ANÁLISE COMPARATIVA DA EFICÁCIA DE SOFTWARES DE PROTEÇÃO GRATUITOS EM CENÁRIOS DE ARQUIVOS INFECTADOS COM MALWARES.

MÁRCIO MENDES LORENZETO[1]
LUCIANO GONÇALVES DE CARVALHO[2]

RESUMO

O artigo examina a eficácia de antivírus gratuitos na detecção de diferentes tipos de malwares, utilizando o serviço VirusTotal, que agrupa resultados de vários motores de antivírus. O estudo focou em malwares como Trojans, ransomware, RevengeRAT e Andromeda, destacando como essas ameaças agem no sistema. Através da análise das amostras de malware, o VirusTotal foi usado para verificar quais antivírus gratuitos foram capazes de detectar as ameaças e comparar sua eficácia.

Palavras-chave: Antivírus; Detecção; Eficácia; Malware; Ransomware; Trojan.

ABSTRACT

The article examines the effectiveness of free antivirus software in detecting different types of malware, using the VirusTotal service, which aggregates results from various antivirus engines. The study focused on malware such as Trojans, ransomware, RevengeRAT, and Andromeda, highlighting how these threats act on the system. Through the analysis of malware samples, VirusTotal was used to verify which free antivirus software were able to detect the threats and compare their effectiveness.

Key words: Antivirus; Detectio; Effectiveness; Malware; Ransomware; Trojan.

INTRODUÇÃO

Com o avanço constante do uso da tecnologia para várias atividades do nosso cotidiano, também houve um aumento nos ataques cibernéticos. Na grande maioria desses ataques, o intuito é roubar informações pessoais dos usuários, como CPF, RG, número do cartão e senhas de acesso.

Para prevenir, detectar e remover malwares, surgiram ferramentas conhecidas como antivírus, que buscam oferecer maior segurança para os usuários em relação

[1]Graduando, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP. márcio.lorenzeto@fatec.sp.gov.br
[2]Docente, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP.

aos seus dados, protegendo-os de possíveis ataques, como links suspeitos, sites mal-intencionados, cavalos de Troia, entre outros tipos de ameaças.

No entanto, atualmente, existe uma grande variedade de antivírus no mercado, o que acaba dificultando para os usuários a escolha do ideal e de melhor eficácia. Considerando que nem todos estão dispostos a pagar por um antivírus como Norton, McAfee ou NordVPN, por exemplo, muitos acabam recorrendo a opções gratuitas oferecidas por empresas como Kaspersky, Avast e AVG, que, além das versões pagas, também disponibilizam uma versão gratuita de seus softwares.

Dessa forma, este artigo tem como objetivo analisar os antivírus disponíveis no mercado, considerando as versões gratuitas que algumas empresas distribuem, com o propósito de comparar essas ferramentas em cenários de arquivos infectados por malware.

MATERIAL E MÉTODOS

Por se tratar de malwares, foram selecionados tipos específicos de vírus, disponibilizado em um repositório do GitHub para interessados na análise de malwares.

Dessa forma, realizaremos uma análise comparativa entre os antivírus selecionados para determinar qual das ferramentas apresenta a melhor taxa de desempenho em cenários com arquivos infectados.

Como parte das medidas de segurança adotadas para a execução dos testes com arquivos maliciosos, configuramos uma máquina virtual dedicada. Essa abordagem foi escolhida para evitar qualquer risco de infecção no sistema principal, uma vez que estamos lidando com malware ativo.

A máquina virtual foi criada utilizando o software Oracle VM VirtualBox e configurada com a última versão LTS (Long Term Support) do sistema operacional Ubuntu Linux. Esse ambiente possui 25 GB de armazenamento e 8 GB de memória

RAM, garantindo a performance necessária para o processamento dos testes sem comprometer a segurança.

O uso de uma máquina virtual proporciona um isolamento eficaz, reduzindo o risco de propagação dos malwares e permitindo que os arquivos contaminados sejam manipulados com segurança. Esse cuidado foi essencial para o desenvolvimento da metodologia de testes, assegurando a integridade tanto do sistema anfitrião quanto da rede envolvida.

Para avaliar a eficácia dos antivírus em suas versões gratuitas, foram realizados testes com amostras de arquivos contaminados por diferentes tipos de malware. O objetivo desses testes é verificar quais softwares antivírus são capazes de identificar e classificar corretamente essas ameaças.

Primeiramente, foram coletadas amostras de arquivos infectados, representando uma variedade de tipos de malware. Essas amostras foram obtidas no repositório GitHub "TheZoo", que disponibiliza malwares vivos e criptografados (https://github.com/ytisf/theZoo/), a fim de simular um ambiente de infecção realista para estudo. Em seguida, esses arquivos foram submetidos ao serviço de análise VirusTotal, que agrega resultados de diversos motores antivírus, para verificar a detecção e classificação de cada ameaça.

