APT28携小众压缩包诱饵对北约、中亚目标的定向攻击分析

By 高级威胁研究院

Archived: 2026-04-05 13:43:13 UTC

APT-C-20,又被称为（APT28, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, STIONTIUM等），是一个具有军方情报机构背景的APT组织。该组织最早的攻击活动可以追溯到2004年至2007年之间，主要攻击目标为北美、中亚和欧洲的政府机构、外交机构、科研机构等。

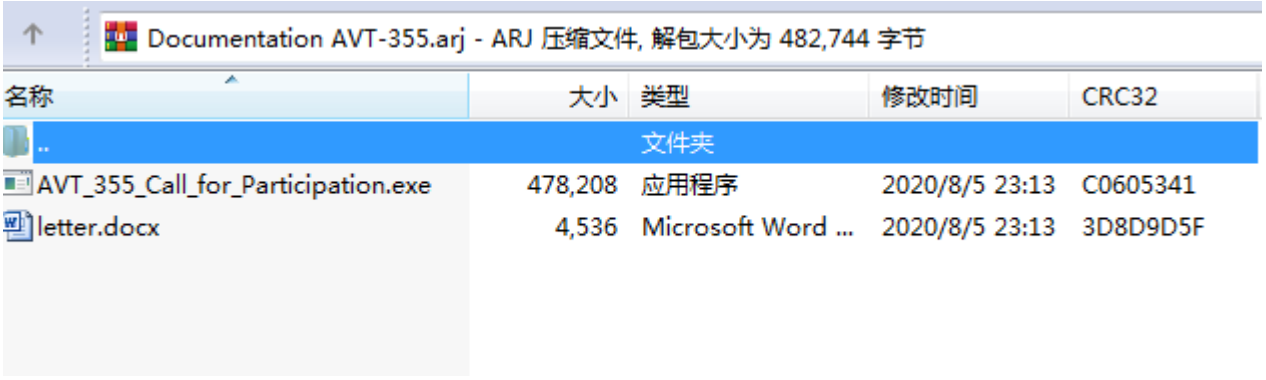
2020年7月1号，360高级威胁研究院就APT28针对东欧和中亚等外交机构的攻击活动进行了追踪分析，并发布了《游走在东欧和中亚的奇幻熊》*[1]*分析报告。近期，我们发现APT28又升级了技战术，携最新的nim zebrocy downloader 和delphi zebrocy downloader等武器针对北约、中亚目标进行攻击。其最新的攻击方式利用了arj压缩格式和VHD虚拟磁盘格式打包恶意荷载，部分杀毒软件对这类小众压缩包形式存在扫描机制的缺陷，导致相关的恶意文件可能规避安全软件的查杀。

nim zebrocy downloader

APT28在历史的攻击活动中多次使用zebrocy downloader。zebrocy downloader包括delphi版本，nim版本，autolt版本，VB.NET版本，Visual C++版本，C#版本以及go版本。zebrocy downloader主要功能为收集目标计算机的信息，在目标被确认后，植入下一阶段攻击组件。

攻击活动分析

在疑似针对北约组织目标的攻击活动中，APT28使用nim版本的 zebrocy downlaoder进行攻击。依然使用压缩包附件形式的诱饵，但此次攻击使用了ARJ格式的小众压缩包格式，压缩包中包含一个nim zebrocy downloader和诱饵文档。压缩包的打包时间是2020年08月5号。同时在2020年的7月到8月我们捕获到了APT28的多个nim zebrocy downloader测试版本。



诱饵文档内容如下。

NATO Science & Technology Organization

Dear colleagues,
Call for Participation AVT-355 Research Workshop (RWS) on Intelligent Solutions for Improved Mission Readiness of Military UxVs
Thursday, 20. May 2021 until Friday, 21. May 2021

Abstract Submission Deadline: 6 October 2020

All details about the event, deadlines and schedule, as well as the abstract and presentation format requirements are provided in the PDF document "Call for Participation" in the attachment.

