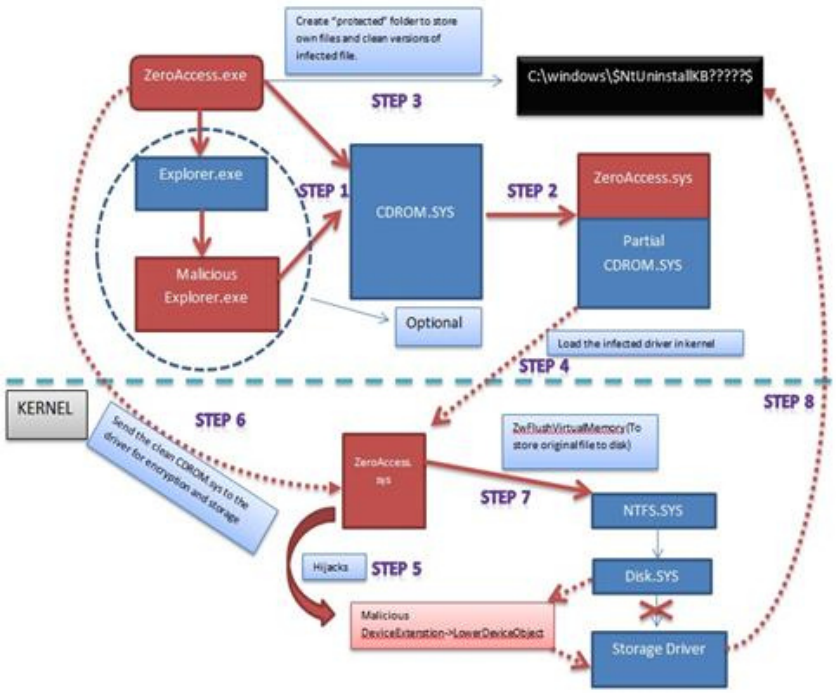
Raport consolidat eveniment cibernetic

ZeroAccess.Botnet

ZeroAccess Botnet cunocut uneori și ca Sirefef.Botnet este un troian specializat care afectează sistemele de operare Windows și descarcă malware pe o mașină infectată pentru a forma un botnet (de ex. Trojan.Win32.Jorik.IRCbot.xkt.) Așa cum a descoperit Symantec, troianul este distribuit folosind Blackhole Exploit Toolkit și Bleeding Life Toolkit.

Troianul apoi creează propriul sistem de fișiere ascuns, descarcă mai mult malware din mediul conectat și deschide backdoor pentru acces pe sistemul compromis.

Atacatorul poate apoi să efectueze acțiuni conform cerințelor sale, iar sistemul victimei devine parte a botnetului. Numele ZeroAccess a fost creat datorită faptului că o șir găsit în codul driverului kernel indică către folderul original al proiectului ZeroAccess. Este de asemenea numit codul max++ datorită capacității sale de a crea un obiect de kernel __max++>.



Informații sumare

TIP	**Botnet**
ALIAS	Sirefef, Zeroaccess, Kazy, Conjar, ZAccess, Zacess
Mod de infectare	Inițial are loc plasarea fișierelor: • %Application Data%\8c0f0459\@ • %Application Data%\8c0f0459\X • %Windows%\1493438348 Creează următoarele repozitorii: • %Application Data%\8c0f0459 • %Application Data%\8c0f0459\U
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	Modificările din registru pe care se spune că le face acest troian în sistemul victimei includ, de obicei, următoarele registre: HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices[FILE NAME OF INFECTED DRIVER]"ImagePath" = "*" HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices[FILE NAME OF INFECTED DRIVER]"Type" = "1" HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices[FILE NAME OF INFECTED DRIVER]"Start" = "3"
IOC comunicare C&C	IP adrese: • 69.176.14.76 • 76.28.112.31 • 24.127.157.117 • 117.205.13.113 • 200.59.7.216 • 113.193.49.54 NTP servere: • ntp2.usno.navy.mil • ntp.adc.am • chronos.cru.fr • wwv.nist.gov • clock.isc.org

	• time.windows.com • time2.one4vision.de • time.cerias.purdue.edu • clock.fihn.net • ntp.duckcorp.org • ntp.ucsd.edu • ntp1.arnes.si • ntp.crifo.org • tock.usask.ca
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://kryptoslogic.blogspot.com/2016/01/zeroaccess-3-analysis.html