TRUST IN GERMAN SICHERHEIT

G Data press release 2015

Programul spyware Babar inregistreaza toate datele

Din revelatiile lui Snowden - expertii G DATA analizeaza un program malware documentat de catre serviciul de informatii canadian.

Bucuresti (Romania) 26.02.2015

G DATA SecurityLabs a investigat o mostra spyware care inregistreaza si transfera intrari de pe tastatura, date clipboard, date de monitorizare si conversatii audio, confirmand astfel dezvaluirile lui Snowden referitoare la o tulpina spyware de provenienta franceza, informatii documentate de catre serviciul de informatii canadian CSEC (Communication Security Establishment Canada). Ziarul francez Le Monde a fost primul care a semnalat existenta acestor documente cu aproape un an in urma. Expertii G Data au publicat detaliile tehnice pentru prima data, in urma analizei malware-ului Babar, care a fost realizata in tandem cu alte agentii de cercetare de securitate internationale. Analistii nu au putut stabili daca aceste servere de control malware au fost in mod deliberat puse in functiune sau au fost compromise. In opinia expertilor, dezvoltarea unui astfel de program necesita investitii substantiale de personal si infrastructura. Nivelul de complexitate al malware-ului sugereaza ca ar proveni de la un serviciu secret. Serviciul de informatii canadian considera ca responsabile de malware-ul Babal sunt serviciile secrete franceze. Solutiile de securitate G Data detecteaza si blocheaza malware-ul.

"Babar este un program spyware foarte sofisticat care putea fi produs doar de programatori foarte bine pregatiti", explica Eddy Willems, Security Evangelist G DATA Software AG. " Babar este proiectat aă functioneze in mod special in retelele companiilor, autoritatilor, organizatiilor si institutelor de cercetare, de unde sustrage date sensibile. Ca rezultat, conversatii audio, cum ar fi cele de pe Skype, de exemplu, pot fi inregistrate. Chiar si un atac directionat asupra utilizatorilor individuali pare posibil. O distributie in masa a unui astfel de malware este, totusi, foarte putin probabil", spune Willems.

Istoricul documentelor CSEC

In martie 2014, cotidianul francez Le Monde primeste un raport referitor la documentele serviciului de informatii canadian CSEC (Communication Security Establishment Canada), datat din 2011, care a iesit la lumina in timpul dezvaluirilor lui Edward Snowden. Revista germana de stiri, Der Spiegel, a preluat subiectul in ianuarie 2015 si a publicat un continut suplimentar al acestor documente - Operatiunea Snowglobe.

Ce este Babar?

Babar este un instrument de administrare la distanta (RAT), a carui functie principala este de a spiona date. Potrivit serviciului de informatii canadian, in urma analizei malware-ului EvilBunny din decembrie 2014, Babar a fost si numele de cod al unei operatiuni a unui serviciu secret national numit Snowglobe. Acest lucru arata ca Babar ar putea fi a doua tulpina malware identificata a fi fost conectata la campania spyware Snowglobe. Numele de "Babar" vine de la o serie de carti frantuzesti pentru copii, al carei erou este un elefant.

TRUST IN GERMAN SICHERHEIT

Din cauza similitudinilor dintre ele, expertii in securitate de la G Data sunt convinsi ca cele doua tulpini provin de la aceeasi dezvoltatorii.
Informatii tehnice detaliate pot fi gasite pe blogul G Data:
https://blog.gdatasoftware.com/blog/article/babar-espionage-software-finally-found-and-put-under-the-microscope.html

-###-