ОБНАРУЖЕНИЕ КРИПТОМАЙНЕРОВ В ОС WINDOWS ИНСТРУМЕНТАМИ ТЕХНОЛОГИИ ETW

Казаков О.А.[1], Коркин И.Ю.[2]

Цель статьи: *предотвращение экономического ущерба путём раннего обнаружения несанкционированного использования вычислительных ресурсов.*

Метод: *экспериментальный метод для поиска признаков работы программ по добыче криптографической валюты, метод построения бинарного дерева принятия решения для создания алгоритма принятия решения о заражении.*

Полученный результат: *показана необходимость обнаружения программ-добытчиков криптографической валюты методом анализа поведения, выделены индикаторы заражения операционной системы программой-добытчиком криптографической валюты (криптомайнером), предложен способ обнаружения криптомайнеров, реализовано программное средство обнаружения криптомайнеров.*

Ключевые слова: *криптографическая валюта, обнаружение криптомайнеров, поведенческий анализ, признаки работы криптомайнеров, ETW, WPR, WPA, C#.*

DOI:10.21681/2311-3456-2019-5-83-88

1.Введение

В настоящее время многие аналитические компании отмечают рост популярности криптографической валюты. Добыча криптографической валюты является крайне ресурсоёмким процессом и требует больших компьютерных мощностей. Отмеченный рост популярности криптографических валют мотивирует нарушителей использовать заражённые компьютеры для несанкционированной добычи криптографической валюты и собственного обогащения. Отчёты компаний BitDefender [1], Sucuri [2], Swissborg [3], Recorded Future [4] говорят о большом числе атак, результатом которых становится несанкционированная добыча криптографической валюты на компьютере жертвы. За 2018 год количество атак программными средствами добычи криптографической валюты превысило количество атак другими вредоносными программными средствами, такими, как, например, программами-вымогателями [5].

При таком заражении каскада компьютеров организация, которой принадлежат эти компьютеры будет нести огромные финансовые потери, связанные с оплатой возросшего количества потребляемой электроэнергии, а также заменой вышедшего из строя оборудования из-за роста нагрузки на вычислительные ресурсы.

Задача раннего обнаружения скрытого ПО, занимающегося добычей криптографической валюты, в ОС Windows является крайне актуальной, поскольку позволит минимизировать отмеченные убытки для компании. В связи с этим целью данной работы стало создание программного средства обнаружения скрытых программ-добытчиков криптографической валюты в ОС Windows с целью предотвращения экономического ущерба.

2.Постановка задачи

Задача обнаружения вредоносного ПО является одной из наиболее актуальных в научно-практическом мире информационной безопасности. Существует два основных подхода к решению такого рода задач: статический анализ и динамический анализ. Статический анализ заключается в поиске в исследуемом файле определённых сигнатур и отличается высокой степенью надёжности при обнаружении. Динамический анализ заключается в исследовании поведения уже запущенной программы, поэтому его ещё называют поведенческим анализом. Рассмотрим примеры использования обоих этих способов для обнаружения криптомайнеров.

Рассмотрим работы, являющиеся примерами использования динамического анализа.

Средство, представленное в работе [6], собирает информацию о запросах к системе доменных имён, ключах реестра и вызовах системных функций Windows, позволяет обнаруживать трояны, рекламное ПО, потенциально нежелательные программы.

В статье [7] большое внимание уделено анализу вызовов системных функций. В результате были классифицированы следующие виды вредоносного программного обеспечения: трояны, черви, вирусы, программы-шпионы, программы-вымогатели.

PyTrigger — решение, предлагаемое в работе [8]. Здесь анализировались запросы к реестру ОС Windows,

1 Казаков Олег Александрович, НИЯУ МИФИ, студент кафедры «Криптология и кибербезопасность», Москва, Россия. E-mail: oleg.al.kazakov@gmail.com

2 Коркин Игорь Юрьевич, кандидат технических наук, ведущий инженер-исследователь отдела информационной безопасности ООО «Центр Специальной Системотехники», г. Москва, Россия. E-mail: igor.korkin@gmail.com

динамически подгружаемые библиотеки, взаимодействие с файловой системой, порождение новых процессов исследуемым файлом. PyTrigger сравнивает обычное поведение системы, без исполнения зловредного файла, с поведением при исполнении. Авторы статьи утверждают, что их приложение способно обнаружить несколько десятков различных типов вредоносного программного обеспечения, среди которых, однако, нет добытчиков криптографической валюты.

