



Зачем хакеру клавиатура?

Василий Кравец

Начальник отдела ИИТ

Перспективный мониторинг



Обо мне

Ampire 360°

CVE-2019-14743

CVE-2019-15316

CVE-2019-17180

CVE-2019-19247

CVE-2019-19248

CVE-2019-20383

CVE-2020-23967

CVE-2021-25261

CVE-2021-25263

CVE-2022-28226

CVE-2022-28225

CVE-2023-5993

CVE-2023-7016



Клавиатура?

Точно темой не ошибся?



Как люди представляют себе хакерскую клавиатуру



Как на самом деле выглядят хакерские клавиатуры

Ampire 360°



Что или чем атакуем

- Атака на клавиатуру
- Атака с помощью клавиатуры



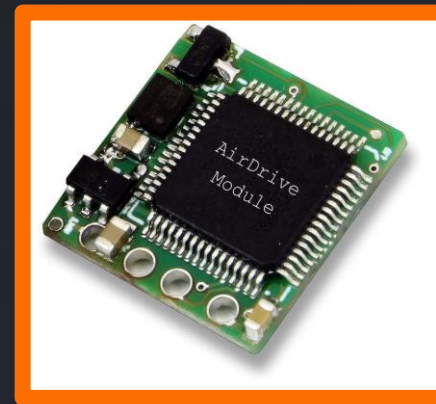
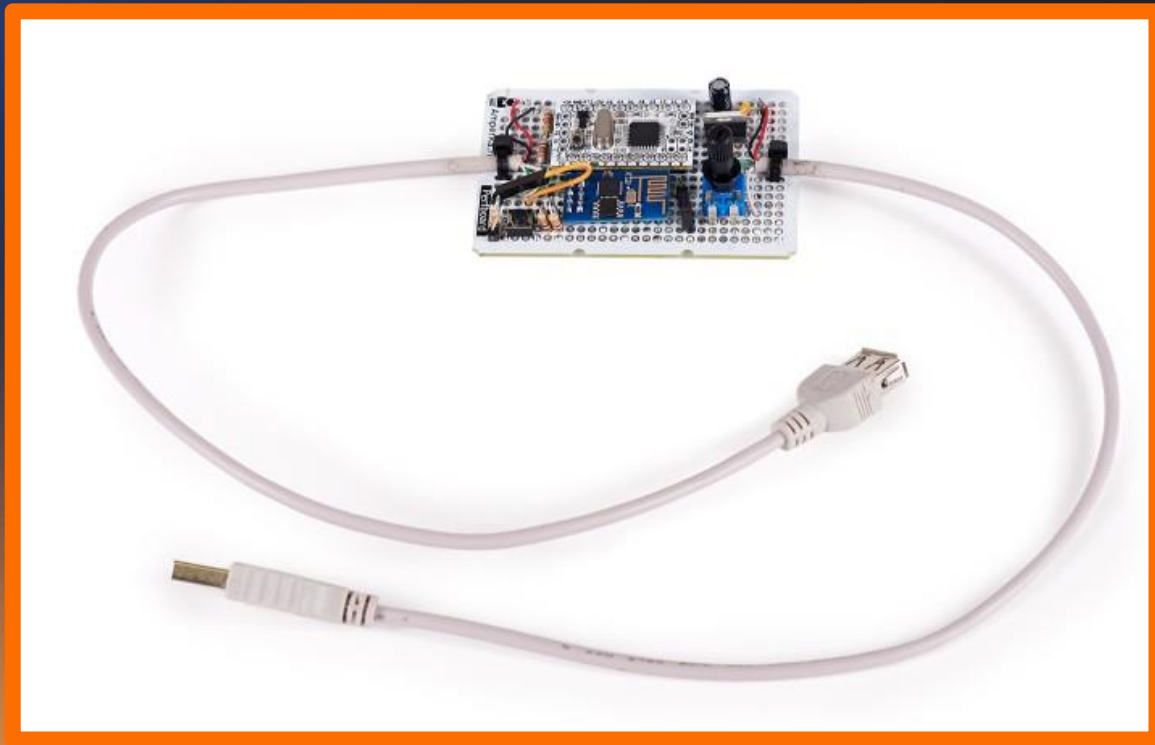
Атака на клавиатуру

Заставляем устройство
вести себя неправильно



Keylogger

Ampire 360°



Плюсы и минусы

Ampire 360°

Плюсы

- Малая заметность
- Нет зависимости от платформы
- Пассивное устройство

Минусы

- Надо устанавливать и забирать
- Обработка результатов
- Пассивное устройство

Бонусы

- Wi-Fi
- Батарейка
- Режим активного устройства



Сканер штрих-кодов



Keyboard Wedge Host Types

Keyboard Wedge Host Types

Select the keyboard wedge host by scanning one of the bar codes below.



IBM PC/AT & IBM PC Compatibles¹



IBM PS/2 (Model 30)



IBM AT NOTEBOOK



NCR 7052

✓ **NOTE** User selection is required to configure this interface and this is the most common selection.

Keystroke Delay

This is the delay in milliseconds between emulated keystrokes. Scan a bar code below to increase the delay when hosts require a slower transmission of data.



