



匿名用户

IOC 15

APT 高级可持续攻击 BlueMushroom PowerShell 蓝宝菇

【微步在线报告】BlueMushroom组织最新动向及近年攻击活动揭露



匿名用户

2018-11-21 16:53:43 126

TAG：高级可持续攻击、APT、BlueMushroom、Bfnet、PowerShell、蓝宝菇、亚太

TLP：黄（仅限接受报告的组织内部使用）

日期：2018-11-14

概要

BlueMushroom又名“蓝宝菇”，具备地缘政治背景，自2011年开始活跃，长期针对我国政府、教育、海洋、贸易、军工、科研和金融等重点单位和部门开展持续的网络间谍活动。

本报告内容主要包含BlueMushroom组织分析，其最新活动分析，以及首次公开的该组织近年的攻击活动。部分发现如下：

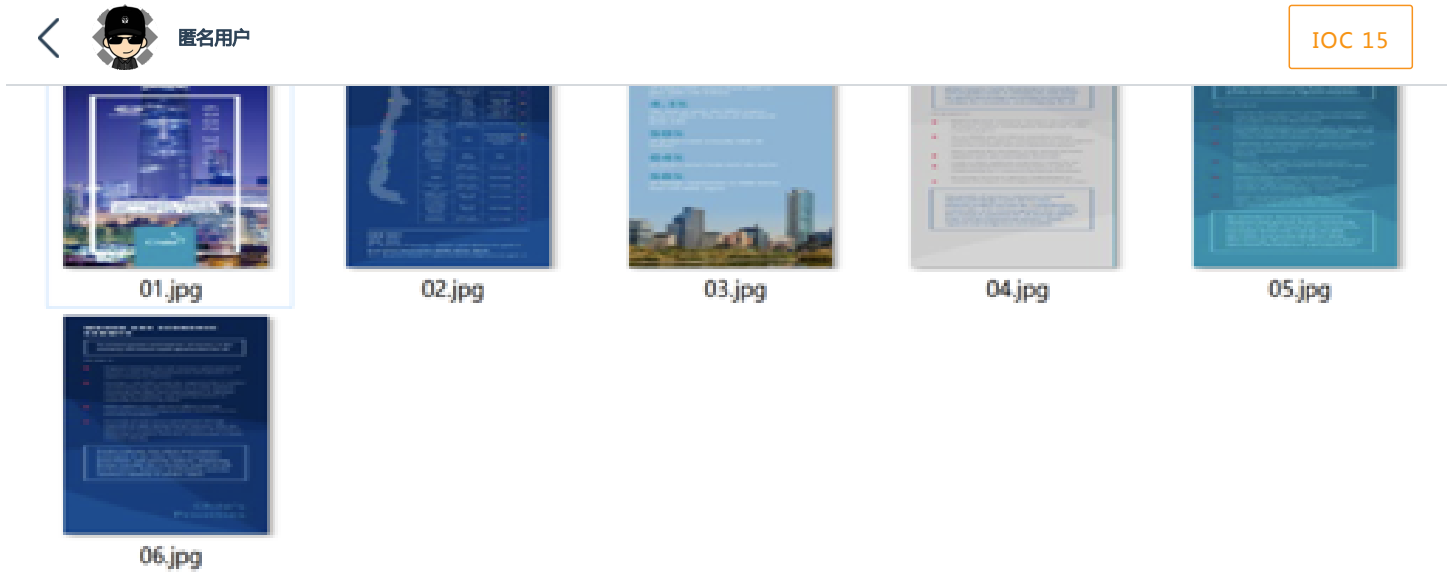
- 根据微步在线威胁情报云，BlueMushroom持续活跃，最近于2018年11月初前后发起过多次攻击，受害者包含APEC等大型会议相关目标。
- BlueMushroom经常使用各种会议、智库和期刊的采访和约稿等作为诱饵，以伪装成文件夹和Word文档的可执行文件，以及包含PowerShell脚本的LNK文件作为木马投递载体。其目的是窃取目标机器上的jpg、txt、eml、doc*、xls*、ppt*、pdf、wps、wpp和et格式文件，和进一步的渗透。
- 2015年至今，BlueMushroom主要使用自己开发的后门进行攻击，该后门的一大特征是删除WPS相关组件程序，以及通过修改LNK文件实现持久化。
- BlueMushroom比较关注亚太政治，北京和上海等地是其重点关注地区。综合分析其攻击目标，木马工具等信息，判断BlueMushroom可能具备亚太地缘政治背景。
- 微步在线通过对相关样本、IP和域名的溯源分析，共提取11条相关IOC，可用于威胁情报检测。微步在线的威胁情报平台（TIP）、威胁情报订阅、API等均已支持此次攻击事件和团伙的检测。

