SystemBC: il malware per nascondere il malware

Ago 02, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS 0

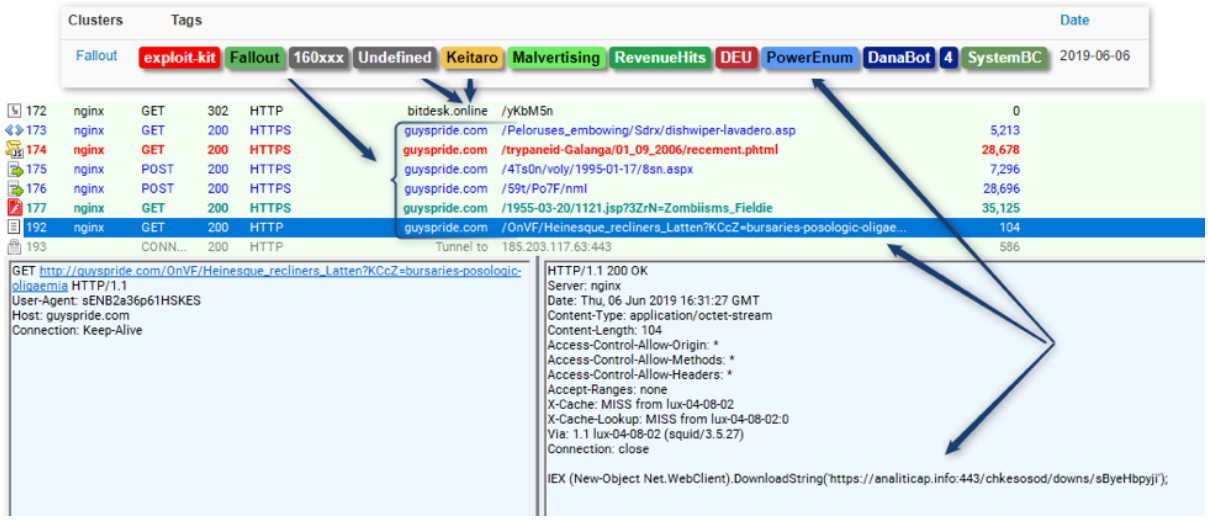
Il virus installa sui PC infetti un proxy che permette di nascondere il traffico Internet di altri software dannosi per impedirne il rilevamento.

I pirati informatici più scaltri utilizzano spesso strumenti per offuscare le comunicazioni dei malware che utilizzano. Il motivo è piuttosto ovvio: la presenza di comunicazioni sospette è infatti uno degli indizi che i software di sicurezza utilizzano per individuare la presenza di software dannoso.

Di solito strumenti di questo tipo sono inclusi nei malware più complessi, spesso dotati di una struttura modulare, e non sono molto diffusi.

Da oggi, però, sembra che tutti i cyber-criminali possano contare su un formidabile strumento di offuscamento. Si chiama **SystemBC** ed è un malware autonomo, che ha la funzione specifica di "supportare" altri programmi nocivi.

