Буян С. Донгак
Томский государственный университет систем управления и радиоэлектроники, ул. Ленина, д. 40, г. Томск, 634050, Россия
e-mail: d_n_buyan@list.ru, https://orcid.org/0000-0002-7889-0264

МОНИТОРИНГ СЕТЕВОЙ АКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ ОРГАНИЗАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.2.06

Аннотация. В статье рассмотрен вопрос мониторинга сетевой активности рабочих компьютеров сотрудников для обеспечения информационной безопасности организации от внешних угроз, связанных с использованием аппаратного и программного обеспечения иностранного производства, в том числе и информационными сервисами, которые собирают разного рода информацию о пользователях сети Интернет. Показаны основные проблемы, возникающие в процессе выполнения анализа защищенности организации в сфере информационной безопасности (далее – ИБ). Приведен краткий обзор существующих инструментальных решений мониторинга сетевого трафика. Проведен эксперимент в использовании аппаратных и программных средств иностранного производства в организации. Эксперимент направлен на выявление негативных факторов, влияющих на информационную безопасность. Представлены результаты эксперимента. Сделаны выводы о недостатках методов и средств информационной защиты, а также рассмотрен вопрос оптимального соотношения использования инструментария фильтрации сетевого трафика.

Ключевые слова: межсетевой экран, мониторинг трафика, сетевая активность, информационная безопасность.

Для цитирования. ДОНГАК, Буян С.. МОНИТОРИНГ СЕТЕВОЙ АКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ ОРГАНИЗАЦИИ. Безопасность информационных технологий, [S.l.], n. 2, p. 71-79, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1111>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.06.

Buyan S. Dongak
Tomsk state University of control systems and Radioelectronics, Lenina str., 40, Tomsk, 634050, Russia
e-mail: d_n_buyan@list.ru, https://orcid.org/0000-0002-7889-0264

Monitoring of network activity of the employees automated workplaces

DOI: http://dx.doi.org/10.26583/bit.2018.2.06

Abstract. The article addresses the issue of monitoring of the network activity of employee's computers in order to ensure information security of the organization from external threats caused by the use of hardware and software of foreign origin, including services collecting all kinds of information about Internet users. The major problems arising in the process of analysis of the security of the organization in the field of information security are discussed. A brief overview of existing network traffic monitoring tool solutions is given. The experiment with the use of the foreign hardware and software in the organization was carried on. The experiment is aimed at identifying negative factors affecting the information security. The results of the experiment are presented. Finally the conclusions about the shortcomings of methods and means of information protection are made, as well as optimal ways to use the tools for the network traffic filtering are addressed.

Keywords: firewall, traffic monitoring, network activity, information security.

For citation. DONGAK, Buyan S.. Monitoring of network activity of the employees automated workplaces. IT Security (Russia), [S.l.], n. 2, p. 71-79, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1111>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.06.

Введение

Развитие информационных технологий в настоящее время обеспечивает повышение качества жизни людей. Сегодня невозможно представить мир без сотовых телефонов, Интернета, информационных систем, которые разработаны с основной целью – облегчить нашу жизнь, сделать ее комфортной и безопасной. Однако, существует и ряд вопросов, которые необходимо решить для их нормального функционирования. Основным и наиболее важным вопросом при создании и эксплуатации информационных систем является обеспечение информационной безопасности. Информационная безопасность достигается путем применения последовательных, взаимосвязанных действий, направленных на обеспечение конфиденциальности, целостности и доступности информации в информационных системах. В России данное направление с каждым годом усовершенствуется [1]: меняется законодательная база, нормотворческая и методическая база защиты информации, модернизируются системы и комплексы защиты информации, но несмотря на это, существует основная проблема, аппаратные и программные обеспечения иностранного производства, которые используются в нуждах, как в государственном, так и в частном секторе. К ней относится распространенность иностранного аппаратного и программного обеспечения [2]. Это и неудивительно — ведь российский рынок, в буквальном смысле, наводнен продукцией западных разработчиков. В условиях напряженной геополитической обстановки и открытой информационной войны, ряд российских экспертов в области информационной безопасности считают, что главной угрозой информационной безопасности является использование иностранного программного обеспечения с закрытым, либо сложным, либо постоянно обновляющимся программным кодом, отследить изменения которого невозможно в режиме реального времени [3].

