IC InfoCamere

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

INDICE DI ESPOSIZIONE CYBER

PARTNER TECNOLOGICO

YOROI®
TINEXTA GROUP

COSA FA VEDERE?

- Le prime, veloci e accessibili informazioni sui potenziali rischi cyber che l'azienda sta correndo (senza alcuna scansione attiva all'interno dell'azienda)

QUALI INFORMAZIONI FORNISCE?

- La dimensione del perimetro digitale esposto in rete (tanto più grande, maggiore sarà il rischio)
- Le vulnerabilità già note in relazione a quel perimetro (note vuol dire che sono già "sfruttate" dai cyber criminali)
- I furti di dati dell'azienda già avvenuti e presenti nel dark web (in particolare se le e-mail aziendali e le relative password sono state compromesse)

A COSA SERVE?

- A verificare se sia possibile ridurre il perimetro di esposizione a potenziali attacchi cyber
- A controllare immediatamente se alcuni software in uso in azienda siano aggiornati alle ultime versioni rilasciate dal produttore
- A valutare se il modo in cui vengono definite le password in azienda sia adeguato e se l'utilizzo delle mail aziendali sia corretto o se esse vengano utilizzate per scopi impropri

A CHI POTENZIALMENTE INTERESSANO QUESTE INFORMAZIONI?

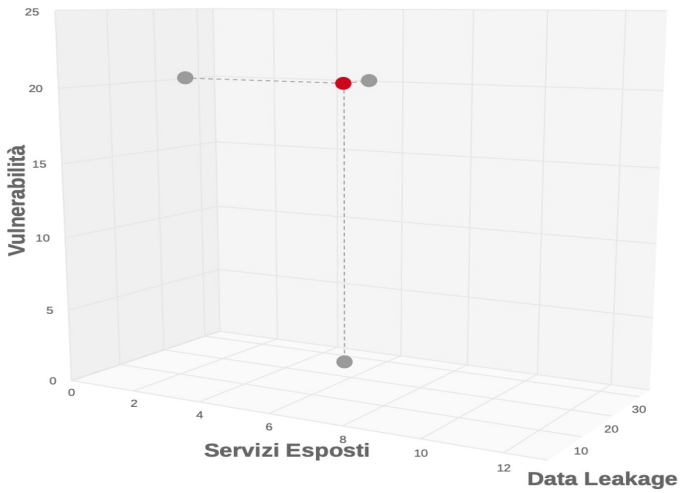
- Ai cyber criminali per verificare se un'azienda appare essere più o meno debole
- All'azienda per adottare eventuali procedure e contromisure per ridurre i rischi
- A un cliente che intende verificare se i suoi fornitori sono a rischio di attacchi informatici (tema della supply chain)
- A una banca che sta valutando di affidare un'azienda
- Ad un'assicurazione che sta valutando l'emissione di una polizza cyber
- A un potenziale acquirente di un'azienda

IC InfoCamere

DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

Indice di Esposizione Cyber



Il punto **ROSSO** rappresenta l'indice di esposizione Cyber dell'azienda.

Servizi Esposti	5
Vulnerabilità	20*
Data Leakage	27*

Indice di Esposizione Cyber

Nome Cliente

Data di elaborazione: 24/05/2022

IC InfoCamere

DINTEC CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

Partner tecnologico

YOROI TINEXTA CYBER

Servizi Esposti

In questa sezione vengono listati i vari servizi esposti all'esterno (rete Internet) i quali rappresentano appunto, la superficie di attacco esterna. Per ridurre la superficie di attacco, un'azienda dovrebbe analizzare tutti gli IP e servizi esposti all'esterno e ridurre l'accesso solo a quelli strettamente necessari. Per l'individuazione di tali servizi non sono state effettuate scansioni attive.

Host ***.197.168.123 **Posizione** Trieste, it **Servizi** 3	Porta: 22 Porta: 80 Porta: 443	Servizio (versione): OpenSSH (7.2p2 Ubuntu 4ubuntu2.10) Servizio (versione): Apache httpd (2.4.18) Servizio (versione): Apache httpd (2.4.18)
Host ***.40.23.136 **Posizione** Milano, it **Servizi** 1	Porta: 443	Servizio : Cloudflare http proxy
Host ***.61.191.142 **Posizione** Trieste, it **Servizi** 1	Porta: 443	Servizio : Apache httpd

Vulnerabilità

In questa sezione vengono rappresentati i *servizi esposti* con le annesse vulnerabilità di rete riscontrate.

Host : Porta
*****.197.168.123 : 80**
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1312

Gravità:

CRITICAL

Score:

9.8

Vettore di Attacco:

NETWORK

Data:

26/03/2018 17:29

Descrizione:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Vulnerabilità

In questa sezione vengono rappresentati i *servizi esposti* con le annesse vulnerabilità di rete riscontrate.

