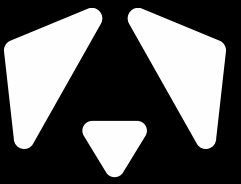


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

RE vs Security Cryptography Programmers

Насколько полезен реверс-инжиниринг при исследовании защищенности программно-аппаратных решений?

Main questions and answers

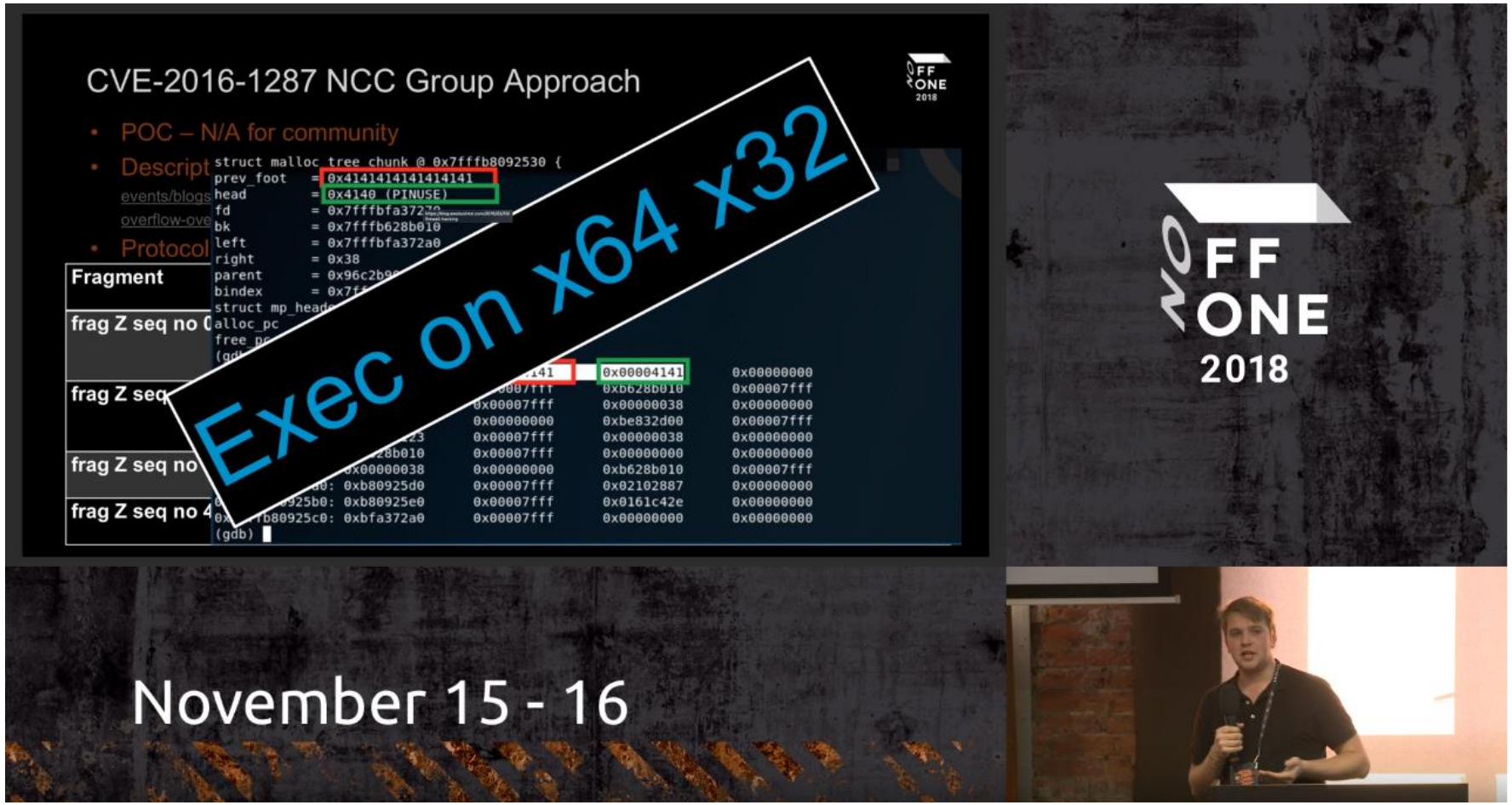
Способы исследования защищенности ПАК:

- построение стенда, реализующего типовые сценарии ПАК
- исследование системы управления ПАК (в большинстве случаев WEB)
- исследование функциональных сервисов
- исследование взаимодействия компонентов ПАК при помощи RE

Для каких задач применяется реверс-инжиниринг при поиске уязвимостей:

