



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 АPT на промышленные организации

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

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

Эпизод при расследовании АРТ
на промышленном
предприятии...

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

5

Удаляет указатели на callback-функции ядра:

*PsSetCreateProcessNotifyRoutine
PspCreateProcessNotifyRoutine
PspSetCreateProcessNotifyRoutine
PsSetCreateThreadNotifyRoutine
PspCreateThreadNotifyRoutine
PspSetCreateThreadNotifyRoutine
PsSetLoadImageNotifyRoutineEx
PsSetLoadImageNotifyRoutine
PspLoadImageNotifyRoutine...*

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

6

The screenshot shows the GitHub interface for the repository 'ly4k / CallbackHell'. The repository is public and has 95 forks and 443 stars. The main branch is 'main'. The file 'CallbackHell.cpp' is selected, showing a commit by 'ly4k' from 2 years ago. The code is an executable file with 650 lines (503 loc) and a size of 20.4 KB. The code includes headers for Windows, stdio, winddi, winterl, psapi, and tlhelp32. It defines a shellcode payload for a Windows command prompt.

```
1  #pragma warning( disable : 4005 )
2
3  #include <Windows.h>
4  #include <stdio.h>
5  #include <winddi.h>
6  #include <winterl.h>
7  #include <psapi.h>
8  #include <tlhelp32.h>
9
10 // [Shellcode here]
11 // (Run cmd.exe)
12 unsigned char payload[] =
13 "\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50\x52\x51" \
14 "\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x18\x48\x8b\x52" \
```

Kaspersky
ICS CERT

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

...которая эксплуатирует уязвимость CVE-2021-40449

7

The screenshot shows a GitHub repository interface. On the left is a file explorer with the following items: 'main' (selected), 'Go to file', 'CallbackHell' folder, '.gitignore', 'CallbackHell.sln', 'LICENSE', 'README.md' (highlighted), and 'poc.png'. Below the file list are links for 'Documentation' and 'Share feedback'. The main content area has tabs for 'Preview', 'Code', and 'Blame', with 'Preview' selected. It shows '152 lines (115 loc) · 6.97 KB'. The title is 'CallbackHell'. Below the title is the text 'Exploit for CVE-2021-40449 (Win32k - LPE)'. A list of links includes 'CallbackHell', 'Description', 'Technical Writeup', 'PoC', and 'References'. The 'Description' section contains the following text: 'CVE-2021-40449 is a use-after-free in Win32k that allows for local privilege escalation. The vulnerability was found in the wild by [Kaspersky](#). The discovered exploit was written to support the following Windows products:'. A list of supported Windows products follows: 'Microsoft Windows Vista', 'Microsoft Windows 7', 'Microsoft Windows 8', 'Microsoft Windows 8.1', 'Microsoft Windows Server 2008', and 'Microsoft Windows Server 2008 R2'.

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

Kaspersky
ICS CERT

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

8

CVE-2021-40449 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Win32k Elevation of Privilege Vulnerability

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



CNA: Microsoft Corporation

Base Score: 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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

Microsoft MSRC | Security Updates Acknowledgements { } Developer

Looking for email notifications? Please create your profile with your preferred email address to sign up for notifications. [See our blog post for more information.](#)