В данной статье приведен эксперимент в использовании аппаратных и программных средств иностранного производства в нуждах организации, одной из целей которой является защита коммерческой тайны. Эксперимент направлен на выявление негативных факторов, влияющих на информационную безопасность.

Задача: Мониторинг сетевой активности автоматизированных рабочих мест сотрудников организации, находящихся внутри (NAT) защищаемой сети с использованием межсетевого экрана (МЭ) на внешней границе сети Интернет, а также оценка эффективности правил фильтрации сетевого трафика.

Объект исследования: Автоматизированные рабочие места сотрудников организации, на которых используются прикладные программные продукты, работающие с сетью Интернет.

Предмет исследования: Принцип работы фоновых прикладных программных продуктов, использующихся на автоматизированных рабочих местах сотрудников организации, в том числе и зарубежного производства, во время обновления самого себя (собственного кода) с использованием сети Интернет, а также сетевая активность интернет-браузера, использующего веб-ресурсы, предназначенные для сбора информации о пользователях сети Интернет.

Обзор методик и существующих инструментальных решений мониторинга сетевого трафика

На сегодняшний день наиболее актуальна проблема обеспечения информационной безопасности организации от внутренних угроз, связанных с

действиями собственных сотрудников, и от внешних угроз, в том числе при использовании аппаратных и программных средств иностранного производства. Данная проблематика изучается многими исследователями в области защиты информации. Так, например, исследователями рассматриваются различные варианты систем мониторинга действий персонала [4], в том числе предлагается методика мониторинга сетевой активности персонала на основе прокси-серверов и анализа URL-адресов запросов [5]. Иной подход предлагается в методике анализа существующих классификаций инсайдерских угроз [6] и злоумышленников [7] и [8].

Анализ различных методик выявления угроз позволяет сделать вывод об отсутствии в настоящее время всеобъемлющей и последовательной классификации информационных угроз, в виду отсутствия общего для исследователей терминологического поля. По этой причине в работе [9] предложен метод классификации угроз инсайдеров с использованием кластеризации инцидентов. Для определения критериев классификации и критериев оценки результатов был проведен анализ собранных статистических данных. На основе кластеризации инцидентов была разработана классификация угроз инсайдерской безопасности. В настоящее время инциденты ИБ стали не только более многочисленными и разнообразными, но и более разрушительными, так как превентивные средства управления и контроля на основе результатов оценки рисков ИБ снижают большинство, но не все инциденты ИБ [10]. Таким образом, для быстрого обнаружения инцидентов ИБ, необходима система управления инцидентами ИБ, сводящая к минимуму потери информации [11], смягчающая уязвимости, которые были использованы [12], и восстанавливающая ИТ-инфраструктуру организации и ее услуги. Такие системы могут быть реализованы на основе центра управления безопасностью (ЦУБ). На основе анализа проведенных исследований представлены миссия и основные функции ЦУБ. Автором [13] предложена классификация ЦУБ и основные показатели инцидентов ИБ. Определены серьезные ограничения первого поколения ЦУБ.

Для выявление негативных факторов, влияющих на информационную безопасность, по мнению ряда исследователей [14], необходимо точно определить возможности нарушителя, которые он может использовать для разработки и проведения атак. Модель нарушителя является важной частью информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывают различные методы классификации нарушителей, меж тем многие специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы [15], так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. Несмотря на то, что многие модели имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось.

Что касается инструментальных решений, то многими иностранными и отечественными компаниями, специализирующимися на мониторинге и анализе сетевого трафика, разработаны и предложены различные программные и программно-аппаратные инструменты [16]. Эти инструменты различаются, прежде всего, по уровню и совершенству используемых математических методов, положенных в основу процедур анализа трафика. В зависимости от этого, они обладают разными возможностями [17], например, анализаторы протоколов или сетевые сниферы, которые позволяют захватывать трафик локальных сетей, представлять его в удобном

для анализа виде, но, собственно, анализ данных оставляют администратору. Или, например, маршрутизаторы, поддерживающие протокол NetFlow [18], собирающие обобщенные данные о трафике глобальных сетей, передавая его для анализа программным системам, которые автоматизируют поиск атак и угроз. Системы обнаружения вторжений специализируются на автоматическом распознавании вторжений и угроз в прослушиваемом трафике локальных сетей [19].

