УДК 004.056

И.А. Огнев, И.В. Никрошкин, М.А. Медведев, А.Д. Красников

Исследование встроенных средств защиты информации Unix-систем на примере заражения вредоносным программным обеспечением

Приводится сравнительный анализ встроенных средств защиты информации операционных систем семейства Unix на примере заражения операционной системы вредоносным программным обеспечением. В рамках исследования были задействованы операционные системы с открытым исходным кодом – Debian и отечественные операционные системы – Alt Linux, RedOS, Astra Linux Special Edition. В качестве вредоносного программного обеспечения был использован вирус-шифровальщик (ransomware). Представленные результаты демонстрируют наибольшую способность операционной системы Astra Linux противостоять заражению вредоносным программным обеспечением.

Ключевые слова: информационная безопасность, защита информации, вредоносное программное обеспечение, вирус-шифровальщик, операционная система, средство защиты информации.
DOI: 10.21293/1818-0442-2023-26-4-29-34

Разнообразие вредоносных программ, которые широко используются, уменьшает эффективность текущих систем безопасности, что приводит к заражению миллионов устройств различными видами вредоносного ПО, такими как черви, вымогатели, бэкдоры, компьютерные вирусы и троянские программы [1–3]. Программы-вымогатели, также известные как шифровальщики, представляют собой тип атаки, при которой злоумышленники используют различные тактики и приемы для блокировки или шифрования данных жертвы [4–8]. Эта атака обычно заканчивается ультиматумом: жертва должна заплатить за разблокировку или дешифрование, иначе все ее данные будут потеряны. Хотя крипто-вымогатели являются наиболее распространенным типом атаки, программы-вымогатели блокировок все еще актуальны [9, 10], особенно на мобильных платформах [11].

Вредоносное программное обеспечение существует с начала 1970-х гг., когда вирус Creeper впервые появился в ARPANET. За ним последовали Elk Cloner и the Brain в 1980-х гг., причем последний стал первым компьютерным вирусом в дикой природе. Это ознаменовало эпоху, когда даже машины подвержены болезням [12, 13]. Антивирусные программы также появились в начале 1970-х гг., начиная с Reaper, который был разработан для борьбы с Creeper. С тех пор появилось множество вирусов и антивирусных программ, которые борются друг с другом. В цифровую эпоху безопасность компьютеров конечных пользователей в значительной степени зависит от эффективных антивирусных сканеров, что делает антивирусные программы незаменимыми [14].

Согласно отчетам, программы-шифровальщики представляют серьезную угрозу бизнес-процессам организаций. Из отчета Fortinet [15] следует, что:

1. Из 569 опрошенных организаций, реализовавших комплекс мер по борьбе с ВПО, половина пострадала от заражения программами-шифровальщиками.

2. Из организаций, столкнувшихся с инцидентом с программами-вымогателями, 71% заявили, что заплатили хотя бы часть требуемого выкупа.

3. 35% пострадавших от программ-вымогателей восстановили все свои данные после инцидента.

4. Стремительное развитие киберпреступного мира, в частности, бизнес-схемы злоумышленников Ransomware-as-a-Service (часть схемы Malware-as-a-Service), приводит к появлению новых и более изощренных экземпляров ВПО.

Согласно отчету Check Point [16], современные тренды в технологиях, используемых в разработке и доставке ВПО, с одной стороны, используют новейшие наработки в сфере искусственного интеллекта, с другой стороны, возвращаются к классическим методам доставки и распространению ВПО через USB-носители. Команда Check Point Research указывает на заметный всплеск кибератак по всему миру. Только во втором квартале года еженедельные кибератаки выросли на 8%, что стало самым значительным всплеском за последние два года.

Согласно аналитическому отчету Kaspersky [17], в 2022 г. шифровальщики были одной из самых опасных угроз информационной безопасности в мире. Новые варианты, обходящие существующие меры безопасности, появляются регулярно. При этом в отчете показано, что для противодействия ВПО необходимо использовать комплексный подход, состоящий из применения специализированных средств защиты информации для детектирования и удаления ВПО и из реализации мер по разграничению доступа и настройке активов с учетом требований по безопасности для снижения потерь при компрометации активов.

