蓝色魔眼（APT-C-41）组织首次针对我国重要机构定向攻击活动披露

By 高级威胁研究院

Archived: 2026-04-05 16:12:35 UTC

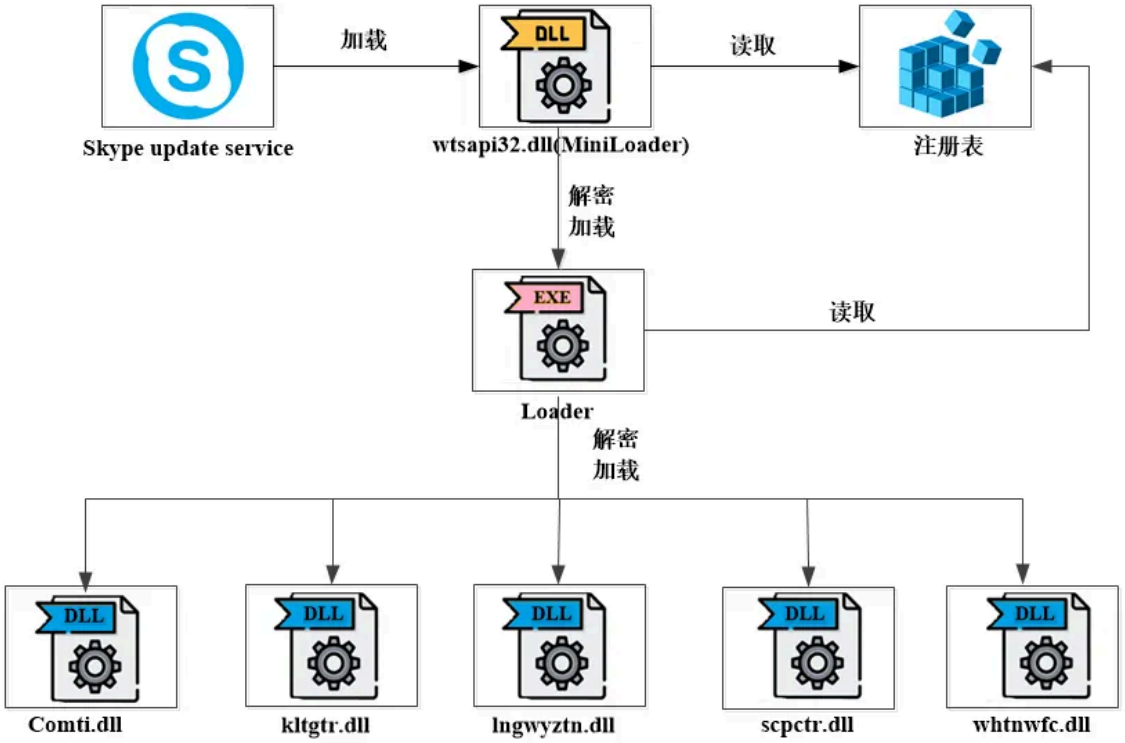
蓝色魔眼（APT-C-41），又被称为Promethium、StrongPity，该APT组织最早的攻击活动可以追溯到2012年。该组织主要针对意大利、土耳其、比利时、叙利亚、欧洲等地区和国家进行攻击活动。360安全大脑监测到该组织在2020年1月首次针对中国进行了攻击活动，并捕获到了该组织最新V4版本的攻击组件。经过360高级威胁研究院的深入分析研判，此次攻击的针对性极强，是该组织罕见地针对我国相关重要机构发起的首起定向攻击行动。由于是首次捕获和披露该组织对我国的攻击，我们为其分配了新的编号APT-C-41，并根据该组织活跃地区的文化特色将其命名为“蓝色魔眼”。

2016年10月，卡巴斯基发布了《on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users》，披露了该组织针对意大利和比利时地区的APT攻击活动。同年12月14号，微软的安全情报报告中披露了该组织Promethium行动和Neodymium行动。Bitdefender研究人员在今年6月披露了该组织最新针对土耳其和叙利亚的攻击活动，发现该组织对库尔德人社区尤其感兴趣，从样本时间戳分析发现恰好与土耳其发动了对叙利亚东北部的军事攻势“和平之泉”行动（Operation PeaceSpring）相吻合。

