Scientific and Practical Cyber Security Journal (SPCSJ) 3(2): 49- 53 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

Методы защиты от современных векторов кибер атак в странах Европы

Security methods against modern cyber attack vectors in countries of Europe

Георгий Иашвили[1], Максим Явич[1], Сергей Гнатюк[2] Андрей Фесенко [3]
1.Кавказский Университет, Тбилиси, Грузия
2. Национальный Авиационный Университет, Киев, Украина
3. Киевский национальный университет им. Тараса Шевченко, Киев, Украина

АННОТАЦИЯ. Для получения данных организаций, сервисов и пользователей кибер преступники прибегают к изощренным и продвинутым методам атак. К концу 2017 года европейским центром по кибер преступности – ECC была выработана стратегия по борьбе с мошенничеством и преступностью в сети. В данной статье мы проанализтровали тенденцию улучшения безопасности пользователя на примере эксперимента с фишинг тренажерами. Знание, и массивное представление распространённых видов кибер атак может послужить одним из ключевых моментов в борьбе с преступностью в интернете, столь популярной на территории Европы.

ABSTRACT. Cyber criminals use sophisticated and advanced attack methods in order to obtain the data of organizations, services and users. By the end of 2017, the European Center for Cyber Crime - ECC has developed a strategy to deal with fraud and crime in the network. In this article, we have analyzed the tendency of improving user's security using the example of an experiment with phishing simulators. Knowledge, and a massive representation of common types of cyber attacks can be one of the key moments in the fight against crime on the Internet, that is rather popular in Europe.

КЛЮЧЕВЫЕ СЛОВА: кибер атаки, атаки на Европу, кибер преступность

KEYWORDS: cyber attacks, attacks on Europe, cyber crime

Для получения данных организаций, сервисов и пользователей кибер преступники прибегают к более изощренным и продвинутым методам атак. Так в 2017 году было скомпрометировано более 2 миллиардов записей, а к началу 2018 года их количество возросло до 4.5 миллиардов. По данным мирового финансового форума одними из самых распространённых методов кибер атак в странах Европы являются: продвинутые наборы фишинга; атаки удаленного доступа; атаки с помощью смартфонов; использование уязвимостей умных домов и интернета вещей; использование искусственного интеллекта; вымогатели – ransomware [2].

Продвинутые наборы фишинга

На сегодняшний день фишинг остается самым распространённым и действенным методом атак. Несмотря на сравнительной небольшой цикл жизни фишинг сайтов (в лучшем случае 2-3 дня), охват целевой аудитории достаточно большой. Для создания фишинг схемы не требуется особых технический знаний, и даже средний пользователь сети сможет выстроить механизм атаки. С

выходом более мощных и продвинутых инструментов фишинг становится все более опасным орудием в руках злоумышленников. На просторах dark web сегодня можно встретить огромное количество наборов фишинг атак.

Атаки удаленного доступа

Количество удаленных атак растет с каждым годом, и данные атаки становятся все более изощренными. Одним из основных типов атак удаленного доступа в 2018 году был cryptojacking, нацеленный на удаленный майнинг с использованием машины жертвы. Еще одной популярной целью атак удаленного доступа является устройства с открытыми портами, которыми и пользуются злоумышленники. К данному виду устройств относятся IP камеры, сетевые устройства, и другая периферия.

Атаки с помощью смартфонов

Наиболее распространенные векторы атак на смартфоны связаны с небезопасным использованием интернет ресурсов. Владельцы портативных устройств подвержены фишингу и атакам с помощью вредоносного программного обеспечения. По данным RSA, более 60% мошенничества в интернете совершается с помощью мобильных платформ, в то время, как 80% противозаконных действий с помощью мобильных устройств достигается с помощью мобильных приложений вместо мобильных веб-браузеров [3]. Большое количество пользователей производит финансовые операции при помощи мобильных устройств в незащищенных сетях. В результате чего их данные утекают в сеть и зачастую размещаются на специальных торговых площадках в dark web. Наряду с этим, за последние годы все чаще фиксируются DDoS атаки, произведенные с помощью смартфонов.

Использование уязвимостей умных домов и интернета вещей

Согласно прогнозам экспертов из Gartner, к 2020 году количество устройств интернета вещей достигнет отметки в 7 миллиардов единиц. Подавляющее количество пользователей IoT не видят в них потенциальной угрозы в силу того, что у многих устройств попросту нет пользовательского интерфейса. Данный факт может привести к проблемам с пониманием того, какие данные устройство собирает и какими управляет.

Использование программ / скриптов вымогателей – ransomware

Раньше объектами программного обеспечения вымогателей были компьютеры. За последние годы данный тип угрозы претерпел изменения и на сегодняшний день используется для атак на всевозможные устройства. Суть ransomware заключается в шифрации файлов жертвы на компьютере либо другом умном устройстве с целью получения денежных средств в обмен на ключи для расшифровки файлов.

Согласно проведенному ENISA – ом анализу, в 2018 году происхождение и методы примерно 21% проведенных атак так и не были установлены. В Threat Landscape Report – е сообщается, что пользователи и организации из стран Европы подвергались большому количеству до тех пор неизвестным атакам со стороны злоумышленников, что подтверждает приведенная статистика (рис. 1). В список так же вошли атаки типа DDoS и Brute force, но уже с явным отставанием, так как большинство современных механизмов защиты с легкостью отражают подобные атаки [4].