Os resultados fornecidos pelo VirusTotal indicam quais motores de antivírus detectaram o malware e quais não o fizeram, permitindo uma análise comparativa entre as soluções antivírus gratuitas disponíveis. Essa metodologia proporciona uma visão prática e objetiva da eficácia dessas ferramentas na identificação de ameaças digitais, destacando suas limitações e pontos fortes em um cenário de uso real.

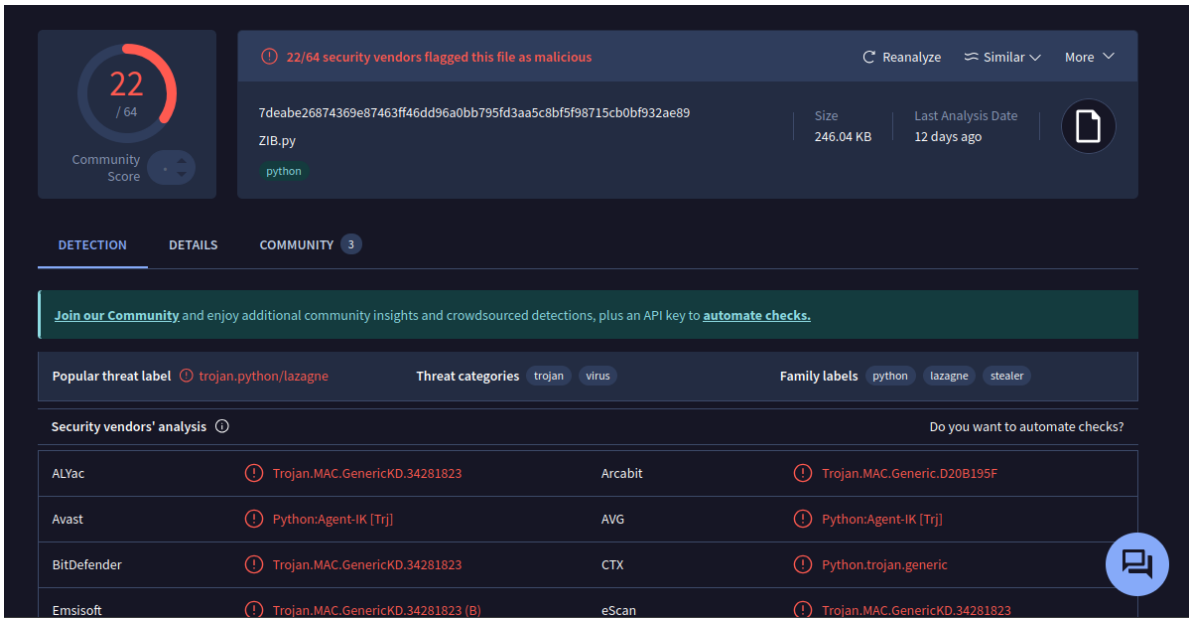
Para o início dos testes, usaremos o arquivo executável da amostra do Zib_Trojan, que será anexado no site VirusTotal, onde receberemos um resultado de detecção entre os principais antivírus. Faremos o mesmo com as demais amostras preparadas.

RESULTADOS E DISCUSSÃO

Trojan, também conhecido como cavalo de Troia, é um tipo de malware que aparenta ser inofensivo para o usuário, mas, na verdade, causa muitos problemas. Ele geralmente é disfarçado como um aplicativo ou link que, ao ser instalado ou acessado, inicia seu processo de infecção no sistema.

Observamos na figura 1 que 22 dos 64 motores de antivírus detectaram o arquivo como malicioso. Esse número é importante, pois indica a taxa de detecção dessa amostra específica. Quanto mais motores identificarem o arquivo como malicioso, maior é a probabilidade de que ele seja realmente um malware.

Figura 1. Análise do Executável Zib_Trojan.py pelo Virus Total_P1.



