© Chernihivskyi I., Kriuchkova L. Testing antivirus solutions for the corporate segment // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 3, pp. 407-413. ©

DOI: 10.18372/2225-5036.30.20362

ТЕСТУВАННЯ АНТИВІРУСНИХ РІШЕНЬ ДЛЯ КОРПОРАТИВНОГО СЕГМЕНТУ

Іван Чернігівський, Лариса Крючкова

Київський столичний університет імені Бориса Грінченка

ЧЕРНІГІВСЬКИЙ Іван Андрійович, аспірант
Рік та місце народження: 1998 рік, м. Київ, Україна
Освіта: Київський національний торговельно-економічний університет.
Посада: аспірант Київського столичного університету імені Бориса Грінченка
Наукові інтереси: захист інформації, кібербезпека, computer forensics, комп'ютерні мережі, інформаційно-комунікаційні системи.
Публікації: близько 10 наукових публікацій, серед яких наукові статті та тези, матеріали доповідей на конференціях.
E-mail: i.chernihivskiy@gmail.com
Orcid ID: 0009-0003-4568-3212.

КРЮЧКОВА Лариса Петрівна, доктор технічних наук, професор
Рік та місце народження: 1954 рік, м. Прилуки, Україна
Освіта: Одеський електротехнічний інститут зв'язку ім. О. С. Попова з відзнакою
Посада: професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.
Наукові інтереси: захист інформації, кібербезпека, електродинаміка інформаційних систем, електромагнітна сумісність, конфліктна взаємодія інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, підручники, патенти, матеріали доповідей на конференціях.
E-mail: l.kriuchkova@kubg.edu.ua
Orcid ID: 0000-0002-8509-6659.

Анотація. *Розробка ефективних методів виявлення комп'ютерних вірусів є актуальним завданням, значимість якого визначається сучасними тенденціями розвитку обміну даними в інформаційних системах та вимогами до їхньої захищеності. Кількість і складність вірусних атак на інформаційні системи підприємств постійно зростає, тому існує необхідність обирати антивірусне рішення в умовах недостатніх ресурсів або як базовий захист для кінцевих точок, або для заміни наявного рішення на більш досконале. Процес тестування антивірусних програм обумовлює необхідність застосування програм і тестів для оцінки ефективності захисних рішень. Мета публікації – визначення тестів і програм, яких буде достатньо для оцінки ефективності захисного рішення у корпоративному середовищі. Показано, що аналізу реакцій антивірусу на кілька шкідливих програм з сімейства Ransomware та на програми, що імітують їх поведінку, цілком достатньо, для отримання базового уявлення про евристичний модуль антивірусу та його можливість протидіяти новим загрозам. Визначено набір тестів і програм, достатній для оцінки ефективності захисного рішення. Запропоновано тест, здатний надати перше уявлення про антивірусне рішення, відкинувши необхідність подальшого тестування. Визначено критерії, за якими очікується спрацювання антивірусу на шкідливі програми сімейства Ransomware а також запропоновано скрипт, що імітує поведінку відомих Ransomware, для тестування евристичного модулю антивірусу. Зазначено, що проведення тестування у конкретному середовищі власними фахівцями надає можливість визначити слабкі сторони антивірусів та або закрити їх за участю вендора, або вибрати більш актуальне рішення, що дозволить підвищити загальний рівень кіберзахисту на підприємстві. Подальші дослідження можуть бути зосереджені на вдосконаленні методів вивантаження цифрових артефактів з урахуванням типових завдань для аналітика інформаційної безпеки в корпоративному середовищі.*

Ключові слова: *кібербезпека, комп'ютерні віруси, Ransomware, антивірусні рішення, NGAV, EDR, тестування, захист кінцевих точок, Windows*

