任务2:

* **t5/keyword/hint\_hit\_precision:**0.386046511627907
* **t5/word/hint\_hit\_recall:**0.06806282722513089
* **gpt3/lexical/rouge\_rouge1:**0.5251989389920425
* **gpt3/lexical/rouge\_rouge2:**0.16533333333333336
* **gpt3/lexical/rouge\_rougeL:**0.21750663129973474
* **gpt3/lexical/rouge\_rougeLsum:**0.21750663129973474

**Windows**; **CVE-2021-40449**; **vulnerability**; the **Win32k** **driver**; the **exploit**; **use**; **kernel** modules; **MysterySnail**; **Trojan**; **the RAT**; **commands(加粗是标注重叠)**

generated\_text:"**Kaspersky**; a **zero-day**; **Microsoft**; **use**; **privilege** exploits; **servers**; a **vulnerability**; the **Win32k** driver; the **CVE-2021-40449**; ~~use~~; user-mode callbacks; API functions; ~~a kernel function~~; hdcOpenDCW; GreResetDCInternal; GDI palette objects; memory; ~~a kernel function~~; a primitive; ~~memory~~; the exploit process; the attackers; **Chinese**; APT; 2012; malicious code; ~~Chinese~~; IP; the **attack**; the zero-day **exploit**; ~~vulnerabilities~~; at least 90 days; the exploit chain; code similarity; re-use; **C2** infrastructure; ~~this attack~~; **IronHusky**; ~~APT~~; APT activities; email; detection; compromise."

generated\_text:"**Kaspersky**; a **zero-day**; **Microsoft**; **use**; **privilege** exploits; servers; a vulnerability; the Win32k driver; the CVE-2021-40449; ~~use~~; user-mode callbacks; API functions; ~~a kernel function~~; hdcOpenDCW; GreResetDCInternal; GDI palette objects; memory; ~~a kernel function~~; a primitive; ~~memory~~; the exploit process; the attackers; Chinese; APT; 2012; malicious code; ~~Chinese~~; IP; the attack; the zero-day exploit; ~~vulnerabilities~~; at least 90 days; the exploit chain; code similarity; re-use; C2 infrastructure; ~~this attack~~; IronHusky; ~~APT~~; APT activities; email; detection; compromise."

----------------

ref\_text:"<START-1>The PDF describes cyberattacks by a threat actor dubbed MysterySnail that exploited a new Windows **zero-day** **vulnerability**. The zero-day **exploit** elevates **privilege**s on Windows **servers** by targeting a **use**-after-free flaw in the **Win32k** kernel driver. **Kaspersky** discovered **attack**s using this exploit in late August 2021 and promptly reported it to **Microsoft**. Microsoft assigned **CVE-2021-40449** to the vulnerability and patched it in the October 2021 Patch Tuesday update. The exploit supports a wide range of Windows versions including Server 2008 through 2019. Kaspersky believes it was sold as a server privilege escalation exploit. The attacks delivered a remote access trojan dubbed MysterySnail RAT that gathers system info and can execute commands. The RAT has various anti-analysis features and tried to hide its **C2** communications. Kaspersky connected these attacks to a **Chinese**-speaking advanced persistent threat actor called **IronHusky**. Evidence showed the group has been active since at least 2012, targeting IT companies, military contractors, and diplomatic entities. In summary, the PDF provides details on a new Windows zero-day exploit used by a sophisticated cyberespionage actor in attacks starting in August 2021. Kaspersky worked with Microsoft to patch the vulnerability used in the exploits. <END-1>"

"In late August and early September 2021, **Kaspersky** detected **attack**s using a **zero-day** elevation of **privilege** **exploit** on **Microsoft** Windows **servers**. The exploit targeted a **vulnerability** in the **Win32k** driver, specifically **CVE-2021-40449**, allowing attackers to execute arbitrary kernel functions through user-mode callbacks. The exploit chain was not fixed by Microsoft until October 2021. This exploit was linked to a malware payload known as MysterySnail, which has been used in espionage campaigns against IT companies, military contractors, and diplomatic entities. The malware was connected to the **Chinese**-speaking APT group **IronHusky**, with code similarity and **C2** infrastructure re-**use** dating back to 2012. The attackers were able to compromise systems using GDI palette objects and a kernel function to read and write kernel memory. The exploit process ran with Medium IL, allowing for the leakage of kernel module addresses. The MysterySnail RAT family was identified as a remote shell Trojan intended to be executed by the elevation of privilege exploit. This attack highlights the importance of timely patching and detection to prevent malicious activity."

