"summary": "The document discusses malware campaigns targeting organizations involved with the 2018 Pyeongchang Winter Olympics. Security researchers at McAfee uncovered new malware implants associated with intrusion activity that began in December 2017 with a PowerShell implant delivering basic system information to the attackers. The new implants discovered include: Gold Dragon - Gathers system information and profiles the victim system. It establishes persistence on machines running the Korean word processor Hangul. Brave Prince - Korean-language implant that profiles system config and contents. Exfiltrates data via email and HTTP posts. Ghost419 - Based on Gold Dragon and Brave Prince. Gathers system reconnaissance information. RunningRat - Remote access Trojan that captures keystrokes and exfiltrates them. Contains additional unused functionality. The tactics, techniques, and infrastructure analysis indicates these new implants are part of the same intrusion set that targeted the Olympics with the initial PowerShell implant. The expanded capabilities enable long-term persistence and data exfiltration from victim networks. The implants demonstrate anti-analysis and anti-forensics techniques. The campaign establishes permanent system access exploiting the high profile nature of the Olympics. McAfee assesses with high confidence the activity is part of a nation-state sponsored cyber espionage operation. ",

"chatglm\_gen\_texts": "The Advanced Threat Research (ATR) report of January 2018 discovered four malware implants: Gold Dragon, Brave Prince, Ghost419, and Running Rat. These implants were part of an operation to gain persistence for continued data exchange and targeted access. Gold Dragon, the second-stage payload in the Pyeongchang Olympics attack, had a more robust persistence mechanism than the initial PowerShell implant and enables the attacker to do more to the target system. The malware was observed in the wild since December 24 and contains elements, code, and similar behavior to implants Ghost419 and Brave Prince. The malware does not establish persistence for itself but for another component on the system, and it begins by looking for an instance of the Hangul word processor (HWP) running on the system. The report also describes a DLL-based implant created on December 21 that was downloaded by a Gold Dragon variant created December 24, and the five variants of Gold Dragon compiled December 24 appeared heavily during the targeting of the Olympics organizations."

“summary”：分别介绍了4个植入程序

“chatglm\_gen\_texts”： 只介绍Dragon一个植入程序，并且和其他三个植入程序功能混淆

“summary”：“该文件讨论了针对参与 2018 年平昌冬奥会的组织的恶意软件活动。McAfee 的安全研究人员发现了与入侵活动相关的新恶意软件植入物，该活动始于 2017 年 12 月，当时 PowerShell 植入物向攻击者提供了基本的系统信息。发现的新植入物包括：Gold Dragon - 收集系统信息并分析受害者系统。它在运行韩语文字处理器 Hangul 的机器上建立了持久性。Brave Prince - 韩语植入物，可分析系统配置和内容。通过电子邮件和 HTTP 帖子泄露数据。**Ghost419 - 基于 Gold Dragon 和 Brave Prince**。收集系统侦察信息。RunningRat - 捕获击键并泄露它们的远程访问木马。包含其他未使用的功能。策略、技术和基础设施分析表明，这些新植入物是与最初的 PowerShell 植入物针对奥运会的同一入侵集的一部分。扩展的功能可实现长期持久性和从受害者网络泄露数据。这些植入物展示了反分析和反取证技术。该活动利用奥运会的高调性质建立了永久的系统访问权限。McAfee 高度确信该活动是国家支持的网络间谍活动的一部分。“，

“chatglm\_gen\_texts”：“2018 年 1 月的高级威胁研究 (ATR) 报告发现了四种恶意软件植入程序：Gold Dragon、Brave Prince、Ghost419 和 Running Rat。这些植入程序是获得持久性以进行持续数据交换和有针对性访问的行动的一部分。Gold Dragon 是平昌奥运会攻击的第二阶段有效载荷，它比最初的 PowerShell 植入程序具有更强大的持久性机制，使攻击者能够对目标系统进行更多操作。**该恶意软件自 12 月 24 日起在野外被发现，包含与 Ghost419 和 Brave Prince 植入程序类似的元素、代码和行为**。该恶意软件不会为自己建立持久性，而是为系统上的另一个组件建立持久性，它首先寻找在系统上运行的 Hangul 文字处理器 (HWP) 实例。该报告还描述了 12 月 21 日创建的基于 DLL 的植入程序，该植入程序由 12 月 24 日创建的 Gold Dragon 变体下载，12 月 24 日编译的五个 Gold Dragon 变体在针对奥运会组织的攻击中大量出现。”

"summary": "The report details an attack campaign attributed to the China-based threat group BRONZE PRESIDENT, which targeted Russian speakers with updated PlugX malware. In March 2022, researchers analyzed a malicious executable file masquerading as a Russian-language document about a Russian border detachment. The file's name and content suggest it was crafted to target officials familiar with the Russia-China border region. When executed, the file displayed a decoy English-language document about EU sanctions on Belarus while downloading additional files from a staging server. Analysis revealed this to be a typical PlugX attack involving DLL search order hijacking to execute the malware payload. The server also hosted domains linked to previous BRONZE PRESIDENT campaigns using similar techniques. The targeting of Russian speakers and European entities indicates the group has likely received updated intelligence requirements from China due to the war in Ukraine. Rather than its usual Southeast Asian targets, BRONZE PRESIDENT appears to be gathering political and military intelligence of value to China during this period. The report provides indicators of compromise for the malware samples, staging server, and command and control infrastructure. It advises organizations to review access to these to mitigate exposure. The adaptable nature of BRONZE PRESIDENT highlighted means entities in regions of interest to China should closely monitor for similar activity. ",

"chatglm\_gen\_texts": "The article highlights a threat actor, the BRONZE PRESIDENT, that has targeted Russian speakers with an updated malware payload. The target is likely to have been chosen to collect intelligence from allies and friends in the region. The researchers at Secureworks detected the malware in an executable file masquerading as a Russian document, and the move could be related to changes in China's intelligence collection requirements due to the war in Ukraine. The heavily obfuscated file downloaded additional files from a staging server, and the files were typical of the malware's use of DLL search order hijacking to execute the PlugX payload. The authors suggest that the Decoy document display and the use of the ping command to incorporate a delay could be used to fool victims."

