Raport consolidat eveniment cibernetic

Informații suplimentare

Denumire	**H-Worm (alias: Houdini, Wshrat)**
Tip	Remote Access Trojan
Descriera	H-Worm este un malware bazat pe **VBS** (Visual Basic Script), care este proiectată să preia controlul asupra unui computer infectat. Tehnica folosită pentru cod îi foarte simplă: o variabilă este definită ca fals, apoi blocurile de cod sunt executate dacă variabila este adevărată. Utilizează **DNS dinamic** pentru comunicarea cu C&C servere.Solicitările C&C utilizează de obicei parametrii '**cmd**' și '**param**' Analiștii malware suspectează că autorul este o persoană care se numește 'Houdini' și se află în Algeria.
Vectori de infecție	• H-Worm este distribuit în principal prin campanii de phishing, folosind diferite niveluri de ofuscare ca: atacuri de inginerie social executate inteligent, documente malițioase, fișiere VBS sau scripturi auto-executabile (**T1566**) • Se mai poate răspândi cu ajutorul dispozitivelor de memorie externă (T1200).
Vectori de atac	• Furtul informațiilor și parole de sistem (**T1082**). • Keylogging (**T056.001**) • Descărcarea, redenumirea, executarea și ștergerea fișierelor • Înregistrarea capturilor de ecran. • Vizualizarea camerei web **(T1123**). • Executarea programelor și ștergerea datelor. • Controlul de la distanță a dispozitivului • Descoperirea Dispozitivului Periferic (**T1120**).

Persistența	• Se auto-copiază în directoare critice (***%AppData%, %Temp%, Startup***) (**T1547.001**). • Utilizarea scripturile malițioase pentru seta o cheie în Registry, astfel încât să ruleze la fiecare pornire a sistemului (**T1059**) (***HKEY_CURRENT_USER\Software\Microsoft\Windoww\CurrentVersion\Run***) • Manipularea de la distanță a dispozitivului în scopul ascunderii prezenții sale (**T1622**).
IOC	http[:]//kiomanito[.]freemyip[.]com/ http[:]//kezs[.]duckdns[.]org http[:]//franmhort[.]duia[.]ro http[:]//chongmei33[.]publicvm[.]com http[:]//paypalintelsassistant[.]duia[.]ro 133.242.129.155 212.193.30.230 198.12.123.17 37.0.14.198 104.168.7.110 34.105.85.231
Detectarea:	• Prezența fișierelor VBS necunoscute în %AppData% • Conexiuni suspecte către servere externe neautorizate • Chei de registru modificate pentru persistenta • Proces wscript.exe activ în mod anormal

Resurse externe

	https://isc.sans.edu/diary/Houdini+is+Back+Delivered+Through+a+JavaScript+Dropper/28746