocco sulle loro protezioni perimetrali, rendendo di fatto **irraggiungibili i servizi delle aziende di gaming attaccate** ai loro utenti e viceversa.

Questa tecnica di attacco è molto complicata da contrastare, poiché si basa su una falla nella validazione del traffico in ingresso da parte di alcuni provider.
Questo consente dunque all'attaccante di cambiare l'IP con cui si presenta su Internet e di rendere irriconoscibile questa modifica nei passaggi successivi dell'instradamento del pacchetto, rendendo di fatto impossibile l'attivazione di una mitigazione efficace.

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

L'analisi dei dati relativi al secondo semestre del 2019 e alle evidenze generali emerse durante tutto l'anno mette in evidenza alcuni temi interessanti:

// TREND 1

Il trend relativo agli eventi complessivi rilevati ha visto una flessione nel secondo semestre dell'anno. Questo però è stato accompagnato da una contestuale **crescita degli eventi di gravità critica**, evidenziando una maggiore precisione degli attaccanti e la costruzione di attacchi mirati ed avanzati, che possono potenzialmente avere conseguenze catastrofiche per le aziende colpite.

Gli eventi principali rilevati sono relativi a evidenze di compromissione nelle prime fasi: come evidenziato nel "Caso reale" descritto nel prossimo paragrafo del report, la fase critica dell'attacco viene preceduta da **compromissioni intermedie**. Solo identificandole repentinamente, sarà possibile mitigare l'attacco prima che questo provochi un impatto consistente sull'infrastruttura.

Ovviamente, per poter raggiungere un livello di rilevazione dell'evento sufficientemente rapido, è indispensabile dotarsi di strumenti e procedure che garantiscano un controllo continuativo nell'arco delle 24 ore.

// TREND 2

La seconda considerazione è relativa alla tipologia di attacchi che vengono rilevati dal SOC. Se un tempo buona parte degli attacchi non era riconducibile ad attori definiti, le attività svolte nel secondo semestre del 2019 (e all'inizio del 2020) evidenziano un **modus operandi comune** a diversi gruppi di attaccanti. Ne è sicuramente un esempio il caso reale riportato all'interno di questo report, che non descrive un singolo incidente, ma una serie di eventi simili gestiti su infrastrutture totalmente diverse tra loro. Questo evidenzia una procedura di industrializzazione degli attacchi che permette ai gruppi di cyber criminali di riprodurre in modo relativamente semplice le stesse tecniche su ambienti diversi e di ottimizzare i tempi necessari per la preparazione, messa in opera e gestione dell'attacco stesso.

Un ulteriore tema di attenzione è quello relativo alla **minaccia** da parte degli attaccanti della **diffusione di dati personali** raccolti durante l'esecuzione dell'attacco *(link)*: chi esegue l'attacco ha capito che, in virtù delle regolamentazioni in tema privacy come il GDPR, la diffusione di informazioni sensibili o personali,

riconducibili a un leak perpetrato ai danni dell'azienda, rappresenta una minaccia di una magnitudo **comparabile alla perdita dei dati dovuti alla cifratura**.

// TREND 3
Il terzo trend da sottolineare è relativo all'aumento delle attività malevole rivolte verso il settore del **gaming**. Questo trend è supportato dalle rilevazioni di attività di tipo DDoS corredate da spoofing dell'IP sorgente, che ha causato diversi problemi alle società del settore nel periodo di ottobre-novembre 2019.

Infatti, alla "normale" attività di saturazione delle risorse dovuta ad un attacco di tipo DDoS (Denial of Service distribuito), si è aggiunta un'ulteriore tecnica di attacco che ha causato la diminuzione della reputazione degli indirizzi IP afferenti ad alcune società di gaming. Questa tecnica è difficilmente contrastabile e si basa su una vulnerabilità di alcuni provider internet, i quali non verificano se l'effettiva provenienza del pacchetto che si vuole trasmettere e l'informazione contenuta al suo interno coincidano.

In questo modo un malintenzionato può modificare a piacere il contenuto del pacchetto e ingannare il nodo successivo, il quale prenderà quell'informazione come reale.

In aggiunta a quanto detto, si sottolinea la continua permanenza del settore **manifatturiero** come quello più colpito anche nell'arco del secondo trimestre, indice della continua attenzione da parte di attaccanti verso questo specifico settore industriale.

