4. Raciti M. Anomaly Detection in Water Management Systems / M. Raciti, J. Cucurull, S. Nadjm-Tehrani. — Text : direct // Critical Infrastructure Protection. Lecture Notes in Computer Science. — 2012. — Vol. 7130. — P. 98-119. — DOI: 10.1007/978-3-642-28920-0_6.
5. Meleshko A. V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems / A. V. Meleshko, V. A. Desnitsky, I. V. Kotenko. — Text : direct // IOP Conference Series: Materials Science and Engineering. International Conference on Modern Trends in Manufacturing Technologies and Equipment, 2019. — 2020. — P. 033034.

Д. Г. Бурилов, К. В. Подобрий, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ПО ВИРУСНОМУ АНАЛИЗУ

Аннотация. *В ходе работы были рассмотрены основные техники и методы вирусного анализа, а также представлено описание разработанных методических материалов по вирусному анализу.*

Ключевые слова: *вирусный анализ, статический анализ, динамический анализ, компьютерный вирус, индикаторы компрометации, обфускация, вредоносное программное обеспечение.*

Введение. В настоящее время практически все сферы деятельности человека связаны с применением компьютеров, а информация является одним из самых дорогих ресурсов. Так как компьютерные системы и программное обеспечение постоянно развиваются, возрастает объем и повышается уязвимость хранящихся в них данных.

Сейчас можно утверждать, что компьютерные вирусы остаются одной из наиболее распространенных причин искажения и уничтожения важной информации, как следствие, возникают финансовые и временные потери. Согласно интерактивной карте угроз от Лаборатории Касперского, во всем мире ежедневно происходит до

7,5 млн обнаружений вредоносных программ, около 20% из них являются вирусами [1]. На рис. 1, 2 отображена статистика для России за май 2022 г.

Проблема исследования. Вследствие этого возникает потребность в специалистах, которые могут анализировать вирусы, способы их распространения и заражения, характер их появления, а также способы борьбы с ними. Из-за нехватки квалифицированных работников в области вирусного анализа, возникает необходимость подготовки таких специалистов. Соответственно, актуальной текущей работы определяется этим фактором. Задачей данной работы является разработка методических материалов по вирусному анализу для обучения студентов основам вирусного анализа.

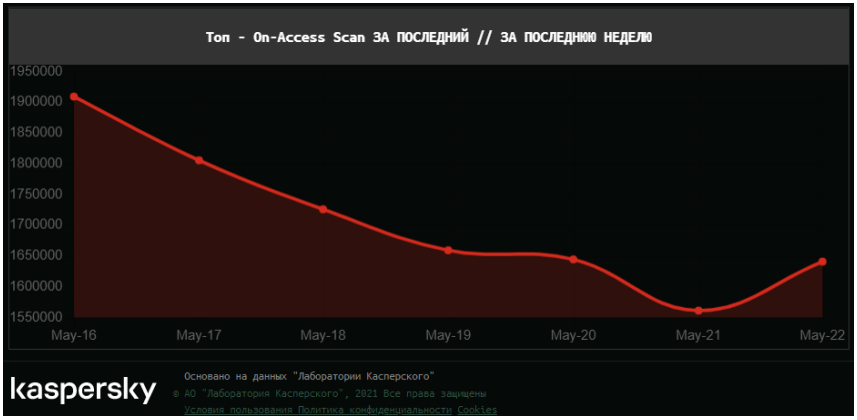

Рис. 1. Обнаружения вредоносных программ в России за май 2022 г.

Топ - On-Access Scan ЗА ПОСЛЕДНИЙ // ЗА ПОСЛЕДНЮЮ НЕДЕЛЮ		
1	DangerousObject.Multi.Generic	13.62%
2	Trojan.Win32.Agent.gen	5.94%
3	Trojan-Dropper.Win32.Convagent.gen	4.19%
4	Trojan.BAT.Miner.gen	2.9%
5	Trojan.Win32.Agent.ifdx	2.69%
6	HackTool.Win32.Convagent.gen	2.07%
7	Trojan.Win32.Hosts2.gen	1.82%
8	VHO:Trojan-Dropper.Win32.Convagent.gen	1.62%
9	Trojan.WinLNK.Starter.dh	1.61%
10	Email-Worm.Win32.Brontok.q	1.49%

Рис. 2. Наиболее распространенные вредоносные программы в России за май 2022 г.