*No Delay



Medium Delay (20 msec)



Long Delay (40 msec)

Keyboard Wedge Country Types (Country Codes)

Scan the bar code corresponding to the keyboard type. If your particular keyboard type is not listed, see [Alternate Numeric Keypad Emulation on page 5-9](#).



*North American



German Windows



French Windows



French Canadian Windows 95/98



French Canadian Windows XP/2000



French Belgian Windows

MouseJack



Атака **MouseJack** — отправка нелегитимных, но корректных управляющих сообщений, которые обрабатываются приемником сигнала радио-мыши как нажатия клавиш

Атака с помощью клавиатуры

Приносим своё устройство



BadUSB



Атака **BadUSB** — устройство представляется компьютеру жертвы клавиатурой, а по истечении некоторого времени начинает отправлять последовательности нажатий клавиш

Мой сценарий использования BadUSB

Ampire 360°



Эксфильтрация данных 1

Ampire 360°



«Вымаргиватель»

10 байт в секунду

Эксфильтрация данных 2



Специальный HID-дескриптор
1 килобайт в секунду

```
const uint8_t report_descriptor[] {  
    // Keyboard  
    0x05, 0x01, // USAGE_PAGE (Generic Desktop) // 47  
    0x09, 0x06, // USAGE (Keyboard)  
    0xa1, 0x01, // COLLECTION (Application)  
    0x85, 0x02, // REPORT_ID (2)  
    0x05, 0x07, // USAGE_PAGE (Keyboard)  
  
    0x19, 0xe0, // USAGE_MINIMUM (Keyboard LeftControl)  
    0x29, 0xe7, // USAGE_MAXIMUM (Keyboard Right GUI)  
    0x15, 0x00, // LOGICAL_MINIMUM (0)  
    0x25, 0x01, // LOGICAL_MAXIMUM (1)  
    0x75, 0x01, // REPORT_SIZE (1)  
  
    0x95, 0x08, // REPORT_COUNT (8)  
    0x81, 0x02, // INPUT (Data,Var,Abs)  
    0x95, 0x01, // REPORT_COUNT (1)  
    0x75, 0x08, // REPORT_SIZE (8)  
    0x81, 0x03, // INPUT (Cnst,Var,Abs)  
  
    0x95, 0x06, // REPORT_COUNT (6)  
    0x75, 0x08, // REPORT_SIZE (8)  
    0x15, 0x00, // LOGICAL_MINIMUM (0)  
    0x25, 0x73, // LOGICAL_MAXIMUM (115)  
    0x05, 0x07, // USAGE_PAGE (Keyboard)  
  
    0x19, 0x00, // USAGE_MINIMUM (Reserved (no event indicated))  
    0x29, 0x73, // USAGE_MAXIMUM (Keyboard Application)  
    0x81, 0x00, // INPUT (Data,Ary,Abs)  
    0xc0,      // END_COLLECTION  
  
};
```

Wi-Fi клавиатура

- Создает Wi-Fi точку доступа
- Подключается к существующему Wi-Fi
- Управляется через web-интерфейс



ESP32 S3

Ampire 360°

Основные характеристики

- Двухъядерный 32-битный процессор Tensilica Xtensa LX7
- 512кб ОЗУ, 8мб ПЗУ
- Wi-Fi 802.11 b/g/n (2,4 ГГц) и Bluetooth v5.0 с BLE
- Универсальный USB (питание, прошивка, подключение)
- SPI (экраны)

IDE: Arduino IDE и PlatformIO
для Visual Studio Code



Разработка

MainSettingsKeyboard ActionsFile ActionsDuckScriptAdditional

Keyboard

ESC	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12				
~`	!¹	@²	#³	\$⁴	%⁵	^⁶	&⁷	*⁸	(⁹	)⁰	_ -	+ =	BACK	INS	HOME	PG UP
TAB	Q ^q	W ^w	E ^e	R ^r	T ^t	Y ^y	U ^u	I ⁱ	O ^o	P ^p	{ [	}]	ENTER	DEL	END	PG DWN
CAPS	A ^a	S ^s	D ^d	F ^f	G ^g	H ^h	J ^j	K ^k	L ^l	; [;]	" ["]	' [']				
SHIFT	[~]	Z ^z	X ^x	C ^c	V ^v	B ^b	N ⁿ	M ^m	< [,]	> [.]	? [/]	SHIFT			↑	
CTRL	WIN	ALT							ALT	WIN	MENU	CTRL		←	↓	→

Keyboard command (readonly)

SHIFT + H

RELEASE MODIFIERSSEND

Data

String

String without modifiers

Put string here...

SEND

Идеальное устройство-клавиатура

- Создает Wi-Fi точку доступа
- Подключается к существующему Wi-Fi
- Управляется через web-интерфейс
- Настраиваемые VID, PID, Serial, ...
- Может работать и как пассивный **кейлоггер**, и как пассивный **BadUSB**



Еще пара интересных атак

То, что не подошло под
классификацию



Android приложение-клавиатура



Мультимедийные клавиши

Ampire 360°



Специальные клавиши, которые позволяют быстро выполнять специальные действия: запуск калькулятора, браузера, email-клиента и другие

Спасибо за внимание!

Василий Кравец

@xitauw

Vasily.Kravets@amonitoring.ru



Ampire 360°