

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

**Студенттер мен жас ғалымдардың
«GYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«GYLYM JÁNE BILIM - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 2025»**

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

**«GYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың
XX Халықаралық ғылыми конференциясы = XX Международная
научная конференция студентов и молодых ученых «GYLYM JÁNE
BILIM – 2025» = The XX International Scientific Conference for
students and young scholars «GYLYM JÁNE BILIM – 2025». – Астана:
– 3813 б. - қазақша, орысша, ағылшынша.**

ISBN 978-601-08-5373-7

**Жинаққа студенттердің, магистранттардың, докторанттардың және жас
ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті
мәселелері бойынша баяндамалары енгізілген.**

**The proceedings are the papers of students, undergraduates, doctoral students and young
researchers on topical issues of natural and technical sciences and humanities. В сборник
вошли доклады студентов, магистрантов, докторантов и молодых ученых по
актуальным вопросам естественно-технических и гуманитарных наук.**

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.1			
Цифровая трансформация образования			
204.	Адалбек Н.	«Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А.	«Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е.	«Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т.	«Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р.	«Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М.	«Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д.	«Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А.	«Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е.	«Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П.	«Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М.	«Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б.	«АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б.	«Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е.	«Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М.	«Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А.	«HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDSAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944
------	---	-----

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған ai дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «ИОТ Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
Подсекция 2.4		
Информационная безопасность		
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvecton және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзұмов А.М. «WebSocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Рамагуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

- TLS/SSL пайдалану: барлық WebSocket қосылымдары деректердің құпиялылығы мен тұтастығын қамтамасыз ету үшін шифрланған арналарды (wss://) пайдалану;
- Сайтаралық сценарийден қорғау (XSS): пайдаланушы енгізуін санитариялау, Content Security Policy (CSP) қауіпсіздік тақырыптарын орнату және басқа шаралар арқылы XSS-тің алдын алу;
- CSRF шабуылдарынан қорғау: веб-пішіндер мен басқа күйді өзгертетін сұраулар үшін CSRF шабуылдарына қарсы белгілерді пайдалану;
- Аутентификация және авторизация: OAuth, JWT немесе HTTP-Only және Secure cookie сеанстарын пайдалануды қоса алғанда, барлық кезеңдерде сенімді аутентификация мен авторизацияны қамтамасыз ету;

Пайдаланылған дереккөздердің тізімі

1. WebSocket: Lightweight Client-Server Communications, Andrew Lombardi 2015, 141p
2. The Definitive Guide to HTML5 WebSocket, Frank Salim Peter Moskovits, 2013, 227 p
3. <https://cyberleninka.ru/article/n/kak-ispravit-mezhsaytovuyu-uyazvimost-web-socket>
4. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9182458>
5. <https://book.hacktricks.xyz/pentesting-web/websocket-attacks>
6. <https://medium.com/swlh/hacking-websocket-25d3cba6a4b9>
7. <https://portswigger.net/web-security/websockets>
8. <https://ably.com/topic/websocket-security>
9. <https://www.shodan.io/>
10. <https://datatracker.ietf.org/doc>
11. <https://infosecwriteups.com/cross-site-websocket-hijacking-cswsh-ce2a6b0747fc/html/rfc6455>
12. <https://infosecwriteups.com/cross-site-websocket-hijacking-cswsh-ce2a6b0747fc>

УДК 004.056

АВТОМАТИЗАЦИЯ ПРОЦЕССА АНАЛИЗА ОПЕРАТИВНОЙ ПАМЯТИ С ИСПОЛЬЗОВАНИЕМ PYTHON

Майданов Алихан Серикович

Alikhan.m.01@gmail.com

Магистрант кафедры Информационная безопасность ЕНУ им. Л.Н. Гумилева, Астана, Казахстан Астана, Казахстан
Научный руководитель – Ахметова Ж.Ж.

Аннотация. В данной работе будет рассмотрен **Volatility Framework** и его ключевые возможности, связанные с анализом оперативной памяти. Будут продемонстрированы примеры использования плагинов, связанных с выявлением аномалий в процессах, закрепившихся в оперативной памяти, анализ подгруженных dll-файлов и их указателей, а также исследование оперативной памяти на предмет внедренного кода. Более того, в данной статье рассмотрены правила Yara Rules, а также скрипты на Python, позволяющие автоматизировать процесс анализа памяти. Результатом исследования станет создание набора автоматизации на базе Python, которые позволят автоматизировать рутинные задачи по анализу оперативной памяти, для ускорения процесса расследования кибератак и повышения его точности.

Ключевые слова: кибербезопасность, Volatility Framework, цифровая криминалистика, анализ оперативной памяти, автоматизация анализа памяти, аномалии в процессах, внедренный код, Yara Rules.

