

## Overview

Spear phishing has always been one of the easiest ways to get into a corporate network. Spear phishing attacks are often used against large corporations, banks, or influencers. The most common targets are high-level employees who have access to rich information, or department employees who need to open a large number of external files at work. Generally, the attack file is a macro code written in Microsoft Word or JavaScript code. This kind of file is very small, there is no extra program built into the file, and its sole purpose is to download a more destructive malicious code in the target object's computer. After the malware is downloaded, it is further spread in the target network, or it is simply used to steal all available information to help attackers find targets in the network.

Recently, the Red Raindrop team of Qi'anxin Threat Intelligence Center has captured a large number of spear-phishing attack samples targeting Korean companies in their daily threat hunting. It infects documents or chm files with vulnerabilities, distinguishes the current operating system bitness, and executes the macro code corresponding to the system bitness to achieve the best attack effect. After research, the characteristics of this attack are as follows:

1. The initial infection documents are downloaded and executed using the CVE-2017-0199 remote code execution vulnerability; 2. Subsequent attacks use the UAC Bypass technology of the local RPC interface to escalate privileges; 3. Follow-up load packing interference analysis, and use simple means to detect whether it is in the sandbox;

### Sample analysis

#### 0x01 Decoy file

The attack samples captured this time are docx files, all of which use the remote code execution vulnerability of Microsoft Office/WordPad. The vulnerability number is CVE-2017-0199. The bait analysis of the relevant samples is as follows:

The decoy file induces victims to click "enable content" in a number of ways. For example, 긴급재난지원금신청서양식.docx (application form for emergency disaster assistance) induces users to click to enable the content by displaying garbled file content.

诱饵文件대한광산개발(주).docx(大韩矿山开发股份)则显示该文档由Windows11制作，诱导受害者点击启用内容。

或者假冒微软的错误提示，目的同样是诱导用户点击启用内容。

#### 0x02 恶意宏

这里以 투자서.docx(通知书)为例进行分析，点击执行诱饵文件后，访问远程模板<http://VM2rJOnQ.naveicoipg.online/ACMS/0hUxr3Lx/police0?mid=h1o5cYfJ>下载执行，下载执行的文件如下所示。

文件内嵌的宏代码首先从外部下载附加有效载荷(32Bit/64Bit)：

有效载荷的挂载页面：

随后有效载荷经解密后被注入winword.exe进程。

#### 0x03 注入的代码

被注入的代码在主函数中首先进行反沙箱检测。

同时，会检测当前运行的进程中是否包含v3l4sp.exe，如包含则退出程序。v3l4sp.exe为韩国AhnLab公司免费杀毒软件V3 Lite的子程序，此举说明本次攻击目标不是针对韩国的个人用户。

随后在%AppData%\Local\Microsoft\TokenBroker目录下释放error.log，并写入“s/o2ldz9l95itdj2e/error.txt?dl=0”，并在同目录下解密释放RuntimeBroker.exe。

然后利用本地RPC接口的UAC Bypass技术执行RuntimeBroker.exe。

最后通过注册表启动项使其持久化运行。

#### 0x04 RuntimeBroker.exe

RuntimeBroker.exe通过加UPX壳来干扰研究人员分析，经过脱壳处理后，发现其同样在主函数对沙箱进行检测，并且也检测当前运行的进程中是否包含v3l4sp.exe和AYAgent.aye。AYAgent.aye是韩国ESTsoft公司互联网安全套件ALYac的一部分。

校验当前运行的程序路径是否是%AppData%\Local\Microsoft\TokenBroker目录下的RuntimeBroker.exe，不是则自删除，此举目的为躲避沙箱的动态检测。

随后使用PowerShell命令将其添加到Windows Defender的排除列表中。

读取释放的error.log文件内容，将其与云服务器Dropbox的网址dl.dropboxusercontent.com进行拼接，使其作为中介传递C2信息。

然后以指定格式“uid=%s&avtype=%d&majorv=%d&minorv=%d”将用户信息上传至hxxp://naveicoipg.online/post2.php，其中，当没有指定杀软时avtype的值为1，存在v3l4sp.exe时为2，存在AYAgent.aye时为3。

后续访问naveicoipg.online的“/fecommand.acm”页面获取载荷，其中uid为之前回传C2的受害者标识。

获取的指令内容调用函数sub\_401410执行，恶意软件内部维护着一个大小为100的结构体数组，用来记录执行过的指令。

如果指令之前没执行过，则调用函数sub\_401280从C2下载相应的后续载荷，下载后续的URL格式为“<指令名称>”，获取的内容会作为PE文件执行。

遗憾的是，截至分析时后续内容暂无法获取。

#### 溯源与关联

通过在数据库中检索关键字“fecommand.acm”，我们发现了攻击样本的另一种传播方式，通过使用CHM文件进行分发。

检索到的chmext.exe恶意程序，其母体文件为一CHM文件。

诱饵chm文件中的短链接被重定向至韩国疾病控制和预防中心的实际网站，这与诱饵文件名相呼应，使受害者更容易中招。

经比较，chmext.exe与上述注入的代码基本一致，仅C2不同，chmext.exe的C2为naveicoipc.tech。

在继续追踪溯源中，我们还发现了其冒充韩国互联网信息中心的钓鱼邮件。结合种种迹象，我们怀疑此次攻击出自APT组织之手，其攻击目标非个人普通用户，攻击手段复杂多变，其后续真正的载荷较为隐蔽，且攻击样本数量较大，短期内我们便捕获了大量攻击样本。

