УДК 004.056

Краткий социально-экономический профиль киберпреступника и технологии атаки Magecart

Рассмотрен современный рынок киберпреступности и вредоносного программного обеспечения.
Сформирован краткий социально-экономический профиль киберпреступника.
Проведено исследование актуальных подходов/методов, используемых киберпреступниками для реализации атаки Magecart, приводящей к массовому экономическому и репутационному ущербу в системах электронной коммерции.

Ключевые слова:
вредоносное программное обеспечение, краткий социально-экономический профиль киберпреступника, атака Magecart.

В.В. МАЛИКОВ,
канд. техн. наук, доцент,
начальник цикла технических и специальных дисциплин
УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД РБ

Введение. В настоящее время в мире и Республике Беларусь происходит стремительный и масштабный переход экономических отношений с потребителем на цифровые технологии.

Общение между производителями и потребителями различной продукции и услуг осуществляется, как правило, удаленно по цифровым каналам сопряжения и коммуникации. Одновременно с такими процессами в обществе значительно активизируется деятельность различного рода киберпреступников, которые используют возможности современных технологий в своих криминальных целях (рис. 1).

Приведенные в рамках данной статьи материалы носят исключительно научно-исследовательский характер. Исследование проводилось авторами строго в научных целях, его результаты не являются и не могут признаваться руководством к совершению каких-либо противоправных действий. При проведении исследования авторы действовали в рамках

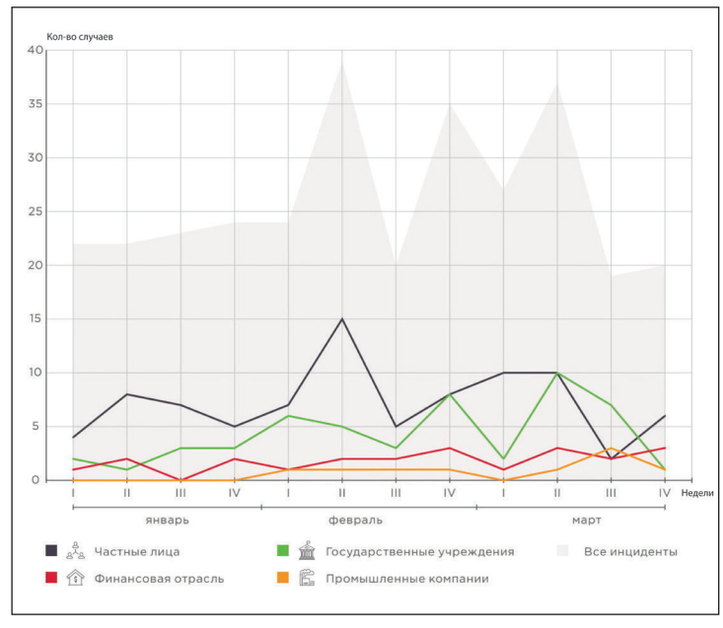
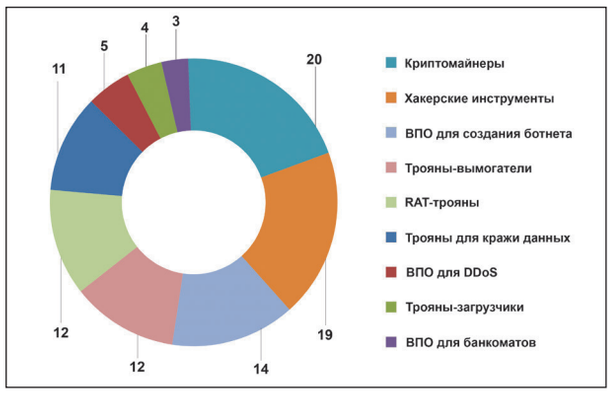


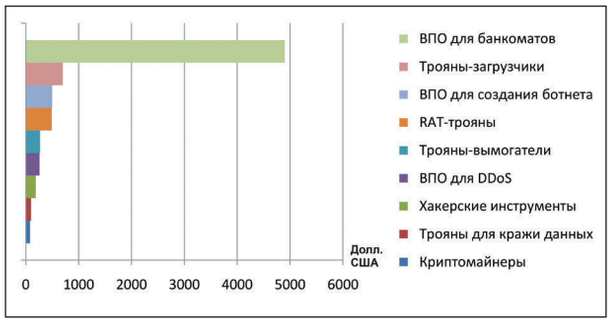
Рисунок 1 – Статистика по киберинцидентам в I квартале 2018 г. [1]

законодательства Республики Беларусь. Авторы не несут ответственности за инциденты в сфере информационной безопасности, имеющие отношение к тематике исследования.

