Kaspersky Industrial Cybersecurity Conference 2023

Чего бояться, с чем бороться и чем жертвовать

взгляд на текущие вызовы ИБ промышленных предприятий

Евгений Гончаров,
Руководитель Kaspersky ICS CERT

kaspersky

Сложные тактики и техники

в атаках APT на промышленные организации

> Говори, что знаешь; делай,
> что обязан; и пусть будет,
> что будет.

— Софья Ковалевская, Марк Аврелий, Царь Соломон, Авраам,...

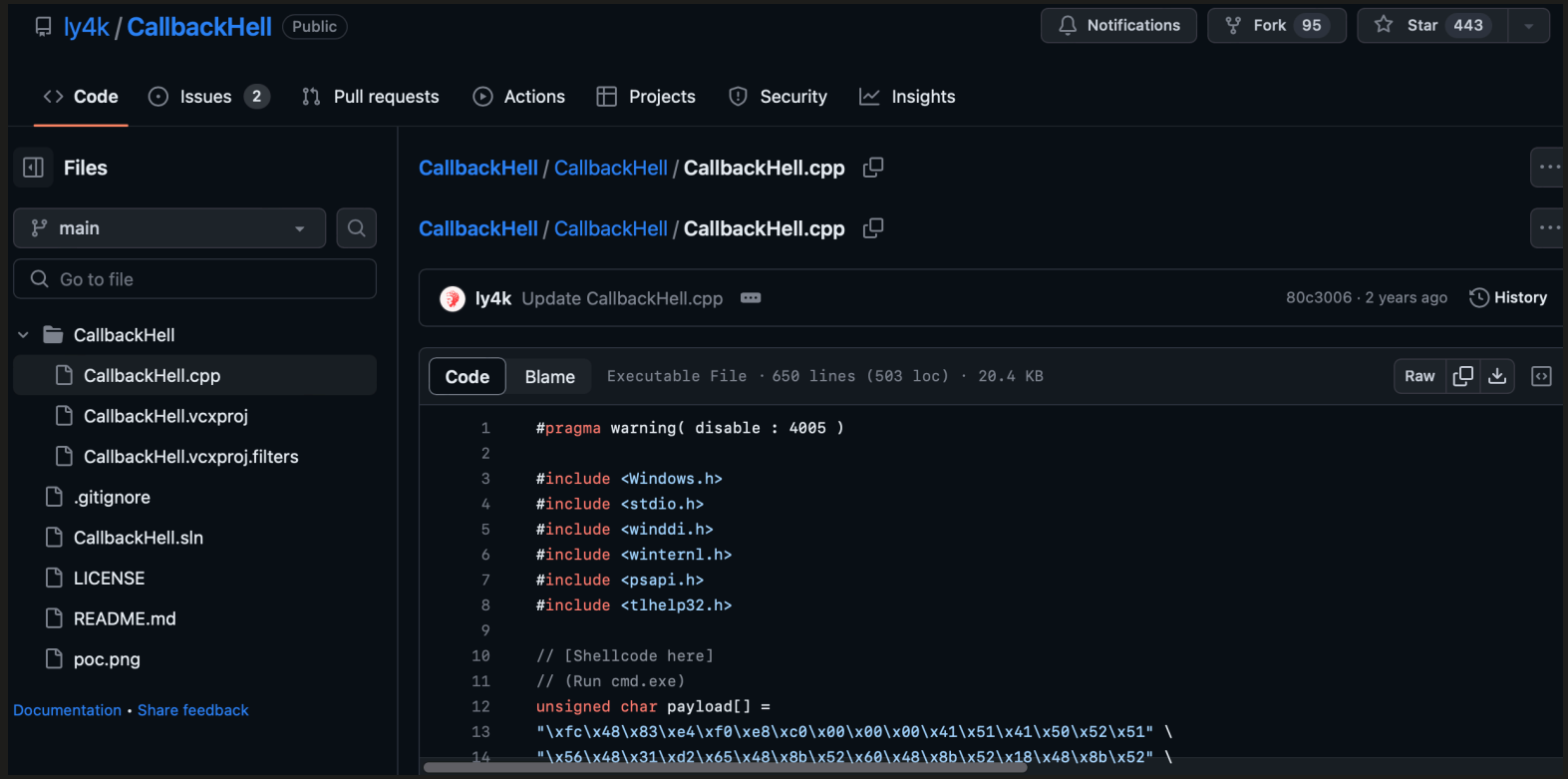
Эпизод при расследовании APT на промышленном предприятии...