Host : Porta
***.197.168.123 : 80**
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1312

Gravità:

CRITICAL

Score:

9.8

Vettore di Attacco:

NETWORK

Data:

26/03/2018 17:29

Descrizione:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Host : Porta
***.197.168.123 : 80**
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1333

Gravità:

HIGH

Score:

7.5

Vettore di Attacco:

NETWORK

Data:

18/06/2018 20:29

Descrizione:

By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

Host : Porta
***.197.168.123 : 443**
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1312

Gravità:

CRITICAL

Score:

9.8

Vettore di Attacco:

NETWORK

Data:

26/03/2018 17:29

Descrizione:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Host : Porta
***.197.168.123 : 80
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1333

Gravità:

HIGH

Score:

7.5

Vettore di Attacco:

NETWORK

Data:

18/06/2018 20:29

Descrizione:

By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

Host : Porta
***.197.168.123 : 443
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1312

Gravità:

CRITICAL

Score:

9.8

Vettore di Attacco:

NETWORK

Data:

26/03/2018 17:29

Descrizione:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Data Leakage

Questa sezione presenta quali leak contenenti account aziendali sono potenzialmente disponibili ad un attaccante. Nel caso in cui un leak contenga una password, sia essa in chiaro o meno, verrà mostrata l'icona di *Data Leakage* sotto la dicitura *Passwords*. La sorgente di un data leak può avere diverse origini come: collezioni di credenziali, basi di dati esposte o simili .

Account		
*****@customer.com	Sorgente del leak:	Copy of apollo.io.v5__3___part_1.csv
	Data di ultima rilevazione:	23-10-2021 00:00
	Passwords:	Hash della Password

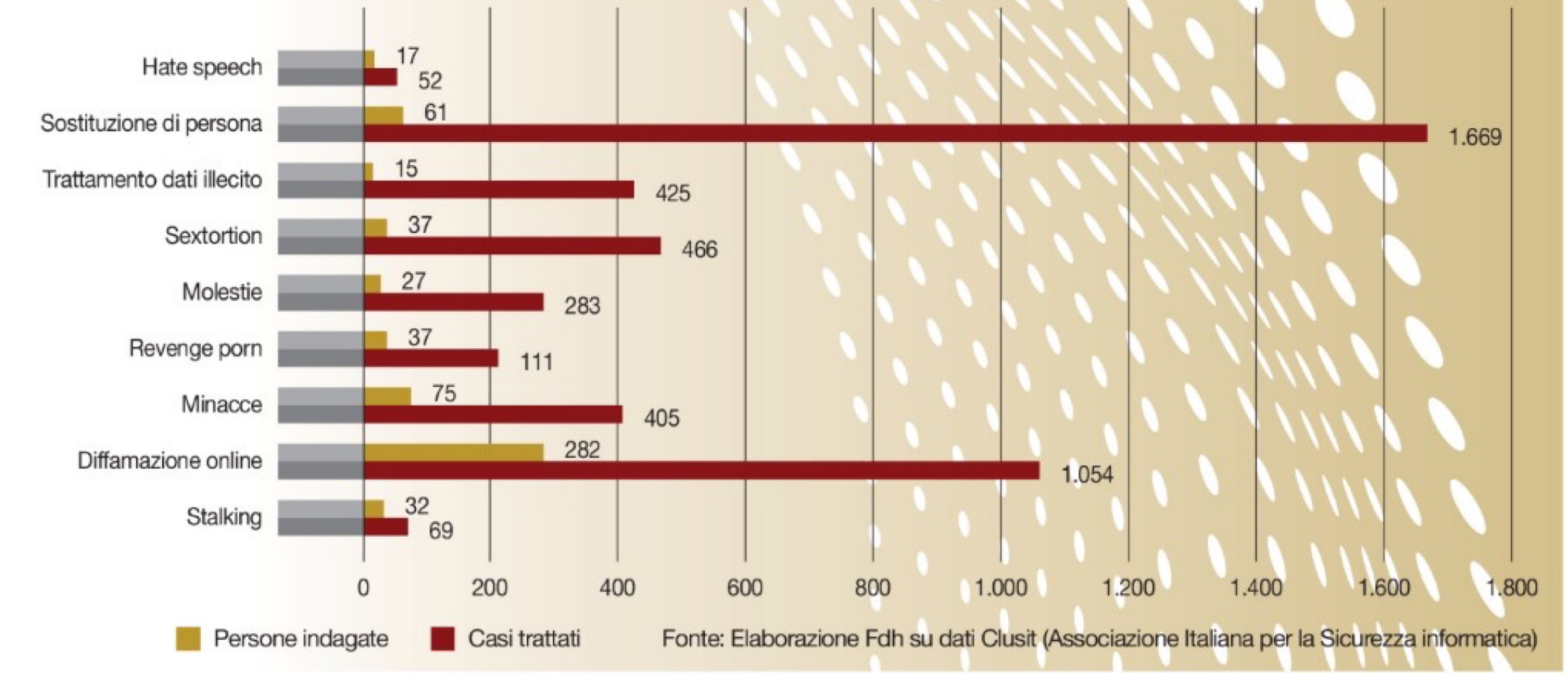
Account		
*****@customer.com	Sorgente del leak:	Flashbay.com 208k.txt
	Data di ultima rilevazione:	05-10-2021 00:00
	Passwords:	Hash della Password

Account		
*****@customer.com	Sorgente del leak:	United_States.txt.00
	Data di ultima rilevazione:	24-09-2021 12:00
	Passwords:	Hash della Password

Account		
*****@customer.com	Sorgente del leak:	Italy.txt
	Data di ultima rilevazione:	24-11-2021 12:00
	Passwords:	Password in Chiaro


BUY
SELL
HOME
LAND
RENT

Attività della polizia postale nei primi sei mesi del 2022



Fonte: Elaborazione Fdh su dati Clusit (Associazione Italiana per la Sicurezza informatica)


95-59
NL

IC InfoCamere

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

Partner tecnologico

YOROI
TINEXTA CYBER

Authorized to Use CERT℠
CERT is a mark owned by Carnegie Mellon University

TF-CSIRT
Trusted Introducer