Несмотря на имеющиеся инструментальные решения фильтрации сетевого трафика и мониторинга, любой новый тип атаки (особенно на 80 порт) имеет все шансы «просочиться» через межсетевые экраны и достичь внутренних серверов защищаемой сети. Обнаружить следы атак, которые смогли преодолеть барьер межсетевого экрана, можно путем мониторинга и аудита сетевого трафика.

Компании, специализирующие в области сетевой безопасности, предлагают комплексные инструментальные решения класса SIEM для управления событиями и информацией ИБ с целью выявления инцидентов в режиме реального времени и сетевых сканеров, работающих на эвристическом анализе сетевого трафика.

1. Экспериментальная часть

Вышеупомянутые работы авторов, без сомнения, минимизируют ущерб информационным системам. Остается еще одно направление, которое волнует многих специалистов в области информационной безопасности. Это использование иностранного программного обеспечения с закрытым, либо сложным, либо постоянно обновляющимся программным кодом, отследить изменения, которого невозможно в режиме реального времени [20]. Были проведены исследования, целью которых является изучение принципа функционирования фоновых прикладных программных продуктов на автоматизированных рабочих местах сотрудников организации, в том числе и зарубежного производства, во время обновления программного кода с использованием сети Интернет, а также сетевая активность интернет-браузера, использующего веб-ресурсы, предназначенные для сбора информации о пользователях сети Интернет.

Несмотря на то, что в данной организации выполняются все необходимые организационно-технические требования безопасности информации, и все информационные системы имеют аттестаты соответствия требованиям безопасности конфиденциальной информации, исследование показало ниже представленные результаты.

1.1. Ход эксперимента

В результате проведения ряда аудитов трафика на информационную безопасность выявлена особенность сетевой активности, связанная с работой иностранного программного обеспечениями. Так, современные процессоры Intel на АРМах пользователей позволяют использовать отладочный интерфейс через доступный на многих платформах порт USB 3.0 для получения полного контроля над системой, что дает возможность проводить атаки, которые не отслеживаются современными системами безопасности. Также, веб-ресурсы, использующие для работы программные продукты иностранного производства, являются самым популярным объектом для современных кибератак. Также, были зафиксированы скачковые увеличения исходящего интернет-трафика от пользовательских компьютеров. Такие скачки происходили во время политических мероприятий (например, в период выборов, общественно-значимых мероприятий). В результате исследования сетевого трафика, было выявлено, что ряд прикладных программных продуктов, в том числе и зарубежного производства (Adobe Reader, Cleaner), используя технические протоколы и порты (порты для обновлений, порт 80, 445), выгружают

внушительный объем преобразованной информации на различные зарубежные сайты и сервисы. Причем, выгрузка идет не с каждого компьютера одновременно, а используется некий последовательный алгоритм, который не вызывает подозрения у межсетевых экранов, администраторов сети и пользователей: например, в ночное время, когда пользователь находится не на рабочем месте или во время обеденного перерыва (см. рис. 1).

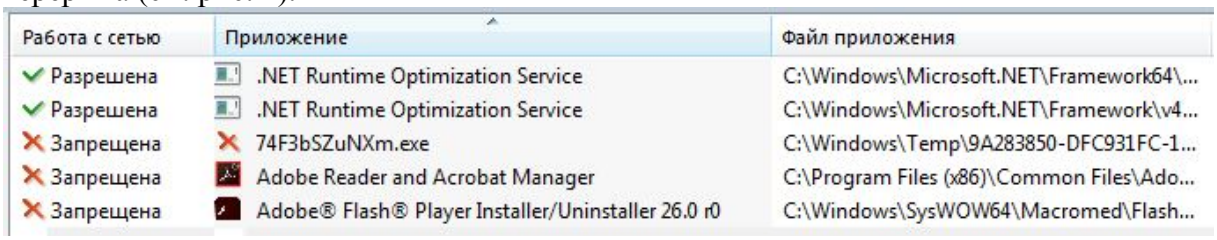

Рис. 1. Работа с сетью приложения была настроена на «запрещена» с помощью средства контроля активности приложений
(Fig. 1. Working with the application network was configured to "disabled" using the application activity monitoring tool)

Программное обеспечение предназначено для работы с офисными файлами, для чтения файлов в формате .pdf. Возникает вопрос, что может так долго и постоянно обновляться в программном продукте? (см. рис. 2).

