Swascan
TINEXTA GROUP

Botnet in Italia: il report 2021

www.swascan.com
info@swascan.com

Botnet: 95.000 Dispositivi In Italia Sono Infetti

I potenziali rischi analizzati nel report Swascan, che ha identificato oltre 95.000 dispositivi infetti nel 2021.

Le botnet sono una crescente minaccia nel panorama Cyber del 2022. Queste reti di computer infetti (molto spesso a insaputa degli utenti), vengono utilizzate per lanciare cyber attacchi o per compiere massicce operazioni di sorveglianza e raccolta e vendita delle informazioni e credenziali rubate.

Il Security Operation Center di Swascan, attraverso la sua piattaforma proprietaria di **Cyber Threat Intelligence**, ha analizzato e identificato oltre 95.000 dispositivi parte di Botnet nel nostro Paese lo scorso anno. Dispositivi che – nel periodo preso in esame – sono stati utilizzati per connettersi a Facebook Si precisa che Facebook che non ha nessuna responsabilità, piuttosto, le responsabilità ricadono sui singoli utenti.

Nel report seguente, una breve analisi delle implicazioni derivanti da questi comportamenti osservati.

Sommario

Premessa P.04

Cos'è una botnet? P.04

Come si diffonde una botnet P.05

Le credenziali P.07

Social networks P.07

I rischi Cyber P.08

I rischi per le aziende P.08

Le Botnet nelle regioni Italiane P.09

Come difendersi: i privati P.10

Come difendersi: le aziende P.11

Cyebr Security framework P.12

About us P.13

Disclaimer P.14

Premessa

Nel 2021 il Security Operation Center di Swascan, tramite la piattaforma proprietaria di Cyber Threat Intelligence, ha identificato oltre **95mila dispositivi infetti** (zombie o bot) facenti parte di botnet.
Parliamo di malware che potenzialmente hanno anche funzionalità di spyware: copiano e rubano tutto quello che l'utente digita sulla tastiera.

Cos'è Una Botnet?

Per comprendere i rischi associati a questi dati, dobbiamo fare un passo indietro e comprendere come opera una botnet.

Una botnet (abbreviazione di "rete di robot") è una rete di dispositivi – pc, notebook, cellulari, tablet, apparati IOT quali gli elettrodomestici di ultima generazione - infettati da malware. Tutti questi bot sono sotto il controllo di un unico aggressore che può controllarli ed eseguire dei comandi a totale insaputa del legittimo proprietario. Ogni singola macchina sotto il controllo del Criminal Hacker è conosciuta come un bot.

Da un'unica interfaccia, l'attaccante può comandare ogni dispositivo della sua botnet per eseguire simultaneamente un'azione criminale coordinata.

La dimensione di una botnet (molte sono composte da milioni di bot) permette all'attaccante di eseguire azioni su larga scala.

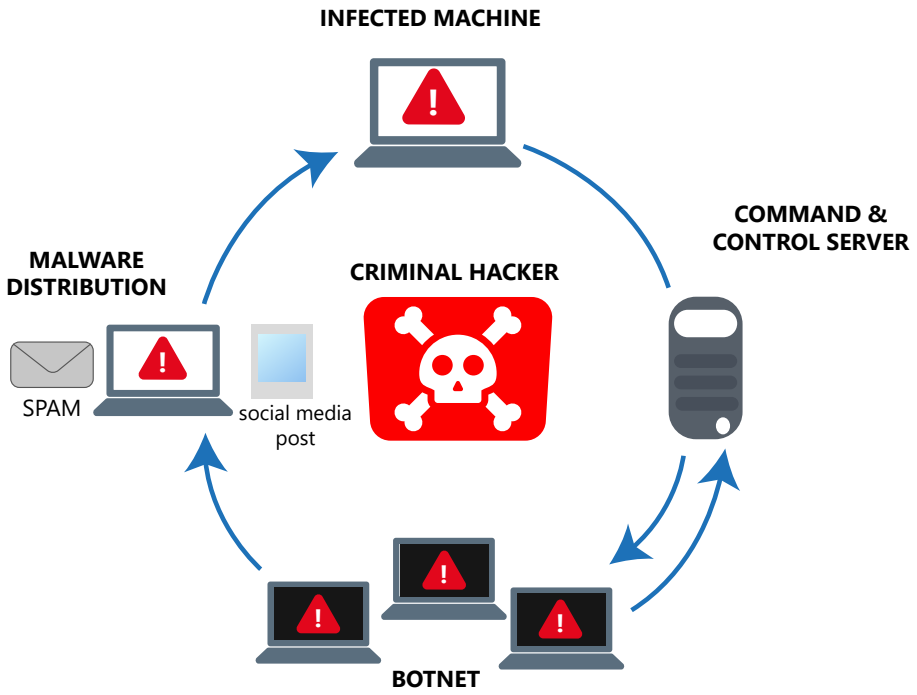
Poiché le botnet rimangono sotto il controllo di un aggressore remoto, le macchine infettate pos-sono essere spente, avviate, riavviate, ricevere aggiornamenti e cambiare il loro comportamento in pochi istanti.

