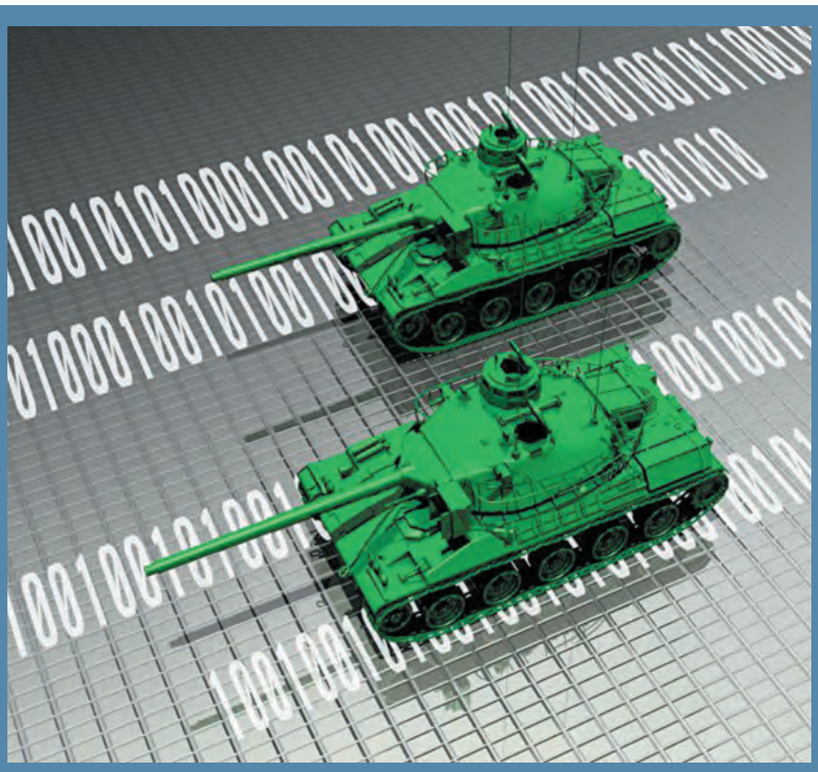
О жизни в эпоху кибервойн



Виктор ЖОРА,
директор компании «Инфосейф ИТ»

Вирусы-шифровальщики давно не новость, вот и в нынешнем году мир пережил несколько эпидемий. Но в лице Petya.A, кажется, нас посетило нечто иное.

В конце июня Украину «поздравил» с Днем Конституции вирус-шифровальщик Petya.A, который быстро распространился, поразив банки, энергетические компании, государственные предприятия и множество коммерческих организаций. Согласно сообщению киберполиции, источником распространения вируса, вероятно, стала бухгалтерская программа M.E.doc — «зловред» рассылался вместе с очередным обновлением. При этом подавляющее число зараженных компьютеров находилось на территории Украины, а в совокупности с признаками того, что получение выкупа в этот раз явно не было главной целью злоумышленников, дает основания судить о том, что мы столкнулись с кибероружием.

О том, так ли это, ждать ли подобных атак в будущем и как обороняться, «СиБ» расспросил директора компании ***«Инфосейф ИТ» Виктора Жору***.

— Чем все-таки был Petya.A? Это кибероружие или просто неудавшаяся атака вымогателя?

— Безусловно, это было кибероружие, причем достаточно современное. География стран, затронутых этой атакой, достаточно обширна, однако согласно статистике, подготовленной компанией ESET, 75% пострадавших организаций находились на территории Украины. Из этого можно сделать вывод, что именно наше государство было целью этой атаки. Сам размер ущерба, который понесла украинская экономика, свидетельствует о том, что вовсе не желание заработать двигало организаторами этой атаки, а нанесение как можно большего урона стране в целом.

