М. А. Баранов, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень
УДК 004.056

ИССЛЕДОВАНИЕ МЕТОДОВ НАСТУПАТЕЛЬНОЙ ЗАЩИТЫ ДЛЯ ДЕАНОНИМИЗАЦИИ ЗЛОУМЫШЛЕННИКА

Аннотация. В данной статье представлен обзор методов наступательной защиты, которые помогают выявить личность киберпреступника, а также предлагаются пути улучшения эффективности данных методов.

Ключевые слова: деанонимизация, контратака, наступательная безопасность, honeypot, сканеры уязвимостей.

Введение. С каждым годом увеличивается число атак на различные информационные системы. Государственные и коммерческие организации, в основном, используют только пассивные методы защиты. Согласно отчету от компании Ростелеком-Солар [1], число кибератак на российские компании в 2022 г. составило 911 тыс., что в два раза больше, чем в 2021. Злоумышленники постоянно придумывают новые методы атак, улучшают свои навыки и анонимность. Вследствие чего, правоохранительным органам все труднее раскрывать их личность.

Для более глубокого изучения данного направления мы использовали различные источники. Так, например, в статье [2] изучается проблема киберпреступлений и их раскрытия. В статьях [3, 4] авторами исследуются различные методы обнаружения и идентификации злоумышленника. Основой для дальнейшей работы стали статьи [5, 6], в которых авторы предлагают методы атак для выявления личности злоумышленника. Изучив научные работы различных авторов, можно сделать вывод, что данная тема является актуальной и требует дальнейшего развития.

Проблема исследования. Для деанонимизации следует использовать активные методы обороны, контратаковать злоумышленника. Однако, на данный момент, методы контратаки почти не используются организациями. Задачей данной работы является исследование существующих методов наступательной защиты, с целью выявить

причины, по которым они не используются и предложить идеи по улучшению.

Материалы и методы. Для решения данной задачи были изучены несколько научных работ. В [5] статье авторы изучают уязвимости сканеров уязвимостей путем разработки прототипа, который сможет доказать, что сканирующая сторона может быть атакована сканируемой, с помощью атаки типа XSS (межсайтовый скриптинг). Суть работы сканеров уязвимостей (рис. 1) состоит из четырех этапов: если сканируемая сторона сможет подменить этап 4 (отчет), то сканирующая сторона может получить различную полезную нагрузку. После разработки прототипа были проведены тесты 78 различных сканеров уязвимостей, 36 из которых (46%) были признаны уязвимыми (рис. 2).

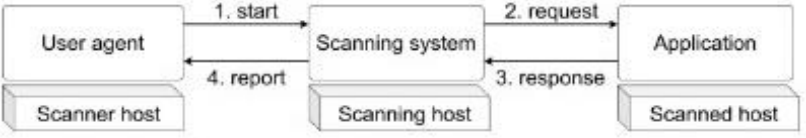

Рис. 1. Схема работы сканеров уязвимостей

	Name	T	V	M	Name	T	V	M	Name	T	V	M
	AddMe	11	11	✓	InternetOfficer	2	1	✓	Security Headers	13	-	
	AdResults	14	-		*[Anonymous]*†	11	1	✓	SEO Review Tools	-	-	
	Arachni	14	-		iplocation.net	-	-		SeoBook	12	11	✓
	AUKSEO	-	-		IPv6 Scanner	-	-		SERP-Eye	-	-	
	BeautifyTools	13	-		itEXPERsT	-	-		Server Headers	13	12	✓
	BrowserSPY	9	-		IVRE	2	-		Site 24x7	13	13	✓
	CheckHost	1	-		JoydeepDeb	13	13	✓	SQLMap Scanner	1	1	✓
	CheckMyHeaders.com	1	-		JSON Formatter	13	13	✓	SSL Certificate Tools	12	-	
	CheckSERP	11	-		LucasZ ZeleznY	2	1	✓	StepForth	12	11	✓
	CheckShortURL	1	1	✓	Metasploit Pro	11	3	✓	StraightNorth	-	-	
	Cloxy Tools	11	-		Monitor Backlinks	12	-		SubnetOnline	14	13	✓
	CookieLaw	1	-		Nessus	11	-		Sucuri Site Check	3	-	
	CookieMetrix	2	1	✓	Nikto Online	2	2	✓	SureOak	9	8	✓
	DNS Checker	1	1	✓	Nmap	14	-		TheSEOTools	1	1	✓
	DNSTools	-	-		Nmap Online	12	1	✓	Tutorialspots	13	13	✓
	Dupli Checker	1	-	✓	Online SEO Tools	12	12	✓	Url X-Ray	1	-	
	evilacid.com	12	12	✓	OpenVAS	3	-		Urlcheckr	10	-	
	expandUrl	1	-		OWASP ZAP	4	-		Urlex	-	-	
	FreeDirectoryWebsites	13	13	✓	Pentest-Tools	2	1	✓	w-e-b.site	13	13	✓
	GDPR Cookie Scan	-	-		Port Checker	10	-		W3dt.Net	12	11	✓
	GeekFlare	12	-		Redirect Check	11	10	✓	Web Port Scanner	-	-	
	Hacker Target	13	-		Redirect Detective	2	-	✓	Web Sniffer	14	-	
	HTTP Tools	12	12	✓	ReqBin	13	-		WebConfs	13	12	✓
	httpstatus.io	14	-		Resplace	12	-		WebMap	14	1	✓
	InsightVM	3	-		RexSwain.com	13	1	✓	What Is My IP	12	-	
	InternetMarketingNinjas	1	-		Search Engine Reports	1	1	✓	WMap	12	10	✓

Рис. 2. Результаты проверки количества уязвимых потоков сканеров уязвимостей

В работе [6] был разработан новый метод контратаки для выявления личности киберпреступника, использующего VPN (Virtual private network). Для реализации данного метода используется Honeypot («горшочек с медом»). Honeypot — это уязвимая система, приманка для злоумышленника, при проникновении в которую, защищающаяся сторона может отслеживать действия и методику атак хакеров [7]. Внутри Honeypot мы размещаем honeytokens (файлы-приманки) форматов PDF, DOCX, XLS и так далее, содержащие вредоносный код.

