YARIX
a vargroup company

YSOC SECURITY REPORT

Q2 2019

YARIX
a vargroup company

Sommario

Introduzione

Il documento restituisce una elaborazione dei dati ricevuti e analizzati dal SOC di Yarix nel periodo aprile-giugno 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 aprile-giugno 2019** e rappresenta un documento dinamico che sarà aggiornato su base trimestrale 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.

© 2019 Yarix - All rights reserved

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:

// **ANALISI 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

// **ANALISI 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.

© 2019 Yarix - All rights reserved

1. Dati analizzati

I dati analizzati in questo secondo report 2019 sono relativi a circa 15 mila eventi di sicurezza

I dati analizzati in questo secondo report sono relativi ai **circa 15 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 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.

© 2019 Yarix - All rights reserved

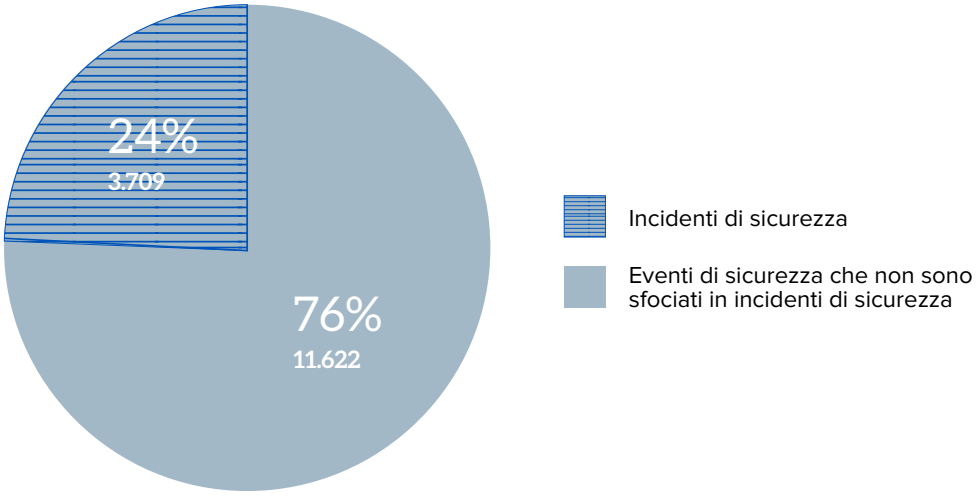
A titolo esemplificativo e non esaustivo, gli eventi di sicurezza analizzati consistono in:

- 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 email di phishing;
- comunicazione con IP, domini, URL riconducibili ad attività malevole.

Gli eventi analizzati **in totale sono 15.331**, di cui **3.709 si sono evoluti in incidenti di sicurezza**, di diversa criticità *(fig.1)*.

Figura 1

Eventi totali analizzati

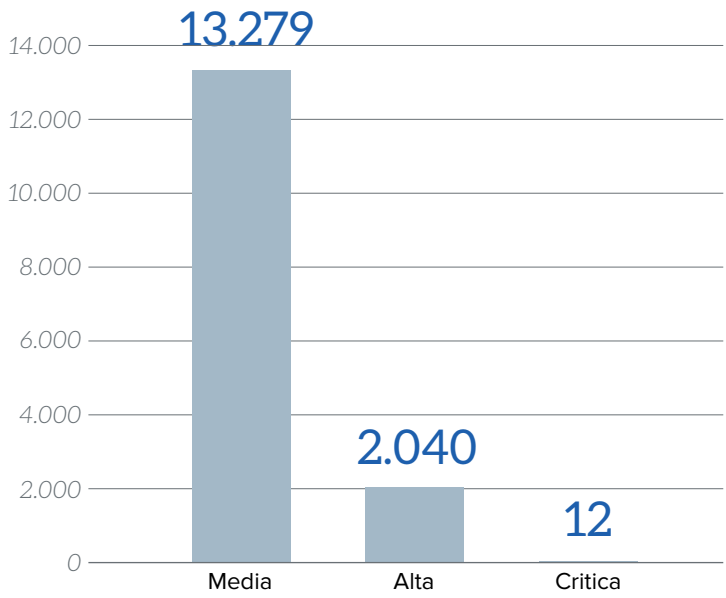


La criticità degli eventi viene calcolata sulla base delle indicazioni contenute nel manuale operativo dei singoli clienti del servizio, e definita secondo le metriche e le procedure concordate, basate su **standard nazionali e internazionali**.
Questa classificazione permette di allineare le tipologie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