Согласно отчету Positive Technologies [18], активность программ-вымогателей значительно возросла в 1-м квартале 2023 г.: доля программ-вымогателей в атаках вредоносных программ на организации составила 53%, что на 9% больше, чем в предыдущем квартале, а количество инцидентов увеличи-

лось на 77% по сравнению с 1-м кварталом 2022 г. Основные мотивы злоумышленников – кража конфиденциальной информации и нарушения или остановка основной деятельности организаций.

Тем не менее ряд организаций не реализует эффективные методы защиты от киберугроз или использует реализованные методы неэффективно [19–23].

Постановка задачи

Для противодействия ВПО, включая программы-шифровальщики, применяются 2 типа методов:

1) применение антивирусных программ, призванных детектировать и удалять ВПО до того, как оно будет выполнено и будет нанесен ущерб. Данный метод постоянно развивается и совершенствуется [24–29];

2) применение политик разграничения доступа и настроек технических средств с учетом требований по безопасности с целью минимизации ущерба от реализованных программ-шифровальщиков [17].

Целью данного исследования является оценка эффективности встроенных средств защиты информации операционных систем семейства Unix, реализующих политики разграничения доступа в системе. Учитывая факт наличия санкций со стороны заграничных коммерческих организаций, реализующих операционные системы, а также политику импортозамещения в Российской Федерации, при которой субъекты КИИ обязаны перейти на отечественные операционные системы, которые, в свою очередь, принадлежат семейству Unix, исследование эффективности встроенных средств защиты информации противодействию ВПО представляет наибольший интерес в рассматриваемом случае.

При таком подходе рассмотрим встроенные средства и методы защиты информации операционных систем и оценим их эффективность по следующим параметрам:

– скорость заражения файловой системы ОС;

– процент заражения файловой системы ОС;

– сохранение работоспособности ОС.

Описание объекта исследования

Объект исследования – механизмы разграничения доступа операционных систем (ОС) семейства Unix:

– Debian.

– Alt Linux.

– RedOS.

– Astra Linux Special Edition.

При этом под доступом в данной работе понимается наличие прав на изменение объектов системы.

Механизмы разграничения доступа, применяемые в рассматриваемых ОС, можно разделить на 2 категории:

– механизм дискреционного разграничения доступа. Данный механизм работает по принципу точечного назначения прав доступа субъектов системы к объектам – пользователь имеет доступ к объекту, если он является суперпользователем или владельцем объекта, входит в группу пользователей, которым разрешен доступ к объекту, доступ к объекту разрешен всем пользователям системы:

$$R_{\text{d}} = \begin{cases} 1, P \Leftrightarrow P_{\text{s}} \cup P \Leftrightarrow P_{\text{o}} \cup P \Leftrightarrow P_{\text{g}} \cup P \Leftrightarrow P_{\text{ot}}, \\ 0, \end{cases} \quad (1)$$

где R_{d} – дискреционные права доступа субъекта системы; P – пользователь системы, P_{s} – суперпользователь системы, P_{o} – владелец объекта системы, P_g – группа пользователей системы, P_{ot} – остальные пользователи системы;

– механизм мандатного разграничения доступа. Данный принцип работает по принципу разделения объектов и субъектов системы на разные группы иерархически или неиерархически.

Иерархический принцип подразумевает назначение специальных меток в числовом виде (мандатных меток), и доступ назначается на основании результата сравнения меток.

$$R_{\text{mh}} = \begin{cases} 1, M_{\text{s}} \geq M_{\text{o}}, \\ 0, M_{\text{s}} < M_{\text{o}}, \end{cases} \quad (2)$$

где M_{s} – мандатная метка субъекта системы (пользователя), M_{o} – мандатная метка объекта системы, R_{mh} – иерархические мандатные права доступа субъекта системы. При $R_{\text{mh}} = 0$ пользователь не имеет доступа к объекту системы, а при $R_{\text{mh}} = 1$ – имеет.

