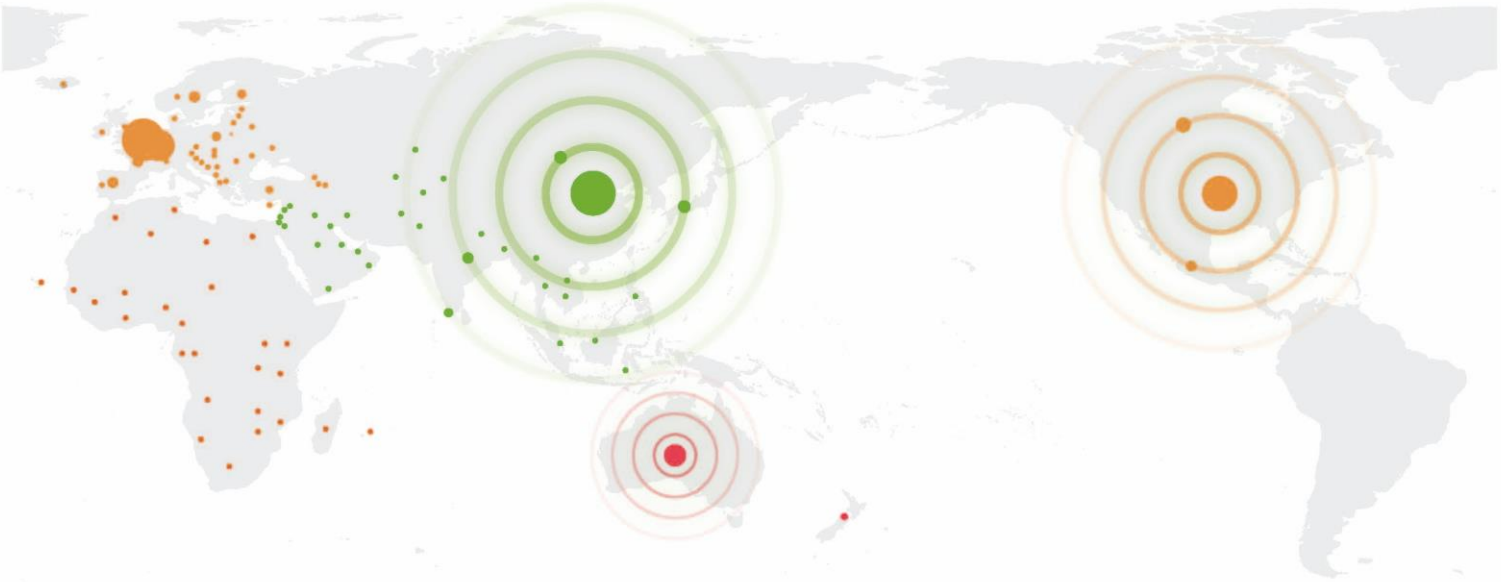
NSFOCUS

绿盟威胁情报周报

2020年第7周（2020.02.10-2020.02.16）



绿盟威胁情报中心（NTI）

本周热点概览

威胁通告

- 微软更新多个产品高危漏洞
- Django SQL注入漏洞

暗网情报

- 5条金融行业暗网情报，覆盖银行、证券和保险业
- 3条互联网行业情报

热点资讯

- Adobe 2月安全更新安全
- Apache Dubbo反序列化漏洞
- 美国政府机构披露朝鲜多个恶意软件家族
- Google从应用商店中删除了500多个恶意Chrome扩展程序
- Outlaw组织更新工具包针对更多系统进行挖矿
- 针对巴基斯坦人的网络间谍活动

一、 威胁通告

- 微软更新多个产品高危漏洞

  【发布时间】2020-02-13 10:40:00 GMT

  【概述】

  北京时间 2 月 12 日，微软发布 2 月安全更新补丁，修复了 100 个安全问题，涉及 Internet Explorer、Microsoft Edge、Microsoft Exchange Server、Microsoft Office 等广泛使用的产品，其中包括提权和远程代码执行等高危漏洞。

  【链接】

  http://blog.nsfocus.net/microsoft-releases-multiple-announcement-for-critical-threats/

- Django SQL 注入漏洞

  【发布时间】2020-02-13 11:00:00 GMT

  【概述】

  近日，Django 官方发布安全通告公布了一个通过 StringAgg（分隔符）的潜在 SQL 注入漏洞（CVE-2020-7471）。如果将不受信任的数据用作 StringAgg 分隔符，则部分版本的 Django 将允许 SQL 注入。通过将精心设计的分隔符传递给 contrib.postgres.aggregates.StringAgg 实例，可以打破转义并注入恶意 SQL。