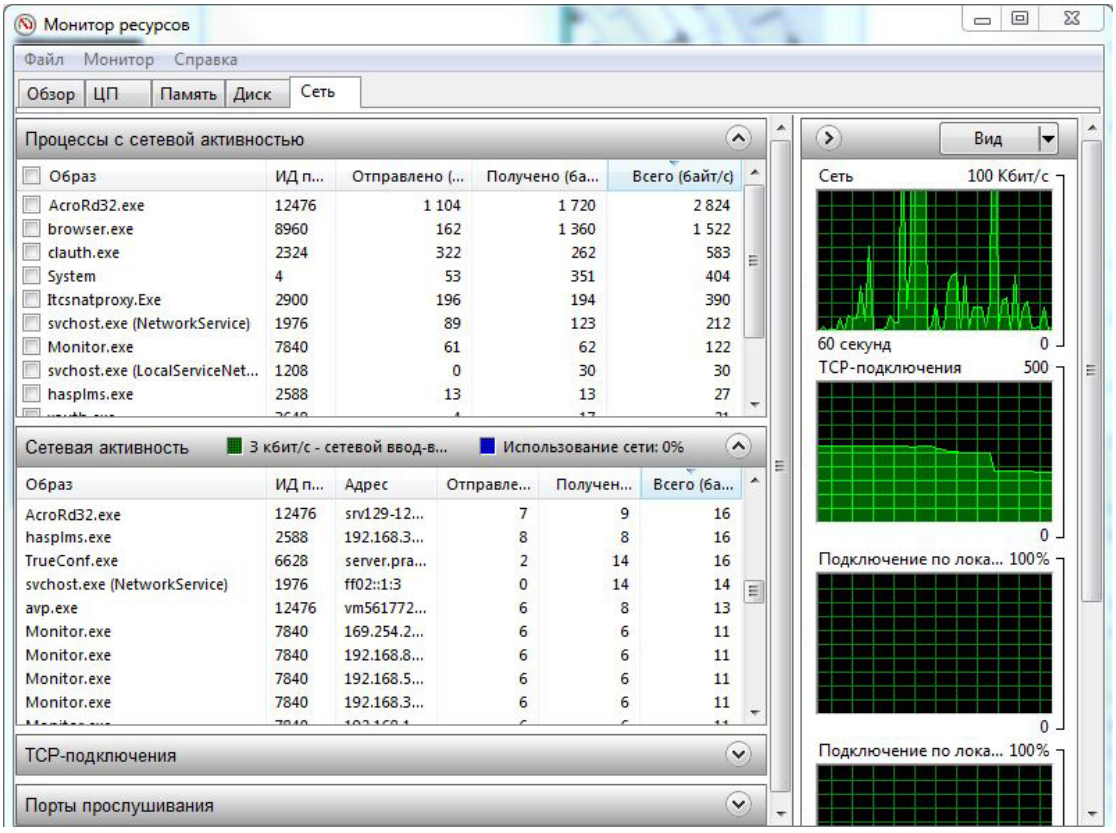

Рис. 2. Сетевая активность программного продукта AcroRd32.exe в режиме онлайн
(Fig. 2. Network activity software product AcroRd32.exe online)

Работающих в фоновом режиме программных продуктов очень много, только опытному пользователю видно, чем именно занимаются программные службы. Но не у всех пользователей данной организации наблюдаются аномалии сетевого трафика. В основном, жалобы на медленную работу компьютеров поступали от сотрудников, занимающих руководящие должности. Возникает дополнительный вопрос: каким

образом ПО распознает занимаемую должность пользователя? Ответ на этот вопрос будет подробно рассмотрен в дальнейших публикациях. На сегодняшний момент существует ряд гипотез, которые требуют экспериментальной проверки. Одной из самых вероятностных гипотез является способность распознавания должности пользователя по низкочастотным поисковым запросам в облачных поисковых системах, которые делают пользователи, занимающие руководящие посты в организации, в том числе специалисты в области информационной безопасности.