Постановка проблеми

Оскільки потреби корпоративних користувачів значно вимогливіші на відміну від потреб звичайних користувачів, для вибору рішення не достатньо переглянути статті у інтернеті та порівняльні таблиці від компаній, що тестують антивіруси [1], а для оцінки ефективності рішення необхідно виконати його тестування у корпоративному середовищі на реальних ПК (Demo, POC). Також можлива ситуація, коли вендор стверджує, що «EDR захищає від загроз сімейства X, та може виявляти навіть невідомі загрози» (приклад: SentinelOne – забезпечує комплексний захист від відомих і невідомих загроз [2]). При тестах з відомим шкідливим програмним забезпеченням (ШПЗ) АВ їх дійсно видаляє, але якщо ШПЗ невідоме для АВ, або ШПЗ не використовує достатню кількість технік MITRE [3], які б активізували евристичний модуль АВ, воно буде пропущене і виконає всі закладені зловмисні дії. Це підводить нас до рішення, що

потрібно тестувати АВ самостійно у конкретному середовищі, не зважаючи на результати тестувань, отриманих сторонніми фахівцями, та запевнення маркетологів цих захисних рішень.

Аналіз останніх досліджень і публікацій

У працях науковців Svitlana M. Shevchenko, Pavlo M. Skladannyi, Maksym Martseniuk [4] робиться порівняння антивірусних рішень за наявністю тієї чи іншої функції (наприклад, наявність файерволу або батьківського контролю на додаток до основної функції – захисту від вірусів), проте не перевіряється якість реалізації цих модулів у різних вендорів. Науковці Barry Irwin, Jameel Haffejee [5] протестували сигнатурний модуль 49 антивірусів (використовуючи сервіс VirusTotal) та прийшли до висновку, що зловмисники можуть відносно легко обходити сигнатурний антивірусний захист, тому антивіруси не дуже ефективні для ще невідомих загроз. І так як всі вендори пропонують майже той самий набір функцій із тими ж самими пропозиціями (наприклад: «антивірус Х захистить ваш ПК від вірусів»), потрібен певний набір тестів (однаковий для кожного вендора), щоб можна було порівняти саме якість захисту кінцевих точок у реальних умовах.

Так як зазвичай при підготовці до вірусної кампанії вірусний файл доводять до статуса Fully Undetectable (FUD), то вибір рішення яке базується на сигнатурному аналізі з недорозвиненим евристичним модулем, є некоректним.

Існують спеціальні програми для тестування антивірусу, які лише імітують шкідливі дії, але не виконують їх, наприклад, програма RanSim імітує поведінку Ransomware за 24 критеріями [6], проте їх використання має ряд недоліків:

1. Антивіруси нерідко видаляють зазначені програми сигнатурними методами [7], що призводить до неможливості протестувати евристичний модуль АВ.
2. Використання зазначених програм потребує даних про компанію та корпоративну електронну пошту, на яку будуть надсилатись маркетингові повідомлення.

Процес тестування антивірусних програм обумовлює необхідність застосування програм і тестів для оцінки ефективності захисних рішень. При цьому має бути визначено тест, здатний надати перше уявлення про антивірусне рішення та відкине необхідність подальшого тестування (у вивільнений час можна більш детально протестувати інше рішення, яке має більш досконалі поведінкові та евристичні аналізатори).

Мета та постановка завдання

Метою дослідження є визначення тестів і програм, яких буде достатньо для оцінки ефективності захисного рішення у корпоративному середовищі.

Виклад основного матеріалу дослідження

Як основне рішення ешелонованого захисту в корпоративному середовищі для кінцевих точок досі залишається антивірус (Endpoint Protection). Антивірусні модулі обов'язково є в рішеннях класу Endpoint Detection and Response (EDR) & Next Generation Anti-Virus (NGAV). Разом з тим, для кожної компанії настає час, коли потрібно вибирати вендора (надавача антивірусного рішення) та інтегратора (локальна компанія, яка надає послуги з впровадження і підтримки конкретного антивірусного рішення та активно комунікує з вендором). З одного боку, достатньо вибрати топ-5 рішень з найкращими показниками від компанії, яка спеціалізується на тестуванні антивірусів (АВ) та провести тендер на найдешевшу ціну від інтегратора. Проте рішення, яке цілком підійшло б для звичайного користувача і яке має найвищі оцінки за показниками сигнатурного аналізу, може не дати ефективного результату для компанії, оскільки евристичний модуль (виявлення загроз на основі поведінки програми) недостатній для корпоративних загроз (наприклад: не моніторить дії системних файлів, та виконуваних файлів з актуальним цифровим підписом, не аналізує потенційно шкідливі аргументи програм), а також для кожної компанії можуть бути свої кейси і своє бачення, які дії повинен виконувати антивірус. Так, при цільових атаках від Advanced Persistent Threat (APT) зазвичай використовується легальне програмне забезпечення і зловмисна активність маскується під «користувацьку» або «адміністраторську». Все ще можна зустріти віруси, які автономно заражають флеш-накопичувачі, а антивіруси видаляють тільки вірусний файл та autorun.inf і не відновлюють файли користувача.