Неиерархический метод подразумевает разделение субъектов и объектов системы на специальные категории (мандатные категории). Субъекты имеют доступ к объектам только в рамках одной категории:

$$R_{\text{mnh}} = \begin{cases} 1, K_{\text{s}} \Leftrightarrow K_{\text{o}}, \\ 0, \end{cases} \quad (3)$$

где K_s – мандатная категория субъекта системы, K_o – мандатная категория объекта системы, R_{mnh} – неиерархические мандатные права доступа субъекта системы. При $R_{\text{mnh}} = 0$ пользователь не имеет доступа к объекту системы, а при $R_{\text{mnh}} = 1$ – имеет.

Постановка эксперимента

Метод исследования – наблюдение за распространением программы-шифровальщика по файловой системе ОС (ФС).

Особенности постановки эксперимента:

– программа-шифровальщик не содержит опциональный функционал, направленный на повышение привилегий или закрепление в системе;

– все ОС устанавливались на одинаковые аппаратные составляющие, поэтому далее не будет учитываться зависимость скорости шифрования от аппаратных особенностей ПК.

Исследуемые параметры:

1) скорость заражения файловой системы ОС – $U_{\text{шиф}}$:

$$U_{\text{шиф}} = \frac{V_{\text{шиф}}}{t_{\text{шиф}}}, \quad (4)$$

где $V_{\text{шиф}}$ – объем зашифрованных данных в Мбайт, $t_{\text{шиф}}$ – время, потраченное на шифрование данных в секундах;

2) процент заражения файловой системы ОС – $V_{\text{зар}}$:

$$V_{\text{зар}} = \frac{V_{\text{шиф}}}{V_{\text{общ}}} \times 100\%, \qquad (5)$$

где $V_{\text{шиф}}$ – объем зашифрованных данных в Мбайт, $V_{\text{общ}}$ – общий объем данных в Мбайт. При этом $V_{\text{шиф}} \subseteq V_{\text{общ}}$, а $V_{\text{общ}} \supseteq (F_{\text{крит}} \cup F_{\text{ч.крит}} \cup F_{\text{псев}})$, где $F_{\text{крит}}$ – множество разделов файловой системы ОС, критичных для работоспособности системы (разделы /bin, /sbin, /boot, /lib, /lib64, /etc), $F_{\text{ч.крит}}$ – множество разделов файловой системы ОС, шифрование которых приведет к незначительным нарушениям работоспособности системы или не приведет к нарушению работоспособности системы (/tmp, /home, /media, /mnt, /opt, /root, /srv), $F_{\text{псев}}$ – множество разделов файловой системы ОС, которые являются псевдофайловыми системами (/proc, /run, /sys, /dev);

– сохранение работоспособности ОС – K:

$$K = \begin{cases} 2, \ F_{\text{крит}} \subseteq V_{\text{шиф}}, \\ 1, \ (F_{\text{крит}} \not\subseteq V_{\text{шиф}}) \wedge (F_{\text{ч.крит}} \subseteq V_{\text{шиф}}), \\ 0, \ (F_{\text{крит}} \cup F_{\text{ч.крит}}) \not\subseteq V_{\text{шиф}}. \end{cases} \qquad (6)$$

Физический смысл данной формулы заключается в следующем: при значении, равном 0, целевая система полностью сохраняет работоспособность, при K, равном 1, система сохраняет работоспособность частично (часть прикладного программного обеспечения выходит из строя), а при K, равным 2, целевая система полностью теряет работоспособность.

Результаты

Рассмотрим два случая.

Случай 1. Программа-шифровальщик направлена на получение выкупа от пользователя (цель программы-шифровальщика – захватить пользовательские файлы, оставив систему работоспособной).

Случай 2. Программа-шифровальщик направлена на реализацию деструктивного воздействия на систему (цель программы-шифровальщика – нарушить или прекратить нормальное функционирование системы).

