

Cyber threat assessment

Demo Test

Executive Summary

Cyber threat assessment
20/05/2020

COME VIENE CONDOTTA

L'analisi viene condotta interrogando database pubblici e privati al fine di rilevare evidenze di eventi che possano aver messo/mettersi a rischio la sicurezza del perimetro esaminato. Ove previsto, viene effettuato un assessment della rete pubblica con scanner di rete in grado di rilevare le vulnerabilità dell'infrastruttura esposta.

P2P

85

Applicazioni scaricate
tramite file sharing con
potenziale codice
malevolo.

MALWARE

281

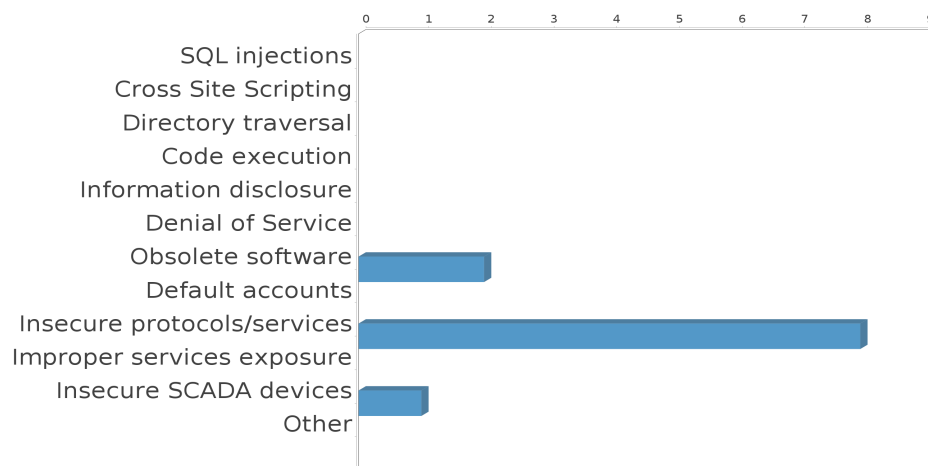
Eventi riportati attraverso
analisi di botnet

BREACHES

38

Dati aziendali riscontrati in
databreach

VULNERABILITIES



CYBER INCIDENTS



19%

degli host analizzati ha almeno una
vulnerabilità grave

114

numero totale degli incidenti riportati

Infezioni Malware

Cyber threat assessment
20/05/2020

Malware, diminutivo di malicious software, è un termine con cui ci si riferisce ad una varietà di minacce software. Questi software sono sviluppati specificatamente per ottenere accesso, spiare, rubare dati o danneggiare computer senza che il proprietario ne sia a conoscenza. Ci sono vari tipi di malware come virus, worm, cavalli di troia, ransomware, spyware, adware e scareware.

0 infezioni
attive

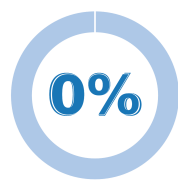
infezioni recentemente identificate
che fanno pensare alla presenza
attiva di minacce all'interno della
rete aziendale

14 infezioni
inattive

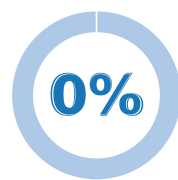
Infezioni passate correlate a
minacce non più attive all'interno
della rete aziendale

8 potenziali
infezioni

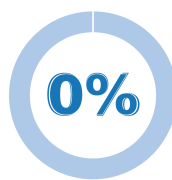
infezioni che possono essere state
bloccate da antivirus o altri sistemi
di sicurezza della rete aziendale



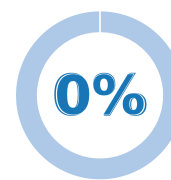
Data stealer



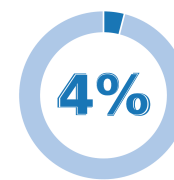
Rootkit



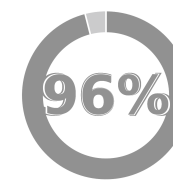
Extortion



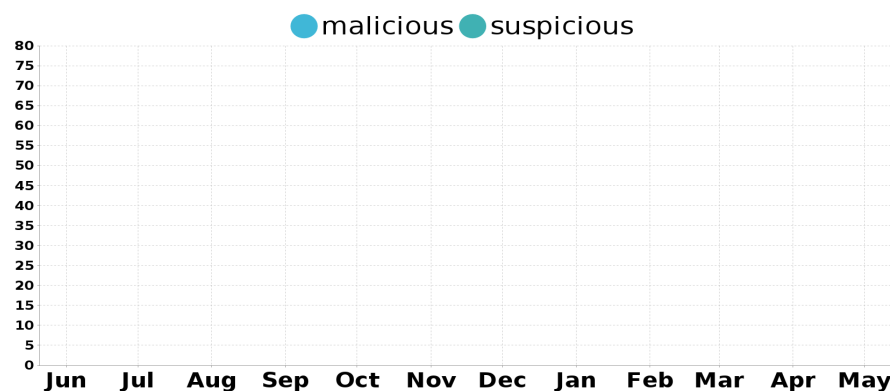
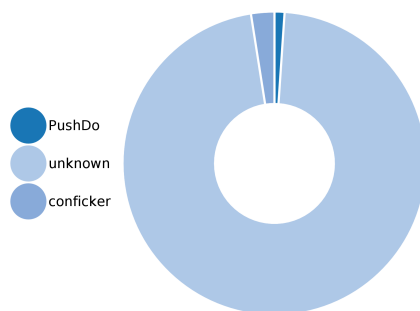
Cryptomining