© 2019 Yarix - All rights reserved

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. Garantiscono 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;

© 2019 Yarix - All rights reserved

• **Gestire** corsi di aggiornamento tecnico a tutti i livelli, in particolare per gli utenti finali;

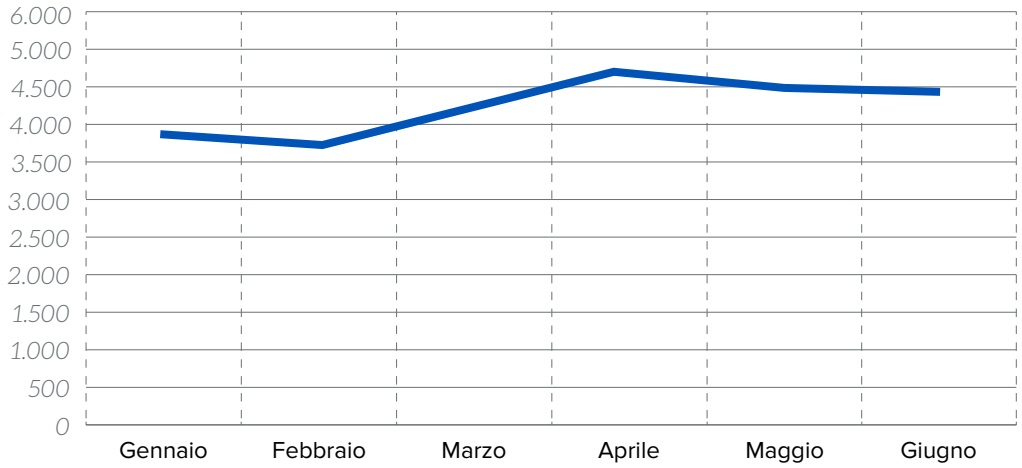
• **Mantenere aggiornati** allo stato dell'arte gli strumenti e le metodologie per la sicurezza;

• **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** *(fig.3)*, come già intravisto nel report relativo al primo trimestre.

Figura 3

Distribuzione temporale degli eventi nel 2019



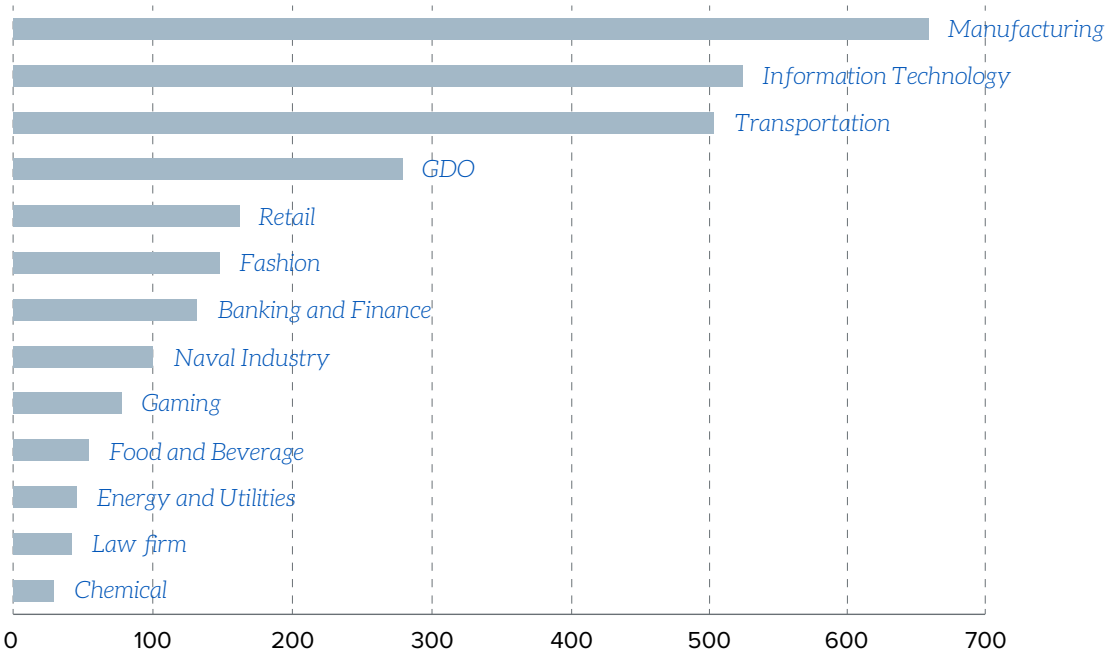
Il prospetto dei dati sui primi sei mesi del 2019 evidenzia un **trend in crescita** relativamente al numero di casi gestiti. Questo evidenzia la continuità degli eventi di sicurezza sul panorama delle aziende italiane e deve far **alzare il livello di guardia**: è sufficiente anche solo uno di questi eventi per portare danni potenzialmente catastrofici.