Статья [9] приводит пример обнаружения вредоносного программного обеспечения, основанного на анализе дескрипторов файлов. Важно отметить, что полученное средство не имеет возможности обнаружения программ-добытчиков криптографической валюты.

В качестве примеров средств обнаружения, использующих статистические подходы, можно назвать антивирусы и решение SMARTbot [10]. Оба этих решения могут обнаруживать криптомайнеры, но только те, для которых уже были выявлены сигнатуры.

В соответствии с отчётом компании McAfee [11] за 2018 год появилось около 4 миллионов новых образцов криптомайнеров, для которых ещё не получены сигнатуры и которые не будут обнаружены существующими средствами обнаружения. С задачей обнаружения ранее не встречавшихся образцов хорошо справляются методы поведенческого анализа. Проведённый анализ показал, что средств обнаружения криптомайнеров, основанных на использовании методов поведенческого анализа, не существует. Данной работа посвящена вопросу проектирования и реализации такого средства обнаружения.

Разрабатываемое средство должно реализовывать следующие этапы: сбор данных о работе анализируемой программы, извлечение из этих данных признаков заражения и дальнейший анализ признаков с целью принятия решения о заражении. Для этого необходимо выбрать инструменты, которые будут использованы для получения признаков заражения, необходимо найти сами признаки заражения, а кроме того необходимо предложить алгоритм принятия решения о заражении.

3.Выбор инструментов получения признаков заражения

В качестве инструмента получения данных о работе запущенных в ОС Windows процессов будет использоваться технология Event Tracing for Windows.

Event Tracing for Windows (ETW) или система трассировки событий ОС Windows — технология журналирования и отслеживания событий ОС Windows, работающая на уровне ядра операционной системы, однако позволяющая отслеживать не только события, происходящие в ядре операционной системы, но и события, определённые в пользовательских приложениях[3]. Разбор событий позволяет получать данные об использовании любых ресурсов ОС Windows любым запущенным процессом.

Существует много средств, позволяющих получать события ОС Windows через ETW. Эти средства можно охарактеризовать следующим образом.

Использование системных библиотек C/C++/.NET больше всего подходит для реализации журналирования и простого получения определённых событий с целью определения поведения собственного пользовательского приложения при том или ином событии, происходящем в ОС Windows;

Использование системных утилит и приложений больше всего подходит для настройки системного журналирования и простого расследования ошибок, произошедших в течение работы ОС Windows;

Для реализации программного средства по обнаружению программ по добыче криптографической валюты больше всего подходят разработанные компанией Microsoft инструменты Windows Performance Recorder (WPR) и Windows Performance Analyser (WPA), поскольку они предоставляют широкие возможности по выбору и фильтрации необходимых для получения признаков работы программы, по использованию их возможностей из кода собственного приложения, а также возможность получения необходимых данных о работе исследуемого приложения в табличном виде.

4.Поиск индикаторов заражения

С целью поиска признаков (или индикаторов) заражения ОС Windows криптомайнером в рамках исследования, описываемого в данной статье, был проведён эксперимент, в процессе которого было проанализировано порядка 100 образцов вредоносных криптомайнеров, а также несколько легитимных ресурсоёмких приложений с целью исключения нахождения признаков, характерных не только для криптомайнеров. Набор образцов криптомайнеров оказалось возможным разделить на две категории: отдельные исполнимые файлы Windows и криптомайнеры, реализованные в виде исполнимого сценария браузера.

Поиск индикаторов заражения был начат с анализа использования ресурсов центрального процессора.