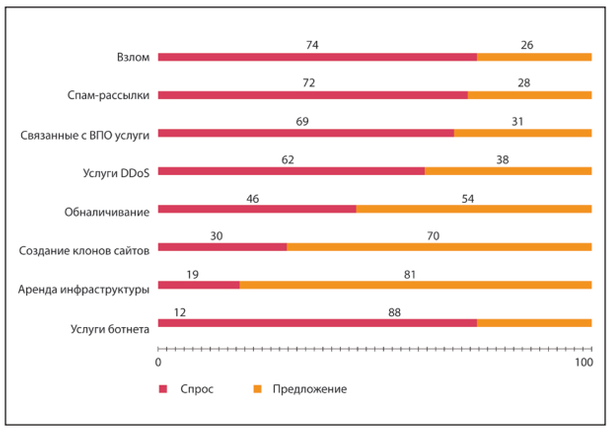
Содержательная постановка задачи. Согласно данным исследований [1, 2], криминальная деятельность киберпреступников имеет централизованную структуру и сформированную иерархию коммуникаций/отношений. При этом в настоящее время спрос на вредоносное программное обеспечение (ВПО) по многим позициям опережает предложение, что в свою очередь ведет к развитию рынка ВПО и повышению надежности оказываемых криминальных услуг (рис. 2).



а) доли объявлений о продаже ВПО разных типов, %



б) средняя стоимость ВПО



в) соотношение спроса и предложения услуг на рынке киберуслуг, %

Рисунок 2 – Статистические данные по рынку ВПО [1, 2]

Для формирования новых и повышения эффективности существующих подходов в борьбе с криминальной деятельностью киберпреступников необходимо понимание социально-экономического профиля киберпреступника, факторов и предпосылок, способствующих осуществлению ими противоправной деятельности.

В рамках настоящей статьи:

– проведем оценку современного рынка киберпреступности и сформируем краткий социально-экономический профиль киберпреступника;

– выполним исследование актуальных подходов/методов, используемых киберпреступниками для реализации атаки Magecart [3], приводящей к массовому экономическому и репутационному ущербу в системах электронной коммерции.

Результаты и обсуждение. По результатам проведенного анализа отчетов вендоров, криминальных сайтов/чатов по рынку киберпреступности [1, 2, 3], а также профилей 59 преступников (актуальный розыск ФБР (США), раздел Cyber's Most Wanted) [4] (рис. 3) автором предлагается краткий социально-экономический профиль киберпреступника (табл. 1), позволяющий дать характеристику уровня его подготовки, опыта, мотивации и степени общественной опасности.

Таблица 1 – Краткий социально-экономический профиль киберпреступника

Квалификационная характеристика	Детализация	Дополнительные параметры
Гражданство	Страна / дата приобретения гражданства	Наличие двойного гражданства (страна / дата приобретения гражданства)
Дата рождения	Дата / место рождения	Пол: мужской/женский
Место проживания / регистрации	Страна / адрес проживания (регистрации)	Дата проживания
Социальное положение	Холост/женат/разведен/вдовец (для мужчин)	Наличие детей (страна/место проживания/возраст)
Образование (базовое)	ВУЗ (специальность/квалификация)	Очное/заочное/дистанционное обучение
Опыт работы (лет)	до 1, 1–3, 3–5, 5–10, более 10 лет	Компания/должность, основные выполненные проекты
Криминальный опыт работы (лет)	до 1, 1–3, 3–5, 5–10, более 10 лет	Выполненные проекты, рекомендации, наличие судимости (статья/срок), нахождение в розыске (статья / решение суда), используемые псевдонимы
Опыт службы в силовых структурах	Возможность поддержания контакта с правоохранительными органами	Знание законодательства, оперативных методов/форм работы силовых структур
Режим занятости	Полный/сменный (по графику)	Наличие испытательного срока
Работа в команде	Руководитель/подчиненный	Выполненные проекты/результаты
Оплата труда	Фиксированная/сдельно-премиальная	Возможность легализации доходов, полученных криминальным путем
Социально-коммуникационные навыки	Навыки ведения переговоров, умение манипулировать людьми	Работа в режиме многозадачности, стрессоустойчивость
Степень общественной опасности	Не опасен / опасен / особо опасен	Склонность к сокрытию от правосудия, к побегу, возможность потенциального использования оружия