...ВПО «ослепляет» средства защиты узлов...

Удаляет указатели на callback–функции ядра:

PsSetCreateProcessNotifyRoutine
PspCreateProcessNotifyRoutine
PspSetCreateProcessNotifyRoutine
PsSetCreateThreadNotifyRoutine
PspCreateThreadNotifyRoutine
PspSetCreateThreadNotifyRoutine
PsSetLoadImageNotifyRoutineEx
PsSetLoadImageNotifyRoutine
PspLoadImageNotifyRoutine…

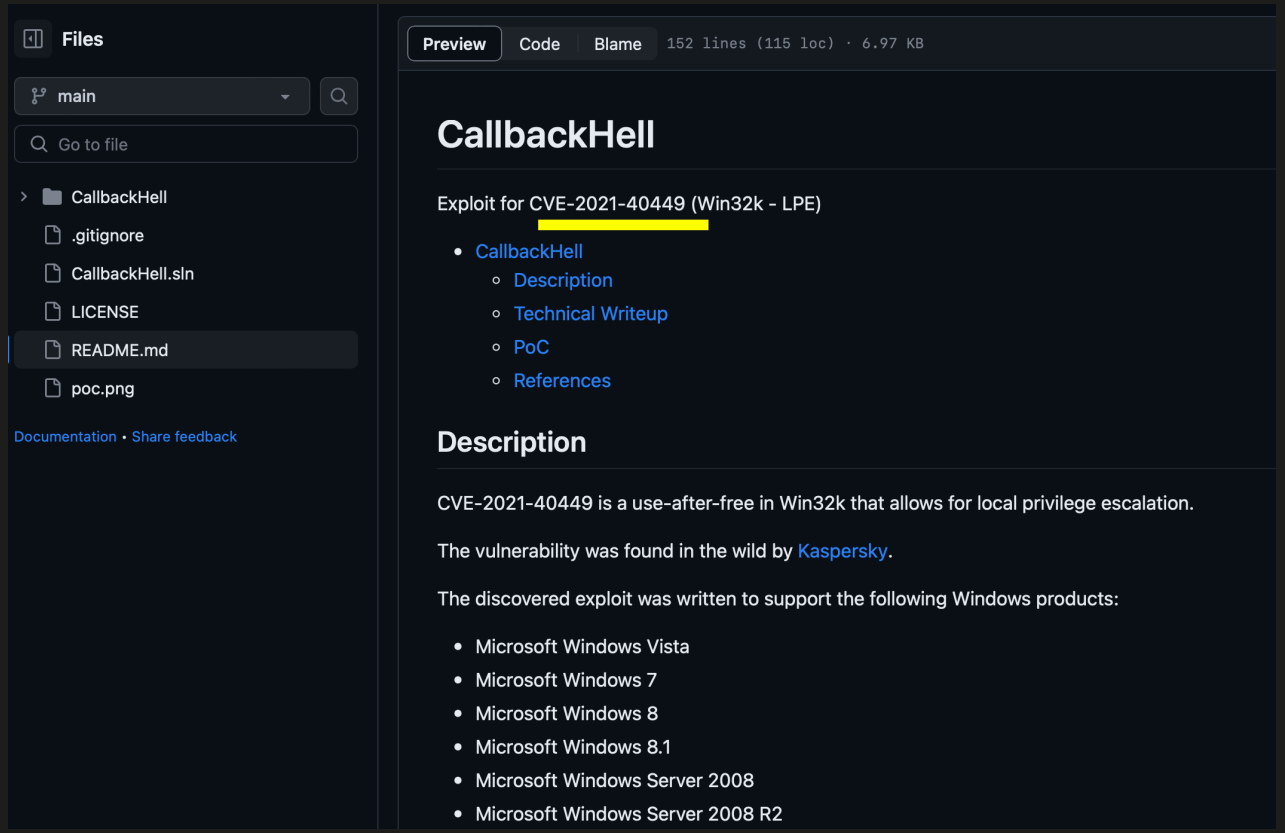
ВПО оказывается сделанным на основе утилиты с отрытым исходным кодом...



