УДК 327+004

DOI: 10.37468/2307-1400-2021-1-111-116

МУЦЕНЕК ВИТУС ЕВГЕНЬЕВИЧ

КАНАЛЫ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ В КОНТЕКСТЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

АННОТАЦИЯ

В статье рассматриваются разрушительные программные воздействия как частный случай вредоносного программного обеспечения, исторические аспекты рассмотрения подобных вредоносных программ в качестве оружия, современные тенденции использования и развития разрушительных программных воздействий.

Ключевые слова: информационная безопасность, разрушительное программное воздействие, вредоносное программное обеспечение.

MUTSENEK V. E.

DESTRUCTIVE SOFTWARE IMPACTS IN THE CONTEXT OF INFORMATION CONFRONTATION

ABSTRACT

The article covers destructive programs as a kind of malware, historical aspects of weaponization of such malware, contemporary tendencies of use and development of destructive programs.

Keywords: information security, destructive program impact, malware.

Термин «разрушающее программное воздействие» (РПВ) в российской нормативно-правовой базе в области информационной безопасности восходит к документам Государственной технической комиссии. Там РПВ впервые были определены как «изменение состояния АС, вызванное выполнением кода специально созданного программного субъекта или совокупности таких субъектов не обладающих свойством репликации», основным термином для таких воздействий предлагалось считать «вирусоподобное воздействие»[1]. Термин в форме «разрушающее программное воздействие», по сравнению с термином «вирусоподобное воздействие», реже упоминается в современном корпусе отраслевых стандартов и нормативно-правовых документов. К сожалению, систематически, в научных трудах и даже учебных материалах, смысл изначального определения РПВ оказывается утрачен. Более того, смысловая нагрузка терминов «вирусоподобное воздействие» и «разрушительное программное воздействие» не позволяет чётко объединить их к одному и тому же классу вредоносного программного обеспечения.

Проиллюстрируем вышесказанное. Авторы учебно-методического пособия [1] ошибочно наделили разрушающее программное воздействие «способностью к самодублированию,

1 Руководящий документ ГТК РФ «Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов» (проект, текст доступен по URL http://www.profinfo.ru/biblio/antivir.rtf, в том числе через Internet Wayback Machine http://archive.org/web; по утверждению экспертов форума itsec.ru, проект введён в действие не был: https://lib.itsec.ru/forum.php?sub=6711&from=10)

в том числе созданию модифицированных своих копий». В этом утверждении они ссылаются на другой источник, в котором, однако же, термин РПВ не употребляется, а приписанные ему свойства отнесены к термину «программа с потенциально опасными последствиями» [2]. И уже именно этот термин включен в Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных[2] как синоним термина «вредоносная программа» (напрямую он там не упоминается, однако возможности вредоносной программы сформулированы идентичным образом). В своей статье [3] Е.Б. Дроботун, ссылаясь на вышеупомянутое учебно-методическое пособие, так же наделяет РПВ функцией самодублирования.

Даже если не принимать во внимание неопределённость относительно первоисточника термина РПВ, очевидно, что не все вредоносные программы можно отнести к компьютерным вирусам, и не все компьютерные вирусы способны воздействовать на целостность и доступность информации, то есть осуществлять разрушающее действие. Наличие же или отсутствие механизма самодублирования у РПВ нельзя считать значительным определяющим признаком.

Справедливо будет отметить, что противоположные, временами столь же противоречащие очевидному, точки зрения на РПВ существуют и среди зарубежных специалистов. Так, в австралийской программе подготовки персонала ICASAS206A[3] к РПВ (*destructive software*) относят файловые вирусы, перехватчики клавиатуры, макровирусы, инструменты удалённого управления, шпионское программное обеспечение, вирусы системной области, троянские программы и черви. Однако, как уже говорилось, не все представители этих категорий программ могут приводить к ущербу целостности и конфиденциальности атакуемого ресурса. Поэтому в дальнейшем будем придерживаться определения РПВ, данного компанией IBM: «Разрушающая вредоносная программа – вредоносная программа с возможностью приведения затрагиваемых систем в неработоспособное состояние, требующее восстановления. Большинство вариантов РПВ причиняют разрушения через удаление, или стирание, файлов, критичных для способности операционной системы работать»[4] [4].

