Universitatea Tehnică a Moldovei

ANALIZA ȘI INVESTIGAREA PROGRAMELOR MALIȚIOASE FĂRĂ FIȘIERE

ANALYSIS AND INVESTIGATION OF FILELESS MALWARE

Masterand:

Nemerenco Ecaterina

Conducător:

conf. univ., dr Beșliu Victor

Chişinău - 2020

MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Şef departament:
Ion Fiodorov, conf. univ., dr
„20" decembrie 2019

ANALIZA ȘI INVESTIGAREA PROGRAMELOR MALIȚIOASE FĂRĂ FIȘIERE

Teză de master în Securitate Informațională

Masterand: (E.Nemerenco)
Conducător: (V.Beşliu)

Chişinău - 2020

ABSTRACT

Hunting for a fileless threat can be a tedious and labor-intensive task for any analyst. It is, most often than not, extremely time-consuming and requires a significant amount of data gathering. On top of that, the traditional tools, methods, and defenses seem to be less effective when dealing with these almost invisible threats. Threat actors are frequently using attack techniques that work directly from the memory or using legitimate tools or services pre-installed in the system to achieve their goals.

It is a popular technique among targeted attacks and advanced persistent threats (APT), and now it has been adopted by conventional malware such as trojans, ransomwares, and even the most recent emerging threat – cryptocurrency miners. In some incidents, searching for a malicious file that resides in the hard drive seems to be insufficient. This study explores the different variations of fileless attacks that targeted the Windows operating system and what kind of artifacts or tools can provide clues for forensic investigation.

In this paper, we took a deep dive into the Sodinokibi ransomware infection process, and showed that even though the obfuscation techniques used by the ransomware authors are quite simple, they are still proving to be very effective in bypassing most antivirus vendors.

This analysis further supports the suspicion that the threat actors behind the Sodinokibi ransomware are the same allegedly retired authors who created the GandCrab ransomware, based on findings detailed in this report, such as: similarities in the language and countries whitelist (Russian-speaking countries and even Syrian Arabic), the “revengeful” targeting of an Ahnlab product for process injection, and the similarities in the URL-generation routine.

Since April 2019, the Sodinokibi ransomware has become very prolific and has become the 4th most common ransomware within less than 4 months after its first appearance. It has since gone through several minor updates, and it is our assessment that its industrious authors will continue to develop the ransomware, adding more features and improving its evasive capabilities.

ABSTRACT

Analiza și investigarea programelor fără fișiere este o sarcină obositoare și care necesită o muncă intensă pentru orice analist. Este, cel mai adesea, extrem de consumator de timp și necesită o cantitate semnificativă de culegere de date. În plus, instrumentele, metodele și apărările tradiționale par a fi mai puțin eficiente atunci când se confruntă cu aceste amenințări aproape invizibile. Actorii amenințători folosesc frecvent tehnici de atac care funcționează direct din memorie sau folosesc instrumente sau servicii legitime preinstalate în sistem pentru a-și atinge obiectivele.

Este o tehnică populară printre atacurile țintite și amenințările persistente avansate (APT), iar acum a fost adoptată de malware convenționale, cum ar fi troieni, răscumpărare și chiar cea mai recentă amenințare emergentă - minerii de criptocurrency. În unele incidente, căutarea unui fișier rău intenționat care se află pe hard disk pare a fi insuficientă. Acest studiu explorează diferitele variații ale atacurilor fără filă care au vizat sistemul de operare Windows și ce fel de artefacte sau instrumente pot oferi indicii pentru investigarea criminalistică.

În această lucrare, am făcut o scufundare profundă în procesul de infecție cu ransomware-ul Sodinokibi și am arătat că, deși tehnicile de ofusculare folosite de autorii ransomware-ului sunt destul de simple, acestea se dovedesc încă foarte eficiente în ocolirea celor mai mulți furnizori de antivirus.

Această analiză susține în continuare suspiciunea că actorii amenințători din spatele ransomware-ului Sodinokibi sunt aceiași autori care se presupune pensionari, care au creat ransomware-ul GandCrab, pe baza descoperirilor detaliate în acest raport, precum: asemănări în limba și țările din lista albă (țări de limbă rusă și chiar sirian arab), vizionarea „răzbunătoare” a unui produs Ahnlab pentru injecția proceselor și asemănările din rutina de generare a adreselor URL.

Din aprilie 2019, ransomware-ul Sodinokibi a devenit foarte prolific și a devenit al patrulea ransomware cel mai frecvent în mai puțin de 4 luni de la prima apariție. De atunci a trecut prin mai multe actualizări minore, iar evaluarea noastră este că autorii săi speciali vor continua să dezvolte ransomware-ul, adăugând mai multe caracteristici și îmbunătățind capacitățile sale evazive.

