TESTING GROUND LABS

Ransomware Protection Test

Consumer Product / Windows Platform

2023 May

• • • Celebrating Technology Innovation

Table of Contents

Report version 1.0, published on 2023.06.19, initial version

© 2020-2023 Testing Ground Labs

Chap.1 Background

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.

Starting as early as 1989 with the first documented ransomware known as the AIDS trojan, the use of ransomware scams has grown internationally. There were 181.5 million ransomware attacks in the first six months of 2018. This record marks a 229% increase over this same time frame in 2017. In June 2014, vendor McAfee released data showing that it had collected more than double the number of ransomware samples that quarter than it had in the same quarter of the previous year. CryptoLocker was particularly successful, procuring an estimated US$3 million before it was taken down by authorities, and CryptoWall was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over US$18 million by June 2015. In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. The losses could be more than that, according to the FBI. According to a report by SonicWall, there were around 623 million ransomware attacks in 2021.

Above words are taken from https://en.wikipedia.org/wiki/Ransomware

© 2020-2023 Testing Ground Labs

Chap.2 Test Process & Test Software

Detailed process is as follows:

1. ~100-200 ransomware samples are selected from TGL's collection (part of them are sourced from TGL's 1 million daily spam collection). Each sample is validated manually to make sure the sample is fully functional in the testing environment.
2. Platform: Windows 11.
3. A broad set of user-files of different types will be prepared and placed in different folders through the File System, their state (filename and checksum) will be recorded by our script. And they will also be used for sorting out the functional ransomware samples.
4. Install selected security applications on the prepared VMware OS image in default configuration.
5. Update the security applications and their antivirus bases.
6. Copy the sample set to a system with a security application and make a record about the detected\deleted samples.
7. Run each missed ransomware sample and take every action suggested by security solution. Compare the file system and check if the user-files are fully protected or been recovered.
8. Detection from on access scan, protection after sample is executed (all user-files are in their initial state), failure to protect file system, are recorded.

Vendor	Software	Version
Ahnlab	Ahnlab V3 Endpoint Security	9.0.78.9 (Build 1972)
Avast	Avast Premium Security	23.5.6066(Version 23.5.8195.784)
Avira	Avira Internet Security	1.1.88.1
Bitdefender	Bitdefender Internet Security	26.0.36.193
ESET	ESET Internet Security	16.1.14.0
G DATA	G DATA Internet Security	25.5.15.21
Kaspersky	Kaspersky Plus	21.13.5.506
Malwarebytes	Malwarebytes Premium	4.5.29.268
McAfee	McAfee Total Protection	26.6.161
Microsoft	Windows Defender	4.18.2304.8
NortonLifeLock	Norton 360	22.23.3.8
Sophos	Sophos Home Premium	4.3.0.5
Trend Micro	Trend Micro Internet Security	17.7.1503 - Q4EXP

© 2020-2023 Testing Ground Labs

Chap.3 Tested Result (The test results are shown on the following tab)

Vendor	Total Samples	Missed Samples	Detected Samples	Detection Rate	Total Score
Ahnlab	104	0	104	100.00%	100
Avast	104	0	104	100.00%	100
Avira	104	0	104	100.00%	100
Bitdefender	104	0	104	100.00%	100
ESET	104	0	104	100.00%	100
G DATA	104	0	104	100.00%	100
Kaspersky	104	0	104	100.00%	100
Malwarebytes	104	0	104	100.00%	100
McAfee	104	0	104	100.00%	100
Microsoft	104	0	104	100.00%	100
NortonLifeLock	104	0	104	100.00%	100
Sophos	104	0	104	100.00%	100
Trend Micro	104	0	104	100.00%	100

- For each security solution, a Final Score is calculated once the full test is performed:
  Final Score = (Protection rate%) *100
  Protection= on access scan protection plus protection during sample execution
  Basing on the Final Score, the correspondent rating is grated to each participating security solution, in accordance with the tab below:

final score	monthly award
98.00 - 100.00	5-star rating
95.00 - 97.99	4-star rating
90.00 - 94.99	3-star rating

© 2020-2023 Testing Ground Labs

Chap.4 Test Summary & Monthly Award

- Monthly Award:

2023 May	Ransomware Protection Test 2023 May (Windows / Consumer)
Ahnlab Avast Avira Bitdefender ESET G DATA Kaspersky Malwarebytes McAfee Microsoft NortonLifeLock Sophos Trend Micro	**5 Star Monthly Award 2023 May** **Consumer Product / Windows Platform**

Chap.5 Compliance

This test was made in accordance with the requirements of the AMTSO Testing Protocol Standard v.1.3 https://www.amtso.org/standards/. At the moment AMTSO is finalizing the compliance check. Once it is confirmed, the report will be updated with this information.