Введение

Современные киберугрозы становятся все более сложными и изощренными, что делает цифровую криминалистику важным направлением в области информационной безопасности. Одним из ключевых аспектов цифровой форензики является анализ оперативной памяти, поскольку именно в памяти можно обнаружить артефакты вредоносной активности, которые не всегда сохраняются на диске. Исследование дампа оперативной памяти позволяет получить критически важные данные, такие как процессы, сетевые соединения, зарегистрированные учетные записи, загруженные библиотеки и даже зашифрованные коммуникации вредоносных программ.

В этом контексте Volatility Framework является одним из наиболее популярных и высокофункциональных инструментов для анализа памяти. Volatility Framework — это платформа с открытым исходным кодом, предназначенная для анализа оперативной памяти различных операционных систем, включая Windows, Linux, macOS и Android. Она предоставляет обширный набор плагинов, позволяющих исследовать процессы, драйверы, файлы, сетевые соединения, реестр операционных систем, а также извлекать вредоносный код из памяти. Возможности Volatility делают его незаменимым инструментом в расследованиях кибератак, анализе вредоносного программного обеспечения (ПО) и реагировании на инциденты безопасности.

Однако, несмотря на функциональность Volatility, процесс исследования оперативной памяти остается достаточно сложным и требует значительных временных затрат. Запуск различных плагинов, анализ их результатов и поиск подозрительной активности вручную — трудоемкая задача. Кроме того, анализ может включать обработку больших объемов данных, что делает его подверженным человеческим ошибкам.

Анализ оперативной памяти является одной из ключевых задач цифровой криминалистики и расследования инцидентов информационной безопасности. Однако традиционные методы анализа требуют значительных временных и вычислительных ресурсов, а также высокой квалификации специалиста. Дамп памяти содержит огромный объем информации: активные процессы, загруженные библиотеки, сетевые соединения, открытые файлы, системные артефакты и даже следы вредоносной активности. Обнаружение атакующих действий в этом массиве данных вручную — сложная, трудоемкая и подверженная ошибкам задача.

Материалы и методы

В этом контексте автоматизация анализа памяти с помощью Python-скриптов и Volatility Framework становится необходимостью. Она позволяет сократить время расследования, исключить человеческий фактор при анализе и выявлять аномалии быстрее и точнее.

Volatility Framework — это мощный инструмент цифровой криминалистики, предназначенный для анализа дампов оперативной памяти (RAM). Он позволяет исследовать активные процессы, сетевые соединения, загруженные библиотеки (DLL), следы вредоносного ПО и многое другое [1].

Volatility был разработан как проект с открытым исходным кодом и распространяется под лицензией GNU General Public License (GPL). Это означает, что любой может использовать, изменять и распространять код. Разработчики могут создавать собственные плагины и расширять функциональность. Пример использования Volatility: `python vol.py -f memDump.bin windows.pstree`

Плагин `pstree` в Volatility 3 используется для **построения дерева процессов, запущенных в момент создания дампа памяти**. Он помогает определить родительские и

дочерние процессы, что особенно полезно при расследовании вредоносной активности, так как позволяет выявить: **аномальные процессы, которые не соответствуют типичной иерархии, процессы, запущенные без родительского процесса или с необычными родителями, использование утилит для повышения привилегий или выполнения команд удаленно.**

Плагин `psxview` в `Volatility 3` используется для обнаружения скрытых процессов в дампе оперативной памяти. Этот инструмент помогает обнаружить процессы, которые могут быть замаскированы вредоносным ПО (например, руткитами) и не отображаются в стандартных списках процессов Windows.

