Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef departament: dr. conf.univ. Fiodorov I.

_____

„__”_____ 2022

Analiza amenințării persistente avansate APT29 - șablon comportamental, metode de identificare și prevenție

Teza de master

Student:	**Malai Ion, gr. SI-201M**
Coordonator:	**Antohi Ionel, lect. univ.**

Chișinău 2022

Adnotare

Grupurile de atacatori APT reprezintă un mare pericol pentru lumea cibernetică și documente confidențiale. Din acest motiv am ales studiul despre APT29, deoarece ei activează în așa țări ca Regatul Unit, SUA și CSI, și Scopul am pus de aflat ce instrumente și tehnici ei utilizează, cum alte țări sau companii le-au depistat, cum de prevenit următoarele atacuri și care a fost impactul atacurilor pe Republica Moldova. Teza conține patru capitole unde în primul capitol se descrie cum ei colaborează cu alte grupuri sau ce instrumente folosesc, care au fost modificațiile lor. Al doilea capitol descrie tacticile, tehnicile și procedurile care au fost depistate după ingineria inversă a codurilor și aplicațiilor malițioase și cum analiticii înțeleg ce grup de atacatori a efectuat acest atac. Ce reprezintă șablonul de comportament și analiza funcțională, care scopuri ei au și ce informații ei caută. Țintele și obiectivele lor, și care e cea mai utilizată metodă prin care ei primesc ce doresc sunt descrise în capitolul al treilea. O analiză atacului în 2017, cronologia și instrumentele, cum a fost utilizat infrastructura altui grup de hackeri. În ultimul capitol sunt descrise atacurile care au fost depistate în ultimii ani în țările mari și în regiunea noastră, care a fost impactul și scopul lor. Ca concluzii am descris importanța ca lucrătorii să aibă cunoștințe minime de securitate cibernetică, ca să evităm și să ne învățăm pe greșelile precedente.

Annotation

APT attack groups pose a great danger to the cyber world and confidential documents. That is why I chose the APT29 study because they work in countries like the UK, the USA, and the CIS, and I set out to find out what tools and techniques they use, how other countries or companies have found them, how to prevent the following attacks and the impact of the attacks on the Republic of Moldova. The thesis contains four chapters where the first chapter describes how they collaborate with other groups or what tools they use, what were their modifications. The second chapter describes the tactics, techniques and procedures that were detected after the reverse engineering of malicious codes and applications and how analysts understand which group of attackers carried out this attack. What is the pattern of behavior and functional analysis, what are its purposes and what information is it looking for. Their goals and objectives, and what is the most used method by which they receive what they want, described in the third chapter. An analysis of the attack in 2017, the chronology and tools, how the infrastructure of another group of hackers was used. The last chapter describes the attacks that have been detected in recent years in the big countries and in our region, what was their impact and purpose. In conclusion, I described the importance of workers having a minimum knowledge of cybersecurity, in order to avoid and learn from previous mistakes.

Cuprins

Introducere

The Dukes sunt un grup de spionaj cibernetic bine resursat, foarte dedicat și organizat, care posibil că lucrează pentru Federația Rusă din cel puțin 2008 pentru a colecta informații sau să ia decizii în sprijinul politicii externe și de securitate. CozyBear arată o încredere neobișnuită în capacitatea lor de a-și continua compromiterea cu succes a țintelor, precum și în capacitatea lor de a opera impun. CozyDuke vizează în primul rând guvernele occidentale și organizațiile conexe, cum ar fi ministerele și agențiile guvernamentale, grupurile de reflecție politice și subcontractorii guvernamentali. Obiectivele lor au inclus, de asemenea, guvernele membrilor Comunității Statelor Independente; guvernele din Asia, Africa și Orientul Mijlociu; organizațiile asociate cu extremismul cecen și vorbitorii de limbă rusă care se ocupă cu comerțul ilicit de substanțe și droguri controlate. Se știe că Dukes folosește un set vast de instrumente malware, pe care le identificăm după așa denumiri, ca: MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke și GeminiDuke. În ultimii ani, APT29 s-au angajat în campanii aparent bianuale la scară largă de phishing împotriva sutelor sau chiar a mii de destinatari asociați cu instituțiile guvernamentale și organizațiile afiliate. Aceste campanii utilizează o abordare „smash-and-grab" care implică exfiltrarea a cât mai multor date posibile. Ei utilizează unele tactici mai mult axate pe compromisul persistent și colectarea informațiilor pe termen lung. Amenințările

