

# Exploitation of the CVE-2021-40444 vulnerability in MSHTML

SL [securelist.com/exploitation-of-the-cve-2021-40444-vulnerability-in-mshtml/104218/](https://securelist.com/exploitation-of-the-cve-2021-40444-vulnerability-in-mshtml/104218/)



Incidents

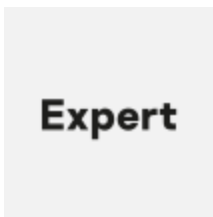
Incidents

16 Sep 2021

minute read



Authors



AMR

## Summary

---

Last week, Microsoft reported the remote code execution vulnerability CVE-2021-40444 in the MSHTML browser engine. According to the company, this vulnerability has already been used in targeted attacks against Microsoft Office users. In attempt to exploit this vulnerability, attackers create a document with a specially-crafted object. If a user opens the document, MS Office will download and execute a malicious script.

According to our data, the same attacks are still happening all over the world. We are currently seeing attempts to exploit the CVE-2021-40444 vulnerability targeting companies in the research and development sector, the energy sector and large industrial sectors, banking and medical technology development sectors, as well as telecommunications and the IT sector. Due to its ease of exploitation and the few published Proof-of-Concept (PoC), we expect to see an increase in attacks using this vulnerability.

### *Geography of CVE-2021-40444 exploitation attempts*

Kaspersky is aware of targeted attacks using CVE-2021-40444, and our products protect against attacks leveraging the vulnerability. Possible detection names are:

- HEUR:Exploit.MSOffice.CVE-2021-40444.a
- HEUR:Trojan.MSOffice.Agent.gen

- PDM:Exploit.Win32.Generic

All events > Process started

Isolate kt-es-1.kata.infra Create a prevention rule Create a task

Details Events (4)

**Process started**

IOA tags	suspicious_process_spawned_by_office_app
File	"C:\Windows\System32\control.exe"
Process ID	7896
Launch parameters	"C:\Windows\System32\control.exe" ".cpl.../msword.inf,"
MD5	62d970d8b60f75c12d21c740f2d8a5da
SHA256	d6e21da3be0701162a36f8c9f94e616b1a0c5f4cc1b52ef81959cb257957c1
Size	115 KB
Event time	15 September 2021 14:45:50.591
Process end time	15 September 2021 14:45:58.180

**Parent process**

File	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE"
Process ID	2656
Launch parameters	"C:\Program Files\Microsoft Office\Office16\WINWORD EXE" /n "C:\Users\administrator\Desktop\document.docx" /o ""
MD5	ce33fc3c687d3c01159a8caea7f5482e
SHA256	5d75d0ea8bb5b652f7b72cf728c0032bd486d54a5c4978ceacdf70b4317ee6

**System info**

Host name	kt-es-1.kata.infra
Account type	Non-administrator

### Killchain generated by KEDR during execution of CVE-2021-40444 Proof-of-Concept

Experts at Kaspersky are monitoring the situation closely and improving mechanisms to detect this vulnerability using Behavior Detection and Exploit Prevention components. Within our Managed Detection and Response service, our SOC experts are able to detect when this vulnerability is exploited, investigate such attacks and notify customers.

## Technical details

The remote code execution vulnerability CVE-2021-40444 was found in MSHTML, the Internet Explorer browser engine which is a component of modern Windows systems, both user and server. Moreover, the engine is often used by other programs to work with web content (e.g. MS Word or MS PowerPoint).

In order to exploit the vulnerability, attackers embed a special object in a Microsoft Office document containing an URL for a malicious script. If a victim opens the document, Microsoft Office will download the malicious script from the URL and run it using the MSHTML engine. Then the script can use ActiveX controls to perform malicious actions on the victim's computer. For example, the original zero-day exploit which was used in targeted attacks at

the time of detection used ActiveX controls to download and execute a Cobalt Strike payload. We are currently seeing various types of malware, mostly backdoors, which are delivered by exploiting the CVE-2021-40444 vulnerability.

## Mitigations

---

- Follow [Microsoft security update guidelines](#).
- Use the latest [Threat Intelligence information](#) to keep up to date with TTPs used by threat actors.
- Businesses should use a security solution that provides vulnerability, patch management and exploit prevention components, such as the [Automatic Exploit Prevention](#) component in Kaspersky Endpoint Security for Business. The component monitors suspicious actions in applications and blocks malicious file execution.
- Use solutions like [Kaspersky Endpoint Detection and Response](#) and [Kaspersky Managed Detection and Response](#) service, which help identify and stop an attack at an early stage before the attackers achieve their final goal.