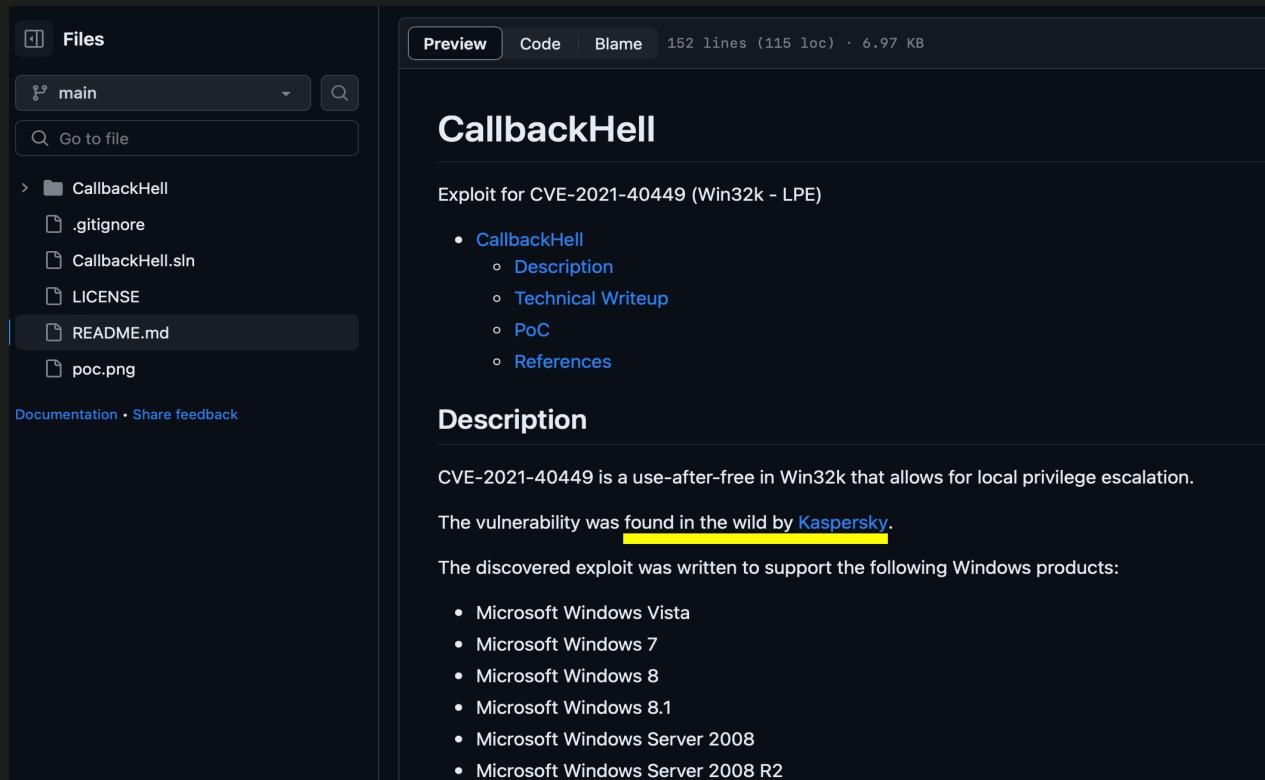
[Go to profile to subscribe](#) [Hide for](#)

[CVE-2021-40449](#)

Impact: Elevation of Privilege Max Severity: Important

CVSS:3.1 7.2

Metric	Value
> Base score metrics (8)	
∨ Temporal score metrics (3)	
▶ <u>Exploit Code Maturity</u>	∨ Functional <u>Functional exploit code is available. The code works in most situations where the vulnerability exists.</u>



The screenshot shows a GitHub repository page for 'CallbackHell'. The left sidebar displays the file structure, including a 'main' branch and files like '.gitignore', 'CallbackHell.sln', 'LICENSE', 'README.md', and 'poc.png'. The main content area shows the 'CallbackHell' directory, which is an exploit for CVE-2021-40449 (Win32k - LPE). It includes a 'Description' section and a list of supported Windows products.

Files

main

Go to file

- CallbackHell
 - .gitignore
 - CallbackHell.sln
 - LICENSE
 - README.md
 - poc.png

Documentation · Share feedback

Preview Code Blame 152 lines (115 loc) · 6.97 KB

CallbackHell

Exploit for CVE-2021-40449 (Win32k - LPE)

- CallbackHell
 - Description
 - Technical Writeup
 - PoC
 - References

Description

CVE-2021-40449 is a use-after-free in Win32k that allows for local privilege escalation.

The vulnerability was found in the wild by Kaspersky.

The discovered exploit was written to support the following Windows products:

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

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



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/>

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

12

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 АРТ на промышленные организации