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 *(fig.4)*. Per tale motivo sono state fatte delle considerazioni di tipo statistico che verranno descritte nella sezione successiva.

© 2019 Yarix - All rights reserved

Figura 4

Eventi di sicurezza duddivisi per settore industriale



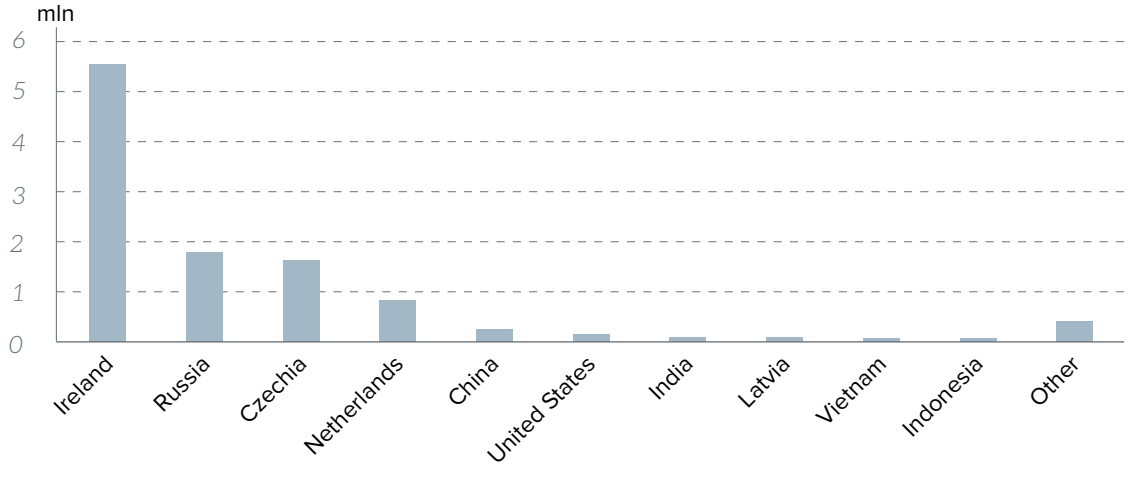
Come nel report precedente il settore Manufacturing rimane il più colpito.
È da evidenziare invece il **sensibile aumento di eventi rivolti verso il settore dei trasporti** che ha sostanzialmente raddoppiato la sua presenza rispetto al trimestre precedente.

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.5)*.

Figura 5

Geolocalizzazione delle minacce



© 2019 Yarix - All rights reserved

Rispetto ai dati raccolti nel trimestre precedente si denota un **aumento complessivo di eventi** (si passa dai sette milioni a circa dieci milioni e mezzo di rilevazioni) con l'Irlanda che rimane sempre al primo posto come paese da cui provengono la maggior parte degli eventi rilevati dalla rete di honeypot.

La maggior parte delle infezioni rilevate in questo contesto vengono propagate sfruttando 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.

Questi protocolli vengono utilizzati per i collegamenti remoti alle macchine e tendenzialmente sono servizi che non dovrebbero essere esposti pubblicamente, a meno di opportuni accorgimenti, come VPN o accessi limitati a entità autorizzate. Infatti, qualora questo avvenga, l'esposizione viene rilevata da tool di scansione che periodicamente scandagliano la rete alla ricerca di potenziali "punti di ingresso" ai sistemi informatici. Per poter sfruttare queste esposizioni, ci sono due modalità:

- **Sfruttamento di vulnerabilità** note dei protocolli esposti
- **Tentativo di bruteforce**, ovvero, login ripetuti con utenze standard e password comuni.

