ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

ҚазҰТЗУ ХАБАРШЫСЫ

ВЕСТНИК КазНИТУ

VESTNIK KazNRTU

№ 3 (139)

АЛМАТЫ 2020 ИЮНЬ

ISSN 1680-9211

Учредитель:

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Регистрация:

Министерство культуры, информации и общественного согласия
Республики Казахстан № 951 – Ж "25" 11. 1999 г.

Основан в августе 1994 г. Выходит 6 раз в год

Адрес редакции:

г. Алматы, ул. Сатпаева, 22,
каб. 609, тел. 292-63-46
Nina. Fedorovna. 52 @ mail.ru

болады. Сонымен қатар теориялық мәні мен модульдеу арқылы а лынған мән арасында аз мөлшерде айырмашылық бар екенін байқауға болады. FBG га түскен механикалық кернеу неғұрлым үлкен болса, толқын ұзындығының ығысуы соғұрлым үлкен болады және сызықтық қатынасты көрсетеді, ал есептеу нәтижесі мен модельдеуден шыққан нәтиже бойынша, алғашқы толқын ұзындығының центрі мен толқын ұзындығының ең жоғары мәні бір-бірімен қабысады, ол спектр пішінінің симметриялы екенін көрсетеді, ал механикалық кернеу артқан сайын толқын ұзындығының ығысуы да артады, ол спектрдің симметриядан ауытқуының артуын көрсетті, қортындылай келе бұл модельдеу арқылы алған нәтиже мен теориялық нәтиже бір- бірімен толықтай сәйкес келетінінің дәлелдейді

ӘДЕБИЕТТЕР

[1] Hill K O, Fujii Y, Johnson D C, et al. Photosensitivity in optical fiber waveguides: application to reflection filter fabrication [J].Appl Phys Lett, 1978, 32: 647-649.

[2] S.M.Melle, K. Liu. A passive wavelength demodulation system for guided-wave Bragg grating sensors [J]. IEEE Photon. Technol. Lett.,Vol. 4, 1992, 516

[3] Han K J, Lee Y W. Simultaneous measurement al strain and temperature incorporating a long period fiber grating inscribed on a long-period fiber grating inscribed on a polarization maintaining fiber [J]. Photonics Technology Letters, IEEE, 2002,16(90):2114-2116

[4] Jin W, Ho H L, Liao Y B, et al. Development of a wavelength detection system for fiber grating sensors. Advanced sensor systems and application [C].proc of SPIE, 2004:68-76

[5 SW James, ML Dockney, RP Tatam, Simultaneous independent temperature amd strain measurement using in-fiber Bragg grating sensors [J]. Electron. Lett, 1996.

[6] Кусамбаева Н.Ш ,Касимов А.О, Влияние аподизации сменно периодической брэгговской решетки на поляризационно-модовую дисперсию* Новости науки Казахстана. № 1 (135). 2018

[3] Джа Жынан, Фон Фй, Бір уақытта Талшықты оптикалық тор темпаратурасы мен штамм өлшеуінің зерттелу барысы[J]. Жарық толқындық байланыс технологиясы, 2007,(2):41-43

[4] Цзян Дешэн, Хэ Вайб, Талшықты торлы сенсордф қолдану туралы жалпы шолу [J]. Оптоэлектроника-Лазер, 2002, (4) 420-430

[7] Liao Yanti, Li Jiao, Today and Development of Fiber Optic Sensors [J] Sensor World, 2004, (2): 6-12

[8] Ляо Янти, Ли Цзяо, Талшықты оптикалық сенсорлардың бүгіні және дамуы [J] Сенсор әлемі, 2004, (2): 6-12

Расул Д.К. , Касимов А.О.

Талшықты торлы сенсорды зерттеу және қолдану

Резюме Описываются технические преимущества и применение волоконно-оптических датчиков, базовая структура волоконно-оптического датчика и принцип действия волоконно-оптических датчиков. Эта работа анализирует дрейф длины волны, когда механическое напряжение в FBG изменяется через программу Optisystem. Когда механическое напряжение в FBG изменяется, дрейф длины волны принимается анализатором спектра. Предложенный проект был проверен с помощью программы моделирования, и теоретически рассчитанный результат был сопоставлен с результатом дрейфа, полученным с помощью программы моделирования.