Зважаючи на те, що антивірусних рішень у світі дуже багато і фахівці не можуть перевірити їх усі, необхідно визначити вимоги до антивірусних рішень, щоб відсіяти неефективні АВ.

Вимоги які ставляться до антивірусних рішень:

1. Здатність знаходити та знешкоджувати відомі і невідомі загрози різного типу\сімейств, як при скануванні системи, так і при відкритті ШПЗ (для цього тесту потрібні ШПЗ різних сімейств і типів). Вибирається той АВ, який знешкодив більше всього загроз.
2. Здатність знаходити нешкідливі загрози PUA (Potentially Unwanted Program). Наприклад, торенти або легальні програми для адміністрування ПК.
3. Мати евристичний модуль (для його тесту потрібні ШПЗ, які АВ не знаходить сигнатурно, наприклад, накриті протекторами). Вибираємо той АВ, який знешкодив більше всього реальних загроз.

4. Мати модуль Anti-Ransomware (для цього потрібні ШПЗ типу Ransomware як відомі так і невідомі).
5. Виявляти загрози за поведінкою (наприклад, при використанні легітимних інструментів Anydesk\PsExec для зловмисних дій), або виявляти і блокувати шкідливі дії (наприклад, дамп куща реєстру SAM або дамп даних пам'яті процесу lsass.exe).
6. Мати досконалий самозахист (немає можливості вимкнути антивірус навіть якщо ШПЗ\користувач має права адміністратора на ПК або ця можливість складна у реалізації).

В процесі вибору антивірусних рішень доцільно користуватися інформацією щодо лідерів ринку за версією Gartner [8]. Магічний квадрант для рішень захисту кінцевих точок подано на Рис. 1.

Рис. 1. Магічний квадрант для рішень захисту кінцевих точок, Gartner 2024
Джерело: агреговано на основі [8]

Для тестування АВ доцільно відібрати вірусні файли різного типу та різні легітимні програми, що можуть бути використаними для зловживань як користувачами-адміністраторами, так і ШПЗ\APT. Пропонується вибрати наступне:

Програми, що зламують захист ліцензій ОС

Crack
- KMSAuto Net
- KMS Tools Portable
- AACT
- w10digitalactivation

Програми, що перехоплюють та реєструють натискання клавіш

Keylogger
- FreeKeylogger
- LightLogger
- Mipko Personal Monitor
- Radium

Програми, що експлуатують вразливості системи

Exploit
- EternalBlue
- DoublePulsar
- Stuxnet
- Folina (безтілесний)

Інші програми, виконання яких може бути підозрілим для АВ

Other
- AdvancedRun (для запуску від імені інших користувачів)
- Legal RAT:
  - AmmyAdmin,
  - Radmin,
  - TeamViewer,
  - AnyDesk,
  - RMS,
  - RUT.
- NirSoft: Networktools, Passrec (інструменти для відновлення «забутого» паролю користувача)
- ProcessHacker (для вимкнення або «заморозки» окремих процесів, наприклад процесів АВ)
- RemCom
- Tor Browser (компоненти іноді використовується для звязку ШПЗ з С2С сервером, потрібен для тестування реакції АВ на створення додаткових тунелів у мережі)
- RootkitReleaver (широко використовувався ретровірусами для вимкнення АВ)

Програми, що використовуються у тестуванні на проникнення

Pentest
- Advanced IP Scanner
- Nmap
- Hydra-Windows
- CobaltStrike
- Impacket
- MetasploitFramework
- Magnet RAM Capture
- Belkasoft RAM Capturer
- Penetration Testing POC

Програми, що захищають інші програми від реверс-інжинірингу.