На рисунках ниже представлены выводы команд дерева процессов (Рисунок 1)

```
C:\Users\Ra1d3n\Downloads\volatility3-develop\volatility3-develop\python_vol.py -f 'C:\Users\Ra1d3n\Downloads\MemLabs-Lab1\MemoryDump_Lab1.raw' windows.psxtree
Volatility 3 Framework 2.21.0
Programs: 100.00      PDB scanning finished
PID      PPID      ImageFileName      Offset(V)      Threads Handles SessionId  Now64  CreateTime      ExitTime      Audit  Cmd  Path
-----
4        0        System              0x00000000      570      N/A      False  2019-12-11 13:41:25.000000 UTC  N/A      -      -      -
+ 248    4        smss.exe            0x00000000      37       N/A      False  2019-12-11 13:41:25.000000 UTC  N/A      -      -      -
  smss.exe            \SystemRoot\System32\smss.exe  \SystemRoot\System32\smss.exe
++ 376   248     psxs.exe            0x00000000      18       0        False  2019-12-11 13:41:33.000000 UTC  N/A      -      -      -
  psxs.exe            \SystemRoot\System32\psxs.exe  C:\Windows\System32\psxs.exe
320     312     csrss.exe           0x00000000      9        0        False  2019-12-11 13:41:32.000000 UTC  N/A      -      -      -
  csrss.exe           \SystemRoot\System32\csrss.exe  ObjectDirectory:\Windows\SharedSection=1024,20480,768 Windows=0n SubSystemType=Windows ServerDll=baserv
v.1 ServerDll=insrv\UserServerDllInitialization,3 ServerDll=insrv:conServerDllInitialization,2 ServerDll=ssxssrv,4 ProfileControl=Off MaxRequestThreads=16
C:\Windows\System32\csrss.exe
368     360     csrss.exe           0x00000000      7        1        False  2019-12-11 13:41:33.000000 UTC  N/A      -      -      -
  csrss.exe           \SystemRoot\System32\csrss.exe  ObjectDirectory:\Windows\SharedSection=1024,20480,768 Windows=0n SubSystemType=Windows ServerDll=baserv
v.1 ServerDll=insrv\UserServerDllInitialization,3 ServerDll=insrv:conServerDllInitialization,2 ServerDll=ssxssrv,4 ProfileControl=Off MaxRequestThreads=16
C:\Windows\System32\csrss.exe
+ 2268   368     conhost.exe         0x00000000      2        50       1        False  2019-12-11 14:37:54.000000 UTC  N/A      -      -      -
  conhost.exe         \??\C:\Windows\System32\conhost.exe  C:\Windows\System32\conhost.exe
+ 2692   368     conhost.exe         0x00000000      2        50       1        False  2019-12-11 14:34:54.000000 UTC  N/A      -      -      -
  conhost.exe         \??\C:\Windows\System32\conhost.exe  C:\Windows\System32\conhost.exe
488     380     winlogon.exe        0x00000000      8        218      1        False  2019-12-11 13:41:34.000000 UTC  N/A      -      -      -
  winlogon.exe        C:\Windows\System32\winlogon.exe
424     312     wininit.exe         0x00000000      3        75       0        False  2019-12-11 13:41:34.000000 UTC  N/A      -      -      -
  wininit.exe         C:\Windows\System32\wininit.exe
+ 580    424     lsx.exe             0x00000000      11       185      0        False  2019-12-11 13:41:35.000000 UTC  N/A      -      -      -
  lsx.exe             \Device\HarddiskVolume2\Windows\System32\lsx
```

Рисунок 5 Вывод команды psxtree

Одним из наиболее эффективных инструментов в `Volatility` является модуль `Malfind`, предназначенный для поиска следов внедренного кода в адресном пространстве процессов. Вредоносные программы часто используют различные техники инъекций, позволяя атакующим исполнять произвольный код в доверенных процессах Windows.

Принцип работы модуля `Malfind` заключается в том, что он анализирует виртуальные адресные пространства процессов и выявляет аномалии, указывающие на возможные инъекции кода. Основные критерии, по которым `Malfind` обнаруживает подозрительные участки памяти, включают:

1. Выделение памяти с правами исполнения (`PAGE_EXECUTE_READWRITE`) — вредоносный код часто размещается в таких участках.
2. Отсутствие привязки памяти к загруженным модулям — если область памяти не принадлежит ни одной из известных DLL, это может быть признаком внедрения.
3. Наличие исполняемых инструкций в неожиданном месте — например, если процесс загружает код, не относящийся к его стандартному исполняемому файлу.

Вывод плагина включает в себя: PID процесса, в который была выполнена инъекция, виртуальный адрес подозрительного участка памяти, фрагмент содержимого памяти в шестнадцатеричном представлении (hex dump), дизассемблированный код [2].

Другим важным инструментом анализа оперативной памяти является `Dllist` — модуль, позволяющий получить список загруженных динамических библиотек (DLL) для каждого активного процесса [3].

Загрузка вредоносных DLL является одной из распространенных техник маскировки вредоносного ПО. Атакующие могут использовать **DLL Injection** для выполнения своего кода внутри легитимных процессов Windows. Анализ загруженных библиотек помогает выявить такие угрозы, как:

1. **Использование нелегитимных DLL в системных процессах.**
2. **Наличие неизвестных или подозрительных библиотек в процессе.**

3. Отсутствие подписей у загруженных модулей.

Применение Volatility в расследованиях помогает не только выявлять вредоносную активность, но и автоматизировать процесс анализа с помощью Python-скриптов, что особенно актуально для работы с большими объемами данных [4].