Ключевые слова: FBG, сенсорная технология, техническая схема, измерение.Optisystem.

УДК 004. 056.57

[1]B. Abdiyev, [2]N. Karymsakova, [1]D. Satybaldina
[1]L.N. Gumilev Eurasian National University, Nur-Sultan, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan
(E-mail: abdibaur@gmail.com, satybaldina_dzh@enu.kz, nkarymsakova1@gmail.com)

CONDUCTING TEST (TEST) MEASURES TO PROTECT AGAINST TARGETED ATTACKS

Abstract: The paper discusses modern methods of hiding targeted attacks aimed at bypassing Sandbox-systems. The results of behavioral analysis of five files of different formats in several commercial Sandbox-systems are presented in order to identify the effectiveness of detecting malicious functionality of experimental samples. It is shown that the performance of the investigated sandboxes is associated with the implementation of methods to minimize the concealment of traces of attacks of several generations.

Keywords: malware, malware detection, targeted attack, sandbox system

Б. Абдиев[1], Н. Карымсакова[2], Д. Сатыбалдина[1]
[1]Евразийский национальный университет имени Л.Н. Гумилева, Нур-Султан, Казахстан
[2]Казахский национальный университет им. Аль-Фараби
(E-mail: abdibaur@gmail.com, satybaldina_dzh@enu.kz, nkarymsakova1@gmail.com)

ВОЗМОЖНОСТИ ПРОМЫШЛЕННЫХ SANDBOX-СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ ТАРГЕТИРОВАННЫХ АТАК

Аннотация: В работе рассмотрены современные методы скрытия целевых атак, направленные на обход Sandbox-систем. Приведены результаты поведенческого анализа пяти файлов разного формата в нескольких коммерческих Sandbox-систем с целью выявления эффективности детектирования вредоносного функционала экспериментальных образцов. Показано, что производительность исследованных «песочниц» связана с реализаций способов минимизации сокрытия следов атак нескольких поколений.

Ключевые слова: вредоносное программное обеспечение, детектирование вредоносного файла, таргетированная атака, Sandbox-система.

1. Введение

Любое программное обеспечение, которое намеренно причиняет ущерб владельцам информации и работе компьютерам, смартфонам, серверам, компьютерным сетям, считается вредоносным. Англоязычный эквивалент «malware» происходит от сочетания двух слов – «malicious» (злонамеренный) и «software» (программное обеспечение). Существуют различные классы вредоносных программ, включая вирусы, черви, «троянский конь», руткиты, вымогатели и т.д. Каждый класс malware-программ предназначен для воздействия на исходную машину-жертву с различными целями, такими как удаленное выполнение кода, кража конфиденциальных данных и т. д.

В наши дни классификация вредоносных программ усложняется, потому что некоторые экземпляры вредоносных программ могут одновременно представлять характеристики нескольких классов. Вредоносное ПО нового поколения может легко обойти защитное программное обеспечение, работающее в режиме ядра, такое как брандмауэры, антивирусное программное обеспечение. Оно использует несколько различных существующих или новых процессов одновременно и использует некоторые запутанные методы, чтобы скрыть себя и стать постоянным в системе [1]. Вредоносные программы нового поколения могут запускать более разрушительные атаки, например, целевые (или таргетированные) атаки, которых никогда раньше не было, и во время атак используется более одного типа вредоносных программ.

Атаки с использованием такого рода malware-программ имеют катастрофические последствия и наносят значительный материальный ущерб отдельным лицам, частным компаниям и правительственным активам. В связи с этим, вредоносное ПО должно быть обнаружен до повреждения важных активов в компании. Чтобы преодолеть сложные системы обнаружения вторжений, основанные на статическом анализе, злоумышленники используют запутывание (обфускацию) кода, включая методы полиморфизма и метаморфизма, применение которых не выявляется на уровне проверки сигнатуры вредоносного ПО. В связи с этим динамический поведенческий анализ представляется единственным надежным подходом для обнаружения современных вредоносных программ [2]. Учитывая сложность в качестве и массивность в количестве современных атак, имеет смысл выполнить глубокий поведенческий анализ на выделенных серверах, которые предоставляют всю необходимую вычислительную мощность для выявления вредоносной активности. Такой подход реализуется как выполнение неизвестного исполняемого файла в среде тестирования, известной как «песочница» (malware sandbox), в которой можно наблюдать вредоносную активность ПО без ущерба для существующей ИТ-системы [3, 4].

