ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ № ?(??), 2015, с.??—??

УДК 004.75

Рыжков С.Р., Фаткиева Р.Р.

Таксономия атак на облачную инфраструктуру по месту реализации атаки [1]

Аннотация. Представлен обзор таксономий атак на облачную инфраструктуру. Представлен обзор технологий отслеживания пользователя. Рассмотрена возможность применения технологии геометок, как инструмента контроля территориального перемещения данных на протяжении всего их жизненного цикла.

Ключевые слова и фразы: облака, облачные вычисления, периметр безопасности, геотегирование

Введение

Информационная система, построенная с использованием технологий облачных вычислений (далее ИСОТ), состоит из множества различных аппаратно–программных средств, поддерживающих функционирование виртуальной среды. Использование разнотипных средств, зачастую от разных производителей, может повлечь за собой не только сбои в работе виртуальной среды, но и множество различных атак на неё [1]. При этом процесс эволюции как программно–аппаратных средств, так и непосредственно информационной среды можно сравнить с биологической эволюцией: коэволюция атакующих – защищающихся приводит к тому, что для обеспечения безопасности обработки информации облачной инфраструктуры недостаточно установки какого–либо одного средства защиты информации. Из–за повышения вероятности преодоления систем защиты при получении несанкционированного доступа к управлению виртуальной средой возрастает значимость ряда

[1] (Рекомендована к публикации.... Поддержана...!)

процессов обеспечения информационной безопасности (ИБ). Важным условием для обеспечения ИБ ИСОТ является определение потенциального места проведения атаки с целью её предотвращения. Согласно представленному далее обзору, технология геометок описанная нами ранее [2], перспективна для реализации механизма контроля географического перемещения данных – геоконтроля. Геометки позволяют контролировать «частную собственность» в виртуальной среде.

1. Обзор таксономий атак на облачную инфраструктуру

Концепция геоконтроля представлена в работе [3]. Таксономия безопасности облачных вычислений рассматривается в свете количественного анализа актуальных проблем безопасности для облачных вычислений, которые зависят от архитектуры (Таблица 1). Базовая архитектурная классификация содержит сети, хосты, приложения, данные (их безопасность и хранение), управление безопасностью, идентификацией и доступом – все эти элементы напрямую связаны с инфраструктурой и архитектурой реализации облачных решений. Данная таксономия позволяет осуществлять детализированный контроль компонент виртуальной среды в совокупности с возможностями контроля географического перемещения данных:

Таблица 1. Таксономия по архитектурному признаку

Архитектура		
Сетевая безопасность	Безопасность передачи	Распределённая архитектура
	Брандмауэры	Изоляция виртуальных машин
	Конфигурация безопасности	протоколы
Интерфейсы	API	[illegible] виртуализации
	Административный интерфейс	Удалённый контроль ресурсов
	[illegible]	Использование служб
	Аутентификация	Доступ разрешён
Вирту-ализация	Изоляция [illegible]	Логическая
	[illegible]	Виртуализация
	Утечка данных	Конфиденциальность
	Идентификация ВМ	Различные процессы
	Атаки Кросс –ВМ	Кража криптоключа
		Общие
		Синхронизация
		Данные в
		Фильтрация
		Защита от DOS
		Адаптированные решения
		Системы
		Технологии
		Эффективность
		Динамические библиотеки
		Управление виртуальными
		Программный кол
		Развертывание
		Разработка
		Контроль доступа пользо-
		Конфигурации
		Использование ресурсов
		Типы аккаунтов
		Мультитенантность
		Физическая
		Закрытые решения
		Целостность
		Различные ресурсы
		Различные пользователи
		Захват ВМ

В [4] отмечается, что виртуальность облачных технологий привела к исчезновению традиционного физического периметра на основе контрольных точек, обеспечивавшего конфиденциальность информации.

Наиболее масштабная таксономия ИБ ИСОТ представлена в исследовании [5], однако концепция географического контроля не нашла себе места в классификации по месту проведения атаки. Согласно указанной классификации необходимо разделять защиту сетевых аппаратно-программных компонентов и протоколов.

Часть классификации, связанная с местом реализации атаки, представлена в таблице 2.