В случае 1 целью программы-шифровальщика будет являться каталог /home, который входит в множество $F_{\text{ч.крит}}$. В табл. 1 показаны результаты наблюдений над работой программы-шифровальщика в условиях функционирования ОС без встроенных средств защиты информации.

Таблица 1

Работа программы-шифровальщика без встроенных СЗИ с шифрованием пользовательских каталогов

ОС	Наличие прав суперпользователя	Скорость шифрования, Мбит/с	Процент поражения ФС, %	Сохранение работоспособности ФС
Debian	Нет	3,77	0,72	0
	Есть	31,52	17,26	1
RedOS	Нет	12,31	0,03	0
	Есть	41,96	2,66	1
Astra Linux	Нет	2,20	0,24	1
	Есть	66,77	24,16	1
Alt Linux	Нет	0,76	0,0044	0
	Есть	72,36	2,12	1

Из табл. 1 виден закономерный результат, что наличие прав суперпользователя при исполнении программы-шифровальщика приводит к более серьезным последствиям для системы – шифрование большего количества каталогов и нарушение работоспособности прикладного ПО. При этом во всех случаях цель программы-шифровальщика достигнута. Различия среди показателей скорости шифрования и процента поражения файловой системы обусловлены различным комплектом поставки ОС.

Далее рассмотрим работу программы-шифровальщика в таких же условиях, но при включенных встроенных средствах защиты (табл. 2).

Таблица 2

Работа программы-шифровальщика со встроенными СЗИ с шифрованием пользовательских каталогов

ОС	Наличие прав суперпользователя	Скорость шифрования, Мбит/с	Процент поражения ФС, %	Сохранение работоспособности ФС
Debian	Нет	3,77	0,72	0
	Есть	31,52	17,26	1
RedOS	Нет	11,58	0,03	0
	Есть	42,18	2,48	1
Astra Linux	Нет	0,06	0,007	0
	Есть	13,12	1,57	0
Alt Linux	Нет	0,76	0,0044	0
	Есть	72,36	2,12	1

Результат похож на предыдущий – цель программы-шифровальщика достигнута, однако в данном случае Astra Linux показал полное сохранение работоспособности прикладного ПО в любых условиях, что демонстрирует ограничение суперпользователя в правах.

Далее рассмотрим случай 2 в условиях функционирования ОС без встроенных средств защиты (табл. 3) и со встроенными средствами защиты (табл. 4).

Полученные данные также показывают критичность захвата учетной записи суперпользователя, а также демонстрируют способность ОС Astra Linux сохранять работоспособность системы даже при компрометации учетной записи суперпользователя.

Таблица 3

Работа программы-шифровальщика без встроенных СЗИ с шифрованием всех каталогов

ОС	Наличие прав суперпользователя	Скорость шифрования, Мбит/с	Процент поражения ФС, %	Сохранение работоспособности ФС
Debian	Нет	3,41	0,73	0
	Есть	31,22	18,31	2
RedOS	Нет	1,64	0,03	0
	Есть	36,13	3,64	2
Astra Linux	Нет	1,91	0,23	1
	Есть	63,84	25,67	2
Alt Linux	Нет	0,13	0,0044	0
	Есть	32,72	2,98	2

Таблица 4

Работа программы-шифровальщика со встроенными СЗИ с шифрованием всех каталогов

ОС	Наличие прав суперпользователя	Скорость шифрования, Мбит/с	Процент поражения ФС, %	Сохранение работоспособности ФС
Debian	Нет	3,41	0,73	0
	Есть	31,22	18,31	2
RedOS	Нет	1,65	0,03	0
	Есть	31,11	3,47	2
Astra Linux	Нет	0,06	0,007	0
	Есть	11,38	1,57	0
Alt Linux	Нет	0,13	0,0044	0
	Есть	32,72	2,98	2

Заключение

Ряд проведенных экспериментов показал несостоятельность встроенных средств защиты информации различных систем на базе Unix перед программами-шифровальщиками, целью которых является шифрование пользовательских файлов и требование выкупа за информацию. Для защиты от таких угроз необходимо использовать средства антивирусной защиты, EDR-решения и системы резервного копирования.

