广东省信息安全测评中心

关于境外 APT 组织借新型冠状肺炎疫情对我国发起网络攻击事件的初步分析报告和自检建议

贵单位:

近期，境外 APT 组织趁我国抗击新型冠状病毒疫情之际，冒充国家卫生健康委员会、疫情防疫等相关部门，向我国单位和个人投放与新型冠状肺炎疫情相关的钓鱼邮件。钓鱼邮件附带恶意链接与包含恶意代码的 office 文档附件，利用仿冒页面实现对用户信息的收集，诱导用户执行恶意文档中的宏，向受害用户 windows 主机上植入木马程序，实现远程控制和信息窃取。

经关联分析发现，相似样本至少于 2019 年底开始使用，根据样本特征、攻击手法及资产特点判断，幕后攻击者疑似为印度背景黑客组织“白象”。其仿冒站点域名为“nhc-gov.com”，于 2020 年 1 月 23 日注册，1 月 30 日上线，极其类似我国卫健委官网 “nhc.gov.cn” 。钓鱼邮件附件为新型肺炎话题，伪造散布 “武汉旅行信息收集申请表.xlsm”、“卫生部指令.docx”等疫情相关字眼的 office 文档附件，诱导用户点击下载具备信息窃取、远程控制功能的远控木马。我中心进一步对样本进

行分析，发现受害者经诱导对 office 文档进行相关操作，将被植入远控木马，一旦植入成功，则可造成隐私泄露、数据丢失、人员敏感信息泄露、计算机故障等危害，危及个人乃至企业、政府等单位的网络和信息安全。

现将我中心针对本次攻击事件样本分析情况及排查建议提供贵单位，建议贵单位开展相应梳理排查工作，通过宣贯提高相关人员安全意识，培养良好上网习惯，时刻警惕仿冒网站，针对网络上常见的水坑攻击，钓鱼攻击等事件，警惕来源不明的邮件及文本信息，勿轻易访问未经核实的链接及附件，安装杀毒软件并及时更新病毒库，积极落实网络安全法相关责任要求，采取技术措施和其他必要措施，消除安全隐患。相信在我们的共同努力下，定能守住网络空间的安宁，为我国当前抗击新冠肺炎疫情保驾护航。

*（**注：**“白象”又名 Patchwork、摩诃草，江湖人称正规三军，是具有印度背景的 APT 组织，自 2015 年 12 月开始活跃，长期针对中国军队、政府等部门开展渗透攻击，历来蹭中国新闻热点极其积极，此前曾就军运会为诱饵发起过攻击。）*

附件：APT 攻击样本分析及排查方法和建议

广东省信息安全测评中心

2020 年 2 月 13 日

APT 攻击样本分析及排查方法和建议

一、 样本分析

（一）“卫生部指令.docx”

1. 通过访问链接 http://nhc-gov.com/h_879834932/卫生部指令.docx，将直接下载名为“卫生部指令.docx”的文档；

2. 打开文档如图，未作操作时，文档即发送三个请求；

3. 当受害者填完表中信息后，点击“提交”，word 里的代码将下载“submit_details.exe”文件，此.exe 文件即真正的木马文件；

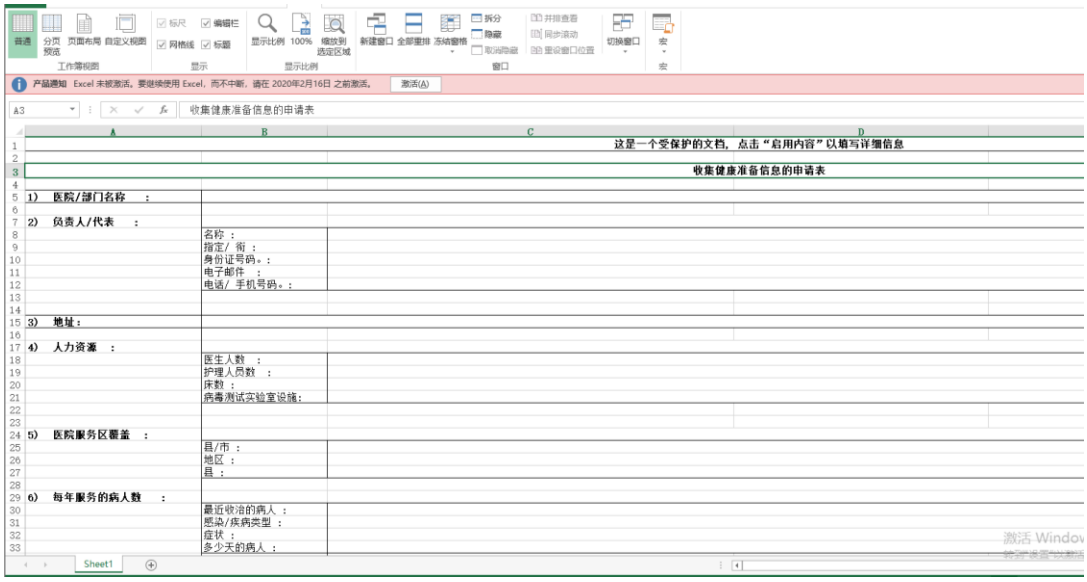
4. 在文档中最后一行使用说明的小字的诱导下，受害者会点击该文件，此时木马被执行。

