**Twórcy ransomware SamSam na celowniku FBI**

**34-letni Faramarz Shahi Savandi i 27-letni Mohammad Mehdi Shah Mansouri, to dwóch Irańczyków wobec których FBI wystosowało akt oskarżenia o odpowiedzialność za stworzenie ransomware SamSam i spowodowanie im szkód na ponad 30 milionów dolarów (z czego sami uzyskali 6 milionów). Wirus SamSam jest aktywny od 2015 roku i jego celem mogło paść nawet 200 dużych sieci.**

**Twórcy ransomware SamSam na celowniku FBI**

34-letni Faramarz Shahi Savandi i 27-letni Mohammad Mehdi Shah Mansouri, to dwóch Irańczyków wobec których [FBI wystosowało akt oskarżenia](https://darkwebnews.com/law-enforcement/fbi-indics-samsam-ransomware-suspects/) o odpowiedzialność za stworzenie ransomware SamSam i spowodowanie im szkód na ponad 30 milionów dolarów (z czego sami uzyskali 6 milionów). Wirus SamSam jest aktywny od 2015 roku i jego celem mogło paść nawet 200 dużych sieci, głównie szpitali, uniwersytetów (jak np. Uniwersytet w Calgary), czy instytucji rządowych. Był wykorzystywany do klasycznego szantażu okupem, jednak twórcy zadbali m. in. za dobieranie pór ataków (głównie poza godzinami pracy), dobrze dobierali szyfrowane zasoby i dążyli do szyfrowania backupu. W ich wiadomości o okupie byli bardzo uprzejmi i w ramach „uczciwości” dawali klucz odszyfrowujący jeden plik za darmo, jako „dowód zaufania”. Sami korzystali aktywnie z sieci Tor by ukrywać swoją tożsamość.

Specjaliści firmy [pancernik.it](http://pancernik.it/) uważają iż [w 2018 roku SamSam pomimo iż jest dość znanym zagrożeniem](https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/), nadal pozostaje groźny i wciąż ewoluuje. Obecnie można spotkać go w wersjach wykorzystujących m. in. podatności: w protokołach RDP, w web-serwerach opartych na języku Java, czy w serwerach FTP, a także przy standardowych włamaniach typu „[brute force](https://pl.wikipedia.org/wiki/Atak_brute_force)” próbujących w ten sposób łamać łatwe hasła.

(zdjęcie: pcrisk.com)

Pomimo aktu oskarżenia, nie należy cieszyć się przedwcześnie. Obaj Irańczycy bowiem nadal pozostają w Iranie, który z powodu konfliktu z USA [(o której nieco pisaliśmy w poprzedniej notce](http://blog.pancernik.it/ostatnie-ataki-hakerskie-pokazuja-jak-wazne-jest-cyber-bezpieczenstwo/)) raczej nie pali się do ekstradycji swoich obywateli. Jedyna szansa to gdy któryś z nich opuści kraj i przekroczy granicę kraju sojuszniczego dla USA.

Autor: Karol Mondry

Źródła:

darkwebnews.com

pcrisk.com

wikipedia.irg

blog.pancernik.it

blog.malwarebytes.com