В случае если целью программы-шифровальщика является нарушение или прекращение работоспособности системы, то проведенные эксперименты показывают большую критичность учетной записи суперпользователя, а также высокую эффективность подхода, применяемого в ОС Astra Linux – ограничение прав суперпользователя.

Литература

1. Maniriho P. API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // Journal of Network and Computer Applications. – Amsterdam: Elsevier Ltd., 2023. – P. 1–18.

2. Jing C. Ensemble dynamic behavior detection method for adversarial malware / C. Jing, Y. Wu, C. Cui // Future Gener. Comput. Syst. – 2022. – No. 130. – P. 193–206.

3. Maniriho P. A study on malicious software behavior analysis and detection techniques: Taxonomy, current trends and challenges / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // Future Gener. Comput. Syst. – 2022. – No. 130. – P. 1–18.

4. Лабутин Н.Г. Предотвращение проникновения вирусов-шифровальщиков в корпоративные информационные системы // Современные тенденции развития науки и технологий. – Белгород: ООО «Агентство перспективных научных исследований», 2017. – С. 113–115.

5. Байздренко Е.А. Информационные угрозы для малого бизнеса: вирусы-шифровальщики // Актуальные вопросы учета и управления в условиях информационной экономики. – Севастополь: ООО «Рибест», 2018. – С. 270–274.

6. Путивльская И.Ю. Анализ рынка вирусов шифровальщиков / И.Ю. Путивльская, А.О. Ткач // Наука и образование: отечественный и зарубежный опыт. – Белгород: ООО «ГиК», 2018. – С. 37–41.

7. Тепловодских А.Д. Аспекты защиты от вирусов-шифровальщиков / А.Д. Тепловодских, С.С. Зотов // Аллея науки. – 2017. – № 12. – С. 367–371.

8. Долматов М.П. Вирусы-шифровальщики / М.П. Долматов, К.А. Ярмош, В.Л. Склярук // Современные проблемы радиоэлектроники и телекоммуникаций. – 2018. – № 1. – С. 209.

9. Begovic K. Cryptographic ransomware encryption detection: Survey / K. Begovic, A. Al–Ali, Q. Malluhi // Computers & Security. – 2023. – № 132. – P. 1–16.

10. Berrueta E. Survey on Detection Techniques for Cryptographic Ransomware / E. Berrueta, D. Morato, E. Magana, M.A. Izal // IEEE Access. – 2016. – № 7. – P. 1–21.

11. Su D. Detecting Android locker–ransomware on Chinese social networks / D. Su, J. Liu, X. Wang, W. Wang // IEEE Access. – 2017. – P. 20381–20393 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/329769980_Detecting_Android_Locker-Ransomware_on_Chinese_Social_Networks (дата обращения: 12.10.2023).

12. Murali R. Evolving malware variants as antigens for antivirus systems / R. Murali, P. Thangavel, C.Sh. Velayutham // Expert Systems with Applications. – 2023. – № 226. – P. 1–15.

13. Dwan B. The computer virus – From there to here: An historical perspective // Computer Fraud & Security. – 2000. – № 12. – P. 13–16.

14. Mawgoud A.A. A malware obfuscation AI technique to evade antivirus detection in counter forensic domain Enabling AI applications in data science / A.A. Mawgoud, H.M. Rady, B.S. Tawfik // Springer. – 2021. – P. 597–615 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/344349230_A_Malware_Obfuscation_AI_Technique_to_Evade_Antivirus_Detection_in_Counter_Forensic_Domain (дата обращения: 12.10.2023).

15. The 2023 Global Ransomware Report [Электронный ресурс]. – Режим доступа: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf (дата обращения: 08.09.2023).

16. 2023 Mid-year cyber security report: report reveals 48 ransomware groups have breached over 2,200 victims [Электронный ресурс]. – Режим доступа: https://research.checkpoint.com/2023/2023-mid-year-cyber-security-report-report-reveals-48-ransomware-groups-have-breached-over-2200-victims/ (дата обращения: 08.09.2023).