4. Caso reale

Attacco perpetrato da un gruppo APT utilizzando un malware 0-day.

4.1 La dinamica

Durante il secondo semestre del 2019 si è assistito ad un aumento considerevole di incidenti di sicurezza che si sviluppavano secondo un pattern definito e proceduralizzato. Tali incidenti hanno portato alla compromissione dell'infrastruttura e alla successiva attivazione della cifratura tramite ransomware (abitualmente Ryuk).
L'ingaggio dell'YCERT è avvenuto molto spesso a incidente avvenuto, poiché chi ha subito tali compromissioni non disponeva di un servizio di monitoraggio proattivo delle minacce tramite un team SOC H24.

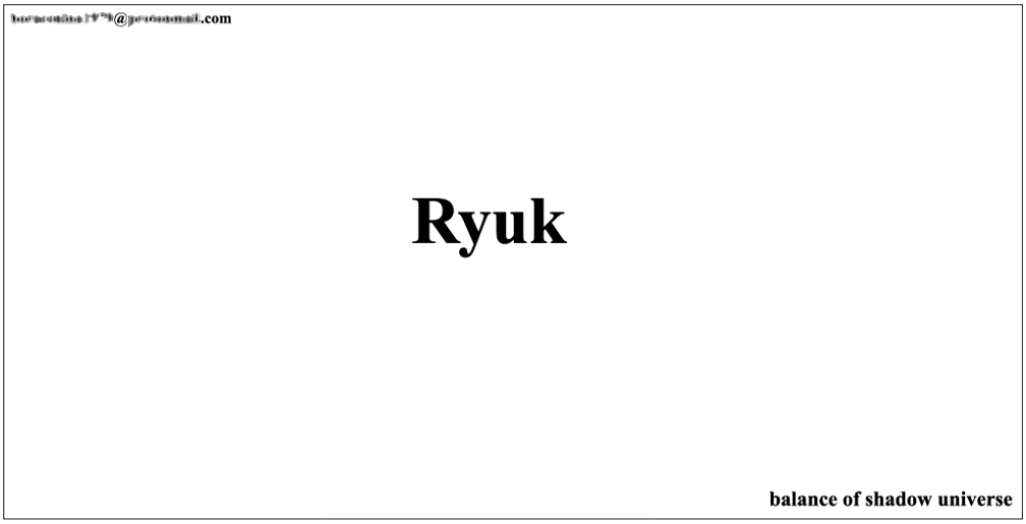
4.2 Analisi dell'attaco

// LA COMPROMISSIONE

Gli incidenti analizzati sono stati ricondotti nella maggior parte dei casi al ransomware Ryuk che esegue una cifratura dei file presenti all'interno della macchina colpita. Questo tipo di **cifratura** è **irreversibile** e l'unico modo di decifrare i file è quello di conoscere la chiave usata per la loro cifratura. Tale chiave viene venduta dai criminali in seguito al pagamento del riscatto.
L'ammontare del riscatto viene richiesto contattando gli attaccanti all'indirizzo di posta elettronica visualizzato nella pagina html presente in tutte le directory, oltre che nei menu standard di Windows *(fig.7)*.

