Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ІННОВАЦІЇ

Матеріали Міжнародної науково-практичної конференції

(м. Дніпро, 4 листопада 2021 р.)

Дніпро
2021

УДК 33+004+4+35
Е40

Схвалено науково-методичною радою
Дніпропетровського державного університету
внутрішніх справ протокол № 3 від 18.11 2021)

Е 40 **Економічна та інформаційна безпека: актуальні питання та інновації** : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 4 листоп. 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 399 с.

ISBN 978-617-8032-40-1

Збірник містить матеріали однойменної міжнародної науково-практичної конференції. У заході взяли участь науковці, викладачі та здобувачі вищих навчальних закладів та наукових установ України і зарубіжжя, а також фахівці-практики правоохоронних органів. Тематика публікацій охоплює актуальні питання економічної та інформаційної безпеки.

Матеріали конференції можуть бути використані в науково-дослідній роботі та навчальному процесі спеціалізованих ВНЗ, а також у законотворчості та правоохоронній діяльності.

ISBN 978-617-8032-40-1

З М І С Т

ТЕЗИ ВИСТУПІВ

КУРСАНТИ ТА СТУДЕНТИ

Волчок Є. В.,
здобувач 2-го курсу магістратури
Одеського державного
університету внутрішніх справ,
співробітник відділу security analyst
ТОВ «Група інформаційної безпеки
«ФС ГРУП», м. Одеса

Науковий керівник – Ісмайлов К. Ю.,
старший науковий співробітник НДЛ
з проблемних питань кримінального
аналізу Одеського державного
університету внутрішніх справ,
начальник 5-го відділу 3-го управління
ДКП НПУ, кандидат юридичних наук,
доцент, підполковник поліції

ЕКСПЛУАТАЦІЯ ВРАЗЛИВОСТЕЙ В МОБІЛЬНІЙ КРИМІНАЛІСТИЦІ IOS-ПРИСТРОЇВ

Внаслідок розвитку інформаційних технологій та різноманітної електронно-обчислювальної техніки, таких як комп'ютери, ноутбуки, мобільні телекомунікаційні пристрої, з'являються нові методи та заходи захисту інформації від несанкціонованої передачі та витоку її.

В багатьох пристроях як первинний захист використовується метод шифрування накопичувача різними засобами: як запроваджений розробником операційної системи (Google або Apple, якщо ми говоримо про мобільні пристрої), так і безпосередньо виробниками пристроїв.

В нашому випадку мова буде йти безпосередньо про витяг і подальший криміналістичний аналіз отриманої інформації з Apple пристроїв на основі операційної системи iOS (iPhone, iPod) та iPadOS (iPad), їх методи захисту Secure Enclave Protection (TouchID, FaceID), DAP та їх можливі вразливості як апаратного, так і програмного характеру. Оскільки пристрої виробництва Apple досить поширені серед населення (приблизно 30–40 % від загальної кількості смартфонів на території України), тому має сенс звернути увагу саме на цей прошарок, адже на сьогодні є багато методів щодо отримання інформації з пристроїв на операційній системі Android (як апаратними методами, так і за допомогою програмних властивостей безпосередньо від розробників цих самих пристроїв або операційної системи). Наприклад, компанія Samsung розробила власну систему захисту даних Knox, але навіть вона беззахисна в деяких випадках. Нижче наведені порівняльні таблиці 1 і 2 з кількістю знайдених вразливостей на Android та iOS за весь час [1, 2]:

Таблиця 1

Кількість знайдених вразливостей в Android

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2009	5	3							1			
2010	1	1	1									
2011	9	1	1		1		1		4	1	3	
2012	7	5	3	2						1		1
2013	4		1	1	1				1	1	1	
2014	12	2	4	1		1			1	2	1	1
2015	95	46	49	50	37				13	14	17	
2016	500	104	72	91	38				47	96	236	
2017	840	86	206	170	32			1	30	113	36	
2018	609	32	84	143	12	2	1	2	17	63	3	
2019	491	37	107	41	24	3		1	39	22	1	
2020	859	46	97	104	27	9		5	148	97	3	
2021	394	17	44	35	33	2		3	40	10	6	
Total	3826	380	669	638	205	17	2	12	341	420	307	2
% of all		9.9	17.5	16.7	5.4	0.4	0.1	0.3	8.9	11.0	8.0	

Отже, метою нашого дослідження є використання різноманітних програмних та апаратно-програмних методів і способів для можливості отримання інформації з пристроїв Apple для проведення оперативно-розшукових заходів та проведення криміналістичного аналізу отриманої інформації. А саме приклад буде наведений на основі застосування мініатюрного комп'ютера Raspberry Pi 4 [2].

