– Twitter Framework – Підтримка Twitter інтегрованого в систему. Дає можливість ділитися з багатьма даними у застосунках;

– UIKit Framework – надає життєво важливу інфраструктуру для застосування графічних програм, пов'язаних із подіями на iOS. Деякі важливі функції комплекту UI Kit:

– підтримка багатозадачності;
– основне управління додатками та інфраструктурою;
– управління інтерфейсом користувача;
– підтримка подій натискань і руху.

Підсумовуючи, можна сказати що iOS є провідною операційною системою у світі мобільних пристроїв. Вона дуже добре організована, безпечна та захищена. Також вбудовані сервіси iOS дають великий простір для роботи розробників та є мають широко описані документації.

Список використаних джерел:

1. Apple Developer Documentation [Електронний ресурс]. – Режим доступу до ресурсу: https://developer.apple.com/documentation/

2. Swift Documentation [Електронний ресурс]. – Режим доступу до ресурсу: https://swift.org/documentation/

3. Ray Wenderlich Tutorials for iPhone / iOS Deelopers and Games [Електронний ресурс]. – Режим доступу до ресурсу: https://www.raywenderlich.com/

Степанов А.С.

студент,
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»

ОБЗОР КРУПНЕЙШЕЙ В ИСТОРИИ УКРАИНЫ КИБЕРАТАКИ, ЕЕ ПРИЧИН И ПУТЕЙ ПРЕДОТВРАЩЕНИЯ

Кибератака, которая была произведена 27 июня 2017 года в Украине стала самой масштабной на территории страны за всю ее историю. Была поражена работа целого ряда частных и государственных ведомств, структур и предприятий. В числе пораженных оказались сайты министерств, сайты крупнейших украинских компаний, информационные системы мобильных операторов, энергетических предприятий и даже аэропортов и метрополитенов. Под атаку попали также и медицинские компании. Была прекращена трансляция нескольких телеканалов. В общей сложности жертвами атаки стали треть украинских банков, включая одни из крупнейших банков.

Вирус, породивший атаку получил название Petya. Другие названия: Petya.A, Win32/Diskcoder.Petya, Trojan.Ransom.Petya, PetrWrap, Diskcoder.C, WannaCry-2, Trojan.Encoder.12544. Вирус использует уязвимости, которые были ранее опубликованы хакерской группой The Shadow Brokers. По

заявлениям группы, опубликованные уязвимости стали результатом взлома информационных систем Агентства национальной безопасности США (АНБ). К упомянутым уязвимостям относятся уязвимость CVE-2017-0144 (кодовое название EternalBlue) и CVE-2017-0145 (кодовое название EternalRomance). Данные уязвимости основаны на просчетах в реализации протокола SMB (Server Message Block), которые позволяют доставить вредоносную программу через TCP-порт 445.

Этим уязвимостям подвержены компьютеры под управлением операционных систем семейства Windows. Стоит заметить, что масштабная вирусная атака под названием WannaCry, которая месяцем ранее получила широкое распространение в мире, однако почти не затронув Украину, так же использовала вышеупомянутые уязвимости. Вскоре после публикаций вышеуказанных уязвимостей и до момента начала распространения атак Petya и WannaCry компанией Microsoft было выпущено обновление MS17-010 от 14 марта 2017 года, которое исправляло проблемы. Описанные уязвимости были признаны критическими, и обновления были выпущены даже для закончившей свой срок поддержки операционной системы Windows XP.

Исследования, проведенные рядом компаний среди которых Microsoft, ESET, McAfee, показали, что инициализация и основное заражение вирусом произошло с территории Украины посредством компонента обновления распространенного в стране корпоративного программного обеспечения для отчетности и документооборота – M.E.Doc. Этим объясняется высокое распространение вируса именно на территории Украины (более 75% от общего количества обнаруженных атак). Атакующие получили доступ к серверу обновлений M.E.Doc и с его помощью направляли зараженные обновления с автоматической установкой пользователям. По информации исследований, для заражения корпоративной сети достаточно одного уязвимого компьютера, на котором не были установлены обновления безопасности MS17-010. С его помощью вредоносная программа попадет в сеть, получает права администратора и распространяется на остальные компьютеры сети.