Figura 7

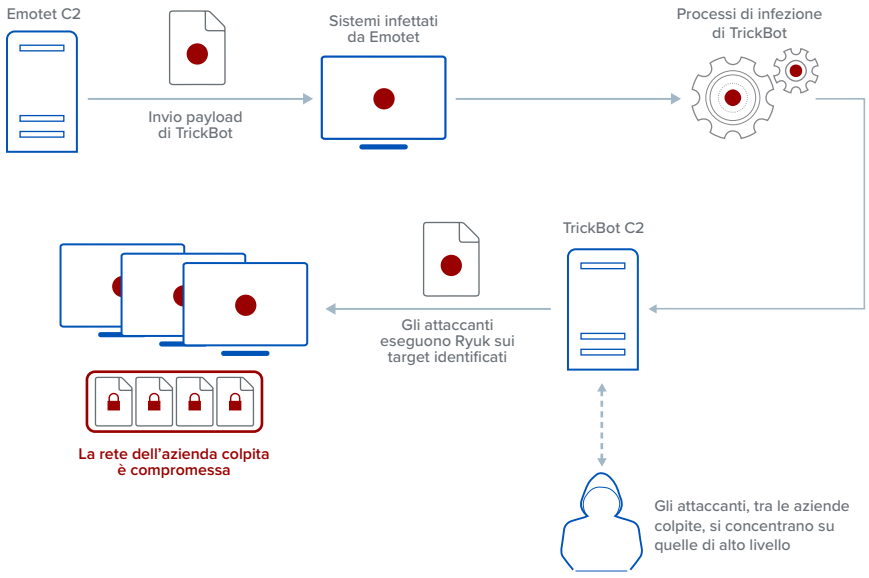
Pagina di richiesta del riscatto



Il ransomware **Ryuk** viene utilizzato come **fase finale dell'attacco**: quella in cui i file vengono cifrati. Per giungere a questa fase vengono utilizzati prima altri due malware per infiltrarsi e prendere il controllo totale dell'infrastruttura.
Il ciclo di vita dell'attacco *(fig.8)* è completato da altri due malware, varianti delle famiglie Emotet e Trickbot, che vengono utilizzati in precedenza dall'attaccante per infiltrarsi e prendere il controllo totale dell'infrastruttura.

Figura 8

Compromissione Emotet, TrickBot, Ryuk (link)



// COM'È AVVENUTA LA COMPROMISSIONE

Il malware Emotet

Emotet viene diffuso principalmente **tramite e-mail di malspam** (e-mail che contengono link o allegati malevoli) e recentemente ha visto grande diffusione l'utilizzo della **PEC** (Posta Elettronica Certificata) per tali finalità malevole.
È un malware avanzato, persistente e modulare la cui funzionalità primaria è quella di veicolare altri malware, come nel caso in analisi ha veicolato l'infezione da Trickbot prima e da Ryuk poi.

Inoltre, Emotet è un **trojan polimorfo**, che muta continuamente ed è in grado di superare i controlli di sicurezza basati su firme (come ad esempio i classici antivirus). Contempla diverse modalità di persistenza, che includono la registrazione di task schedulati e di servizi con start automatico all'avvio della macchina compromessa. Una volta avviato, Emotet instaura una chiamata verso i suoi server di Command & Control (C2) ed inizia la fase di esfiltrazione dati quali:

- Credenziali di accesso salvate nei browser
- Informazioni dell'utente e della macchina
- Informazioni sull'attività quotidiana dell'utente: cosa viene digitato, salvato, etc...
- Invio spam con allegati infetti dall'account dell'utente.

Per ottenere persistenza, Emotet inietta codice malevolo in processi noti, come *svchost.exe* o altri processi in esecuzione. Le informazioni raccolte vengono solitamente inviate all'esterno verso i server C2. Una volta stabilita la connessione, il malware riceve comandi, scarica ed esegue nuovi moduli, effettua l'upload di dati verso l'esterno.

Il malware Trickbot
Durante questa fase Emotet scarica un nuovo malware, Trickbot, che ha il compito di espandersi nella rete con movimenti laterali e, grazie alla sua natura modulare, è in grado di prendere il **controllo totale di tutti i client e di tutti i server della rete**.

Trickbot nasce come un malware relativamente semplice, ma nel corso del tempo ha fatto evolvere le sue funzionalità di raccolta informazioni e di evasione dalle piattaforme di sicurezza più comuni. Viene eseguito in memoria ed è dunque **difficilmente rilevabile dagli antivirus** che si basano esclusivamente sulla firma dell'eseguibile per riconoscere le componenti malevole.
Di seguito le sue principali funzionalità:

- Disabilitazione autonoma delle soluzioni antivirus
- Raccolta informazioni dai browser come password, dati di carte di credito, etc...
- Creazione di backdoor per accesso remoto
- Furto di credenziali digitate sul sistema e nei principali software usati comunemente
- Movimento laterale sulla rete utilizzando vulnerabilità note, ad esempio, Eternal Blue
- Furto di credenziali presenti in memoria utilizzando tool come Mimikatz.

Questa fase ha una durata variabile e può durare ore, giorni, settimane.
Una volta che gli attaccanti ritengono di aver raggiunto il completo controllo della rete, viene attivata l'ultima fase dell'attacco, quella distruttiva, con il ransomware Ryuk che esegue la cifratura.