2021 年 8 月底和 9 月初，卡巴斯基检测到使用零日特权提升漏洞对 Microsoft Windows 服务器发起的攻击。该漏洞针对 Win32k 驱动程序中的漏洞，具体来说是 CVE-2021-40449，允许攻击者通过用户模式回调执行任意内核函数。直到 2021 年 10 月，微软才修复了该漏洞链。该漏洞与一种名为 MysterySnail 的恶意软件负载有关，该负载已用于针对 IT 公司、军事承包商和外交实体的间谍活动。该恶意软件与使用中文的 APT 组织 IronHusky 有关，其代码相似性和 C2 基础设施重用可追溯到 2012 年。攻击者能够使用 GDI 调色板对象和内核函数来读取和写入内核内存，从而破坏系统。漏洞利用过程使用 Medium IL 运行，从而导致内核模块地址泄露。MysterySnail RAT 家族被确定为旨在通过特权提升漏洞执行的远程 shell 木马。这次攻击凸显了及时修补和检测以防止恶意活动的重要性。

PDF 描述了一个名为 MysterySnail 的威胁行为者利用新的 Windows 零日漏洞进行的网络攻击。该零日漏洞利用 Win32k 内核驱动程序中的释放后使用漏洞来提升 Windows 服务器上的权限。卡巴斯基在 2021 年 8 月下旬发现了利用此漏洞的攻击，并立即向微软报告。微软为该漏洞分配了 CVE-2021-40449，并在 2021 年 10 月的补丁星期二更新中对其进行了修补。该漏洞支持多种 Windows 版本，包括 Server 2008 至 2019。卡巴斯基认为它是作为服务器权限提升漏洞出售的。攻击传递了一种名为 MysterySnail RAT 的远程访问木马，它可以收集系统信息并执行命令。该 RAT 具有各种反分析功能，并试图隐藏其 C2 通信。卡巴斯基将这些攻击与一个讲中文的高级持续威胁行为者 IronHusky 联系起来。证据表明，该组织至少自 2012 年以来一直活跃，目标是 IT 公司、军事承包商和外交实体。总之，该 PDF 提供了有关一个老练的网络间谍行为者在 2021 年 8 月开始的攻击中使用的新 Windows 零日漏洞的详细信息。卡巴斯基与微软合作修补了漏洞利用中使用的漏洞。

* **t5/keyword/hint\_hit\_precision:**0.36363636363636365
* **t5/word/hint\_hit\_recall:**0.08376963350785341
* **gpt3/lexical/rouge\_rouge1:**0.5250737463126843
* **gpt3/lexical/rouge\_rouge2:**0.2077151335311573
* **gpt3/lexical/rouge\_rougeL:**0.2890855457227139
* **gpt3/lexical/rouge\_rougeLsum:**0.2890855457227139
* **Windows**; **CVE-2021-40449**; **vulnerability**; the **Win32k** **driver**; the **exploit**; **use**; **kernel** modules; **MysterySnail**; **Trojan**; **the RAT**; **commands(加粗是标注重叠)**

generated\_text:"**the attack**; the **zero-day**; compromise; **Win32k**; **CVE-2021-40449**; **use**; a technique; leak; kernel modules; **The exploit**; ~~exploits~~; the base addresses; ~~kernel modules~~; ~~use;~~ a root cause; the **vulnerability**; ~~the kernel;~~ the exploit process; ResetDC; the bootloader; the kernel; the code; **Chinese**; APT; **2012**; **attacks**; ~~the zero-day;~~ the exploit chain; the C2 infrastructure; a solution; **privileges**; **servers**; the exploits."

ref\_text:"<START-1>The PDF describes cyberattacks by a threat actor dubbed MysterySnail that exploited a new Windows **zero-day** **vulnerability**. The zero-day exploit elevates **privileges** on Windows **servers** by targeting a **use**-after-free flaw in the **Win32k kernel** driver. Kaspersky discovered **attacks** using this exploit in late August 2021 and promptly reported it to Microsoft. Microsoft assigned **CVE-2021-40449** to the vulnerability and patched it in the October 2021 Patch Tuesday update. **The exploit** supports a wide range of Windows versions including Server 2008 through 2019. Kaspersky believes it was sold as a server privilege escalation exploit. **The attack**s delivered a remote access trojan dubbed MysterySnail RAT that gathers system info and can execute commands. The RAT has various anti-analysis features and tried to hide its C2 communications. Kaspersky connected these attacks to a **Chinese**-speaking advanced persistent threat actor called IronHusky. Evidence showed the group has been active since at least **2012**, targeting IT companies, military contractors, and diplomatic entities. In summary, the PDF provides details on a new Windows zero-day exploit used by a sophisticated cyberespionage actor in attacks starting in August 2021. Kaspersky worked with Microsoft to patch the vulnerability used in the exploits. <END-1>"

"The article discusses a recent attack utilizing a **zero-day** exploit targeting **Win32k** in Microsoft Windows **servers**. **The exploit**, identified as **CVE-2021-40449**, involves a **use**-after-free **vulnerability** in the NtGdiResetDC function, allowing attackers to compromise **kernel** memory. **The attack** relies on a technique to leak kernel module addresses and was discovered in espionage campaigns linked to the **Chinese**-speaking APT group IronHusky dating back to **2012**. The exploit was promptly reported to Microsoft and patched in the October Patch Tuesday. Additionally, the attack was found to be associated with the MysterySnail RAT family, indicating a sophisticated and coordinated effort to target IT companies, military contractors, and diplomatic entities. The exploit was designed to elevate **privileges** on servers running various versions of Windows, highlighting the need for enhanced security measures to prevent such **attacks** in the future."