A Comparative Experimental Evaluation of the Detection Rates and Removal Abilities of Fifteen Malware Detector Tools on Xpaj.MBR Rootkit

S. O. Subairu[1], J. K. Alhassan[2], V. O. Nwaocha[3] and I. R. Saidu[4]
[1,2]Cyber Security Science, Federal University of Technology,
Minna, Nigeria
[3]Department of Computer Science, NOUN, HQ, Abuja.
[4]Department of Intelligence and Cyber Security,
Nigerian Defence Academy, Kaduna, Nigeria.
Email:[1]lanrezubair@yahoo.com, [2]jkalhassan@futminna.edu.ng
[3]onwaocha@noun.edu.ng, [4]rambo@nda.edu.ng

ABSTRACT

Information Security experts have been focusing on the study of malwares because of its rise recently, with great interest on rootkits. Rootkits are a notably dangerously type of malware with the ability to cover their presence on the compromised system and allow malicious codes via spyware and other more obvious types of malware undetected. Once a rootkit gains access to the kernel of a system, it can be very tough to track and do away with it. In this research, various malware detector tools were critically analyzed and studied to ascertain their effectiveness in combating a deadly malware called Xpaj.MBR. An analytical model developed was used to obtain all experimental results and findings shows that detector with the highest detection rate is emco malware destroyer and it successfully removed the rootkit, while the detector with the least detection rate is malwarebytes, though it equally removed the rootkit successfully.

Keywords: *Rootkit, Xpaj.MBR, Antimalware, Malware, Detector*

African Journal of Computing & ICT Reference Format:

S.O. Subairu, J. K. Alhassan, V. O. Nwaocha and I. R. Saidu (2020), A Comparative Experimental Evaluation of the Detection Rates and Removal Abilities of Fifteen Malware Detector Tools on Xpaj.MBR Rootkit, *Afr. J. Comp. & ICT*, Vol. 13, No. 3, pp. 42 – 54.

I. INTRODUCTION

In recent years, rootkits have compromised windows operating system, with a capacity to hide portions of the file system, registry entries and other inner objects of operating system. Sadly enough, rootkits can continue to act with impunity until the system is utterly reformatted-or equally crafty technological tool is employed to get rid of it [1]. Figure 1 shows a relationship between computer hardware and application software via the kernel.

In many instances, rootkits are distributed in an open-source that means that even amateur programmers can easily manipulate rootkit code. Rootkit has the ability to conceal its virus signature; thereby making it difficult for most antiviruses, whose detection techniques is to look for virus's signature to detect [3]. There are various antimalware tools, whose efficacy such as detection rate, ability to get rid of malware has not been subjected to experimental analysis aside what the developer of such tools claimed. This research tends to fill this gap by subjecting a dangerous xpaj.MBR rootkit to fifteen antimalware tools and then determine their detection rate and ability to get rid of such malware from a compromised system.

The recent attack model of rootkit and other malware has grown to strong threat than before; the malware authors have developed various means to deliver their malicious codes. Most often through the internet via social networks like Facebook and others, through open source download, freeware download and social engineering techniques [4].

Malware could also be distributed through legitimate website that the hackers have injected malicious iframe into it. With the javascript on the hacker controlled website and the malware in their server, as soon as the user hit the legitimate website, the iframe executes the malicious code on the browser and request it to download the malware from the hacker server. This is downloaded silently and installed on the victim system making it part of a botnet [5] or other malicious system.

Malware detectors tools are software developed using various rootkit detection algorithms such as signature-based detection, heuristic/behavioral detection, cross view-based detection, hooking and integrity-based detection [6]. Each of these detection techniques are effective than one another and to get a desired result, combination of these detections may be adopted as claimed by rootkit detector tools developers. A typical malware attack model is shown in Figure 3.

II. PROBLEM STATEMENT

Most people are conversant with the concept of virus and anti-virus but a lot are ignorance about malware and anti-malware tools. Rootkit which serves as the gateway to other deadly malware is on the rise and according to McAfee Mobile Threat Report, August 2019, there are over three hundred and seven new threats every minute, and that is more than five per seconds. As of the third quarter of 2019, total number of malware exceeds sixty millions samples (Figure 2).

Numbers of systems in botnet has risen much more than before, even with updated antivirus. Personal identification theft, Denial of service (DOS), bank fraud, Government confidential data theft, industrial espionage and other crime are all rising due to the presence of malicious code in system across the globe [9].