При заражении вирус Petya, который идентифицируется как ransomware-шифровальщик, т.е. шифровальщик-вымогатель, обладая правами администратора перезаписывает главную загрузочную запись жесткого диска MBR, и шифрует остальные разделы и файлы на диске. При перезагрузке компьютера перезаписанная MBR направляет пользователя на страницу с требованием перечислить выкуп за расшифровку данных.

После выявления заражений через программу M.E.Doc, ее разработчиками было выпущено исправленное нескомпрометированное обновление программы. Однако, это обновление распространялось через сайт M.E.Doc, который работает по протоколу HTTP, а не HTTPS. Это означает, что предлагаемое к загрузке обновление передается по незашифрованному каналу, и обладает уязвимостью перед MITM (Man in the middle) атакой. Так же следует отметить, что программа M.E.Doc для своей полноценной работы требует от пользователя запуск с правами администратора, что является архитектурным просчетом и нарушением принципов безопасности.

Проанализировав вышеприведенную информацию можно выделить основные пути предотвращения подобных атак в будущем. А именно:

– Использовать наиболее актуальную версию операционной системы;

– В независимости от используемой операционной системы проверять наличие актуальных обновлений или использовать автоматическое обновление;

– Использовать средства защиты в виде антивируса и файрвола, также использовать их актуальные версии и автоматические обновления;

– Использовать контроль учетных записей пользователей: по умолчанию работать с правами обычного пользователя, при необходимости требовать запрос прав администратора/суперпользователя;

– По возможности, отказываться от программ, по умолчанию требующих для работы права администратора;

– По возможности, отказываться от использования программ из ненадежных источников, канал распространения которых не зашифрован, а также исполняемых файлов без электронных подписей;

– Руководствоваться остальными правилами информационной безопасности: не запускать исполняемые файлы прикрепленные к входящей корреспонденции от неизвестных источников, не переходить по ссылкам из неизвестных источников и т.д.;

– Регулярно делать «холодное» резервное копирование данных, т.е. делать копии, изолированные от локальных и глобальных сетей.

Широкое распространение и заражение компьютерных сетей Украины посредством вируса Petya набрало государственных масштабов, стало самым крупным за всю историю страны, и выявило необходимость широкого ряда структур, организаций и предприятий более ответственно подходить к вопросу обеспечения своей информационной безопасности.

Список использованных источников:

1. ESET обнаружила сложный бэкдор, который использовался для установки шифраторов Petya и XData [Электронный ресурс]. – Режим доступа: https://www.esetnod32.ru/company/press/center/eset-obnaruzhila-slozhnyy-bekdor-kotoryy-ispolzovalsya-dlya-ustanovki-shifratorov-petya-i-xdata-/

2. Эпидемия шифратора Win32/Diskcoder.C Trojan. Рекомендации ESET [Электронный ресурс]. – Режим доступа: https://www.esetnod32.ru/company/press/center/epidemiya-shifratora-win32-diskcoder-c-trojan-rekomendatsii-eset-/

3. «Petya» Ransomware: What we know now [Электронный ресурс]. – Режим доступа: https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/

4. New ransomware, old techniques: Petya adds worm capabilities [Электронный ресурс]. – Режим доступа: https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

5. DoublePulsar malware spreading rapidly in the wild following Shadow Brokers dump [Электронный ресурс]. – Режим доступа: https://www.scmagazine.com/doublepulsar-malware-spreading-rapidly-in-the-wild-following-shadow-brokers-dump/article/652518/

6. Украина подверглась самой крупной в истории кибератаке вирусом Petya [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/331762/

7. Petya: «I Want To Believe» [Электронный ресурс]. – Режим доступа: https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/