ИХ РАЗЫСКИВАЕТ ФБР

АЛЕКСЕЙ БЕЛАН

Сговор с целью совершения компьютерного мошенничества и злоупотребления компьютерами; несанкционированный доступ к компьютерам с целью получения коммерческой выгоды и личной финансовой выгоды; повреждение компьютера путем передачи кода и команд; промышленный шпионаж; кража коммерческой тайны; мошенничество с использованием устройств доступа; кража личных данных при отягчающих обстоятельствах; мошенничество с использованием электронных средств связи

ПРИМЕТЫ

Псевдонимы: Алексей Белан, Алексей Алексеевич Белан, Абыр Валгов, «Abyrvalg», «Fedyunya», «Magg», «M4G», «Moy.Yawik», «Quarker»

Использованные даты рождения: 27 июня 1987г.	**Место рождения:** Рига, Латвия
Цвет волос: каштановый	**Глаза:** голубые
Рост: 6 футов (183 см)	**Вес:** 172 фунта (78 кг)
Пол: мужской	**Раса:** белый
Род деятельности: компьютерный/сетевой инженер, программист	
Номер, присвоенный в Национальном центре информации о преступности: W507648159	**Национальность:** латвиец

ВОЗНАГРАЖДЕНИЕ

ФБР предлагает вознаграждение в сумме до 100,000 долларов США за информацию, ведущую непосредственно к аресту Алексея Белана.

ПРИМЕЧАНИЕ

Белан является гражданином России; также известно, что у него есть российский паспорт. Говорит по-русски; возможно, совершает поездки в Россию, Грецию, Латвию, на Мальдивы и в Таиланд. Может пользоваться очками и перекрашивать каштановые от природы волосы в рыжий цвет или становиться блондином. Последнее известное местонахождение Белана - Краснодар, Россия.

ВНИМАНИЕ: РОЗЫСК!

Алексею Белану были трижды предъявлены официальные обвинения за преступления, имеющие отношение к взломам компьютеров. В период с января 2014 г. по декабрь 2016 г. Алексей Белан предположительно вступил в сговор с сотрудниками российских спецслужб, включая Дмитрия Александровича Докучаева, Игоря Анатольевича Сушин и других. Целью сговора являлось получение несанкционированного доступа к компьютерным сетям и к учётным записям пользователей, хостинг которых обеспечивался крупными компаниями, предоставлявшими веб-сервис электронной почты, а

Рисунок 3 – Пример (показана часть) краткого профиля киберпреступника (актуальный розыск ФБР (США), раздел Cyber's Most Wanted) [4]

На данный момент в мире злоумышленники активно реализуют атаки Magecart [3, 5] (рис. 4), направленные на похищение данных банковских карт пользователей сетевых ресурсов. В ходе такой атаки взламываются сайты, использующие открытую E-commerce-систему для организации электронной коммерции Magento [6]. Технологии взлома имеют разнонаправленный характер и используют уязвимости систем управления контентом (Content Management System, CMS) или их плагинов.

По последним данным [3], атаками Magecart сейчас занимаются как минимум семь хакерских групп, от деятельности которых пострадали уже более 100 000 магазинов электронной торговли. Выявлен факт продажи порядка 3000 скомпрометированных ресурсов, стоимость доступа к которым варьируется от 0,5 до 1000 долл. США [7].