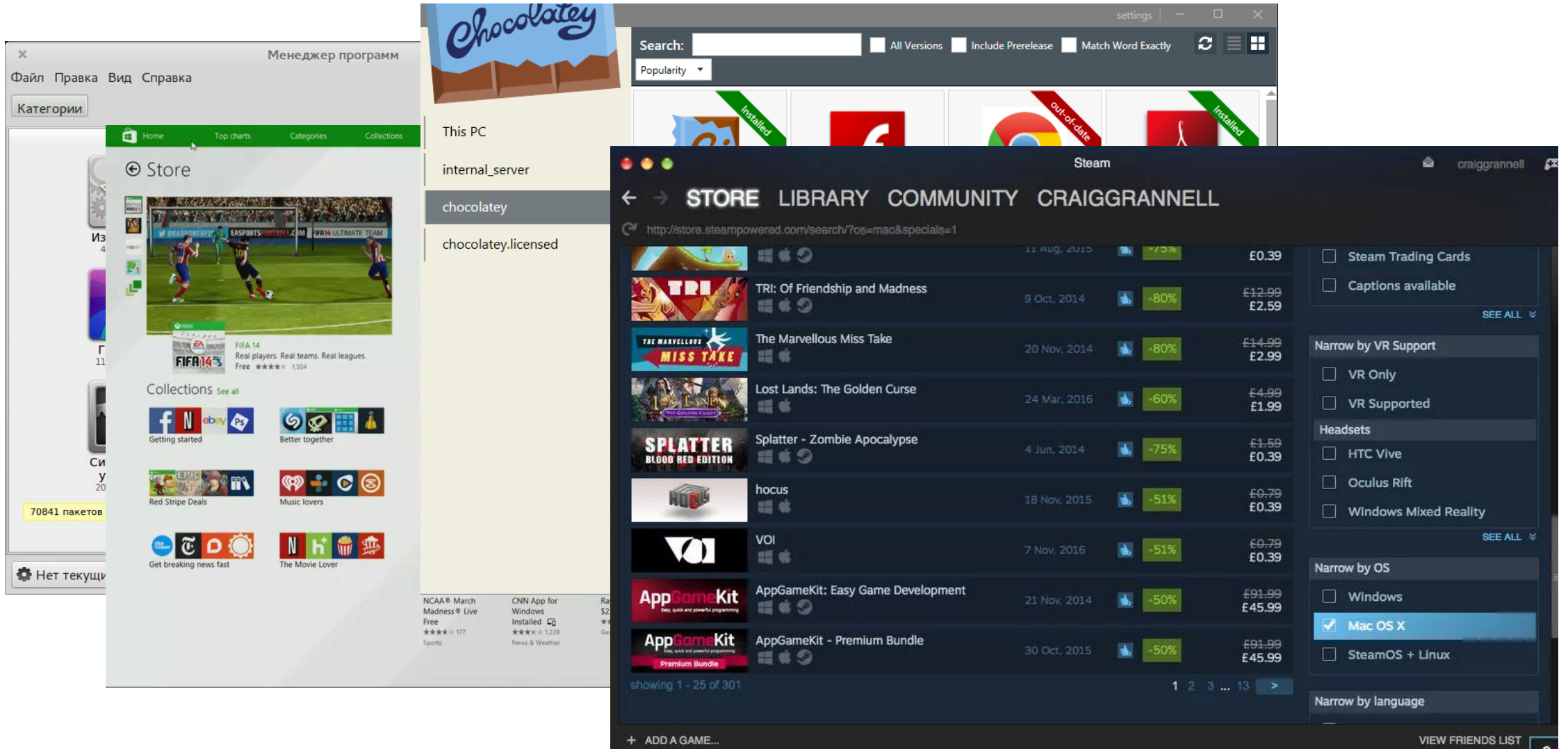
- анализ причин аномального поведения служб при эксплуатации
- изучение принципов функционирования ПАК и его отдельных механизмов
- отладка и реализация инструментов эксплуатации (PoC)

