331-13

id\_worker

name

addr

kod\_object

kod\_object

type

addr

id\_worker

numer\_contract

numer\_contract

date\_contract

stoimost\_contract

kod\_object

worker

object

contract

Percentage процент

Rate –уровень

increase – увеличение

интернет вещей – концепция вычислительной сети физических предметов оснащённых встроенными технологиями для взаимодействия друг с друuом или внешней средой

Average – среднее число

malicious-злонамеренный

leaky –текущий

sensitive – чувствительный

further- далее

Мотивы совершения целевых атак : мотивы атакующих можно узнать несколькими способами. Во первых обратить внимание на деятельность фирмы, во вторых на способности и возможности инструментов используемых для проникновения и в третьих какие компьютеры организации атакующие выбрали в качестве своей цели и какую информацию могут похитить из них

Гевин огорман

Бабочка - вероятно, самая интересная группа, которая была мною замечена. Они были одной из немногих

групп проводивших целевые атаки, которые, казалось, не были связаны ни с какой страной

но всё таки были включены в корпоративный электронный шпионаж,

по-видимому для финансового усиления. В течение нескольких

лет , они поставили под угрозу влияние главных корпораций,

такой как Twitter™, Facebook™, Apple®, и Microsoft®.

Каждый раз, когда я иду на конференцию, люди спрашивают меня о

них, желая знать, наблюдали ли мы ещё атаки.

Ответ – на это, что они исчезли полностью. Их

операционная безопасность была некоторой из лучших, которые мы видели.

Например, они работали на серверах командования и управления

зашифрованные виртуальные машины на поставивших под угрозу серверах.

Это - что-то, что мы не видим каждый день.

Они удалились? Я сомневаюсь относительно этого. Уязвимости нулевого дня

они использовали, потребует большого количества времени и навыка

чтобы получить самостоятельно и они были наиболее вероятно куплены

вместо этого. Нулевые дни стоившие много денег, оправдывали

средства которые они зарабатывали много.

Если я предпологаю, они завершают работу временно и

разработанный абсолютно новый набор инструментов.их создание

требовало слишком большого количества денег, чтобы только так просто уйти.”

Алан невил

Turla было одним из первых больших расследований,

и это - все еще один из самых интересных. Они использовали много

из инструментов и приемов, которые я не видел прежде и действительно

демонстрировали тот, уровень изощренности, на котором данные

группы работают. Даже прослеживая разработку их набора инструментов

, это было многочисленной, хорошо организованной группой

имевшей много денег, чтобы поддержать их операции. Была, очевидна, группа

высокой квалификации, состоящая из различных людей, чтобы разработать

каждый компонент.

Например, их Яд, поливающий платформу дыры,

шаг выше того, что мы обычно видим. Они были одним из

первые группы, которые будут использовать системные методы снятия отпечатков пальцев,

посредством чего они проанализировали посетителей орошающих дыр и

собранный достаточно информации, чтобы определить, если потенциал

жертва представляла интерес для группы, и если так, смогла

чтобы определить лучшее используют, чтобы поставить, чтобы получить a

точка опоры в пределах организации их цели. Но рядом

это, была также их возможность пойти на компромисс многократный

серверы, чтобы разместить их использовать платформу набора как средство

заключение компромисса жертв. У них, очевидно, был такой диапазон

навыки, доступные им и это демонстрировалось

переменный уровень изощренности инструментов они использовали, их

возможность работать в пределах многократных сред, и

факт они были активными в течение такого длительного периода времени,

заключение компромисса многократных правительств. По сей день, Turla

продолжайте их операции и останьтесь одним из наиболее

интересные группы, чтобы отследить.”

Доклад 2

Quantifying –количесвенная

identities –тождетства

exposed – подвергаются

Total –всего

Средние тождества

разоблачение за нарушение

Среднее количество облачных приложений

используется для каждой организации

Процент широко распространенных данных

Health Care здравоохранение

Поставщик DNS Dyn Inc.