Результаты. Авторы статьи разработали алгоритм (рис. 3), позволяющий удалить VPN из реестра ОС злоумышленника, что в дальнейшем позволит его деанонимизировать. На рис. 4 можно увидеть схему работы данного метода.

Algorithm 1 To Defeat the VPN in Counterattack

```
INITIALIZE: OS-info [], Presisinfo[]
foreach All-Software's-with-persistence[]
  in software []
        Presisinfo [] ← software-Name
        Presisinfo [] ← software-location
end
foreach Presisinfo [] in soft do
    Remove Registry Value(soft)
end
foreach startupfolder-software[] in soft do
     Delete (soft)
end
Startupfolder←Download←custom-information-
  gather.exe
Reboot()
```

Рис. 3. Алгоритм удаления VPN из реестра

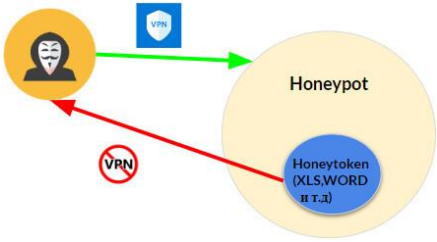

Рис. 4. Схема работы метода с использованием Honeypot

Однако данный метод не может применяться на практике организациями, так как такой способ выявления личности не является законным, что является чуть ли не основным критерием. Также, при применении на практике, организации могут столкнуться с проблемой выявления личности опытных преступников, так как данный метод атаки легко распознаваем, и злоумышленник может легко избежать деанонимизации.

Для решения вышеописанных проблем мы предлагаем использовать методы машинного обучения, а также сотрудничество с правоохранительными органами. Алгоритмы машинного обучения могут помочь лучше изучить поведение и методы злоумышленника для дальнейшей организации контратаки. Сотрудничество с правоохранительными органами позволит добиться легального использования методов контратак, тем самым улучшив количество раскрытых киберпреступлений.

В результате данной работы исследованы существующие методы контратаки с целью деанонимизации, выявлены их недостатки и предложены способы улучшения этих методик.

Заключение. Проблема выявления личности киберпреступников еще долгое время будет оставаться актуальной. Существующих методов недостаточно для улучшения количества раскрытых киберпреступлений. В будущем мы планируем разработать собственный метод, который будет учитывать недостатки предыдущих решений и сможет легально применяться организациями на практике.

СПИСОК ЛИТЕРАТУРЫ

1. Кибератаки на российские компании в 2022 году. — Текст: электронный // Ростелеком-Солар официальный сайт компании: [сайт]. — URL: https://rt-solar.ru/analytics/reports/3332/ (дата обращения: 25.04.2023).
2. Дерюгин, Р. А. Киберпреступность в России: современное состояние и актуальные проблемы / Р. А. Дерюгин. — Текст : электронный // Вестник уральского юридического института МВД России. — 2019. — № 2. — URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-sovremennoe-sostoyanie-i-aktualnye-problemy/viewer (дата обращения: 01.05.2023).

3. Басыня Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский. — Текст : электронный // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2019. — Т. 22, №. 2. — URL: https://cyberleninka.ru/article/n/metod-identifikatsii-kiberprestupnikov-ispolzuyuschih-instrumenty-setevogo-analiza-informatsionnyh-sistem-s-primeneniem-tehnologiy/viewer (дата обращения: 01.05.2023).
4. Перевозчиков В. А. Разработка и реализация метода обнаружения злоумышленника с использованием сетевого протокола FTP / В. А. Перевозчиков, А. О. Прокофьев, Т. А. Шаймарданов. — Текст : электронный // Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов им. ЕВ Арменского. — 2017. — С. 328–329. — URL: https://elibrary.ru/item.asp?id=29157361 (дата обращения: 02.05.2022).
5. Valenza, A. Never Trust Your Victim: Weaponizing Vulnerabilities in Security Scanners / A. Valenza, G. Costa, A. Armando. — Text: electronic. // 23rd International Symposium on Research in Attacks, Intrusions and De fenses (RAID 2020). — 2020. — URL: https://www.usenix.org/system/files/raid20-valenza.pdf (date of the application 10.05.2023)
6. Rana M. U. Offensive Security: Cyber Threat Intelligence Enrichment With Counterintelligence and Counterattack / M. U. Rana [et al.]. — Text : electronic. // IEEE Access. — 2022. — T. 10. — URL: https://ieeexplore.ieee.org/abstract/document/9915579/ (date of the application 10.05.2023)
7. Что такое honeypot? Как ловушки служат кибербезопасности. — Текст: электронный // Защитные решения кибербезопасности для дома и бизнеса | Лаборатория Касперского : [сайт]. — URL: https://www.kaspersky.ru/resource-center/threats/what-is-a-honeypot (дата обращения: 11.05.2023).