Others research

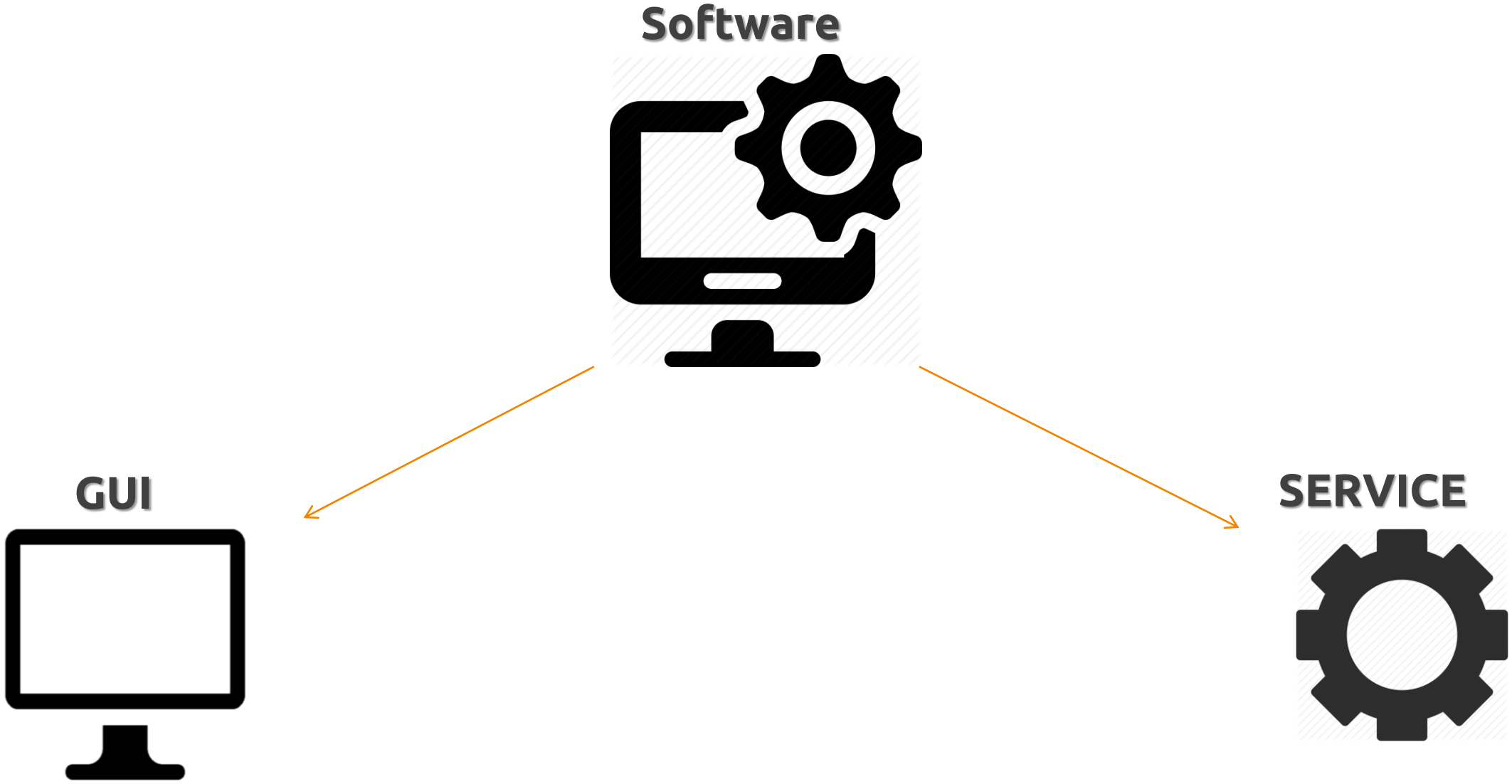


https://www.youtube.com/watch?v=4QV0CTfeRzw

Package managers & Software installers



“Under the hood”



User mode

System

“C:\Program Files**CUSTOM_PATH**”

?

- \Program Files\ *
- \Windows\system32\ *
- \Program Files (x86)\ *

OK

https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/user-account-control-only-elevate-uiaccess-applications-that-are-installed-in-secure-locations

User mode

System

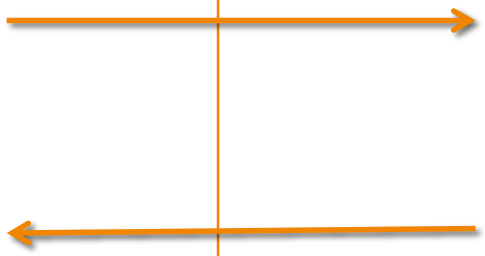
GUI

SERVICE

PIPE

RE

Command: Copy A to B



?

- \Program Files\ *
- \Windows\system32\ *
- \Program Files (x86)\ *

https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/user-account-control-only-elevate-uiaccess-applications-that-are-installed-in-secure-locations

RE Counter : 1

User mode

GUI

\+

Evil “version.dll” in User folder

Command: Copy A to B

System

SERVICE

PIPE

RE

```
BOOL
GetNamedPipeClientProcessId(
  HANDLE Pipe,
  PULONG ClientProcessId
);
```

Decryption/Encryption method error!

RE Counter : 2

User mode

GUI

IV ? Key?

