G Data press release 2014

G DATA A PUBLICAT ANALIZA PROGRAMELOR DE CYBER-SPIONAJ

EXPERTII IN SECURITATE AU CERCETAT DEZVOLTAREA MALWARE-ULUI AGENT.BTZ TIMP DE SAPTE ANI.

Bucuresti (Romania) 19.01.2015

Atacuri cibernetice orientate asupra institutiilor guvernamentale, companiilor si organizatiilor internationale au crescut in ultimii ani. Malware-ul este arma aleasa. Timp de sapte ani, G DATA a urmarit activitatea uneia dintre cele mai cunoscute programe malware: Agent.BTZ. In 2008, tulpina malware a fost implicata intr-un atac cibernetic asupra Pentagonului din Statele Unite ale Americii. In 2014, s-a constatat ca programul spyware Uroburos a atacat atat Ministerelor de Externe belgian, cat și pe cel finlandez. In noiembrie 2014, ComRAT (succesorul Agent.BTZ a) a fost descoperit si analizat in detaliu, dezvaluind similitudini tehnice cu rootkit-ul Uroburos. In toate mostrele malware analizate, expertii G DATA au gasit coduri de program similare. Cum procedeaza autorii pentru a atinge conceptul de cyber-spionaj? Pentru a ilustra modul in care este dezvoltat un program spyware extrem de complex, expertii in securitate au investigat indeaproape Agent.BTZ si ComRAT - in total 46 de probe diferite au fost analizate intr-o perioada de sapte ani.

"Ca urmare a analizei, acum avem date privind sapte ani de dezvoltare a malware-ului, care a fost folosit de catre un grup de infractori in atacuri indreptate asupra unor tinte extrem de sensibile, cum ar fi Pentagonul SUA in 2008, Ministerul de Externe Belgian si Ministerul de Externe Finlandez in 2014", explica Ralf Benzmuller, seful G Data SecurityLabs.

Modificari minore ale software-ului

Pana la versiunea 3.00, in 2012, expertii de securitate G Data detecteaza doar modificari minore ale software-ului. S-au făcut modificari pentru versiunile de Windows, au fost eliminate erori de programare si s-au adaugat metode camuflate de atac. Cea mai mare actualizare a avut loc in versiunea 3.00 a malware-ului ComRAT. Cu toate acestea, metodele atacatorilor nu sunt foarte clare. Expertii de securitate banuiesc ca in spatele malware-ului sunt hackeri bine pregatiti, care stiu cum sa-si acopere urmele.

Analistii G Data sunt siguri ca grupul din spatele Uroburos, Agent.BTZ si ComRAT continua sa fie activ in atacuri malware si in zona APT (Advanced Persistent Threat). Cele mai recente dezvaluiri si anumite legaturi duc la speculatii ca mai multe atacuri pot fi de asteptate in viitor.

Analiza detaliata a programului complex spyware este descrisa pe:
https://blog.gdatasoftware.com/blog/article/evolution-of-sophisticated-spyware-from-agentbtz-to-comrat.html

Expertii G Data au analizat succesorul lui Agent.BTZ, ComRAT: https://blog.gdatasoftware.com/blog/article/the-uroburos-case-new-sophisticated-rat-identified.html

Deturnarea de obiecte COM este cercetata in detaliu pe G DATA SecurityBlog: https://blog.gdatasoftware.com/blog/article/com-object-hijacking-the-discreet-way-of-persistence.html

Analiza Uroburos poate fi gasita pe G DATA SecurityBlog (https://blog.gdatasoftware.com/blog/article/uroburos-highly-complex-espionage-software-with-russian-roots.html), impreuna cu o analiza tehnica detaliata a functionalitatilor malware-ului (https://blog.gdatasoftware.com/blog/article/uroburos-deeper-travel-into-kernel-protection-mitigation.html).

-###-