详情

微步在线长期跟踪全球150多个黑客组织，其中包含多个长期针对我国进行攻击的APT组织。近期，微步在线监测到具备地缘政治背景的APT组织BlueMushroom针对我国的多起攻击活动。在具体的攻击（多为鱼叉式网络钓鱼）中，BlueMushroom一般会制作与目标高度相关的诱饵，利用伪装成文件夹和Word文档的可执行文件，以及包含PowerShell脚本的LNK文件作为木马投递载体。

最新活动

2018年10月底至11月初，微步在线监测到BlueMushroom针对我国发起了多次定向攻击，其中受害者包含APEC等大型会议相关目标。以针对APEC相关目标的攻击为例，攻击者使用伪装为文件夹的可执行文件作为木马投递载体，运行后会释放内容为Chile APEC 2019日程相关的图片作为诱饵，以及多个DLL和配置文件。



图：诱饵文件夹内容

综合分析木马编译时间，诱饵文件创建修改时间，以及首次发现时间等信息，判断此次攻击发生在10月底，潜在被攻击目标为出席APEC会议的政府领导和工商企业人士。更进一步分析发现，近几年，BlueMushroom基本每年都会在10月底以APEC为诱饵发起一波攻击，这可能是由于每年APEC领导人非正式会议将于11月中旬举行。下图为2016年10月底 APEC相关攻击活动中使用的诱饵。

匿名用户

IOC 15

TENTATIVE PROGRAMME

APEC 2017 INFORMAL SENIOR OFFICIALS' MEETING (ISOM)

SYMPOSIUM ON APEC 2017 PRIORITIES

National Convention Center, Ha Noi, Viet Nam

08 - 09 December 2016

Thursday

08 December

SYMPOSIUM ON APEC 2017 PRIORITIES

09:00 – 09:30

Opening Session

09:30 – 09:45

Family Photo

09:45 – 10:45

Session I

Creating New Dynamism, Fostering a Shared Future of the Asia - Pacific

10:45 – 12:00

Session II

Promoting Sustainable, Innovative and Inclusive Growth

12:00 – 13:30

Lunch

13:30 – 14:45

Session III

Deepening Regional Economic Integration: The role of APEC

15:00 – 16:00

Session IV

MSMEs' Competitiveness and Innovation in the Digital Age

16:00 – 17:00

Session V

Enhancing Food Security and Sustainable Agriculture in Response to Climate Change

17:00 – 17:20

Closing Session (the participants then proceed to the Marriot Hotel nearby for the Dialogue)

17:45 – 19:00

Dialogue between APEC and Business Community on APEC Viet Nam 2017

19:00 – 21:00

Welcome Dinner

Friday

09 December

APEC 2017 INFORMAL SENIOR OFFICIALS' MEETING (ISOM)

09:00 – 09:15

Opening Remarks

09:15 – 10:25

Session I

Implementing the Lima Mandate

10:25 – 10:30

Family Photo

10:45 – 12:00

Session II

Theme and Priority Areas for 2017

图：2016年APEC相关攻击中使用的诱饵

近年活动

BlueMushroom善于利用社工手法进行钓鱼攻击，制作的诱饵也与被攻击目标高度相关。在历年的活动中，BlueMushroom多次利用各种智库和政治类期刊的“约稿”和“采访”，以及各种会议作为诱饵进行定向攻

下表为2015年以来微步在线独家发现的BlueMushroom组织的部分攻击活动。

时间节点	
2015年初	以“两会会议案”为诱饵，发起钓鱼攻击。
2016年6月	以“京卡-互助服务卡”为诱饵，疑似针对北京理工大学教职工发起定向攻击。
2016年10月	以APEC议程为诱饵，针对APEC与会者发起定向攻击。
2017年7月	以“一带一路”对策建议为诱饵，定向攻击国内顶级智库相关目标。
2017年8月	以“《太平洋学报》征稿启事”，“运筹优化软件GAMS及CGE模型核心技术与应用培训”等为诱饵，针对研
2017年9月	以北京大学国际战略研究院院长王缉思批注的人大国发院针对“一带一路”的对策建议为诱饵，定向攻击国内
2018年4月	以上海“2017智慧政务与信息技术研讨会”为诱饵发起定向攻击，此次攻击中使用了64位的木马。
2018年10-11月	针对某大型会议相关目标发起定向攻击。
	以APEC为诱饵，针对APEC与会者发起定向攻击；
	以《国际商报》采访作为诱饵，针对某大型会议与会者发起钓鱼攻击。

