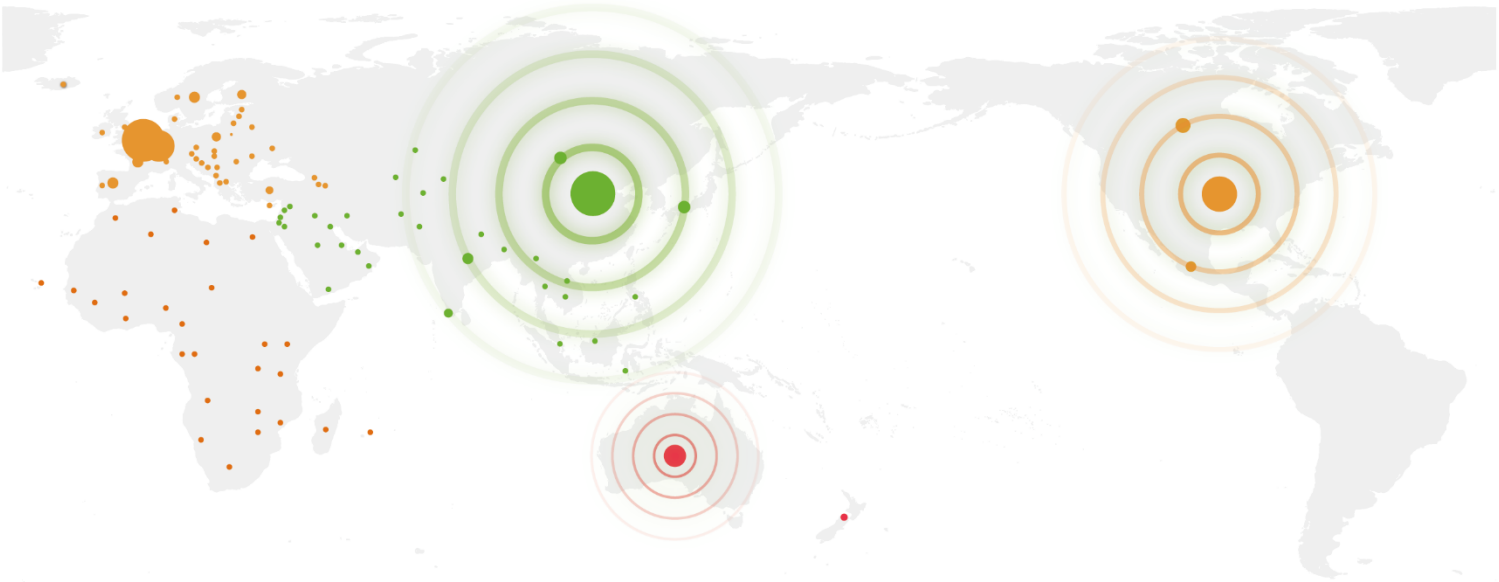
NSFOCUS

绿盟威胁情报周报

2019年第52周(12.23-12.29)



绿盟威胁情报中心(NTI)

本周热点概览

威胁通告

- Apache Log4j反序列化远程代码执行漏洞

暗网情报

- 2条金融行业暗网情报；
- 4条互联网行业暗网情报；

热点资讯

- 绿盟科技协助ABB修复PB610多个漏洞
- FIN7组织复盘分析
- APT20组织针对10个国家多个行业的战役
- Chrome浏览器一系列新漏洞Magellan2.0
- BIOLOAD工具利用DLL搜索顺序劫持

一、 威胁通告

- Apache Log4j 反序列化远程代码执行漏洞

  【发布时间】2019-12-25 19:00:00 GMT

  【概述】

  当地时间 12 月 19 号, Apache 官方发布了一则 Apache Log4j 存在反序列化可导致远程代码执行(CVE-2019-17571)漏洞的通告。Log4j 是美国阿帕奇（Apache）软件基金会的一款基于 Java 的开源日志记录工具。Log4j 1.2 版本中包含一个 SocketServer 类，在未经验证的情况下，该 SocketServe 类很容易接受序列化的日志事件并对其进行反序列化，在结合反序列化工具使用时,可以利用该类远程执行任意代码。

  【链接】

  http://blog.nsfocus.net/cve-2019-17571/

二、 暗网情报

分类	发现时间	暗网交易标题
金融	2019/12/21 14:11	30w 条某银行信用卡用户信息
金融	2019/12/23 00:40	某大额网贷数据 33800 条

互联网	2019/12/25 00:16	某电商手机卡销售数据 23w
互联网	2019/12/26 19:36	160 万某招聘网数据
互联网	2019/12/27 16:56	2019 年股民数据 700 多万条
互联网	2019/12/27 17:07	网贷投资人详细数据_含身份证银行卡

*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. 绿盟科技协助 ABB 修复 PB610 多个漏洞

【概述】

近日， ABB 发布了安全通告修复了 PB610 中的 4 个漏洞，影响 PB610 Panel Builder 600 2.8.0.424 及之前的版本。

Panel Builder 600 是由 ABB 推出的一款专业的 HMI 编程设计软件，通过该软件可以完成 HMI 的设计和安装，其中 ABB HMISimulator 是 HMI 模拟器，通过该模拟器可以在开发的时候进行仿真调试。本次修复的 4 个漏洞涉及 HMIStudio 以及 HMISimulator。

【参考链接】

http://blog.nsfocus.net/nsfocus-assists-abb-in-fixing-several-vulnerabilities-in-pb610/

2. FIN7 组织复盘分析

【概述】

绿盟科技伏影实验室对 FIN7 组织进行复盘分析，分为 part1 投递和执行、part2 木马和工具两部分。第一部分介绍 FIN7 多种投递技术；第二部分分析了该组织的木马与工具，包括 CARBANAK、TiniMet、DRIFTPIN、BOOSTWRITE。

【参考链接】

http://blog.nsfocus.net/fin7-review-analysis-part1-delivery-and-execution/

http://blog.nsfocus.net/fin7-review-analysis-part2-trojan-and-tools/

3. APT20 组织针对 10 个国家多个行业的战役

【概述】

Operation Wocao 被用来描述由与中国相关的威胁组织发起的战役，近日发现该活动针对巴西、美国、墨西哥、中国、法国、英国、德国、意大利、西班牙、葡萄牙的政府机构、托管服务提供商、能源、医疗保健和高科技等众多行业，活动由威胁组织 APT20 发起，该组织是一个与中国有关的威胁组织。

【参考链接】

https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf

4. Chrome 浏览器一系列新漏洞 Magellan2.0

【概述】

Google 修复了五个名为 Magellan 2.0 的 SQLite 漏洞，攻击者可以利用这些漏洞在 Chrome 浏览器中远程执行恶意代码。Magellan 2.0 是 SQLite 中存在的一些漏洞，Google Chrome 内部使用 SQLite 数据库来存储各种浏览器设置和用户数据。

【参考链接】

https://securityaffairs.co/wordpress/95633/hacking/chrome-magellan-2-0-flaws.html

5. BIOLOAD 工具利用 DLL 搜索顺序劫持

【概述】

近期发现 FIN7 组织的新工具 BIOLOAD，它与 BOOSTWRITE 具有通用的代码库，带有 Carbanak 后门，并具有嵌入的加密有效负载 DLL，攻击者可滥用 DLL 搜索顺序来加载恶意 DLL。FIN7 是一个有财务动机的威胁组织，自 2015 年以来主要针对美国零售、餐饮和酒店业。

【参考链接】

https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html

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