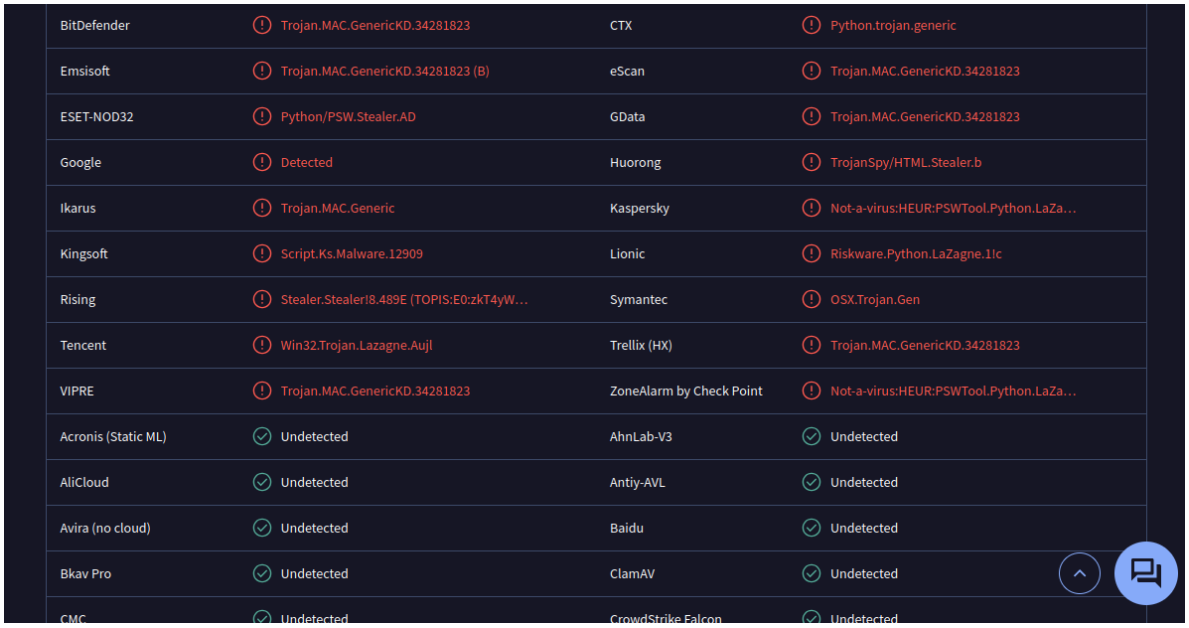
Fonte: Autores, (2024).

Abaixo das informações do arquivo, o VirusTotal exibe as etiquetas atribuídas a essa ameaça por diferentes motores de antivírus. Ela é classificada como um trojan, ou cavalo de Troia, o que sugere que pode executar ações maliciosas em segundo plano sem o consentimento do usuário. Além disso, o malware possui etiquetas como

"python" e "lazagne", indicando que foi identificado como um malware escrito em Python e provavelmente está relacionado ao projeto "Lazagne", uma ferramenta de recuperação de senhas frequentemente abusada em atividades maliciosas.

Na figura 2, podemos ver uma lista dos motores de antivírus que detectaram o arquivo como malicioso. Cada entrada inclui o nome do motor (como ALYac, Avast, BitDefender) e o nome específico da ameaça que ele detectou. Observa-se que a maioria dos antivírus classificou o arquivo como uma variante genérica de trojan ou stealer (malware que rouba dados). Nomes como Trojan.MAC.GenericKD e Python indicam que se trata de um malware genérico do tipo trojan, adaptado para sistemas que suportam Python.

Figura 2 Análise do Executável Zib_Trojan.py pelo Virus Total_P2.



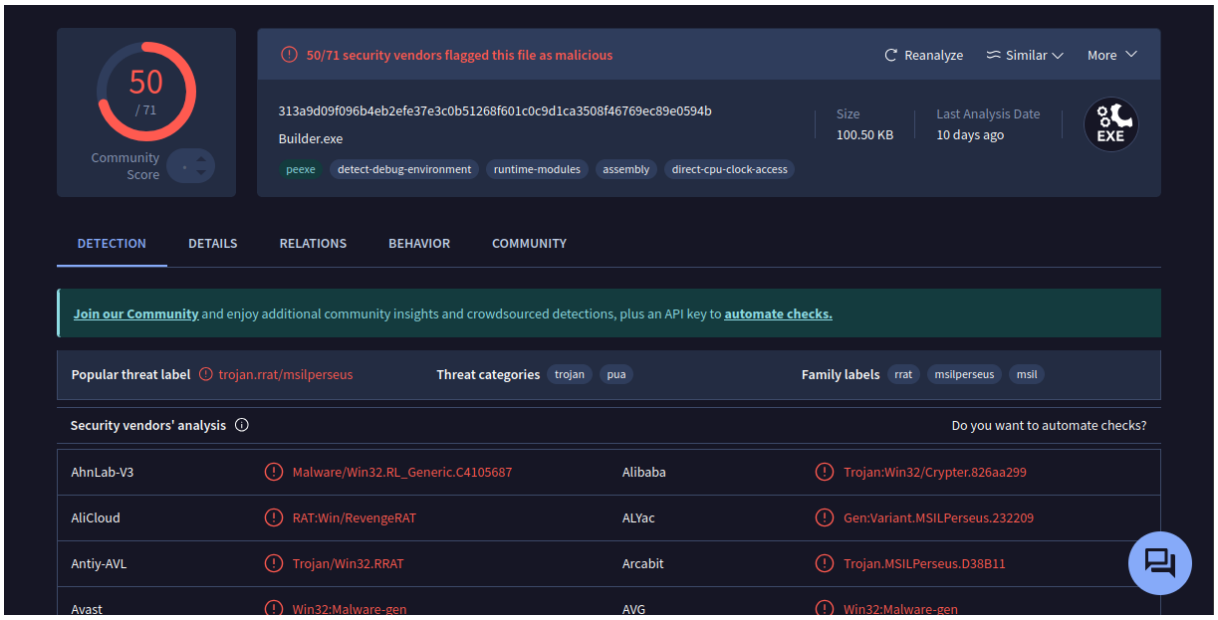
BitDefender	Trojan.MAC.GenericKD.34281823	CTX	Python.trojan.generic
Emsisoft	Trojan.MAC.GenericKD.34281823 (B)	eScan	Trojan.MAC.GenericKD.34281823
ESET-NOD32	Python/PSW.Stealer.AD	GData	Trojan.MAC.GenericKD.34281823
Google	Detected	Huorong	TrojanSpy/HTML.Stealer.b
Ikarus	Trojan.MAC.Generic	Kaspersky	Not-a-virus:HEUR:PSWTool.Python.LaZa…
Kingsoft	Script.Ks.Malware.12909	Lionic	Riskware.Python.LaZagne.1!c
Rising	Stealer.Stealer!8.489E (TOP!S:E0:zkT4yW…	Symantec	OSX.Trojan.Gen
Tencent	Win32.Trojan.Lazagne.Aujl	Trellix (HX)	Trojan.MAC.GenericKD.34281823
VIPRE	Trojan.MAC.GenericKD.34281823	ZoneAlarm by Check Point	Not-a-virus:HEUR:PSWTool.Python.LaZa…
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	Antiy-AVL	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected