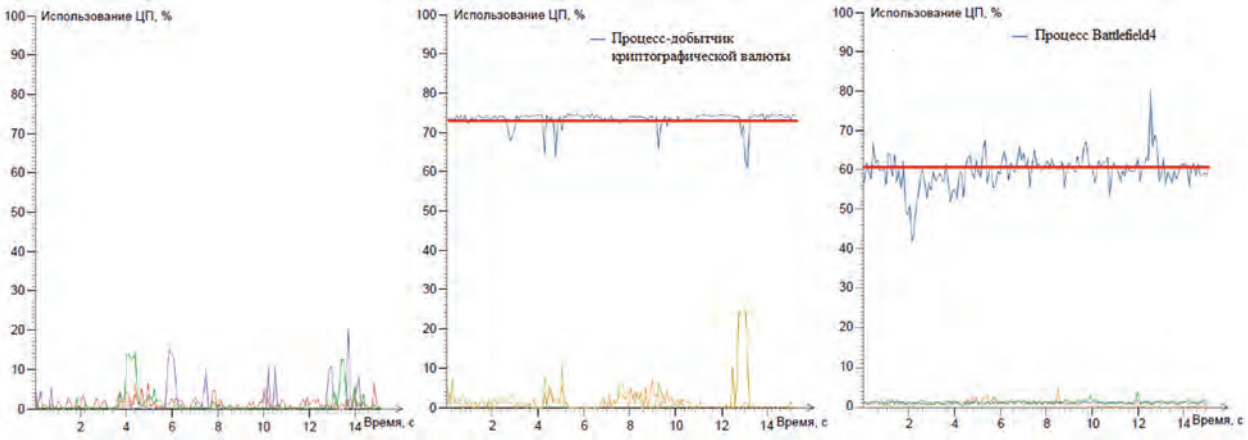
Эксперименты показали, что криптомайнеры крайне интенсивно используют ресурсы центрального процессора и средняя доля использования ЦП криптомайнерами составляла более 70%. Это можно заметить на рисунке 1б), а на рисунке 1а) изображено использование ресурсов ЦП процессами, среди которых нет ресурсоёмких — разница очевидна. С другой стороны некоторые легитимные ресурсоёмкие приложения также активно используют ресурсы центрального процессора, что опказано на рисунке 1в). Поэтому использовать только один индикатор является недостаточным для обнаружения.

Вторым индикатором был выбран объём используемой оперативной памяти. Эксперимент показал, что криптомайнеры в процессе своей работы практически не потребляют оперативную память в отличие от легитимных ресурсоёмких приложений.

Третьим индикатором было выбрано среднее квадратичное отклонение доли использования центрального процессора.

3 https://docs.microsoft.com/en-us/windows/desktop/etw/about-event-tracing

УДК 004.491.42: 004.492.3 DOI: 10.21681/2311-3456-2019-5-83-88

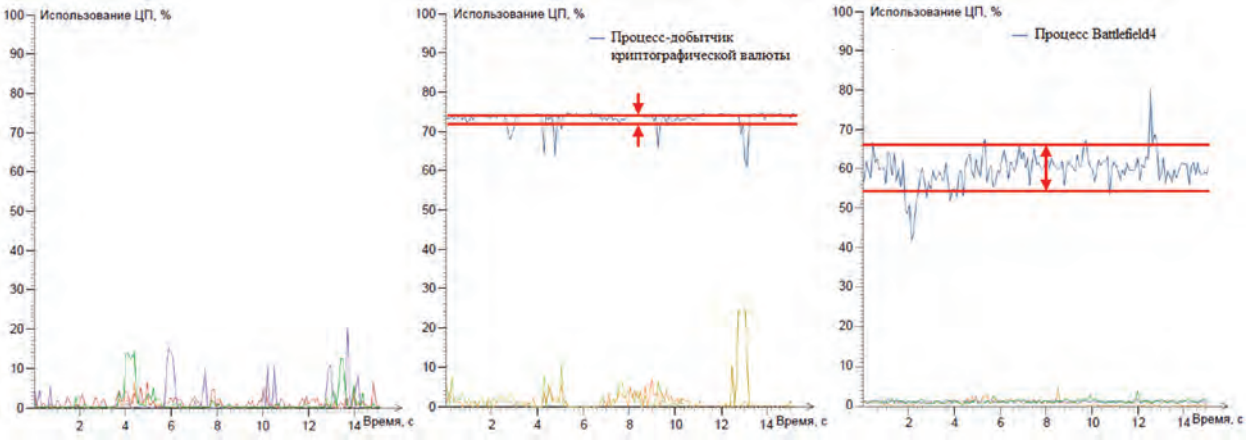


а) б) в)

Рисунок 1. Средняя доля использования ресурсов ЦП процессами ОС Windows: а) в которой не запущено ресурсоёмких приложений; б) в которой запущен криптомайнер; в) в которой запущена игра Battlefield 4

Анализ экспериментальных данных показал, что для криптомайнеров это значение не превосходит 3, в то время как для легитимных ресурсоёмких приложений значение среднего квадратичного отклонения оказывается больше 7 (рисунок 2).