Come Si Diffonde Una Botnet

I malware che trasformano il computer in un bot sono come qualsiasi altro malware;

- Possono diffondersi, ad esempio, attraverso azioni di social engineering (il malware è all'interno di un allegato ricevuto via e-mail o di una mobile app);
- Attraverso azioni più complesse, sfruttando vulnerabilità di altri software, vulnerabilità trovate, magari, grazie all'utilizzo della botnet stessa, utilizzata per fare la scansione di altri computer, alla ricerca dei punti deboli.

Una volta che il destinatario apre il file dannoso sul suo computer o comunque viene infettato, il bot "fa rapporto" al server di comando e controllo dove il bot-herder può dettare i comandi ai computer infetti o estrapolarne dati sensibili a suo piacimento, dati che includono spesso e volentieri le credenziali.



BOTNET E CREDENZIALI

FASE 1. DIFFUSIONE BOTNET E INFEZIONE

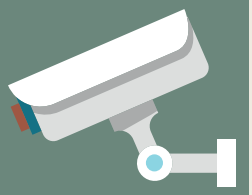
LE BOTNET SONO COME QUALSIASI ALTRO MALWARE, POSSONO ESSERE DIFFUSE SIA COME PAYLOAD DI UN VIRUS/TROJAN SIA ATTRAVERSO SOCIAL ENGINEERING (MAGARI ALLEGANDO IL MALWARE AD UNA MAIL...)

FASE 2. BOTNET ATTIVO SU PC BERSAGLIO

UNA VOLTA CHE IL DESTINATARIO APRE IL FILE DANNOSO SUL SUO COMPUTER O COMUNQUE VIENE INFETTATO, IL CRIMINAL HACKER PUÒ DETTARE I COMANDI AI COMPUTER INFETTI O ESTRAPOLARME DATI SENSIBILI A SUO PIACIMENTO, DATI CHE INCLUDONO SPESSO E VOLENTIERI LE CREDENZIALI

FASE 3. BOTNET SCARICA KEYLOGGER

LE BOTNET TRAMITE KEYLOGGER RACCOLGONO LE CREDENZIALI DEGLI UTENTI: NICKNAME, NOMI UTENTI, PASSWORD, PIN CODE E QUANT'ALTRO VIENE USATO PER ACCEDERE AI PROPRI PROFILI SOCIAL, ALLE PROPRIE MAIL SIA AZIENDALI CHE PRIVATE, ALLA VPN AZIENDALE PER LAVORARE DA REMOTO, AL PROPRIO CONTO CORRENTE BANCARIO E ALLA PROPRIA CARTA DI CREDITO.



FASE 4. LE NOSTRE CREDENZIALI VENGONO COMPROMESSE ED ESFILTRATE

UNA VOLTA CHE LE NOSTRE CREDENZIALI SONO STATE VIOLATE I CRIMINAL HACKER POSSONO COMPIERE FURTO DELL'IDENTITÀ, RICATTI E ATTIVITÀ DI SOCIAL ENGINEERING NEI CONFRONTI DEI NOSTRI CONTATTI SOCIAL.

Le Credenziali

Come accennato uno dei compiti delle botnet è quello di raccogliere le credenziali degli utenti: nickname, nomi utenti, password, pin code e quant'altro viene usato per accedere ai propri profili social, alle proprie mail sia aziendali che private, alla VPN aziendale per lavorare da remoto, al proprio conto corrente bancario e alla propria carta di credito.

Ma anche se spesso sentiamo parlare di credenziali compromesse, il rischio che scaturisce dal furto di credenziali tramite Botnet è più alto, non solo per gli account di singoli privati, ma anche per gli account aziendali.
Questo perché sono i nostri dispositivi ad essere stati compromessi da un malware.
È una minaccia completamente endogena al nostro device.

Social Networks

Swascan ha osservato e identificato numerose botnet all'opera sul territorio del nostro Paese.

Durante l'analisi sono stati identificati **95.991 dispositivi italiani compromessi che si sono connesse al social più diffuso del mondo.**

I dati fanno riferimento, in particolare, ai dispositivi che – mentre erano sotto il controllo di botnet – si erano connessi a "it-it.facebook.com".