Fonte: Autores, (2024).

RevengeRAT (Remote Access Trojan) é uma variante do cavalo de Troia que, além das características mencionadas anteriormente, concede acesso remoto à máquina da vítima. Dessa forma, o atacante pode acessar informações sensíveis da vítima, como senhas e dados confidenciais.

Na figura 3, vemos que 50 dos 71 motores de antivírus identificaram o arquivo como malicioso. Esse número sugere uma alta probabilidade de que o arquivo realmente contenha algum tipo de malware, dado que a maioria dos motores o sinalizou como uma ameaça.

Figura 3. Análise Revenge Rat_P1.



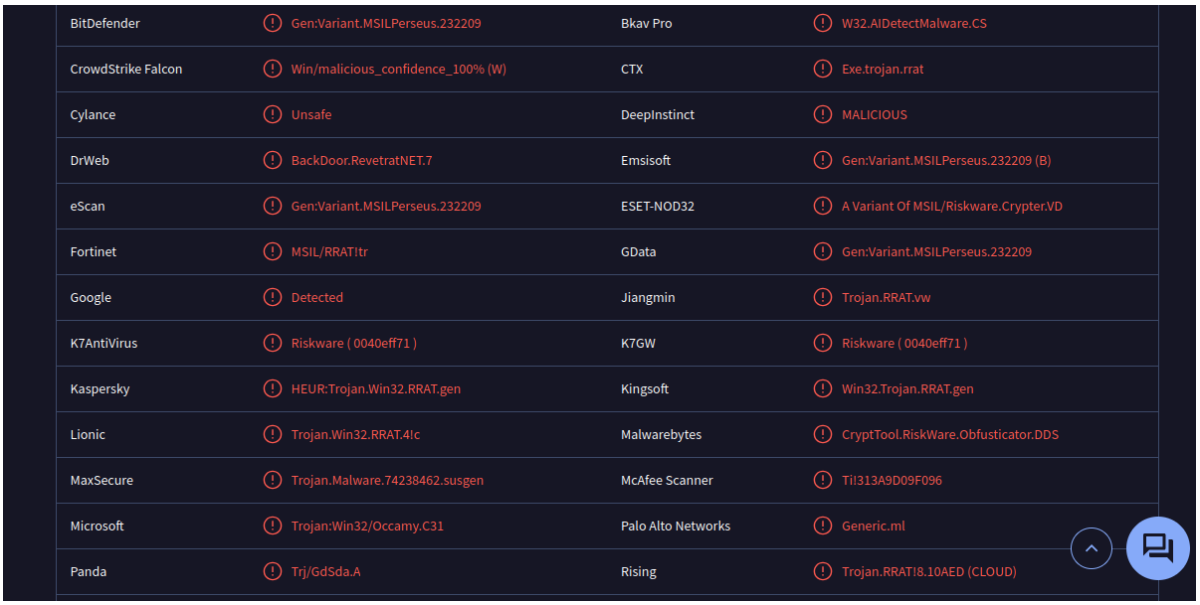
Fonte: Autores, (2024).