Различные исследования продемонстрировали влияние методов кластерного анализа, машинного обучения на эффективности обнаружения и классификации вредоносных файлов при sandbox анализе [1, 2, 5]. Кроме того, точность этих моделей машинного обучения может быть улучшена за счет использования алгоритмов выбора признаков для выбора наиболее важных функций и уменьшения размера набора данных, что приводит к меньшим вычислениям. В связи с этим в настоящей работе представлены результаты экспериментального исследования нескольких промышленных систем динамического поведенческого анализа с целью выявления взаимосвязи их функциональных особенностей и эффективностью обнаружения и классификации вредоносных программ различных типов.

Остальная часть статьи организована следующим образом. Во втором разделе мы обсуждаем методы уклонения вредоносного ПО для обхода «песочниц». В разделе III рассмотрены различные типы коммерческих Sandbox-систем, используемых для экспериментального исследования образцов вредоносных программ. В разделе IV представлены сравнительные экспериментальные результаты анализа поведения пяти файлов разного формата в нескольких Sandbox-систем с целью детектирования их вредоносного функционала. Последний раздел содержит заключение.

2 Методы уклонения вредоносного ПО для обхода «песочниц»

Технологии и векторы атак меняются быстрыми темпами, появляются новые поколения скрытых атак, которые не обнаруживаются стандартными средствами защиты информации. Для максимизации уровня обнаружения угроз и минимизации ложных срабатываний необходимы также и технологии поведенческого анализа нового поколения. В этих условиях раннее обнаружение имеет решающее значение для предотвращения целенаправленных атак от несанкционированного доступа к информационным ресурсам и поддерживающей инфраструктуре компании. Организации и крупные предприятия нуждаются в адаптивных Sandbox-систем, в которых на постоянной основе обновляются методы детектирования атак новых поколений. В связи с этим в данном разделе представлены современные варианты целенаправленных атак, направленные на обход «песочниц». Анализ методов сокрытия следов активности целевого нападения позволяет определить функциональные отличия исследованных в данной работе коммерческих Sandbox-систем.

Использование хакерами методов уклонения приводят к тому, что целевые атаки не детектируются или не исполняются в изолированной среде, а запускаются лишь на рабочей станции – жертве.

Первое поколение скрытых атак связано с детектом виртуализации, то есть возможностью обнаруживать артефакты виртуальных машин (файлы, записи в реестре, какие-то процессы, которые связаны с гипервайзером, виртуальной машиной). Если вредоносное ПО обнаруживает, что находится в виртуальной среде, то оно не запускается, для противодействия детектированию его вредоносности. В этих условиях адаптивная Sandbox-система, ее детектор, который работает на уровне виртуальной машины, должны отслеживать запросы исследуемой malware-программы к ядру операционной системы. Если запрос происходит от того файла, который исследуется в виртуальной машине, Sandbox-система должен давать ему ложные ответы, чтобы вирус не смог распознать, что это виртуализация (например, если файл называется VirtualBox, то он просто переименовывает) (см. рисунок 1).

Рис. 1. Первое поколение скрытых атак и метод их детектирования

Второе поколение атак связана с задержкой исполнения. Прежде чем приступить к своей вредоносной активности malware-программы включает таймер задержки на полчаса, так как любое динамическое обследование происходит от 30 секунд до 7 минут в любой Sandbox-системе, соответственно. Следовательно, если использовать задержку, файл включит на исполнение свой вредоносный функционал уже после проверки в «песочнице». Для детектирования атак данного