Details about the test compliance are available on page: https://www.amtso.org/tests/testing-ground-labs-ransomware-protection-test-may-2023/ .

© 2020-2023 Testing Ground Labs

Chap.6 Rights Statement

Unless otherwise stated, Testing Ground Labs (hereinafter referred to as "TG Labs"), owns the copyright of this report. Without prior written consent of TG Labs, no other unit or individual shall have the right to alter the contents of this report and use it for commercial purposes by any means (including but not limited to transmission, dissemination, reproduction, excerpt, etc.).

Unless otherwise stated, TG Labs shall be the rightful owner of the trademarks and service marks used in the report. Any action of infringing upon the legal rights of TG Labs is prohibited. TG Labs shall have the right to pursue the legal liability of the infringer in accordance with the law.

Chap.7 Disclaimer

Note that before using the report issued by Testing Ground Labs (hereinafter referred to as "TG Labs"), please carefully read and fully understand the terms and conditions of this disclaimer (hereinafter referred to as "Disclaimer"), including the clauses of exclusion or restriction of the liabilities of TG Labs and the limitations of the rights of users. If you have any objection to the terms and conditions of this Disclaimer, you have the right not to use this report, the act of using this report will be regarded as acceptance and the recognition of the terms and conditions of this Disclaimer, so by using this report, you agree to the following terms and conditions:

1. The report is provided by TG Labs, all the contents contained herein are for reference purposes only, and will not be regarded as the suggestion, invitation, or warranty for readers to choose, purchase or use the products mentioned herein. TG Labs will not guarantee the absolute accuracy and completeness of the contents of the report; you should not rely solely on this report, or substitute the viewpoints of the report for your independent judgment. If you have any queries, please consult the relevant departments of the State, and then choose, purchase or use products by your independent judgment.
2. The contents contained herein is the judgment made by TG Labs to the product characteristics as of the date the report was published. In the future, TG Labs will have the right to issue new reports which contain different contents or draw different conclusions, but TG Labs has no obligation or responsibility to update the original report or inform readers of the update of it. In this case, TG Labs will bear no responsibility for readers' loss for using the original report.

© 2020-2023 Testing Ground Labs

3. The report may contain links to other websites, which are provided solely for the readers' convenience. The contents of the linked websites are not any part of this report. Readers shall assume the risks and losses or bear the costs when visiting such websites. TG Labs will not guarantee the authenticity, completeness, accuracy, and legitimacy of the contents of such websites (including but not limited to advertising, products or other information). TG Labs does not accept any liability (direct or indirect) for readers' damages or losses arising from their clicking on or viewing such websites to obtain some information, products, or service.
4. TG Labs may have or will have a business relationship with the companies which produce the products mentioned in this report, but have no obligation to notify readers about it, it doesn't matter if there has already been, or there will be such business relationship in the future.
5. The act of readers' receiving this report is not regarded as the establishment of the business relationship between readers and TG Labs, so there is no customer relationship existing. TG Labs does not accept any legal liability as the readers' customer.
6. The products which are used to be tested as samples by TG Labs are bought through the official channels and legal means, so the report is proper for products bought through the same, not for products bought through unofficial channels and/or illegal means. Therefore, it's the users buying such products that will be responsible for any risk or loss arising there from. TG Labs will not have or accept any liability whatsoever for any such risk or loss.
7. Some trademarks, photos or patterns owned by units or individuals will probably be used in this report, if you think your legal right and interests are infringed, please contact TG Labs promptly, TG Labs will handle the matter as quickly as possible.

TG Labs reserves the rights to interpret, modify, and update the Disclaimer.

Attorney: Zhejiang CongDian Law Firm

© 2020-2023 Testing Ground Labs