2017 年 2 月 23 日，星期四

# 韩国恶意文档投放恶意新年礼物

作者：Warren Mercer 和 Paul Rascagneres。

## 执行摘要

Talos 调查了一种针对韩国用户的有针对性的恶意软件攻击活动。该攻击活动在 2016 年 11 月至 2017 年 1 月之间高度活跃，专门针对有限数量的人群。其感染媒介为 Hangul 文字处理器 (HWP) 文档。HWP 是 Hancom 开发的，用于替代 Microsoft Office。

本文所涉及的恶意文档采用韩语编写，标题如下：

5170101-17 년_북한_신년사_분석.hwp（翻译为：5170101-17 __ 朝鲜 _ 新年 _ 分析.hwp）
本文档声称是韩国统一部编写的，而且在页脚部分有韩国统一部的徽标。

我们分析的恶意文档的有一点很有趣，那就是该文档会尝试从韩国政府官方网站 kgls.or.kr（韩国政府法律服务部门官网）下载文件。下载的文件通常是伪装成 jpeg 文件的二进制文件，随后系统在感染过程会执行该二进制文件。攻击者很可能已经攻击该网站，试图使其 HTTP GET 尝试合法化以便获取最终负载，而任何系统管理员对于这种流量都不会感到陌生。

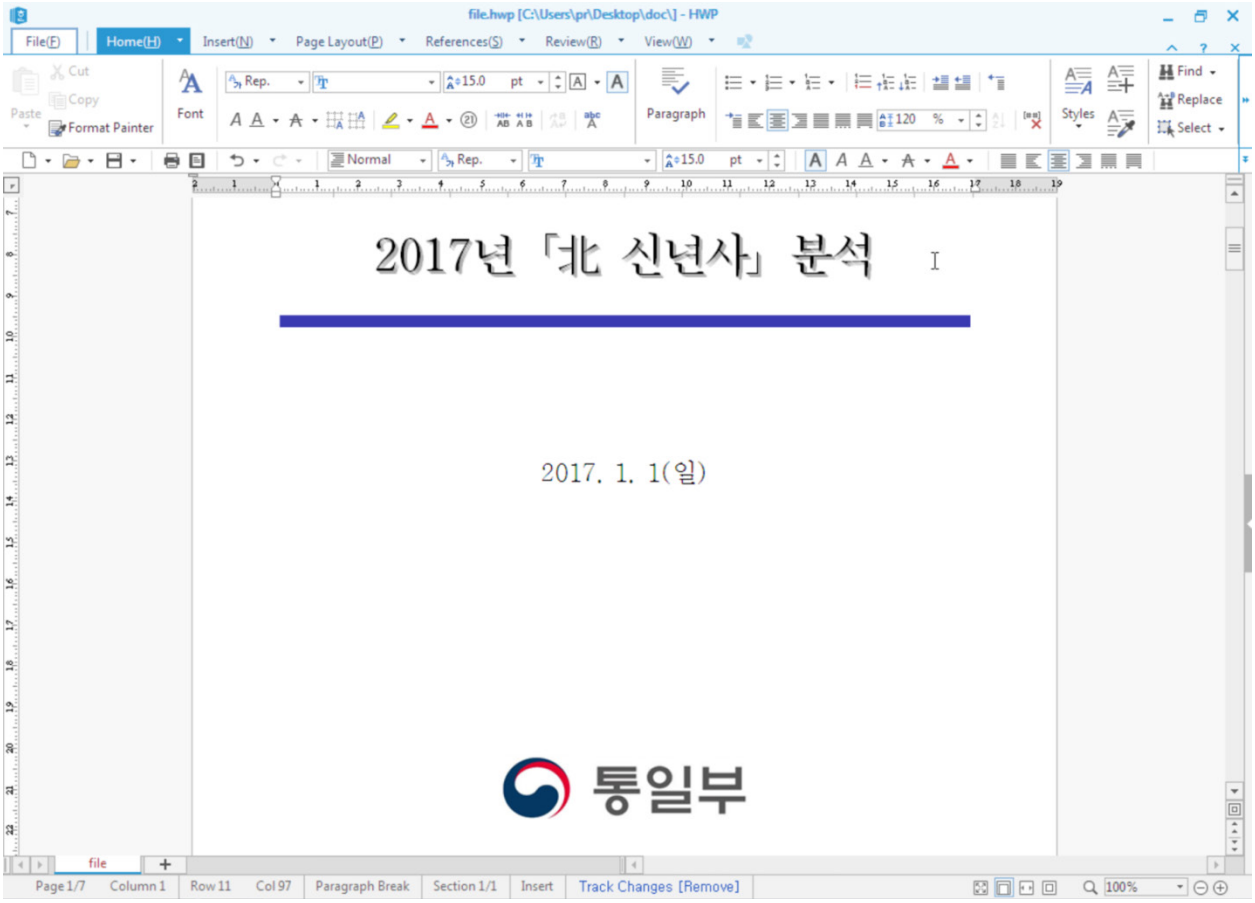
攻击者的基础设施似乎只是一次性运行几天，我们没有观察到他们重复使用这些基础设施。遗憾的是，攻击者已经清理或移除所有受攻击的站点，因此 Talos 无法获得最终负载。老练的攻击者经常实施这种程度的运营安全。