- Sysinternals:
  - ProcessExplorer (для вимкнення або «заморозки» окремих процесів, наприклад процесів АВ),
  - PsExec (для підвищення привілеїв до SYSTEM та виконання команд на віддалених ПК),
  - Sdelete (для невідворотного видалення файлів),
  - ShellRunAS (для запуску від імені інших користувачів),
  - PsKill (для завершення процесів),
  - Procdump (для дампу памяті процесів),
  - ADRestore (перегляд видалених об'єктів AD),
  - ADExplorer (перегляд AD).

Ці програми потрібні для тестування реакції АВ як на самі протектори, так і на ШПЗ, що накриті протекторами. Наприклад, для тесту буде достатньо ШПЗ Mimikatz & WannaCry. Якщо в результаті, будь-який з них при виконанні зможе реалізувати усі свої можливості, отримуємо висновок, що АВ не захищає ПК якісно.

Protectors
- Themida
- UPX
- VMProtect
- Enigma

Програми, що не завжди є вірусами, але є потенційно небажані для користувача

PUA
- PUA.Softonic (themida)
- PUP.Optional.DriverPack

Програми, що дозволяють отримати паролі та геши LM\NTLM\Kerberos паролів Windows

Password dump
- Mimikatz
- LaZagne
- NTDS dump
- Process lsass.exe dump (by procdump.exe)
- Registry hive SAM & SECURITY & SYSTEM dump
- Shadow copy of SAM & SECURITY & SYSTEM files

Програми, що дозволяють отримати паролі користувачів у відкритому вигляді з різних систем (браузери, буфер обміну, дані для входу в інші програми)

Stealer
- LummaStealer
- RacoonStealer

Програми, що шифрують файли користувача (іноді з подальшою ексфільтрацією даних) та вимагають гроші за відновлення файлів

Ransomware
- WannaCry
- Petya
- NotPetya
- REvil
- Ryuk
- VaultCrypt
- TeslaCrypt

Програми, що надають зловмисникам віддалений доступ до зараженого комп'ютера

RAT
- RDPWrap
- Dark Comet RAT
- Emotet
- njRAT
- PS RDP Backdoor
- QTBot
- QuazarRAT
- Silent RMS
- Silent TeamViewer

Програми, що можуть використовуватись корпоративними користувачами для ексфільтрації даних. Будуть корисними, якщо у АВ є DLP модуль та функціонал видання алерту на специфічні програми або специфічні аргументи до них.

Social
- Telegram Desktop
- Viber Desktop
- Google Drive Desktop
- OneDrive Desktop
- Dropbox Desktop
- MEGA (GUI\CLI)

Програми, що тільки імітують шкідливу поведінку, а самі безпечні і контрольовані.

Такі програми потрібні для тестування специфічних сценаріїв та аналізу спрацювань евристичного модулю АВ. Наприклад:

- RanSim, AESCrypt, PSRansom потрібні для тестування модулю Anti-Ransomware, якщо він видалив відомі загрози Ransomware;
- LNK Worm для тестування старого, але все ще актуального методу розповсюдження ШПЗ через флеш-накопичувачі у закритій

мережі. Деякі антивіруси реагують на пустий autorun.inf, але цю загрозу вони не виявляють; в разі виявлення загрози – видаляють вірусний файл і не відновлюють «пошкоджені» користувацькі файли;

- Anti-Keylogger Tester (AKLT) для тестування можливості АВ виявити виклики потенційно шкідливих функцій, які використовують ШПЗ сімейства Keylogger.

Test-virus
- LNK Worm
- AESCrypt
- PSRansom
- RanSim
- AKLT
- Eicar.com

Програми, що можуть використовуватись користувачами для незаконного завантаження фільмів та зламаних програм

Torrent
- Bittorent (Desktop\Web)
- uTorrent
- Mediaget

Інші ШПЗ.

Virus-in-the-wild – усі віруси, якими корпоративні ПК раніше заражалися; VirusPack – архів з великою кількістю вірусних файлів (завантажується все, що знайдено в мережі за поточний та попередній рік, чим більше тим краще, файли можуть важити десятки гігабайт).

