Raport consolidat eveniment cibernetic

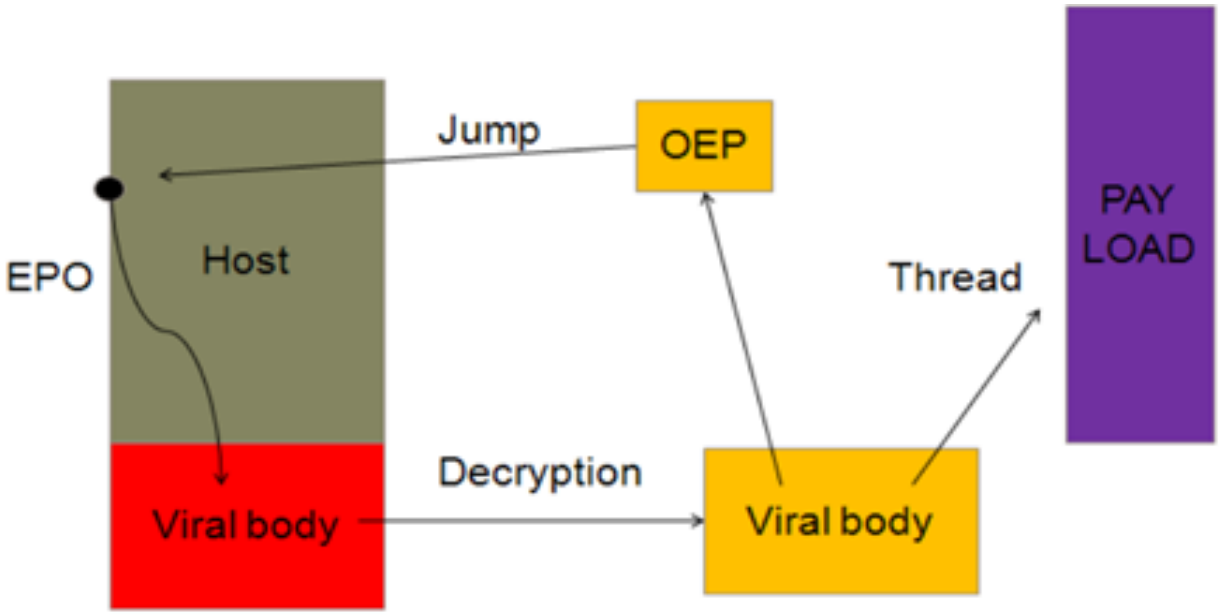
Sality Malware

Sality deseori adaugă propriul său cod malițios la sfârșitul fișierului infectat (sau gazdă), o tehnică cunoscută sub numele de prepending. Codul viral pe care Sality îl inserează este polimorfic, o formă de cod complexă menită să îngreuneze analiza.

Odată instalat pe sistemul computerului, virusurile Sality execută de obicei și o încărcătură malițioasă. Acțiunile specifice depind de varianta specifică în cauză, dar în general virusurile Sality vor încerca să termine procese, în special cele legate de programele de securitate.

Virusul poate încerca, de asemenea, să deschidă conexiuni către site-uri remote, să descarce și să ruleze fișiere malițioase suplimentare și să fure date de pe mașina infectată.

Sality se adaugă prin crearea unei noi secțiuni cu un nume de secțiune de „ {random characters} data” și are o dimensiune de 20480 de octeți.



Informații sumare

TIP	***Sality Malware***
Instrumente pentru analiză	1. **Pentru scanarea rețelei –** Wireshark, TCPDUMP 2. **Pentru scanarea de viruși și malware –** Software antivirus existente
Caracteristici	**ALIAS** · Virus:W32/Sality, · Virus.Win32.Sality, · Win32.sality, · Spyware.Pws.A, · Win32.sality.e **MD5** 5511db5cf4617bbce8cac0ccab17cea0 **SHA1** bfc6880eaf88f4a8aedceaf712d7be42d3fa4f93 **SHA256** 8e20fa7212d2922a157d7b986eb5f621e8e8eef5038ad1f07fd1d6523571fb55
Infectare	Comunica printr-o rețea peer-to-peer (P2P). Poate infecta oricare dintre următoarele extensii căutând fișiere care încep de la „C:\”: **.exe .scr** De asemenea, infectează fișierele cu extensii .EXE care sunt menționate ca date în următoarele chei de registry: **[HKCU\Software\Microsoft\Windows\CurrentVersion\run]** **[HLKM\Software\Microsoft\Windows\CurrentVersion\run]**
Recomandări generice	• **Izolarea dispozitivului compromis** -Identificați dispozitivul sau sistemele suspecte și izolați-le de rețeaua principală. Izolarea poate fi efectuată prin: deconectarea fizică a dispozitivelor sau restricționarea accesului acestora la rețea. • **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. • **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://aroundcyber.wordpress.com/wp-content/uploads/2012/11/sality_peer_to_peer_viral_network.pdf*
	*https://www.vmray.com/analyses/8e20fa7212d2/report/ioc.html*