示例一：

在2016年的一次攻击中，攻击者以“京卡-互助服务卡”为诱饵，疑似针对北京理工大学教职工发起定向攻击。分析诱饵文档的元数据，发现文档为“刘明奇”创建，此人系中国教育工会北京理工大学委员会常务副主席，在2016年确实有从事相关工作（推动本校工会系统服务平台建设）。推测此文档应是攻击者窃取而来。京卡·互助服务卡原名“职工互助服务卡”，是北京推出的一种维护职工权益的智能卡，持卡人可享受免费保险、优惠逛公园、看电影等12项服务。

包含诱饵的木马文件图标：



诱饵文档内容：

京卡·互助服务卡简介

一、北京工会京卡·互助服务卡介绍

京卡·互助服务卡是北京银行与北京市总工会首次合作联合发行的认同卡，卡片性质为借记卡，该卡作为北京市总工会会员的唯一身份识别标志，具备北京银行现有京卡借记卡除开立副卡以外的全部金融功能，并在此基础上实现互助保险金发放，同时持卡人享有北京市总工会为其会员所提供的如法律咨询、职业培训以及特定商户消费打折等增值服务。

(一)、产品金融功能

图：京卡-互助服务卡

示例二：

2017年8月前后，攻击者以“《太平洋学报》征稿启事”为诱饵（内容是从《太平洋学报》网站复制），针对研究海洋、社会科学和国际关系的专家学者发起定向攻击。《太平洋学报》关注太平洋区域政治、经济、海洋、文化以及国际关系。相关木马伪装成文件夹，双击后会释放并打开，其中包含两个诱饵文件。

文件图标	诱饵文件夹	诱饵文件
 《太平洋学报》征稿启事.exe	 《太平洋学报》征稿启事	 《太平洋学报》2017年重点选题方向.docx  《太平洋学报》征稿启事.docx

诱饵文件内容：

根据全国海洋工作会议精神,综合编委通讯会议征集的重点选题方向,经 2017 年 2 月 24 日第五届编委会第二次会议审议通过,确定《太平洋学报》2017 年重点选题方向如下:

1. 海洋强国建设研究(包括海权理论、海洋强国思想等)。
2. 推进 21 世纪海上丝绸之路建设与风险防范研究。
3. “蓝色经济”、陆海统筹与可持续发展研究。
4. 亚太地区安全与合作研究。
5. 海洋生态文明建设研究。
6. 大国海洋战略研究、周边国家和地区海洋战略研究。
7. 极地、大洋等领域全球治理研究。
8. 亚太海洋争端等热点问题深入研究。
9. 日本核事故对海洋核污染的研究。

欢迎广大研究者踊跃投稿。

《太平洋学报》第五届编委会第二次会议召开



图：《太平洋学报》2017年重点选题方向

《太平洋学报》创刊于1993年，由中国太平洋学会主办，著名经济学家于光远先生曾长期担任主编，是我国海洋领域社科类期刊，先后入选全国中文核心期刊、中文人文社会科学引文数据库来源期刊、中国人文社会科学核心期刊、中国人民大学复印报刊资料重要转载来源期刊、中国政法类核心期刊。创刊二十年来，一直秉承“立足中国海，探索太平洋，关注国家发展，理论世界大局”的办刊宗旨，凝聚了一大批学术思路活跃、潜心研究社会科学和国际关系问题的专家学者，刊发了大量高水平的学术论文，成为热心想太平洋区域学术问题的各界人士的良好益友。

本刊常设栏目：政治与法律、国际关系、经济与社会、发展与战略、历史与文化。根据国内外形势需要，今后本刊将更注重理论研究深入的论文，仍以国际政治为主，并全面向海洋方面的内容倾斜，努力在海洋人文社会科学研究领域，打造独具海洋特色的期刊。为了进一步提高办刊质量，我们诚挚邀请国内外潜心研究太平洋区域国际问题的专家学者，踊跃在本刊这个权威平台上发表文章、交流观点。现将征稿简则通报如下：