Тестування, документування та написання звіту за всіма критеріями з тестуванням усіх програм може затягнутися на тиждень, або навіть і більше. Це можливо виправити, якщо для оцінки продуктів ЕДР з антивірусним модулем (NGAV) тестувати лише один найбільш необхідний критерій – евристичний модуль для найбільш руйнівного класу загроз (Ransomware), які ще невідомі антивірусу. Для цього буде достатньо 1-2 робочих днів і вже буде відомо, чи підходить це рішення, чи ні (якщо загрози пропущені і вендор не може це виправити додатковими політиками, або вендор не вважає це за загрозу бо «націлений тільки на запобігання реальним атакам» – таке рішення не підходить), що дасть економію часу у майже 3-5 робочих днів та дає 80% загального уявлення про рішення.

Для тестування евристичного модулю наявного антивірусу обрано основне сімейство загроз (Ransomware) та критерії, за якими очікується виявлення ШПЗ антивірусними рішеннями. Критерії типової поведінки Ransomware обрано на прикладах: Petya\NotPetya, Ryuk [9,10], REvil [11,12], Wannacry [13], Vault:

1. Наявність пошуку файлів в кореневому каталозі C:\ та пошук файлів на інших дисках (D:\ F:\ тощо).

2. Вибір файлів із певним розширенням (наприклад: файли документів .doc, .docx, .xls, .xlsx та інші) [13].

3. Шифрування файлів за допомогою симетричного алгоритму (усі програми-вимагачі роблять це для більшої швидкості).

4. Шифрування кожного файлу один за одним, у всіх підкаталогах.

5. Модифікація (шифрування) прихованих файлів-приманок. Файли-приманки – спеціальні приховані файли, що створюються захисним ПЗ у каталогах користувача для виявлення активності Ransomware. Це виключає дії користувачів, які "просто хочуть зашифрувати папку".

6. Видалення вихідного файлу та залишення лише зашифрованої версії.

7. Додавання до зашифрованих файлів такого специфічного розширення, яке не збігається з розширенням легального програмного забезпечення (наприклад, .aes, .gpg). Це може бути розширення .encrypted, .vault, .enc, .wncry, .ryk та інші.

8. Використання встановлених або портативних версій легального програмного забезпечення для шифрування з правами адміністратора або без них.

9. Зміна шпалер на робочому столі та додавання записки з викупом (зазвичай у форматі .txt \ .html) у всіх підкаталогах або тільки на робочому столі користувачів.

10. Видалення тіньових копій\точок відновлення\резервних копій, або застосування утиліт для безпечного видалення файлу до кожного файлу, який був зашифрований, або затирання вільного місця на диску.

11. Перевірка розкладки клавіатури на ПК і коригування своїх дій в залежності від цього (наприклад, припинити виконання шкідливих дій та затерти сліди).

Індикатори компрометації (IOC) для Ransomware (тестовий файл має відповідати одному або кільком критеріям, що потрібно для подальшої предметної комунікації з вендором):

• ShadowCopyDeletion;
• EFSRansomware;
• RansomwareMarker;
• PossibleRansomNoteCreation (Revil note + BTC address);
• KnownRansomwareFiles (known extensions and name of ransom notes);
• RansomwareDecoyTamper;
• T1490 Inhibit System Recovery [14];
• T1059 Command and Scripting Interpreter [15];
• T1486 Data Encrypted for Impact [16];

• T1547 Boot or Logon Autostart Execution [17];

• T1614.001 System Location Discovery: System Language Discovery (used by Cuba, REvil, Ryuk) [18].

За сукупністю критеріїв (4 і більше), однозначно можливо ідентифікувати процес як шкідливий, що відноситься до класу Ransomware, при цьому, якщо АВ видаляє файл одразу, як він з'являється на комп'ютері, або відразу при відкритті – це означає, що файл було видалено сигнатурним методом і необхідно шукати інший файл, на який не буде спрацювань АВ при відкритті.

Для перевірки, як евристичний модуль антивірусу справляється з сімейством Ransomware, можна або накрити протекторами відомі Ransomware та запустити їх на окремому ізольованому ПК (проте є шанс що АВ буде сигнатурно детектувати наявність протектора та блокувати файл), або використовувати самописний код.