Специализированный новостной портал Cyber Security Intelligence, цитируя документы IBM X-Force и используя также иные источники информации, относит к недавним примерам РПВ вредоносные программы, предположительно созданные в интересах противоборствующих государств, такие как Stuxnet, Shamoon и Dark Seoul, а также вредоносные программы, создаваемые компьютерными преступниками, такие как LockerGoga и MegaCortex [5].

Особенностями Stuxnet, позволяющими отнести его к РПВ, являются заражение системы управления технологическими процессами Siemens Simatic Step7 с последующим выполнением модификации PLC-кода[5] на контроллерах Siemens с целью деструктивного воздействия на физическое оборудование. Его функционирование давно подробно изучено. Ориентированность на узкий ассортимент конфигураций АСУ ТП может свидетельствовать об использовании Stuxnet в качестве инструмента противоборства в киберпространстве. В своей работе [6] А.С. Марков и А.А. Фадин группируют вредоносное ПО, используемое для противостояния в киберпространстве в категорию «целенаправленная вредоносная программа» (ЦВП), и на примере Stuxnet иллюстрируют ту часть ассортимента ЦВП, которая предназначена для деструктивных действий. Вторым направлением противоборства в кибер-

2 утв. Заместителем директора ФСТЭК России 15 февраля 2008 г.

3 ICASAS206A Detect and protect from spam and destructive software. - Innovation and Business Skills Australia, 2012.

4 В оригинале - Destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution. Most destructive malware variants cause destruction through the deletion, or wiping, of files that are critical to the operating system's ability to run.

5 IProgrammable Logic Controller

пространстве авторы обозначают разведывательное. Авторы утверждают, что «Stuxnet является первым широко известным программным средством, имеющим точечную целевую функцию компрометации конкретной конфигурации АСУ ТП» [6].

По известным сведениям, Shamoon комбинирует разведывательные действия с разрушающими воздействиями (перезаписывание файлов «мусорными» фрагментами и модификацией главной загрузочной записи через официальный драйвер EldoS Raw Disk). Это целенаправленная вредоносная программа. Однако некачественность подготовки атаки, выраженная в неработоспособности части применяемых модулей, может свидетельствовать о том, что ресурсы стороны, стоявшей за созданием модуля, были существенно ограничены. В то время как ответственность за применение РПВ взяла на себя хакерская группа The Cutting Sword of Justice, нет явных доказательств связи авторов РПВ и самой атаки с каким-либо правительством. США возложили ответственность за атаку на правительство Ирана, которое в свою очередь отрицало причастность и настаивало на международном расследовании атаки [7].

Ответственность за применение РПВ Dark Seoul, так же сочетавшего разведывательные действия с перезаписыванием секторов на жёстких дисках «мусорными» фрагментами, взяла хакерская группа NewRomanic Cyber Army Team. Согласно выводам HP Security, к атакам была причастна также группа Whois Team. По утверждению аналитиков компании McAfee, атаке Dark Seoul предшествовали таргетированные фишинговые атаки, связанные с ведением военной разведки против Южной Кореи. Позже, аналитики CrowdStrike и Федерального бюро расследований США атрибутировали атаки DarkSeoul северокорейским хакерам [8].

Ещё одним примером РПВ может являться вредоносное ПО NotPetya, названное так по причине схожести кода с вирусом-вымогателем Petya. В модифицированном коде функция расшифровки файлов была отключена. Ущерб компании Maersk от РПВ составил порядка трёхсот миллионов долларов США [9].

Приведенные примеры не являются единичными случаями использования РПВ, но возможно одними из самых известных. Несомненно, они не были первыми попытками применения вредоносного ПО в целях нанесения ущерба противнику. В частности, уже довольно долго существует термин «кибероружие». РПВ по способности наносить физический ущерб определённо может быть отнесено к кибероружию.

В статье [10] Омри Хайзлер иллюстрирует эволюцию применения вредоносного ПО противоборствующими сторонами с 1980 года по настоящее время, и в частности смены парадигм США по вопросам применения кибероружия, через доктрины «информационного оружия», «информационных операций» и «кибероружия».

Хайзлер приводит три исторических периода применения кибероружия. Первый, связанный с советской троянской программой «Яйцо кукушки» (*Cuckoo's Egg*) и вирусом Морриса, характеризовался малой вовлеченностью государств в противоборство в киберпространстве, позволить которое могли себе лишь сверхдержавы. Второй этап связан с операциями кибершпионажа второй половины 1990х годов, а также осознанием применимости вредоносного ПО силами международного терроризма. На этом этапе к сверхдержавам в возможностях по применению кибероружия присоединились менее значимые силы. На текущем третьем этапе, названном «милитаризацией», прогнозируется увеличение роли межправительственных соглашений для сдерживания применения кибероружия акторами-государствами в чересчур уязвимой кибернетической среде, в условиях когда возможностями по применению кибероружия стали обладать ещё больше государственных и негосударственных акторов [10].