https://github.com/ly4k/CallbackHell/

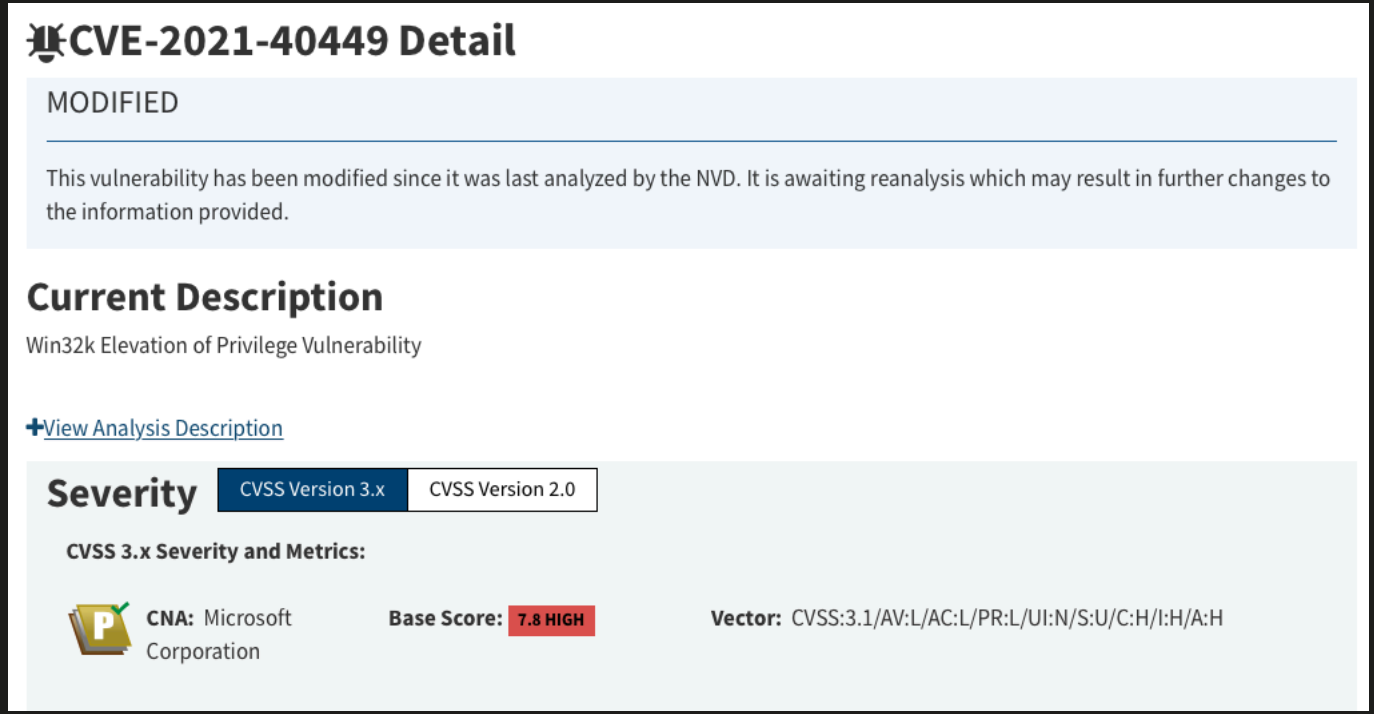
Kaspersky
ICS CERT

...которая эксплуатирует уязвимость CVE-2021-40449