从历史攻击活动看，蓝色魔眼组织的攻击战备资源充足，具备0day漏洞作战能力，拥有一套复杂的模块化攻击武器库，并长期持续迭代更新。该组织的基础网络资源丰富，足以在每次攻击活动中有多套备用资源以便迅速更新持续对抗。早期该组织曾使用过0day漏洞发起攻击活动。而后被披露针对目标用户进行水坑攻击，伪装成用户常用合法软件或仿冒相关应用官方网站，从早期伪装WinRAR、TrueCrypt、Opera浏览器等软件，扩展到伪装TeamViewer、WhatsApp等应用软件。同时该组织还曾被发现一些ISP级别的网络劫持攻击活动迹象。该组织的攻击组件从2016年至今在不断进行升级改进，基于360安全大脑遥测数据来看，该组织的攻击组件至少已经有4次较大的更新迭代，今年活跃的主要是V3和V4两个版本。

后门攻击流程

该组织在攻破主机后，会在失陷主机上部署最新V4版本的后门程序，在内存中加载各种功能插件进行攻击活动。该后门程序的执行流程如下图所示:



具体的执行流程：

1.Skype的升级服务程序被持久驻留执行

2.Skype的升级程序加载同路径下的wtsapi32.dll执行

3.wtsapi32.dll读取注册表HKCR\Software\Appdatalow\Software\Skype下的数据，并解密执行Loader组件。

4.Loader组件读取注册表HKCR\Software\Appdatalow\Software\Skype下数据，解密执行其他的攻击插件。

各模块对应功能如下表所示:

样本	**功能**
Skype update serivce	Skype的升级服务程序
wtsapi32.dll(Miniloader)	Loader加载程序
Loader	插件加载程序

comti.dll	通信模块
lngwyztn.dll	磁盘文件信息记录模块
scpctr.dll	屏幕截图模块
whtnwfc.dll	磁盘文件内容记录模块
kltgtr.dll	键盘记录模块

攻击组件分析

1

Skype Update Service

由于原版的Skype升级服务程序在加载wtsapi32.dll动态库时未对其合法性进行验证，被该组织作为DLL恶意荷载的白利用加载程序。

项	**信息**
编译时间	2014-12-11 18:20:55
公司名称	SkypeTechnologies
文件描述	SkypeUpdater Service

2

初始加载器 - Miniloader

该组件的模块名为MiniLoader，组件通过Skype更新服务程序的加载执行，主要功能是通过解密注册表HKCU\Software\AppDataLow\Software\Skype数据，获得插件模块并加载功能插件Loader。MiniLoader文件信息如下。

项	**信息**
样本名	wtsapi32.dll

路径	%appdata%\{rand10()}\wtsapi32.dll
编译时间	2020年01月08日

在MiniLoader在首次被加载时，在对本身的文件格式进行校验之后，修改入口点代码，将功能函数地址赋值给ebx,然后跳转ebx，这样当发生如DLL卸载等事件时可以执行功能函数。

功能函数主要实现在注册表HKCU\Software\AppDataLow\Software\Skype下获取加密的数据

在获取Payload数据后，程序会使用rc4加密算法解密还原Payload

最终查找Payload即第一个插件(Loader)入口点，并通过CreateThread函数在内存中执行荷载。

3
插件 - Loader

项	**信息**
编译时间	2020-01-08 19:27:20
类型	32位exe

Loader为EXE文件类型，是负责解密加载其他功能插件的核心组件。在其main函数中，首先加载序号为大于2的功能插件，然后加载序号为2的通信功能插件。

其通过递增插件序号，加载其他功能的插件执行。

最终获得插件的导出函数Start，通过CreateThread调用在内存中执行。

4
插件 - 通信后门

通信组件模块名为Comti.dll，主要负责命令控制和数据传输，利用Winnet API上传其他插件模块所产生的数据，如屏幕截图，键盘记录等信息，以及负责植入后续攻击组件。攻击者会使用后门版本号加C盘VolumeSerialNumber计算设备唯一标识符，用以标记中招机器。

