NSFOCUS

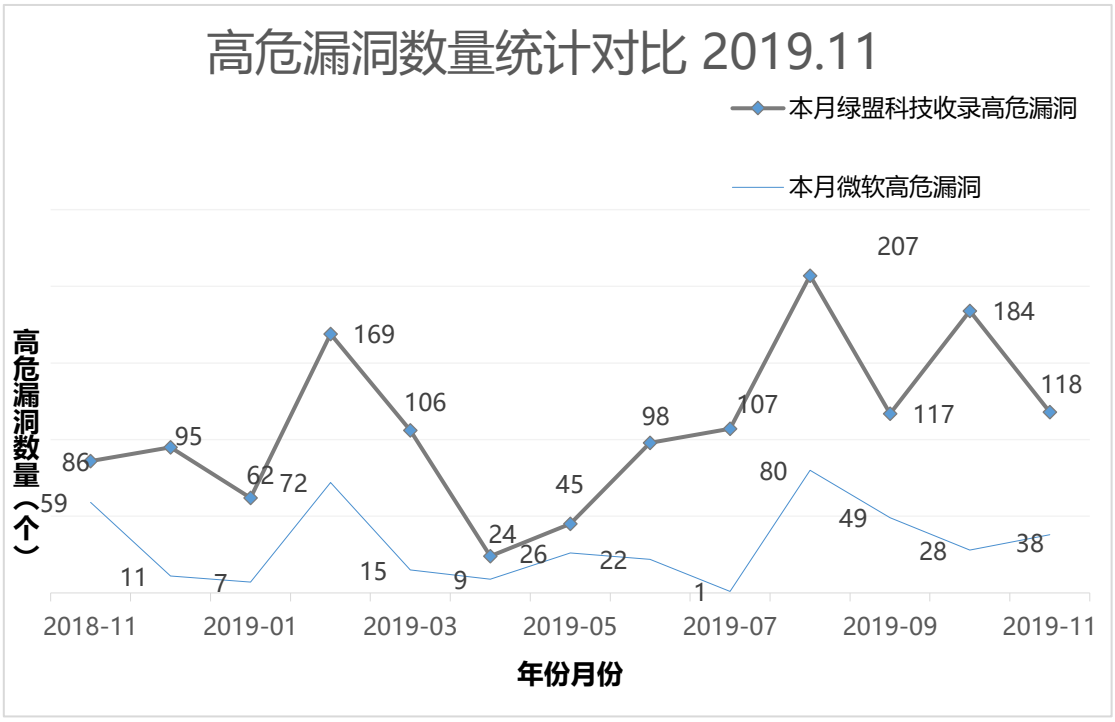
绿盟威胁情报月报

2019年11月

绿盟威胁情报中心(NTI)

一、 漏洞态势

2019 年 11 月绿盟科技安全漏洞库共收录 218 漏洞，其中高危漏洞 118 个，微软高危漏洞 38 个。



* 数据来源：绿盟科技威胁情报中心，本表数据截止到 2019.11.28

注：绿盟科技漏洞库包含应用程序漏洞、安全产品漏洞、操作系统漏洞、数据库漏洞、网络设备漏洞等；

二、 威胁事件

1. Lazarus 组织的 Mac 后门针对韩国用户

【标签】Lazarus、NUKESPED

【时间】2019-11-20

【简介】

最近发现 Mac 后门新变种，该变种关联到 Lazarus 威胁组织。Mac 后门样本使用了带有嵌入式宏的 Excel 文档，一旦运行，宏将运行 PowerShell 脚本，并尝试连接到三台 C2 服务器，其上有 Mac 应用程序捆绑包含恶意和合法的 Flash Player，恶意 Flash Player 文件实则是 MacOS 木马新变种 NUKESPED。本次攻击活动针对韩国用户。

【关联的攻击组织】

Lazarus（又名 HIDDEN COBRA、Guardians of Peace、ZINC 和 NICKEL ACADEMY）是一个威胁组织，归属于朝鲜政府，该组织至少从 2009 年以来一直活跃。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/mac-backdoor-linked-to-lazarus-targets-korean-users/

【防护措施】

绿盟威胁情报中心关于 Lazarus 组织的关注可追溯到 2017 年，关于 Lazarus 组织相关事件存在 28 件。Lazarus 组织相关联 IP22 个，相关联域名 31 个，相关联样本 112 个。绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