Multi-purpose



Other/unknown



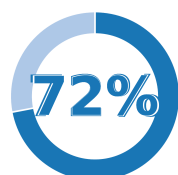
Data breach

Cyber threat assessment
20/05/2020

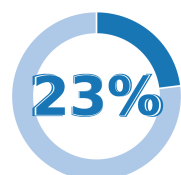
Con il termine data breach si intende un incidente informatico in cui i dati sensibili, riservati o aziendali vengono consultati, copiati, diffusi da un soggetto non autorizzato, solitamente esterno all'organizzazione della vittima.

1 data breach sensibili verificati

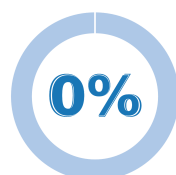
Data breach che sono stati verificati e che contengono dati sensibili



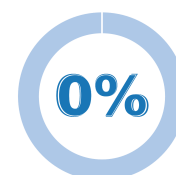
Third party breach



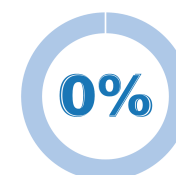
Deepweb combo list



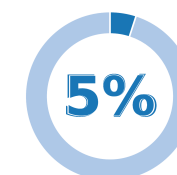
Deepweb spam list



Hacker forum post



Code-snippet post



Text-sharing post

2 data breach verificati

Data breach che sono stati verificati e che non contengono dati sensibili

4 data breach non verificati

Data breach che non sono stati verificati e che necessitano di ulteriori approfondimenti

35

email addresses

14

cleartext pwd/keys

43

non cleartext pwd/keys

0

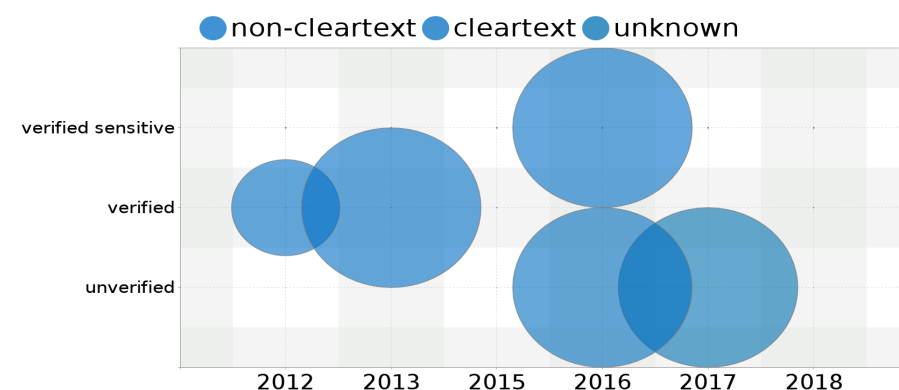
db dump/PII

3

IT assets

0

financial assets



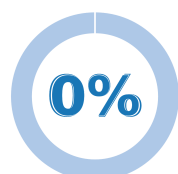
File sharing

Cyber threat assessment
20/05/2020

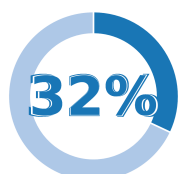
BitTorrent è un protocollo di condivisione file peer-to-peer (P2P) utilizzato per lo scambio di file in rete. Sebbene il termine BitTorrent non sia sinonimo di pirateria, il suo utilizzo più comune riguarda il download di materiale potenzialmente pericoloso e protetto da copyright, inclusi giochi, libri protetti dal diritto d'autore, film e così via.