Таблица 2. Атаки на информационную систему, построенную с использованием технологий облачных вычислений (ИСОТ) по месту реализации атаки

Вектор атаки на ИСОТ по месту реализации атаки		
Атаки на ИСОТ (сторона пользователя)		Атаки на ИСОТ (сторона провайдера)
по информационному признаку	по неавторизованному доступу	
Доступность	*Маскирующийся*	*Аутентификация*
Конфиденциальность	*Превышение доступа*	*Авторизация*
Целостность	*Подбор пароля*	*Доступ к основным функциям*
Неопровержимость, невозможность отказа от авторства		*Повышение привилегий*

Для ИСОТ основная угроза – это распределённые атаки типа Отказ в обслуживании (Denial of service, DOS), направленные на сетевую и вычислительную инфраструктуры. Атаки с вектором на доступность направлены на конкретный сегмент сети или вычислительный ресурс, они отличаются большим числом нерегламентированных вычислений и сетевых запросов/ответов, что характерно для распределённых DOS атак.

В работе [6] предложен способ обнаружения подобных атак на ИСОТ. В основе метода модель графов атаки для обнаружения атак и предсказуемости поведения, что повышает точность обнаружения, и не учитывает фазы эксплуатации жертвы. Графы сценария атаки обнаруживают все взаимосвязи между путями атак.

Уязвимость в графе атак означает, что предупреждение, вероятно, указывает на настоящую атаку, количество ложноположительных срабатываний не возрастает. В случае обнаружения уязвимости злоумышленником и при отсутствии обнаружения со стороны сканера уязвимостей, оповещения, будучи настоящими, будут рассматриваться как ложные. Количество ложноотрицательных срабатываний возрастет. В качестве механизма фильтрации срабатываний может выступать функция отбора по специальному логическому выражению фильтра, которое может вернуть Истину - в случае удовлетворения логическому выражению фильтра, либо Ложь в случае не удовлетворения логическому выражению фильтра:

Срабатывание —> [Фильтр] = Истина | Ложь

В [7] предлагается для повышения эффективности обнаружения DDoS атак в ИСОТ, а также уменьшения числа ложных срабатываний оперировать математической теорией очевидностей (свидетельств) Демпстера–Шафера (Dempster–Shafer Theory (DST)). Благодаря правилу комбинации доказательств Демпстера число предупреждений будет уменьшаться, а конфликты, появляющиеся из–за наложения информации, предоставленной несколькими датчиками, полностью исключаются.

В [8] представлено комплексное решение для повышения уровня доверия в ИСОТ, при этом администраторы провайдера описаны как инсайдеры. В основе этого решения – мандатный контроль доступа и надежные вычислительные технологии (измеряемая загрузка, аттестации и запечатывания) на базе интегрированных ап-

паратно-программных средств, реализующих принципы криптографии, межсетевого экранирования, системы разграничения доступа и системы обнаружения вторжений. Такой подход создаёт гарантированную среду и явно связывает зашифрованные виртуальные машины с ранее аттестованными узлами. Возможно, данное решение при использовании технологии геометок позволит контролировать территориальное перемещение данных на протяжении всего их жизненного цикла.

Предлагается создание автоматизированной информационной системы для наблюдения и контроля размещения распределенной обработки данных. В основу системы предлагается онтологическое описание географического ландшафта вычислительной структуры, позволяющей классифицировать угрозы выхода за границу ландшафта, обеспечить требуемый контроль и предоставить удобный интерфейс на основе ГИС.

Например, возможно использовать следующий принцип поиска:

Определяются приблизительные координаты пользователя, относительно этих координат осуществляется поиск в определенном радиусе.

В онлайн базе данных, где хранятся координаты, проводится поиск и выводятся те координаты, которые удовлетворяют условию:

$$(x - X_1)^2 - (y - Y_1)^2 \leq R^2$$

Где R - радиус поиска, X_1Y_1 координаты пользователя, x y координаты в зоне поиска. Подобная методика не нова и уже используется для географического контроля пользователей.