APT29 este un grup de amenințări adaptativ și disciplinat care își ascunde activitatea în rețeaua unei victime, comunicând rar și într-un mod care seamănă foarte mult cu traficul legitim. Prin utilizarea serviciilor web populare legitime, grupul poate profita și de conexiunile SSL criptate, făcând detectarea și mai dificilă. APT29 este unul dintre cele mai evoluate și mai capabile grupuri de amenințări. Implementează noi backdoor-uri pentru a-și rezolva propriile bug-uri și pentru a adăuga caracteristici. Monitorizează activitatea apărătorilor de rețea pentru a menține controlul asupra sistemelor. APT29 utilizează numai servere compromise pentru comunicarea CNC. Acesta combate încercările de remediere a atacurilor. De asemenea, menține un ciclu de dezvoltare rapid pentru malware-ul său, modificând rapid instrumentele pentru a împiedica detectarea.

APT29 a folosit site-uri de socializare precum Twitter sau GitHub, precum și servicii de stocare în cloud, pentru a retransmite comenzi și extrage date din rețele compromise. Grupul transmite comenzi prin intermediul imaginilor care conțin date ascunse și criptate. Informațiile sunt extrase dintr-o rețea compromisă și fișierele sunt încărcate în serviciile de stocare în cloud.

Pe lângă aceste campanii la scară largă, Dukes se angajează în mod continuu și concomitent în campanii mai mici, mult mai direcționate, utilizând seturi diferite de instrumente. Aceste campanii direcționate au loc de cel puțin 13 ani. Țintele și momentul acestor campanii par să se alinieze cu interesele cunoscute de politică externă și de securitate ale Federației Ruse în acele momente.

Bibliografie

1. Analysis of WellMail malware's Command and Control (C2) server [citat 17.09.2020]. Disponibil: https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html
2. How WellMess malware has been used to target COVID-19 vaccines [citat 16.07.2020]. Disponibil: https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/
3. HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Disponibil: https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
4. Who is behind APT29? What we know about this nation-state cybercrime group [citat 23.09.2021]. Disponibil: https://portswigger.net/daily-swig/who-is-behind-apt29-what-we-know-about-this-nation-state-cybercrime-group
5. ESET Research, "En Route with Sednit," 10 2016. Disponibil: https://www welivesecurity com/wp-content/uploads/2016/10/eset-sednit-full.pdf
6. How Russian Hackers Spiked the Currency Exchange Rate. [citat 08.02.2016]. Disponibil: https://fortune.com/2016/02/08/russian-hackers-currency-rate/
7. Leviathan: Espionage actor spearphishes maritime and defense targets [citat 16.10.2017]. Disponibil:https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
8. Spear Phishing Fileless Attack with CVE-2017-0199 [citat 30.05.2017]. Disponibil: https://blog.fortinet.com/2017/05/30/spear-phishing-fileless-attack-with-cve-2017-0199
9. Disponibil: https://github.com/AlexusBlack
10. Atacuri asupra jurnaliștilor și angajaților din mass-media în moldova în anul 2020. Disponibil: http://api.md/upload/files/API-Moldova_Report_2020_ROM_final.pdf
11. Cine este „Fancy Bear", gruparea suspectată de implicare în atacul cibernetic asupra MAE [citat 12.05.2017]. Disponibil: https://www.digi24.ro/stiri/actualitate/evenimente/cine-este-fancy-bear-gruparea-suspectata-ca-a-atacat-cibernetic-mae-723191
12. Marea Britanie: Un grup de hackeri ruşi încearcă să fure cercetări despre un vaccin împotriva COVID-19 [citat 16.07.2020]. Disponibil: https://www.defenseromania.ro/marea-britanie-un-grup-de-hackeri-rusi-incearca-sa-fure-cercetari-despre-un-vaccin-impotriva-covid-19_604314.html
13. NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks [citat 01.06.2021]. Disponibil: https://www.sentinelone.com/labs/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/
14. NATO a lansat în Republica Moldova un mecanism de reacție la atacurile cibernetice [citat 22.01.2021]. Disponibil: https://zonadesecuritate.md/nato-a-lansat-in-republica-moldova-un-mecanism-de-reactie-la-atacurile-cibernetice/