Материалы и методы. Цель вирусного анализа, как правило, заключается в предоставлении информации, которая понадобится для предотвращения заражения. Обычно задачами является определение того, как произошло заражение и обнаружение всех зараженных объектов или компьютеров. При анализе подозрительных вредоносных программ цель будет заключаться в определении возможных действий опасного двоичного файла, как обнаружить его в сети и как измерить ущерб, который он нанес. После определения файлов, которые требуют полного анализа, нужно разработать сигнатуру для обнаружения этого вируса. В основном используются методы на основе хостовых или сетевых сигнатур.

Существует два основных подхода к анализу вирусов: статический и динамический. Статический анализ включает в себя изучение вредоносного программного обеспечения (ПО) без его запуска. Динамический же наоборот, включает в себя запуск такого ПО [2].

Базовый статический анализ состоит из изучения исполняемого файла [3]. Такой анализ может подтвердить, является ли файл вредоносным, предоставить информацию о его функциональности, а иногда и предоставить информацию, которая позволит создать простые сетевые сигнатуры. Базовый статический анализ довольно

прост и может быть быстрым, однако он в значительной степени неэффективен против сложных вирусов, поэтому можно пропустить важные модели поведения.

Базовый динамический анализ обычно включает в себя запуск вируса и наблюдение за его поведением в системе для того, чтобы удалить «инфекцию», а также создание эффективных сигнатур, или же все вместе [4]. Однако, прежде чем запускать вирусное ПО, следует создать среду, которая позволит изучать запущенные вредоносные программы без риска повреждения системы или сети. В результате данной работы была создана такая среда.

Расширенный статический анализ состоит из обратного проектирования (реверс-инжиниринга) внутренних компонентов вредоносных программ посредством загрузки исполняемого файла в дизассемблер (например, IDA, W32DASM, PE Explorer, REDasm) и просмотра основных инструкций для того, чтобы узнать, что делает программа. Однако продвинутый статический анализ более сложный для обучения, чем базовый статический анализ и требует специальных знаний по разборке конструкции кода и концепции операционной системы.

Расширенный динамический анализ использует отладчик (OllyDBG, GNU Debugger, SoftICE, Microsoft Debugger) для изучения внутреннего состояния, запущенного вредоносного исполняемого файла. Передовые методы динамического анализа обеспечивают еще один способ извлечения подробной информации из вируса. Эти техники наиболее полезны, при попытке получить информацию, которую трудно собрать с помощью других методов. Расширенный динамический анализ вместе с расширенным статическим анализом позволяют полностью проанализировать подозрительные вирусные программы.

Цель лабораторных работ, являющихся практическим результатом данной статьи — ознакомить студентов с техниками и методами вирусного анализа. Для имитации реалистичного анализа вредоносных программ, студентам не было представлено никакой информации о вирусах. Во всех лабораторных вирусным файлам были даны общие имена для имитации неизвестных вредоносных программ, которые обычно используют бессмысленные или вводящие в заблуждение

имена. Каждая из лабораторных работ состоит из краткой теории, вредоносного файла, нескольких вопросов, ответы на которые потребуются для составления отчета, и в некоторых случаях примера.

В разработанных методических материалах рассматриваются следующие темы:

- исследование различных артефактов, указывающих прямо или косвенно на то, что файл заражен;
- использование различных антивирусных баз;
- различные варианты ручной распаковки упакованных файлов;
- деобфускация обфусцированного вредоносного кода;
- исследование сетевой активности, создаваемых процессов, изменений в реестре, файловой системе, планировщике задач;
- создание правил, на основе которых генерируются индикаторы компрометации (Indicator of Compromise, IoC);
- работу с различными программами для вирусного анализа;
- основные моменты дизассемблирования.