2. Технологии отслеживания пользователя

Благодаря недавно обнародованным данным итальянской Hacker Team (компания, специализирующаяся на разработке систем для проникновения и слежки за пользователями и тесно сотрудничающая с рядом правительственных организаций и право-

охранительных органов) выяснилось, что внедряемое ими программное обеспечение Hacking Team's Remote Control System (RCS) содержит модуль, отвечающий за обнаружение местоположения инфицированного узла. [9]. RCS использует WLAN (wirelessLAN) функции API из стандартной динамической библиотеки WLANAPI.DLL (штатная библиотека ОС начиная с Windows XP SP2) для обнаружения ближайших от жертвы беспроводных сетей (Рис. 1). Такой метод позволяет установить местоположение узла несмотря на возможное использование прокси–серверов или VPN, т.к. определяет местоположение пользователя мобильного устройства по ближайшим точкам доступа Wi–Fi без использования GPS или других систем спутниковой навигации. Задействуются сервисы, аналогичные «Яндекс.Локатор» [10]. В большинстве настольных устройств нет GPS–приемника, поэтому определение местоположения по WiFi и IP – единственный доступный способ. «Яндекс.Локатор» — сервис геолокации, позволяющий определять координаты местоположения пользователя с указанием радиуса погрешности по GSM– и WiFi–сетям, в зоне действия которых находится пользователь.

```
if (pWlanGetNetworkBssList(hClient, &pIfInfo->InterfaceGuid, NULL, dot11_BSS_type_infrastructure, FALSE, NULL, &pB
    // Ha trovato un interfaccia valida ed enumera le reti wifi
    wifiloc_additionaheader.version = WIFI_HEADER_VERSION;
    wifiloc_additionaheader.type = TYPE_LOCATION_WIFI;
    wifiloc_additionaheader.number_of_items = pBssList->dwNumberOfItems;
    hf = Log_CreateFile(PM_WIFILOCATION, (BYTE *)&wifiloc_additionaheader, sizeof(wifiloc_additionaheader));
    for (j=0; j<pBssList->dwNumberOfItems; j++) {
        pBss = (WLAN_BSS_ENTRY *) &pBssList->wlanBssEntries[j];

        memcpy(wifiloc_data.MacAddress, pBss->dot11Bssid, 6);
        wifiloc_data.uSsidLen = pBss->dot11Ssid.uSSIDLength;
        if (wifiloc_data.uSsidLen>32)
            wifiloc_data.uSsidLen = 32; // limite massimo del SSID
        memcpy(wifiloc_data.Ssid, pBss->dot11Ssid.ucSSID, wifiloc_data.uSsidLen);
        wifiloc_data.iRssi = pBss->lRssi;
        Log_WriteFile(hf, (BYTE *)&wifiloc_data, sizeof(wifiloc_data));
    }
    Log_CloseFile(hf);
    break;
}
```

Рисунок 1. Фрагмент кода RCS, отвечающий за геолокацию

Северная Корея, известная своим высоким уровнем безопасности и изолированностью критически важных объектов благодаря провалившейся атаке с использованием червя Stuxnet [11], также

ведёт работы по гарантированной цифровой идентификации пользователей.

Аналитик немецкой ИБ – компании ERNW Florian Grunow, провёл независимое тестирование программного обеспечения Linux–дистрибутива RedStarOS 3.0., разрабатываемого в Корейском компьютерном центре (Пхеньян, КНДР), внимание специалиста привлёк нестандартный модуль ядра rtscan, также был обнаружен бинарный файл с именем opprc наряду с другими, имевшими похожий код, один из них (scnprc) замаскирован под антивирус. Исследователь обратил внимание на необычную функцию бинарного файла GPS Watermarking Information, наряду с функционалом по созданию «водяных знаков» он выполнял и функции шифрования, на рисунке видны функции добавления водяных знаков в документы, фотографии и даже в аудио файлы (Рис. 2).