1.信息不符合：summary的攻击目标是俄中边境地区的官员，chatglm的攻击目标是盟友和朋友的情报

2.内容提取不全面：只有少量信息和目标摘要重合，信息提取不准确

“summary”：“该报告详细介绍了归因于中国威胁组织 BRONZE PRESIDENT 的攻击活动，该组织使用更新的 PlugX 恶意软件针对俄语使用者。2022 年 3 月，研究人员分析了一个伪装成俄语文档的恶意可执行文件，该文件是关于俄罗斯边境支队的。该文件的名称和内容表明，它是为针对熟悉俄中边境地区的官员而制作的。执行时，该文件显示了一份关于欧盟对白俄罗斯制裁的诱饵英文文档，同时从暂存服务器下载其他文件。分析显示，这是一次典型的 PlugX 攻击，涉及劫持 DLL 搜索顺序以执行恶意软件负载。该服务器还使用类似技术托管了与以前的 BRONZE PRESIDENT 活动相关的域。针对俄语使用者和欧洲实体的攻击表明，由于乌克兰战争，该组织可能已收到中国更新的情报要求。与通常的东南亚目标不同，BRONZE PRESIDENT 似乎在此期间收集了对中国有价值的政治和军事情报。该报告提供了恶意软件样本、登台服务器和命令与控制基础设施的入侵指标。它建议组织审查对这些内容的访问，以减轻风险。BRONZE PRESIDENT 的适应性突出，这意味着中国感兴趣地区的实体应密切监视类似活动。“，

“chatglm\_gen\_texts”：“本文重点介绍了一个威胁行为者，即 BRONZE PRESIDENT，该威胁行为者使用更新的恶意软件负载针对俄语使用者。该目标很可能被选中来收集该地区的盟友和朋友的情报。Secureworks 的研究人员在一个伪装成俄罗斯文档的可执行文件中检测到了该恶意软件，此举可能与中国因乌克兰战争而改变情报收集要求有关。这个被严重混淆的文件从暂存服务器下载了其他文件，这些文件是恶意软件使用 DLL 搜索顺序劫持来执行 PlugX 负载的典型文件。作者认为，诱饵文档显示和使用 ping 命令来包含延迟可用于欺骗受害者。”

"summary": "Zscaler ThreatLabZ analyzed a malicious Office document campaign delivering both Dridex banking trojan and Kasidet backdoor. The macro inside the Office document downloads the malware payload from URLs hosted on compromised sites. Kasidet installs itself in the appdata folder and uses anti-VM checks to avoid sandboxes. It steals data via memory scraping and browser hooking, sending it to a C2 server. The browser hooking injects code into Firefox, Chrome, and IE to steal sensitive data from these browsers. Network communication uses hardcoded HTTP headers and encrypted C2 commands. Locale checks disable theft from Russian systems. Dridex is also delivered by the same macro document. The shared infrastructure shows criminals reuse delivery mechanisms. Zscaler recommends blocking the identified C2 domains and IOCs listed. The campaign shows blended threats combining banking trojan and backdoor for maximum monetization. ",

"chatglm\_gen\_texts": "The article discusses the malicious Office documents and the Kasidet and Dridex malware. The malicious macro inside the document is obfuscated, and the malware is spread through spear phishing emails as part of a campaign. The malware installs itself into the %APPDATA% folder and uses a mutex name with a hardcoded string. The AntiVM check detects analysis systems during execution, and the malware also checks for sandbox related strings and Vmware, VirtualBox, QEMU and Bochs. The article also describes Kasidet's information stealing capabilities."

信息错误：summary中宏下载恶意软件，chatglm中宏被混淆

信息提取不够全面、不够准确

**整体较差**

“summary”：“Zscaler ThreatLabZ 分析了一个恶意 Office 文档活动，该活动同时传播了 Dridex 银行木马和 Kasidet 后门。Office 文档中的宏从受感染网站上托管的 URL 下载恶意软件负载。Kasidet 将自身安装在 appdata 文件夹中，并使用反 VM 检查来避免沙盒。它通过内存抓取和浏览器挂钩窃取数据，并将其发送到 C2 服务器。浏览器挂钩将代码注入 Firefox、Chrome 和 IE，以从这些浏览器中窃取敏感数据。网络通信使用硬编码的 HTTP 标头和加密的 C2 命令。区域设置检查可禁用来自俄罗斯系统的盗窃。Dridex 也由相同的宏文档传播。共享基础设施显示犯罪分子重复使用交付机制。Zscaler 建议阻止已识别的 C2 域和列出的 IOC。该活动显示了结合银行木马和后门的混合威胁，以实现最大收益。”，

"chatglm\_gen\_texts": "本文讨论了恶意 Office 文档以及 Kasidet 和 Dridex 恶意软件。文档中的恶意宏被混淆，恶意软件作为活动的一部分通过鱼叉式网络钓鱼电子邮件进行传播。恶意软件将自身安装到 %APPDATA% 文件夹中，并使用带有硬编码字符串的互斥名称。AntiVM 检查在执行期间检测分析系统，恶意软件还会检查沙箱相关字符串以及 Vmware、VirtualBox、QEMU 和 Bochs。本文还介绍了 Kasidet 的信息窃取能力。"