NSFOCUS

绿盟威胁情报周报

2020年第12周 (2020.03.16-2020.03.22)

绿盟威胁情报中心(NTI)

https://nti.nsfocus.com/

本周热点概览

威胁通告

- VMware权限提升漏洞

热点资讯

- NetWire木马控制者投放nCoV-19疫情诱饵文档
- IPv6物联网资产暴露情况研究
- Ursnif木马新变种针对日本用户
- TrickBot以美国和香港的电信行业为目标
- EnigmaSpark活动针对中东实体
- 以冠状病毒为主题的新攻击使用了伪造的WHO主题邮件
- APT36利用冠状病毒潮流传播Crimson

一、 威胁通告

- VMware 权限提升漏洞

  【发布时间】2020-03-18 20:00:00 GMT

  【概述】

  3 月 17 日，VMware 官方发布编号为 VMSA-2020-0005 的安全公告，修复了存在于 VMware Fusion，VMRC for Mac 和 Horizon Client for Mac 中的权限提升漏洞（CVE-2020-3950），由于 VMware 错误的使用了 setuid，攻击者利用此漏洞可将目标系统中的普通用户权限提升至管理员权限。

  【链接】

  http://blog.nsfocus.net/vmware-cve-2020-3950-0318/

二、 热点资讯

1. NetWire 木马控制者投放 nCoV-19 疫情诱饵文档

   【概述】

   近期，绿盟伏影实验室发现，NetWire 远控木马控制者也开始使用 nCoV-19 疫情相关的诱饵文档来投放木马。NetWire，又称 NetWireRC 或 Recam，是一款最早出现在 2012 年的远控木马，曾被尼日利亚的黑客用于攻击企业目标。多年以来，NetWire 一直在更新版本，并演化出多条不同的攻击链。

【参考链接】

http://blog.nsfocus.net/netwire-ncov-19-0318/

2. IPv6 物联网资产暴露情况研究

【概述】

随着物联网应用的蓬勃发展、IPv4 地址的耗尽，IPv6 普及已成为必然趋势。IPv6 网络上暴露的物联网资产将成为攻击者的重点目标，所以能够对 IPv6 资产和服务准确的测绘，对于网络安全具有着重要的意义。绿盟格物实验室介绍国内、新加坡和日本的 IPv4 物联网资产的实际暴露情况，部分的 IPv6 地址集中的物联网资产暴露情况。

【参考链接】

https://mp.weixin.qq.com/s/Bj6PRqcxDoYwmXStShvYOw

3. Ursnif 木马新变种针对日本用户

【概述】

近期发现针对日本用户的 Ursnif 木马新变种的攻击活动，该恶意软件是通过来自垃圾邮件中受感染 Microsoft Word 文档分发的。Ursnif，也称为 Gozi，是一个信息窃取器，它从浏览器和电子邮件应用程序收集登录凭据，具有监视网络流量、屏幕捕获和按键记录功能。

【参考链接】

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-ursnif-campaign-targets-users-in-japan?_ga=2.95453402.710669801.1584953460-1997041092.1571902105

4. TrickBot 以美国和香港的电信行业为目标

【概述】

最近在针对美国和香港电信组织的攻击活动中发现 TrickBot 的变体，该新变体包括一个用于远程桌面协议（RDP）暴力破解的模块，包括对 check、trybrute 和 brute 三种攻击模式的支持。TrickBot 恶意软件主要通过垃圾邮件进行分发。

【参考链接】

https://www.bitdefender.com/files/News/CaseStudies/study/316/Bitdefender-Whitepaper-TrickBot-en-EN-interactive.pdf

5. EnigmaSpark 活动针对中东实体

【概述】

EnigmaSpark 活动针对新的中东和平计划，攻击者利用中东地缘政治发展，精心制作详细政治指控文件诱导收件人，已分发 EnigmaSpark 恶意软件。此次攻击活动疑似与 Molerats 有关，Molerats 是一个出于政治动机的威胁组织，自 2012 年以来一直活跃，该组织的受害者主要在中东、欧洲和美国。

【参考链接】

https://securityintelligence.com/posts/EnigmaSpark-Politically-Themed-Cyber-Activity-Highlights-Regional-Opposition-to-Middle-East-Peace-Plan/

6. 以冠状病毒为主题的新攻击使用了伪造的 WHO 主题邮件

【概述】

随着冠状病毒在全球范围内的传播，以冠状病毒为主题的攻击也日趋增加。近期发现攻击

者使用声称是有世界卫生组织 WHO 负责人发送的网络电子钓鱼邮件诱导用户，提供恶意软件 HawkEye 新变种，该恶意软件是一个键盘记录器。

【参考链接】

https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

7. APT36 利用冠状病毒潮流传播 Crimson

【概述】

APT36，也被称为 Transparent Tribe、ProjectM、Mythic Leopard 和 TEMP.Lapis，是一个至少从 2016 年活跃至今的巴基斯坦威胁组织，主要针对印度政府、国防部和使馆。目前 APT36 正在使用冠状病毒相关健康咨询文档作为诱饵来传播远程管理工具 Crimson。

【参考链接】

https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/

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。

NSFOCUS
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