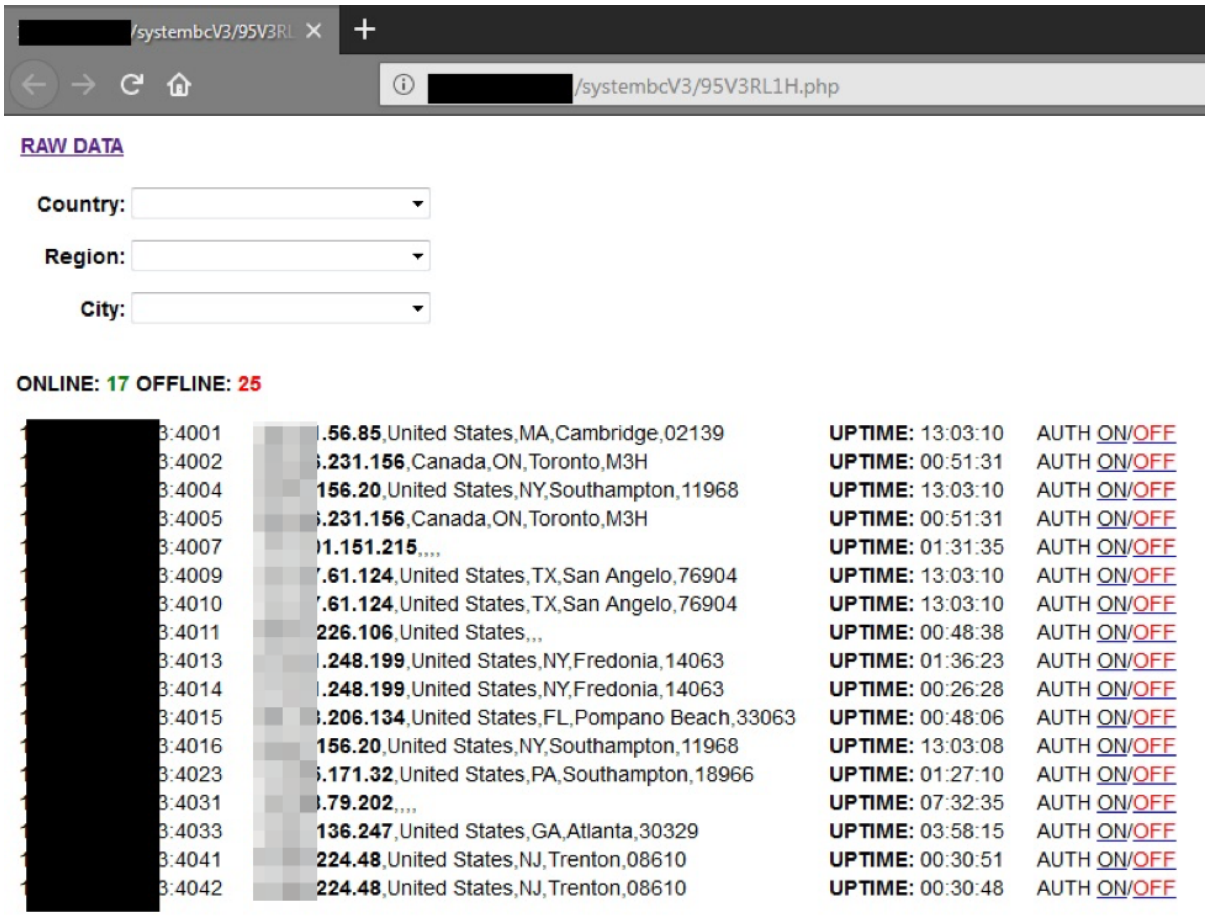
Come spiegano i ricercatori di **Proofpoint** in questo report, SystemBC installa sul computer infetto un proxy SOCKS5 che consente di occultare il traffico di qualsiasi "collega" installato sullo stesso computer.



Gli esperti di sicurezza lo hanno individuato per la prima volta lo scorso 6 giugno, mentre analizzavano una campagna di attacchi portata attraverso un Exploit Kit e che aveva come obiettivo principale la diffusione del ransomware **Maze**.

Nelle settimane successive, però, dalle parti di Proofpoint hanno incrociato SystemBC più volte in occasione di attacchi portati da altri gruppi di cyber-criminali, ad esempio per diffondere il trojan bancario **Danabot**. La conclusione dei ricercatori è che il malware sia venduto nei bassifondi del Web come strumento di copertura.

Intuizione confermata quando i ricercatori hanno trovato un “annuncio pubblicitario” che, oltre alla descrizione di SystemBC, conteneva anche degli screenshot del sistema di controllo.



SystemBC utilizza **un sistema di crittografia XOR a 40 byte** per proteggere informazioni come l'indirizzo del server Command and Control e dei DNS utilizzati, evitando di conservare questi dati su un file, ma iniettandoli nella memoria del computer per renderne più difficile il rilevamento.

Tutte le comunicazioni in entrata e in uscita sono protette attraverso una chiave crittografica **RC4**, utilizzando una particolare procedura che rende più complicata l'individuazione della trasmissione dati.

Insomma, come sottolinea Proofpoint, con SystemBC ci troviamo di fronte a un'ulteriore evoluzione di quella filosofia di "cyber-crimine collaborativo" che negli ultimi anni sembra vivere una crescita esponenziale.

Condividi l'articolo

Raffica di attacchi ransomware ai NAS

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/08/02/systembc-il-malware-per-nascondere-il-malware/