Nelle ultime ore c'è una sorta di fermento, pare che un gruppo di Hackers che si fanno chiamare "The shadow Brokers" siano riusciti a penetrare NSA, nella fattispecie il gruppo di punta di hacking - ovvero Equation Group, e a trafugare tutti i tool del gruppo.

Parliamo di tool avanzati e che quindi possiamo tranquillamente comparare ad armi.

Hanno pubblicato un estratto free, apparso su Github e prontamente reso inaccessibile dal team del famoso repository libero. I file più interessanti, fra i quali il tanto famoso stuxnet
a quanto pare, sono messi all'asta per 1 milione di Bitcoin (circa 568 milioni di dollari al prezzo attuale).

Alcuni nomi dei tools annessi all'estratto free, coincidono con i leak di Snowden, come "bananaglee", quindi sembra confermato. Attendiamo sviluppi ulteriori su questa pericolosa situazione.

Avere in giro persone poco affidabili con delle armi (si sono armi) cosi sofisticate è molto pericoloso.

UPDATE 16/08/2016

Da analisi approfondite, risulta che sia probabilmente una operazione *false flag*. Gli account di questi presunti hackers sono stati creati a partire dal 1 Agosto (twitter, github, etc).

Piccola analisi fatta dagli esperti

- **EGBL**: **EGREGIOUSBLUNDER** versione 3.0.0.1 - Una web-based exploit che prende di mira i firewall FortiGate (varie build del firmware FGT_60-V300) compresi i modelli 60, 60M, 80C, 200A, 300A, 400A, 500A, 620B, 800, 5000, 1000A, 3600 e 3600A. un ricercatore nota che Avast chiama CVE-2006-6493 , che è una vulnerabilità in OpenLDAP.

- **ELBA**: **ELIGIBLEBACHELOR** - Un exploit contro un fornitore non specificato, che colpisce le versioni 3.2.100.010, 3.3.001.050, 3.3.002.021 e 3.3.002.030. Questo exploit utilizza la libreria di terze parti da Keld Simonsen chiamato ISO / IEC 14652 i18n FDCC-set.

- **ELBO**: **ELIGIBLEBOMBSHELL** versione 1.2.0.1 - basata su web Un exploit segnalato per essere contro i firewall cinesi TOPSEC e colpisce le versioni 3.3.005.057.1 a 3.3.010.024.1. Alcuni e' come se fossero stati aggiunti nel 2009 e hanno le loro designazioni nome in codice, tra cui WOBBLYLLAMA, FLOCKFORWARD, HIDDENTE MPLE, CONTAINMENTGRID, e GOTHAMKNIGHT.

- **ELCA**: **ELIGIBLECANDIDATE** versione 1.1.0.1 - Una linea nell'exploit si definisce Questa web-based exploit obiettivi lo script /cgi/maincgi.cgi di firewall cinesi TOPSEC versione 3.3, 005.057.1 a 3.3.010.024.1.
- **ELCO**: **ELIGIBLECONTESTANT** versione 1.1.0.1 - Una linea nell'exploit si descrive come "Un pacchetto cade in un router. Qualcuno lo sente? "Questo web-based exploit ha tra gli obiettivi lo script /cgi/maincgi.cgi di firewall TOPSEC prima della versione 3.3.

- **EPBA**: **EPICBANANA** versione 2.1.0.1 - Questo exploit obiettivi diversi modelli di Cisco PIX Firewall e Cisco Adaptive Security Appliance dispositivi (ASA). Utilizza il in Python scritto da Noah Spurrier e comprende una lunga lista di crediti per aiutare lo sviluppo del modulo. Le immagini dei dispositivi ASA colpite includono 711, 712, 721, 722, 723, 724, 80432, 804, 805, 822, 823, 824, 825, 831, e 832. Il PIX interessata immagini dei dispositivi includono 711, 712, 721, 722 , 723, 724, e 804.
- **ESPL**: **ESCALATEPLOWMAN** versione 1.1.0.1 - Un exploit contro un fornitore sconosciuto.
- **EXBA**: **EXTRABACON** versione 1.1.0.1 - Un exploit contro il servizio SNMP di dispositivi Cisco Adaptive Security Appliance (ASA) che colpisce la versione 8.0 (2) a 8,4 (4).
Ha altri strumenti e script, con nomi in codice meravigliosi come BANANAGLEE (impatta dispositivi Juniper), BARGLEE, BLATSTING, BUZZDIRECTION, SCREAMPLOW, e BANANADAIQUIRI.

fonte

fonte update