O nome do arquivo é Builder.exe, indicando que se trata de um executável do Windows. Executáveis com o nome "Builder" estão frequentemente associados a malwares que criam (ou "constroem") outras amostras de malware. O VirusTotal atribui as etiquetas "trojan" e "pua" (potencialmente indesejado) a essa ameaça, sugerindo que é um trojan que pode realizar ações indesejadas ou maliciosas no sistema. As etiquetas adicionais, como "rrat", "msilperseus" e "msil", indicam que o malware pode ser um trojan de acesso remoto (RAT) construído em .NET (Microsoft Intermediate Language - MSIL), conhecido por dar acesso remoto ao invasor.

Na figura 4, vemos uma lista dos motores de antivírus que detectaram o arquivo como malicioso, com os nomes específicos das ameaças. Alguns exemplos incluem:

- AhnLab-V3 identifica o arquivo como Malware/Win32.RL_Generic.C4105687.
- AliCloud o classifica como RAT /RevengeRAT, um trojan de acesso remoto conhecido.
- Avast o detecta como Win32, indicando características genéricas de malware.

Figura 4. Análise Revenge Rat_P2.



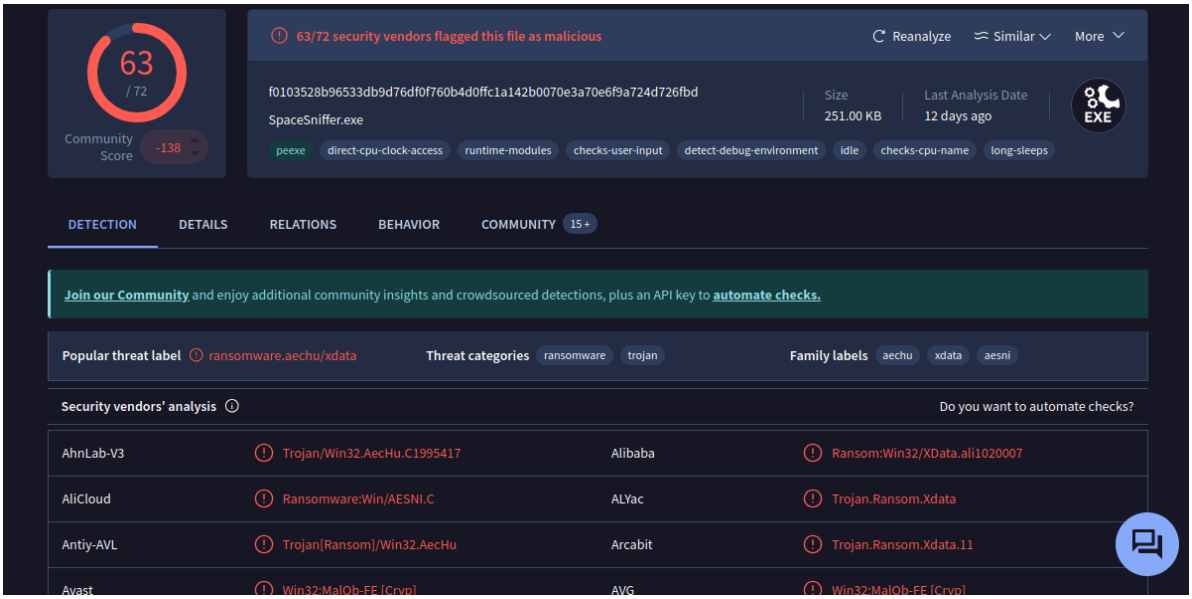
BitDefender	Gen:Variant.MSILPerseus.232209	Bkav Pro	W32.AIDetectMalware.CS
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.rrat
Cylance	Unsafe	DeepInstinct	MALICIOUS
DrWeb	BackDoor.RevetratNET.7	Emsisoft	Gen:Variant.MSILPerseus.232209 (B)
eScan	Gen:Variant.MSILPerseus.232209	ESET-NOD32	A Variant Of MSIL/Riskware.Crypter.VD
Fortinet	MSIL/RRAT!tr	GData	Gen:Variant.MSILPerseus.232209
Google	Detected	Jiangmin	Trojan.RRAT.vw
K7AntiVirus	Riskware (0040eff71)	K7GW	Riskware (0040eff71)
Kaspersky	HEUR:Trojan.Win32.RRAT.gen	Kingsoft	Win32.Trojan.RRAT.gen
Lionic	Trojan.Win32.RRAT.4!c	Malwarebytes	CryptTool.RiskWare.Obfusticator.DDS
MaxSecure	Trojan.Malware.74238462.susgen	McAfee Scanner	Ti!313A9D09F096
Microsoft	Trojan:Win32/Occamy.C31	Palo Alto Networks	Generic.ml
Panda	Trj/GdSda.A	Rising	Trojan.RRAT!8.10AED (CLOUD)

Fonte: Autores, (2024).