RE

IV – is a hardcode value

KEY – in “public“ folder with read permissions

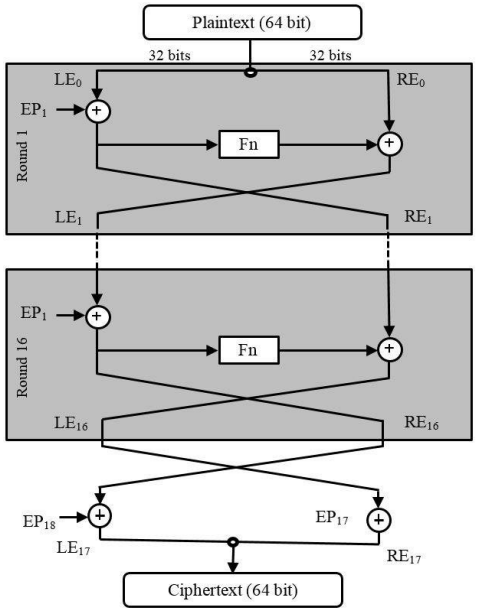
System

SERVICE

PIPE

RE

Blowfish



RE Counter : 4

User mode

IV – is a hardcode value

KEY – in “public“ folder with read permissions

+

Evil “version.dll” in User folder

Command: Copy A to **B**

System

PIPE

Error! Incorrect folder

RE

substr (destination_path, “C:\Program Files\Company Prod\”)

RE Counter : 5

User mode

- ..\..\..\..\..\..\..\
- %2e%2e%2f
- %c0%af

RE

Command list:

- Copy A to B
- Register
- Start Process

System

PIPE

substr (destination_path, “C:\Program Files\Company Prod\”)

Error! Incorrect folder

RE Counter : 6

User mode

GUI

IV – is a hardcode value

KEY – in “public“ folder with read permissions

+

Evil “version.dll” in User folder

Command: Start_process **B**

System

SERVICE

PIPE

Error! Incorrect Process

RE

B

RE Counter : 7

User mode

GUI

version.dll

If run from **system** Evil code 2

If run from **User** Evil code 1

IV – is a hardcode value

KEY – in “public“ folder with read permissions

+

Evil “version.dll” in User folder

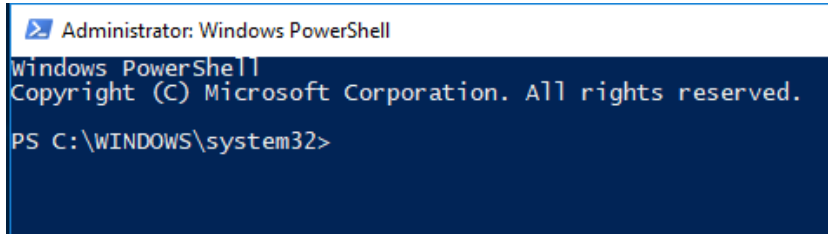
Command: Start_process **GUI**

System

SERVICE

PIPE

SUCCESS



User mode

Reboot machine

System

GUI

SERVICE

No Service
No PIPE

RE

Blowfish → **Some string** →

→ **Int** → **PID** →

→ PID 

RE Counter : 8

User mode

GUI

PID

→ Int →

→ String → Blowfish

version.dll

If run from **system** Evil code 2

If run from **User** Evil code 1

IV – is a hardcode value

KEY – in “public“ folder with read permissions

+

Evil “version.dll” in User folder

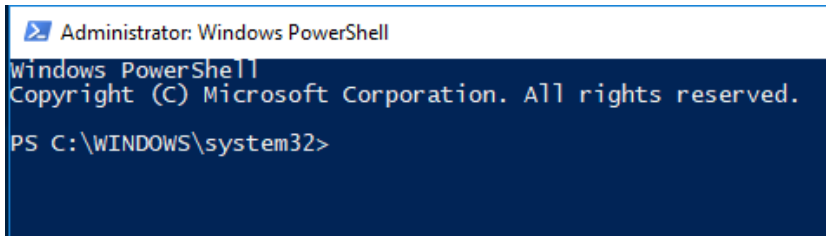
Command: Start_process **GUI**

Reboot machine

System

SERVICE

Service PIPE



Final exploit and results

1. Start Service
2. Pipe for commands
3. Start_process cmd.exe

1. Bypass signature x3
2. Bypass Blowfish x3
3. Root privilege shell

Спасибо за внимание!

«Ищите да обрящете»

Овчинников Сергей

Эксперт-исследователь

компании «Перспективный мониторинг»

Sergey.Ovchinnikov@amonitoring.ru

Telegram: @malchikserega
Twitter: @malchikseregas