Rootkit.MBR.xpaj is a dangerous malware that has the ability to change the MBR of a compromised system each time the system boot [10]. Being a rootkit, it hides its presence from being discovered within the operating system, hence it makes it difficult to get detected and eliminated.

Moreover, once an MBR is overwritten or changed by Xpaj.MBR rootkit; it loads its own codes into operating system as the system boot, thus compromising the system security architecture [11]. Xpaj.MBR Rootkit usually facilitates the connection of other malwares to a compromised system and open indirect access to execute command from remote assailants. Sensitive private data, organization data, could be stolen and used unlawful [11].

III. LITERATURE REVIEW

[12] Pointed out various rootkit and other malware threats which threats have grown more than before, as malware authors now developed various medium to spread their malicious codes. The internet which now provide the backbone for most of their deployment

especially social networks, open source download, freeware and other social engineering approach.

[13] Work on comparative analysis of rootkit detection, five samples of rootkit and twenty rootkit detectors were deployed for the research. The work adopted scanning and forensic analysis to detect presence of rootkit on a compromised system. This research was conducted in 2011, hence is in need of more findings as most of the detectors used are no longer being supported by their authors, hence detection capability cannot stand more recent rootkit like xpaj.MBR.

[14] Established that most rootkit and malwares often utilized an obfuscation approach to hide their malicious code and evade detection by antimalware tools. This obfuscation method varies from one malware to the other but with one purpose, which is to continue to compromise a system without being detected.

[15] Work on the various capabilities of rootkit detectors; a thorough work using five malwares and fifteen antimalware tools. The Authors based their result on collective analysis, however they failed to explain vividly or give a clear insight into each of the rootkit detector performance on each of the sample malwares as shown in their rootkit detectors ranking.

Therefore this research is keen to unravel and add value to the work of [15] by giving a detail analysis of the fifteen malware detectors performance on one of the sample malware called xpaj.MBR rootkit

[16] This independent organization often performed comparative analysis of most antivirus to determine their performance as against authors claimed in terms of security protection. The analysis is conducted periodically and reports are release stating the ranking of antivirus samples. However, the analysis report failed to state samples of malware that these tools were tested on. This is a serious issue when it comes to protecting our system, for a tool cannot offer protection against all various types' of malwares in circulation as the authors adopts various malicious obfuscation techniques. A tool may perform best at a particular malware but poorly perform with other type of malware.

[17] Proposed a novel approach in detecting kernel rootkit in virtual machine residence in private cloud. The authors adopted a machine learning approach after obtaining the malware features through forensic analysis of memory dump to train the classifier. The result presented by the authors was encouraging, but the limitation of the work could be seen as malware could easily detect virtual environment and tends to alter its payload codes.

IV. MATERIALS

The materials for this research are fifteen Computers system, Rootkit sample Xpaj-MBR. Fifteen Rootkit detectors namely: aswMBR, TDSS killer, Gmer, Rootkit remover, Bootkit remover, Malwarebytes Anti-rootkit, Comodo cleaning essential (cce), AVZ4, Vba32 Antirootkit, Emco Malware Destroyer, Stinger, Roguekiller, Unhackme, Regrun Plantinum, Rising Antivirus; Microsoft Kernel Debugger (KD.Exe) and Diskwipe for wiping the Hard Disk Drive.

V. EXPERIMENTAL PROCEDURE

An analytical study model was developed to guide our work as shown in Figure 4. Fifteen malware detectors that are actively been supported and a life xpaj.mbr rootkit were used for our study. Characteristics of all the tools were considered according to their respective authors claimed and as obtained in our experimental analysis as shown in Table 2. Each tool was run on a clean uninfected system to form a baseline of our study while false positive was observed for one of the tools as shown in Table 1. False positive is a false alert of threat when in reality none exist.

Thereafter each of the tools were run on an infected system with xpaj.mbr malware under a control environment, Ability to detect, remove and time duration were observed for all the tools as shown in Table 3 of our results.