Рис.1

Такое количество неизвестных атак обусловлены очень частым выходом новых векторов атак, а также всевозможными вредоносными программами / скриптами, которые пока не изучены, следовательно, защитные механизмы против них и сопутствующая информация выходят с определенной задержкой.

Следующие по списку похищения профилей и целевые атаки, напрямую связанные с разнообразными веб ресурсами, будь то социальная сеть, либо информационный сайт. Довольно прибыльный вид атак, так как получив нужные данные, злоумышленники продают их на специальных ресурсах.

Но на первом месте несмотря на известные векторы атак остается вредоносное программное обеспечение. Злоумышленники под разными предлогами подкладывают жертвам всевозможные скрипты и программы, с помощью которых в результате производятся атаки разных категорий.

Методы борьбы с кибер преступностью

К концу 2017 года европейским центром по кибер преступности – ECC была выработана стратегия по борьбе с мошенничеством и преступностью в сети. Каждый квартал агентство публикует данные и тенденции развития в направлении кибер безопасности. Система ECC основана на трех основных компонентах: кибер стратегия; судебная экспертиза; спец операции.

Борьба с кибер преступностью напоминает вечную погоню. Только получается выявить новый вектор атак и организовать соответствующий защитный механизм против него, как на рынке появляется что-то совершенно новое, поражающее десятки, а то и сотни тысяч пользователей. Особо актуальной целью хакеров являются страны Европы. Из-за большого масштаба и развития технологий, объектов для атаки с каждым годом становится все больше.

Международными организациями предпринимаются определенные меры для предотвращения глобальных кибер атак. Для более четкого контроля данных и уменьшения утечек данных пользователей из стран Европы, в мае 2018 года был установлен общий регламент по защите данных GDPR — General Data Protection Regulation. Согласно GDPR посетителя веб сайта необходимо в максимально понятной форме оповещать о любой попытке получения и обработки его персональных данных этим ресурсом.

Основным и более действенным методом борьбы с ориентированными на пользователя кибер атаками является повышение уровня знаний в отрасли кибер безопасности у сотрудников организаций. Зачастую работники даже не подозревают о существовании того или иного вида атак, что служит причиной утечек ценных данных.

Тренировка сотрудников должна стать неотъемлемой частью механизма защиты организации от кибер атак. По заявлению IT Governance в 2017 – 2018 годах процент успешных атак на пользователей – сотрудников компаний существенно возрос по сравнению с предыдущими годами. В марте нынешнего года knowbe4 опубликовали статистику результатов годового фишинг тренинга сотрудников различных крупных и малых организаций в странах Европы. Параллельно проводился анализ успешно прошедших атак на этих пользователей (рис. 2).

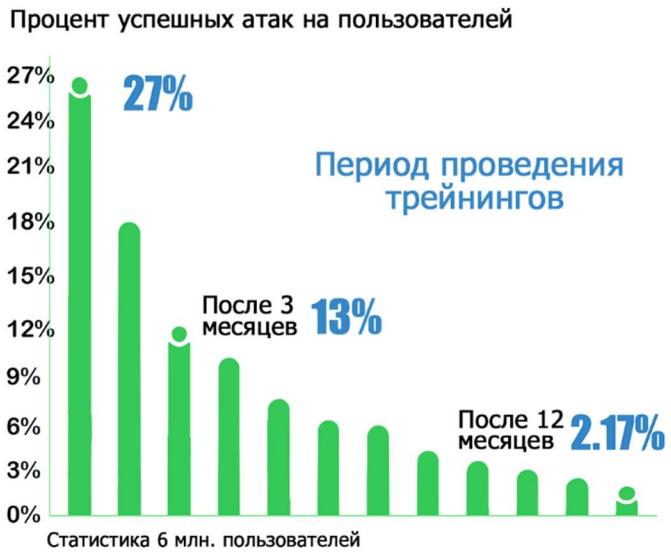

Рис. 2

Для анализа и проведения атак использовались различные фишинг симуляторы, с помощью которых отсылались письма с вредоносными ссылками, контентом и прикрепленными файлами. По результатам эксперимента, за один год тренинга процент попадания на фишинг уловки сократился с 27% до 2.17%, что безусловно положительно сказалось на общем развитии пользователей, и количестве утекшей в сеть конфиденциальной информации.

Мы считаем, что тренинги с участием работников крупных, средних, а также малых организации по основным направлениям кибер безопасности и разновидностям кибер атак положительно скажутся на общей картине кибер безопасности в странах Европы. В данной статье мы разобрали тенденцию улучшения безопасности пользователя на примере эксперимента с фишинг тренажерами. Подобные тренинги необходимо проводить регулярно, охватываю все больше тематик и современных векторов атак. Лучшее оружие для пользователя интернета - это знание, и массивное представление распространённых видов кибер атак может послужить одним из ключевых моментов в борьбе с преступностью в интернете, столь популярной на территории Европы.

Использованная литература:

[1] Center for strategic and international studies - Significant Cyber Incidents, May 2019 https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

[2] Einaras von Gravrock - Here are the biggest cybercrime trends of 2019, March 2019 - https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

[3] RSA - CURRENT STATE OF CYBERCRIME, 2018 https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

[4] Radware - Mobile Security Threats on The Rise as Hackers Can Launch DDoS Attacks on Their Mobile Phones, 2016 https://security.radware.com/ddos-threats-attacks/cyber-attacks-in-the-palm-of-your-hand/