Исследование различных артефактов файла подразумевает под собой изучение таких параметров как энтропия, хэш-файла, подключаемый библиотеки, строки, наличие упаковщика. Данные параметры, а также исследование изменений в реестре можно увидеть на рис. 3, 4, 5.

Также одной из рассмотренных тем в методических материалах является обфускация кода. В одной из лабораторных работ в качестве примера был рассмотрен троян Emotet, который был впервые идентифицирован в 2014 г. как банковское вредоносное ПО, крадущее конфиденциальную информацию. Данный вирус был встроен в макрос документа Microsoft Word. Содержимое данного документа можно увидеть на рис. 6. Наиболее частой причиной заражения данным вирусом являются фишинговые письма, в которых находится зараженный документ Microsoft Word [5].

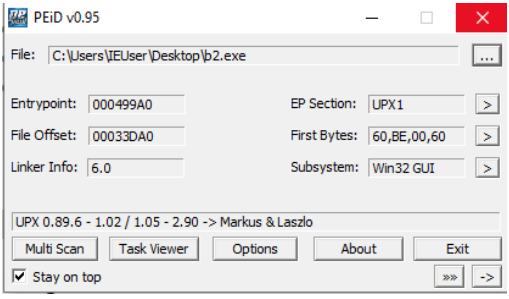

Рис. 3. Наличие упаковщика в файле

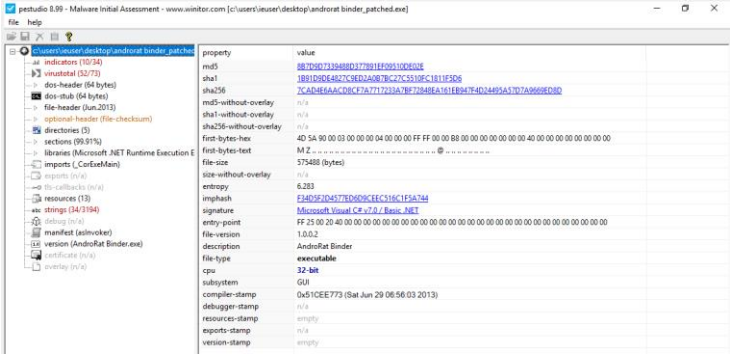

Рис. 4. Исследование с помощью pestudio

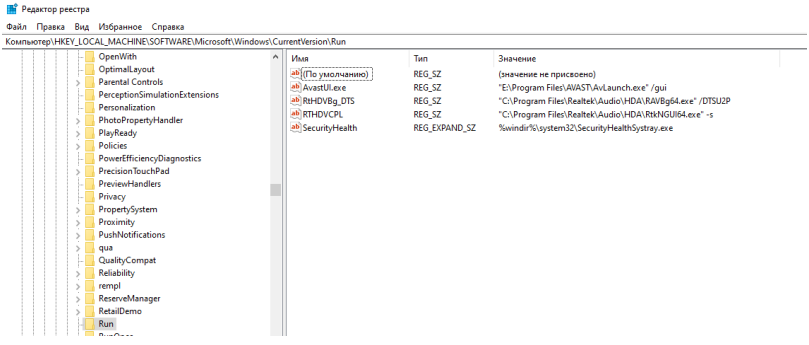

Рис. 5. Исследование реестра

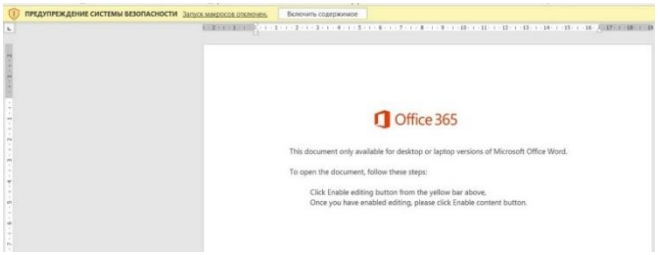

Рис. 6. Содержимое вредоносного файла

В процессе анализа была найдена точка входа в макрос — функция Awzttocpmk(), код которой приведен в рис. 7.