В докладе на Международной конференции по кибероружию и безопасности ICCWS 2018 доктор Чак Исттом констатирует наличие двух противоположных точек зрения относительно применимости кибероружия. Некоторые экс-

перты являются сторонниками недопущения дальнейшего распространения кибероружия, а кто-то даже утверждает, что на государства-акторы возложена этическая ответственность за активизацию работы по противодействию распространения кибероружия. Другие же настаивают на выработке правил ведения кибервойны, чтобы для специфических операций необходимо было выбирать соответствующее вредоносное ПО [11].

Участвовавший в той же конференции доктор Кори Хирш отметил: «Кибератаки, даже такие как Stuxnet и NotPetya, которые были очень целенаправленными, могут быть источником серьёзного сопутствующего урона, даже большего, чем урон от традиционного военного оружия, и радиус их поражения не связан с физической дистанцией до цели» [12].

Ещё одной тенденцией, связанной с возможностью неограниченного тиражирования информации, является повторное использование вредоносного кода, созданного ранее, в целях ведения войны в киберпространстве. Вне зависимости от того, кто является автором вредоносного кода, этот код может быть изучен, модифицирован и применён против новых целей уже другими акторами (причём в некоторых случаях даже без доступа к исходным текстам).

В работе [13], представленной на 10 международной конференции по киберконфликтам CyCon X, приводятся общие сведения о технологии переоснащения вредоносного программного обеспечения. Рассматриваются действия независимого неопределённого актора (в качестве такового могут оказаться как государства, так и негосударственные структуры, преступные элементы, взломщики-одиночки). Личность актора, модифицирующего кибероружие, в контексте исследования не важна. Авторы рассмотрели несколько стратегий поведения по переоснащению образцов вредоносных программ, актуальных на 2017 год. В частности, основными стратегиями являются подмена подсистемы управления и подмена «полезной нагрузки».

Подмена подсистемы управления возможна за счёт того, что авторы вредоносного кода пользуются шаблонными технологиями построения этих подсистем и склонны к повторному использованию кода. Отмечается, что этим способом могут воспользоваться злоумышленники со средним потенциалом. Подмена «полезной нагрузки» применяется в случаях, когда злоумышленник уже обладает работоспособными средствами доставки, либо временные ограничения не позволяют провести полноценную подмену подсистемы управления, либо когда цель операции – разрушающее воздействие.

Так или иначе, отмечают К.Подинс и К. Герс, повторное использвание вредоносного кода влечёт невозможность точного определения источника атаки (признаки, характерные для специфических источников, играют всё меньшую роль). В качестве дополнительных факторов риска называется рост числа операций под «чужим флагом», негативное влияние на дипломатические отношения.

Поскольку проблемам вредоносного ПО посвящено значительное количество докладов и публикаций, наверняка в тех, что остались за границами обсуждения, в какой-то степени раскрываются и вопросы, связанные с РПВ. Однако уже на основе того немногого, что послужило основой для написания данной статьи, можно сделать следующие выводы.

Кибероружие, включающее в себя как обычные компьютерные вирусы и программы для несанкционированного получения информации, так и средства, способные вызвать отказ компьютерных систем, сетей и АСУ ТП, не является чем-то новым, пришедшим в мир информационных технологий в XXI веке. На протяжении длительной истории информационного противоборства все заинтересованные стороны так или иначе участвовали в его разработке и могли санкционировать применение. Текущая ситуация характеризуется потерей контроля над распространением этого вида оружия.

Терминология в области вредоносного ПО, и в частности РПВ, нуждается в упорядочивании. Разрушительная природа этого вида вредонос-

ных программ, включая сопутствующий ущерб от их применения, должна быть определяющим фактором для их выделения в отдельную группу. Это позволит вплотную заняться гармонизацией международного права в вопросах нераспространения и неприменения РПВ, основываясь на понятном всем заинтересованным сторонам терминологическом аппарате коммуникации.