## IoC

---

### MD5

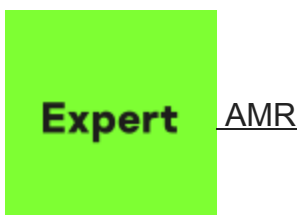
[ef32824c7388a848c263deb4c360fd64](#)  
[e58b75e1f588508de7c15a35e2553b86](#)  
[e89dbc1097cfb8591430ff93d9952260](#)

### URL

[hidusi\[.\]com](#)  
[103.231.14\[.\]134](#)

- [Malware Descriptions](#)
- [Microsoft](#)
- [Microsoft Internet Explorer](#)
- [Proof-of-Concept](#)
- [Security technology](#)
- [Targeted attacks](#)
- [Vulnerabilities and exploits](#)
- [Zero-day vulnerabilities](#)

Authors



Your email address will not be published. Required fields are marked \*



## Table of Contents

- [Summary](#)
- [Technical details](#)
- [Mitigations](#)
- [IoC](#)

## GReAT webinars

13 May 2021, 1:00pm

## **GReAT Ideas. Balalaika Edition**

---

26 Feb 2021, 12:00pm

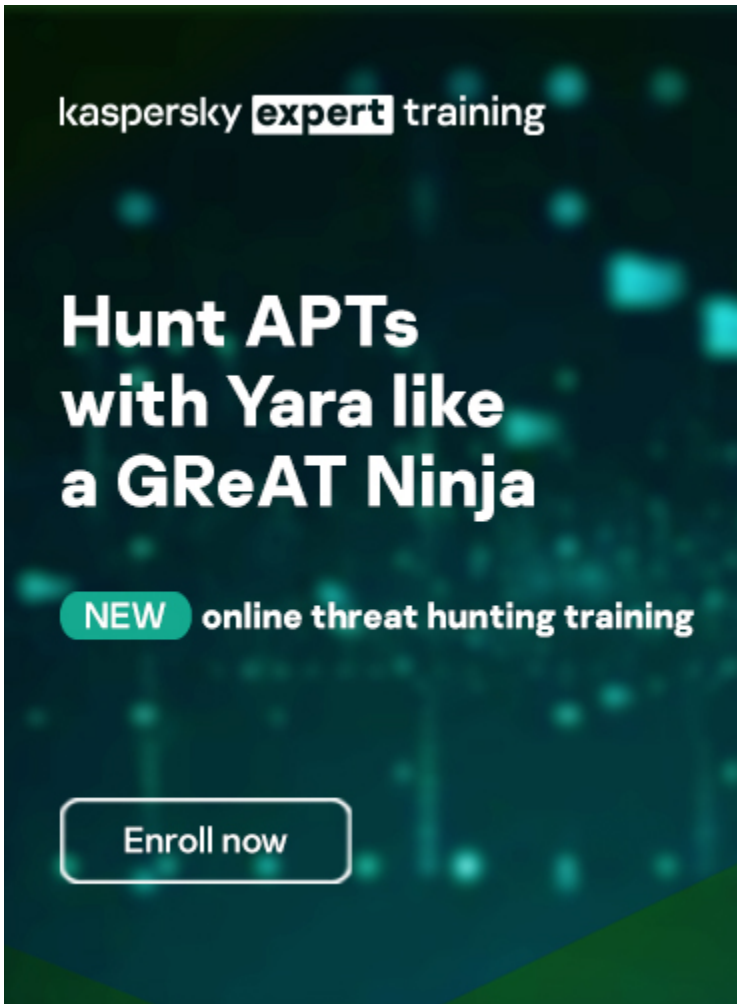
17 Jun 2020, 1:00pm

26 Aug 2020, 2:00pm

Subscribe to our weekly e-mails

The hottest research right in your inbox

- 
- 
-



Reports

### **APT trends report Q1 2022**

---

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

### **Lazarus Trojanized DeFi app for delivering malware**

---

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

### **MoonBounce: the dark side of UEFI firmware**

---

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

### **The BlueNoroff cryptocurrency hunt is still on**

---

---

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

A promotional banner for Kaspersky Expert Training. The background is a vibrant green with teal triangular accents in the corners. At the top left, the text "kaspersky expert training" is displayed, with "expert" in a black box. The main headline reads "Improve threat hunting & reversing skills with GReAT experts". At the bottom, there is a white button with a black border containing the text "Learn more".

kaspersky **expert** training

**Improve threat hunting & reversing skills with GReAT experts**

Learn more

Subscribe to our weekly e-mails

The hottest research right in your inbox

- 
- 
-

kaspersky **expert** training

# Improve threat hunting & reversing skills with GReAT experts

[Learn more](#)