услуги были прерваны

Распределенный отказ в обслуживании

атака беспрецедентного

сила от ботнета Мирай

скомпрометированных устройств IoT.

Сообщалось, что нападение

скорость потока 1,2 Тбит / с от

100 000 зараженных устройств.

11-часовое переключение Dyn из их

Службы поиска DNS вызвали

проблемы доступности для пользователей

Amazon.com, Comcast, HBO,

Netflix, The New York Times,

PayPal, Spotify, Verizon, The

Wall Street Journal, Yelp, среди

многие другие платформы и

услуги, зависящие от Dyn как

DNS-провайдер.

Веб-службы Amazon

пострадали от их

Служба облачных хранилищ S3

в течение приблизительно 4 часов.

отключение повлияло на некоторые популярные

интернет-услуги, веб-сайты,

и других предприятий, использующих

эту инфраструктуру. Стена

Street Journal сообщил, что

отказ был вызван

человеческая ошибка - сотрудник

ошибся команда, вызывающая

каскадный провал, который сбил

S3 и другие Amazon

Сервисы. Оценки Киенса

что компании в S & P

500 зависит от Amazon's

услуги утратили аппроксимацию

150 млн. Долл. США в результате

отключение.

Агрессивное вымогательство

была развернута кампания

заражение сотен тысяч

конечных точек по всему миру

поскольку. Выручка, названная

WannaCry (AKA WannaCrypt,

Wana Cryptor, wcrypt), предназначенный для

незагруженная Microsoft Windows

машины, использующие EternalBlue

эксплуатируют. Известные жертвы

Национальная служба здравоохранения

(NHS) в Соединенном Королевстве,

Ниссан Мотор Производство

Великобритании и Renault. Уолл-стрит

Журнал сообщил, что

оценка потенциала в размере 8 млрд. долл. США

экономические потери из-за

событие, проистекающее из потерянного дохода

и возмещения расходов на

организации с инфицированными или

уязвимых систем.

Новые варианты Петя

ransomeware начал распространяться

глобально (дублируется NotPetya),

хотя большая часть

сообщили в Украине. однажды

вредоносное ПО впервые заразило его

хост, он затем попытался распространить

далее по всему местному

сети с использованием EternalBlue

эксплоит, который использовался

WannaCry за месяц до этого.

Чернобыльская ядерная энергетика

Power Plan отправился в автономный режим, Индия

крупнейший порт был

простоя и числа

глобальных компаний

влияние, включая A.P. Moller

Maersk, WPP, DLA Piper, Merck

& Co., FedEx и другие.

Рейтер сообщил, что Сайенс

$ 850 млн.

оценка этого события

октябрь 2016 февраль 2017 май 2017 июнь 2017

Провайдер Веб-службы Атака вымога- Атака вымогателя

Dyn Inc Amazon теля WannaCry Petya началась

подвергся подверглись известные жертвы: с Украины, ущерб около

DDOS отключению Nissan,Renault, 850 млн

атаке службы Национальная

с помощью облачных Служба Здравох-

Mirai со хранилищ ранения Великоб-

скоростью из-за ошибки ртиании, ущерб

1,2 Тбит / с от сотрудника, около 8 млрд

100 000 ущерб от

зараженных отключения

устройств около 150 млн

Insurance-страхование

Retail-розничная торговля

GROWTH-рост

This chart depicts a monthly average of the ransomware events that occurred from January to September in 2015 and 2016.

While the number of events varied, the increase in events in 2016 over the prior year is significant – and worrisome.

На этой диаграмме показано среднемесячное число событий выкупа, которые произошли в период с января по сентябрь в 2015 и 2016 годах.

Несмотря на то, что количество событий изменилось, увеличение событий в 2016 году по сравнению с предыдущим годом является значительным - и вызывает тревогу.