鉴于这些因素，可以推断这种加载程序很可能是资金雄厚的组织专门设计的，旨在对韩国的公共部门实体发起有针对性的攻击。其中所采用的很多技术类似于之前与特定政府组织的攻击相关的活动情况。

## 感染媒介：HANGUL 文字处理器

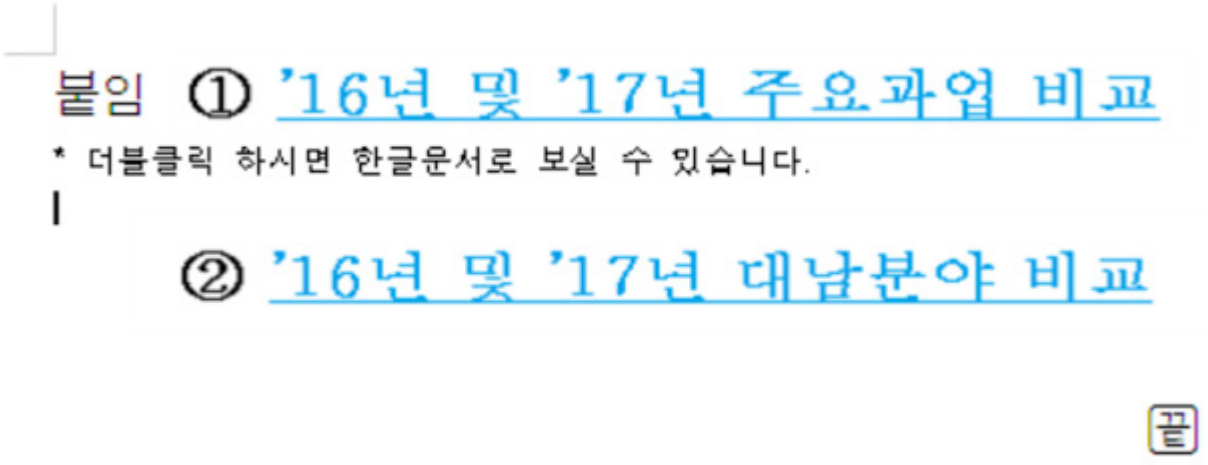
Talos 确定的感染媒介是 HWP 文件。由于该软件在韩国之外很少使用，攻击者很少选择这种媒介，但它在韩国却使用得很普遍（就连韩国政府部门也在使用）。由于这只是一种区域性文件格式，所以许多安全设备并不具备处理 HWP 文件的功能。这可能为攻击者提供了一种被安全扫描设备检出的风险较低的感染媒介。