（注：此翻译拙劣的界面可见多处明显的错别字，可能为翻译器生硬翻译得来，国家单位所发正式文件多经过审核，出现此情况的概率极低，在安全意识教育中可作为非技术人员识别 apt 攻击诱饵文件的一种方法。）

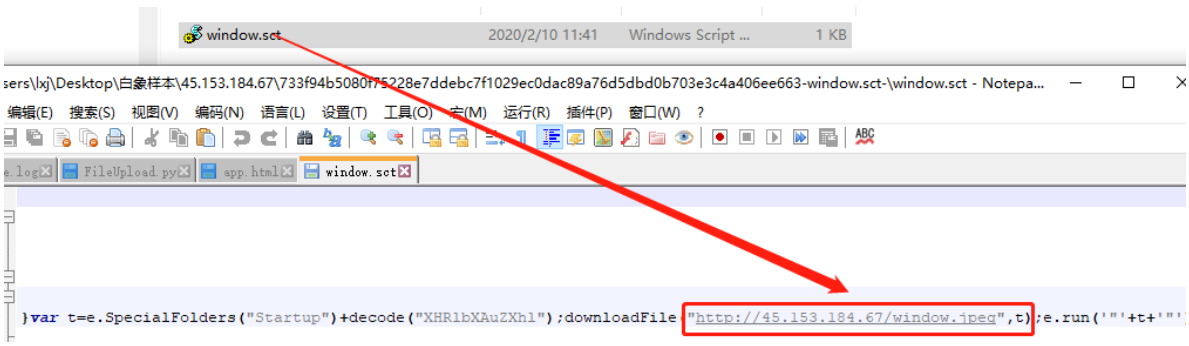
（二）“武汉旅行信息收集申请表.xlsm”

1. 通过访问链接 http://nhc-gov.com/form.html?OZBTg_TFORM，将直接下载名为“武汉旅行信息收集申请表.xlsm”的文档；

2. 打开文档，若宏已启用，则宏代码发送请求到远程服务器下载 window.sct，即使宏未启用，文档中亦有“启用内容”字样诱导目标启用宏；



3. Window.sct 文件用于下载伪装成 jpeg 的 exe 文件，即真正的木马文件，如下图：



二、 排查方法

1. 全盘搜索 submit_details.exe、submit_details.exe、kt_new.png、CnC_Client.pdb，查找可执行文件是否存在，存在则删除。

2. 打开注册表->编辑->查找 输入 submit_details.exe 查找注册表是否有相关值，有则删除。

3. 查找 C:\Windows\Prefetch\路径下是否有类似于 SUBMIT_DETAILS.EXE-xxxxxxxx.pf 预读取文件，有则删除。

4. 全盘查找 window.sct，window.jpeg，CnC_Client.pdb 文件并删除。

5. 查找 C:\Microsoft\msupdate.exe 和 C:\Users\用户名\AppData\Roaming\msupdate.exe 并删除。

6. 打开控制面板，小图标视图下打开“管理工具”->“任务计划程序”，查看是否有如下图所示的启动任务程序 C:\Microsoft\msupdate.exe，有则表示主机已被攻击。删除该计划任务。

三、 安全建议

1. 不要轻易点击和打开来历不明的链接和附件，已打开钓鱼邮件链接或附件的用户，应立即修改相关账号密码并及时联系网络安全技术人员，进行风险排查同时谨慎使用 Office 宏功能。

2. 及时升级系统，安装杀毒软件，并更新病毒库，定期查杀;

3. 强化风险意识，切实加强安全防范，不要通过 QQ、微信等社交媒体打开、传播可疑文档或.EXE 文件。

广东省信息安全测评中心

2020 年 2 月 13 日