一、关于权利的申明

图：《太平洋学报》征稿启事

示例三：

2017年8月中上旬，以中国管理科学研究院人才战略研究所举办的“运筹优化软件GAMS及CGE模型核心技术与应用”培训为诱饵，针对金融和经济等企事业单位技术骨干、科研院所研究人员以及高校教职工等目标发起定向攻击。

相关木马亦伪装成文件夹，双击后会释放并打开，其中包含两个诱饵文件。

文件图标	诱饵文件夹	诱饵文件
		<div> 报名回执表.docx</div> <div> 运筹优化软件---北京.doc</div>

诱饵文件内容：



匿名用户

IOC 15

中国管理科学研究院人才战略研究所

人才所[2017]第(28)号



关于举办“运筹优化软件GAMS及CGE模型核心技术与应用”培训通知

各企事业单位：

通用代数建模系统(GAMS)是特别为建模线性、非线性和混合整数最优化问题而设计的。GAMS支持一系列模型：LP 线性规划，MIP 混合整数规划，NLP 非线性规划，MCP 混合互补问题，MPEC 带方程式约束的数学规划，CNS 受约束的非线性系统，DNLP 带非连续导数的非线性规划，MINLP 混合整数非线性规划，QCP 二次约束规划以及 MIQCP 混合整数二次约束规划。为了推进国内运筹学的教学和科研工作，促进国内经济学研究和应用的发展，提升相关科技工作者的技术水平，中国管理科学研究院人才战略研究所特举办“运筹优化GAMS及CGE模型核心技术与应用”培训班，由北京汇文育才教育科技有限公司承办，具体事宜如下。

【培训目标】本次培训采取深入浅出的方法，先以简单的案例引入GAMS的基本原理。随后重点讲解多种常用单元的功能和特性，以及有GAMS和可计算一般均衡(CGE)模型的实用技术和处理方法，紧密结合应用实例，针对工作中存在的疑难问题进行分析讲解和专题讨论，有效提升学员解决复杂问题的能力。

【培训对象】各省市、自治区从事金融、运筹学、管理科学、计算机、数学、经济学、物流、工业工程及多与仓储等行业相关的企事业单位技术骨干、科研院所研究人员和大专院校相关专业教学人员及在校研究生、硕士、博士等相关人员，以及GAMS软件和可计算一般均衡(CGE)模型的广大爱好者。

图：运筹优化软件---北京


联系人			
联系电话		传真/Email	
详细地址			
参加培训人员详细表			
姓名	性别	职务	手机/联系电话/Email
"	"	"	"
"	"	"	"
"	"	"	"
"	"	"	"
"	"	"	"
"	"	"	"
缴费方式:		<input type="checkbox"/> 银行转账。 单位名称: 北京汇文育才教育科技有限公司。 开户行: 中国建设银行股份有限公司北京市房山支行。 账号: 11050169520000001219	<input type="checkbox"/> 会场交费 (可刷卡)。
发票开具	公司名称/发票抬头		
	开票项目	<input type="checkbox"/> 培训费 <input type="checkbox"/> 会议费 <input type="checkbox"/> 会务费 <input type="checkbox"/> 资料费	
另交费项目: 是否需要住宿: <input type="checkbox"/> 是 <input type="checkbox"/> 否 () 单间 () 标间		参会学员签名: 年 月 日	

图：报名回执表

样本分析

根据公开情报，在早期（2011-2014）的活动中，BlueMushroom主要使用公开的Poison Ivy的木马进行攻击，从2014年末至今，较多使用自己开发的Bfnet后门。Bfnet属DLL后门，主要通过伪装成Word文档、文件夹以及其他方式进行投递，其显著特点是运行后会删除WPS相关程序和修改LNK文件实现持久化。