È evidente che, se tali connessioni non sono presidiate, il rischio di intrusione nel sistema aziendale aumenta vertiginosamente. Le principali famiglie di malware rilasciate dagli attaccanti sono:

- una variante di "**Zusy Trojan**" (60%), ovvero, un malware bancario che tipicamente si diffonde attraverso email contenente allegato malevolo. Tale malware, che si può diffondere all'interno della rete attraverso caratteristiche di tipo worm, ha la finalità di raccogliere informazioni relative a credenziali bancarie dell'utente.
- una delle tante varianti del ransomware "**Wanna Cry**" (30%), malware noto alla cronaca per aver avuto una diffusione globale nel 2017, in aumento rispetto al trimestre precedente. Nonostante il malware sia ormai diffuso da due anni, rimane comunque tra i metodi di attacco più utilizzati.

2.3 E-mail analysis

Come nel report relativo al primo trimestre, anche nel periodo analizzato vengono evidenziate le **principali modalità di frode che sfruttano l'e-mail come vettore**.
Tra queste si riconoscono le due principali campagne presenti anche nel precedente report, ovvero quelle legate al ricatto (Sextortion) e le campagne e-mail che utilizzano la PEC come mezzo di comunicazione.
In aggiunta, nel trimestre analizzato, si sono evidenziati un numero consistente di tentativi di truffa basati sull'impersonificazione di una figura di spicco all'interno dell'azienda, le cosiddette e-mail "CEO phishing".

Nel seguito vengono riportate le principali campagne phishing rilevate nel trimestre in esame, con relativi trend di diffusione all'interno del perimetro monitorato.

// SEXTORTION

La campagna in questione è costantemente presente in tutto il periodo analizzato. La causa è riconducibile alla semplicità con cui si può costruire una campagna di questo tipo: è sufficiente infatti costruire un'e-mail simile a quella riportata in figura e inviarla a un numero molto elevato di destinatari.

© 2019 Yarix - All rights reserved

Il fattore di successo ovviamente non è molto elevato, ma analizzando i portafogli Bitcoin riportati all'interno di alcune di queste e-mail, si rileva che sono stati eseguiti dei pagamenti anche recentemente. A più di un anno dalla sua apparizione questa campagna rimane una tra le più diffuse *(fig.6)*.

Figura 6

Sextortion - sample #1

Da: [redacted]

Per: [redacted]

Data: 08/04/2019 10:34

Oggetto: Il tuo account e stato violato! Pericolo di infezione dell'intero sistema operativo!

Ciao!

Come avrai notato, ti ho inviato un'email dal tuo account.
Ciò significa che ho pieno accesso al tuo account.

Ti sto guardando da alcuni mesi.
Il fatto è che sei stato infettato da malware attraverso un sito per adulti che hai visitato.
Se non hai familiarità con questo, ti spiegherò.
Virus Trojan mi dà pieno accesso e controllo su un computer o altro dispositivo.
Ciò significa che posso vedere tutto sullo schermo, accendere la videocamera e il microfono, ma non ne sai nulla.

Ho anche accesso a tutti i tuoi contatti e tutta la tua corrispondenza.

Perché il tuo antivirus non ha rilevato il malware?
Risposta: il mio malware utilizza il driver, aggiorno le sue firme ogni 4 ore in modo che Il tuo antivirus era silenzioso.

Ho fatto un video che mostra come ti accontenti nella metà sinistra dello schermo, e nella metà destra vedi il video che hai guardato.
Con un clic del mouse, posso inviare questo video a tutte le tue e-mail e contatti sui social network.
Posso anche postare l'accesso a tutta la corrispondenza e ai messaggi di posta elettronica che usi.

Se vuoi impedirlo, trasferisci l'importo di 257€ al mio indirizzo bitcoin (se non sai come fare, scrivi a Google: "Compra Bitcoin").