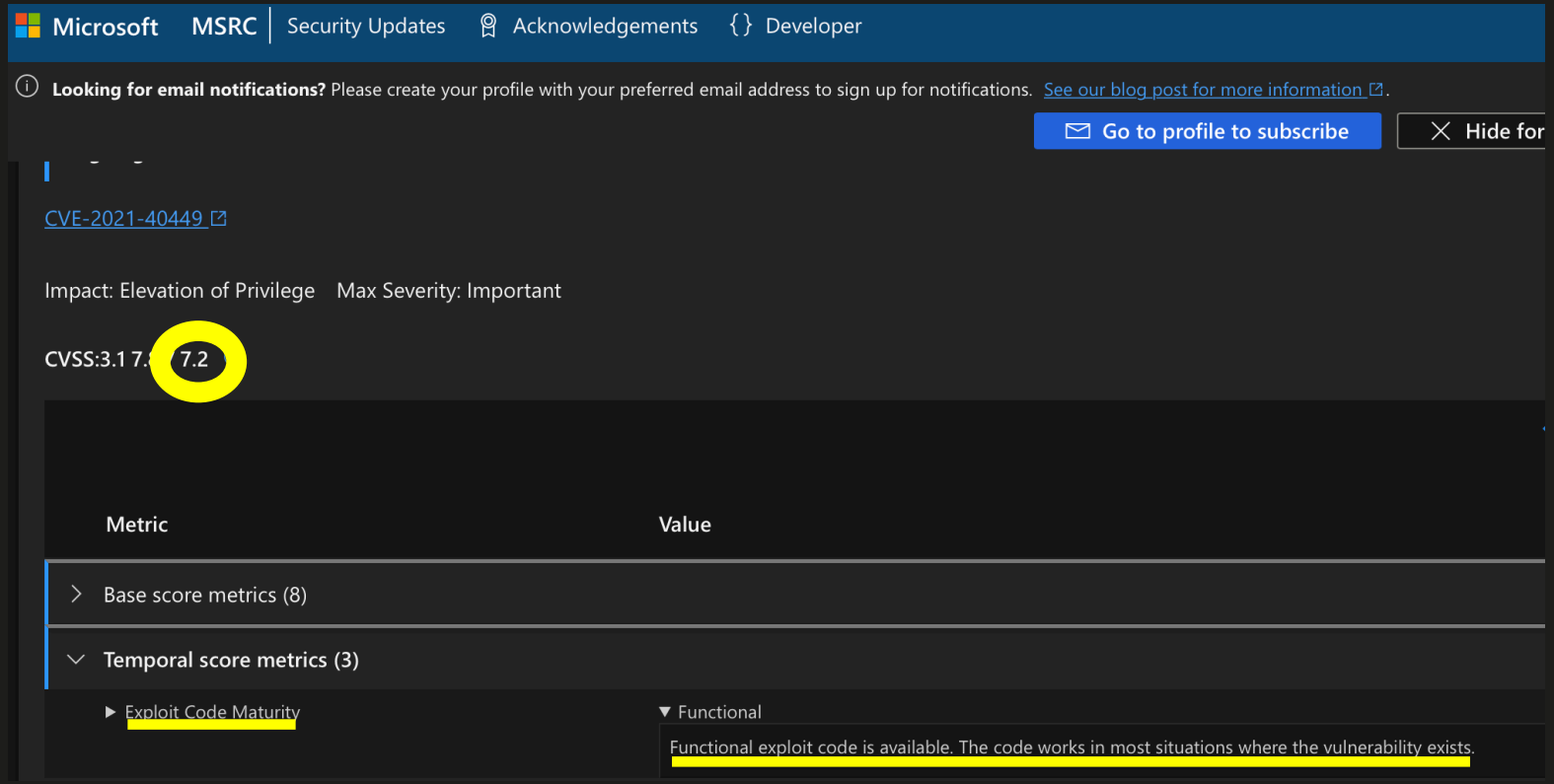


https://github.com/ly4k/CallbackHell/

Как жертва могла понять, что нужно установить патч?
Посмотреть CVSS score и вкктор?