На Bitcoin-кошельки, опубликованные злоумышленниками, по факту был перечислен эквивалент нескольких десятков тысяч долларов. Это не тот заработок, который интересует киберпреступников такого уровня — даже по программе Bug Bounty, по которой разработчики ПО предлагают вознаграждение за обнаружение уязвимостей, можно заработать гораздо больше, причем проще и легально. А заплатившие выкуп ключ так и не получили, то есть зашифрованные данные восстановить не удалось. Поэтому можно сказать, что это не типичное вымогательство, а разрушительная атака с целью нанести как можно больший ущерб инфраструктуре атакованных организаций, экономике Украины в целом и, скорее всего, она содержит скрытую составляющую, дающую возможность осуществить кражу данных, которую путем уничтожения информации на рабочих станциях и серверах также пытались скрыть. Боюсь оказаться пророком, но вполне вероятно, что эти данные, как и возможные потерянные ноу-хау, коммерческая тайна, информация об организации внутренней инфраструктуры предприятий могут быть использованы для дальнейших атак.

— Известно, что пострадали и организации в других странах, в том числе в России…

— У меня практически нет сомнений в том, что эта операция была организована и координировалась нашим северным соседом, поэтому к сообщениям о том, что пострадали российские предприятия, я бы относился осторожно. Но даже если это правда, скорее всего, либо это были точечные заражения для отвода подозрения, либо ситуация в какой-то момент вышла из-под контроля — вирус ведь распространялся хаотично, и полностью изолировать инфраструктуру собственного государства от его воздействия не удалось.

— Какие вообще могут быть прямые или косвенные признаки, свидетельствующие о том, что это именно кибероружие?

— В качестве основных признаков я бы выделил масштаб ущерба. По факту можно говорить, что это была крупнейшая кибератака в истории человечества. В частности, Maersk заявил о потерях в размере $300 млн, и это только одна компания. У нас приблизительные оценки ущерба в масштабах страны были сделаны на уровне 0,5% ВВП, они основаны на том, что в течение трех дней треть экономики не работала. Заместитель главы президентской администрации Дмитрий Шимкив оценил количество зараженных компьютеров в 10%. И хотя официальной информации о размере ущерба нет, я считаю, что эти цифры недалеки от реальности. Именно это может свидетельствовать о том, что это спланированная атака против нашей страны.

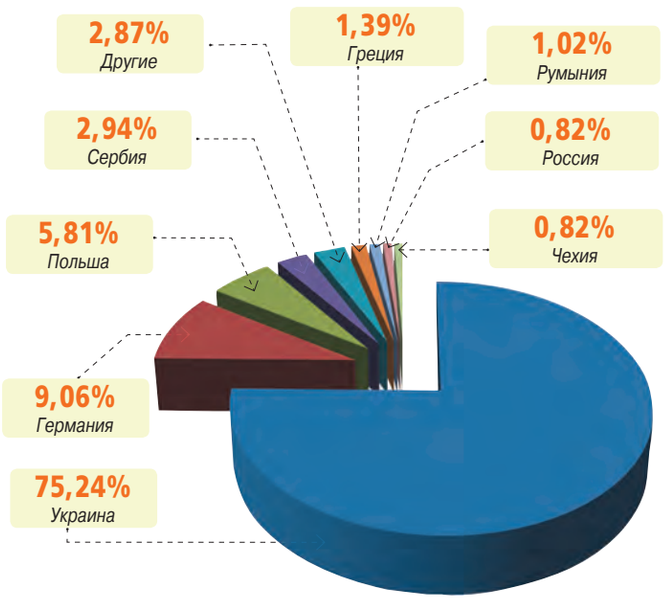
Использование цепочки поставок программного обеспечения — достаточно типичная схема организации компьютерных взломов в мире. Инновационность заключается в том, что способ проникновения был выбран наиболее массовый. Было использовано доверенное ПО от известного разработчика, которое установлено в сетях множества организаций. Понятно, что это не был единственный канал проникновения вредоносного кода, однако, согласно официальной информации, он был основным.

Первое кибероружие было «высокоточным» и нацеленным на конкретные объекты, но сейчас в качестве такого объекта выступила целая страна. Petya.A можно сравнить с оружием массового поражения.

— Высказывались опасения, что это была пробная атака и за ней могут последовать другие. Происходили ли подобные атаки раньше и чего ждать в будущем?