以下是该文档打开后的屏幕截图：

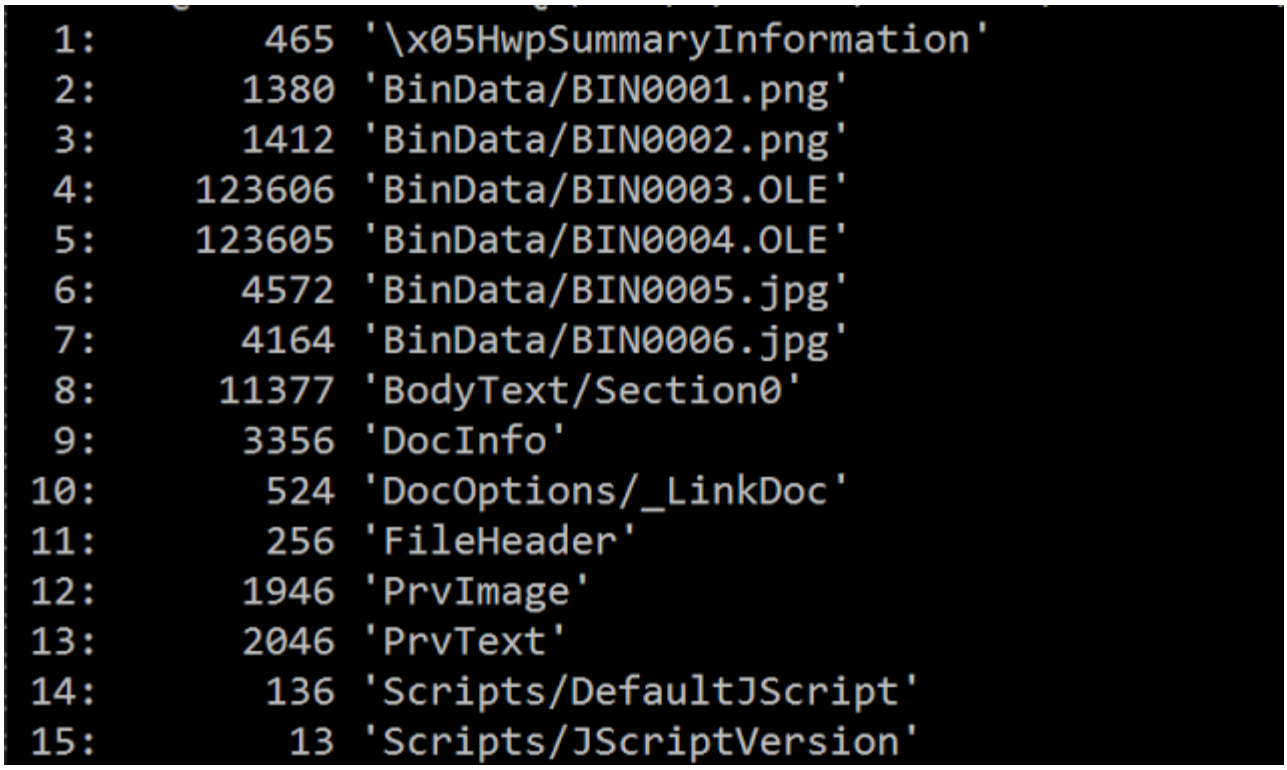



该文档的标题是“2017 年‘朝鲜新年’分析”。该文档底部是韩国统一部的徽标。韩国统一部致力于实现朝鲜和韩国的统一。该文档介绍与朝鲜新年庆祝活动相关的信息。

该文档结尾是两个其他文件的链接。该恶意文档指出，用户应双击链接才能访问这两个文档，其中文档 1 标识为“2016 年与 2017 年的重大任务比较”；文档 2 标识为“2016 年与 2017 年的比较”