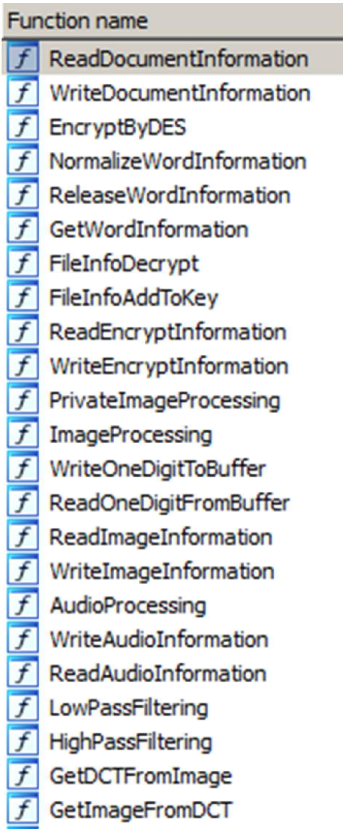

Рис. 2. Список функций бинарного файла

Исследователь провёл опыт и подключил съёмный носитель информации с документом в формате DOCX к тестовому стенду с установленной RedStarOS; несмотря на то, что файл не открывался предустановленным офисным ПО SogwangOffice, а также не копировался на сам стенд, его контрольная сумма MD5 изменилась. В контейнер DOCX была добавлена уникальная скрытая идентификационная метка, которая позволяет явно идентифицировать пользователя, связав его с файлом и оборудованием [12].

Заключение

Облачные технологии не только изменили понятие платформы, виртуализировав взаимоотношения операционной системы с оборудованием, но и остро поставили задачу по созданию периметра безопасности в облачной среде.

При наличии периметра безопасности на основе геометок, не только поставщик, но и клиент–пользователь могут предотвратить атаки, ограничив разрешённые географические места обработки данных.

Список литературы

[1] Amoroso E. G. Fundamentals of Computer Security Technology. Prentice Hall PTR, Upper Saddle River, NJ. 1994.

[2] В. И. Воробьев, С. Р. Рыжков, Р. Р. Фаткиева. «Защита периметра облачных вычислений», Программные системы: теория и приложения, 2015, 6:1(24), с. 61–71.URL http://psta.psiras.ru/read/psta2015_1_61–71.pdf

[3] «A quantitative analysis of current security concerns and solutions for cloud computing» Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11 URL http://www.journalofcloudcomputing.com/content/1/1/11

[4] «Analysis of Cloud related Security and risks mitigation» IRACST – International Journal of Advanced Computing, Engineering and Application (IJACEA), Vol. 1, No.2, p. 40–49, 2012

[5] Sanchika Gupta, Padam Kumar «TAXONOMY OF CLOUD SECURITY» International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, No.5, p. 47–67, October 2013

[6] URL http://ijircce.com/upload/2015/february/93_Attack.pdf

[7] URL http://univagora.ro/jour/index.php/ijccc/article/download/170/pdf_14

[8] Citation:Simma, A. (2015). Trusting Your Cloud Provider: Protecting Private Virtual Machines.MagdeburgerJournalzurSicherheitsforschung, 1, 530–539.RetrievedJune 17, 2015, URL http://www.sicherheitsforschungmagdeburg.de/publikationen.html
[9] URL http://labs.bromium.com/2015/07/10/government–grade–malware–a–look–at–hackingteams–rat/
[10] URL https://blog.yandex.ru/post/34348/
[11] URL http://www.reuters.com/article/2015/05/29/us–usa–northkorea–stuxnet–idUSKBN0OE2DM20150529
[12] URL http://www.insinuator.net/2015/07/redstar–os–watermarking/

Об авторах:

Рыжков Сергей Романович
(аспирант, Федеральное государственное бюджетное учреждение науки Санкт–Петербургский институт информатики и автоматизации Российской академии наук)
e–mail: *ryzhkov@awax.ru*

Фаткиева Роза Равильевна
(к.т.н., с.н.с.,
Федеральное государственное бюджетное учреждение науки Санкт–Петербургский институт информатики и автоматизации Российской академии наук)
e–mail: *rrf@iias.spb.su*

Образец ссылки на публикацию:

Рыжков С.Р, Фаткиева Р.Р. Таксономия атак на облачную инфраструктуру по месту реализации атаки // Программные системы: теория и приложения: электрон. научн. журн. 2015. Т. ?, № ?(??), с. ??–??.
URL: http://psta.psiras.ru/read/???

Ryzhkov S.R, Fatkieva R.R. (Cloud infrastructure attacks taxonomy by the place of attack).

Abstract.

A review of cloud infrastructure attacks taxonomiesn. A review of user tracking technologies. The possibility of applying geo–tagging technology, as a tool of territorial control the movement of data throughout its lifecycle.

Key Words and Phrases: cloud, cloud computing, security perimeter, geo tagging.