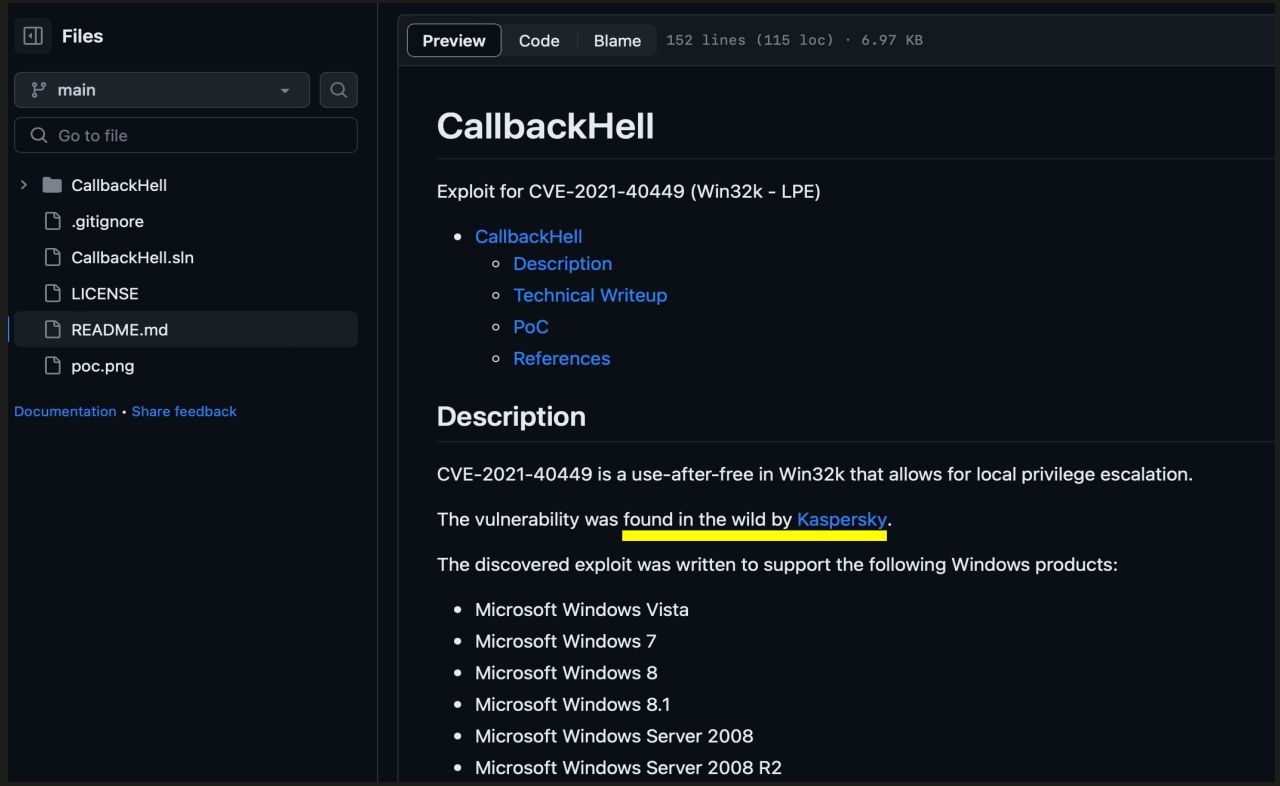


Посмотреть advisory вендора? Там есть CVSS Temporal score & vector.



Kaspersky
ICS CERT

Понять, использовалась ли в атаках?



https://github.com/ly4k/CallbackHell/

Как понять, устанавливать ли патч в ОТ? Читайте TI-отчёты.

vulnerabilities

Search blog posts

MysterySnail crawls through zero-day vulnerability

Our security technologies detected the exploitation of a previously unknown vulnerability in the Win32k driver.

Hugh Aver October 12, 2021

SECURELIST by Kaspersky

Solutions Industries Products Services Resource Center About Us GDPR

Content menu Search...

MysterySnail attacks with Windows zero-day

RESEARCH 12 OCT 2021 6 minute read

03 Apr 2023	Industrial	b46a37d9-ce93-4cf9-500c-ec1a546aefe0-ics	Updated MATA attacks on defense contractors in Eastern Europe In the second half of 2022, Kaspersky experts uncovered a major series of attacks on industrial enterprises in Eastern Europe, including military contractors. This campaign remained active until March 2023, leveraged new generations of the MATA malicious framework. We believe that the attackers' goal is the theft of

Defense Industrial Military contractors Oil and gas Eastern Europe Lamberts Lazarus

https://www.kaspersky.com/blog/mysterysnail-cve-2021-40449/42448/

https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

Kaspersky ICS CERT

Что если патч, всё-таки, не установить, ...или не защититься от BYOVD? Читайте TI-отчёты...

Дополнительные меры защиты:

.... Enable two-factor authentication for logging in to administration consoles and web interfaces of security solutions. In the Kaspersky Security Center, for example, this can be done by following these instructions....

