任务1:

* **t5/keyword/hint\_hit\_precision:**0.2894736842105263
* **t5/word/hint\_hit\_recall:**0.07853403141361257
* **gpt3/lexical/rouge\_rouge1:**0.5565217391304347
* **gpt3/lexical/rouge\_rouge2:**0.19241982507288627
* **gpt3/lexical/rouge\_rougeL:**0.24927536231884057
* **gpt3/lexical/rouge\_rougeLsum:**0.24927536231884057

**Windows**; **CVE-2021-40449**; **vulnerability**; the **Win32k** **driver**; the **exploit**; **use**; **kernel** modules; **MysterySnail**; **Trojan**; **the RAT**; **commands**

generated\_text:"the **zero-day**; **Kaspersky**; **cyberattacks**; **Microsoft** Windows; **use**; a **vulnerability**; the **Win32k** driver; **CVE-2021-40449**; ~~use;~~ user-mode callbacks; API functions; **the exploit**; the base addresses; **kernel** modules; IOCs; ~~this vulnerability~~; **attacks**; **military**; defense **contractors**; **diplomatic entities**; **2012**; ~~the exploit~~; ~~arbitrary~~ **~~kernel~~** ~~function~~; GDI palette objects; memory; a primitive; the **C2** infrastructure; evidence; ~~the exploit;~~ **Chinese**; APT; ~~the exploit~~ process; compromise; ~~the zero-day~~; espionage campaigns; technical details; this cluster; ~~the zero-day exploit~~."

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

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 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 **cyberattacks** using a **zero-day** exploit targeting multiple **Microsoft** **Windows** servers. **The exploit** targeted a previously unknown **vulnerability** in the **Win32k** **driver,** allowing attackers to elevate privileges and execute arbitrary **kernel** functions using user-mode callbacks. The exploit also utilized GDI palette objects to manipulate memory and leak kernel addresses. The exploit was linked to a malware payload known as MysterySnail RAT, which has been **use**d in espionage campaigns against IT companies, **military**/defense **contractors**, and **diplomatic entities** since **2012**. The **C2** infrastructure used in these **attacks** was connected to the IronHusky APT group, suggesting **Chinese**-speaking involvement. Microsoft patched the vulnerability (**CVE-2021-40449**) on October 12, 2021, as part of the October Patch Tuesday. This cluster of attacks highlights the ongoing threat posed by sophisticated cyber actors exploiting zero-day vulnerabilities for espionage purposes."

* **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."

**参考摘要：**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。

**好的：**2021 年 8 月底和 9 月初，卡巴斯基检测到利用零日漏洞攻击多台 Microsoft Windows 服务器的网络攻击。该漏洞利用 Win32k 驱动程序中一个以前未知的漏洞，允许攻击者使用用户模式回调提升权限并执行任意内核函数。该漏洞还利用 GDI 调色板对象来操纵内存并泄露内核地址。该漏洞与一种名为 MysterySnail RAT 的恶意软件负载有关，自 2012 年以来，该恶意软件负载一直用于针对 IT 公司、军事/国防承包商和外交实体的间谍活动。这些攻击中使用的 C2 基础设施与 IronHusky APT 组织有关，表明有中文人员参与其中。微软于 2021 年 10 月 12 日在 10 月补丁星期二修补了该漏洞 (CVE-2021-40449)。这一系列攻击凸显了老练的网络行为者利用零日漏洞进行间谍活动所带来的持续威胁。

**不好的：**本文讨论了最近一次利用零日漏洞攻击 Microsoft Windows 服务器中的 Win32k 的攻击。该漏洞被标识为 CVE-2021-40449，涉及 NtGdiResetDC 函数中的释放后使用漏洞，允许攻击者破坏内核内存。该攻击依赖于一种泄露内核模块地址的技术，是在 2012 年与讲中文的 APT 组织 IronHusky 有关的间谍活动中发现的。该漏洞被迅速报告给微软，并在 10 月的补丁星期二进行了修补。此外，该攻击被发现与 MysterySnail RAT 家族有关，这表明这是一次复杂而协调的攻击，目标是 IT 公司、军事承包商和外交实体。该漏洞旨在提升运行各种 Windows 版本的服务器的权限，这凸显了加强安全措施以防止将来再次发生此类攻击的必要性。