итоги

Одними из самых главных угроз на сегодняшний день являются шифровальщики-вымогатели. Количество семейств данных вредоносов как и сумма выкупа с 2014 по 2016 года увеличилось более чем в три раза. Наряду с этим увеличилось и число мобильных вредоносов, так например если в 2015 году число большинство новых вредоносов было ориентировано на IOS, то в 2016 картина изменилась в пользу Android.

Лидерами среди европейских стран подвергающимся кибератакам являются Германия, Великобритания, Бельгия, Испания. В основном атака подвергаются финансовые институты, энергетика, здравоохранения, розничная и оптовая торговля.

С увеличением числа организаций использующих облачные сервисы необходимо учитывать риски атак на данные сервисы и их отказов

Лидерами среди европейских стран подвергающимся кибератакам являются Германия, Великобритания, Бельгия, Испания. В основном атака подвергаются финансовые институты, энергетика, здравоохранения, розничная и оптовая торговля.

С увеличением числа организаций использующих облачные сервисы необходимо учитывать риски атак на данные сервисы и их отказов

polzovatel object1 object2 object3 object4 masha own,e,r,w e,r own,e e,w admin own,e,r,w own,e own,r own,r,w user own,e,r own,r own,r,e own,r,w river

Получив доказательства и сделав судебно-медицинскую копию, пришло время начать искать доказательства.

Это свидетельство может иметь разные формы. Инструменты, упомянутые в предыдущем разделе, могут быть использованы для

выведите это доказательство для вас. Однако в этом разделе я покажу вам, что это за поиск этих инструментов

для. Важно не просто срывать то, что говорит вам какой-то автоматизированный инструмент, а скорее понимать

что это инструмент делает.

Поиск доказательств в браузере

Браузер может быть источником как прямых доказательств, так и косвенных или подтверждающих доказательств. очевидно в случаях детской порнографии, браузер может содержать прямое доказательство конкретного преступления. Однако, если вы подозреваете кого-то из

создателей вируса, заразившего сеть, вы, вероятно, найдете только косвенные доказательства, такие как

кто искал темы создания вирусов / программирования.

Даже если человек стирает свою историю браузера, все равно можно ее восстановить. Windows хранит много информации

в файле index.dat (информация, такая как веб-адреса, поисковые запросы и недавно

открытые файлы).

Соглашения об уровне обслуживания

Организации, которые продают облачные сервисы, имеют соглашения об уровне обслуживания (SLA) со своими клиентами,

которые также называются «соглашениями об основных услугах». SLA - это контракт между CSP

и клиент, который описывает, какие услуги предоставляются и на каком уровне. Должно

также указать параметры поддержки, штрафы за предоставленные услуги, производительность системы (периоды

времени простоя и времени простоя, например), сборов, программного обеспечения или оборудования и т. д.

(Www.webopedia.com/TERM/S/Service\_Level\_Agreement.html). Важно, чтобы SLA

подробно определить объем услуг, предоставляемых CSP, и какие обязанности ожидаются

клиента, в том числе:

• Часы работы

• Ограничения, применяемые клиентом CSP

• Наличие облака для клиента

• Уровни поддержки для клиента

• Время отклика для передачи данных

• Пропускная способность, ограничения

• План реагирования на непредвиденные обстоятельства

План обеспечения непрерывности бизнеса и аварийного восстановления

• Плата за подписку на облако и плату за дополнительные услуги по мере их возникновения

• Меры безопасности

• Терминология облачных систем и приложений

Эксперты по цифровой экспертизе должны быть в наибольшей степени обеспокоены ограничениями, применяемыми к клиентам

и меры безопасности. Эти компоненты CSP должны указать, кому разрешено доступ к данным

и каковы ограничения при проведении приобретений для расследования. Потому что многие

поставщики облачных вычислений распространяют системы хранения данных в разных странах, CSP также должен

адресуйте любые проблемы, связанные с несколькими проблемами, и определите, как конфликты между законами разных

страны будут решены.