Il malware Ryuk
Il ransomware viene iniettato nelle share nascoste che sono abilitate di default sui sistemi Windows per scopi amministrativi e predispone l'ambiente per l'attacco finale, che esegue la contemporanea cifratura delle macchine di cui i criminali hanno ottenuto il controllo, solitamente la totalità dei server Windows presenti nell'infrastruttura.

L'**esecuzione** di questi attacchi avviene tendenzialmente nel momento in cui l'attaccante presume che il **presidio da parte della vittima sia al minimo**: generalmente la sera o all'inizio del weekend, in questo modo la cifratura non viene interrotta prima di riuscire a compromettere completamente l'infrastruttura della vittima.

In seguito l'attività di questi gruppi criminali si è ulteriormente evoluta, andando a pubblicare su un sito web le informazioni esfiltrate durante l'attacco, si veda ad esempio il seguente *link*.

Quest'evoluzione aggiunge ulteriore complessità nella gestione di incidenti di questo tipo: in precedenza, non era necessario notificare al garante questo tipo di violazioni, nel caso in cui tutti i dati personali fossero stati completamente recuperati dai sistemi di backup e in assenza di evidenze certe di esfiltrazioni.
Oggi, al contrario, la normativa **GDPR impone la notifica al garante**, dal momento che questa tipologia di attacco ransomware viene classificata come **data breach**.

5. Conclusioni

Il terzo report evidenzia che il trend degli attacchi è in complessiva diminuzione, con un aumento però dei casi di gravità elevata

Il terzo report redatto dal SOC Yarix evidenza un trend degli eventi di sicurezza in complessiva diminuzione, con un **aumento** però dei casi di **gravità elevata**.

Nonostante ciò, si possono apprezzare alcune variazioni significative, in particolare con riferimento all'analisi della tipologia di attacchi che sono stati analizzati durante il secondo semestre del 2019. Infatti, le tecniche utilizzate, i gruppi di cybercriminali coinvolti e il rate di successo registrato in questo periodo di analisi sono di grande interesse e meritano un approfondimento dettagliato.

Come descritto in precedenza sono da evidenziare le metodologie di compromissione che hanno coinvolto diverse famiglie di malware noti che, combinati tra loro, hanno prodotto **una nuova tipologia di attacco** la quale ha causato diverse "vittime" a livello sia nazionale che internazionale.
Infatti, l'evidenza del numero di attacchi di questo tipo andati a buon fine è sicuramente un punto di attenzione per il secondo semestre del 2019 e lo sarà probabilmente anche per buona parte del 2020.

Questo aumento può essere sicuramente ricondotto alla **capacità da parte dei gruppi di cybercriminali di standardizzare le loro attività** e di ridurre al minimo il tempo necessario per il passaggio dalla fase di prima compromissione a quella di esecuzione dell'attacco finale (tipicamente la cifratura), rendendo sempre più complicata la detection e la successiva risposta all'attacco.

Per poter rispondere ad attacchi di questo tipo, vanno messe in campo diverse soluzioni:

• Utilizzare tecnologie di livello avanzato per la **protezione dei server e dei client** quali piattaforme di EDR, che permettono di riconoscere e quindi bloccare questo tipo di minaccia.

• Utilizzare tecnologie di livello avanzato per l'**analisi del traffico di rete**, in modo da rilevare e quindi contenere attacchi provenienti da dispositivi out-of-scope come, ad esempio, piattaforme NVR, stampanti, telecamere, etc.

