Uuring heidab valgust, kas tuntud häkkerirühmitused võisid tegutseda juba 90ndatel

9 aastat tagasi - 10.04.2017 Autor: AM

90ndate esimesel poolel, kui Arvutimaailm alustas, ilmusid ka lood esimestest häkkeritest, nende häkkerirühmitused oskasid modemite kaudu arvutisse sisse imbuda ja tegid telefonijaamade lollitamist, et neid modemeid telefonivõrgust üles leida. Kaspersky Lab'i eksperdid ja King's College London ülikooli uurijad alustasid 90ndatel toimunud USA valitsusressursside küberrünnakute sarja ja kaasaegsete küberspionaaži võimalike seoste uurimist ning jõudsid järeldusele, et seos võib olemas olla - meil võib eksisteerida häkkerirühmituste dünastia.

Uurides Moonlight Maze´i rünnakute, millest said kannatada Pentagon, NASA ja USA Energeetikaministeerium üksikasju, leidsid analüütikud rea kahjutoova tarkvara näidiseid ja muid lausa 20 aasta vanuseid artefakte. Edasine analüüs näitas, et tagaukseprogramm, mida selles operatsioonis kasutati, omab palju ühist selle *backdoor*'iga, mida kasutati Turla kahjutoovas kampaanias aastal 2011 ning avastati korduvalt märtsis 2017.

Kui õnnestub tõestada seos gruppide Moonlight Maze ja Turla vahel, siis tuleb välja, et viimane on peaaegu sama pikaealine, nagu ka kuulsaks saanud grupp Equation, mille aktiivsust õnnestus jälgida aastani 1996.

Aastal 1998 alustasid FBI ja USA Kaitseministeerium riigi valitsus- ja sõjaorganisatsioonide ning samuti mõnede ülikoolide ja uurimisinstituutide võrkude lahtimurdmise juhtumite uurimist. Avalikkus sai teada Moonlight Maze´i rünnakutest alles aasta pärast – 1999. aastal, uuringu üksikasjad jäid tol ajal siiski saladuseks. Aastate möödudes tegid kolmest erinevast riigist uurijad üksteisest sõltumata järelduse, et grupeering Moonlight Maze transformeerus Turlasse, mille taga on eeldatavasti venekeelsed ründekorraldajad ja häkkerirühmitused. Veel hiljuti arvati, et Turla (tuntud ka kui Snake, Uroburos, Venomous Bear ja Krypton) alustas oma tegevust aastal 2007.

Töötades oma raamatu „Rise of the Machines" kallal, võttis Thomas Rid King's College Londoni ülikoolist aastal 2016 ühendust kunagise süsteemiadministraatoriga, kes töötas samas organisatsioonis, mille serverid

häkiti ja muudeti Moonlight Maze´i proxy-serveriks. Pensionile läinud IT-spetsialist säilitas serveri enda ja kõigi 1998. aasta rünnakutega seotud artefaktide koopiad. Kõik materjalid edastas ta King’s College Londoni uurijatele ja Kaspersky Lab’i ekspertidele. Analüütikud suutsid üheksa kuuga rekonstrueerida Moonlight Maze´i operatsioonid, nende vahendid ja tehnikad ning püüdsid leida kinnitust selle grupeeringu seosele Turlaga.

Oma rünnakutes Solarise operatsioonisüsteemiga võrkudesse ja arvutitesse kasutas Moonlight Maze vahendeid, mis on üles ehitatud avatud lähtekoodiga UNIX-i platvormil. Ohvrite süsteemidesse tungimiseks kasutasid ründajad backdoor’i LOKI2, mis on programm, mis lasti väljajuba aastal 1996 ja mis oli mõeldud andmete väljaõngitsemiseks varjatud kanalite kaudu. See leid sundis analüütikuid korduvalt käsitlema kahjutoova tarkvara Turla (loodud Linuxi jaoks) harvu näidiseid, mis avastati aastal 2014. Selgus, et kahjutoojad kirjutati valmis samuti LOKI2 baasil. Peale selle kasutati nendes koodi, mis kirjutati aastatel 1998 kuni 2004.

Märkimisväärne on see, et vana koodi taaskasutatakse siiamaani rünnakutes, mis omistati kunagi Turlale. Aastal 2011 märgati seda koodi kahjutoovas operatsioonis, mis oli sihitud Šveitsi militaarhankija Ruag’i vastu. Märtsis 2017 võeti välja seda koodi sisaldava *backdoor*’i näidis Saksamaa ettevõtte võrgust. Võimalik, et grupeering Turla kasutab vana koodi rünnakuteks Linuxiks eriti tähtsatele ja hästikaitstud sihtmärkidele, sest sel viisil on neil kergem võrku tungida, võrreldes Windowsi standardvahendite kasutamisega.

„90ndate lõpus ei mõistnud veel keegi, kuivõrd pikaajalised ja mastaapsed saavad olla küberspionaaži koordineeritud kampaaniad. Moonlight Maze´i kahjutoova tarkvara ja koodi analüüs ei ole lihtsalt põnev reis minevikku, vaid järjekordne meeldetuletus sellest, et hästi ettevalmistatud häkkerirühmitused ei kao kuhugi ning ei lõpeta ma tegevust niisama. Meie ühine ülesanne on mõista, miks ründajad kasutavad siiani edukalt vana koodi ning korrigeerida kaitset sedasi, et see arvestaks rünnakute kõikvõimalike vektoritega,“ räägib Juan Andres Guerrero-Saade, Kaspersky Lab’i juhtiv ekspert viirusetõrje alal.

Moonlight Maze´i operatsioonide uurimisest ja nende võimalikust seosest Turlaga saab lugeda Kaspersky Lab’i aruandest.

- Uudised
- Tarkvara

- Turvalisus

Pilt