поколения используется следующий способ: вредоносная программа, делает запрос о системной времени, Sandbox-системе содержит способы ускорения и удаления задержек, ядро (драйвер «песочницы») передает положительный ответ вредоносной программе. Но практически вредоносная программа будет отключаться не на полчаса, а на одну миллисекунд. Кроме того, существует способ микрозадержки исполнения кода циркуляции, т.е., когда ядро Sandbox-системе не сообщит о вредоносной программе «необходимо отключить на полчаса», передаст на выполнение команду «разбить на 100 миллисекунд и выполнить цикл по 100 миллисекунд», заменив тем самым 30 минут (см. рисунок 2). В рамках синхронизации механизмов системные процессы Windows могут отправить запрос на отключение. Если все процессы сообщаются, то можно быстро сменить 100 миллисекунд на 0 везде. Это приводит к тому, что ОС Windows может выйти в аварийный режим. Поэтому во многих песочниках нет механизма при микро-задержках, и, соответственно, не все Sandbox-системы могут детектировать атаки такого типа.

Следующее поколение (поколение 3) целевых атак использует это системный элемент, например, диалоговое окно – инсталлятор для определенной программы. Соответственно, пока не нажмешь на инсталлятор программы «продолжить дальше», «установить», никакие действия не произойдут. Поскольку «песочницы» не умеют этого делать, соответственно, это самый сегодня современный механизм обхода большинства Sandbox-системы. Для противодействия данному методу сокрытия разработчики «tLab» предлагают использовать симулятор пользователя, который фактически выполняет действия, связанные с нажатиям на кнопки «продолжить дальше», он может раскрутить целый инсталлятор до конца, довести до полной инсталляции программы и дальше анализировать поведение потенциально вредоносного ПО (см. рисунок 3).

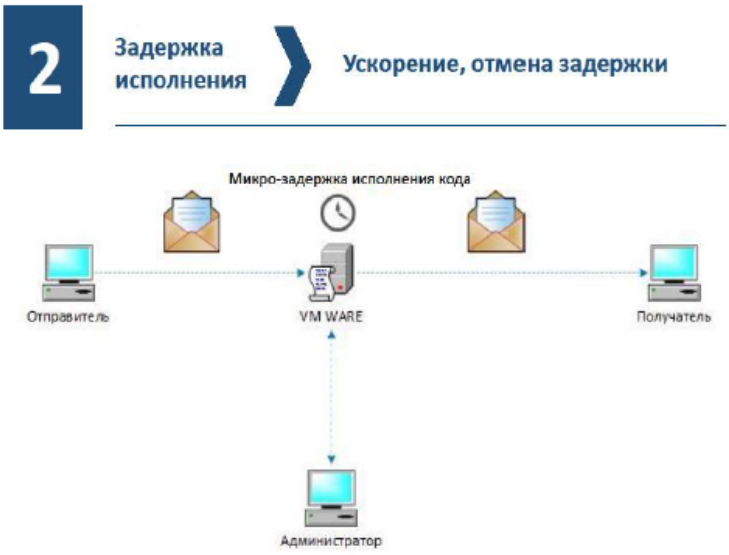

Рис. 2. Микро-задержка исполнения кода

Атаки четвертого поколения используют несистемные элементы. Дело в том, что системные элементы опрашивают кнопки, опрашивают окно, спрашивают класс окна, спрашивают название окна и дальше уже по нему начинают опрашивать системный элемент. Это набор системных элементов Windows – кнопка, поля редактирования и так далее. Новый способ – это статичное изображение, то есть нет никаких полей, никакого окна, просто есть картинка, которая была создана как скриншот диалогого окна, и там нарисована кнопка. Но когда нажимаешь мышкой на эту картинку, получается, что программа отслеживает координаты нажатия мышки.