<

匿名用户

IOC 15

多引擎检测

威胁情报IOC

行为签名

情报判定系统

基本信息

静态信息

执行流程

进程详情

运行截图

网络行为

释放文件

⚠ 经检测该文件为恶意


文件名称: 0f8ec57dada552766dcdf43cb2a827133bbbfba242c925d744f2698a3ebc8ff9

SHA256: 0f8ec57dada552766dcdf43cb2a827133bbbfba242c925d744f2698a3ebc8ff9

运行环境: win7_sp1_enx86_office2013

提交时间: 2018-11-13 17:27:19

样本标签: PE32 语言chinese Trojan GenKryptik

113分

重新分析

报告

PCAP

样本

收藏

📌 多引擎检出率 3 / 25

API 接口 | API 上传

反病毒软件	检测结果
ESET	🔴 a variant of Win32/GenKryptik.CPTH trojan
Baidu-China	🔴 Win32.Trojan.WisdomEyes.151026.9950.9988
Avast	🔴 Win32:Malware-gen
江民 (JiangMin)	🟢 非恶意

最新样本分析

下面以Chile_Apec2019.exe为例进行分析。

1.该样本基本信息如下：

文件类型	PE32 executable (GUI) Intel 80386, for MS Windows
文件大小	6150922
文件名	Chile_Apec2019.exe
SHA256	0f8ec57dada552766dcdf43cb2a827133bbbfba242c925d744f2698a3ebc8ff9
SHA1	55d1cf05904c16f5d813dd9f708bd1ab6f353324
MD5	41344a2854d4cc46d8ec36dd9c8caa2d

2.该样本的整体执行流程如下：

https://m.threatbook.cn/detail/909?from=groupmessage&isappinstalled=0

10/17



3.样本执行后会释放出3个DLL文件、1个配置文件和6张诱饵图片。

文件名	作用
dx9_9.bak	伪后门DLL，会将导出函数的调用转移到dx9_9.bak上
dx9_9_bak	实际的后门DLL
dx13_32.dat	配置文件
op.bak	用于启动资源管理器展示诱饵图片

4.dx9_9.bak是该样本的主要后门模块，提供了多个导出函数，如下表所示。

导出函数名	功能
DxEntry	创建互斥量，解密配置文件，并触发后门程序
DxInstall	生成批处理文件nv32_update.bat并执行
DxUninstall	
DxCanUnload	生成批处理文件nv32_update.bat
DxSetClassObject	感染符合条件的快捷方式文件，以实现驻留
DxUnsetClassObject	无实际用处
DxCopyClassObject	将参数1指定的文件复制到参数2指定的路径
DxMoveClassObject	将参数1指定的文件移动到参数2指定的路径
DxMoveClassObjectEx	将参数1指定的文件复制到参数3指定的路径
DxDelClassObject	将参数1指定的文件拷贝到%TEMP%下
DxServiceBegin	调用cmd.exe /c执行参数指定的命令
DxServiceBeginEx	

1) 字符串解密算法。

样本中字符串的解密算法是一个简单的替换过程。对ANSI字符串和Unicode字符串使用了不同的函数进行处理，但算法的思路相同，做法为：

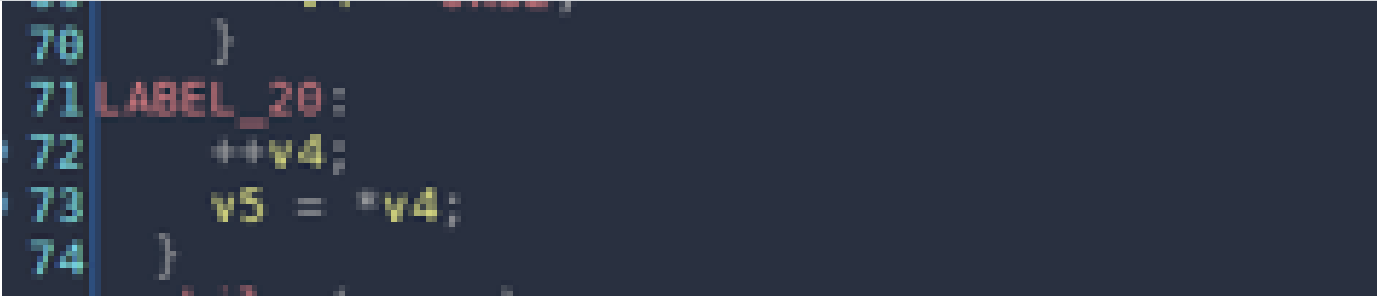
- 对于大写字母，如码点值大于等于0x4A，则将码点值-9，否则将码点值+17；
- 对于小写字母，如码点值大于等于0x6A，则将码点值-9，否则将码点值+17；
- 对于数字，如码点值大于等于0x39，则将码点值-9，否则将码点值+1；
- 将空格（0x20）和大于号（0x3E）对调；
- 以竖线（0x7C）作为字符串结束符。