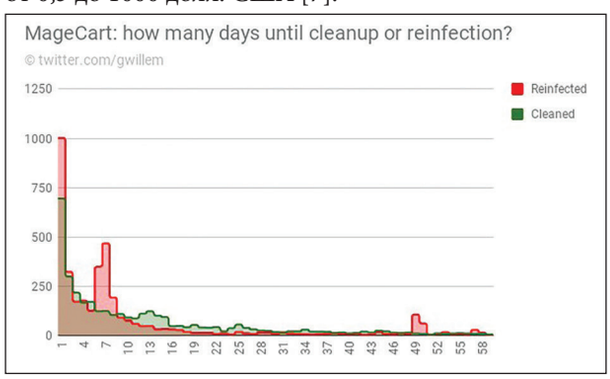
Проведем исследование сетевых ресурсов, использующих E-commerce-систему Magento, на предмет наличия уязвимостей (открытая база уязвимостей сервиса Vulners [8], сетевой сканер Censys [9], сетевой сканер Magereport [10]), а также способов их эксплуатации через сетевые каналы сопряжения и коммуникации.

По результатам проведенного исследования (табл. 2) можно сделать выводы:

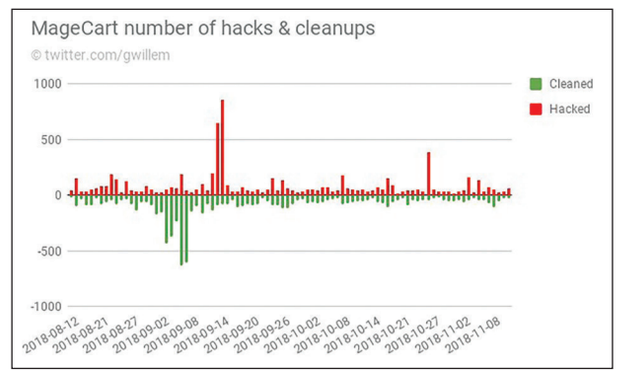
– множество сетевых ресурсов имеют доступ к портам/протоколам «21/ftp» (48 278 шт.), «23/telnet» (53 шт.), «445/smb» (76 шт.), которые содержат большое число уязвимостей, в т. ч. в составе вредоносных эксплойт-паков [8];

– при этом совместное использование портов/протоколов «23/telnet» и «21/ftp» (23 шт.), «445/smb» и «21/ftp» (21 шт.) значительно понижает уровень информационной безопасности исследованных сетевых ресурсов [10].

В ходе проведенного дополнительного исследования [8, 9, 10] 44 сетевых ресурсов на основе Magento [6] с использованием портов/протоколов «23/telnet» и «21/ftp» (23 шт.), «445/smb» и «21/ftp» (21 шт.) выявлено 11 ресурсов (25 %), имеющих высокую вероятность взлома злоумышленниками. Детальное тестирование одного уязвимого сетевого ресурса (табл. 3) на предмет реализации атаки Magecart показало значительное число уязвимостей, что демонстрирует отсутствие должного внимания владельцев ресурса к обновлению и модернизации эксплуатируемого ПО.



а) зависимость случаев реинфекции/отражения атаки Magecart (количество/дни)



б) зависимость случаев атак хакеров / активности служб безопасности (количество/дата)

Рисунок 4 – Статистические данные по активности реализации атаки Magecart [5]

Таблица 2 – Результаты тестирования хостов, использующих Magento

Описание проводимого теста	Описание запроса теста (сетевой сканер Censys [9])	Результаты теста, шт.
Количество хостов (IPv4 Hosts), использующих Magento [6]	Magento	102 379
Количество хостов (IPv4 Hosts), использующих Magento с открытым портом «2323/telnet» или «23/telnet»	(Magento) AND protocols: «2323/telnet»	13
	(Magento) AND protocols: «23/telnet»	40
Количество хостов (IPv4 Hosts), использующих Magento с открытым портом «21/ftp»	(Magento) AND tags.raw: "ftp"	48 278
Количество хостов (IPv4 Hosts), использующих Magento» с открытым портом «445/smb»	(Magento) AND protocols: "445/smb"	76
Количество хостов (IPv4 Hosts), использующих Magento с открытыми портами «23/telnet» и «21/ftp»	((Magento) AND protocols: "23/telnet") AND protocols: "21/ftp"	23
Количество хостов (IPv4 Hosts), использующих Magento с открытыми портами «445/smb» и «21/ftp»	((Magento) AND protocols: "445/smb") AND protocols: "21/ftp"	21