Algorithm

Wipe HDD of each system using Diskwipe

Install each malware on each of the system
Run malware detector…. {Check for any false positive}

Install xpaj.MBR on each of the system

Run Microsoft Kernel Debugger to {confirmed malware Installation}

Run malware detector on each system {check the following parameters: scan time, detection ability, removal option, and success of removal attempt.}

V. RESULT AND DISCUSSION

The result as shown in Table 3 indicated that out of fifteen rootkit detector that were made to Run on xpajMBR infected system, five detectors were able to detect xpajMBR rootkit and only three of them were successful in removing this threat. These five detectors are emco, malware destroyer, gmer, malwarebytes, mcAfee stinger and roguekiller. The detector with the highest detection rate is emco malware destroyer and it successfully removed the rootkit, while the detector with the least detection rate is malwarebytes, though it equally removed the rootkit successfully.

Roguekiller detector result cannot be relied upon as it detected a malware on a clean system (False positive) as shown in Table 2. Figure 5, Figure 6 and Figure 7 shows their detection snapshot.

REFERENCES

[1] Chris, R. Inside Windows Rootkits. Vigilantmind Inc. 2006. Retrieved February 15, 2020 from http://repo.hackerzvoice.net/depot_madchat/vxdevl/library/Inside%20Windows%20Rootkits.pdf,1-18.

[2] Saliman, M. Rootkit: Attacker undercover tools. 2001. Retrieved February 22, 2020 from http://www.cyber security.my/data/content_files/13/82.pdf, 1-15.

[3] Ashwin, R. Detecting kernel rootkits. Master's Thesis Proposal Dartmouth Computer Science Technical Report TR2008-627, 2008. Retrieved April 9, 2020 from http://www.ists.dartmouth.edu/library/409.pdf, 2-5.

[4] Rehman, R., Hazarika, D., Chetia, G. Malware Threats and Mitigation Strategies: A Survey. Journal of Theoretical and Applied Information Technology. Vol. 29 No.2, 69-72, 2011.

[5] Rehman, R., Hazarika, D., Chetia, G. Malware Threats and Mitigation Strategies: A Survey. Journal of Theoretical and Applied Information Technology. Vol. 29 No.2, 69-72, 2011.

[6] Mashevsky, Y., Sapronov, K. and Monastyrsky, A. Rootkits and How to Combat Them, 2005. Retrieved April 22, 2020 from https://securelist.com/rootkits-and-how-to-combat-them/36055/

[7] Bits. Malware Risks and Mitigation Report. 2011 Retrieved May 5, 2020 from http://www.nist.gov/itl/ upload/BITS-Malware-Report-Jun2011.pdf

[8] McAfee Mobile Threat Report, August 2019. Retrieved March 10, 2020 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

[9] Microsoft Security Intelligence Report Volume 17 | January through June, 2014.Retrieved April 9, 2020 from http://www.emc.com/collateral/guide/11455-customer-faq.pdf.

[10] Miller, L.C. Malware for Dummies. 2012. Retrieved January 6, 2020 from https://www.paloaltonetworks.com/content/dam/paloa

ltonetworks-com/en_US/assets/pdf/education/MM%20for%20Dummies%20Unlimited%20Download%20eBook%20File.pdf

[11] Bridges, R., Hernandez Jimenez, J., Nichols, J., Goseva-Popstojanova, K., and Prowell, S. Towards malware detection via CPU power consumption: Data collection design and analytics. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. doi:10.1109/trustcom/bigdatase.2018.00250

[12]Rehman, R., Hazarika, D., Chetia, G. Malware Threats and Mitigation Strategies: A Survey. Journal of Theoretical and Applied Information Technology. Vol. 29, No.2, 69-72, 2011.

[13] Arnold, T. M. A Comparative Analysis of Rootkit Detection Techniques (Master's thesis), 2011. Retrieved January 6, 2020 from http://sce.uhcl.edu/yang/research/A%20Comparitive%20Analysis%20of%20Rootkit%20Detection%20Techniq ues.pdf

[14]Marpaung, J.A.P.; Sain, M. and Hoon-Jae, L, 'Survey on Malware Evasion Techniques: State of the Art and Challenges', *14th International Conference on Advanced Communication Technology* (ICACT), pp. 744-749, 2012**.**

[15]Alhassan, J. K; Subairu, S.O and Misra, S., 'Evaluating Capabilities of Rootkits Tools', *International Journal of Advanced Multidisciplinary Research and Studies* (IJAMRS), Vol. 1, Issue 1, pp. 27-30, 2016.

