NSFOCUS

绿盟威胁情报周报

2019年第50周(12.09-12.15)

绿盟威胁情报中心(NTI)

本周热点概览

威胁通告

- Gitlab EE 多个高危漏洞

暗网情报

- 3条金融行业暗网情报，覆盖银行、保险等；
- 2条互联网行业暗网情报；

热点资讯

- 微软发布12月补丁修复38个安全问题；
- Adobe 12月安全更新；
- Gallium威胁组织瞄准全球电信行业；
- WaterBear针对东亚的技术公司和政府机构；
- 勒索软件Zeppelin针对美国和欧洲的科技和医疗行业；
- Trickbot木马新变体Anchor的攻击活动与Lazarus组织有关。

一、 威胁预警

- Gitlab EE 多个高危漏洞

【发布时间】2019-12-11 18:00:00 GMT

【概述】

当地时间 2019 年 12 月 10 日，GitLab 官方发布了重要版本更新的通告，公布了三个 GitLab EE（企业版）的高危漏洞。GitLab 是一个用于仓库管理系统的开源项目，使用 Git 作为代码管理工具，并在此基础上搭建起来的 web 服务。

CVE-2019-19628：由于 maven 包的注册中心没有做好准确的参数设置，攻击者可在一定条件下实现权限提升和远程代码执行。

CVE-2019-19629：在将公共项目导入私有群组时，Elasticsearch 上集成的 Group Search API 可能导致私有代码泄露。

CVE-2019-19604：用户在使用 git submodule update 功能时，攻击者利用该漏洞可执行定义在.gitmodules 文件中的任意命令。

【链接】

http://blog.nsfocus.net/cve-2019-19604-cve-2019-19628-cve-2019-19629/

二、 暗网情报

分类	发现时间	暗网交易标题
金融	2019/10/26 16:10	保险公司数据 200 多万条 姓名/身份证/手机 可按 省份 出售
金融	2019/10/26 17:18	银行四大件 CVV 和一卡通 1500 余条（姓名/卡号/取款密码/身份证号/手机号等） 自动发货
互联网	2019/12/11 09:29	个人简历最全集合 31G 压缩包简历数据自动发货
互联网	2019/12/11 20:12	前程无忧智联招聘猎聘等个人简历数据 373G
金融	2019/12/12 11:56	50W 以上的股票帐户 15000 条适合电销的精准数据

*更多详细内容，可与绿盟科技商务人员联系或通过 csc@nsfocus.com 与我们联系

三、 热点资讯

1. 微软发布 12 月补丁修复 38 个安全问题

【概述】

微软于周二发布了 12 月安全更新补丁，修复了 38 个从简单的欺骗攻击到远程执行代码的安全问题。本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞共有 7 个，分别存在于 Hyper-V、Windows font library 以及 Visual Studio 中。除此之外，还包含多个重要（Important）漏洞。

【参考链接】

http://blog.nsfocus.net/microsoft201912/

2. Adobe 12 月安全更新

【概述】

当地时间 12 月 11 日，Adobe 官方发布了 12 月安全更新，修复了 Adobe 多款产品的多个漏洞，包括 Adobe Photoshop CC、Adobe Acrobat and Reader、Brackets 以及 Adobe ColdFusion 等。

【参考链接】

http://blog.nsfocus.net/%e3%80%90%e5%a8%81%e8%83%81%e9%80%9a%e5%91%8a%e3%80%91adobe-12%e6%9c%88%e5%ae%89%e5%85%a8%e6%9b%b4%e6%96%b0/

3. Gallium 威胁组织瞄准全球电信行业

【概述】

针对全球电信提供商的持续不断攻击活动由威胁组织 GALLIUM 发起，该活动在 2018 年到 2019 年中期活跃，GALLIUM 组织在攻击活动中利用未修补的漏洞攻击 WildFly/JBoss 应用程序服务器系统。

【参考链接】

https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

4. WaterBear 针对东亚的技术公司和政府机构

【概述】

WaterBear 是一项使用模块化恶意软件的活动，与网络间谍组织 BlackTech 有关，主要针对东亚（尤其是台湾、日本和香港）的技术公司和政府机构。在最近的一项攻击活动中，WaterBear 使用 API Hooking 技术将其网络行为从安全产品中隐藏起来。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection/

5. 勒索软件 Zeppelin 针对美国和欧洲的科技和医疗行业

【概述】

近期发现 Zeppelin 勒索软件针对欧洲和美国的科技、医疗保健公司的攻击活动。Zeppelin

是基于 Delphi 的勒索软件即服务系列新成员，最初被称为 Vega 或 VegaLocker，于 2019 年初首次发现。

【参考链接】

https://threatvector.cylance.com/en_us/home/zeppelin-russian-ransomware-targets-high-profile-users-in-the-us-and-europe.html

6. Trickbot 木马新变体 Anchor 的攻击活动与 Lazarus 组织有关

【概述】

Anchor 恶意软件专门针对金融目标，通过 DNS 进行通信，是 Trickbot 木马的一个新变体，其由多个部分组成，包括 anchorInstaller、anchorDeInstaller、AnchorBot、Bin2hex、psExecutor 和 memoryScraper。近期发现 Lazarus 组织使用 Anchor 发起针对一系列定向攻击活动针对金融、制造和零售业。

【参考链接】

https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/

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