повторяемости, определяемый как частное от общего количества всех вызванных системных функций к количеству вызываемых функций. Данный индикатор позволил выявлять работу криптомайнеров, реализованных в виде исполнимого сценария интернет обозревателя.



а) б) в)

Рисунок 2. Среднее квадратичное отклонение доли использования ЦП процессами ОС Windows: а) в которой не запущено ресурсоёмких приложений; б) в которой запущен криптомайнер; в) в которой запущена игра Battlefield 4

Эксперименты показали, что найденные три индикатора отлично обнаруживают программ криптомайнеры, реализованные в виде отдельного файла, но они не позволяют обнаружить криптомайнер в виде исполнимого сценария браузера.

Дальнейшие исследования были посвящены поиску соответствующего признака.

Известно, что криптомайнеры в цикле выполняют одни и те же вычисления.

Была выявлена следующая закономерность: функции, вызываемые криптомайнерами, часто повторяются, то есть при работе криптомайнера часто вызываются функции из фиксированного набора. Было предложено рассчитывать, так называемый, коэффициент

5.Алгоритм принятия решения о заражении

На основании данных, полученных в результате эксперимента по поиску признаков заражения, был разработан алгоритм обнаружения заражения криптомайнерами, основой которого является концепция дерева принятия решений (рисунок 3). Данный алгоритм выявляет программы, которые являются добытчиками криптографической валюты. Алгоритм способен выявлять как средства добычи криптографической валюты, реализованные в виде исполнимого файла ОС Windows, так и в виде исполнимого сценария интернет обозревателя.

На рисунке 3 введены следующие обозначения:

С — доля использования ЦП, %;

M — объём используемой ОП, Мб;

D — среднее квадратичное отклонение доли использования ЦП

R — коэффициент повторяемости.

Числа на рисунке — пороговые значения для каждого параметра, установленные в результате эксперимента.

ки), а вот объём используемой оперативной памяти большой, около 700 Мб.

- Последний этап принятия решения является самым быстрым и наименее ресурсозатратным: используется менее 1% ЦП и около 80 Мб оперативной памяти, длительность оказывается не больше секунды.

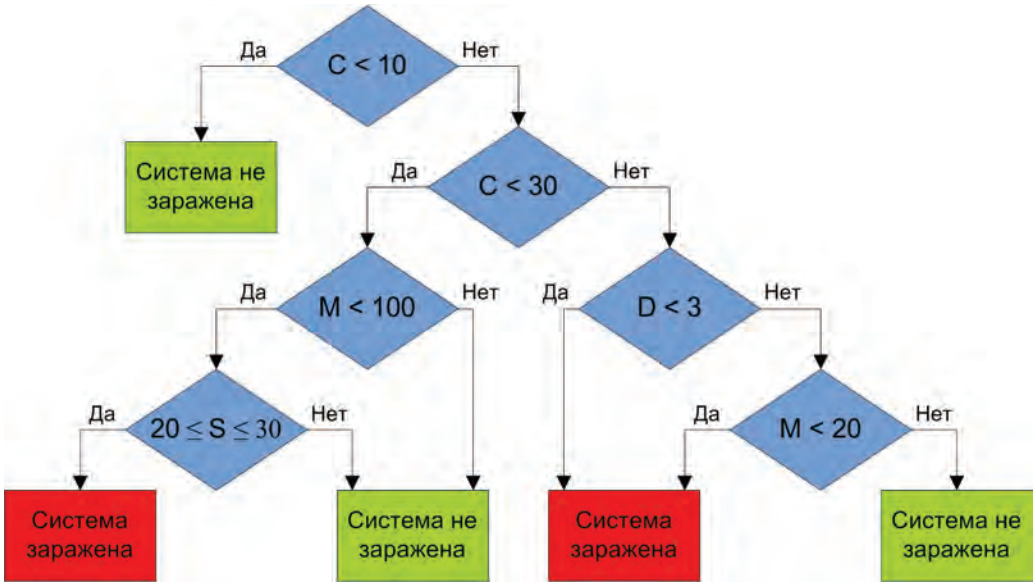


Рисунок 3. Схема работы алгоритма принятия решения о заражении криптомайнером

6.Характеристики реализованного средства обнаружения

Средство обнаружения криптомайнеров реализовано на языке C# в виде утилиты командной строки.