[16] AV-Comparative. 2020. Retrieved July 22, 2020 fromhttps://www.av-comparatives.org/tests/business-security-test-2020-march-june/

[17] Wang, X., Zhang, J., Zhang, A., and Ren, J. TKRD: Trusted kernel rootkit detection for cybersecurity of VMs based on machine learning and memory forensic analysis. *Mathematical Biosciences and Engineering*, *16*(4), 2650-2667, 2019. doi:10.3934/mbe.2019132

Figure1: Kernel connecting Computer Hardware to Application Software [2]

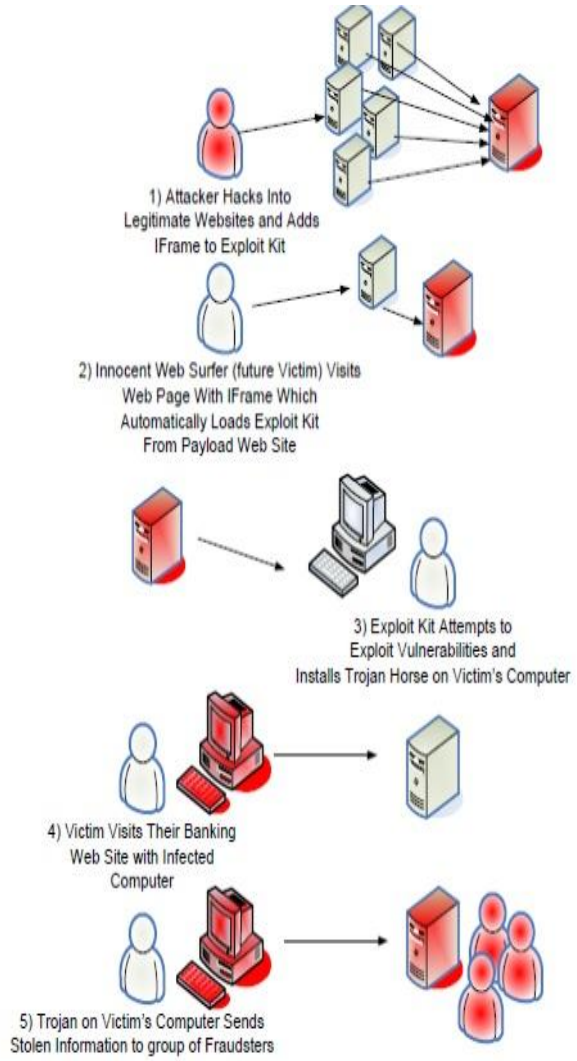

Figure 3: Malware Attack Model [7]

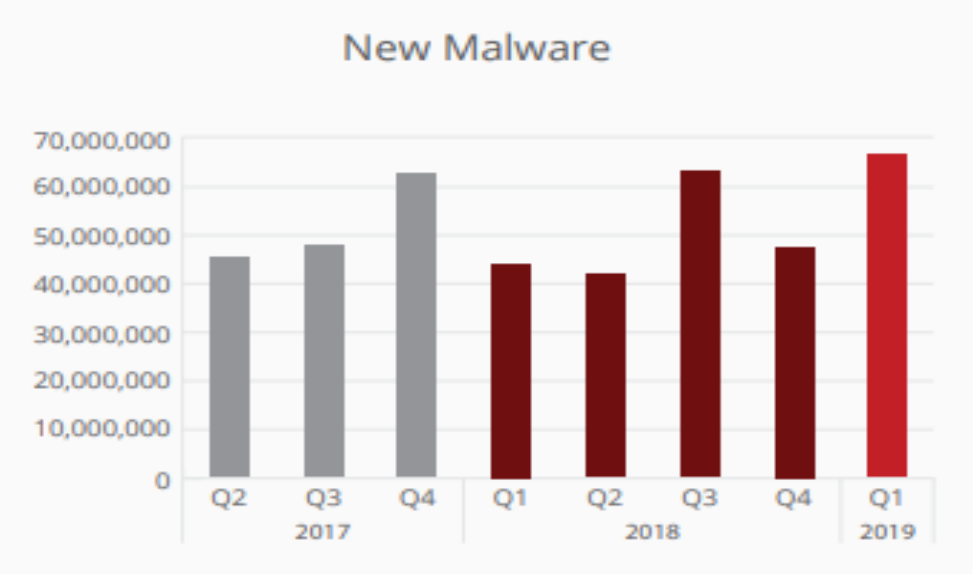

Figure 2: Total Number of New malware [8]

