AhnLab

安全月刊

2020.06 Vol.91

Trula 黑客组织分析报告

Turla黑客组织分析报告

关注恐怖的黑客组织 Turla 在韩国的活动

近期，发现俄罗斯黑客组织Turla曾试图针对韩国国防工业企业进行高级持续性威胁（APT）攻击。Turla是使用俄语的恐怖的黑客组织，针对全世界的政府、外交、国防、教育和研究调查机构的进行攻击。AhnLab分析了今年3月韩国国防工业企业举报的恶意代码后，发现了Turla组织从2016年3月开始在韩国活动。在本文中，我们详细分析了Turla组织使用的Skipper恶意代码，并详细介绍了其在韩国开展的攻击活动。

黑客组织Turla又被称为Group 88、KRYPTON、Hippo Team、Snake、Uroburos、Venomous Bear、Waterbug、Wraith、Pfinet、TAG_0530、Pacifier APT、Popeye、SIG23、Iron Hunter、MAKERSMARK等，并被怀疑受到特定国家的支援。众所周知，该组织对各国政府和外交机构等展开攻击，自2014年以来，多家网络安全企业纷纷发布了分析报告。

攻击者主要利用电子邮件和水坑攻击（Watering hole）方式感染恶意代码。

在阅读ESET于2020年3月12日发布的关于Turla组织的博客后，确认了韩国国防工业企业在2020年3月也举报了Turla组织使用的Skipper恶意代码变种。随后，我们对AhnLab收集到的Skipper变种恶意代码在韩国的活动进行了研究，发现Turla组织从2016年5月开始在韩国活动。

Skipper 时间线

2016年5月，瑞士计算机应急响应小组（CERT）揭晓了网络攻击RUAG，7月，比特梵德（BitDefender）揭晓了网络间谍组织Pacifier APT的信息。经确认，这些报告揭晓的恶意代码是Turla组织的Skipper。

ESET一直对Turla组织进行追踪， 并发布了几份报告。2019年， 意大利网络安全公司Telsy也介绍了关于Skipper恶意代码的详细分析资料。

ESET在2020年3月宣布，到2019年底，至少有4个亚美尼亚网站遭到Trula APT的水坑攻击受到感染。

这些恶意代码与之前的攻击有关，一些模块与2017年发现的恶意代码类似，当访问者访问被黑客入侵的网站时，建议访问者安装假冒的Flash Player并感染访问者的系统。2020年3月， 在韩国发现了与该博客中公开的Skipper恶意代码类似的变种。

虽然该黑客组织在韩国的活动到现在才被确认， 但是与Skipper相关的大部分恶意代码已在AhnLab产品群中被检测到。另外， AhnLab安全应急响应中心（ASEC）还跟踪了该组织，并对未被诊断出的变种恶意代码做出了响应。但是，由于恶意代码的特性，可能还存在未诊断的变种。

Skipper 恶意代码

Turla组织使用了多种恶意代码 ， 但在此报告仅涵盖了Skipper恶意代码的内容。Skipper是Turla组织使用的恶意代码，该恶意代码于2015年首次发现。通常以DLL文件格式存在，文件长度为10,752~139,800字节。

Skipper病毒释放器（Dropper）是将Skipper下载到系统并安装的一种恶意代码，大部分是可以自解压的程序。2017年发现的病毒释放器是Cabinet SFX(Cabinet Self Extractor)形式的文件。该病毒释放器压缩了13个文件，

这些文件的生成日期为2016年3月。2020年3月在韩国发现的Skipper病毒释放器的变种是RAR SFX文件形式。

Skipper由多个DLL文件组成，并存在特殊的导出（Export）函数。2015年版本中存在CI、CS和SHR导出（Export）函数，从2016年版本的变形开始增加了kp函数。另外，2019年发现的变种存在CI、CS、_GetTempPathA@8、SHR和SHRforCS。

有些变种存在程序数据库（Program Data Base，PDB）路径字符串。通过该字符串，可以确认制作者的用户名似乎是work4和George。另外，不仅可以推测出编译程序和恶意代码的名称为Kotel，还能获知恶意代码的制作时间。除此之外，制作者还会继续使用“tranport”这个词，这可能是“transport”的错别字。

Skipper 恶意利用的证书

在2017年2月发现的变种中，发现了“AHC Hard & Software Ltd”证书。该证书目前已被吊销。用该证书签名的文件共有43个，并且似乎是在2016年12月发现的Skipper变种中首次使用。

用该证书签名的文件中，2016年12月发现的Skipper变种和2017年5月6日以后收集的文件的病毒释放器尚未得到确认。

Turla 组织在韩国的活动

据推测，Turla组织的Skipper恶意代码有170个以上。AhnLab对这些恶意代码的变种在韩国的活动进行了调查，并确认了Turla组织从2015年5月开始在韩国的活动。尽管大多数的攻击对象尚不明确，但这是在2019年6月和2020年3月对同一国防工业企业的攻击。出于安全方面的原因，一些样品没有公开哈希信息。

时间	攻击对象	内容
2016 年 5 月	无法特定	感染方法及攻击对象不明
2016 年 7 月	无法特定	感染方法及攻击对象不明
2019 年 6 月	国防工业企业	尝试使用包含宏（macro）的 Word 文档攻击
2020 年 3 月	国防工业企业	感染方法不明，2019 年 6 月试图攻击的同一国防工业企业

[表1] Turla组织在韩国的活动

2016年5月26日，Turla组织在韩国的活动痕迹首次被发现。但是，尚未确认到正确的攻击对象。在2016年7月，也发现了活动痕迹，但此次也未能确认到攻击对象。

在2019年6月初，尝试对韩国国防工业企业进行攻击。Word文档伪装成审批申请书，文档修改时间是2019年6月4日，作者是John。

当用户打开文档时，界面会显示“与该版本的Microsoft Word不兼容。请将Microsoft Word更新为最新版本或点击‘激活内容’键。”的提示，引导用户点击“使用内容”键来运行宏。

2020年3月，曾试图对同一国防工业企业进行攻击。

分析对象的基本信息如下：

文件名	pcinternetcheck.exe
文件长度	504,018 bytes
文件创建时间	2016 년 2 월 3 일 19 시 38 분 31 초 (UTC 기준)
MD5	ee1599b62f08df5f527d6771efd078dd
SHA1	875a64f5453ff0d9618e55e55dda9ff09563cc56
SHA256	c6edf5c441b58140f80229170e4673f41531b531fad4216a9bae296f0ae0b7c1
主要功能及特点	释放器
AhnLab 诊断名	Dropper/Win32.Turla

[表2] 2020年攻击中使用的文件信息

总结

AhnLab通过本公司的产品群支持对Turla组织使用的恶意代码进行诊断和检测。在首次追踪似乎与Turla组织有关的恶意代码在韩国的活动的同时， 还期待或许能确认到目前为止尚未发布的新内容。但遗憾的是， 虽然在韩国捕获到了被推测为Turla组织的活动， 但只确认了他们的初期阶段的攻击形式。对其他分析报告进行研究的结果，由于攻击者的特性，很可能在下一阶段的存在Skippe恶意代码。而且，尚未得到确认到是如何被感染的。

通过此报告， 期待Turla组织的Skipper恶意代码在韩国广为人知， 并且相关恶意代码信息将被共享， 从而可以尽快发现其他恶意代码。Turla组织存在多样的变种， 甚至在此报告结束的这一节点， 仍发布了有可能与该组织有关的恶意代码信息。尤其是政府机构和国防工业企业可能会成为Turla组织的攻击对象， 因此要特别关注与该组织相关的信息。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com