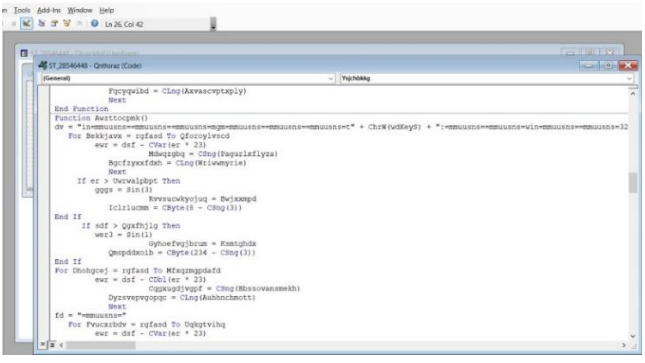

Рис. 7. Обфусцированный код

В результате различный преобразований получили деобфусцированный код, который можно увидеть на рис. 8. Проанализировав его, можно понять, что с помощью данного макроса с URL-адресов, перечисленных в массиве $list, загружается и сохраняется под именем 937.exe вредоносный файл.

Рис. 8. Деобфусцированный код

На тему индикаторов компрометации были рассмотрены инструменты Yara и YarGen. Правила Yara напоминают язык программирования. Основная их задача — определять переменные в шаблонах, найденных в образце вредоносного ПО [6]. При полном или частичном совпадении этот алгоритм может быть использован для успешной идентификации вредоносного ПО. Некоторые из сгенерированных и отредактированных вручную правил можно увидеть на рис. 9.

Результаты. В результате данной работы были созданы методические материалы по вирусному анализу, которые включают в себя 15 лабораторных работ, 2 виртуальные машины, 20 примеров вредоносных файлов, теорию, которая охватывает основные темы, описанные раннее. Также была проведена апробация лабораторных работ на студентах группы 22ИБАСс-178 Института математики и компьютерных наук. Результаты апробации можно увидеть на рис. 10, 11. Под термином «удача» подразумевается заинтересованность студентов и отправка отчетов по выполнению лабораторных работ.

```
/* Rule Set ----------------------------------------------------------------- */

rule Lab01_01 {
   meta:
      description = "Chapter_1L - file Lab01-01.dll"
      author = "PMA Labs"
      reference = "PMA Labs - Chapter 1"
      date = "2022-04-01"
      hash1 = "f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba"
   strings:
      $x1 = "SADFHUHF" fullword ascii
      $x2 = "127.26.152.13" fullword ascii
      $x3 = "1Y2a2g2r2" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 500KB and
      1 of ($x*)
}

rule Lab01_04 {
   meta:
      description = "Chapter_1L - file Lab01-04.exe"
      author = "PMA Labs"
      reference = "PMA Labs - Chapter 1"
      date = "2022-04-01"
      hash1 = "0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126"
   strings:
      $x1 = "\\system32\\wupdmgrd.exe" fullword ascii
      $x2 = "\\winup.exe" fullword ascii
      $s1 = "\\system32\\wupdmgr.exe" fullword ascii
      $s2 = "http://www.practicalmalwareanalysis.com/updater.exe" fullword ascii
      $s3 = "SeDebugPrivilege" fullword ascii /* Goodware String - occured 141 times */
      $s4 = "<not real>" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 100KB and
      1 of ($x*) and 2 of ($s*)
}

rule Lab01_01_2 {
   meta:
      description = "Chapter_1L - file Lab01-01.exe"
      author = "PMA Labs"
      reference = "PMA Labs - Chapter 1"
      date = "2022-04-01"
      hash1 = "58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47"
   strings:
      $x1 = "C:\\windows\\system32\\kerne132.dll" fullword ascii
      $x2 = "kerne132.dll" fullword ascii
      $x3 = "WARNING_THIS_WILL_DESTROY_YOUR_MACHINE" fullword ascii
      $s1 = "Lab01-01.dll" fullword ascii
      $s2 = "C:\\Windows\\System32\\Kernel32.dll" fullword ascii
      $s3 = "Kernel32." fullword ascii
      $s4 = "ugh 0@" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 50KB and
      1 of ($x*) and 2 of ($s*)
}
```

