俄罗斯APT在东欧攻击中部署新的“Kapeka”后门 | CTF导航

大家好，我是紫队安全研究。建议大家把公众号“紫队安全研究”设为星标，否则可能就无法及时看到啦！因为公众号现在只对常读和星标的公众号才能大图推送。操作方法：先点击上面的“紫队安全研究”，然后点击右上角的【…】,然后点击【设为星标】即可。

摘要：据芬兰网络安全公司WithSecure称，一种名为Kapeka的以前未记录的“灵活”后门已经在至少从2022年中期以来针对东欧，包括爱沙尼亚和乌克兰的网络攻击中“零星”出现。

该发现来自芬兰网络安全公司WithSecure，该公司将这种恶意软件归因于与俄罗斯相关的高级持续性威胁（APT）组织，被追踪为沙虫（又名APT44或海螺暴风雪）。微软将同一恶意软件跟踪名称命名为KnuckleTouch。

安全研究人员Mohammad Kazem Hassan Nejad表示：“该恶意软件是一个灵活的后门，具有作为操作员早期工具包所需的所有功能，并且还能够为受害者提供长期访问权限。”

Kapeka配备了一个分发程序，旨在在感染的主机上启动和执行后门组件，然后将其自身移除。该分发程序还负责为后门设置持久性，可以作为计划任务或自动运行注册表进行设置，具体取决于进程是否具有SYSTEM特权。

微软在其于2024年2月发布的公告中描述Kapeka参与了多次分发勒索软件的活动，并且可以用于执行各种功能，例如窃取凭据和其他数据、进行破坏性攻击，并授予威胁行为者对设备的远程访问权限。

后门是一个使用C++编写的Windows DLL，具有嵌入式的命令和控制（C2）配置，用于与操作者控制的服务器建立联系，并保存有关需要定期轮询服务器以检索命令的频率的信息。

除了伪装成Microsoft Word插件以使其看起来真实外，后门DLL还收集有关受感染主机的信息，并实现多线程以获取传入指令、处理它们，并将执行结果传输到C2服务器。

“后门使用WinHttp 5.1 COM接口（winhttpcom.dll）来实现其网络通信组件，”Nejad解释道。“后门与其C2通信以轮询任务并将指纹信息和任务结果发送回来。后门利用JSON从其C2发送和接收信息。”

该植入物还能够在轮询期间从C2服务器接收新版本以即时更新其C2配置。后门的一些主要功能允许它从磁盘读取和写入文件，启动载荷，执行shell命令，甚至升级和卸载自身。

目前尚不清楚该恶意软件传播的确切方法。但微软指出，分发程序是使用certutil实用程序从被入侵的网站检索的，强调了使用合法的Living-off-the-Land二进制（LOLBin）来组织攻击。

Kapeka与Sandworm的联系体现在与先前披露的家族如GreyEnergy和Prestige等概念和配置的重叠。

“很可能Kapeka曾在导致2022年底部署Prestige勒索软件的入侵中使用，”WithSecure表示。“Kapeka很可能是GreyEnergy的后继者，后者本身很可能是Sandworm的工具库中BlackEnergy的替代品。”

“后门的受害者、偶发出现、隐秘和复杂程度表明APT级别的活动，极有可能是俄罗斯的。”

欢迎喜欢文章的朋友点赞、转发、赞赏，你的每一次鼓励，都是我继续前进的动力。

> 原文始发于微信公众号（紫队安全研究）：俄罗斯APT在东欧攻击中部署新的“Kapeka”后门