17. Аналитический отчёт: техники, тактики и процедуры (TTPs) группировок шифровальщиков [Электронный ресурс]. – Режим доступа: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Common%20TTPs%20of%20modern%20ransomware.pdf (дата обращения: 08.09.2023).

18. Cybersecurity threatscape: Q1 2023 [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q1/ (дата обращения: 08.09.2023).

19. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model / L. Bekkers, S. van 't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, E.R. Leukfeldt // Computers & Security. – 2023. – № 127. – P. 1–12.

20. Johns E. Cyber Security Breaches Survey 2021: Statistical Release. – 1 изд. – London: Department for Digital, Culture, Media and Sport. – 2021. – 66 p.

21. Rohn E. Explaining small business InfoSec posture using social theories / E. Rohn, G. Sabari, G. Leshem // Inform. Comput. Secur. – 2016. – No. 24 (5). – P. 434–556.

22. Osborn E. Risk and the small-scale cyber security decision making dialogue – a UK case study / E. Osborn, A. Simpson // Comput. J. – 2018. – No. 61 (4). – P. 472–495.

23. Van der Kleij R. Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security / R. Van der Kleij, R. Leukfeldt // International Conference on Applied Human Factors and Ergono-

mics. – 2019. – P. 16–27 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/3336455 50_Cyber_Resilient_Behavior_Integrating_Human_Behavioral_Models_and_Resilience_Engineering_Capabilities_into_Cyber_Security (дата обращения: 12.10.2023)

24. Vashishtha L.K. An Ensemble approach for advance malware memory analysis using Image classification techniques / L.K. Vashishtha, K. Chatterjee, S.S. Rout // Journal of Information Security and Applications. – 2023. – No. 77. – P. 1–14.

25. Bozkir A.S. Utilization and comparision of convolutional neural networks in malware recognition / A.S. Bozkir, A.O. Cankaya, M. Aydos // 27th signal processing and communications applications conference. – 2019. – P. 1–4.

26. MaleVis dataset home page [Электронный ресурс]. – Режим доступа: https://web.cs.hacettepe.edu.tr/~selman/malevis/ (дата обращения: 12.10.2023).

27. A forensic analysis of android malware-how is malware written and how it could be detected? / K. Allix, Q. Jérome, T.F. Bissyandé, J. Klein, R. State, Y. Le Traon // IEEE 38th annual computer software and applications conference. – 2014. – P. 384–393.

28. Rathnayaka C. An efficient approach for advanced malware analysis using memory forensic technique / C. Rathnayaka, A. Jamdagni // IEEE Trustcom/BigDataSE/ICESS. – 2017. – P. 1145–1150.

29. Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud / N. Nissim, O. Lahav, A. Cohen, Y. Elovici, L. Rokach // Computers & Security. – 2019. – No. 87. – P. 1–20.

Огнев Игорь Александрович
Аспирант, ассистент каф. защиты информации (ЗИ)
Новосибирского государственного технического университета (НГТУ)
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0003-3884-7170
Тел.: +7-999-465-77-31
Эл. почта: i.ognev.2016@corp.nstu.ru

Никрошкин Иван Владимирович
Аспирант, ассистент каф. защиты информации ЗИ НГТУ
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0003-4824-7419
Тел.: +7-996-377-90-71
Эл. почта: i.nikroshkin@corp.nstu.ru

Медведев Михаил Александрович
Аспирант, ассистент каф. защиты информации ЗИ НГТУ
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0001-7674-9964
Тел.: +7-923-148-20-85
Эл. почта: m.medvedev@corp.nstu.ru

Красников Артем Дмитриевич
Лаборант инжинирингового центра
«Информационная безопасность» (ИЦ ИБ) НГТУ
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0009-0002-4437-9764
Тел.: +7-913-986 6199
Эл. почта: player7004@yandex.ru

Ognev I.A., Nikroshkin I.V.,
Medvedev M.A., Krasnikov A.D.