Совместные усилия всех заинтересованных сторон должны способствовать снижению напряженности, как создаваемой в результате инцидентов с применением РПВ, так и влекущей к применению таких средств. Возможно, если бы вредоносные программы были по своим характеристикам аналогичны традиционному оружию, для сдерживания было бы достаточно условиться о правилах применения. Однако способность любых акторов, даже не имеющих значительных ресурсов, к переоснащению РПВ, создающая угрозу неправильного определения источника воздействия и негативно влияющая на международные отношения, является сигналом к тому, что верным курсом стал бы отказ от применения кибероружия.

Список литературы

1. Разрушающие программные воздействия: Учебно-методическое пособие / А.Б. Вавренюк, Н.П. Васильев, Е.В. Вельмякина, Д.В. Гуров, М.А. Иванов, И.В. Матвейчиков, Н.А. Мацук, Д.М. Михайлов, Л.И. Шустова; под ред. М.А. Иванова. – М.: НИЯУ МИФИ, 2011. – 328 с.
2. *Гриняев С.Н.* Интеллектуальное противодействие информационному оружию. – М.: Синтег, 1999. – 134 с.
3. *Дроботун Е.Б.* Синтез систем защиты автоматизированных систем управления от разрушающих программных воздействий // Программные продукты и системы. – 2016. – № 3. – с.51–59.
4. Противодействие разрушающим вредоносным программам (на англ. языке) / Combating Destructive Malware [Электронный ресурс]. – Режим доступа: https://www.ibm.com/downloads/cas/XZGZLRVD (дата обращения 20.12.2019).
5. IBM X Force анализируют разрушающую способность вредоносного программного обеспечения (на англ. языке) / IBM X Force Dissect The Destructive Power Of Malware // Cyber Security Intelligence [Электронный ресурс]. – Режим доступа: https://www.cybersecurityintelligence.com/blog/ibm-x-force-dissect-the-destructive-power-of-malware--4438.html (дата обращения 20.12.2019)
6. *Марков А. С., Фадин А. А.* Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. №1. URL: https://cyberleninka.ru/article/n/organizatsionno-tehnicheskie-problemy-zaschity-ot-tselevyh-vredonosnyh-programm-tipa-stuxnet (дата обращения: 20.12.2019).
7. Shamoon – что это было? [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/159049/ (дата обращения 19.12.2019).
8. *Кребс Б.* Кейс о роли КНДР во взломе Sony (на англ. языке) / The Case for N. Korea's Role in Sony Hack // Krebs On Security [Электронный ресурс]. – Режим доступа: https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack (дата обращения 19.12.2019).
9. *Тершуков Д.А.* Анализ современных угроз информационной безопасности // NBI-technologies. – 2018. – №3. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (дата обращения: 15.03.2020).
10. *Хайзлер О.* История кибероружия США: последствия для современных структур кибероперациий и выработки политик. (на англ. яз.) / Omry Haizler, The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking // Cyber, Intelligence, and Security. – Volume 1 – No. 1 – January 2017. – pp. 33 – 45.
11. *Исттом Ч.* Роль поставленного на вооружение вредоносного ПО в кибер-конфликте и шпионаже (на англ. яз) / Chuck Easttom, The Role of Weaponized Malware in Cyber Conflict and Espionage //// 13th International Conference on Cyber Warfare and Security (ICCWS 2018). – Sonning Common: Academic Conferences and Publishing International Ltd., 2018. – pp. 191–199.

12. *Хирш К.* Результаты сопутствующего урона кибероружия велики, несмотря на целенаправленность (на англ. Языке) / Corey Hirsch. Collateral Damage Outcomes are Prominent in Cyber Warfare, Despite Targeting // 13th International Conference on Cyber Warfare and Security (ICCWS 2018). – Sonning Common: Academic Conferences and Publishing International Ltd., 2018. – pp. 281–286.

13. *Подинс К., Герс К.* Лампа Алладина: похищение и повторное использование вредоносного кода (на англ. яз) / Kārlis Podiņš, Kenneth Geers Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code // 2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. – NATO CCD COE Publications, Tallinn, 2018. – pp. 187–202.

Статья поступила в редакцию 30 сентября 2020 г.
Принята к публикации 26 февраля 2021 г.

Ссылка для цитирования: Муценек В.Е. Каналы разрушающих программных воздействий в контексте информационного противоборства // Национальная безопасность и стратегическое планирование. 2021. № 1(33). С. 111-116. DOI: https://doi.org/10.37468/2307-1400-2021-1-111-116