— Мы живем в стране, которая постоянно выступает в качестве тестовой лаборатории. Проба сил происходит на протяжении как минимум последних трех лет. В качестве первого пробного шара я бы рассматривал хакерскую атаку на сервер ЦИК во время президентских выборов 2014 года. После нее было и много других — например, атака BlackEnergy на медиахолдинги, затем на облэнерго, аэропорт «Борисполь», на «Киевэнерго» в декабре прошлого года. К сожалению, вероятность того, что вслед за атакой 27 июня последуют другие, не менее серьезные, очень высока, потому что страна, которая заинтересована в дестабилизации Украины, получила доказательства того, что наша инфраструктура не является защищенной. С другой стороны, в результате проведенной атаки наверняка была получена информация, которая сможет послужить ключом для

География атаки Petya.A (по данным ESET)



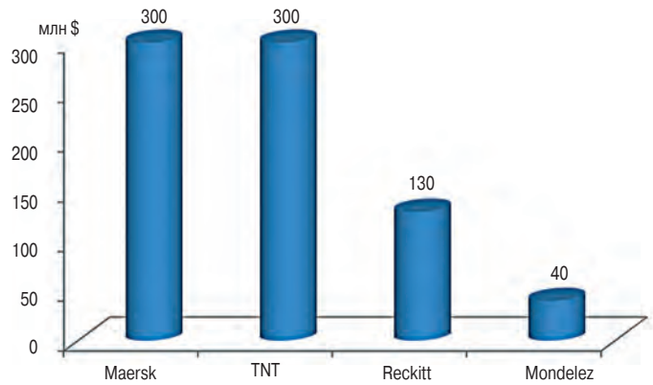
Атака Petya.A затронула 60 стран мира. Подавляющее число зараженных компьютеров пришлось на Украину

Потери некоторых глобальных компаний, $ млн

✧ Reckitt (TM Nurofen, Durex и Vanish) сократил прогноз годового роста с 3% до 2%

✧ Mondelez (TM Oreo и Cadburry) потерял 2% роста во втором квартале

✧ Среди других пострадавших — международная юридическая фирма DLA Piper, британская рекламна компания WPP, французский строительный гигант Saint Gabain, российская «Роснефть»



Аналитическая фирма Cyence оценивает мировой ущерб от Petya.A в $850 млн. Предыдущая атака WannaCry стоила $8 млрд

Lloyd's полагает, что масштабная глобальная кибератака нанесет ущерб до $53 млрд, что сравнимо с последствиями крупной природной катастрофы

По оценкам Markets and Markets, мировые расходы на кибербезопасность достигнут $101 млрд в 2018 году и $170 млрд в 2020 году

последующих атак. В целом нужно осознавать, что Украина не является единственной целью.

После атаки Petya.A звучал вопрос, чего ждать дальше, что может быть хуже того, что уже произошло. Все будет зависеть от фантазии тех людей, которые будут готовить дальнейшие деструктивные действия по отношению к нашему государству. Не хотел бы быть источником идей для этих недружественных сил, но коллеги озвучивали такие предположения, как использование уязвимостей и написание «зловредов» для Linux-инфраструктуры, которая в основной своей массе используется в работе государственных баз данных и реестров, — это один из возможных векторов последующих атак.

— Каким образом можно защититься от таких атак, особенно если вредоносное ПО уже проникло в систему?

— Есть элементарные правила компьютерной гигиены: не работать с административными правами, устанавливать обновления ПО, не открывать сообщения и вложения из сомнительных источников, использовать сложные пароли либо схемы многофакторной аутентификации. Это базовые вещи. Как предотвратить проникновение APT и написанного для «целевого заказчика» вредоносного кода? Есть довольно модный сейчас класс продуктов, таких как системы обнаружения нарушений (Breach Detection Systems) и решения для обнаружения атак на рабочих станциях (Endpoint Detection and Response). Они не производят сигнатурный или эвристический анализ, но используют «облачный интеллект» и эмулируют работу программ в виртуальной среде, генерируя индикаторы компрометации, которые позволяют судить, опасен код или нет.

Для больших организаций совершенно очевидной является потребность в построении центра управления безопасностью (Security Operations Centre — SOC), который позволит повысить наблюдаемость процессов. Обеспечив сбор и корреляцию данных из различных сегментов сети, серверов, рабочих станций, сетевого оборудования, можно создать целостную систему мониторинга, которая в подавляющем большинстве случаев позволит обнаружить атаку на ранних стадиях, то есть увидеть аномальное поведение процессов в сети.

