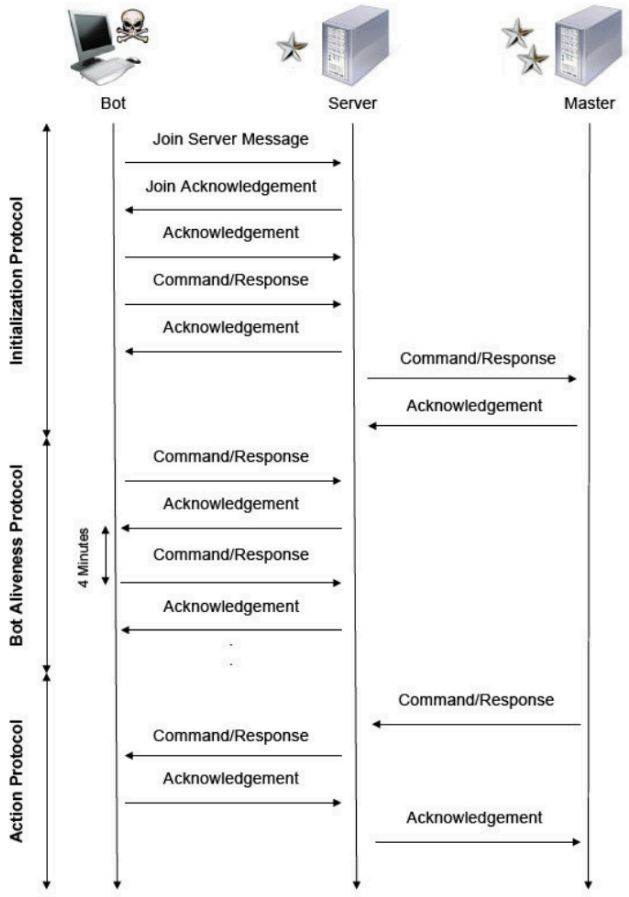
Raport consolidat eveniment cibernetic

Mariposa.Botnet

Botnetul Mariposa s-a răspândit prin intermediul unor atașamente de e-mail malițioase, site-uri web compromise și vulnerabilități ale sistemelor de operare. Odată ce un sistem era infectat, malware-ul Mariposa se instala și se conecta la un server C&C.

- **Colectarea datelor:** Mariposa colectează informații personale, date de autentificare și alte date sensibile de pe sistemele infectate.
- **Atacuri DDoS:** Botnetul poate fi folosit pentru a lansa atacuri de tip Denial-of-Service (DoS) împotriva unor ținte specifice.
- **Spam:** Mariposa poate fi folosit pentru a trimite spam și mesaje de phishing.
- **Alte activități malițioase:** Botnetul poate fi folosit pentru a efectua diverse alte activități malițioase, cum ar fi furtul de identitate, fraudarea conturilor bancare și distribuirea de malware.



Informații sumare

TIP	***Botnet***
MD5	1. 6939c088f59258da7410f66837c62192 2. f4e2c305ef2d38b6d4e4be9d19de16ed 3. 98812839bd6597ec86fad72a0f20d4e5 4. 56902dc35453158a34e85db5b590ab19 5. c4e13b7cb9425ef18d95d446cad9c3e0
SHA	1. **SHA1:** 500bb963602d45584303a4dc3f6fd6052a6752d8 2. **SHA256:**996c2667b2bcf86c9c7c20d7c79a3024131c84e0d82d5338db99812830ad778a
Instrumente pentru analiză	1. **Pentru scanarea rețelei** – Wireshark, TCPDUMP, Angry IP Scanner 2. **Pentru scanarea de viruși și malware** – Software antivirus existente 3. **Anliză și detectare procese** - Lordpe, Sysmon , Procces Hacker
Comunicarea C&C	Mariposa folosește diverse metode de comunicare pentru a se conecta la serverele C&C, inclusiv: • **TCP/IP:** Botnetul poate comunica prin porturile TCP 80, TCP 8080 și UDP 53. • **DNS:** Mariposa poate comunica prin intermediul solicitărilor DNS. • **P2P:** Botnetul poate comunica prin intermediul rețelelor peer-to-peer (P2P).
DNS domain name ce comunica ca C&C server	• lalundelau.sinip.es • bf2back.sinip.es • thejacksonfive.mobi • thejacksonfive.us • thejacksonfive.biz • butterfly.BigMoney.biz • bfisback.sinip.es • bfisback.no-ip.org • qwertasdfg.sinip.es • shv4b.getmyip.com • shv4.no-ip.biz • butterfly.sinip.es • defintelsucks.sinip.es • defintelsucks.net • defintelsucks.com • gusanodeseda.sinip.es • gusanodeseda.net • legion.sinip.es • booster.estr.es • sexme.in • extraperlo.biz • legionarios.servecounterstrike.com • thesexydude.com • yougotissuez.com • gusanodeseda.mobi

	• tamiflux.org • tamiflux.net • binaryfeed.in • youare.sexidude.com • mierda.notengodominio.com
Detectare	1. Scanarea discurilor pentru fișiere executabile specifice 2. Monitorizarea traficului de rețea și porturilor menționate 3. Analiza detaliată a activității și modificărilor la nivel de registru 4. Verificarea prezenței unor procese, servicii sau conexiuni necunoscute
Recomandări generice	• **Izolarea dispozitivului compromis** -Identificați dispozitivul sau sistemele suspecte care ar putea face parte din botnet și izolați-le de rețeaua principală. Izolarea poate fi efectuată prin : deconectarea fizică a dispozitivelor sau restricționarea accesului acestora la rețea. • **Întreruperea comunicării cu serverul de comandă și control (C&C)** - Blocați traficul de ieșire către adresele IP cunoscute asociate cu serverele de comandă și control ale botnet-ului, le găsiți în descrierea din Anexă. Pentru aceasta utilizați firewall-uri sau soluții de filtrare a traficului. • **Actualizarea software-ului și a sistemelor (patch &update)** - Asigurați-vă că toate dispozitivele și sistemele din rețea sunt actualizate la cele mai recente versiuni, inclusiv sistemele de operare, aplicațiile și software-ul de securitate. Acest lucru ajută la remedierea vulnerabilităților cunoscute și la prevenirea reinfectării. • **Scanarea și curățarea dispozitivelor compromise** - Utilizați un antivirus actualizat și soluții anti-malware pentru a scana toate dispozitivele compromise în căutarea amenințărilor. Eliminați sau izolați fișierele și programele malware identificate. • **Resetarea dispozitivelor la starea implicită** - În cazul dispozitivelor care nu pot fi curățate sau încredințate, luați în considerare resetarea acestora la setările implicite de fabrică. Asigurați-vă că după resetare toate parolele implicite sunt schimbate și actualizate. • **Analiza log-urilor** - Analizați log-urile de securitate pentru a identifica activitatea suspectă și modelele de atac. Astfel puteți afla dacă unele porturi au rămas deschise sau sunt configurate greșit, iar remedierea acestor vulnerabilități va ajuta la creșterea nivelului de securitate din rețeaua locală. • **Reevaluarea securității rețelei** - Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.

Resurse externe

	https://defintel.com/docs/Mariposa_White_Paper.pdf