Правила детектирования и индикаторы компрометации:

```
"""
import "pe" rule apt_Mata_signed { meta: description = "Rule to detect
signed Mata APT samples"
author = "Kaspersky"
copyright = "Kaspersky"
distribution = "DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY
MULTISCANNER OR SHARE ON ANY THREAT INTEL PLATFORM" version =
"1.1"
last_modified = "2023-03-28"
hash = "1b889de65913138f75c87483c24....
```

«Простые» тактики и техники

в атаках APT на промышленные организации

> Keep things as simple as possible, but not simpler

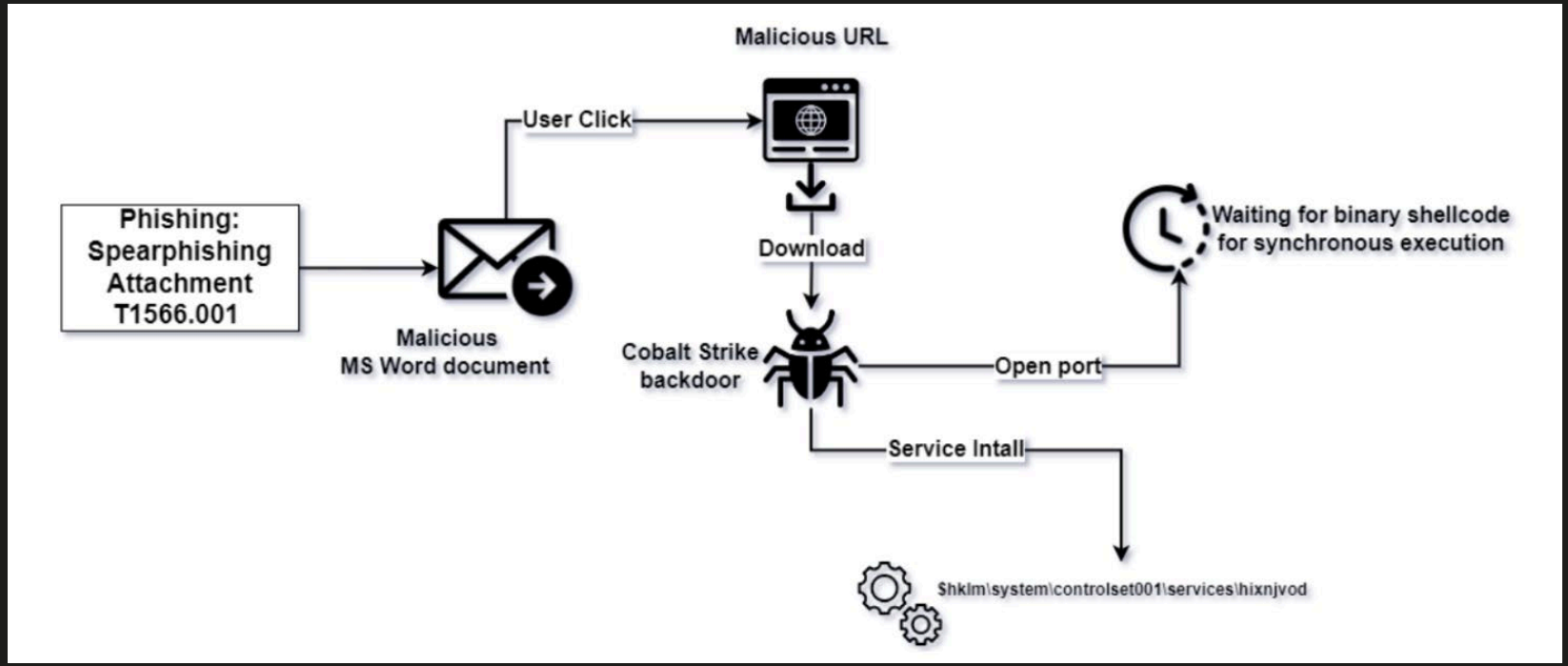
— Albert Einstein?

It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience

Albert Einstein

«Просто». фишинг

Расследование APT в Пакистане. Скомпрометированы инженеры OT.