ff Keep things as simple as possible, but not simpler

_____ Albert Einstein?

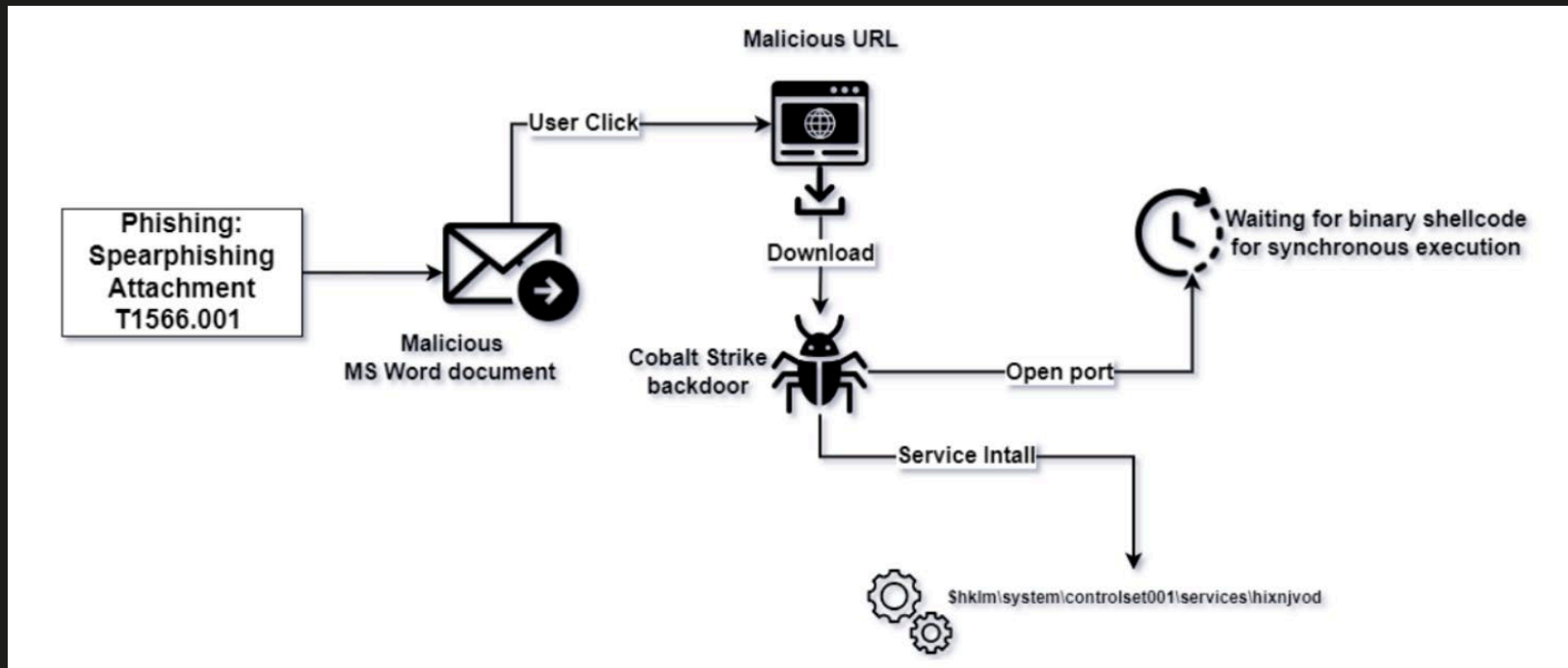


It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience

_____ Albert Einstein

«Просто». ФИШИНГ

Расследование АРТ в Пакистане. Скомпрометированы инженеры ОТ.



«Просто» DLL Hijacking / Side Loading

17

Пример1: АРТ в Пакистане, ОТ-инженеры (см. предыдущий слайд)

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

Пример2: АРТ 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: АРТ 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 АРТ на предприятии ВПК в восточной Европе