Questo è un indicatore importante: Il livello di diffusione di utenti del popolare social network permette infatti di contestualizzare il numero di dispositivi "infetti" associati e dunque anche le relative credenziali, potenzialmente compromesse.
Siamo di fronte, quindi, ad oltre 95mila utenti che – inconsciamente – hanno potenzialmente utilizzato il proprio device per inserire credenziali, mentre erano sotto osservazione.

Facebook è stato, in un certo senso, il canarino nella miniera...

I Rischi Cyber

Ovviamente nessuna responsabilità è ascrivibile a Facebook, che è stata usata semplicemente come indicatore. Piuttosto, le responsabilità ricadono sui singoli utenti. Ed infatti, le conseguenze di rendere disponibili a livello pubblico e semipubblico credenziali di accesso ai social espone ogni utente ad attacchi informatici di diverso tipo:

- Account take Over: furto dell'identità
- Ricatto
- Attività di social engineering nei confronti dei contatti social

Non dobbiamo dimenticare che, nel caso specifico, parliamo di dispositivi infettati da un malware che copia tutto e che permette all'attaccante di poter avere accesso a ogni dato e a ogni comando digitato. Di conseguenza non parliamo solo delle credenziali di Facebook, ma potenzialmente di qualsiasi credenziale abbiamo usato per altri sociali o per altri servizi, quali l'home banking; inoltre oltre le credenziali, anche i nostri documenti, le foto, le nostre immagini e i nostri video salvati sul dispositivo, o magari su un nostro cloud, possono essere evidentemente sotto il totale controllo del criminale.

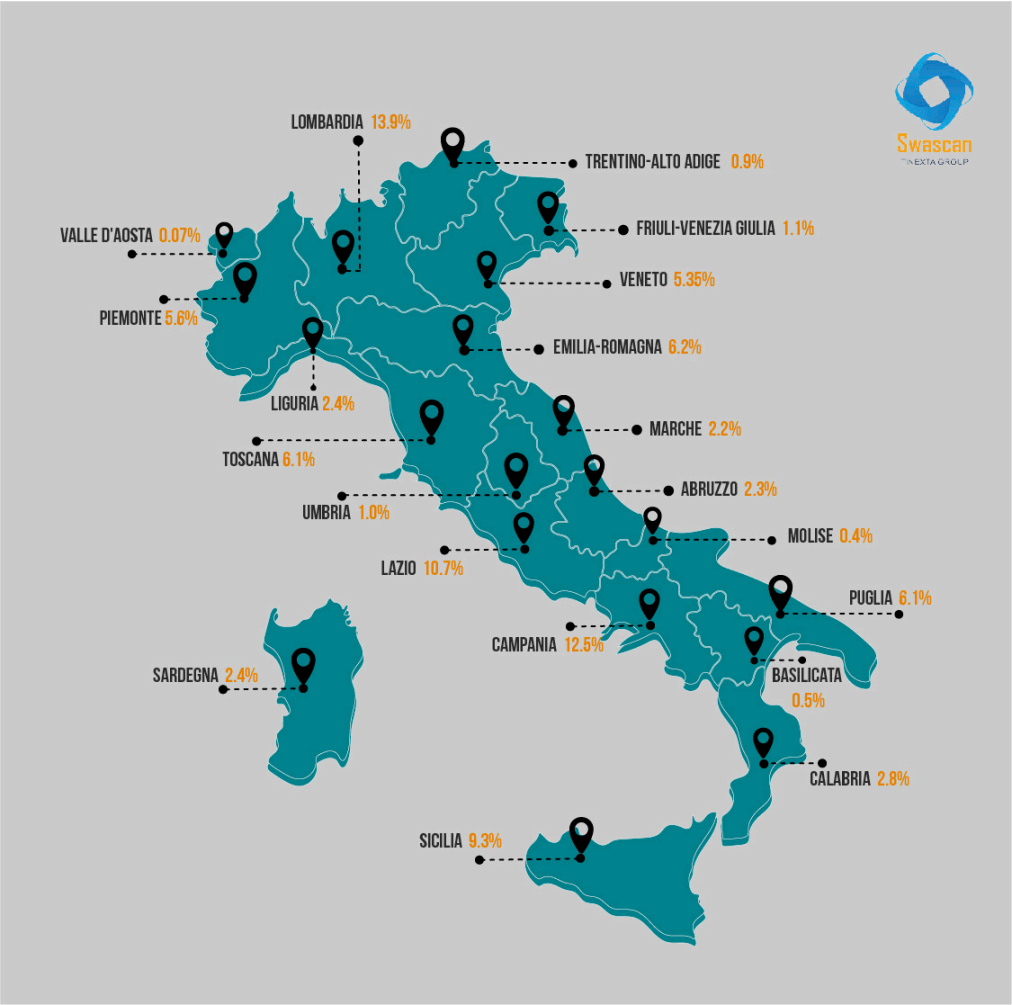
I Rischi Per Le Aziende

I dispositivi infettati sono anche quelli che usiamo spesso anche per lavoro. Quindi possono essere a disposizione degli attaccanti anche le credenziali di accesso ai sistemi webmail, ai sistemi di connessione remota e anche a documenti riservati, esponendo le aziende per le quali operiamo a rischi di:

- Attacchi ransomware
- Phishing e Spear Phishing
- Spionaggio
- ...