Также существует угроза того, что ПО «распознает» пользователя по анализу информации с контроллера домена сети организации, так как в доменной сети каждый сотрудник имеет свою учетную запись и определенное место (приоритет) в структуре сети. Системный администратор вносит данные сотрудника в контроллер домена, вплоть с указанием должностей и, таким образом, происходит учет и идентификация каждого пользователя, в том числе их сетевая активность в сети Интернет.

Для подтверждения гипотезы о возможности распознавания пользователя по учетной записи и временным отклонениям от нормы в работе проведен следующий эксперимент:

1) Зарегистрирован новый ПК в сети организации и создана локальная учетная запись – user-1;
2) Установлен весь необходимый офисный набор ПО для работы;
3) Результаты мониторинга сетевой активности «user-1» в течении первого месяца не показали каких-либо отклонений от нормы в дневное и ночное время работы. Сетевая активность была не выше средней активности каждого пользователя (см. рис. 3).

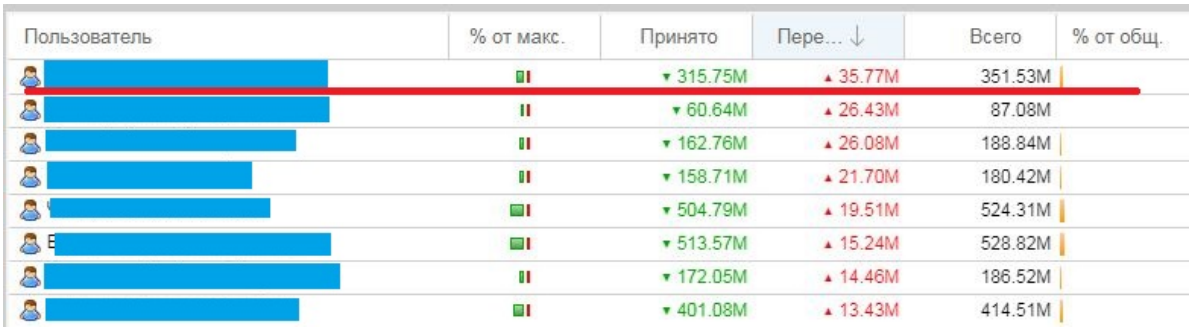

Рис. 3. Сетевая активность пользователя "user-1», в рабочее время
(Fig. 3. Network activity of user "user-1", during working hours)

4) Были внесены изменения в учетную запись «user-1» (была дописана высокая должность) в контроллере домена, работающего на базе Windows 2012 Server.

Результаты ночной сетевой активности данного пользователя значительно изменились (см. рис. 4).

Сетевой трафик в дневное (рабочее) время практически не меняется, но сильно меняются характеристики сетевого трафика в ночное время. Всего за одну ночь с 00:00 до 06:00 был зафиксирован 71 запрос на различные российские и зарубежные интернет-сервисы. При этом на компьютере были запущены: антивирусное программное обеспечение, офисные приложения и интернет-браузер Mozilla Firefox 12. На рисунке 4 показаны результаты запросов, которые исходят от зарубежных интернет-сервисов. Данные были получены из функционирующей в организации системы учета сетевого трафика сети Интернет на служебных автоматизированных рабочих местах. Выявление географии источников IP адресов осуществлялось в ручном режиме, с помощью интернет-сервиса http://2ip.ru/. В этом случае следует отметить, что разница входящего и исходящего трафика сильно отличается. Например, из рисунка 4 видно, что на первой

и второй строке находятся страны Европы (компания Akamai Technologies вх.-529 Мбит/с., исх.-538 Мбит/с и США вх.-1,79 Кбит/с и исх.-616 Мбит/с.).

Эта разница между входящим и исходящим трафиком ставит вопрос о том, какая именно информация (персональная, конфиденциальная, служебная) скачивается с ПК. И почему именно в ночное время.

При этом, несмотря на имеющиеся в организации многочисленные элементы систем защиты информации, не одна из них не подняла тревогу, т.к. это является открытым http трафиком, передающимся по 80-ту порту.