对攻击目标为韩国的APT组织进行梳理，我们发现本次攻击疑似出自APT组织Lazarus之手，早在几年前，Lazarus组织便擅于使用云服务器Dropbox来进行攻击，其次在2月malwarebytes labs披露Lazarus的报告中【1】，Lazarus在攻击流程中也创建了RuntimeBroker进程。

无独有偶，在对C2的溯源过程中我们发现，早在3月25日，国外安全公司Rewterz便对naveicoipc.tech域名作出了预警【2】，其预警中的网址链接与我们早期捕获的样本链接基本一致。

## 总结

截至完稿时，还在有新的攻击样本不断被发现，值得我们警惕！

钓鱼邮件一直是APT组织攻击的重要手段之一，大多数用户安全意识不强，很容易被伪装邮件以及伪装的文档、欺骗性标题所迷惑。奇安信红雨滴团队提醒广大用户，谨防钓鱼攻击，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行标题夸张的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁。

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台 (<https://sandbox.ti.qianxin.com/sandbox/page>) 进行判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析【3】。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

## IOCs

### MD5

44BE20C67A80AF8066F9401C5BEE43CB

65ABAD905E80F8BC0A48E67C62E40119

1FD8FEF169BF48CFDCF506151264128C

7B07CD6BB6B5D4ED6A2892A738FE892B

9AD00E513364E9F44F1B6712907CBA9B

15A7125FE9E629122E1D1389062AF712

749CCB545B74B8EB9DFF57FCB6A07020

1769A818548A0B52C7BE2A0A213A9384

9775EF6514916977D73E39A6B09029BC

210DB61D1B11C1D233FD8A0645946074

B587851D8A42FC8C23F638BBC2EB866B

BDFB5071F5374F5C0A3714464B1FA5E6

C0B24DC8F53227CE0C64439B302CA930

619649CE3FC1682C702D9159E778F8FD

D19DD02CF375D0D03F557556D5207061

D47F7FCBE46369C70147A214C8189F8A

E3FFDA448DF223B240A20DAE41E20CEF

825730D9DD22DBAE7F2BD89131466415

4382384FEB5AD6B574F68E431006905E

AAD5A9F3BE23D327B9122A7F7E102443

556ABC167348FE96ABFBF5079C3AD488

## URL

<http://VM2rJOnQ.naveicoipg.online/ACMS/0hUxr3Lx/police0?mid=h1o5cYfJ>

<http://twlekqnwl.naveicoipg.online/ACMS/0y0fMbUp/supportTemplate7?cid=yypwjelnblw>

<http://olsnvolqwe.naveicoipg.online/ACMS/0y0fMbUp/supportTemplate5?cid=pqwnlqwjqg>

<http://vnwoei.naveicoipg.online/ACMS/0s4AtPuk/wwwTemplate?cid=nnwoieopq>

<http://jvnquetbon.naveicoipg.online/ACMS/0pxCtBMz/policeTemplate1?mid=ksndoqiweyp>

<http://AOsM8Cts.naveicoipg.online/ACMS/0ucLxIjP/toyotaTemplate8?tid=CN2xsRPI>

<http://ADzJvazJ.naveicoipg.online/ACMS/0ucLxIjP/toyotaTemplate1?tid=2uiSmhx2>

<http://CEcOMTp3.naveicoipg.online/ACMS/0o0WQher/ttt3?qwe=v0OSWog5>

<http://123fisd.naveicoipg.online/ACMS/0mFCUrPf/temp04060?ttuq=qcnvoiek>

<http://naveicoipc.tech/ACMS/0Mogk1Cs/topAccounts?uid=3490blxl>

<http://1xJOiKZd.naveicoipa.tech/ACMS/Cjtpp17D/Cjtpp17D64.acm>

<http://uzzmuqwv.naveicoipc.tech/ACMS/1uFnvppj/1uFnvppj32.acm>

<http://naveicoipd.tech/ACMS/018ueCdS/blockchainTemplate>

<http://bcvbert.naveicoipe.tech/ACMS/01AweT9Z/01AweT9Z64.acm>

<http://xjowihgnxcvb.naveicoipf.online/ACMS/07RRwrwK/07RRwrwK64.acm>

## Reference link

[1]. <https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/>

[2]. <https://www.rewterz.com/rewterz-news/rewterz-threat-alert-lazarus-apt-group-iocs-6>

[3]. <https://ti.qianxin.com/portal>

Click to read the original text to ALPHA 5.0

Immediately assist in threat analysis