2. TA2101 组织在攻击活动中分发 Maze 勒索软件和 IceID 木马

【标签】A2101、Cobalt Strike、IcedID、Maze

【针对行业】制造业、卫生保健、IT 服务

【时间】2019-11-14

【简介】

TA2101 组织选择商业化渗透测试工具 Cobalt Strike，在近期的攻击活动中伪装成政府机构，通过恶意电子邮件向德国、意大利和美国的组织分发 Maze 勒索软件和 IceID 木马，影响的行业包括 IT 服务业、制造业和卫生保健等领域。

【关联的攻击组织】

TA2101 是一个相对较新的威胁组织，目前主要针对德国、意大利、美国的企业和组织，通过钓鱼邮件向受害者提供后门恶意软件，受影响的行业有 IT 服务、制造业和卫生保健等。

【关联的攻击工具】

Cobalt Strike 是一个功能齐全的商业化渗透测试工具，旨在执行有针对性的攻击并模仿高级威胁参与者的攻击利用行为。

【参考链接】

https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

【防护措施】

绿盟威胁情报中心关于该事件提取 7 条 IOC。绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

3. APT33 组织使用多层混淆策略定向攻击

【标签】APT33、C&C

【针对行业】能源

【时间】2019-11-13

【简介】

近期发现 APT33 威胁组织使用 12 个实时 C&C 服务器进行定向攻击活动，利用多层混淆处理，以隐藏并运行这些 C&C 服务器，受影响范围包括中东、美国和亚洲的组织。

【关联的攻击组织】

APT33，又名 Elfin，是一个与伊朗有关的威胁组织，至少从 2013 年开始运营，目标针对美国、沙特阿拉伯、韩国的多个行业和组织，尤其对航空和能源领域感兴趣。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/

【防护措施】

绿盟威胁情报中心关于该事件有 18 条相关 IOC；APT33 攻击组织相关事件 6 件，该攻击组织有 15 个关联域名、40 个关联样本；绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

4. DarkUniverse APT 框架

【标签】DarkUniverse、APTframework

【针对行业】军事

【时间】2019-11-05

【简介】

DarkUniverse 是一个至少活跃八年（2009 年-2017 年）的网络间谍活动框架，包含用于收集有关用户和受感染系统的各种信息的所有必要模块，与 ItaDuke 系列活动有关。攻击者利用鱼叉式钓鱼邮件传播恶意软件，向目标发送带有恶意 Microsoft Office 文档的电子邮件。受害者包含平民组织和军事组织，分别位于叙利亚、伊朗、阿富汗、坦桑尼亚、埃塞俄比亚、苏丹、俄罗斯、白俄罗斯和阿拉伯联合酋长国。

【参考链接】

https://securelist.com/darkuniverse-the-mysterious-apt-framework-27/94897/

【防护措施】

绿盟威胁情报中心关于该事件提取 7 条相关 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

5. BlackTech 组织使用 IconDown 恶意软件对日本的攻击

【标签】BlackTech、IconDown

【时间】2019-11-21

【简介】

绿盟威胁情报中心关于 BlackTech 组织关注最早可以追溯到 2017 年，关于 BlackTech 组织相关事件存在 6 件，相关事件主要集中在 2019 年，存在 3 件相关事件，2018 年存在 2 件，2017 年存在 1 件，由此可见 2019 年该组织较为活跃。BlackTech 使用各种类型的恶意软件对日本进行攻击，近期发现该组织利用 IconDown 恶意软件，该恶意软件通过 ASUS WebStorage 的更新功能进行传播。

【关联的攻击组织】

BlackTech 是一个至少从 2011 年活跃至今的威胁组织，主要针对东亚地区。

【参考链接】

https://blogs.jpcert.or.jp/en/2019/11/icondown-downloader-used-by-blacktech.html

【防护措施】

绿盟威胁情报中心关于该事件提取到 5 条相关 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

绿盟威胁情报中心（NTI）

绿盟威胁情报中心（NTI）依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，针对客户不同的需求场景，已经推出了云端情报查询服务（https://nti.nsfocus.com/）、互联网资产核查服务、安全设备/安全平台的威胁情报组件、客户本地威胁情报平台（NTIP）等产品及服务；为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

总部：北京市海淀区北洼路4号益泰大厦
绿盟科技（股票代码300369）

邮编：100089
电话：010-68438880
传真：010-68437328
邮箱：webadmin@nsfocus.com