			Источник	Пользователь-1					
			Часы	00:00-06:00					
Страна	**Город**	**Компания**	**Ip-адрес или домен**	**Первое обращение**	**Количество соединений**	**% от макс. вх.**	**% от макс. исх.**	**Входящий трафик**	**Исходящий трафик**
	Европа	Akamai Technologies	2.20.255.64	25.08.2017 03:11	4			529	538
США	Маунтин-Вью	Google Inc. Ih-in-f139.1e100.r	64.233.161.139	25.08.2017 05:23	6			1.79 K	616
Норвегия	Осло	Opera Software AS	82.145.215.85	25.08.2017 00:38	8			7.24 K	3.47 K
США	Маунтин-Вью		173.194.32.134	25.08.2017 05:23	9			7.84 K	3.42 K
США	Маунтин-Вью		173.194.32.160	25.08.2017 00:23	3			6.68 K	3.11 K
Германия	okis.ru	Hetzner Online AG	188.40.66.5	25.08.2017 00:14	356	100%	3%	14.50 M	507.87 K
США	Маунтин-Вью		gvt1.com	25.08.2017 05:23	2			5.68 K	1.02 K
США	Маунтин-Вью		r6---sn-gvnuxaxjvh-v8cz.gvt1.cor	25.08.2017 05:23	1			4.14 K	685
США	Маунтин-Вью		redirector.gvt1.com	25.08.2017 05:23	1			1.54 K	364
Нидерланды		LeaseWeb Netherlands B.V	dnl-00.geo.kaspersky.com	25.08.2017 00:03	77	1%		190.33 K	17.18 K
Франция	Бонди	Customer LAN Network	dnl-01.geo.kaspersky.com	25.08.2017 02:05	17			20.59 K	3.67 K
Нидерланды		LeaseWeb Netherlands B.V	dnl-04.geo.kaspersky.com	25.08.2017 05:16	4			7.08 K	864
Нидерланды		LeaseWeb Netherlands B.V	dnl-05.geo.kaspersky.com	25.08.2017 04:56	2			3.54 K	432
Франция	Бонди	Customer LAN Network	dnl-06.geo.kaspersky.com	25.08.2017 03:36	8			12.39 K	1.67 K
Европа		Kaspersky Lab TLD	dnl-07.geo.kaspersky.com	25.08.2017 00:04	6			8.75 K	1.25 K
Британия		BBLZ9143	dnl-08.geo.kaspersky.com	25.08.2017 03:36	4			5.27 K	848
Британия		BBLZ9143	dnl-09.geo.kaspersky.com	25.08.2017 01:36	77			108.89 K	17.18 K
Европа		Kaspersky Lab TLD	dnl-10.geo.kaspersky.com	25.08.2017 01:36	14			21.15 K	2.92 K
Франция	Бонди	Customer LAN Network	dnl-14.geo.kaspersky.com	25.08.2017 04:06	4			6.18 K	856
Европа		Kaspersky Lab TLD	dnl-19.geo.kaspersky.com	25.08.2017 04:16	4			6.18 K	856
Германия	okis.ru	Hetzner Online AG	okis.ru	25.08.2017 00:14	557	93%	1%	13.58 M	238.71 K
Германия	okis.ru	Hetzner Online AG	surguul.okis.ru	25.08.2017 00:14	557	93%	1%	13.58 M	238.71 K
			windowsupdate.com	25.08.2017 03:11	1			317	286
			ctldl.windowsupdate.com	25.08.2017 03:11	1			317	286
Всего					**10569**			**43.11 M**	**5.92 M**

Рис. 4. Результаты ночной сетевой активности пользователя «user-1»
(Запросы отфильтрованы по иностранным сервисам)
(Fig. 4. Results of night network activity of the user-1
(Requests are filtered by foreign services))

Выводы

Проведенный эксперимент показал, что существует угроза утечки информации по техническим каналам. Утечка связана с распознаванием программными средствами общего назначения должностного положения пользователя на серверах под управлением Windows.

Таким образом, при использовании иностранного программного обеспечения со сложным, либо постоянно обновляющимся кодом существует вероятность полной информационной открытости рабочих мест сотрудников организации, в том числе угрозы массовой утечки служебной и конфиденциальной информации с ее первичной дифференциацией по должностному уровню пользователей ПК в организации.