Для ускорения ликвидации последствий атак и минимизации ущерба, безусловно, необходимы резервные копии критичных данных — причем, как показал опыт не только этой атаки, но и предыдущих, лучше использовать отключенные от сети хранилища. В случае же, если атака произошла, первое, что необходимо иметь — а ситуация с Petya.A показала абсолютную неготовность организаций Украины к такого рода инцидентам, — это план резервного восстановления (Business Recovery Plan). Он представляет собой набор четких инструкций, предписывающих, что и в каком порядке делать в случае нештатной ситуации и кто за что отвечает. В большинстве случаев, даже если такие инструкции были написаны, они носили крайне размытый, неконкретный характер, это в большей степени высокоуровневые документы, не адаптированные к реальным условиям функционирования информационных систем. Четкий план восстановления позволит сэкономить время и ресурсы, а в конечном итоге — свести потери к минимуму.

Понятно, что наибольший урон такие атаки могут нанести критической инфраструктуре, поэтому ее защите государство должно уделять намного больше внимания. Хотел бы особо подчеркнуть нормативно-правовую составляющую этого вопроса, потому что критическая инфраструктура — это не только государственные монополии, но и частные предприятия, такие как облэнерго, медиахолдинги, телеком-операторы, крупные банки. Как обязать госорганы — понятно, есть закон о защите информации в информационно-коммуникационных системах. Что касается частных компаний, то механизма влияния на них, по сути, нет, в том числе из-за того, что вот уже четвертый год Верховная Рада не может принять законы «Об основных положениях обеспечения кибербезопасности», «Об электронных доверительных услугах», «Об электронных коммуникациях» — базовые документы, которые формируют правила игры в этой сфере и за которыми последует масса подзаконных актов и стандартов. Несмотря на очевидное, на мой взгляд, несовершенство законопроектов, которые готовятся к голосованию, сейчас нужно принять хоть что-нибудь с последующим внесением правок и запустить эти механизмы на всех уровнях.[*)]

— Сможем ли мы, наконец, защититься от этой напасти или обречены страдать?

— Я был бы очень осторожен в высказываниях относительно возможности вообще с высокой степенью гарантии защитить какую-либо компьютерную систему, поскольку уязвимости нулевого дня обнаруживаются ежедневно и могут эксплуатироваться в течение достаточно продолжительного времени, как это было с той уязвимостью, которая была использована во время атаки WannaCry. Могу сказать, что Украине тогда немного повезло, потому что эпидемия нас обошла в основном стороной. Но что касается последовавшего за ним шифровальщика X-Data, у меня есть практически неопровержимые доказательства, что внедрение этой программы было одним из этапов подготовки к атаке с помощью Petya.A, потому что для доставки в ряд пострадавших организаций использовался тот же канал, что и при атаке 27 июня.

Но есть и хорошие новости. Одна из причин, почему атака имела такие последствия, — это отсутствие понимания глубины проблемы собственниками бизнеса. Не секрет, что пострадали в основном коммерческие предприятия и, возможно, государственные монополии. Понятно, что безопасность в большинстве этих организаций финансировалась по остаточному принципу. Одним из позитивных моментов после атаки я бы назвал повышение осведомленности о том, что проблема кибербезопасности может касаться каждого из них и ведет к прямым финансовых потерям. Сейчас мы действительно видим как со стороны бизнеса, так и со стороны госструктур повышение интереса к средствам защиты, которые могут помочь предотвратить такие атаки или, во всяком случае, минимизировать их последствия.

Украина находится в зоне риска, у нас ведутся активные боевые действия, и мы будем мишенью еще некоторое время, и это нужно понимать. Однако особого выбора нет, мы просто должны обладать определенным защитным потенциалом. Если удастся наладить эффективное государственно-частное партнерство в сфере кибербезопасности, использовать возможности международного сотрудничества и опыт зарубежных коллег, я думаю, мы сможем выйти на достаточно высокий уровень защищенности.

Беседовал **Василий ТКАЧЕНКО, СиБ**

[*)] Когда верстался номер, Верховная Рада приняла во втором чтении и в целом законы «Об электронных доверительных услугах» и «О кибербезопасности Украины». («СиБ»).