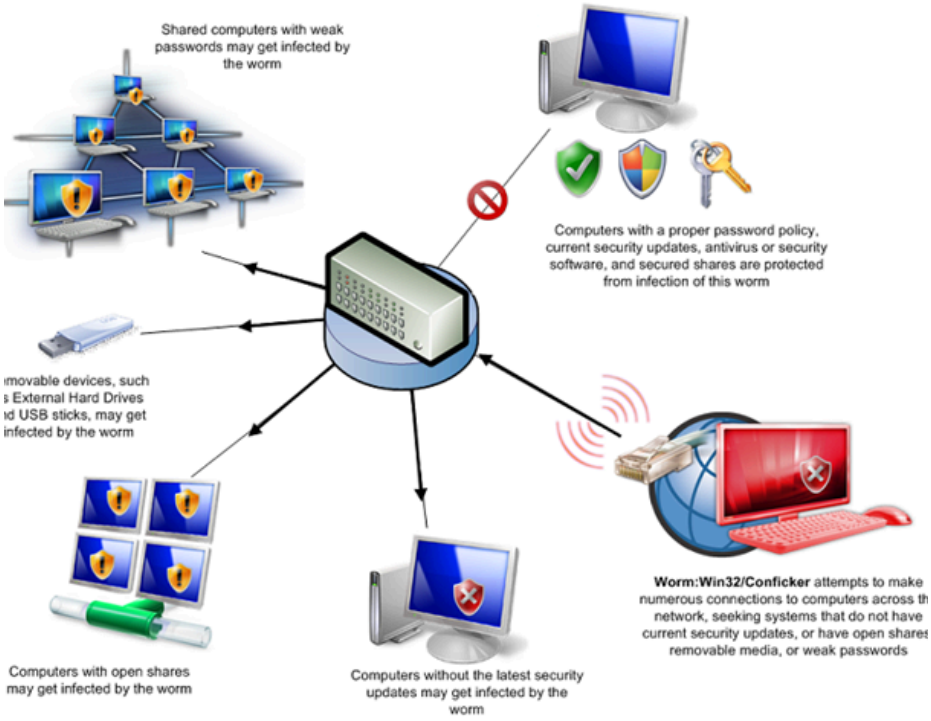
Raport consolidat eveniment cibernetic

Conficker.Botnet

Botnetul Conficker.Botnet exploatează vulnerabilități **RDP și serviciul Server de mesaje** pentru răspândire.

Persistent prin modificări la nivel de servicii, **autocron și registry.** Comunică cu C&C pe porturile TCP/UDP 139, 445, 4444, 80, 8080, 7080



Informații sumare

TIP	***Conficker.Botnet***
Instrumente pentru analiză	• **Pentru scanarea rețelei** – Wireshark, TCPDUMP, Angry IP Scanner ,Nmap • **Pentru scanarea de viruși și malware** – Software antivirus existente • **Analiză și detectare procese**- Lordpe, Sysmon , Procces Hacker
Aliases	• Mal/Conficker-A (Sophos) • Win32/Conficker.A (ESET) • Win32/Conficker.A (CA) • W32.Downadup (Symantec) • W32/Downadup.A (F-Secure) • Conficker.A (Panda) • Net-Worm.Win32.Kido.bt (Kaspersky) • W32/Conficker.worm (McAfee) • Win32.Worm.Downadup.Gen (BitDefender) • Win32:Confi (avast!) • WORM_DOWNAD (Trend Micro) • Worm.Downadup (ClamAV)
Detectare	1. Verificarea actualizării sistemului și patch-urilor critice 2. Monitorizarea porturilor mai sus menționate 3. Analiza fișierelor **system32** pentru localizarea artefactelor malițioase 4. Examinarea activității suspicioase pe nivel de servicii, procese sau conexiuni de rețea
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://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf*