G Data press release 2014

Malware camuflat: botneti controlati prin webmail

In prealabil, malware-ul necunoscut exploateaza e-mailul Yahoo, cu scopul de a primi comenzi pentru functiile sale

Bucuresti (Romania) 20.08.2014

O noua tulpina de malware greu detectabil este capabila de deturnarea unor portaluri web cunoscute, cum ar fi Yahoo si Gmail, pentru a primi comenzi de control. Ceea ce face troianul IcoScript atat de neobisnuit este faptul ca malware-ul utilizeaza propriul limbaj de programare pentru a se conecta automat la un cont de e-mail. Acel cont a fost creat de catre hackeri pentru a lansa comenzi catre computerele infectate. Accesul la servicii de webmail este rareori blocat in retelele companiilor si, prin urmare, troianul poate primi si executa comenzi fara a fi observat. Expertii in securitate de la G DATA au numit malware-ul Win32.Trojan.IcoScript.A. O analiza detaliata a fost publicata in revista de specialitate Virus Bulletin.

Trojanul infecteaza computerele cu sisteme de operare Windows

Malware-ul inselator, numit Win32.Trojan.IcoScript.A, a cauzat probleme inca din 2012, fara a fi descoperit. Troianul, un sistem modular de administrare de la distanta (RAT), infecteaza computerele cu Windows. Alte programe malware de acest gen se autoinjecteaza, de obicei, in procesele aplicatiilor, iar software-ul antivirus nu are nici o problema in a detecta aceasta metoda. IcoScript, pe de alta parte, abuzeaza de interfata COM (Component Object Model) pentru a debloca accesul la Internet Explorer. Printre altele, interfata COM permite dezvoltatorilor sa scrie plug-in-uri pentru browser. Aceasta functionalitate pune la dispozitia programatorilor de malware un loc ascuns pentru a compromite browser-ul, fara a fi observat de catre utilizator sau de protectia antivirus. Ulterior, datele de pe computer si din retea arata ca niste date complet normale de navigare. Mai mult decat atat, autorii de malware nu trebuie sa-si faca griji cu privire la setarile din retea; ele pot fi acceptate, deoarece au fost configurate in browser. "Acest malware adaptabil si variabil, care incorporeaza activitatile sale in fluxuri de date regulate, creaza dificultati majore departamentelor de securitate si sistemelor de protectie IT," spune Ralf Benzmuller, sef al G DATA SecurityLabs. " Malware-ul demonstreaza inca o data cat de bine studiaza dezvoltatorii de malware mecanismele de aparare."

IcoScript utilizeaza in mod abuziv serviciile de webmail pentru a prelua functiile de comanda

IcoScript functioneaza prin utilizarea Internet Explorer pentru a abuza de servicii de webmail, cum ar fi Yahoo, pentru a prelua functiile sale de comanda si control. In scopul de a accesa e-mail-urile incarcate in casuta postala, IcoScript a fost echipat cu propriul sau limbaj de programare. Acest lucru ii permite sa execute actiuni automate pe paginile portalurilor web. IcoScript.A realizeaza acest lucru prin deschiderea portalului de e-mail Yahoo, conectarea la aces-

ta si preluarea e-mail-ului. Cauta codul de control al e-mail-ului, care este apoi transmis catre programul malware ca o comanda. E-mail-ul poate fi utilizat si pentru a trimite date din retea." Acest proces nu este limitat doar la Yahoo, ci poate functiona la fel de bine pentru numeroase portaluri web, cum ar fi Gmail, Outlook, etc. Chiar LinkedIn, Facebook si alte retele sociale ar putea fi utilizate in mod abuziv in acest scop," explica Benzmuller.

Virus Bulletin, o baza solida în industria de antivirus

Analiza a fost publicata in revista britanica de IT, Virus Bulletin, sub titlul "IcoScript: Utilizarea Webmail-ului pentru a controla malware-ul". " IcoScript este un malware foarte neobisnuit. Suntem incantati ca articolul nostru a fost publicat in aceasta revista de renume si privim acest lucru ca pe o recunoastere a cercetariilor intreprinse de echipa noastra. Virus Bulletin este un element determinant in industria de antivirus in care si-a castigat o reputatie excelenta prin informarea independenta, obiectiva si profesionala despre programele malware de-a lungul anilor," spune Benzmuller.

O versiune HTML a intregului articol este disponibila pe website Virus Bulletin: https://www.virusbtn.com/virusbulletin/archive/2014/08/vb201408-IcoScript sau in format PDF: https://www.virusbtn.com/pdf/magazine/2014/vb201408-IcoScript.pdf

-###-