Результаты

На рисунке ниже приведена основная функция, которая используется в написанном автором коде (Рисунок 3).

```
def run_volatility(plugin, dump_file):
    """Запуск Volatility 3 и вывод соотв. информации."""
    cmd = f"python vol.py -f {dump_file} {plugin}"
    result = subprocess.run(cmd, shell=True, capture_output=True, text=True)
    return result.stdout
```

Рисунок 3 Функция запуска Volatility

На основе команды `python vol.py -f` будут впоследствии запускаться различного рода плагины для дальнейшего исследования. Эта функция **автоматизирует работу с Volatility 3**, упрощая анализ дампов памяти. Она позволяет запускать плагины, получать их результаты и использовать их в Python-скриптах для автоматизации цифровой криминалистики.

Данный код является открытым исходным кодом. В python-скрипте будут реализованы следующие плагины для автоматизации исследования оперативной памяти:

```
# Плагины Volatility которые будут запущены
plugins = {
    "Processes (pslist)": "windows.pslist",
    "Hidden Processes (psscan)": "windows.psscan",
    "Hidden and stealthy processes": "windows.psxview",
    "Processes in tree format": "windows.pstree",
    "Malicious Injections (malfind)": "windows.malfind",
    "Loaded DLLs (dlllist)": "windows.dlllist",
```

Рисунок 6 Плагины Volatility

Суть автоматизации данного процесса, в том, что он позволяет избежать рутинных действий и помогает извлекать необходимые для исследования цифровые улики в рамках расследования произошедших атак или инцидентов информационной безопасности.

Обсуждение

Скрипт помогает извлечь все необходимые артефакты, в один клик. К тому же, стандартный вывод выполнения данных плагинов отображается в командной строке, что немного неудобно при длительном изучении. Данный скрипт извлекает информацию и записывает ее в .csv и .txt форматы. В случае, исполнения плагинов pslist и dlllist, в которых вывод представляет собой список, данный скрипт сохраняет их в .csv формате для удобства чтения, а вывод остальных команд сохраняется в .txt. Терминальный вывод работы скрипта, изображен ниже (Рисунок 5).

В ходе исследования были разработаны программные инструменты, позволяющие автоматизировать запуск Volatility и обработку его вывода. Такой подход позволяет эффективно идентифицировать потенциальные угрозы, анализировать активность вредоносного ПО и получать структурированную информацию о состоянии системы на момент создания дампа памяти.

Результаты работы подтверждают, что внедрение автоматизированных решений на основе Python и Volatility Framework может существенно повысить эффективность работы специалистов по цифровой криминалистике.

Список использованной литературы

1. Cohen, M (2020). Incident Response & Computer Forensics, Third Edition. McGraw-Hill Education.
2. Sikorski, M., & Honig, A. (2022). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.
3. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2021). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley.
4. Case, A., & Richard, G. (2019). Memory Forensics: The Path Forward. Digital Investigation, 29, S6-S17.

УДК 004.75.

БЛОКЧЕЙН ҚАЖЕТТІЛІК ПЕ, ӘЛДЕ СӘН БЕ?

Мақсат Әсемай, Нурсеитов Сейіл

nurseitovseil@gmail.com, maksatasemai001@gmail.com

Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің
Ақпараттық қауіпсіздік кафедрасының 3 курс студенттері,
Астана, Қазақстан

Ғылыми жетекші – Казиева Назым Магидулловна

Аңдатпа: Мақалада блокчейн қажет пе? деген сұрақты талдадық. Тақырыпты зерттеу барысында басқа модельдерге сүйене отырып, блокчейн қажет пе, егер блокчейн қажет болған жағдайда, қандай түрді қолдану керек екендігі туралы нақты және дұрыс түсінік алу үшін маңызды ойлар мен сұрақтарды бөлдік.

Түйінді сөздер: блокчейн, криптовалюта, тізілім (реестр), тест-сауалнама.

Кіріспе. Мақалада қазіргі әлемдегі блокчейн технологиясының өзектілігі мен қажеттілігі қарастырылады. Орталықтандырылмаған шешімдерге деген қызығушылықтың артуы жағдайында блокчейн қаржы, логистика, денсаулық сақтау және деректерді басқаруды қоса алғанда, әртүрлі салаларға жаңа мүмкіндіктер ұсынады [1]. Жұмыста блокчейннің негізгі принциптері, оның артықшылықтары мен кемшіліктері, сондай-ақ нақты жобаларда сәтті қолдану мысалдары талданады [2]. Блокчейн әртүрлі салаларда қамтамасыз ете алатын қауіпсіздік, ашықтық және тиімділік мәселелеріне ерекше назар аударылады.

Талдау аясында осы технологияны кәсіпорынның барлық бизнес-процестерінде қолдану қажеттілігі бар-жоғын бағалауға, сондай-ақ олардың міндеттерінің ерекшелігіне байланысты қолайлы блокчейн моделін таңдауға мүмкіндік беретін тест әзірледік. Тест әзірлеу барысында әртүрлі модельдерді зерттеп, сол модельдерге сүйендік. Бұл модельдер туралы қысқаша тоқталып өтейік.