Kaspersky
ICS CERT

https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/

«Просто» DLL Hijacking / Side Loading

Пример1: APT в Пакистане, OT-инженеры (см. предыдущий слайд)

https://ics-cert.kaspersky.ru/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/

Пример2: APT в восточной Европе – предприятия ВПК (см. следующий слайд)

https://ics-cert.kaspersky.ru/publications/reports/2021/02/25/lazarus-targets-defense-industry-with-threatneedle/

Пример3: APT в восточной Европе, производство (через 1 слайд)

https://ics-cert.kaspersky.ru/publications/reports/2023/07/20/common-ttps-of-attacks-against-industrial-organizations-implants-for-remote-access/

https://ics-cert.kaspersky.ru/publications/reports/2023/07/31/common-ttps-of-attacks-against-industrial-organizations-implants-for-gathering-data/

https://ics-cert.kaspersky.ru/publications/reports/2023/08/10/common-ttps-of-attacks-against-industrial-organizations-implants-for-uploading-data/

Объяснения и рекомендации:

https://support.microsoft.com/en-gb/topic/secure-loading-of-libraries-to-prevent-dll-preloading-attacks-d41303ec-0748-9211-f317-2edc819682e1

https://www.mandiant.com/resources/reports/dll-side-loading-thorn-side-anti-virus-industry