Цей пристрій завдяки розміру, форм-фактору та автономності дозволяє зручно переносити буквально в кишені і використовувати його під час проведення слідчих дій, виїзду до місця скоєння правопорушення, або під час затримання підозрюваного суб'єкта без застосування ПК, ноутбука або іншого типу ЕОМ.

Таблиця 2

Кількість знайдених вразливостей в iOS

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2007	1		1	1								
2008	1	1	1									
2009	10	2	3	2	2				2	3		
2010	20	11	9	5	3				4	2	1	
2011	83	52	7	6	6		5		7	13	1	
2012	155	114	70	67	60		8		15	9	1	
2013	95	57	50	42	46		4		17	9	1	
2014	120	50	51	35	33			1	20	24	4	
2015	386	232	211	184	191			5	44	63	13	1
2016	168	113	79	81	81		3		8	42	11	
2017	388	241	222	210	194		14		39	63	5	
2018	125	63	63	55	50		1		19	19	2	
2019	354	9	101	101	167	2	14			26	5	
2020	305	17	141	57	60		8	2	6	13	5	
2021	244	14	118	22	26		5	3	7	6	7	
Total	2455	976	1127	868	919	2	62	11	188	292	56	1
% of all		39.8	45.9	35.4	37.4	0.1	2.5	0.4	7.7	11.9	2.3	0.0

На сьогодні для експлуатації цього методу підтримуються пристрої, які мають апаратну вразливість checkm8, виявлену у вересні 2019 року [3], а саме від моделі Apple iPhone 5S до iPhone X з декількома застереженнями. Етапи отримання інформації з досліджуваного пристрою:

1. Для початку роботи необхідно на пристрій Raspberry Pi встановити та налаштовати операційну систему зі скриптами, підключити зовнішнє джерело живлення або power bank (підзарядник) та Lightning-кабель для підключення Apple пристроїв.
2. Досліджуваний пристрій попередньо необхідно перевести у режим DFU (Device Firmware Upgrade).
3. І залишається тільки підключити до пристрою Raspberry Pi, після

чого буде запущений автоматизований процес експлуатації вразливості checkm8 та збір усієї можливо доступної інформації з пристрою.

Оскільки більша частина інформації знаходиться у зашифрованій області пам'яті та оберігається в тому числі засобами SEP (Secure Enclave Protection), а сам засіб на цей час в стадії PoC (Proof of Concept), можна отримати лише не зашифровану інформацію, яка доступна в стані BFU (Before First Unlock).

Отже, за допомогою цього методу можна автоматизовано отримати таку інформацію:

– дані про Wi-Fi мережі, до яких підключався пристрій + геопозиція по BSSID точок доступу;

– облікові записи на пристрої (iCloud, Apple ID, поштові скриньки, тощо);

– дані ОС (версія, номер збирання, інша технічна інформація);

– дані про встановлені раніше SIM (номер, ICCID);

– дані статусу функції «Екранного часу»;

– заблоковані (додані в чорний список) мобільні номери;

– облікові дані, які використовуються для входу в FaceTime, iMessage;

– дата та спосіб створення (хмара або локально на ПК) останнього бекапу, підключення до ПК (назва самого ПК і версія iOS пристрою).

Вся отримана інформація зберігається у вигляді архіву безпосередньо на накопичувачі MicroSD, з якої і виконується загрузка ОС, або на зовнішній USB накопичувач для більш зручного подальшого дослідження.

Надалі планується багато нововведень та доопрацювань для більшої автоматизації, структуризації і впровадження роботи з тимчасовими даними, додатків з динамічними GUID і, найголовніше, зі зв'язкою ключів (keychain-2.db).

Бібліографічні посилання

1. CVE Details. URL: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224.
2. CVE Details. URL: https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49.
3. Шах и мат! Как устроен нашумевший эксплоит checkm8 и как им воспользоваться. URL: https://xakep.ru/2019/11/21/checkra1n.
4. Raspberry Pi 4 URL: https://www.raspberrypi.com/products/raspberry-pi-4-model-b.