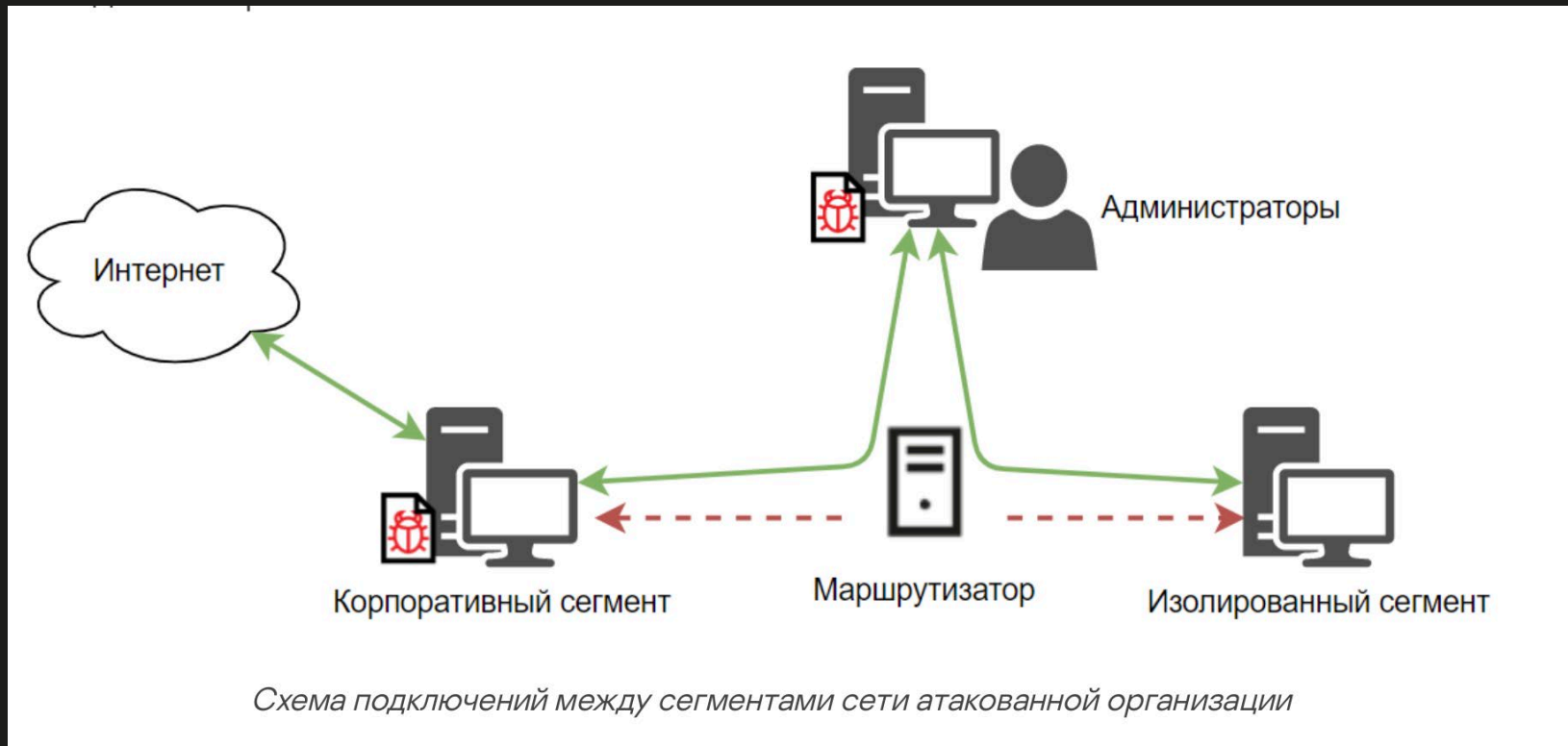
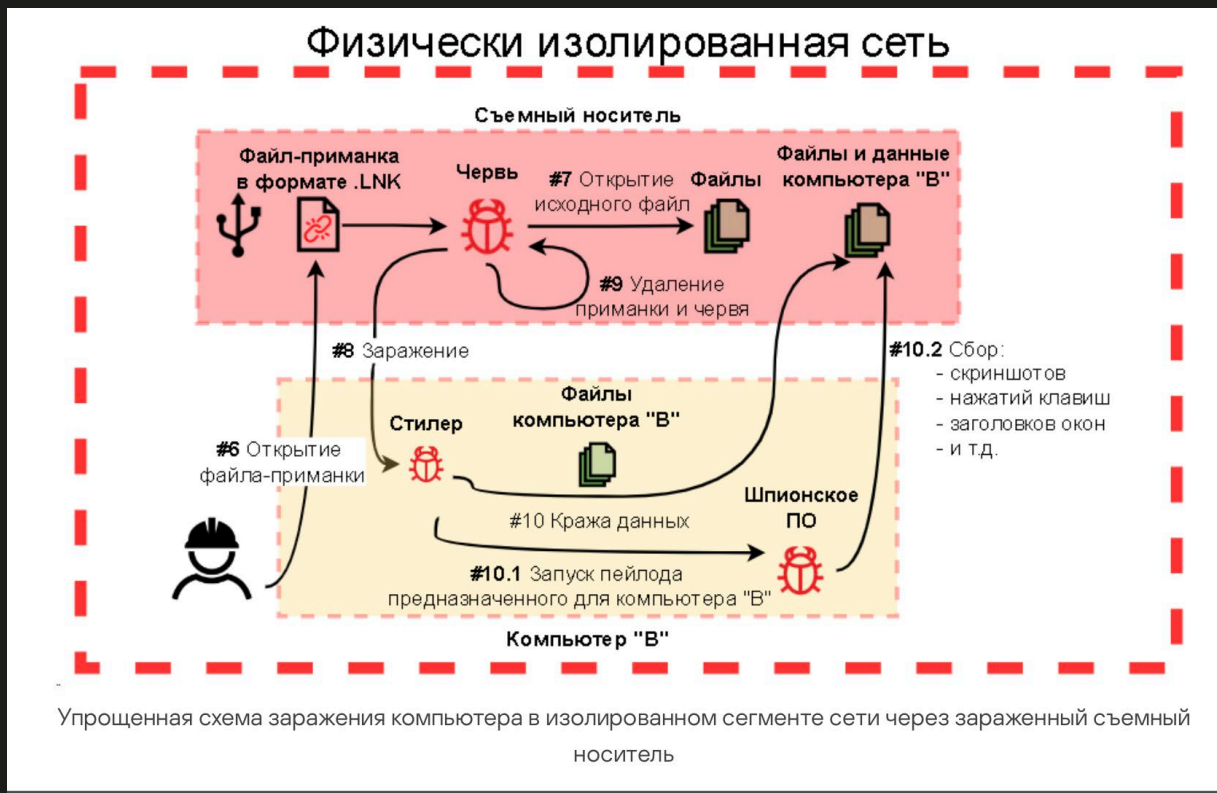


Схема подключений между сегментами сети атакованной организации



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