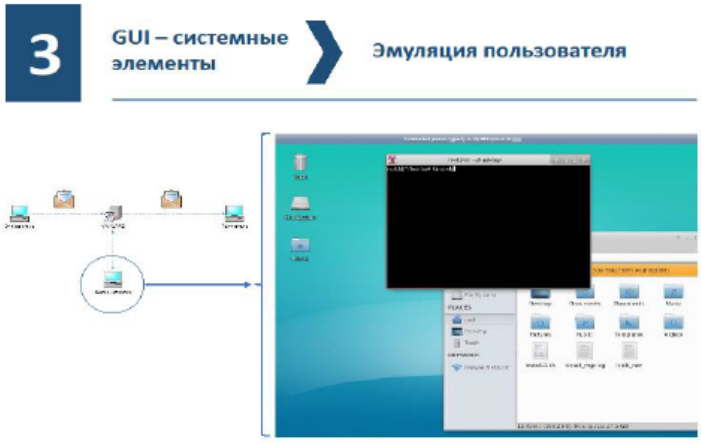

Рис. 3. Эмулирование работы пользователя

Если координаты совпадают с кнопкой, то происходит дальнейшее срабатывание. То есть с точки зрения пользователя, визуально у них ничем отличаться не будет, но когда «песочница» начинает пытаться опрашивать статическое изображение. Система сообщает: здесь наблюдается только картинка, нет никаких кнопок и других программ.

«tLab» – это единственная в мире «песочница», которая имеет встроенное компьютерное зрение, распознает графические элементы и, соответственно, может сама распознать кнопку, поле «редактирование» с помощью специальных алгоритмов. Он может сказать, что этот нарисованный прямоугольник – это именно кнопка. Вот этот нарисованный прямоугольник – это окно, а вот это – допустим, текстовое поле. И он, соответственно, нажимает на нужные элементы. В итоге этот способ использования статического изображения может обойти любую Sandbox-систему, кроме «tLab».

Рис. 4. Распознование malware-программы 4-го поколения.

3. Краткое описание Sandbox-систем и экспериментальных образцов вредоносных файлов

Большая часть вредоносного кода распространяется через исполняемые файлы, файлы офисных документов и т.д. поэтому рекомендуется открывать документы таких типов с помощью «песочницы». Sandbox-системы предлагают ограниченное системное пространство для запуска ненадежных подозрительных исполняемых файлов и обеспечивают защищенную среду для хост-системы. Вредоносные файлы выполняются в среде, которая не имеет доступа к сетевым ресурсам хост-машины, файловой системе и не может повредить хост-устройство. Хорошая идея - предоставить комплексное решение для расследования вредоносных программ, предоставив строго контролируемую среду для

проведения расследования. Ниже представлены некоторые из популярных «песочниц», которые чаще всего используются исследователями безопасности.

Sandblast CheckPoint использует эмуляцию угроз для проверки на уровне процессора инструкций кода в виртуальной среде, чтобы остановить атаки на этапе эксплойта (белый список операций с кодом) до того, как вредоносное ПО сможет развернуться и избежать обнаружения [6]. SandBlast также использует извлечение угроз для доставки безопасного содержимого или чистых и восстановленных версий файлов [7].

Deep Discovery Analyzer от Trend Micro предоставляет пользователям изолированную программную среду Analyzer для расширенного анализа, используя несколько методов обнаружения. Исследует широкий спектр исполняемых файлов: Windows, Microsoft® Office, PDF, веб-файлы и сжатые файлы. Обнаруживает вредоносные программы и эксплойты, распространяемые в распространенных форматах документов, с помощью специального обнаружения и изолированной среды. Выполняет анализ URL-адресов, содержащихся в электронных письмах или отправленных вручную образцах. Автоматически делится новыми интеллектуальными возможностями обнаружения с помощью продуктов Trend Micro и сторонних производителей [8].

tLab от T&T Security – казахстанская система для анализа и обнаружения современных сложных вредоносных программ, в том числе ориентированных на пользователя и целевых атак [10]. Благодаря используемым технологиям tLab идентифицирует и описывает поведение вредоносных программ на различных уровнях семантики, что делает его очень полезным для кластерного анализа [1]. Технически система использует защищенные контейнеры, позволяющие пользователю выполнять анализ среды вредоносного действия в зависимости от среды выполнения. Чтобы обеспечить эффективное обнаружение вредоносных программ, в tLab имеется технология для глубокого динамического контроля поведения всей системы, которая позволяет проводить структурный анализ и создавать так называемые деревья активности, определенные в области функциональных возможностей системы. Модифицированные иерархические цветные сети Петри используются для распознавания функциональных возможностей Malware-системы, включая запутанные и распределенные [2].