Il mio indirizzo bitcoin (BTC Wallet) è: [redacted]

Dopo aver ricevuto il pagamento, eliminerò il video e non mi sentirai mai più.
Ti do 48 ore per pagare.
Non appena apri questa lettera, il timer funzionerà e riceverò una notifica.

Presentare un reclamo da qualche parte non ha senso perché questa email non può essere tracciata come e il mio indirizzo bitcoin.
Non commetto errori!

Se scopro di aver condiviso questo messaggio con qualcun altro, il video verrà immediatamente distribuito.

Auguri!

© 2019 Yarix - All rights reserved

// CAMPAGNA SLOAD VERSO PEC

Questa campagna *(fig.7)*, analizzata anche in un bollettino del CERT-PA *(rif.)*, veicolava una variante del noto malware sLoad attraverso l'utlizzo di PEC precedentemente compromesse. L'utilizzo della PEC per l'invio di e-mail di phishing o con allegati malevoli comporta un'ulteriore complicazione nella rilevazione da parte dell'utente del tentativo di frode. Ci si aspetterebbe infatti che un'e-mail ricevuta tramite PEC possa essere considerata attendibile, quando in realtà la diffusione di questa tecnica per veicolare malware si è ormai affermata. Anche le PEC dunque vanno analizzate e valutate con estrema cautela dall'utente che le riceve.
Nella campagna analizzata l'eseguibile malevolo, dopo una prima comunicazione con il server di comando e controllo (C2), provvedeva all'installazione di task schedulati per mantenere la persistenza all'interno del sistema e garantire all'attaccante un controllo completo della macchina compromessa.

Figura 7

Campagna sLoad verso PEC - sample #2

Oggetto **I: fattura MIX08131 del 18/05/2019**
Mittente [redacted]@pec.ording.roma.it>
Destinatario [redacted]
Data **2019-06-06 17:08**

Da : "Per conto di: [redacted]" posta-certificata@pec.aruba.it
A : [redacted]pec.ording.roma.it
Cc :
Data : Thu, 6 Jun 2019 16:56:27 +0200
Oggetto : POSTA CERTIFICATA: fattura MIX08131 del 18/05/2019

Spett.le
c/a UFFICIO AMMINISTRATIVO

Allegata alla presente email Vi trasmettiamo copia PDF di cortesia della fattura in oggetto.
Documento privo di valenza fiscale ai sensi dell'art. 21 Dpr 633/72. L'originale e disponibile all'indirizzo telematico da Lei fornito oppure nella Sua area riservata dell'Agenzia delle Entrate.
Qualora non foste soggetti all'obbligo della fatturazione elettronica, Vi ricordiamo che siete tenuti a stampare e conservare la fattura allegata come da art. 21 del D.P.R. 633/72 e successive modifiche e dalle R.M. 571134 del 19/07/88, R.M. 450217 del 30/07/90, R.M. 107 del 04/07/01, R.M. 202/E del 04/12/01, C.M. 45/E del 19/10/05.
Non invieremo copia cartacea della fattura.

Se vuole visualizzare in anteprima il documento, puo collegarsi al seguente link:

Fattura MIX08131

Con l'occasione, porgiamo distinti saluti.

// CEO PHISHING

Questa tecnica di frode sfrutta il camuffamento del mittente dell'e-mail per simulare che questa sia stata inviata da una persona di spicco all'interno dell'azienda (da qui il nome di CEO phishing). Il destinatario riceve dunque un'e-mail nella quale gli vengono fatte delle richieste molto specifiche e che simulano quelle che effettivamente potrebbero essere fatte dall'AD *(fig.8)*.
Gli attacchi orchestrati di questo tipo possono richiedere un periodo di studio anche molto lungo, durante il quale l'attaccante identifica le risorse all'interno dell'azienda che sono solite svolgere determinate attività. Questo può avvenire tramite informazioni ottenute da precedenti attacchi o tramite Social Engineering, una tecnica che sfrutta la fiducia riposta dall'utente nella persona con cui sta comunicando per carpire informazioni riservate.
Qualora l'utente dovesse rispondere alla prima e-mail inviata, di solito volutamente generica o poco comprensibile, l'attaccante inizia una comunicazione esclusivamente via e-mail per raggiungere i suoi fini come ottenere informazioni riservate o far effettuare dei pagamenti verso conti a lui riconducibili.
La mitigazione migliore contro questo tipo di attacchi è quella di eseguire una "seconda verifica" con il mittente, ovviamente tramite altro canale di comunicazione per essere certi che l'e-mail arrivi effettivamente dalla persona reale e non da un attaccante.