Работа средства включает в себя три основных этапа, повторяющихся циклически:

- сбор данных о работе всех запущенных процессов,
- расчёт значений выявленных индикаторов,
- применение к ним алгоритма принятия решения о заражении.

При завершении алгоритма с результатом «Система заражена» происходит уведомление пользователя.

Отдельно были рассчитаны временные характеристики, нагрузка на ЦП, а так же использование ОП на каждом этапе работы средства:

- Сбор данных продолжается 1 минуту, при этом используется около 5% ЦП и около 150 Мб оперативной памяти.
- На этапе выделения первых трёх параметров используется около 25% ЦП и 300 Мб оперативной памяти. Этот этап длится около полутора минут.
- Следующий этап — расчёт коэффициента повторяемости. Он продолжается около 3,5 минут. При этом ЦП практически не нагружается (3% загруз-

Общее время срабатывания реализованного средства составило около 5 минут.

7.Выводы

В результате работы удалось найти признаки, по которым возможно однозначное обнаружение работающих программных средств добычи криптографической валюты с низкой вероятностью ложного обнаружения. Реализованное программное средство обнаружения криптомайнеров может стать основой для развития новых средств защиты информации, занимающихся вопросами раннего обнаружения программных средств по добыче криптографической валюты.

С целью нивелировать значимое использование ресурсов ЦП, а также используемый объём ОП при работе предложенного средства обнаружения криптомайнеров, представляется возможным реализовать программно-аппаратный комплекс на основе устройства типа Raspberry Pi. В этом случае все ресурсоёмкие этапы, а именно, получение значений выделенных индикаторов, будут выполняться на устройстве типа Raspberry Pi, а данные между защищаемым компьютером и этим устройством будут передаваться по беспроводным каналам.

УДК 004.491.42: 004.492.3 DOI: 10.21681/2311-3456-2019-5-83-88

Литература

1. Cryptocurrency Mining Craze Going for Data Centers [Электронный ресурс]. Режим доступа к ресурсу: https://www.bitdefender.com/files/News/CaseStudies/study/196/Bitdefender-Whitepaper-Cryptocurrency-Mining-Craze-Going-for-Data-Centers-2018.pdf (дата обращения: 25.05.2018).
2. Cryptocurrency Mining Malware Trends & Threat Predictions [Электронный ресурс]. — Режим доступа к ресурсу: https://sucuri.net/documentation/Sucuri-eBook-Cryptomining-Malware.pdf (дата обращения: 15.05.2018).
3. Cryptocurrencies Outlook 2018 [Электронный ресурс]. Режим доступа к ресурсу: https://swissborg.com/files/swissborg-cryptocurrencies-outlook-2018.pdf (дата обращения: 19.05.2018).
4. Proliferation of Mining Malware Signals a Shift in Cybercriminal Operations [Электронный ресурс]. Режим доступа к ресурсу: https://go.recordedfuture.com/hubfs/reports/cta-2017-1011.pdf (дата обращения: 27.03.2018).
5. Microsoft Security Intelligence Report Cryptocurrency Mining Encounters [Электронный ресурс]. Режим доступа к ресурсу: https://www.microsoft.com/securityinsights/Crypto (дата обращения: 06.03.2019).
6. Czech A. Analysis of Malware Behavior: Type Classification using Machine Learning [Text] / A. Czech, S.S. Hansen, T.M.T. Larsen, J.M. Pedersen, R.S. Pirscoveanu, M. Stevanovic // International Conference on Cyber Situational Awareness, Data Analytics and Assessment. 2015.
7. Detection and Classifcation of Malicious Processes Using System Call Analysis [Электронный ресурс]. Режим доступа к ресурсу:
8. https://pdfs.semanticscholar.org/8060/eae74c98a66cfcc736f4fca61d46f4dbc1d4.pdf (дата обращения: 26.04.2018).
9. Alarif, A. PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior [Text] / A. Alarif, D. Fleck, T. Nykodym, A. Stavrou, A. Tokhtabayev // International Conference on Availability, Reliability and Security. 2013.
10. Li, R. A Behavior-Based Approach for Malware Detection [Text] / R. Li, R. Mosli, Y. Pan, B. Yuan // The International Federation for Information Processing. 2017.
11. Karim, A., Salleh, R., Khan, M. SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications [Электронный ресурс]. Режим доступа к ресурсу:
12. http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0150077&type=printable (дата обращения: 29.03.2018).
13. McAfee Labs Threats Report [Электронный ресурс]. Режим доступа к ресурсу: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf (дата обращения: 11.04.2019).