这两个链接指向该文档中嵌入的两个 OLE 对象（BIN0003.OLE 和 BIN004.OLE）：



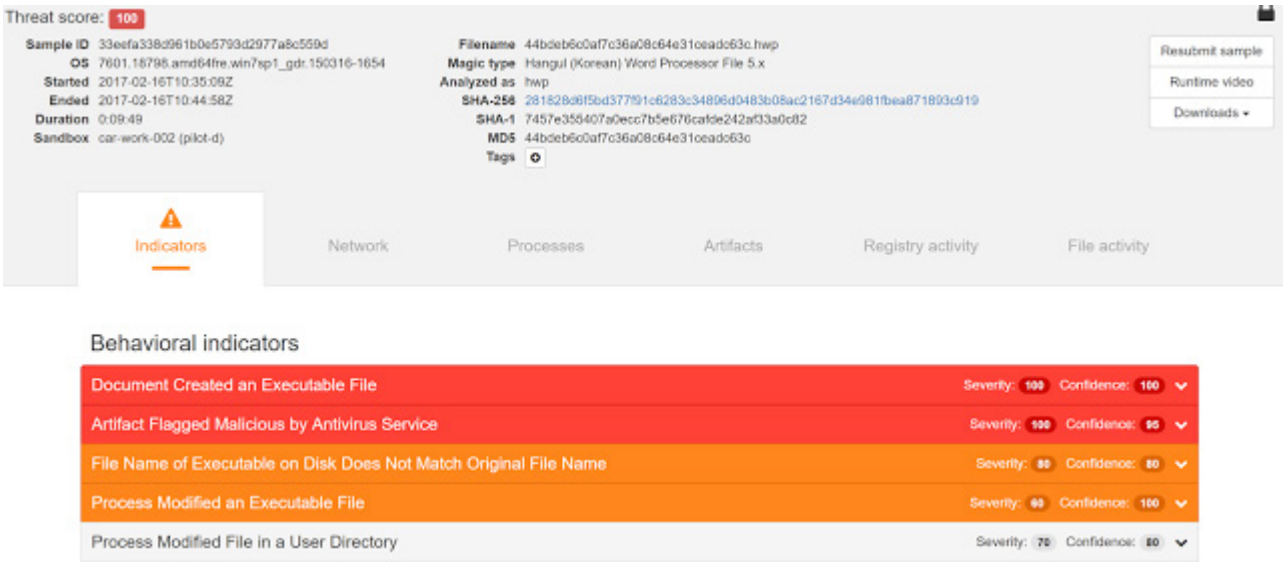

解压之后 (zlib)，我们发现这两个 OLE 文件中嵌入了两个 PE32 文件。如果目标用户双击其中任一链接，该恶意文件就会投放并执行一个 PE32 文件。

在我们的分析中，可以在以下位置找到和执行这两个被投放的二进制文件：

- C:\Users\ADMINI~1\AppData\Local\Temp\Hwp (2).exe
- C:\Users\ADMINI~1\AppData\Local\Temp\Hwp (3).exe

我们可以在该文档中发现一个 JavaScript 对象。该对象不包含恶意内容，是系统默认包含的对象。

以下是在思科 AMP Thread Grid 中执行该 HWP 文件的情况：







## 投放的文件

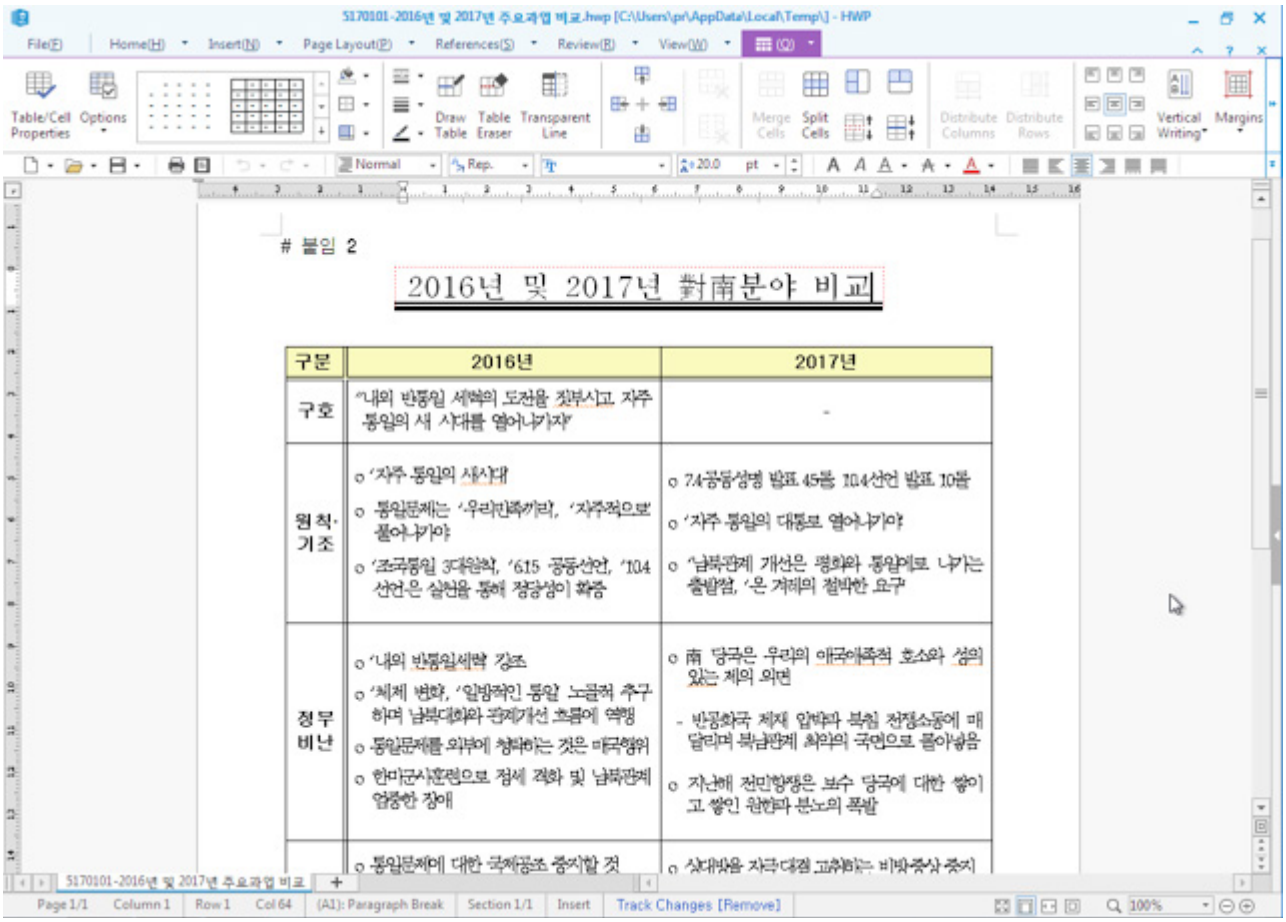
攻击者未删除二进制文件的编译路径，这使得我们可以确定该攻击所采用的工作空间和环境。