Работа по выявлению негативных факторов информационной безопасности будет продолжена с акцентом на два направления:

1. Выявление факторов, провоцирующих ПО общего назначения на активное скачивание информации с ПК пользователя: изменения учетной записи, анализ отклонений от нормы во время работы ПК, действий пользователей с информацией на ПК, а также действий пользователей в облачных поисковых системах.
2. Расшифровка передаваемой с ПК исходящей информации.

В дальнейших исследованиях планируется постановка экспериментов и анализ полученной информации по указанным направлениям.

СПИСОК ЛИТЕРАТУРЫ:

1. Вестник Саратовской государственной юридической академии № 2 (115) – 2017 [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/v/setevye-informatsionnye-voyny-kak-faktor-ugrozy-globalnoy-bezopasnosti.
2. А.В. Царегородцев, М.М. Тараскин «Методы и средства защиты информации в государственном управлении. Учебное пособие. – Издательство «Проспект», 2017 – 193 с.
3. Шейн Харрис, «Кибервойна. Пятый театр военных действий» - Альпина нон-фикшн, 2015. – 392 с.
4. Лохин С.В., Семашко А.В., Егорова А.И. Система мониторинга сетевой активности персонала на основе прокси-сервера. Динамика сложных систем – XXI век. 2017. Том 11, №2. С. 25-29.
5. Лохин С.В., Семашко А.В. Мониторинг сетевой активности персонала в целях обеспечения информационной безопасности предприятия. Вопросы защиты информации. 2017., №2 (117). С. 53-57.
6. Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003.
7. Ходашинский И.А., Савчук М.В., Горбунов И.В., Мещеряков Р.В. Технология усиленной аутентификации пользователей информационных процессов. Доклады Томского государственного университета систем управления и радиоэлектроники. 2011 г., Т. 2. № 3. С. 236-248.
8. Garin E.V., Meshcheryakov R.V. METHOD FOR DETERMINATION OF THE SOCIAL GRAPH ORIENTATION BY THE ANALYSIS OF THE VERTICES VALENCE IN THE CONNECTIVITY COMPONENT. Вестник Южно-Уральского государственного университета. Серия: Математика. Механика. Физика. 2017. Т. 9. № 4. С. 5-12.
9. Зайцев А.С., Малюк А.А. Разработка классификации внутренних угроз информационной безопасности посредством кластеризации инцидентов. Безопасность информационных технологий. 2016., № 3. С. 20-33.
10. Cichonski P., Millar T., Grance T., Scarfone K. «NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide» August 2012.
11. Абросимов М.Б., Камил И.А., Разработка системы предотвращения вторжений с использованием параллельного программирования и системы отказоустойчивости. Безопасность информационных технологий. 2018., № 1 (25) С. 65-73.
12. Ходашинский И.А., Мещеряков Р.В., Горбунов И.В. Методы нечеткого извлечения знаний в задачах обнаружения вторжений. Вопросы защиты информации. 2012 г., № 1. С. 45-50.
13. Милославская Н.Г., Центры управления информационной безопасностью. Безопасность информационных технологий. 2016., № 4. С. 38-51.
14. Егошин Н.С., Конев А.А., Шелупанов А.А. Формирование модели нарушителя. Безопасность информационных технологий. 2017., № 4 (78) С. 19-26.
15. Мещеряков Р.В., Шелупанов А.А. Концептуальные вопросы информационной безопасности региона и подготовки кадров. Труды СПИИРАН. 2014. № 3 (34). С. 136-159.
16. Jean Y. Astier, Igor Y. Zhukov, Oleg N. Murashov, Alexey P. Bardin, A new OS architecture for IOT. Безопасность информационных технологий. 2018., № 1 (25) С. 19-33.
17. С.А. Бабин «Лаборатория хакера» - СПб.: БХВ-Петербург, 2016. – 240 с.: - ил. (Глазами хакера).
18. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – Спб.: Питер, 2016. – 992 с.: ил. – (Серия «Учебник для вузов).
19. Н. Скабцов «Аудит безопасности информационных систем» - СПб.: Питер, 2018. – 272 с.: ил. – (Серия «Библиотека программиста»).
20. Ерохин С.С., Мещеряков Р.В., Бондарчук С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта. Безопасность информационных технологий. 2007 г., № 4. С. 39-46.