Политики, стандарты и руководящие принципы для ПСУ(CSP) У ПСУ есть политика, стандарты,

и руководящие принципы их повседневной деятельности, а следователи цифровой судебной экспертизы должны рассмотреть

их тщательно при подготовке плана облачного расследования. В этом разделе приведены рекомендации

для этих политик, стандартов и рекомендаций от организации SANS

(www.sans.org/security-resources/policies/#name и www.sans.org/security-resources/policies/

computer.php).

Политики - это подробные правила для внутренней операции CSP и обычно включают персонал

обязанности, структура управления, полномочия делегирования, организация-заказчик, ожидания

защиты данных и разрешения на распространение информации. Стандарты дают руководство

персоналу для уникальных операций, оборудования и программного обеспечения и описать их обязательства в

ежедневные операции и безопасность среды CSP. Хотя рекомендации не требуются,

они описывают лучшие практики для облачных процессов и дают сотрудникам пример того, что им следует

стремиться к достижению в своей работе.

Процессы и процедуры CSP Процессы и процедуры - это подробные документы

которые определяют рабочий процесс и пошаговые инструкции для персонала CSP. Они часто включают аппаратные средства

диаграммы конфигурации, сетевые карты и блок-схемы обработки приложений. Цифровая криминалистика

экзаменаторы могут использовать эти документы, чтобы понять, как данные хранятся, обрабатываются,

обеспечено, выполнено резервное копирование, восстановление и доступ к персоналу и клиентам CSP.

Дополнительными документами, представляющими интерес, являются непрерывность бизнеса CSP и аварийное восстановление

планы, которые могут быть полезны при восстановлении и анализе данных, необходимых для вашего расследования.

Эти документы особенно полезны, если у вас есть большое количество данных для сбора и

без надлежащего хранения. Если у CSP есть резервный сайт, указанный в его бизнесе

план непрерывности, вы можете использовать его для хранения цифровых доказательств, которые вы собрали, и

анализируя чрезвычайно большие наборы данных.

Вопросы юрисдикции

Хотя есть планы пересмотреть действующие законы, многие вопросы юрисдикции

были решены. Никакой закон не гарантирует равномерный доступ или требуемые процедуры обработки для облака,

поэтому случаи, которые охватывают несколько юрисдикций, а также характер мультяшности облака,

проблемы для любого расследования. Кроме того, следователи должны быть обеспокоены случаями

включая данные, объединенные с данными других клиентов, не связанные с расследованием

(www.researchgate.net/publication/221352825\_A\_Survey\_of\_the\_Legal\_Issues\_Facing\_Digital\_

Forensic\_Experts). Если правительственные постановления и соглашения не были разработаны в других

страны, следователи могут быть ограничены тем, что они могут сделать для обработки дела.

Часто просто выяснить, какой закон контролирует данные, хранящиеся в облаке, является проблемой.

Хотя SLA или связанные с ним контракты и дополнения могут предписывать, какие законы подлежат исполнению,

они обычно не контролируют вопросы конфиденциальности, а также уголовные или гражданские процедуры. (Добавление

используется для добавления или изменения контракта без необходимости его воссоздания.) Многие страны

с юридическими системами, основанными на общем источнике, например на английском общем праве, может

имеют аналогичные законы, но изменяются в процедурах. Кроме того, как права конфиденциальности определяются в разных

юрисдикции являются основным фактором в проблемах с правом доступа к данным. Например,

Директива ЕС 95/46 / EC (http://searchsecurity.techtarget.co.uk/definition/EU-Data-ProtectionDirective)

является более ограничительным, чем правила в других странах, включая Соединенные Штаты. Эта

директива защищает частную информацию для всех граждан ЕС, заявляя, что граждане ЕС должны быть уведомлены,

до доступа к их личной информации, и к этой информации можно получить доступ только

с их согласия.