Study of built-in information protection tools of Unix systems on the example of malware infection

This article provides a comparative analysis of the built-in information protection tools of the Unix family operating systems using the example of malware infection of the operating system. The study involved open-source operating systems – Debian, and domestic operating systems – Alt Linux, RedOS, Astra Linux Special Edition. A ransomware virus was used as a malicious software. The presented results demonstrate the greatest ability of the Astra Linux operating system to resist malware infection.

Keywords: information security, information protection, malicious software, virus, ransomware, operating system, information protection tool.
DOI: 10.21293/1818-0442-2023-26-4-29-34

References

1. Maniriho P. API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // *Journal of Network and Computer Applications*. Amsterdam: Elsevier Ltd, 2023, pp. 1–18.

2. Jing C. Ensemble dynamic behavior detection method for adversarial malware / C. Jing, Y. Wu, C. Cui // *Future Generation Computer Systems*, 2022, no. 130, pp. 193–206.

3. Maniriho P. A study on malicious software behavior analysis and detection techniques: Taxonomy, current trends and challenges / P. Maniriho, A.N. Mahmood, M.J.M. Chowdhury // *Future Generation Computer Systems*, 2022, no. 130, pp. 1–18.

4. Labutin N.G. [Preventing ransomware from penetrating corporate information systems] // *Current trends in the development of science and technology*. Belgorod: Limited Liability Company «Agency for Advanced Scientific Research», 2017, pp. 113–115 (in Russ.)

5. Baizdrenko E.A. [Information Threats to Small Businesses: Ransomware] // *Topical Issues of Accounting and Management in the Information Economy*. Sevastopol: OOO «Ribest», 2018, pp. 270–274 (in Russ.)

6. Putivlskaya I.Y. [Market analysis of ransomware viruses] / I.Y. Putivlskaya, A.O. Tkach // *Science and Education: Domestic and Foreign Experience*. Belgorod: OOO GiK, 2018, pp. 37–41 (in Russ.)

7. Teplovodskikh A.D. [Aspects of protection against ransomware] / A.D. Teplovodskikh, S.S. Zotov // *Alley of Science*, 2017, no. 12, pp. 367–371 (in Russ.)

8. Dolmatov M.P. [Ransomware viruses] / M.P. Dolmatov, K.A. Yarmosh, V.L. Sklyaruk // *Modern Problems of Radio Electronics and Telecommunications*, 2018, no. 1, 209 p. (in Russ.)

9. Begovic K. Cryptographic ransomware encryption detection: Survey / K. Begovic, A. Al-Ali, Q. Malluhi // *Computers & Security*, 2023, no. 132, pp. 1–16.

10. Berrueta E. Survey on Detection Techniques for Cryptographic Ransomware / E. Berrueta, D. Morato, E. Magana, M.A. Izal // *IEEE Access*, 2016, no. 7, pp. 1–21.

11. Su D. Detecting Android locker-ransomware on Chinese social networks / D. Su, J. Liu, X. Wang, W. Wang // *IEEE Access*. 2017. pp. 20381–20393. Available at: https://www.researchgate.net/publication/329769980_Detecting_Android_Locker-Ransomware_on_Chinese_Social_Networks (Accessed: October 12, 2023).

12. Murali R. Evolving malware variants as antigens for antivirus systems / R. Murali, P. Thangavel, C. Sh. Velayutham // *Expert Systems with Applications*, 2023, no. 226, pp. 1–15.

13. Dwan B. The computer virus – From there to here: An historical perspective //*Computer Fraud & Security*, 2000, no. 12, pp. 13–16.

14. Mawgoud A.A. A malware obfuscation AI technique to evade antivirus detection in counter forensic domain Enabling AI applications in data science / A.A. Mawgoud, H.M. Rady, B.S. Tawfik // Springer, 2021, pp. 597–615. Available at: https://www.researchgate.net/publication/344349230_A_Malware_Obfuscation_AI_Technique_to_Evade_Antivirus_Detection_in_Counter_Forensic_Domain (Accessed: October 12, 2023)

15. The 2023 Global Ransomware Report. Available at: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf (Accessed: September 08, 2023).