e:\Happy\Work\Source\version 12\T+M\Result\DocPrint.pdb

这两个被投放的恶意软件文件的散列值不同，但它们的用途是一样的：

- 打开 HWP 文件（这是对用户在之前文档中执行的双击操作的响应）；
- 从受攻击的主机/C2 下载负载。

所打开的文件嵌入在 PE 中（位于一个名为“DOC”的资源内）：




与之前的文档一样，这个文档也是在论述朝鲜和韩国的关系，而且似乎是一名韩国本土人士撰写的，因为用到的特定用语很地道。

该二进制文件的第 2 阶段执行 wscript.exe 并将 shellcode 注入该流程。shellcode 嵌入在一个名为“BIN”的资源中。该 shellcode 的用途是在合法 wscript.exe 进程中解压第二个 PE32 文件并执行该文件。执行这种注入的是经典的 VirtualAllocEx()、WriteProcessMemory() 和 CreateRemoteThread() API。

解压后的二进制文件用于收集有关受感染系统的信息，并尝试与 C2 通信以便下载最终负载。收集到的信息包括：

- 计算机名称
- 用户名
- 样本的执行路径
- 通过分析 HKLM\System\CurrentControlSet\Services\mssmbios\Data\SMBiosData 注册表项获得的 BIOS 模型。攻击者可以通过这些信息确定虚拟机（在 VirtualBox 上，该模型为“innotek GmbH VirtualBox”）
- 随机生成的用于标识系统的 ID

攻击者可以将这种信息用作侦测阶段，确定是否有适当的平台可用来传输最终负载和避免向沙盒系统发送最终负载。

我们分析的样本按照这种顺序与以下两个 URL 进行网络连接：

- www.kgls.or.kr/news2/news_dir/index.php（发送所收集的信息）
- www.kgls.or.kr/news2/news_dir/02BC6B26_put.jpg

jpg 文档的开头 (02BC6B26) 是先前生成的 ID。我们认为该 jpg 文件是在所收集的数据具有相关性的情况下由 index.php 文件自动生成的。该 jpg 文件的内容保存在一个名为“officepatch.exe”的文件中。最后，恶意软件会执行此新文件，而且解压的可执行文件会自动终止。

网站 kgls.or.kr 是韩国政府法律服务部门的网站。Talos 只能假设攻击者攻击了该网站以传输最终阶段的恶意软件，即该 jpg 文件。在我们进行分析期间，所有基础设施都处于关闭状态，致使我们无法直接分析其负载。