REVEALING CRYPTOCURRENCY MINING MALWARE VIA ETW

Kazakov O.A.[4], Korkin I.Y.[5]

Purpose: *early detection of unauthorized use of computing resources by cryptocurrency miners to prevent economic damage.*

Research methods: *experimental method to find out the behavioral features of computations done by cryptocurrency miners, Decision Tree Concept to develop the cryptocurrency miners infection decision algorithm.*

Results: *a behavioral analysis appeared to be a perspective method for purposes of cryptocurrency mining detection, behavioral features of computations performed by cryptocurrency miners was found out, a new approach for cryptocurrency miners detection was proposed, a cryptocurrency miners detection software was implemented.*

Keywords: *cryptocurrency, cryptocurrency mining detection, behavioral analysis, cryptocurrency mining behavioral features, ETW, WPR, WPA, C#.*

References

1. Cryptocurrency Mining Craze Going for Data Centers. Available at: https://www.bitdefender.com/files/News/CaseStudies/study/196/Bitdefender-Whitepaper-Cryptocurrency-Mining-Craze-Going-for-Data-Centers-2018.pdf (accessed 25.05.2018).
2. Cryptocurrency Mining Malware Trends & Threat Predictions. Available at: https://sucuri.net/documentation/Sucuri-eBook-Cryptomining-Malware.pdf (accessed 15.05.2018).
3. Cryptocurrencies Outlook 2018. Available at: https://swissborg.com/files/swissborg-cryptocurrencies-outlook-2018.pdf (accessed 19.05.2018).

4 Oleg Kazakov, NRNU MEPhI, student at the Department of Cryptology and Cybersecurity, Moscow, Russia. E-mail: oleg.al.kazakov@gmail.com

5 Igor Korkin, Ph.D, Lead Security Research Engineer, Special System Engineering Centre (ssec.ru), Moscow, Russia. E-mail: korkin@ssec.ru, igor.korkin@gmail.com

4. Proliferation of Mining Malware Signals a Shift in Cybercriminal Operations. — Available at: https://go.recordedfuture.com/hubfs/reports/cta-2017-1011.pdf (accessed 27.03.2018).
5. Microsoft Security Intelligence Report Cryptocurrency Mining Encounters. — Available at: https://www.microsoft.com/securityinsights/Crypto (accessed 06.03.2019).
6. Czech A. Analysis of Malware Behavior: Type Classification using Machine Learning [Text] / A. Czech, S.S. Hansen, T.M.T. Larsen, J.M. Pedersen, R.S. Pirscoveanu, M. Stevanovic // International Conference on Cyber Situational Awareness, Data Analytics and Assessment. 2015.
7. Detection and Classifcation of Malicious Processes Using System Call Analysis. Available at:
8. https://pdfs.semanticscholar.org/8060/eae74c98a66cfcc736f4fca61d46f4dbc1d4.pdf (accessed 26.04.2018).
9. Alarif, A. PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior [Text] / A. Alarif, D. Fleck, T. Nykodym, A. Stavrou, A. Tokhtabayev // International Conference on Availability, Reliability and Security. 2013.
10. Li, R. A Behavior-Based Approach for Malware Detection [Text] / R. Li, R. Mosli, Y. Pan, B. Yuan // The International Federation for Information Processing. 2017.
11. Karim, A., Salleh, R., Khan, M. SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications. Available at: http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0150077&type=printable (accessed 29.03.2018).
12. McAfee Labs Threats Report. Available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf (accessed: 11.04.2019).