Ransomware é um tipo de malware que deixa a máquina da vítima inacessível, permitindo o retorno do acesso apenas mediante pagamento de “resgate” pelas informações. O nível de bloqueio dos dados varia entre ransomwares: alguns podem criptografar arquivos individuais, enquanto outros bloqueiam o sistema operacional inteiro.

A figura 5 mostra que 63 dos 72 motores de antivírus detectaram o arquivo como malicioso, indicando uma altíssima probabilidade de se tratar de um malware perigoso, visto que a maioria dos motores de segurança o sinalizou como uma ameaça.

Figura 5. Análise Ransomware.Xdata_P1.



Fonte: Autores, (2024).

O nome do arquivo é SpaceSniffer.exe, o que pode sugerir que ele se apresenta como uma ferramenta legítima para análise de espaço em disco, mas provavelmente foi adulterado para fins maliciosos. O VirusTotal associa as etiquetas "ransomware" e "trojan" a essa ameaça, indicando que esse malware não apenas age como um trojan (executando atividades maliciosas em segundo plano), mas também pode criptografar arquivos e exigir resgate, como é comum em ataques de ransomware. As etiquetas adicionais "aechu", "xdata" e "aesni" sugerem que o ransomware pode estar relacionado a variantes conhecidas do malware, como as que criptografam dados e exigem pagamento para restaurar o acesso.

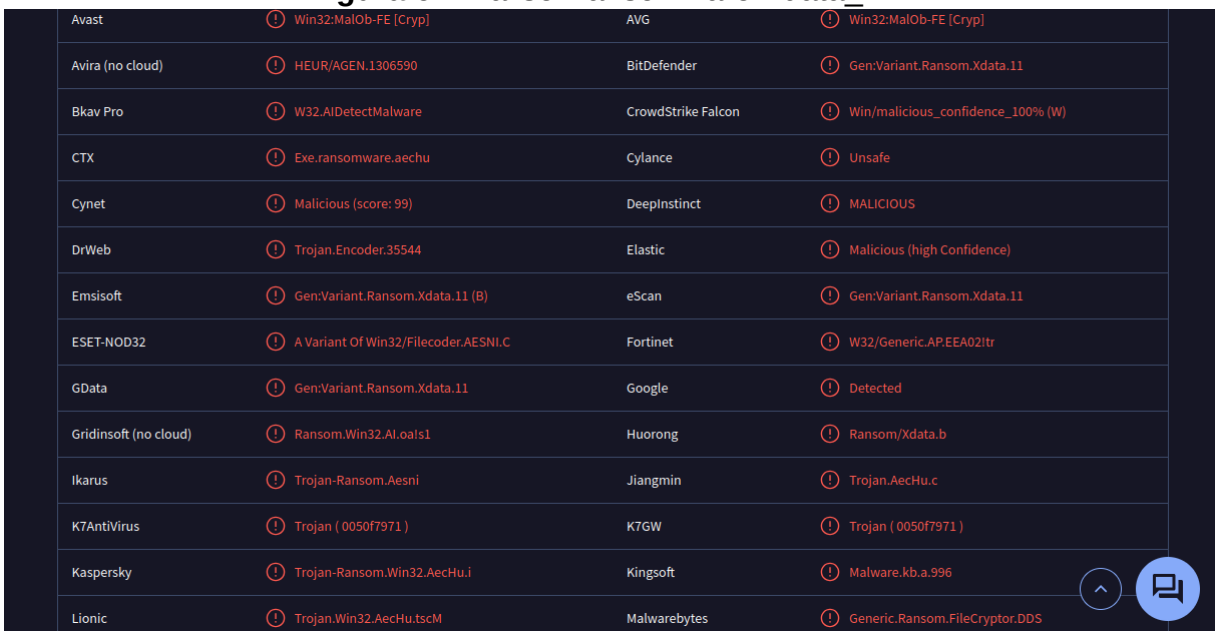
Vários motores de antivírus identificam o arquivo como ransomware, com nomes específicos para a ameaça, como:

- AhnLab-V3 detecta como Trojan/Win32.AecHu.C1995417.
- AliCloud o classifica como Ransomware /AESNI.C, uma conhecida família de ransomware.
- Antiy-AVL o identifica como Trojan[Ransom]/Win32.AecHu.

- Outros motores, como Avast e AVG, também sinalizam o arquivo como variantes de ransomware.

Na figura 6, o padrão de detecção confirma a natureza perigosa do arquivo, indicando que ele foi identificado como ransomware com potencial de causar grandes danos ao sistema infectado.

Figura 6. Análise Ransomware.Xdata_P2.