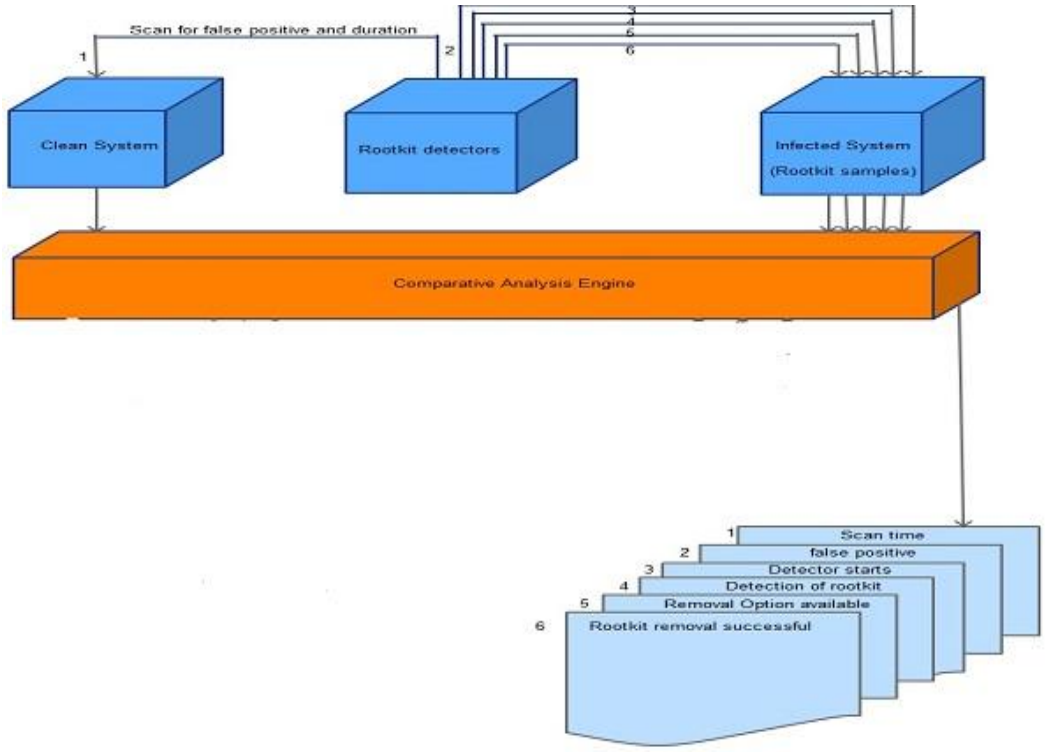

Figure 4: Analytical Study Model

Table 1: Malware Detector on Uninfected System

Malware Detectors	True Negative	False Positive
Avz antiviral Tootkit	✓	
Comodo cleaning essentials	✓	
Emco malware destroyer	✓	
Vba32arkit	✓	
aswMBR	✓	
Gmer	✓	
Malwarebytes	✓	
Mcafe rootkit removal	✓	
Bootkit Removal Tool	✓	
Kaspersky Tdsskiller	✓	
Unhackme	✓	
MacAfee stinger	✓	
*Roguekiller		✓
Regrun Platinum	✓	
Rising Antivirus	✓	

Table 2: Malware detectors characteristic

s/no	Rootkit detector	version	Active and supported	Detection Algorithm					Removal ability	Run on Infected system with sample rootkits
				signature	cross view	heuristic	hooking	Memory scanning		
1	Avz antiviral Toolkit	443	yes	Yes	yes	no	no	yes	yes	yes
2	Comodo cleaning essentials	25.2421772201	yes	Yes	yes	yes	yes	yes	yes	yes
3	Emsi malware destroyer	75.15.1950	yes	Yes	yes	yes	yes	yes	yes	yes
4	Vba32arkit	3124.0	no	Yes	yes	yes	yes	yes	yes	yes
5	aswMBR	10.1.2290	yes	Yes	yes	yes	yes	yes	yes	yes
6	Gmer	21.19357	yes	No	yes	no	yes	yes	yes	yes
7	Malwarebytes	1091.1004	yes	Yes	yes	yes	no	yes	yes	yes
8	Mcafa rootkit removal	08.9.174	yes	No	yes	yes	no	yes	yes	yes
9	Bootkit Removal Tool	30.2.2.011	yes	Yes	no	no	no	no	yes	yes
10	Kaspersky Tdsskiller	30.0.44	yes	Yes	yes	yes	yes	yes	yes	yes
11	Unlockme	771	yes	Yes	yes	yes	no	yes	yes	yes
12	MacAfee stinger	12.1.0.1534	yes	Yes	yes	yes	yes	yes	yes	yes
13	Roguekiller	10.6.5.0	yes					yes	yes	yes
14	Regnum Platnum	77	yes	Yes	yes	no	no	yes	yes	yes
15	Rising Antivirus	23.01.24.80	yes	Yes	yes			yes	yes	yes