В эксперименте использованы пять файлов разного формата (см. Таблицу 1). Образцы вредоносных файлов доступны для анализа на [11].

Таблица 1. **Характеристики экспериментальных образцов**

№	Хэш вредоносного объекта	Размер файла	Тип файла
1	SHA256: b1141ed4760e0d383cf52d35ae54ffc1e626106e6a205fa6fed20741421bc361	15 KB (15 000bytes)	Win32.exe
2	SHA256: f811962b88ea672ba97104887cbd7b8ea92de7ae245ce5db3a2ba095c190ef02	15 KB (15 000bytes)	Win32.exe
3	SHA256: 3f3137874145f7960f8f7e345468225bd11a3b14f5fa916af040fe51783cac7b	16 KB (16 000bytes)	.rtf
4	SHA256: a8e88cda2b501328e278849df489e9a911c973fc5f8babe41542dab886285039	100 KB (100 00bytes)	.pdf
5	SHA256: 6dc16bb090a1eff75524e8dd68c58b843a0adc9c6c0b153e8a331ff17c1c0ab8	13 KB (13 000bytes)	Win32.exe

4. Результаты эксперимента

Были задействованы следующие комплексы по обнаружению таргетированных атак от ряда компании:

- Checkpoint – Sandblast (использует два типа виртуальных машин: под управлением операционной системы Windows XP и под управлением операционной системы Windows 7);
- T&T Security – tLab (используют один тип виртуальной машины: под управлением операционной системы Windows 7);
- Trend Micro - Deep Discovery (использует два типа виртуальных машин: под управлением операционной системы Windows XP и под управлением операционной системы Windows 7);
- Fortinet – FortiSandbox (используют один тип виртуальной машины: под управлением операционной системы Windows 7)

В таблице 2 приведены результаты данных испытаний.

Таблица 2 . **Результаты детектирования вредоносных файлов Sandbox-системами**

Тип ОС	1. SHA256: b1141ed4760e0d383cf52d35ae54ffc1e626106e6a205fa6fed20741421bc361			
	Checkpoint (Sandblast)	T&T security (tLab)	Fortinet (FortiSandbox)	TrendMicro (Deep Discovery)
Windows 7	На снимке экрана виртуальной машины “песочницы” вредоносные действия не зафиксированы.	Обнаружено двумя антивирусными системами вредоносное ПО класса "шифровальщик" (WannaCry). Динамическим анализом зафиксирован 31 (тридцать один) процесс выделенных перечнем данных об угрозах (IOC) вариаций обхода "песочницы".	Анализ обнаружения вредоносного ПО отметил угрозу как одобренную с рейтингом «Clean».	Не выявлено
Windows XP	На снимке экрана виртуальной машины “песочницы” замечена вредоносная активность. Произведен анализ из 8 действий за полторы секунды.	ОС не задействована.	ОС не задействована.	Не выявлено
Тип ОС	2. SHA256: f811962b88ea672ba97104887cbd7b8ea92de7ae245ce5db3a2ba095c190ef02			
	Checkpoint (Sandblast)	T&T security (tLab)	Fortinet (FortiSandbox)	TrendMicro (Deep Discovery)
Windows 7	Система провела анализ и определила вредоносное ПО как известное. Динамический анализ в течении 81 (восьмидесяти одной) секунды активности не обнаружил (на снимке экрана виртуальной машины “песочницы” вредоносные действия не зафиксированы).	Система провела анализ и определила вредоносное ПО как известное. Динамический анализ указал все затрагиваемые файлы и процессы. Также были выявлены основные индикаторы компрометации (IOC) На снимках экранов виртуальных машин “песочниц” в итоге виден процесс шифрования ОС.	Анализ обнаружения вредоносного ПО отметил угрозу как одобренную с рейтингом «Clean».	Не выявлено
Windows XP		ОС не задействована.	ОС не задействована.	Не выявлено
Тип ОС	3. SHA256: 3f3137874145f7960f8f7e345468225bd11a3b14f5fa916af040fe51783cac7b			
	Checkpoint (Sandblast)	T&T security (tLab)	Fortinet (FortiSandbox)	TrendMicro (Deep Discovery)
Windows 7	Действия не зафиксированы, исполняемые файлы не содержат вредоносного содержания.	Антивирусное ядро не обнаружило вредоносной активности. Динамический анализ отражает создание нового процесса и извлечение исполняемого файла с последующим удалением системных файлов. На записи	Анализ обнаружения вредоносного ПО отметил угрозу как одобренную с рейтингом «Clean».	Не выявлено