Некоторые проблемы имеют такое же фундаментальное значение, как определение определений терминов и ролей и определение

какой закон применим. Как уже упоминалось, когда данные хранятся в многоликих странах,

могут произойти ошибки в законах. По этой причине цифровые эксперты по судебной экспертизе могут быть привлечены к ответственности

при проведении расследования с использованием данных облака. Проконсультируйтесь с экспертами-юристами при проведении

облачных экзаменов, чтобы убедиться, что вы знаете о возможных ограничениях в сборе

доказательства.

Технические проблемы в облачной криминалистике

Процедуры облачной криминалистики объединяют множество вычислительных и сетевых задач, таких как данные

восстановление, сетевой анализ для обнаружения вторжений, администрирования баз данных и безопасности, программного обеспечения

безопасности и международных отношений. В следующих разделах вы узнаете о некоторых общих

технические проблемы, с которыми вы столкнетесь при проведении облачной криминалистики.

Рабочая группа NIST Cloud Computing Forensic Science (www.sensei-iot.org/

Презентации / MHerman\_CC\_FSWG.pdf, 2014) разработали следующий перечень проблем в

проводя облачную криминалистику. Некоторые из этих проблем обсуждаются более подробно в

следующие разделы:

• Архитектура

• Сбор данных

• Анализ облачных криминалистических данных

• Анти-криминалистика

• Инцидент первым

13

Технические проблемы в облачной криминалистике 489

Copyright 2016 Cengage Learning. Все права защищены. Может не копироваться, не сканироваться и не дублироваться полностью или частично. Из-за электронных прав некоторые сторонние материалы могут быть подавлены из электронных книг и / или eChapter (s).

Редакционная оценка сочла, что любой подавленный контент не оказывает существенного влияния на общий опыт обучения. Cengage Learning оставляет за собой право удалить дополнительный контент в любое время, если это потребует последующие ограничения прав.

• Управление ролями

• Правовые вопросы

• Стандарты и обучение

Архитектура

Облака различаются по своей архитектуре, поэтому два CSP не настроены точно так же.

В зависимости от типа облачной архитектуры данные клиентов могут быть объединены, что делает

сложно сортировать данные, чтобы определить, что имеет отношение к расследованию. идентифицирующий

также могут возникнуть проблемы с хранилищами данных, поскольку большинство CSP хранят эти местоположения в тайне

по соображениям безопасности. Кроме того, различия в процедурах регистрации или ведения журнала могут

трудно определить происхождение данных и усложнить цепочку доказательств расследования.

Анализ облачных криминалистических данных

Анализ цифровых данных, собранных из облака, требует проверки данных с другими данными

и записи журнала. Возможно, вам потребуется восстановить данные, чтобы определить, что на самом деле произошло

во время инцидента и сравнить сетевые записи, чтобы убедиться, что внутренние часы серверов

синхронизированы правильно. Изучение журналов может быть полезно для сравнения измененного, последнего доступа,

и создавать (MAC) даты и время для файлов. Метаданные из затронутых файлов должны быть проверены,

также для проверки доступа к файлам. Вся эта информация используется для построения временной шкалы, чтобы показать, что

произошло, когда произошел инцидент.

Anti-криминалистика

Уничтожение ESI, которое является потенциальным доказательством, называется «анти-криминалистикой». Тактика анти-криминалистики

используемых в облачных средах, а также в других сетевых средах. Хакеры могут запутаться

инкриминируя файлы или скрывая их простой методикой изменения расширений файлов. специализированный

вредоносное ПО для разгрома коллекции доказательств может добавить время для расследования и результата

в потере ценных доказательств. Дополнительные методы для защиты от криминалистики включают вставку вредоносного ПО

программы в других файлах, используя шифрование для обфускации вредоносных программ, активированных

с помощью других вредоносных программ, а также с помощью утилит для скрытия данных, которые добавляют вредоносное ПО к

существующие файлы. Другие методы влияют на метаданные файла, изменяя изменения и последний доступ

раз. Изменение временных меток файлов может затруднить разработку графика действий хакера.