Запропоновано скрипт рішення задачі імітування Ransomware для тестування евристичного модулю АВ, фрагменти якого подано на рис. 2 і рис. 3.

```
cAFIAeQB1AGsAUgBlAGEAZABNAGUALgB0AHgAdAA=
REM RansomwareMarker\KnownRansomwareFiles
echo password>> %userprofile%\Desktop\password.txt
fsutil file createnew C:\Windows\perfc.dat 362360
for /r "C:\" %%i in (*.xls *.xlsx *.doc *.docx *.rtf) do (
"%Temp%\Windows\aescrypt.exe" -e -p password "%%i"
move /y "%%i.aes" "%%i" && rename "%%i" "%%~nxi.wncry"
echo %%~dpnxi.wncry>> "%Temp%\Windows\cryptlist.txt"
echo %%i>> "%Temp%\Windows\plainlist.txt"
)
powershell.exe -ExecutionPolicy ByPass -EncodedCommand
WwBTAHkAcwB0AGUAbOAuAFOAZOB4AHOALgBFAG4
```

Рис. 2. Фрагмент коду скрипта, який відповідає за тестування виявлення та знешкодження антивірусом маркерів відомих Ransomware.

```
REM ShadowCopyDeletion T1490
vssadmin.exe delete shadows /all /quiet
wmic.exe shadowcopy delete
wbadmin.exe delete catalog -quiet
cipher /w:C:
```

Рис. 3. Фрагмент коду скрипта, який відповідає за тестування виявлення та блокування антивірусом видалення резервних (тіньових) копій та затирання вільного місця на диску.

Якщо після відкриття файлу, який АВ не виявляє сигнатурно, з'явилися зашифровані файли з запискою на робочому столі про необхідність сплатити гроші – це означає, що не спрацював евристичний модуль антивірусу (додатково, у деяких антивірусів є захист Anti-Ransomware). Це можна виправити, попросивши вендора\інтегратора увімкнути більш жорсткіші політики Anti-Ransomware. Якщо і після цього АВ не буде виявляти та блокувати шкідливий процес, що призведе до шифрування файлів, приходимо до висновку, що наявне захисне рішення не здатне самостійно справитися з актуальними загрозами і новими вірусами, які з'являються сотнями тисяч кожного дня [19]. Це у свою чергу означає, що атака на корпоративні ПК ШПЗ типу Ransomware з високою імовірністю призведе до зараження (FUD не буде детектуватись сигнатурами і залишиться лише поведінка, яку досліджуване захисне рішення не може виявити через неефективний евристичний модуль) і неможливості відновити файли. Слід враховувати ці ризики при виборі захисного рішення.

Висновки. Зазначений набір тестів і програм є достатнім для оцінки ефективності захисного рішення у корпоративному середовищі.

Оскільки задача АВ – видалення невідомих ШПЗ (особливо сімейства Ransomware), то аналізу реакцій АВ на кілька ШПЗ з сімейства Ransomware та на програми, що імітують їх поведінку, цілком достатньо для отримання базового уявлення про евристичний модуль АВ та його можливість протидіяти новим загрозам. Це дозволяє не витрачати час на подальше тестування неефективного рішення, а здійснити детальне тестування рішень з більш досконалими поведінковими та евристичними аналізаторами.

Визначено критерії, за якими очікується спрацювання АВ на ШПЗ сімейства Ransomware, а також запропоновано скрипт, що імітує поведінку відомих Ransomware для тестування евристичного модулю АВ.

Проведення тестування у конкретному середовищі власними фахівцями надає можливість визначити слабкі сторони АВ, та або закрити їх з вендором, або вибрати більш актуальне рішення, що дозволить підвищити загальний рівень кіберзахисту на підприємстві.

Подальші дослідження можуть бути зосереджені на вдосконаленні методів вивантаження цифрових артефактів з урахуванням типових завдань для аналітика інформаційної безпеки в корпоративному середовищі.