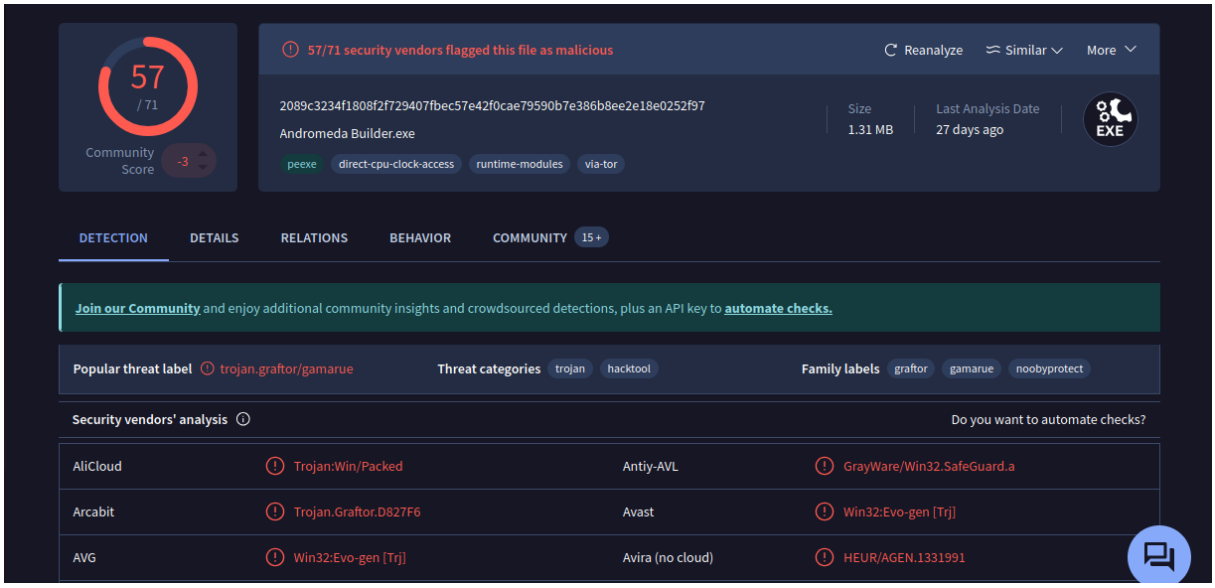


Fonte: Autores, (2024).

Andromeda, também conhecido como Gamarue, é um malware notório por ser um botnet, ou seja, uma rede de computadores infectados controlados remotamente por cibercriminosos. Andromeda foi um malware extremamente perigoso, trazendo grandes problemas a usuários comuns e empresas, sendo utilizado como porta de entrada para distribuir outros malwares e realizar atividades maliciosas, como roubo de dados e ataques DDoS.

Na figura 7, vemos que 57 dos 71 motores de antivírus detectaram o arquivo como malicioso, indicando uma alta probabilidade de ser uma ameaça perigosa, dado que a maioria dos motores de segurança o sinalizou como suspeito.

Figura 7. Análise Andromeda_P1.



Fonte: Autores, (2024).

O arquivo Andromeda Builder.exe pode parecer uma ferramenta de desenvolvimento, mas é provável que tenha sido modificado para fins maliciosos, pois arquivos nomeados "Builder" geralmente estão associados a malwares que criam componentes no sistema infectado. O VirusTotal atribui etiquetas como "trojan.graftor/gamarue" e "hacktool" a essa ameaça, sugerindo que o arquivo pode realizar atividades de trojan (ações maliciosas ocultas) e ser utilizado para hacking.

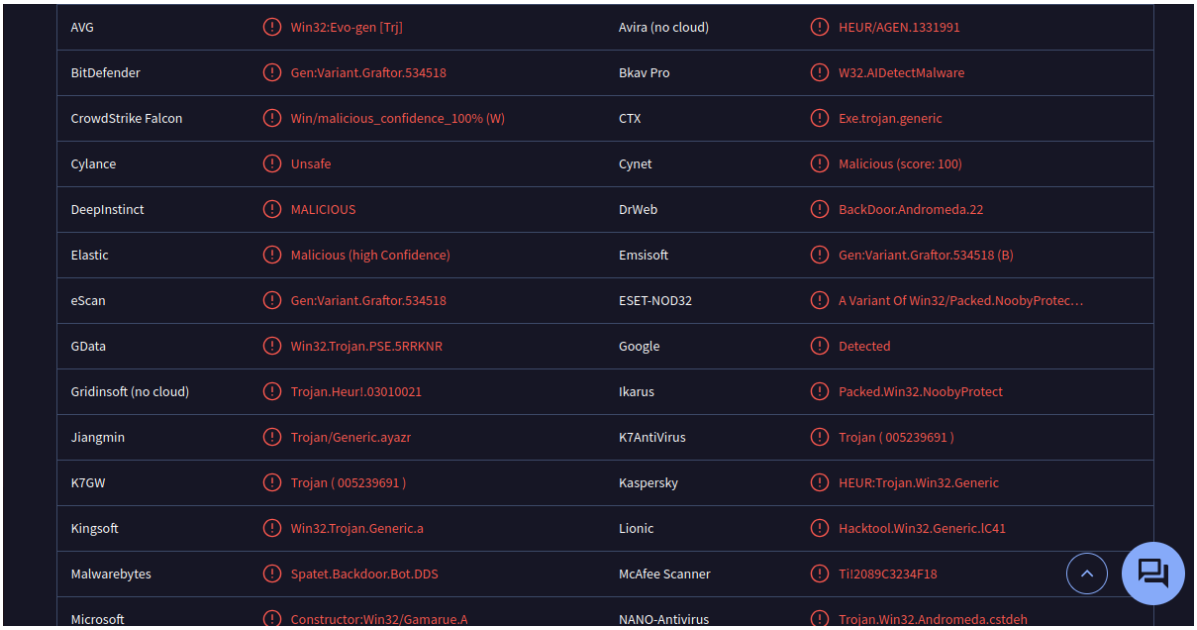
As etiquetas adicionais "graftor," "gamarue," e "noobyprotect" indicam que o malware está relacionado a variantes específicas de trojans conhecidos por comprometer sistemas e roubar informações. Diversos motores de antivírus identificam o arquivo como trojan, com alguns nomes específicos para a ameaça, como:

- AliCloud: Detecta como Trojan/Packed.
- Arcabit: Identifica como Trojan.Graftor.D827F6.
- AVG: Classifica como Win32[Trj].
- BitDefender: Marca como Gen.Graftor.534518.

Na figura 8, outros motores de antivírus, como Avast e Avira, também sinalizam o arquivo com variações de trojan.

Figura 8. Análise Andromeda_P2.

Fonte: Autores, (2024).



As amostras analisadas representam diferentes tipos de ameaças: roubo de informações, controle remoto e ransomware. Cada uma exige medidas específicas de defesa, desde o fortalecimento das práticas de segurança da informação até a implementação de ferramentas antivírus robustas e atualizadas. Além disso, a utilização de ambientes seguros, como máquinas virtuais, é fundamental para a análise de malware, minimizando o risco de infecção em sistemas reais. Essas ameaças evidenciam a importância de uma defesa em profundidade para proteger sistemas contra os diversos vetores de ataque.

CONCLUSÃO

Dessa forma, concluímos que a maioria dos antivírus gratuitos é eficaz na detecção de diversos tipos de malwares comuns, como trojans, oferecendo proteção para grande parte dos usuários. Sendo excelentes para quem busca uma proteção básica e confiável. Por outro lado, os antivírus pagos oferecem um leque mais amplo de recursos, como proteção em tempo real mais robusta, firewall integrado e segurança contra phishing. Em suma, a escolha entre um gratuito e um pago dependerá das necessidades específicas de cada usuário. Se está em busca de uma proteção básica para o uso diário, um antivírus gratuito pode ser suficiente. No entanto, se precisa de uma segurança mais completa e personalizada, um antivírus pago é a melhor opção.

REFERÊNCIAS BIBLIOGRÁFICAS

ALGAR TELECOM. **Vírus de Computador: 10 mais conhecidos e como evitar? (2022)**. Disponível em: https://blog.algartelecom.com.br/conheca-os-5-tipos-de-virus-mais-comuns-na-internet-2/. Acesso em: 11 ago. 2025.

AVAST. **Rede zumbi Andromeda muda de estratégia para infectar usuários**. Disponível em: https://blog.avast.com/pt-br/rede-zumbi-andromeda-muda-de-estrategia-para-infectar-usuarios. Acesso em: 11 ago. 2025.

BITDEFENDER. **O que é um Trojan? Prevenção e Remoção**. Disponível em: https://www.bitdefender.com.br/consumer/support/answer/76493/. Acesso em: 11 ago. 2025.

CHECK POINT. **O que é um Trojan de acesso remoto (RAT)?** Disponível em: https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-remote-access-trojan/. Acesso em: 11 ago. 2025.

CSK INDIA. **Andromeda Alert**. Disponível em: https://www.csk.gov.in/alerts/andromeda.html. Acesso em: 11 ago. 2025.

CYBEREASON. **What is the Andromeda Botnet?** Disponível em: https://www.cybereason.com/blog/what-is-the-andromeda-botnet. Acesso em: 11 ago. 2025.

KASPERSKY. **O que é ransomware?** Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 11 ago. 2025.

KASPERSKY. **Trojan-Downloader.Win32.Andromeda**. Disponível em: https://threats.kaspersky.com/br/threat/Trojan-Downloader.Win32.Andromeda/. Acesso em: 11 ago. 2025.

WELIVESECURITY. **XData entra em cena no meio do susto mundial causado pelo WannaCryptor**. Disponível em: https://www.welivesecurity.com/br/2017/05/24/xdata-entra-em-cena/. Publicado em 24 maio 2017. Acesso em: 11 ago. 2025.