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~~."

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."

* **t5/keyword/hint\_hit\_precision:**0.5259259259259259
* **t5/word/hint\_hit\_recall:**0.07329842931937172
* **gpt3/lexical/rouge\_rouge1:**0.5169230769230768
* **gpt3/lexical/rouge\_rouge2:**0.17956656346749225
* **gpt3/lexical/rouge\_rougeL:**0.2584615384615384
* **gpt3/lexical/rouge\_rougeLsum:**0.2584615384615384
* **Windows**; **CVE-2021-40449**; **vulnerability**; the **Win32k** **driver**; the **exploit**; **use**; **kernel** modules; **MysterySnail**; **Trojan**; **the RAT**; **commands**

"the **zero-day**; **Kaspersky**; **attacks**; multiple **Microsoft** Windows servers; July; September 2021; ~~Kaspersky~~; a use-after-free **vulnerability**; the **Win32k** **driver**; **CVE-2021-40449**; ~~the vulnerability~~; **use**; user-mode callbacks; API functions; **kernel** modules; **the exploit**; a **c2** infrastructure; **Chinese**; APT activity; **2012**; a solution; **privileges**; ~~servers~~; CVE-2016-3309; a ~~zero-day~~; tactics; the exploit chain."

In July and September 2021, **Kaspersky** detected **attacks** on multiple **Microsoft** **Windows servers** utilizing a **zero-day** exploit targeting a **use-after-free** vulnerability in the Win32k **driver**, identified as **CVE-2021-40449**. **The exploit** allowed attackers to escalate **privileges** by manipulating user-mode callbacks and executing unexpected API functions. The exploit chain also involved leaking **kernel** module addresses and utilizing a **C2** infrastructure. These attacks were connected to **Chinese**-speaking APT activity dating back to **2012**, specifically attributed to IronHusky. The exploit was patched by Microsoft in October 2021 as part of the October Patch Tuesday. Additionally, a previously unknown remote shell-type Trojan, dubbed MysterySnail RAT, was discovered to be associated with these attacks, targeting IT companies, military/defense contractors, and diplomatic entities."

2021 年 7 月和 9 月，卡巴斯基检测到多台 Microsoft Windows 服务器受到利用零日漏洞的攻击，该漏洞针对 Win32k 驱动程序中的释放后使用漏洞，该漏洞被标识为 CVE-2021-40449。该漏洞允许攻击者通过操纵用户模式回调和执行意外的 API 函数来提升权限。漏洞链还涉及泄露内核模块地址和利用 C2 基础设施。这些攻击与可追溯到 2012 年的中文 APT 活动有关，具体归因于 IronHusky。微软于 2021 年 10 月在 10 月补丁星期二修补了该漏洞。此外，还发现一种以前未知的远程 shell 类型木马，称为 MysterySnail RAT，与这些攻击有关，目标是 IT 公司、军事/国防承包商和外交实体。”

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>"

**ref\_text**网络安全公司 Arbor Networks 在过去一年中观察到了针对多个亚洲国家的 Poison Ivy 远程访问木马 (RAT) 恶意软件的新活动。技术分析显示，这个绰号为“Korplug”的 Poison Ivy 变体使用 DLL 侧载来感染系统。它会释放暗示目标的诱饵文档、DLL 和 shellcode 文件。该恶意软件会复制合法的 Windows 可执行文件来加载 DLL，该 DLL 会解密配置数据并连接到命令和控制服务器。诱饵文件暗示在最近的选举期间，缅甸的民主团体是目标。其他文件提到了东盟会议和成员，暗示东南亚政府和军事组织是目标。其他诱饵文件是用韩语和蒙古语编写的。基础设施分析显示，Poison Ivy 活动与其他恶意软件家族（包括 Gh0strat 和 Nitol）之间存在重叠，表明可能由一个共同的威胁行为者协调。该恶意软件继续发展，新的配置和工件可能旨在逃避防御。 Arbor Networks 评估称 Poison Ivy 仍是一种活跃威胁，有动机的攻击者在亚洲各地的针对性活动中使用了新变种。他们建议监控系统是否存在相关的入侵指标，并确保防范已知的 Poison Ivy 恶意软件功能。

本文讨论了远程访问木马 Poison Ivy (PIVY) 的新变种，该变种至少在过去一年中针对包括缅甸在内的亚洲国家。该恶意软件使用 DLL 侧载并投放诱饵文档来暗示目标。样本以特定目录格式创建一个名为 ActiveUpdate.dll 的 DLL 和一个名为 Active.dat 的 PIVY shellcode 文件。该恶意软件还将 rundll32.exe 复制到 ActiveFlash.exe 并自行安装在 Windows 启动文件夹中以自动启动。恶意软件的解密配置已被修改以混淆解析工具，并且 C2 服务器通过以特定字符串结尾的主机名来标识。文章还提到与缅甸民主倡议相关的文件在攻击中被用作诱饵。