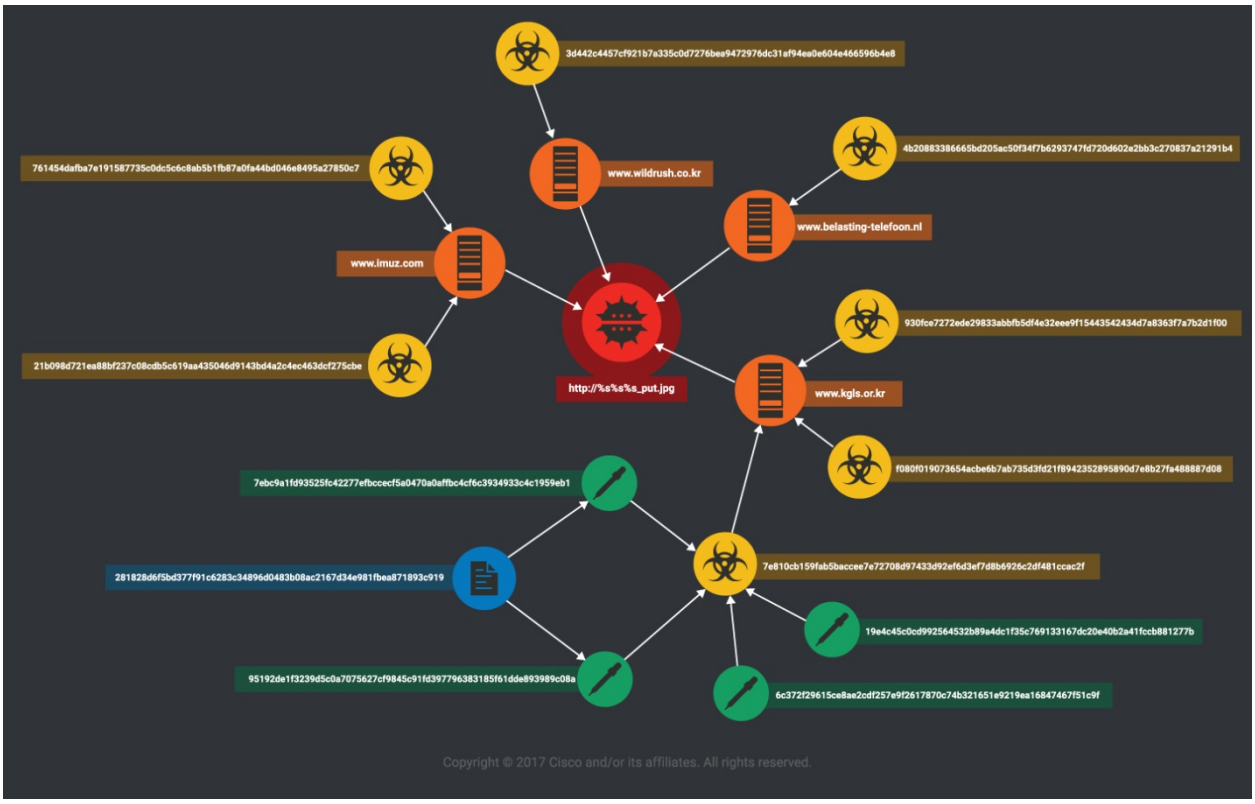
我们收集的二进制文件编译于 22:43:05 UTC 至 4:55:18 UTC 期间（其中在 22:00:00 编译的 3 个文件是 HWP 文档投放的二进制文件，其他文件则是解压的负载）- 攻击者可以轻松地伪造时间戳工件并将之部署为伪造的标志机制，使得研究人员认为攻击者编译的代码来自特定时区，因此不能将时区作为确定攻击或攻击者来源的可靠指标。

## 命令和控制基础设施

在我们的调查中，我们确定了该攻击发起者使用的其他命令和控制基础设施。这四个 C2 位于下列国家：

- 3 个 C2 位于韩国
- 1 个 C2 位于荷兰

这是我们确定的基础设施的全局图：




颜色含义：

- 红色：“_put.jpg”二进制文件（最终负载）
- 橙色：攻击者使用的 C2 基础设施
- 黄色：用来进行连接以下载最终恶意软件的解压样本（绿色圆形部分共用 90% 的相似代码）
- 绿色：由 HWP 文档投放的可执行文件（橙色部分圆形部分共用 90% 的相似代码）
- 蓝色：HWP 文档