https://www.mandiant.com/resources/blog/abusing-dll-misconfigurations

“Просто” недостатки изоляции сети

Расследование APT на предприятии ВПК в восточной Европе

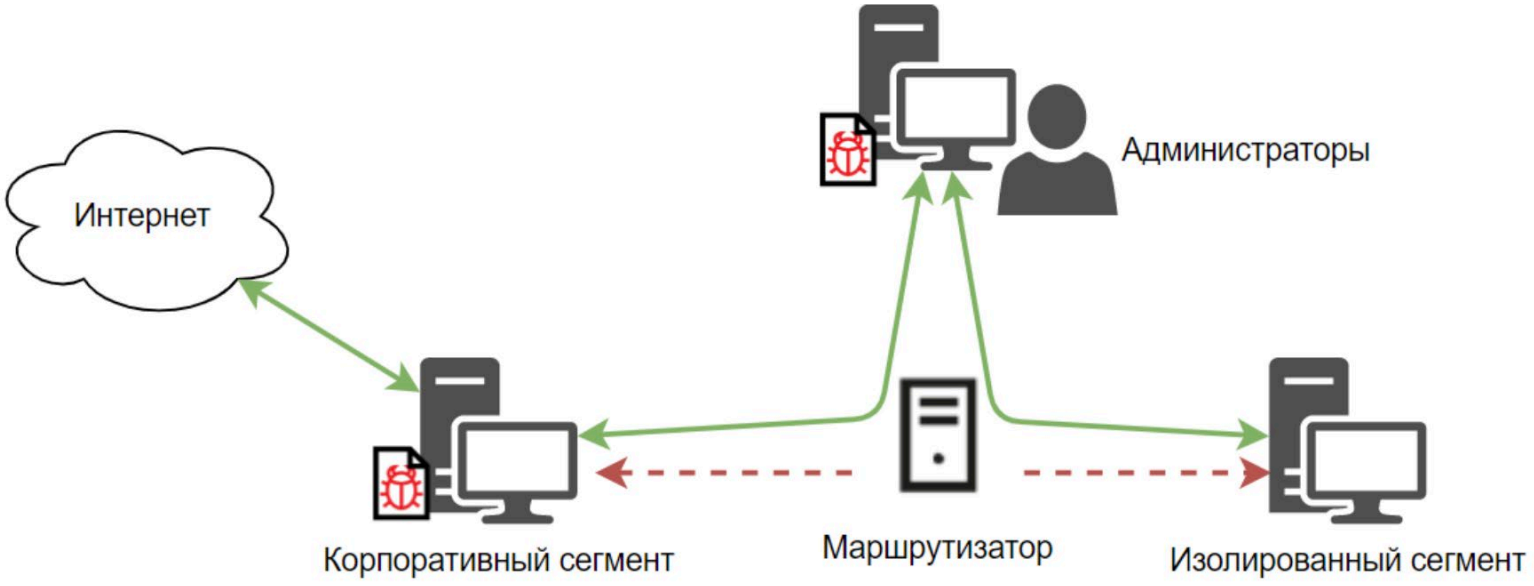


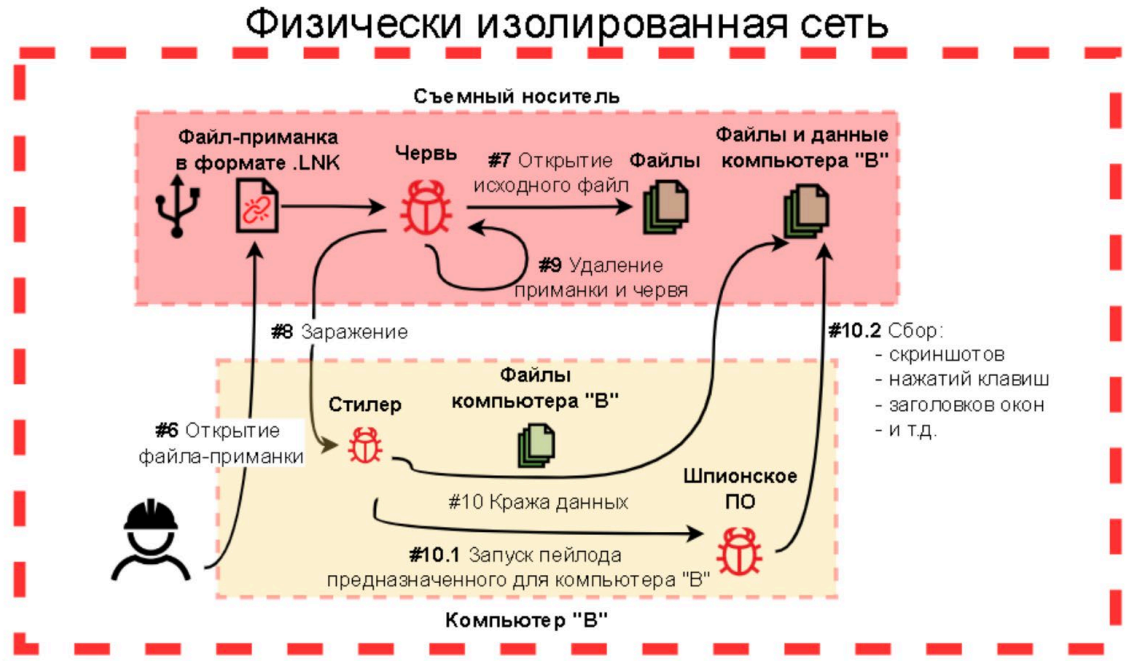
Схема подключений между сегментами сети атакованной организации

ersky
ICS CERT

https://ics-cert.kaspersky.ru/publications/reports/2021/02/25/lazarus-targets-defense-industry-with-threatneedle/

”Просто” кража данных из изолированных сегментов через флэшки

Расследование APT в промышленных организациях в восточной Европе



Упрощенная схема заражения компьютера в изолированном сегменте сети через зараженный съемный носитель

Kaspersky ICS CERT

https://ics-cert.kaspersky.ru/publications/reports/2023/07/31/common-ttps-of-attacks-against-industrial-organizations-implants-for-gathering-data/

Что же делать?

1 Исправляйте уязвимости (или не исправляйте).
Чтобы решить, читайте TI-отчёты.

2

Настраивайте безопасно защитные решения.

Чтобы понять как, читайте TI-отчёты.

3

Защищайтесь от фишинга

Тренируйте регулярно персонал.

И...читайте TI-отчёты

4

Для защиты от DLL Hijacking и BYOVD,
используйте white-listing (default deny)
Или... читайте TI-отчёты

5

Решили изолировать сеть - изолируйте по-настоящему. И... читайте TI-отчёты

6

Изолировали сеть «как надо» - защищайтесь от флешек:

- используйте Device Control
- включайте отображение «скрытых фалов» и расширений файлов
- проверяйте флэшки ДО КОНЦА
- учите персонал отличать документы и бинари от ярлыков

7

Ну и... наймите (так или иначе) людей, которые способны это всё делать.

Евгений Гончаров
Руководитель Kaspersky ICS CERT

evgeny.goncharov@kaspersky.com
ics-cert@kaspersky.com

kaspersky