CUPRINS

INTRODUCERE

Tehnologia deschide un întreg univers de noi oportunități, cu noi produse și servicii care devin parte integrantă a vieții noastre de zi cu zi. În același timp, riscul de a fi victima unei forme de criminalitate informatică sau a unui atac cibernetic este în creștere, iar impactul social și economic al acestor fenomene devine tot mai important.

În zilele noastre, programele malițioase modern fără fișiere utilizează un amestec de tehnici pentru a evita detectarea și să rămână în afara radarului. Actorii amenințători(din engleză Threat Actors) apelează mai des la această tehnică atunci când își desfășoară și inițiază atacurile cibernetice. Atacatorii țintesc întotdeauna spre furt și o caracteristica a programele malițioase fără fișiere, este ingredientul perfect pentru a se amesteca în operațiunile normale de zi cu zi ale unei organizații și poate rămâne nedetectat.

Programele malițioase fără fișiere au fost descrise de majoritatea oamenilor drept atacuri care nu implică scrierea fișierelor pe disc, acest lucru este însă parțial adevărat. Aceste tipuri de atacuri pot fi implementate într-o varietate de metode și nu este întotdeauna exclusive fără fisier în fiecare etapă. Vectorul său de sosire începe la fel ca majoritatea celorlalte atacuri cibernetice. Poate să fie printr-o exploatare a unei vulnerabilități de securitate, drive-by-download, atac brute-force, dispozitive de stocare USB sau un e-mail tip phishing.

Atacurile fără filă abuzează de instrumentele care sunt încorporate în sistemul de operare pentru a efectua și iniția atacuri. În esență, acestea sunt întoarse împotriva sa. Fără un executabil, nu există nicio semnătură pentru detectare de catre software-ul antivirus. Aceasta face parte din ceea ce face atacurile fără filă atât de periculoase - sunt capabile să se sustragă și să se ascundă cu ușurință de produselor antivirus.

Atacurile fără filă au descris inițial amenințările existente și care funcționează exclusiv în memorie volatila. Această tactică evită declanșarea scanării tradiționale a fișierelor antivirus, nu lasă nicio dovadă criminalistică pe disc și necesită experți să captureze sistemul memorie pentru a analiza atacul. Amenințările fără filă se injectează în mod obișnuit procesele legitime ale sistemului, eforturile frustrante suplimentare de detectare. Termenul fără filă a evoluat pentru a include amenințările care folosesc în mod rău un sistem legitim resurse fără a scrie fișiere noi pe disc. Amenințări fără filă care afectează alte persoane resursele de sistem sunt adesea numite atacuri de tip live-off-the-land (LOL). Aceste amenințări poate ridica privilegiile, obține persistență și se poate răspândi prin rețea folosind instrumente precum PowerShell și WMI. Ei își execută sarcinile utile prin rulare scripturi rău intenționate, executarea de DLL-uri sau rularea codului stocat la locații îndepărtate.

Sistemele digitale au devenit atât de complexe încât este imposibil să fie împiedicat fiecare atac. Răspunsul la această provocare constă în detectarea și răspunsul rapid. În timp ce impactul financiar al

atacurilor cibernetice continuă să crească, există o discrepanță alarmantă între costurile de lansare a unui atac și costurile de prevenire, investigare și reparare.

Programele malițioase fără filă reprezintă o amenințare serioasă pentru soluțiile antivirus tradiționale prin utilizarea metode discrete adesea invizibile pentru detectarea standard a amenințărilor. Prin deturnarea legitimă resurse pentru a ataca un sistem gazdă, programele malițioase fără filă poate camufla prezența sa și funcționează neobservat.

CONCLUZII

Programele fără fișiere reprezintă amenințări curente în spațiul cybernetic de astăzi. În prezent, este o tehnică care a fost adoptată în multe infracțiuni informatice. Atacatorii folosesc instrumente legitime și aplicații cu listă alba efectuează atacul lor. Lipsa artefactelor face, de asemenea, depistarea și criminalistica investigație extrem de dificilă. Vestea bună este, cu experiență relevantă, fără filă amenințările sunt încă detectabile prin analize medico-legale. Dezavantajul este însă că analiza medico-legală este o sarcină destul de intensivă. Este nevoie de mult timp, efort și resurse în achiziționarea și analiza imaginii de disc și memorie.

Mașinile compromise sunt gestionabile la număr. Cu toate acestea, efectuarea criminalistică analiza la scară largă pentru a detecta compromisuri pe o rețea de întreprinderi poate fi foarte mare solicitant. În relația cu întreprinderi la scară largă, utilizarea de senzori în mediu este mai bună soluție. Sistemele de apărare împotriva intruziunilor (IDS) vor oferi vizibilitate pe mașini activitate în rețea și poate declanșa rapid o alertă pentru orice potențial compromis al sistemului.