		эмуляции виртуальной машины "песочницы" виден процесс запуска командной строки (cmd).		
Windows XP	Действия не зафиксированы, исполняемые файлы не содержат вредоносного содержания.	ОС не задействована	ОС не задействована	Не выявлено
Тип ОС	4. SHA256: a8e88cda2b501328e278849df489e9a911c973fc5f8babe41542dab886285039			
	Checkpoint (Sandblast)	T&T security (tLab)	Fortinet (FortiSandbox)	TrendMicro (Deep Discovery)
Windows 7	Действия не зафиксированы, исполняемые файлы не содержат вредоносного содержания	Динамический анализ зафиксировал: - создание нового процесса; - закрепление в ОС; - извлечение исполняемого файла который изменяет ключи реестра автозагрузки ОС. На снимке экрана виртуальной машины "песочницы" зафиксирован запуск подозрительного ПО.	Анализ обнаружения вредоносного ПО отметил угрозу как критичную с рейтингом «High Risk»	Не выявлено
Windows XP	Действия не зафиксированы, исполняемые файлы не содержат вредоносного содержания.	ОС не задействована	ОС не задействована	Не выявлено
Тип ОС	5. SHA256: 6dc16bb090a1eff75524e8dd68c58b843a0adc9c6c0b153e8a331ff17c1c0ab8			
	Checkpoint (Sandblast)	T&T security (tLab)	Fortinet (FortiSandbox)	TrendMicro (Deep Discovery)
Windows 7	Действия не зафиксированы, исполняемые файлы не содержат вредоносного содержания.	Статический анализ отобразил критичность уровня вредоносного ПО как Опасное. Динамический анализ зафиксировал: - создание нового процесса и закрепление в ОС с последующим извлечением исполняемого файла - изменение ключей реестра автозагрузки ОС, а также автозагрузки сервиса	Анализ обнаружения вредоносного ПО отметил угрозу как одобренную с рейтингом «Clean».	Не выявлено
Windows XP	Действия не зафиксированы, исполняемые файлы не содержат вредоносного содержания.	ОС не задействована	ОС не задействована	Не выявлено

Как видно из таблицы 2, Checkpoint – «Sandblast» из пяти предоставленных образцов обнаружил два вектора атак, применяя только модель сигнатурного распознавания вредоносного программного обеспечения. Не были обнаружены вредоносные файлы, применяющие технологии обхода «песочницы», т.е. три вида угрозы были пропущены. Также отсутствовала полноценная проверка ссылок в теле письма, ведущих на файловые хранилища типа drop box, а соответственно в рамках mail-gateway данный вектор атак не проверяется.

Trend Micro - Deep Discovery » из пяти предоставленных образцов не обнаружил ни одного вектора атак.

Fortinet – FortiSandbox » из пяти предоставленных образцов обнаружил один вектор атаки, Анализ обнаружения вредоносного ПО отметил угрозу как критичную с рейтингом «High Risk».

T&T Security – tLab из пяти предоставленных образцов обнаружил пять векторов атак. Система tLab провела анализ и определила вредоносное ПО как известное. Динамический анализ указал все затрагиваемые файлы и процессы. Также были выявлены основные индикаторы компрометации (IOC). Статический анализ отобразил критичность уровня вредоносного ПО как опасное.

Заключение

Целью проведения экспериментальный исследований испытаний было сравнение эффективности технологий обнаружения вредоносного ПО, реализованных в нескольких промышленных Sandbox-системы. Выявленные характеристики производительности нескольких «песочниц» связаны с их функциональными различиями по противодействию методов сокрытия атак. Показано, что казахстанский инновационный продукт «tLab» смог обнаружить вредоносный функционал всех исследованных образцов.