匿名用户

IOC 15

```
30
31 {
32     if ( iswupper(v5) )
33     {
34         v6 = *v4 - 9;
35         v7 = *v4 + 0x11;
36         v9 = __OFSUB__(v6, 0x41);
37         v8 = *v4 - 0x4A < 0;
38 LABEL_13:
39         v12 = v7;
40         if ( !(v8 ^ v9) )
41             v12 = v6;
42         *v4 = v12;
43         goto LABEL_20;
44     }
45     if ( iswlower(*v4) )
46     {
47         v6 = *v4 - 9;
48         v7 = *v4 + 0x11;
49         v9 = __OFSUB__(v6, 0x61);
50         v8 = *v4 - 0x6A < 0;
51         goto LABEL_13;
52     }
53     v10 = iswdigit(*v4);
54     v11 = *v4;
55     if ( v10 )
56     {
57         v6 = v11 - 9;
58         v7 = *v4 + 1;
59         v9 = __OFSUB__(v6, 0x30);
60         v8 = v6 - 0x30 < 0;
61         goto LABEL_13;
62     }
63     if ( (_WORD)v11 == 0x3E )
64     {
65         *v4 = 0x20;
66     }
67     else if ( (WORD)v11 == 0x20 )
```



2) 一些与样本功能无关的API调用。

样本在一些函数中加入了无关的API调用，如在DxEntry导出函数中加入了GetCurrentProcess()、GetConsoleWindow()和GetCapture()调用。

3) 生成批处理文件。

a) 样本会收集下列目录中的快捷方式文件名。

%USERPROFILE%\Desktop
%USERPROFILE%\桌面
%APPDATA%\Microsoft\Internet Explorer\Quick Launch
%APPDATA%\Microsoft\Windows\Start Menu
%ALLUSERSPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu
%USERPROFILE%\「開始」功能表
%ALLUSERSPROFILE%\「開始」功能表
%USERPROFILE%\「开始」菜单
%ALLUSERSPROFILE%\「开始」菜单

b) 并过滤出带有下列关键词的字符串。

Startup
啟動
启动
Internet Explorer
Chrome
Firefox
Opera
Safari
Browser
浏览器
瀏覽器
360
我的手机
Windows Explorer
腾讯QQ
微信

c) 最后样本会向批处理文件中写入调用DxSetClassObject感染快捷方式的命令，在生成批处理文件之后，样本通过CreateProcessW调用cmd.exe来启动批处理文件。

4) 感染快捷方式文件。

样本首先会通过CoCreateInstance创建一个IShellLinkW对象，然后拼接多个命令字符串，最后通过IShellLinkW对象提供的接口将这些内容写入快捷方式。

[illegible]

5) 解密配置文件。

解密前的配置文件格式如下所示。

字段	大小
CONFIG-KEY的长度k1	4字节
CONFIG-KEY	k1字节
C2数据的长度k2	4字节
C2数据	k2 - 1字节
定时器触发时间（秒）	4字节
是否驻留	4字节

样本中硬编码了另一个8字节的KEY (0x37 0x43 0x18 0x95 0x47 0x69 0x13 0x68) , 该KEY与CONFIG-KEY做循环异或后得到的结果才用于解密过程。

解密后的配置文件数据部分如下图和下表所示，C2数据之间使用换行符\n（0x0A）进行分割。

[illegible]

C2列表	142.93.65.5282.196.6.100104.248.189.199
定时器触发间隔	0x00000020 = 32秒
是否驻留	0x00000001 = True

6) 后门功能。

样本通过一个定时器 (SetWaitableTimer) 来定期触发, 时间间隔由配置文件指定 (0x20 = 32秒)。随后定时器会尝试逐个回连C2列表中的服务器, 并将"HELLO "和密钥字节流拼接, 作为握手包发送。如成功建立连接, 则C2服务器会回复"!HELLO"以及多个后续命令, 相关命令及执行的操作如下:

命令	操作
!GETINFO	无
!PERSIST	执行DxUninstall导出函数
!PERSIST_UN	执行DxInstall导出函数
!SETIP	修改C2服务器的地址，并写入配置文件
!SETID	设定回连的ID信息
!INTERVAL	修改定时器的触发时间（最大7200秒，最小30秒），并写入配置文件
!DOWNLOAD	下载文件（到当前目录）
!PUT	上传文件
!GET	下载文件
!PLUGIN_RUNDLL	调用DxEntry导出函数
!PLUGIN_RUN	加载DLL文件并调用DLL文件中的DxEntry导出函数
!PLUGIN_WRITE	调用DLL文件中的DxPutClassObject导出函数
!PLUGIN_STOP	调用DLL文件中的DxUnregisterServer导出函数
!EXIT	停止定时器
!RESTART	调用DxEntry导出函数 参数为DxRegisterServer
!RESTART_NEW	
!UNINSTALL	卸除自身模块
!CAB	使用makecab程序对文件进行打包
!ZIP	无
!ZIPLIST	收集在特定时间之后的doc/docx/ppt/pptx/xls/xlsx/txt类型的文件，并存放在%DIRNAME%.zip.lst中



2018年上半年捕获到的BlueMushroom样本有使用PowerShell脚本取代Bfnet后门核心功能的趋势，但在最近捕获的样本中又恢复了原本的做法，即在DLL文件中实现后门功能。

[illegible]

为方便进行跟踪，微步在线将该组织称为BlueMushroom。根据BlueMushroom在攻击中使用的木马工具，网络资产和攻击手法等信息，确定该组织也即“蓝宝菇”组织。

1. 发现该组织在发起攻击之前一般会经过一段时间的精心准备，有时准备时间长达两个月。
2. 该组织攻击手法和私有木马这几年变化均不大，但也在寻求着改变。自活跃以来，该组织主要使用伪装Word文档和文件夹等的PE文件作为载体投递后门木马。在2018年的几次攻击中，该组织开始尝试将部分诸如窃取文档等核心功能转移到使用PowerShell脚本实现，其策略也更倾向于LotL策略，这也是当前APT攻击的一大趋势。
3. 该组织私有木马包含繁体字符，某PowerShell脚本会判断系统语言是否为日语、繁体、简体和英语，最新的某攻击样本中隐藏的用于嘲讽安全研究者的图片也包含繁体字符。此外，一些钓鱼邮件和诱饵文件的内容也说明攻击者的汉语水平较高，再结合该组织攻击目标也多与亚太地缘政治有关等信息，推测该组织可能具备亚太地缘政治背景。

```
ExpandEnvironmentStringsW(L"%APPDATA%\Microsoft\Internet Explorer\Quick Launch", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%USERPROFILE%\Links", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%APPDATA%\Microsoft\Windows\Start Menu", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%ALLUSERSPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%USERPROFILE%\「開始」功能表", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%ALLUSERSPROFILE%\「開始」功能表", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%USERPROFILE%\「開始」菜單", v3, 0x800u);
SearchForSpecifiedFiles(v1, v3, L".lnk");
ExpandEnvironmentStringsW(L"%ALLUSERSPROFILE%\「開始」菜單", v3, 0x800u);
return SearchForSpecifiedFiles(v1, v3, L".lnk");
```

图：历史样本中包含的繁体字符

```
42 $v = [System.Text.Encoding]::Default.EncodingName;
43 if ($v.EndsWith('gbk')) { $p = '5' }elseif ($v.EndsWith('f-16')) { $p = '4' }elseif ($v.EndsWith('utf8')) { $p = '3' }elseif (
44 $f = $a.split(";");
```






图：PowerShell中判断系统默认编码



图：某攻击样本释放的Thumbs.db中的缩略图包含繁体字

威胁指标 (IOC)

IP	端口	域名	样本	标签
82.196.6.100	0	8	0	5
104.248.189.199	1	0	1	5
142.93.65.52	1	1	2	4
Hash	检测结果	样本	标签	
065dd1022d026133...	0/25	0	3	
0f8ec57dada552766...	3/25	0	3	
36e82fc0b160071f4...	8/25	0	3	
53764e5ba1b9972b...	0/25	0	3	
6c242273d5ccd56e1...	11/25	0	3	

 www.psc.org.cn/qk.php
 www.pacificjournal.com.cn/CN/news/news262.shtml
 www.pacificjournal.com.cn/CN/news/news260.shtml
 www.zgyrczl.org/index.php?m=content&c=index&a=show&catid=262&id=5650
 klsd_afj.zzxu.com

0 赞

评论



 已有0条评论，快来说说你想法...

已经到底了，没有更多内容了