16. 2023 Mid-year cyber security report: report reveals 48 ransomware groups have breached over 2,200 victims. Available at: https://research.checkpoint.com/2023/2023-mid-year-cyber-security-report-report-reveals-48-ransomware-groups-have-breached-over-2200-victims/ (Accessed: September 08, 2023).

17. Analyst Report: Techniques, Tactics, and Procedures (TTPs) of Ransomware Groups (in Russ.). Available at: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Common%20TTPs%20of%20modern%20ransomware.pdf (Accessed: September 08, 2023).

18. Cybersecurity threatscape: Q1 2023 (in Russ.). Available at: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q1/ (Accessed: September 08, 2023).

19. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model / L. Bekkers, S. van 't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, E.R. Leukfeldt // *Computers & Security*, 2023, no. 127, pp. 1–12.

20. E. Johns Cyber Security Breaches Survey 2021: Statistical Release. 1 ed. London: Department for Digital, Culture, Media and Sport, 2021, 66 p.

21. Rohn E. Explaining small business InfoSec posture using social theories / E. Rohn, G. Sabari, G. Leshem // *Information and Computer Security*, 2016, no. 24, vol. 5, pp. 434–556.

22. Osborn E. Risk and the small-scale cyber security decision making dialogue – a UK case study / E. Osborn, A. Simpson // *Computer Journal*, 2018, no. 61, vol. 4, pp. 472–495.

23. R. Van der Kleij, R. Leukfeldt Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security // *International Conference on Applied Human Factors and Ergonomics*, 2019, pp. 16–27. Available at: https://www.researchgate.net/publication/333645550_Cyber_Resilient_Behavior_Integrating_Human_Behavioral_Models_and_Resilience_Engineering_Capabilities_into_Cyber_Security (Accessed: October 12, 2023).

24. Vashishtha L.K. An Ensemble approach for advance malware memory analysis using Image classification techniques / L.K. Vashishtha, K. Chatterjee, S.S. Rout // *Journal of Information Security and Applications*, 2023, no. 77, pp. 1–14.

25. Bozkir A.S. Utilization and comparision of convolutional neural networks in malware recognition / A.S. Bozkir, A.O. Cankaya, M. Aydos // *27th Signal Processing and Communications Applications Conference*, 2019, pp. 1–4.

26. MaleVis dataset home page Available at: https://web.cs.hacettepe.edu.tr/~selman/malevis/ (Accessed: October 12, 2023).

27. A forensic analysis of android malware-how is malware written and how it could be detected? / K. Allix, Q. Jérome, T.F. Bissyandé, J. Klein, R. State, Y. Le Traon // *IEEE 38th Annual Computer Software and Applications Conference*, 2014, pp. 384–393.

28. Rathnayaka C. An efficient approach for advanced malware analysis using memory forensic technique / C. Rathnayaka, A. Jamdagni // *IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 1145–1150.

29. Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud / N. Nissim, O. Lahav, A. Cohen, Y. Elovici, L. Rokach // *Computers & Security*, 2019, no. 87, pp. 1–20.

Igor A. Ognev
Postgraduate student, assistant
Information Security Department (IS),
Novosibirsk State Technical University (NSTU)
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0003-3884-7170
Phone: +7-999-465-77-31
Email: i.ognev.2016@corp.nstu.ru

Ivan V. Nikroshkin
Postgraduate student, assistant IS NSTU
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0003-4824-7419
Phone: +7-996-377-90-71
Email: i.nikroshkin@corp.nstu.ru

Mikhail A. Medvedev
Postgraduate student, assistant IS NSTU
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0001-7674-9964
Phone: +7-923-148-20-85
Email: m.medvedev@corp.nstu.ru

Artyom D. Krasnikov
Laboratory Assistant, engineering Center
«Information Security» (IC IS), NSTU
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0009-0002-4437-9764
Phone: +7-913-986-61-99
Email: player7004@yandex.ru