REFERENCES:

[1] Bulletin of the Saratov state law Academy No. 2 (115) – 2017 [Electronic resource] access Mode: https://cyberleninka.ru/article/v/setevye-informatsionnye-voyny-kak-faktor-ugrozy-globalnoy-bezopasnosti. (in Russian).
[2] A. V. Tsaregorodtsev, M. M. Taraskin " Methods and means of information protection in public administration. Textbook. - Prospekt publishing house, 2017 - 193 p. (in Russian).
[3] Shane Harris, "The Cyberwar. The fifth theater of war " - Alpina non-fiction, 2015. - 392 sec. (in Russian).

[4] Lokhin, S. V., Semashko, A. V., Egorova A. I. System monitoring the network activity of the staff through a proxy server. Dynamics of complex systems – twenty-first century. 2017. Volume 11, No. 2. P. 25-29. (in Russian).
[5] Lokhin S. V., Semashko A.V. monitoring of network activity of the personnel for the purpose of ensuring information security of the enterprise. Information security issues. 2017., №2 (117). P. 53-57. (in Russian).
[6] Killcrece G., Kossakowski K.-P., Ruefle R., Zajicek M. Organizational Models for Computer Security Incident Response Teams. December 2003.
[7] Hodinski I. A., Savchuk M. V., Gorbunov I. V., Meshcheryakov R. V. Technology enhanced user authentication information processes. Reports of Tomsk state University of control systems and Radioelectronics. 2011, Vol.2. No. 3. P. 236-248. (in Russian).
[8] Garin E. V., Meshcheryakov R. V. METHOD FOR DETERMINATION OF THE SOCIAL GRAPH ORIENTATION BY THE ANALYSIS OF THE VALENCE VERTICES IN THE CONNECTIVITY COMPONENT. Bulletin of South Ural state University. Series: Mathematics. Mechanics. Physics. 2017. T. 9. No. 4. P. 5-12.
[9] Zaitsev, A. S.; Malyuk, A. A.. Development of information security insider threat classification using incident clustering. IT Security (Russia), [S.l.], v. 23, n. 3, p. 20-29, oct. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/14>. Date accessed: 30 may 2018. (in Russian).
[10] Cichonski, P., Millar, T., Grance, T., Scarfone K. "NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide," August 2012.
[11] Abrosimov, Mikhail B.; Kamil, Iehab A.. Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology. IT Security (Russia), [S.l.], v. 25, n. 1, p. 65-73, mar. 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1094>. Date accessed: 30 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.06. (in Russian).
[12] Miloslavskaya, N. G. Information Security Operations Centers. IT Security (Russia), [S.l.], v. 23, n. 4, p. 38-51, dec. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/257>. Date accessed: 30 may 2018.(in Russian).
[13] Egoshin, Nikolay S; Konev, Anton A; Shelupanov, Aleksander A. Building a model of infringer. IT Security (Russia), [S.l.], v. 24, n. 4, p. 19-26, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/273>. Date accessed: 30 may 2018. doi:http://dx.doi.org/10.26583/bit.2017.4.02.(in Russian).
[14] Mescheryakov R. V., Shelupanov A. A. Conceptual issues of information security in the region and training. Proceedings of SPIIRAS. 2014. No. 3 (34). P. 136-159.
[15] Astier, Jean Y. et al. A NEW OS ARCHITECTURE FOR IOT. IT Security (Russia), [S.l.], v. 25, n. 1, p. 19-33, mar. 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1090>. Date accessed: 30 may 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.02.
[16] S. A. Babin "hacker's Laboratory" - St. Petersburg.: BHV-Petersburg, 2016. - 240 p.: - ill. (Through the eyes of a hacker). (in Russian).
[17] Oliver W., Oliver N. Computer networks. Principles, technologies, protocols: Textbook for universities. 5th ed. – SPb.: Peter, 2016. - 992 p.: ill. (Series "Textbook for higher educational institutions). (in Russian).
[18] N. Skobtsov "Audit of information systems security" - SPb.: Peter, 2018. - 272 p.: ill. (Series "library of the programmer»). (in Russian).
[19] Erokhin S. S., Meshcheryakov R. V., Bondarchuk S. S. Models and methods for assessing information security and information security of the object. 2007, № 4. P. 39-46. (in Russian).

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.