Рис. 9. Правила Yara

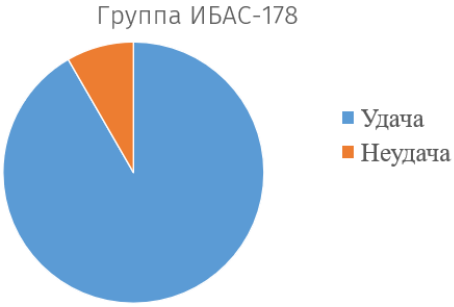

Рис. 10. Апробация лабораторных работ

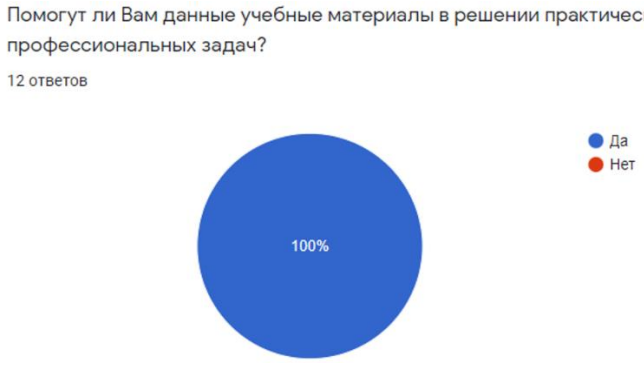

Рис. 11. Результат опроса студентов

Заключение. Во время работы была изучена теория по вирусному анализу, составлены методические материалы, которые помогут студентам в выполнении лабораторных работ, разработан комплекс лабораторных работ по вирусному анализу, а также итоговый тест для проверки усвоения материала.

СПИСОК ЛИТЕРАТУРЫ

1. Интерактивная карта киберугроз : [сайт]. — URL: https://cybermap.kaspersky.com/ru (дата обращения: 12.04.2022). — Текст : электронный.
2. Sikorski M. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software / M. Sikorski, A. Honig. — San Francisco : No Starch Press, Inc., 2012. — 768 p. — Text : direct.

3. Реверсинг малвари для начинающих : [сайт]. — URL: https://xakep.ru/2016/12/08/reversing-malware-tutorial-part1/ (дата обращения: 01.05.2022). — Текст : электронный.
4. Искусство антидетекта : [сайт]. — URL: https://www.securitylab.ru/analytics/485677.php (дата обращения: 01.04.2022). — Текст : электронный.
5. Что такое Emotet? : [сайт]. — URL : https://www.kaspersky.ru/resource-center/threats/what-is-emotet (дата обращения: 02.05.2022). — Текст : электронный.
6. Обзор правил YARA: изучение инструмента исследования вредоносного ПО : [сайт]. — URL: https://habr.com/ru/company/varonis/blog/584618/ (дата обращения: 21.04.2022). — Текст : электронный.

А. Р. Зиянгиров, А. М. Шабалин
Тюменский государственный университет, г. Тюмень

УДК 004.732

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ЦЕНТРАЛИЗОВАННОГО АДМИНИСТРИРОВАНИЯ БЕСПРОВОДНОЙ СЕТИ ПРЕДПРИЯТИЯ С ПОМОЩЬЮ КОНТРОЛЛЕРА

Аннотация. *В статье рассматриваются способы организации и функционирования безопасного централизованного администрирования беспроводной сети предприятия с помощью контроллера. Результатом работы стала модель компьютерной сети предприятия с применением беспроводного контроллера с обеспечением необходимого уровня защиты беспроводных станций.*

Ключевые слова: *WLAN, Wi-Fi, беспроводной контроллер, CAPWAP, безопасность.*

Введение. В наши дни на многих предприятиях активно используются беспроводные сети, а значит существует потребность в том, чтобы обеспечить централизованное администрирование и безопасность таких подключений. Современные сети, построенные на независимых точках доступа, — это устаревшая немасштабируемая архитектура с ограниченным функционалом, поэтому все средние и крупные компании с развитием беспроводных систем переходят на