© 2019 Yarix - All rights reserved

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

Le considerazioni presenti in questa sezione potranno acquisire profondità crescente con il susseguirsi progressivo dei report e l'estensione del periodo di analisi. Lo studio dei sei mesi a cui fanno riferimento i primi due report (gennaio-giugno 2019) permette di condividere alcune osservazioni:

// TREND 1

Il trend relativo alla numerosità degli eventi ha confermato le assunzioni fatte nel primo report evidenziando un ulteriore aumento di eventi e incidenti di sicurezza. Tra questi eventi è da sottolineare anche il trend costante del **numero di incidenti di severità critica**, indice del fatto che tali accadimenti non sono più rari o poco probabili, ma un fattore che coinvolge ormai tutte le aziende.

A maggior ragione va tenuto conto del fatto che i dati provengono da realtà che si sono dotate di misure avanzate di sicurezza di livello elevato, affidandosi anche a servizi esterni per il monitoraggio continuativo H24 della loro infrastruttura.

Gli attacchi che potenzialmente avrebbero potuto raggiungere un livello di criticità molto elevato in realtà, per la loro maggior parte, sono stati identificati e bloccati ancor prima di poter nuocere e si sono risolti in un nulla di fatto o hanno avuto un impatto decisamente minore di quello che avrebbero potuto provocare se non intercettati per tempo.

//TREND 2

La seconda considerazione porta ad approfondire i dati rilevati dalle **sonde honeypot**.

Le principali attività registrate, anche nel secondo trimestre, coinvolgono attività di scansione massiva per servizi esposti vulnerabili. Questi rappresentano per gli attaccanti dei veri e propri varchi nel perimetro di sicurezza aziendale che possono essere sfruttati come punti di ingresso per l'accesso al sistema informativo aziendale con conseguenze anche catastrofiche.

Nell'ultimo periodo si è rilevato un **importante aumento delle scansioni volte a rilevare server con il protocollo RDP esposto**.

Questo protocollo è quello che viene utilizzato per collegarsi da remoto a un server che utilizza il sistema operativo Windows.

Il motivo di questo aumento è da ricondurre con certezza alla divulgazione di una vulnerabilità su tale protocollo *(rif.)* che permette di bypassare l'autenticazione e di avere accesso al server anche senza essere in possesso delle credenziali e delle autorizzazioni per farlo.

Al momento non sono ancora stati rilasciati pubblicamente exploit di questa vulnerabilità, ma gli attaccanti stanno già sondando il terreno alla ricerca di potenziali target.

© 2019 Yarix - All rights reserved

//TREND 3
Il terzo trend da sottolineare è relativo al considerevole **aumento di attività registrato nel settore dei trasporti** durante il secondo trimestre del 2019. Un'analisi di dettaglio degli eventi ha evidenziato che la maggior parte degli attacchi sono da ricondurre a **tentativi di attacco web** (SQL injection e similari) che miravano allo sfruttamento di vulnerabilità note di popolari CMS o applicativi web o allo sfruttamento di errori di configurazione che potessero permettere di eseguire comandi remoti con privilegi elevati.
La protezione dei servizi esposti, in particolar modo quelli web, rimane dunque un tema fondamentale nella politica di controllo e di sicurezza all'interno di un'azienda. L'attivazione di sistemi di application firewall (WAF) in grado di analizzare il traffico, rilevare e bloccare le richieste anomale o non consentite, un logging adeguato delle richieste eseguite verso il server web e un monitoraggio attivo sugli allarmi generati dai dispositivi preposti sono delle ottime contromisure per limitare e contenere i tentativi di attacchi web che vengono rivolti verso le infrastrutture aziendali.

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.

© 2019 Yarix - All rights reserved

4. Caso reale

L'attacco è stato perpetrato da un gruppo APT utilizzando un malware 0-day.