Table 3: Rootkit detectors scan result of xpajMBR infected system

s/no	Detectors	Scan Time	Detection	Removal Option	Removal Successful
1	Avz antiviral Tootkit	00:00 :33	no	yes	No
2	Comodo cleaning essentials	00:24 :02	no	yes	No
3	Emco malware destroyer	00:00 :37	yes	yes	Yes
4	Vba32arkit	00:00 :25	no	yes	No
5	aswMBR	00:00 :41	no	yes	No
6	Gmer	00:02 :01	yes	no	No
7	Malwarebytes	00:04 :55	yes	yes	Yes
8	Mcafe rootkit removal	00:00 :12	no	yes	No
9	Bootkit Removal Tool	00:00 :12	no	yes	No
10	Kaspersky Tdsskiller	00:00 :10	no	yes	No
11	Unhackme	00:00 :25	no	yes	No
12	MacAfee stinger	00:01 :24	yes	yes	Yes
13	*Roguekiller	00:03 :19	yes	yes	No
14	Regrun Platinum	00:00 :39	no	yes	No
15	Rising Antivirus	00:29 :20	no	yes	No

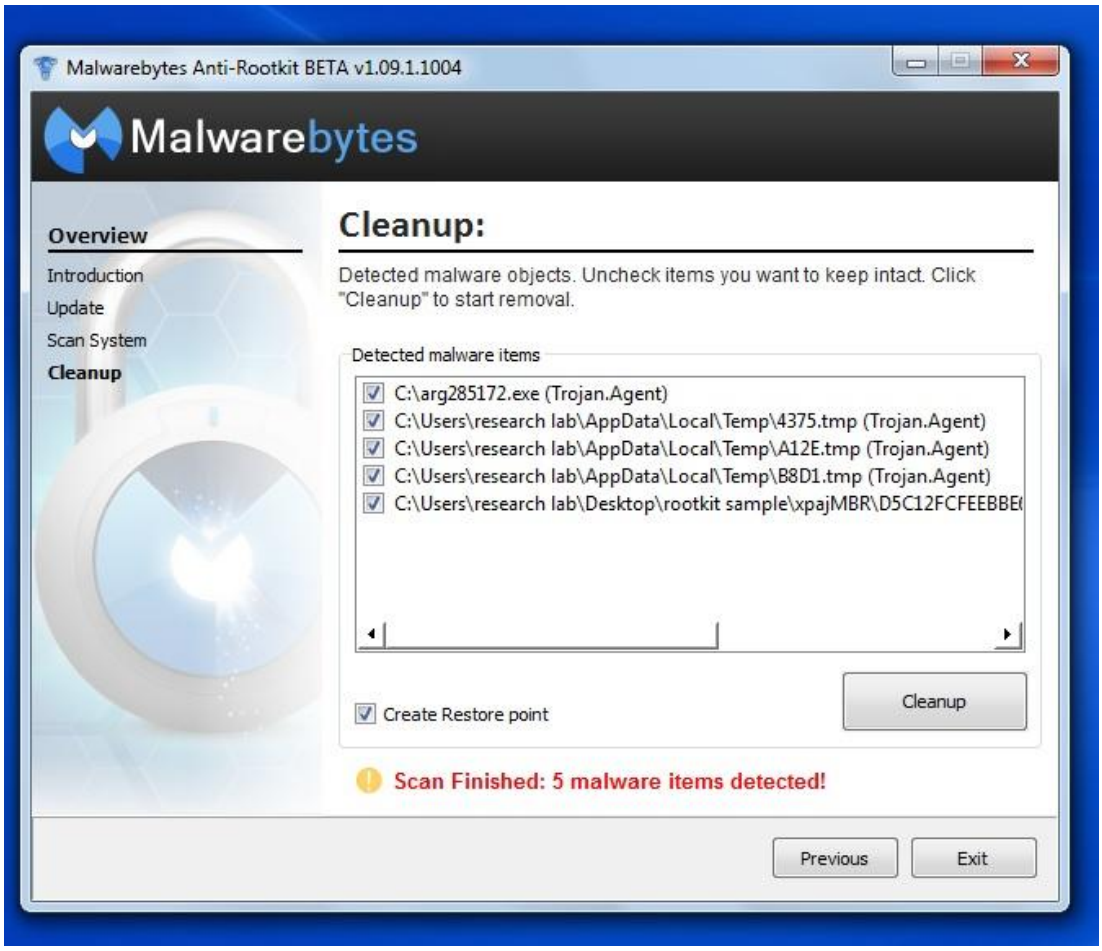

Figure 5: Xpaj.MBR detected by Malwarebytes

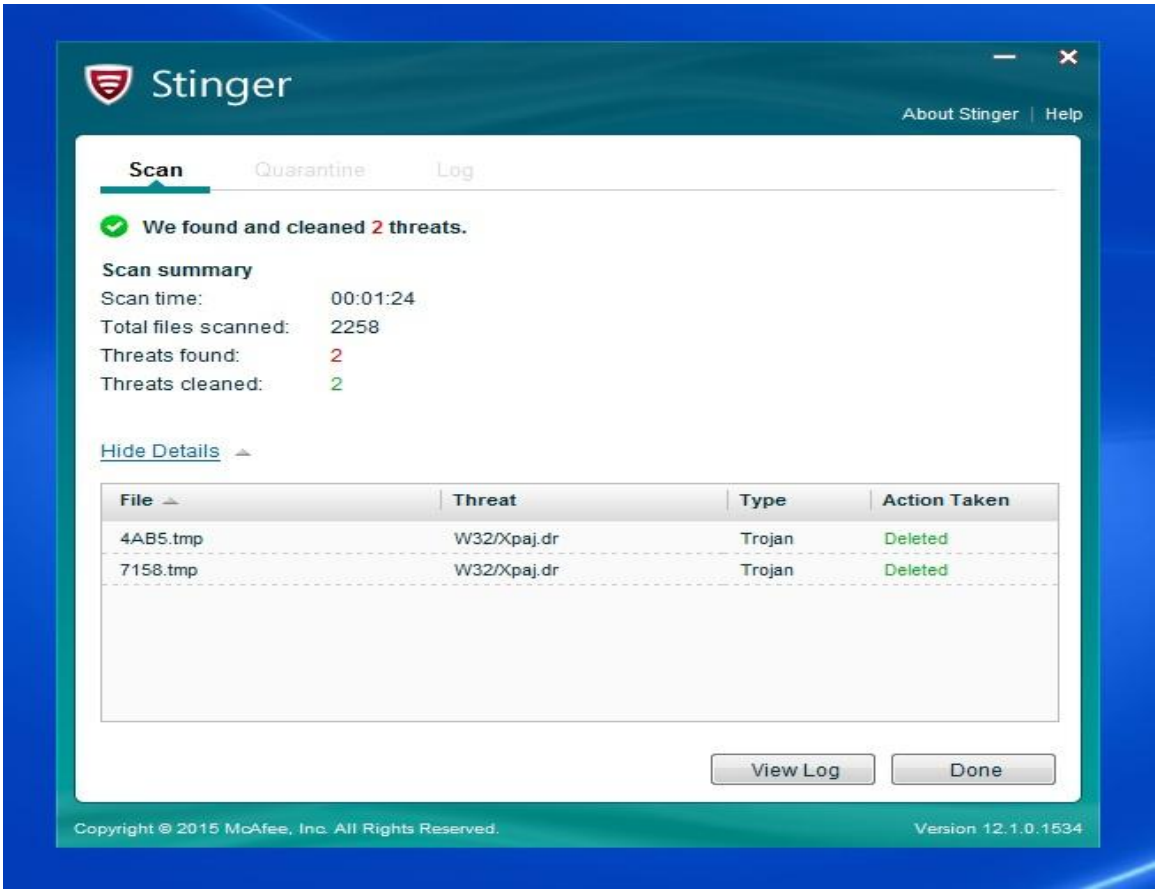

Figure 6: xpajMBR detected by Stinger

Figure 7: Xpaj.MBR detected by Roguekiller