Таблица 3 – Результаты тестирования уязвимого сетевого ресурса

Параметр	Показатель/значение
IP-адрес	78.47.31.171
Операционная система	Ubuntu (v. 2.0)
Страна	Germany (DE)
Номер ASN	AS7018 , AS1299 , AS24940
Используемые протоколы	80/HTTP, 2323/TELNET, 21/FTP, 8080/HTTP, 443/HTTPS, 22/SSH
Веб-сервер	nginx
Уязвимость к атаке Magecart [10]	Уязвим (высокий уровень)
Неустановленная сборка безопасности / дата выхода сборки / имеющиеся уязвимости [6]	SUPEE-10266 /14.09.2017/ Privilege Escalation, Remote Code Execution (RCE), Information Leak (system), Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS, stored), Insufficient Session Expiration
	SUPEE-10415 /28.11.2017/ Denial-of-Service (DOS), XSS (stored), RCE
	SUPEE-9767 /31.05.2017/ RCE, SQL Injection, XSS (reflected, stored), CSRF, Privilege Escalation, Information Leak (system), Insufficient Data Protection, Misc Vulnerabilities, Abuse of Functionality
	Patch SUPEE-8788 /12.10.2016/ RCE, SQL Injection/Improper validation, XSS (reflected, stored), Information Leakage, Insufficient data protection, DOS, CSRF, Man-in-the-Middle (MitM), Timing attack

Заключение. На основании проведенных исследований можно сделать следующие выводы:

1. Рынок киберпреступности имеет централизованную структуру и сформированную иерархию коммуникаций/отношений. Имеются предпосылки к его дальнейшему росту и большей структурированности [2, 4].

2. При отсутствии анализа социально-экономического профиля киберпреступников (см. табл. 1) эффективность имеющихся подходов/методов борьбы с их противоправной деятельностью значительно снижается.

3. В настоящее время в сетевых ресурсах, использующих открытую E-commerce-систему для организации электронной коммерции Magento, имеется значительное число уязвимостей (см. табл. 2, 3). Следует отметить, что уже давно существую сборки безопасности (патчи SUPEE: 8788, 9767, 10266, 10415 и др.[6]), устраняющие выявленные уязвимости (даты выхода патчей: май–ноябрь 2017 г.).

ЛИТЕРАТУРА

1. Актуальные киберугрозы I квартал 2018 года // ptsecurity.com [Электрон. ресурс]. – 2018. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q1-rus.pdf. – Дата доступа: 15.11.2018.
2. Рынок преступных киберуслуг // ptsecurity.com [Электрон. ресурс]. – 2018. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/darkweb-2018/. – Дата доступа: 16.11.2018.
3. Riskiq // riskiq.com [Электрон. ресурс]. – 2018. – Режим доступа: https://www.riskiq.com/research/inside-Magecart/. – Дата доступа: 17.11.2018.
4. Cyber's Most Wanted // fbi.gov [Электрон. ресурс]. – 2018. – Режим доступа: https://www.fbi.gov/wanted/cyber. – Дата доступа: 17.11.2018.
5. Merchants struggle with Magecart reinfections // gwillem.gitlab.io [Электрон. ресурс]. – 2018. – Режим доступа: https://gwillem.gitlab.io/2018/11/12/merchants-struggle-with- Magecart-reinfections/. – Дата доступа: 18.11.2018.
6. Magento // magento.com [Электрон. ресурс]. – 2018. – Режим доступа: https://magento.com/. – Дата доступа: 19.11.2018.
7. Access to over 3,000 backdoored sites sold on Russian hacking forum // zdnet.com [Электрон. ресурс]. – 2018. – Режим доступа: https://www.zdnet.com/article/access-to-over-3000-backdoored-sites-sold-on-russian-hacking-forum/. – Дата доступа: 19.11.2018.
8. Vulners // vulners.com [Электрон. ресурс]. – 2018. – Режим доступа: https://vulners.com/. – Дата доступа: 20.11.2018.
9. Censys // censys.io [Электрон. ресурс]. – 2018. – Режим доступа: https://censys.io/. – Дата доступа: 21.11.2018.
10. Magereport // magereport.com [Электрон. ресурс]. – 2018. – Режим доступа: https://www.magereport.com/scan/. – Дата доступа: 21.11.2018.

The modern market of cybercrime and malicious software is considered. A brief socio-economic profile of a cybercriminal is formed.

A study of current approaches/methods used by cybercriminals to implement Magecart attack, leading to massive economic and reputational damage in e-commerce systems is carried out.

Получено 24.11.2018.