Список літератури

[1]. Test antivirus software for Windows 10 - December 2024. AV-TEST URL: https://www.av-test.org/en/antivirus/business-windows-client/

[2]. What is Malware Detection? Importance & Techniques. SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-malware-detection/

[3]. MITRE ATT&CK®. MITRE ATT&CK®. URL: https://attack.mitre.org/

[4]. Shevchenko S., Skladannyi P., Martseniuk M. Analysis and research of the characteristics of standardized in ukraine antivirus software. Cybersecurity: Education Science Technique. 2019. No. 4. P. 62–71. URL: https://doi.org/10.28925/2663-4023.2019.4.6271

[5]. Haffejee J., Irwin B. Testing antivirus engines to determine their effectiveness as a security layer. URL: https://ieeexplore.ieee.org/document/6950496

[6]. RanSim | KnowBe4. Beyond Security Awareness Training | KnowBe4 Human Risk Mgmt Platform. URL: https://www.knowbe4.com/free-cybersecurity-tools/ransim

[7]. VirusTotal KnowRanSim Detection. URL: https://www.virustotal.com/gui/file/815b99bd82f3685f97f9a2dd24a434c1749d5a5c9097f2b6bcea42f69ae02a05/detection

[8]. CrowdStrike named a Leader. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/resources/reports/gartner-mq/

[9]. RYUK Ransomware. Trend Micro. URL: https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html

[10]. What is Ryuk ransomware? A detailed breakdown. SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/ryuk-ransomware/

[11]. REvil / Sodinokibi: The Crown Prince of Ransomware. Cybereason - AI-Driven XDR Platform, URL: https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack

[12]. The REvil is in the details. URL: https://whitehat.eu/the-revil-is-in-the-details/

[13]. A list of file extensions searched and encrypted by the WannaCry ransomware. Gist. URL: https://gist.github.com/xpn/facb5692980c14df272b16a4ee6a29d5

[14]. Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/T1490/

[15]. Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/T1059/

[16]. Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/T1486/

[17]. Boot or Logon Autostart Execution, Technique T1547 - Enterprise | MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/T1547/

[18]. System Location Discovery: System Language Discovery, Sub-technique T1614.001 MITRE ATT&CK®. URL: https://attack.mitre.org/techniques/T1614/001/

[19]. Husain O. Husain O. 100 chilling malware statistics & trends (2023–2025). Control D Blog. URL: https://controld.com/blog/malware-statistics-trends/#:~:text=As%20of%20mid-2023,%20security,incidents%20so%20far%20in%202023

УДК 004.056.57

Chernihivskyi I., Kriuchkova L. Testing antivirus solutions for the corporate segment.

Abstract. *The development of effective methods for detecting computer viruses is an urgent task, the importance of which is determined by modern trends in the development of data exchange in information systems and the requirements for their security. The number and complexity of virus attacks on enterprise information systems is constantly growing, so there is a need to choose an antivirus solution in conditions of insufficient resources either as basic protection for endpoints, or to replace the existing solution with a more advanced one. The process of testing antivirus programs necessitates the use of programs and tests to assess the effectiveness of protective solutions. The purpose of the publication is to determine the tests and programs that will be sufficient to assess the effectiveness of a protective solution in a corporate environment. It is shown that the analysis of the antivirus's reactions to several malicious programs from the Ransomware family and to programs that imitate their behaviour is quite sufficient to obtain a basic idea of the antivirus's heuristic module and its ability to counteract new threats. A set of tests and programs sufficient to assess the effectiveness of a protective solution has been determined. A test has been proposed that can provide a first idea of the antivirus solution, eliminating the need for further testing. The criteria by which the antivirus is expected to work on malicious programs of the Ransomware family have been determined, and a script that simulates the behaviour of known Ransomware has been proposed for testing the heuristic module of the antivirus. It is noted that testing in a specific environment by our own specialists provides an opportunity to identify the weaknesses of antiviruses and either close them with the participation of the vendor, or choose a more relevant solution, which will increase the overall level of cyber protection at the enterprise. Further research can be focused on improving methods for extracting digital artifacts, taking into account typical tasks for an information security analyst in a corporate environment.*

Keywords: *cybersecurity, computer viruses, Ransomware, antivirus solutions, NGAV, EDR, testing, endpoint protection, Windows*

Чернігівський Іван Андрійович, аспірант Київського столичного університету імені Бориса Грінченка.

Chernihivskyi Ivan, graduate student, Borys Grinchenko Kyiv Metropolitan University.

Крючкова Лариса Петрівна, доктор технічних наук, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.

Kriuchkova Larysa, D. Sc. (Engineering), Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.