4.1 La dinamica

Sferrato l'11 giugno, l'attacco a Bonfiglioli è stato perpetrato da un gruppo APT (Advanced Persistent Threat) utilizzando un malware 0-day. Virus di questo tipo risultano particolarmente aggressivi in quanto realizzati ad hoc per un target aziendale specifico e capaci di restare nascosti: solo analisti specializzati (CERT e Incident Response Team) sono in grado di individuare questi attacchi, rilevando in modo puntuale le azioni e i componenti utilizzati sugli endpoint compromessi.

Attaccando la rete aziendale di Bonfiglioli, il gruppo ha agito in un secondo momento con un ransomware che ha cifrato numerosi sistemi e compromesso l'accessibilità ai file criptati. La violazione ha poi ceduto il passo al più classico degli schemi criminali con una richiesta di riscatto prontamente rifiutata da Bonfiglioli, che ha successivamente richiesto l'intervento di un pool di professionisti di Yarix, divisione Digital Security di Var Group.

4.2 La gestione

In tre giorni è stata contenuta l'aggressione digitale mentre la completa distruzione del malware è stata completata nell'arco di dieci giorni. Considerando la portata dell'attacco, questo importante risultato è stato possibile grazie al coordinamento di più team: gli esperti in analisi forense, incident response e malware analysis attivi in situ hanno operato in collegamento costante con gli analisti del Security Operation Center di Yarix attivi da remoto.

In dettaglio, la gestione dell'attacco ha richiesto un insieme articolato in interventi. A una prima fase di contenimento - culminata nell'isolamento del malware fino ad interrompere ogni possibile comunicazione verso i sistemi remoti - è seguita la fase di eradicazione che ha richiesto l'impiego di software intelligenti di ultima generazione. Nello specifico **è stato utilizzato un sistema EDR (Endpoint Detection and Response) di avanguardia**, capace di distinguere e interpretare, sul piano qualitativo oltre che quantitativo, i comportamenti 'malevoli' tra quelli consueti espressi dai normali processi informatici.

4.3 Il profiling tecnico: l'identikit degli e-criminali

Indicazioni tecniche emerse durante la gestione dell'attacco, come pure l'utilizzo del ransomware Ryuk, condurrebbero al presunto profilo criminale degli hacker responsabili dell'aggressione: un gruppo di e-criminali russi conosciuto come Grim Spider, noto per l'utilizzo di malware sofisticati come quello adottato contro Bonfiglioli. Il gruppo sarebbe attivo da agosto 2018 e agirebbe preferibilmente contro obiettivi aziendali di grandi dimensioni – metodologia 'big game hunting' – a scopo di estorsione e ricatto.

© 2019 Yarix - All rights reserved

4.4 Cybersecurity come forma mentis di prevenzione continuativa

Insieme ad altri dispositivi avanzati di cybersecurity, il software EDR compone oggi la nuova architettura di sicurezza digitale pensata per Bonfiglioli. L'intero sistema di protezione è collegato al Security Operation Center di Yarix, che consente un monitoraggio H24 di ogni movimento anomalo attorno al perimetro informatico aziendale. Intervenendo su una cultura aziendale del partner già predisposta e consapevole dei rischi del cybercrime, lo schema di presidio così disegnato da Yarix per Bonfiglioli realizza uno scudo molto strutturato e certamente capace di competere con la nuova criminalità informatica, in grado di cambiare pelle ed esternare modalità di intrusione diverse ad ogni attacco.

Proprio alla luce di questa considerazione risulta tanto più importante la scelta del Gruppo Bonfiglioli, che ha pubblicamente denunciato il tentativo di violazione ed estorsione subito. Sottrarsi al ricatto del cybercrime significa, infatti, gettare le basi per una cultura più matura e condivisa della legalità digitale, scardinando il meccanismo alla base del cosiddetto 'pizzo 2.0' e innescando un circuito virtuoso di denuncia, responsabilità e trasparenza tra le imprese attaccate.

5. Conclusioni

Il secondo report evidenzia che il trend degli attacchi è rimasto pressoché costante.

Il secondo report redatto dal SOC Yarix evidenza che il trend degli attacchi è rimasto pressocché costante rispetto a quanto evidenziato durante il primo trimestre dell'anno.