Вычисление хэш-значений файлов и сравнение результатов с хэшем известных хороших файлов

значения могут помочь идентифицировать файлы, которые могли быть изменены.

Первые ответчики инцидента

Как правило, ПСУ обучены персоналу для реагирования на сетевые инциденты, такие как система и

сетевых администраторов, которые обрабатывают обычные службы поддержки для облака. Когда сеть

происходит вторжение, они становятся первыми ответчиками на инцидент. Если CSP не имеет

490 Глава 13

Copyright 2016 Cengage Learning. Все права защищены. Может не копироваться, не сканироваться и не дублироваться полностью или частично. Из-за электронных прав некоторые сторонние материалы могут быть подавлены из электронных книг и / или eChapter (s).

Редакционная оценка сочла, что любой подавленный контент не оказывает существенного влияния на общий опыт обучения. Cengage Learning оставляет за собой право удалить дополнительный контент в любое время, если это потребует последующие ограничения прав.

внутренняя команда первого ответчика, эксперт по судебной экспертизе должен организовать персонал CSP для обработки

эти задачи. К числу некоторых факторов, к которым относятся, относятся следующие:

• Будет ли операционный персонал CSP сотрудничать и следовать указаниям, а также будет управлять

выдать приказы о том, что вы являетесь лидером расследования?

• Нужно ли вам информировать персонал об оперативной безопасности? Например, вам может понадобиться

объяснить, что они должны разговаривать только с теми, кто нуждается в

инцидента и деятельности следствия.

• Нужно ли вам обучать персонал процедурам сбора доказательств, включая цепочку

опека?

Управление ролями

Управление ролями в облаке охватывает владельцев данных, защиту идентификаторов, пользователей, средства контроля доступа

(список привилегий и ограничений доступа для каждого пользователя) и т. д. Как следователь, вы

необходимо собрать эту информацию, чтобы вы могли идентифицировать дополнительных жертв или подозреваемых. тождественность

например, защита означает, что вам необходимо определить,

(PII) была скомпрометирована, что расширяет сферу охвата расследования. Вы

также может потребоваться определить, был ли компромисс PII преднамеренным или случайным, и

зная, что разрешения доступа пользователей облачных вычислений могут помочь с этой задачей.

Стандарты и обучение

По мере того, как облако становится более широко используемым, предпринимаются усилия по стандартизации облачных архитектур

для операционных процедур, совместимости, тестирования, проверки и т. д., и

являются общепринятыми стандартами, которые следуют всем ПСУ. Альянс Cloud Security (CSA; https: //

cloudsecurityalliance.org) - это одна организация, которая разработала документацию по ресурсам

для ПСУ и их сотрудников. Он обеспечивает руководство для соглашений о конфиденциальности, мер безопасности,

анкеты и многое другое.

Обучение в облачной безопасности и облачная криминалистика также продолжает развиваться. Облачные исследователи

должны обладать пониманием облачной архитектуры в дополнение к основным цифровым и сетевым

навыки судебной экспертизы. Некоторые источники обучения облачной криминалистике (ISC) 2

Сертифицированный Cyber

Forensics Professional (www.isc2.org/ccfp/Default.aspx), Институт INFOSEC (http: // resources.

infosecinstitute.com/overview-cloud-forensics/), SENS Cloud Forensics с F-Response (http: //

digital-forensics.sans.org/blog/2013/04/09/cloud-forensics-with-f-response), Национальный институт

судебной цифровой судебной экспертизы (только для правоохранительных органов; www.nij.gov/topics/forensics/

доказательства / digital / training / Pages / welcome.aspx) и Университетский колледж Дублинского центра кибербезопасности

и исследование киберпреступности (www.ucd.ie/cci/training.html).