**ВИСШЕ ВОЕННОМОРСКО УЧИЛИЩЕ „Н. Й. ВАПЦАРОВ“**

***9002 Варна, ул. „В. Друмев“ 73, тел. 052/632-015, факс 052/303-163***

***„FILII MARIS SUMUS”***

ФАКУЛТЕТ „ИНЖЕНЕРЕН“ – КАТЕДРА „ИНФОРМАЦИОННИ ТЕХНОЛОГИИ“

КУРСОВ ПРОЕКТ

**по дисциплина „Защита на Web базирани системи“**

**ТЕМА: Разпознаване и разследване на измами с критовалути“**

**Студент: Виктор Лъчезаров Лазаров**

**Специалност: Киберсигурност**

**Фак. № 126202-06**

**гр. Варна**

**2024 г.**

|  |  |
| --- | --- |
| C:\Users\Емил Йорданов\Downloads\logo.png | **ВИСШЕ ВОЕННОМОРСКО УЧИЛИЩЕ „Н. Й. ВАПЦАРОВ“**  ***9002 Варна, ул. „В. Друмев“ 73, тел.052/632-015, факс 052/303-163*** |
| ***“FILII MARIS SUMUS”*** |
| Картина, която съдържа текст  Описанието е генерирано автоматично | УТВЪРЖДАВАМ:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Началник на катедра "Информационни технологии"  / доц. Николова, доктор /  Дата:\_\_\_\_\_\_\_\_\_\_\_2024 г. |

### ЗАДАНИЕ

за курсов проект **Виктор Лъчезаров Лазаров**

фак. № 126202-06

**Тема** : Keyloggers

1. Съдържание на обяснителната записка:

* -
* -
* -

1. Дата на връчване на заданието:
2. Дата на предаване на завършения курсов проект в катедрата:

Студент: \_\_\_\_\_\_\_\_\_\_\_\_\_ Преподавател:\_\_\_\_\_\_\_\_\_\_\_\_\_

/ Лазаров/ / доктор Андреев /

**СЪДЪРЖАНИЕ:**

[СЪДЪРЖАНИЕ 6](#_heading=h.1fob9te)

[1.](#_heading=h.3znysh7) [К](#_heading=h.3znysh7)акво е атака с Keylogger? 7

[2.](#_heading=h.4d34og8) История [10](#_heading=h.4d34og8)

[3](#_heading=h.lnxbz9). [И](#_heading=h.lnxbz9)звестни случаи 13

4[.](#_heading=h.35nkun2) Пример за такава атака 13

5[.](#_heading=h.1ksv4uv) Оптимална защита 13

6[.](#_heading=h.1ksv4uv) Литература 13

### Какво е атака с Keylogger?

Изразява се в непредвиденото записване и изпращане на информация въведена чрез клавиатура, мишка или друго входно устройство на компютъра. Най-често това се прави за да се проследяват комуникациите на жертвата и да се крадат данни за достъп с цел добиване на повече прав в машината/ите на жертвата. Има два основни вида keylogger-и:  
Хардуерни [6]:  
- Безжични – предават информацията си чрез Wi-fi.  
- Клавишни – най-често под формата на допълнителен накрайник за USB-то на клавиатурата която жертвата ще използва.  
- Акустични – използват звука произведен от всеки клавиш за да определят кой бутон е бил натиснат.  
  
Софтуерни:

- Драйверни – инсталира се с ядрото на операционната система като драйвер и това му позволява да достъпи информацията директно.  
- API-базирани – възползват се от програмни интерфейси на операционната система за да наблюдават информацията.

- Инжектирани в паметта – този тип могат да нямат файлове и се инжектират директно в паметта използвана от процесите на компютъра.  
  
 Хардуерни keylogger-и могат да бъдат приложени най-лесно чрез атака на веригата за хардуерни доставки на жертвата. Ако не се получи, софтуерните варианти са по-добри защото не оставят физически следи. Но за сметка на това могат да бъдат по-лесно засечени или блокирани като се ексфилтрира информация. Хардуерния вариант може да предотврати това като съхранява цялата информация на устройството, но за сметка на това трябва да бъде физически взето обратно от нападателя.

### История

### За най-първият пример за „Keylogeer” или допълнително записване на текст може да се счете индиго хартията изобретена през 1801 от италианския изобретател Пелегрино Тури за пишещата машина [1] (модерния патент [2]). Следващата стъпка в развитието им отново е свързана с пишещите машини и се нарича „selectric bug” (защото е насочено към IBM Selectric II и III пишещите машини), представлява малко устройство което засича електромагнитното поле от движещата се пишеща глава. Тази информация се препраща към близък подслушвателен пост чрез радио вълни [3]. Тази атаке се е използвала срещу пишещите машини използвани от американското посолство в Москва, Съветски Съюз през 1970. Пет различни версии са били намерени през годините. След това Unix и компютрите започват да набират още популярност и през 1983 Пери Кивовитз пише първия софтуерен „keylogger” и го публикува в Usenet форумите за Linux, което води до ограничения в правата за достъп до определени ресурси свързани с паметта на устройствата за вход на информация. В последствие се развиват хардуерни варианти за PS/2 [4] портове и USB, някой предаващи информация през мрежа, други които имат памет на устройството и трябва да се приберат ръчно. С продължение на времето тази технология не се използва само за зловредни цели, но и за следене на служители и диагностика на софтуерни проблеми. 3. Известни случаи

- 2015г., популярна част от играта “Grand Theft Auto V” е била заразена с keylogger. [7]  
  
 - 2014~~-~~2017г. хакерска групировка с наименованието APT10 (Advanced Persistent Threat) крадат големи количества информация за достъп от големи технологични компании, някои от които: Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data. [8]  
  
- 2017г., Швейцарска компания в сферата на киберсигурността открива, че аудио драйвери на лаптопите HP са записвали какво са писали потребители им. [5]

### 4. Пример за такава атака

Ако сайт има уязвимост която позволява изпълнение на съхранен код, тогава на всяко зареждане на сайта може да се зарежда keylogger който да изпраща информацията от формата за достъп до защитено съдържание. Струва си да се отбележи, че най-лесно би било такава атака да се включи прикрита като част от популярна библиотека като jQuery, която все още се използва в много WordPress уебсайтове.  
  
5. Оптимална защита:  
- Физическа инспекция на устройства за физически keylogger-и.  
- Изключване на неизползвани физически (и мрежови портове).  
- Whitelist прилагащ се за всички заявки излизащи от мрежата.

- Купуване на хардуер само от сертифицирани/доверени доставчици.  
- Многофакторна автентикация.

**6. Литература**:

[1] <https://www.yourguidetoitaly.com/italian-inventors.html>  
[2] [https://patents.google.com/patent/US2872340?oq=solvent+carbon+columbia#relatedApplications](https://patents.google.com/patent/US2872340?oq=solvent+carbon+columbia" \l "relatedApplications)  
[3] <https://www.cryptomuseum.com/covert/bugs/selectric/index.htm>  
[4] <https://www.youtube.com/watch?v=eSiriQQHGtI>  
[5] <https://www.bleepingcomputer.com/news/security/keylogger-found-in-audio-driver-of-hp-laptops/>  
[6] <https://softwarelab.org/blog/keylogger-types/>  
  
[7] <https://www.pcworld.com/article/427489/malicious-keylogger-malware-found-lurking-in-highly-publicized-gta-v-mod.html>[8] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/