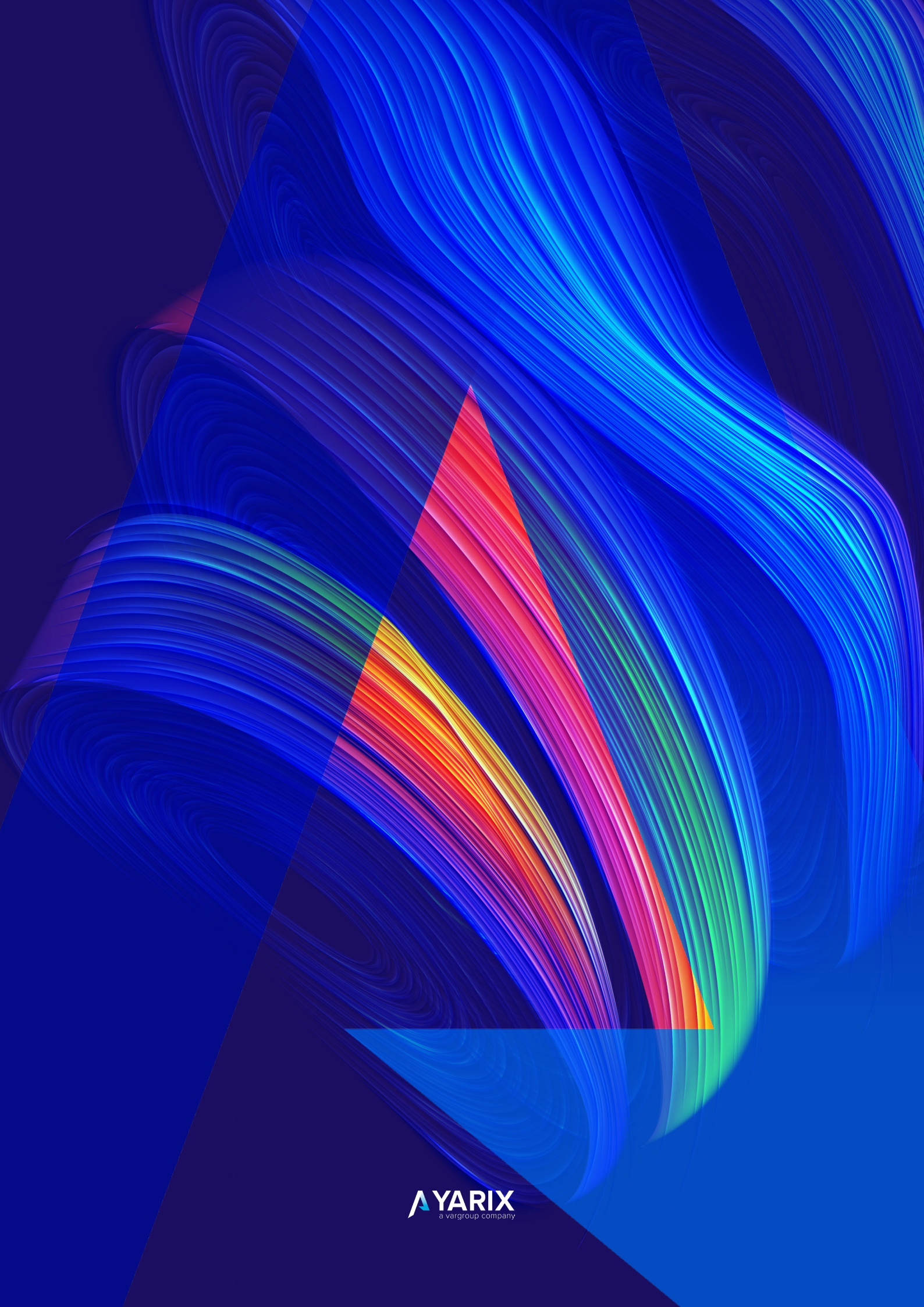
• Utilizzare un servizio di **monitoraggio delle piattaforme di sicurezza** che lavori in stretto contatto con le risorse interne, in modo da assicurare presidio in modalità H24 24x7.

• Implementare **policy più stringenti sul traffico di rete** sia per gli utenti che per gli amministratori di sistema.

• Implementare le **best practice di settore** per il miglioramento della security dell'infrastruttura: processo di aggiornamento continuo e regolare di server e infrastruttura di rete. Segregazione logica e/o fisica delle reti client dalle reti server, hardening delle policy di dominio, etc.

• Implementare un **robusto processo di backup & restore dei dati critici**.
La scelta tecnologica di avere una seconda unità di backup è risolutiva, ma si consiglia fortemente di valutare il suo spostamento in una rete separata. Si suggerisce, ad esempio, la strategia di backup 3-2-1: avere almeno 3 copie di backup, 2 copie locali su due mezzi fisici differenti e scollegati ed 1 completamente off-site (altro data center/ cloud). Il restore dei dati deve essere programmato, provato e verificato almeno una volta ogni 6 mesi.

• Sensibilizzare l'**utente** rispetto al livello di attenzione da mantenere nel corso della sua normale giornata lavorativa. L'utente deve essere informato regolarmente sui rischi che provengono dall'esterno e sui comportamenti da adottare in caso di dubbi sulla liceità di un documento o di un messaggio di posta elettronica.


YARIX
a vargroup company