G Data press release 2014

Uroburos – un program spyware extrem de complex, cu radacini rusesti

G Data a descoperit un program suspectat a proveni de la servicii secrete

Bucuresti (Romania) 04.03.2014

Expertii G Data au descoperit si analizat un program de spionaj extrem de sofisticat si complex. Acesta a fost proiectat pentru sustragerea de date secrete sensibile din retele de calculatoare cu potential, precum institutii nationale, servicii de informatii sau companii mari. Rootkit-ul, numit Uroburos, functioneaza independent si se raspandeste in retelele infectate. Chiar si computerele care nu sunt conectate direct la Internet, sunt atacate de acest malware. G Data considera ca pentru a construi un astfel de program sunt necesare investitii subtantiale in personal si infractructura. Designul si nivelul ridicat de complexitate al malware-ului dau nastere, prin urmare, la ipoteza ca originile se trag de la un serviciu secret. Bazandu-se pe detaliile tehnice, precum nume de fisiere, criptare si comportament, s-a suspectat ca Uroburos ar putea proveni din acceasi sursa care a lansat atacul cibernetic asupra SUA in 2008. Programul utilizat atunci s-a numit "Agent.BTZ". Furnizorul german de securitate IT estimeaza ca acest spyware a ramas nedetectat de mai mult de trei ani. Expertii de la G Data SecurityLabs au publicat detalii tehnice suplimentare si o analiza amanuntita ce poate fi descarcata de pe link-ul:
(https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf).

Ce este Uroburos?

Uroburos este un rootkit care este compus din doua fisiere – un driver si un fisier de sistem virtual criptat. Atacatorii pot folosi acest malware pentru a prelua controlul asupra computerelor infectate, pentru a executa orice cod de program si pentru a-si acoperi actiunile efectuate pe un sistem. Uroburos este totodata capabil sa sustraga datele si sa inregistreze traficul de date din retea. Structura modulara permite atacatorilor sa dezvolte malware-ul prin adaugarea de noi functionalitati.

Datorita acestei flexibilitati si a structurii modulare, G Data il considera a fi deosebit de avansat si de periculos.

Complexitatea tehnologica indica origini ale unor servicii secrete

Complexitatea si designul rootkit-ului Uroburos confirma malware-ul ca fiind foarte sofisticat si costisitor de dezvoltat. G Data crede ca au fost implicati dezvoltatori foarte bine pregatiti. Providerul german deduce ca nu infractorii cibernetici sunt responsabili de dezvoltarea programului si crede ca in spatele Uroburos sta un serviciu secret. Expertii G Data cred, deasemenea, ca programatorii implicati pot fi suspectati de dezvoltatea mai multor programe rootkit avansate care nu au fost inca descoperite.

Uroburos este proiectat sa functioneze in retele mari apartinand companiilor, autoritatilor publice, organizatiilor si institutiilor de cercetare: malware se raspandeste autonom si functioneaza in modul "peer-to-peer", unde computerele infectate dintr-o retea inchisa comunica intre ele. Pentru asta, atacatorii au nevoie de un singur computer cu acces la Internet. Modalitatea de actiune arata ca atacatorii au luat in calcul faptul ca multe retele includ adesea si computere care nu sunt conectate la Internet. Computerele infectate spioneaza documente si alte date si le transfera pe computere cu acces la Internet, de unde sunt transferate de atacatori. Uroburos suporta atat sisteme Microsoft cu 32 bit, cat si cu 64 bit.

Este suspectata o legatura intre atacul rusesc asupra SUA

Bazat pe detaliile tehnice, numele fisierelor, criptare si comportament al malware-ului, expertii G Data au vazut o conexiune intre Uroburos si atacul cibernetic ce a vut loc aspura SUA in 2008 – se presupune ca aceeasi atacatori ar fi in spatele acestor atacuri si a rootkit-ului ce tocmai a fost descoperit. La vremea respectiva, a fost utilizat un program malware numit "Agent.BTZ". Uroburos verifica sistemele infectate pentru a constata daca malware-ul este deja instalat, caz in care rootkit-ul nu devine activ. G Data a gasit, totodata, indicii ca dezvoltatorii ambelor programe sunt vorbitori de limba rusa.

Analiza arata ca atacatorii nu ii vizeaza pe utilizatorii de obisnuiti. Efortul operational este justificat doar pentru tinte care merita, de exemplu, companii foarte mari, institutii guvernamentale, servicii secrete, organizatii si alte obiective similare.

Probabil nedetectat de mai mult de trei ani

Rootkit-ul Uroburos este cea mai avansata piesa a unui program malware pe care expertii in securitate de la G Data au analizat-o vreodata. Cel mai vechi driver analizat a fost creat in 2011. Asta inseamna ca aceasta actiune nu a fost detectata din acea perioada.

Vectorul de infectare ramane un mister

Pana acum, nu a fost posibil sa se determine cum s-a infiltrat initial Uroburos intr-o retea de calibru mare. Atacurile puteau fi executate in mai multe feluri, de exemplu, prin atacuri de phishing, infectii drive-by, stick-uri USB sau inginerii sociale.

Ce reprezenta denumirea malware-ului?

G Data a numit malware-ul "Uroburos" dupa numele corespunzator folosit in codul sursa. Denumirea are la baza un simbol antic grecesc al unui sarpe sau al unui dragon care isi inghite propria coada.