1 trasferimenti
attivi

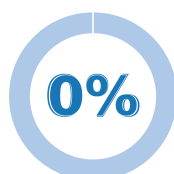
Attività di file sharing identificate
che potrebbero essere tutt'ora
attive



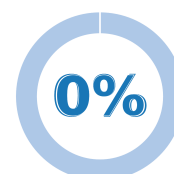
Application



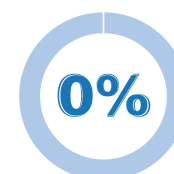
Audio



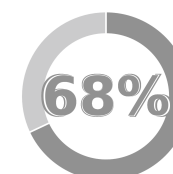
Games



Books



Video



Other/unknown

84 trasferimenti
inattivi

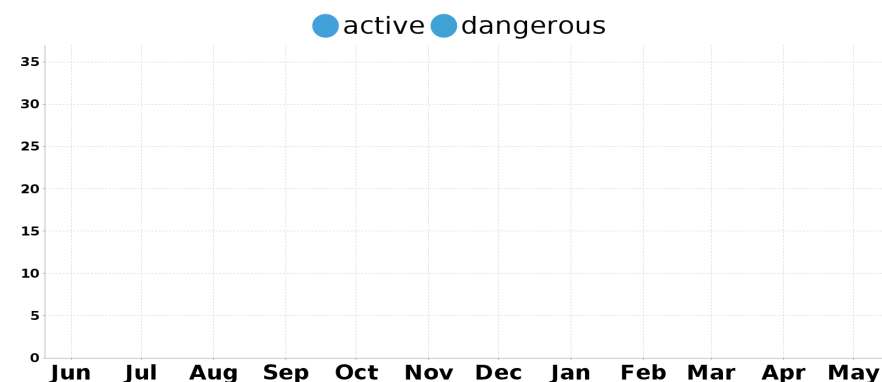
Attività di file sharing identificate
nel passato che probabilmente non
sono tutt'ora attive

0 trasferimenti
pericolosi

Attività di file sharing che
potrebbero contenere applicazioni
pericolose

Lista degli ultimi download:

The.Sims.4.Dine.Out.INTERNAL-RELOADED
This Butt's 4 U 3 - Alexis Texas; Rita Faltoyano; Maria Bellucci
Ryszard Ąwirlej - R  czna Robota [PL] eds [[email   protected]]
Izabela Trojanowska - Na Skos (2016) [[email   protected]]
Georges Brassens - Discografia [Mp3 128-160 kbps] [TNT Village]
Izabela Trojanowska - Na Skos (2016) [[email   protected]]
Ryszard Ąwirlej - R  czna Robota [PL] eds [[email   protected]]
Marcin Wro  ski - Komisarz Maciejewski 1-8 [PL] eds [[email   protected]]
Rezerwat - Dotykaj (2016) [[email   protected]]
Rezerwat - Dotykaj (2016) [[email   protected]]



L'analisi è stata eseguita tramite tecniche di intelligence. Un discovery passivo dei servizi, porte e vulnerabilità degli hosts è stato eseguito attraverso tecniche che non coinvolgono attività di ethical hacking, quindi il rilevamento delle vulnerabilità potrebbe non essere esaustivo.

3 vulnerabilità gravi

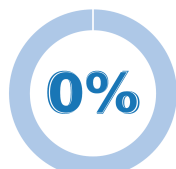
Le vulnerabilità gravi possono consentire ad un attaccante di compromettere la rete aziendale e/o consentire l'esfiltrazione di informazioni riservate.

8 vulnerabilità medie

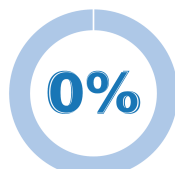
Le vulnerabilità medie possono consentire ad un attaccante di compromettere la rete aziendale, ma in alcuni casi non possono essere sfruttate in modo efficace.

0 vulnerabilità lievi

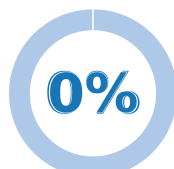
Le vulnerabilità lievi possono consentire ad un attaccante di ottenere informazioni utili a perpetrare attacchi.



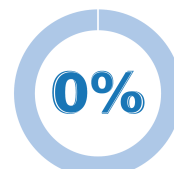
SQL injections



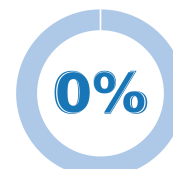
Cross Site Scripting



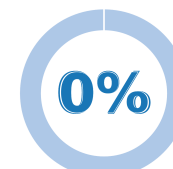
Directory traversal



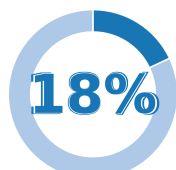
Code execution



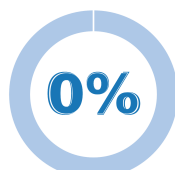
Information disclosure



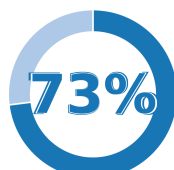
Denial of Service



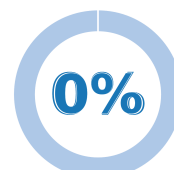
Obsolete software



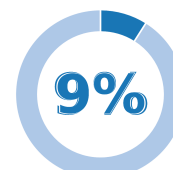
Default accounts



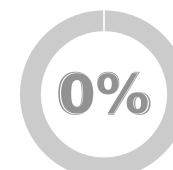
Insecure protocols/services



Improper services exposure



Insecure SCADA devices



Other