Nonostante ciò si possono apprezzare alcune **variazioni significative**, in particolare con riferimento all'analisi degli eventi suddivisi per **settore aziendale**. L'aumento percentuale maggiore è avvenuto nel conteggio degli eventi di sicurezza rilevati e gestiti all'interno dei trasporti, ambito nel quale sono classificate aziende che si occupano a vario titolo dello spostamento di merci e persone.

Va specificato che gli attacchi rilevati non sono rivolti verso le componenti infrastrutturali e di trasporto: non mettono dunque in pericolo la sicurezza fisica dei passeggeri, ma mirano alle informazioni personali e di pagamento che gli utenti condividono o utilizzano per fare le prenotazioni o gli abbonamenti.
Questa la logica alla base di uno degli attacchi diretto contro un'importante compagnia nazionale di trasporti, per il quale le attività di *Incident Response*, *Assessment* e *Digital Forensics* condotte da Yarix e volte a ricostruire la dinamica dell'incidente, hanno portato alla scoperta e neutralizzazione di un **APT** (Advanced Persistent Threat) *(rif.)* **mai rilevato in precedenza** a livello globale.

© 2019 Yarix - All rights reserved

Questo **nuovo strumento di attacco hacker**, oggetto di analisi specifica *(rif.)*, rappresenta una minaccia evoluta per tutte le aziende che gestiscono pagamenti o dati personali.

Attacchi di questo tipo, qualora vadano a buon fine, prendono il nome di "data breach" e possono costituire un rischio molto elevato sia per gli utenti che per le aziende bersagli di questi attacchi.
Il tema "**data breach**" infatti è principalmente noto a causa delle pesanti sanzioni (fino al 4% del fatturato) che possono essere applicate verso le aziende che lo subiscono e che sono soggette alla normativa europea GDPR. Alcuni esempi di tali sanzioni sono quelli rivolti verso British Airways e la catena di hotel Marriott, rispettivamente di 200 e 100 milioni di euro.

Altro tema di interesse evidenziato è quello relativo alle **frodi di tipo CEO phishing**, che rimane una delle principali tecniche di phishing per diffusione e percentuale di successo.
Affinché questi attacchi abbiano maggior probabilità di andare a buon fine, sono necessarie informazioni sul target. Molti dettagli spesso possono essere raccolti tramite l'analisi dei profili social dei CEO scelti per la truffa: essere a conoscenza del luogo in cui la persona è in villeggiatura, chi abitualmente frequenta o anche quali dispositivi utilizza, garantisce all'attaccante un livello di affidabilità maggiore nei confronti dell'interlocutore che dovrà convincere.
Dall'altro lato chi riceve queste e-mail ha la possibilità di sventare l'inganno applicando dei semplici controlli:

- **Prestare attenzione al formato di e-mail e testo**: alcuni messaggi di phishing contengono evidenti errori grammaticali o parole di uso poco comune.
- **Verificare l'attendibilità dei link** presenti nell'e-mail appurando che puntino effettivamente a quanto riportato sullo schermo (ciò può essere effettuato passando il cursore del mouse sopra il link).
- **Controllare la veridicità dell'indirizzo e-mail del mittente**: molte di queste frodi utilizzano tecniche di camuffamento grazie alle quali l'e-mail, apparentemente inviata da una persona affidabile o nota, in realtà contiene una provenienza totalmente diversa. Espandendo i dettagli del mittente, può essere verificata l'anomalia.
- **Diffidare delle e-mail che mettono fretta o che impongono riservatezza**: molto spesso le tecniche di phishing utilizzano l'allarmismo per generare urgenza, confusione e timore nelle persone che devono gestire la richiesta.

Molti di questi controlli sono più efficaci se eseguiti da PC piuttosto che da smartphone: la lettura dell'e-mail da cellulare, infatti, comporta una minore attenzione ai dettagli e una conseguente maggiore probabilità di non notare eventuali elementi sospetti.

Oltre a quanto suggerito, il metodo migliore per affrontare queste truffe rimane sempre la **verifica diretta con il mittente dell'effettivo invio dell'email**. Tale controllo va eseguito utilizzando un canale di comunicazione alternativo, ad esempio, rivolgendosi fisicamente alla persona o contattandola tramite telefonata.

© 2019 Yarix - All rights reserved


YARIX
a vargroup company