项	信息
编译时间	2020-03-05 19:07:10
类型	32位dll
导出模块名	Comti.dll

程序使用后门版本号加VolumeSerialNumber标记中招机器。

对屏幕截图，磁盘记录等插件产生的文件进行上传操作，上传之后删除数据

获取C&C下发的控制命令数据，进行植入攻击组件动作或删除攻击组件动作

攻击组件的植入有两种方式：

1.植入到注册表中，通过Loader调用CreateThread函数在内存中执行，为后门默认的插件执行方式。

2.植入到磁盘中，通过调用CreateProcess直接执行，执行方式是由C&C命令控制发起。

5
插件 - 磁盘文件信息搜集

该组件模块名为lngwyztn.dll，主要负责收集中招计算机文件信息。

项	信息

编译时间	2018-09-11 23:32:39
类型	32位dll
导出模块名	lngwyztn.dll

该组件会遍历磁盘搜集文件信息

搜集的文件信息包括路径信息和文件大小，搜集到的信息异或加密，最终以压缩包形式保存

6
插件 - 屏幕监控

该组件模块名为scpctr.dll，主要负责收集中招计算机指定屏幕截图信息。截屏的图片以bmp格式打包到zip中，再将zip数据加密为*.tbl的文件保存。

项	**信息**
编译时间	2019-03-26 21:37:38
类型	32位dll
导出模块名	scpctr.dll

调用系统API实现截屏，图片类型是bmp格式

将截屏的bmp数据添加到zip压缩包

加密zip数据，以inf_loc_sc_*.tbl等文件名保存。

7
插件 - 键盘监控

该组件模块名为kltgtr.dll，主要负责收集中招用户计算机的键盘记录信息。

项	信息
编译时间	2019-03-26 21:37:06
类型	32位dll
导出模块名	kltgtr.dll

功能为键盘记录，并写入文件隐藏，生成的键盘记录日志名根据格式化字符串而变化。例如：“inf_loc_ky_%u_%02d%02d%02d%02d%02d_.tbl”，其中%u通过GetVolumeInformation获取的磁盘信息生成， %02d%02d%02d%02d%02d是记录时间。

8
插件 - 磁盘文件窃取

该组件模块名为whtnwfc.dll，主要负责收集中招计算机指定文件的文件内容。

项	信息
编译时间	2018-09-13 21:58:54
类型	32位dll

导出模块名	whtnwfc.dll

文件内容记录组件尝试读取rdctv.tmp，rdctv.tmp2或rdctv.cab的加密配置文件，对以上文件内容进行解密后获取想要窃取的文件信息。

创建inf_loc_fiz_.tmp，将想要获取的文件使用zip库压缩至inf_loc_fiz_.tmp文件。

读取inf_loc_fiz_.tmp的文件内容，使用0x800个字节为一组进行加密，加密压缩后的数据后，将数据写入inf_loc_o_fi_”VolumeSerialNumber”_0为文件名的文件中，并将加密次数写入rdctv.ind文件中。

对抗手法

1

填充无用数据

MiniLoader样本中填充大量的无用数据使其膨胀为超大文件以实现规避安全软件的静态扫描。

2

导出函数参数

功能插件DLL全部功能是通过导出函数start实现的，接受的参数a1只是用来做判断，以实现反自动化系统分析。

关联分析

基于本次攻击行动中V4版本和StrongPity早期版本进行关联比较，主要从解密算法、代码结构、通信数据格式等关联分析。

1

解密算法关联

本次攻击活动样本解密算法和早期样本的模式类似

本次攻击活动样本解密算法

早期样本解密算法

2
代码结构关联
本次攻击活动样本和早期样本的代码结构相似。如下图，左图为本次攻击活动中样本获取WinnetApi函数代码结构，右图为公开样本的代码结构。

3
通信数据格式关联
本次攻击活动样本和早期样本都会使用相同FromData格式的HTTP请求上传数据。如下图，本次样本和公开样本具有相同参数的FromData字段。

本次样本中上传文件的FromData格式

公开样本上传文件的FromData格式

4
导出函数关联
本次攻击活动样本和早期样本的导出函数结构相似

附录 IOC

MD5:

d54de33412fc967fef50899ec62a41c7

4477ab2bc31cf3a2e8535967489cdc4b

5963ae6ae5510c5a04b02e18a11d5c1b

9a10108321d2aa0edaa00ebaecb6bb90

9d212f33a37df2c550a981b10c295788

adcdd7cde9e6d2e05bbf9011d50999cf

d3a7a52f1b6e8c91a16f1ed0ab360e3a

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

更多详细情报请联系 360高级威胁研究院

(邮箱：ata@360.cn)