В эпоху постоянно развивающихся методов целевых атак, только развитие адаптивных решений Sandbox-систем, созданных небольшими командами, например, «T&T Security» («tLab»), которые постоянно обновляют движок, детектор, постоянно добавляют новые модули для обнаружения вредоносных программ, позволяют повысить эффективность обнаружения и детектирования новых типов целевых атак.

ЛИТЕРАТУРА

[1] Kopeikin A., Tokhtabayev A., Tashatov N., Satybaldina D. tLab: A System Enabling Malware Clustering Based on Suspicious Activity Trees.// In: Rak J., Bay J., Kotenko I., Popyack L., Skormin V., Szczypiorski K. (eds) Computer Network Security. MMM-ACNS 2017. - Lecture Notes in Computer Science, Springer, Cham.-2017, vol. 10446.-p.195-210.

[2] Tokhtabayev A., Kopeikin A., Tashatov N., Satybaldina D. Malware Analysis and Detection via Activity Trees in User-Dependent Environment. .// In: Rak J., Bay J., Kotenko I., Popyack L., Skormin V., Szczypiorski K. (eds) Computer Network Security. MMM-ACNS 2017. - Lecture Notes in Computer Science, Springer, Cham.-2017, vol. 10446.-p.211-222.

[3] Ö. A. Aslan and R. Samet, A Comprehensive Review on Malware Detection Approaches // *IEEE Access*, vol. 8, pp. 6249-6271, 2020. doi: 10.1109/ACCESS.2019.2963724

[4] K. Yoshioka, Y. Hosobuchi, T. Orii and T. Matsumoto, "Vulnerability in Public Malware Sandbox Analysis Systems," *2010 10th IEEE/IPSJ International Symposium on Applications and the Internet*, Seoul, 2010, pp. 265-268. doi: 10.1109/SAINT.2010.16

[5] S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore and G. R. K. Rao, "Dynamic Malware Analysis Using Cuckoo Sandbox," *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, 2018, pp. 1056-1060. doi: 10.1109/ICICCT.2018.8473346.

[6] Check Point, SandBlast Zero-Day Protection Datasheet, May 2016 url: https://www.checkpoint.com/products/advanced-network-threat-prevention/ (visited on 06/12/2019).

[7] P. K. K. Loh and B. W. Y. Loh, "Cells — A novel IOT security approach," *2016 IEEE Region 10 Conference (TENCON)*, Singapore, 2016, pp. 3716-3719. doi: 10.1109/TENCON.2016.7848753

[8] Trend Micro. Deep Discovery Analyzer. url: https://www.trendmicro.com/en_ca/business/products/network/advanced-threat-protection/analyzer.html (visited on 06/12/2019).

[9] Fortinet. FortiSandbox. url: https://www.fortinet.com/products/sandbox/fortisandbox.html (visited on 06/12/2019).

[10] TOKHTABAYEV A G. Intellectual hardware antiviral system for detecting and preventing malware software, has manipulating objects recognition module that transmits recognition manipulating objects on subsystem level. Патент KZ30984-A4. Основной идентификационный номер Derwent: 2019-209821

[11] http://www.malware-traffic-analysis.net

Абдиев Б., Карымсакова Н., Сатыбалдина Д.

Мақсатты шабуылдардан қорғау жөніндегі сынақ (тестілік) іс-шараларын жүргізу

Түйіндеме: Жұмыста Sandbox-жүйелерді айналып өтуге бағытталған мақсатты шабуылдарды жасырудың қазіргі заманғы әдістері қарастырылған. Эксперименттік үлгілердің зиянды функционалын детектеудің тиімділігін анықтау мақсатында бірнеше коммерциялық Sandbox-жүйелердегі әртүрлі форматтағы бес файлды мінез-құлықтық талдау нәтижелері келтірілген. Зерттелген "құмсалғыштардың" өнімділігі бірнеше ұрпақ шабуылдарының іздерін жасыруды азайту тәсілдерін іске асырумен байланысты.

Түйінді сөздер: зиянды бағдарламалық қамтамасыз ету, зиянды файлды анықтау, таргеттелген шабуыл, Sandbox-жүйе.