Soluția de detecție și răspuns (EndR) poate furniza lanțul de evenimente cu privire la modul în care amenințarea fără filă a fost dislocată atât la nivelul final, cât și la comportamentul acesteia. Mai departe pentru aceasta, Monitorizarea comportamentului poate pune la dispoziție protecție suplimentară împotriva amenințărilor programe care prezintă un comportament rău intenționat, precum și orice posibil abuz de utilizare legitimă sau instrumente de administrare.

BIBLIOGRAFIE

1 The History of Fileless Malware – Looking Beyond the Buzzword accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://zeltser.com/fileless-malware-beyond-buzzword/

2 Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/

3 Detecting fileless attacks with Azure Security Center accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://azure.microsoft.com/en-us/blog/detecting-fileless-attacks-with-azure-security-center/

4 What is fileless malware and how do you protect against it? accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://www.techrepublic.com/article/what-is-fileless-malware-and-how-do-you-protect-against-it/

5 What is Scareware? Scareware Defined, Explained, and Explored accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://www.forcepoint.com/cyber-edu/scareware

6 Borges, A. (2018). A Brief Analysis of a Banking Trojan. accesat 12.09.2019 [Resursă electronică]. – Regim de acces: http://www.blackstormsecurity.com/docs/Congresso_TI_2018.pdf

7 Fewer, S. (2013, September 5). stephenfewer/ReflectiveDLLInjection. accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://github.com/stephenfewer/ReflectiveDLLInjection

8 Gorelik, M., & Moshailov, R. (2017). Fileless Malware: Attack Trend Exposed accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://www.morphisec.com/hubfs/wpcontent/uploads/2017/11/Fileless-Malware_Attack-Trend-Exposed.pdf

9 Hunting for Ghosts in Fileless Attacks accesat 12.09.2019 [Resursă electronică]. – Regim de acces: file:///C:/Users/Ecaterina.Nemerenco/Desktop/teza%20de%20master/hunting-ghosts-fileless-attacks-38960.pdf

10 Trend Micro. Fileless Malware: A Hidden Threat. Accesat 12.09.2019 [Resursă electronică]. – Regim de acces: https://blog.trendmicro.com/fileless-malware-a-hidden-threat/

11 Trend Micro. (2017, October 23). Fileless Malware: A Hidden Threat. Accesat 12.09.2019 [Resursă electronică]. – https://blog.trendmicro.com/fileless-malware-a-hidden-threat/

12 Tancio, B. (2017, June 15). Analyzing the Fileless, Code-injecting SOREBRECT Ransomware Accesat 15.10.2019 [Resursă electronică]. – https://blog.trendmicro.com/trendlabs-securityintelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/

13 Cryptocurrency Miner Uses WMI and EternalBlue To Spread Filelessly Accesat 15.10.2019 [Resursă electronică]. – https://blog.trendmicro.com/trendlabs-securityintelligence/cryptocurrency-miner-uses-wmi-eternalblue-spread-filelessly/

14 Dizon, J., Galang, L., & Cruz, M. (2010, July). Understanding WMI Malware. Accesat 17.10.2019 [Resursă electronică]. – http://la.trendmicro.com/media/misc/understanding-wmi-malware-researchpaper-en.pdf

15 Countercept. (2017, January 19). Memory Analysis Advanced Malware Detection in the Enterprise. Accesat 22.10.2019 [Resursă electronică]. – https://www.countercept.com/blog/memory-analysiswhitepaper/

16 Graeber, M., & Christensen, L. (2018, August). Subverting Sysmon Application of a Formalized Security Product Evasion Methodology. Accesat 22.10.2019 [Resursă electronică]. – https://i.blackhat.com/us-18/Wed-August-8/us-18-Graeber-Subverting-SysmonApplication-Of-A-Formalized-Security-Product-Evasion-Methodology-wp.pdf

17 Monnappa, K. A. (2017, March). What Malware Authors Do Not Want You to Know.

18 Edwards, G., & Studebaker, N. (2017, April 6). Fileless Malware Demystified. Accesat 22.11.2019 [Resursă electronică]. – https://www.youtube.com/watch?v=atL1WmmMJJw&feature=youtu.be

19- Zeltser, L. (n.d.). Deconstructing Fileless Attacks into 4 Underlying Techniques. Accesat 22.11.2019 [Resursă electronică]. – https://blog.minerva-labs.com/deconstructing-fileless-attacksinto-4-underlying-techniques

20 Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Hoboken, NJ: John Wiley & Sons.

21 SODINOKIBI: THE CROWN PRINCE OF RANSOMWARE Accesat 16.12.2019 [Resursă electronică]. – https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack

22 ransomware operation says it's shutting down Accesat 16.12.2019 [Resursă electronică]. – https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

23 Încarcarea unui DLL în Windows Accesat 16.12.2019 [Resursă electronică]. – https://support.microsoft.com/ro-ro/help/2019235/microsoft-office-access-error-in-loading-dll