  【链接】

  http://blog.nsfocus.net/django-sql-injection-vulnerability/

二、 暗网情报

分类	发现时间	暗网交易标题
金融	2020-02-08 13:39	88000 条 19 年活跃股民信息券商内部流出
金融	2020-02-07 22:50	全国保险数据 3600 万左右 31 个省分市可打包
互联网	2020-02-11 10:23	某社工库 120G 数据
金融	2020-02-11 22:31	银行卡数据 1809 条各大行银行卡数据含卡号等
互联网	2020-02-13 00:39	335w 全国宝妈数据 可用于幼教学前教育推广
互联网	2020-02-13 22:16	女性购物平台_某网购数据 16 万
金融	2020-02-13 16:08	2020 年第一批某证券短信拦截股民数据 38w
金融	2020-02-14 09:15	11 万 某网站会员数据账号密码手机

*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. Adobe 2 月安全更新安全

【概述】

当地时间 2020 年 2 月 11 日，Adobe 官方发布了 2 月安全更新，修复了 Adobe 多款产品的多个漏洞，包括 Adobe Experience Manager、Adobe Digital Editions、Adobe Flash Playe、Adobe Acrobat and Reader 以及 Adobe Framemaker 等。

【参考链接】

http://blog.nsfocus.net/%e3%80%90adobe-monthly-update%e3%80%91%e3%80%8aadobe-febuary-security-updates-report%e3%80%8b/

2. Apache Dubbo 反序列化漏洞

【概述】

近日，Chekmarx 团队的研究人员发现并公布了 Apache Dubbo 中存在的一个反序列化漏洞（CVE-2019-17564）。Apache Dubbo 是一款高性能 Java RPC 框架。当在 Dubbo 应用中启用了 HTTP 协议进行通信时存在该漏洞，攻击者可能提交一个包含 Java 对象的 POST 请求来完全破坏 Apache Dubbo 的提供者实例。

【参考链接】

http://blog.nsfocus.net/apache-dubbo-anti-sequential-vulnerabilitycve-2019-17564-security-threats-report/

3. 美国政府机构披露朝鲜多个恶意软件家族

【概述】

Cyber Command(美国网络司令部)、CISA(美国国土安全部下属网络安全和基础设施安全局)和 FBI(美国联邦调查局)在当地时间 2 月 14 日曝光朝鲜六个新恶意软件家族和一个恶意软件的更新，这些恶意软件分别是 BISTROMATH、SLICKSHOES、CROWDEDFLOUNDER、HOTCROISSANT、ARTFULPIE、BUFFETLINE 和 HOPLIGHT，并在 CISA 网站发布详细报告。CISA 将这些恶意软件归于朝鲜政府支持的黑客组织 Lazarus Group，即 HIDDEN COBRA，该组织是朝鲜最大、最活跃的黑客组织。

【参考链接】

https://twitter.com/USCERT_gov/status/1228305555908853760

https://www.us-cert.gov/ncas/analysis-reports

4. Google 从应用商店中删除了 500 多个恶意 Chrome 扩展程序

【概述】

经过思科 Duo Security 团队进行为期两个月的调查之后，Google 已从其官方网上商店中删除了 500 多个恶意 Chrome 扩展程序，删除的扩展程序通过在用户的浏览会话中注入恶意广告进行恶意攻击，扩展注入的恶意代码在特定条件下会激活，并将用户重定向到特定站点。这些扩展是一个已经开展了至少两年的大型恶意软件攻击活动的一部分。

【参考链接】

https://www.zdnet.com/article/google-removes-500-malicious-chrome-extensions-from-the-web-store/

5. Outlaw 组织更新工具包针对更多系统进行挖矿

【概述】

近期发现 Outlaw 攻击组织改进了扫描活动的规避技术，并通过杀死竞争对手和自己以前的矿工来提高了采矿利润，并对工具包的功能进行了更新，这些工具包旨在窃取汽车和金融行业的信息。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/outlaw-updates-kit-to-kill-older-miner-versions-targets-more-systems/

6. 针对巴基斯坦人的网络间谍活动

【概述】

针对巴基斯坦领土上实体和个人发现两个独立的攻击活动 The Spark Campaign 和 The Pierogi Campaign，两者都利用社会工程学，分别通过 Spark 和 Pierogi 后门感染受害者。此次攻击活动归因于 Gaza Cybergang 组织（也被称为 MoleRATs），该组织出于政治动机，自 2012 年以来一直在中东地区开展活动。

【参考链接】

https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one

https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-2-the-discovery-of-the-new-mysterious-pierogi-backdoor

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