Le Botnet Nelle Regioni Italiane

Dagli oltre 95mila device, **Il SOC Swascan** ha isolato e analizzato il **24% degli IP** che sono stati suddivisi per area geografica:



Logicamente, maggiore sarà il numero di abitanti della regione, maggiore sarà la diffusione delle botnet.

Il risultato della ricerca conferma un rischio altissimo per numerosi utenti privati che – a loro insaputa – stanno esponendo la propria identità digitale, ma allo stesso tempo un rischio concreto per le aziende. Le botnet - reti di computer infettati da un malware e controllate da Criminal Hacker - tra le varie funzioni, sono in grado di registrare tutto quello che digita un utente sul proprio dispositivo.

Questa situazione potrebbe tradursi concretamente in un elevato rischio di attacchi ransomware

Come Difendersi: I Privati

Le botnet fanno leva su vulnerabilità molto conosciute e sul social engineering per attaccare i singoli utenti.

Utilizzare dove possibile l'autenticazione a due fattori è un'ottima prima misura.
Altre best practice da non dimenticare sono:

- Mantenere il sistema operativo aggiornato
- Non aprire file da fonti sconosciute o sospette
- Scansionare tutti i file scaricati prima di eseguirli.
- Non cliccare su link sospetti
- Installare un programma antivirus scelto da vendor affidabili e riconosciut

Come Difendersi: Le Aziende

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber:

Sicurezza Predittiva

1. Identifica le minacce aziendali fuori dal perimetro aziendale operando a livello di Web, Darkweb e Deep Web.
2. Ricerca eventuali minacce emergenti.
3. Effettua attività di Early Warning.
4. Fornisce le evidenze alla Sicurezza Preventiva.
5. Indica le aree di attenzione alla Sicurezza Proattiva.

Sicurezza Preventiva

1. Verifica e misura il Rischio Cyber.
2. Definisce i piani di remediation.
3. Indica il Rischio esposto al Layer di Sicurezza Proattiva.
4. Fornisce le aree di Investigazione alla Sicurezza Predittiva.

Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale.
2. Contrasta e blocca gli attacchi informatici.
3. Gestisce i Cyber Inciden.
4. Fornisce le evidenze alla Sicurezza Preventiva.
5. Indica le aree di investigazione alla Sicurezza Predittiva.

Cyebr Security Framework

Sicurezza Predittiva

1. Domain Threat Intelligence
2. Cyber Threat Intelligence
3. Early Warning Threath Intelligence
4. Technology Monitoring
5. Social Threat Intelligence
6. Supply Chain Cyber Risk

Sicurezza Preventiva

1. 1. Vulnerability Assessment
2. 2. Network Scan
3. 3. Penetration Test
4. 4. Code Review
5. 5. Phishing Attack
6. 6. Smishing Attack
7. 7. Security Management
8. 8. GRC Assessment
9. 9. Cyber Academy
10. 10. DevSecOps
11. 11. Cyber Security Framework Checkup
12. 12. Ransomware Attack Simulation
13. 13. SOC Performance Simulation
14. 14. Zero Day Attack Simulation
15. 15. CISO as a Service
16. 16. Competence Center as a Service

Sicurezza Proattiva

1. Security Operation Center
2. Incident Response Team

About us

Swascan

è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa. La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence,** oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo. Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Technical Contributors:

Pierguido Iezzi
Fabrizio Rendina
Andrea D'Angelo
Dario Buonocore
Riccardo Michetti
Riccardo D'Ambrosio
Matteo Biagini
Mario Cambria
Daniele Scozia
David Brunetti
Alessandra Garau
Ricardo Bracale
Soc Swascan Team.

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI

Disclaimer

La ricerca svolta da Swascan si è basata su siti contenenti dati e numeriche fonti di ricerche OSINT e CLOSINT tramite Threat Intelligence.
Questa pubblicazione non rappresenta necessariamente lo stato dell'arte – data la natura transitoria delle fonti – e Swascan si riserva la prerogativa di aggiornamento periodico.
Fonti di terze parti sono citate a seconda dei casi. Swascan non è responsabile del contenuto delle fonti esterne, compresi i siti web esterni a cui si fa riferimento in questa pubblicazione.
La presente pubblicazione ha uno scopo puramente informativo. Essa deve essere accessibile gratuitamente.
Né Swascan né alcuna persona che agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.