## 总结

该攻击发起者似乎有意通过使用 Hangul 限制了攻击面。这使得他们可以躲避某些安全设备，因为这些设备不常处理这种格式。

感染过程是通过一份恶意文档进行多次投放（执行过程完全一样），然后执行 C2 通信以获取最终负载。使用文档作为诱饵的做法非常常见，这表明攻击者想利用社交工程或诱骗方法促使用户打开该文档。

该攻击活动目标明确，针对的是特定用户群，对这种特殊文件格式的使用可以证明这一点。很明显，攻击者采取了一系列措施来限制安全产品检测这种威胁的能力和对严格时间线的遵

循，以免这些恶意文件被发现。攻击者还小心地删除了他们的恶意负载并且没有重复使用基础设施。

我们认为，这是一次针对韩国公共部门用户的有针对性的攻击，执行该攻击的威胁发起者非常老练，而且与韩国本土人士有联系。对上述这些用户的攻击可能是为了获得一个立足点，借以窃取极其宝贵的资产。

## IOC

HWP 文件：

5170101-17 년_북한_신년사_분석.hwp:
281828d6f5bd377f91c6283c34896d0483b08ac2167d34e981fbea871893c919

投放的文件：

95192de1f3239d5c0a7075627cf9845c91fd397796383185f61dde893989c08a
7ebc9a1fd93525fc42277efbccecf5a0470a0affbc4cf6c3934933c4c1959eb1
6c372f29615ce8ae2cdf257e9f2617870c74b321651e9219ea16847467f51c9f
19e4c45c0cd992564532b89a4dc1f35c769133167dc20e40b2a41fccb881277b
3a0fc4cc145eafe20129e9c53aac424e429597a58682605128b3656c3ab0a409
7d8008028488edd26e665a3d4f70576cc02c237fffe5b8493842def528d6a1d8

解压的相关样本：

7e810cb159fab5baccee7e72708d97433d92ef6d3ef7d8b6926c2df481ccac2f
21b098d721ea88bf237c08cdb5c619aa435046d9143bd4a2c4ec463dcf275cbe
761454dafba7e191587735c0dc5c6c8ab5b1fb87a0fa44bd046e8495a27850c7
3d442c4457cf921b7a335c0d7276bea9472976dc31af94ea0e604e466596b4e8
930fce7272ede29833abbfb5df4e32eee9f15443542434d7a8363f7a7b2d1f00
4b20883386665bd205ac50f34f7b6293747fd720d602e2bb3c270837a21291b4
f080f019073654acbe6b7ab735d3fd21f8942352895890d7e8b27fa488887d08

网络：

www.imuz.com/admin/data/bbs/review2/board/index.php
www.imuz.com/admin/data/bbs/review2/board/123.php
www.imuz.com/admin/data/bbs/review2/board/02BC6B26_put.jpg（在此随机生成 02BC6B26）

www.wildrush.co.kr/bbs/data/image/work/webproxy.php
www.wildrush.co.kr/bbs/data/image/work/02BC6B26_put.jpg（在此随机生成 02BC6B26）

www.belasting-telefoon.nl//images/banners/temp/index.php
www.belasting-telefoon.nl//images/banners/temp/02BC6B26_put.jpg（在此随机生成

02BC6B26）

www.kgls.or.kr/news2/news_dir/index.php
www.kgls.or.kr/news2/news_dir/02BC6B26_put.jpg（在此随机生成 02BC6B26）

## 防护

思科客户可通过其他方式检测并阻止此威胁，包括：

| 产品 | 保护 |
| --- | --- |
| AMP | ✔ |
| CWS | ✔ |
| 邮件安全 | ✔ |
| 网络安全 | ✔ |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

高级恶意软件防护（AMP）解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者进行的恶意网络活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置的保护措施。

Umbrella 可防止对与恶意活动相关的域进行 DNS 解析。

发布者：PAUL RASCAGNERES；发布时间：上午 10:00
标签：APT、HWP、韩国、恶意文档、恶意软件、侦测