Best regards,
Kurt Hoffman

北约科学技术组织（STO）的应用车辆技术（AVT）小组正在组织一个有关“为军事UxV改善任务准备的智能解决方案”的研讨会（RWS）。可以看到在RWS官网上，提供了一个“AVT-355 Call for Participation.pdf“。攻击者在压缩包中将nim zebrocy downloader伪装成该文档，诱惑目标进行点击执行。

技术细节分析

文件信息如下

信息	值
md5	98e304e28a51acd92a363346c2b02b2f
Timestamp	1970-01-01 08:00:00

nim zebrocy downloader在功能上与delphi zebrocy downloader类似，主要是获取目标计算机的信息，以及获取屏幕截图信息，并将数据发送到C2。
nim zebrocy downloader在获得目标计算机屏幕截图之后，将其写入到C:/Users/Public/Videos/$$temp.tmp文件中，然后读取文件之后，将其发送到C2。

然后弹出如下的提示框以迷惑目标用户。

nim zebrocy 通过wmi命令来获取目标计算机的信息，收集的信息有计算机版本信息等，然后将信息使用base64编码，命令如下:

wmic os get Caption,CSDVersion,osarchitecture /value

然后将获得屏幕截图信息，目标计算机版本信息，当前时间，通过http post请求发送到C2

key	**value**
adsges	系统时间
wefwqw	系统信息
hntyry	截图数据

数据包如下。

delphi zebrocy downloader

在2020年7-10月，我们捕获到了APT28利用delphi zebrocy downloader进行的多起攻击活动。在疑似针对中亚的某外交机构的攻击活动中，APT28依然利用打包的压缩包中包含delphi zebrocy来进行攻击。

攻击活动分析

但是在其中的一次攻击活动中，我们捕获到了一例新的攻击样本，该组织将delphi zebrocy downloader被打包在虚拟磁盘文件(vhd)内，这类文件在一些压缩软件和文件关联的方式打开后，是通过磁盘挂载的方式显示文件，部分杀毒软件会忽略VHD文件格式的扫描，同时也可能忽略虚拟磁盘的内容，因此攻击者以此特性来规避杀毒软件的扫描查杀。

诱饵文档内容如下。

技术细节分析

delphi zebrocy downloader在功能方面与之前的版本并无差别，主要是获取用户的信息之后上传至C2，并具备执行系统指令的功能。

样本在启动后，判断文件名中是否包含2020，如果包含，则复制downloader到C:\Users\purple\AppData\Roaming\Controller\scrssl.exe，然后执行downloader。

当文件命中不包含2020时，则创建名称为Windows\Component\ModuleUpd的计划任务每三分钟运行一次，实现持久化。

然后启动winword.exe,打开同目录下的同名docx文件，以迷惑用户。

此次Zebrocy delphi Downloader与以往版本不同的是字符串编码方式发生了变化，以往的Zebrocy delphi downloader中，将命令字符信息编码成16进制字符串，如下图。

此次捕获的Zebrocy delphi downloader中，将命令字符信息翻转保存。如下图为创建计划任务的命令字符串。

同时根据virustotal平台的检出结果显示，vhd格式打包的delphi zebrocy downloader有很好的免杀效果。

攻击关联分析

在以往的delphi zebrocy downloader中，将字符串编码成16进制，在nim zebrocy中，将字符信息编码成16进制之后，使用base64在此编码后进行存储。

附录 IOC

诱饵文件

855005FEE45E71C36A466527C7FAD62F

c74aa42b41ec44571a3f4e167b01c53c

D21A025E6BA0DB784ABB1D086B67D3DF

2760C647D03B5D26D3A331428733C809

b66c2aa25d1f9056f09d0a158d20faef

nim zebrocy downloader md5

98e304e28a51acd92a363346c2b02b2f

3792380fd7512cc2ec9b28a686edb0e9

93150535f9dcd9f7e169e255264c787a

573247af55b015d48ab7f6d7d0d6f1db

93150535f9dcd9f7e169e255264c787a

c4a0448925980eacbd22c2dd4869a1c7

fafd702197d758ce2687706336750660

delphi zebrocy downloader md5

72552EF22B484F8868DAB10B0F605779
009f073f66b24677cf7ad66818fe4509
8103bffc16f8fb3e55028a62e1a004f8
a14c1fd7b59b34515e6a8a286114c48f
d5e45a9db7f739979105e000d042f1fe

IP

194.32.78.245

185.205.209.172

31.7.62.103

URL

http://194.32.78.245//protect/get-upd-id.php

http://185.205.209.172/sciencedirect/development/AAF-Progress.php

http://31.7.62.103/tleaw.php

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。

---

[1] https://mp.weixin.qq.com/s/pE_6VRDk-2aTI996sff0og
