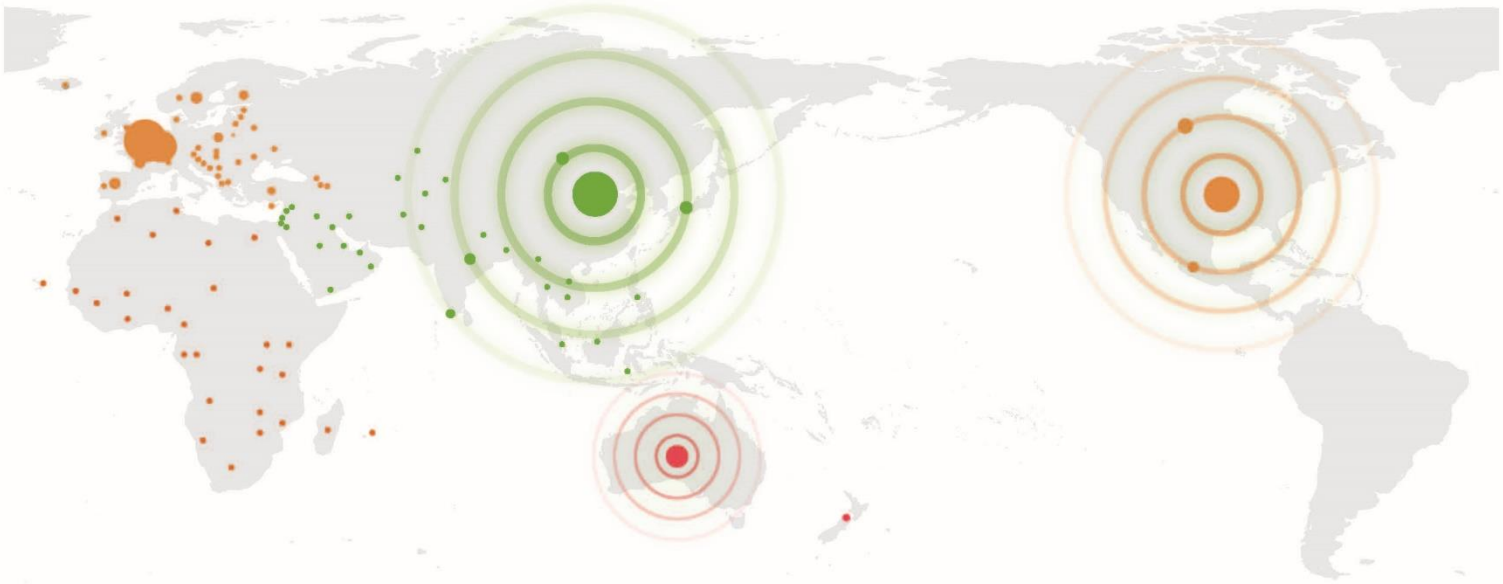
NSFOCUS

绿盟威胁情报周报

2020年第1周（2019.12.30-2020.1.5）



绿盟威胁情报中心（NTI）

本周热点概览

暗网情报

- 2条金融行业暗网情报；
- 5条互联网行业暗网情报；

热点资讯

- 2019 Botnet趋势报告；
- 移动恶意软件与APT活动；
- 微软诉讼与朝鲜有关的威胁组织；
- Maze勒索软件攻击美国电线电缆制造商；
- BRONZE PRESIDENT组织针对非政府机构的攻击；
- 新木马Lampion利用钓鱼邮件传播。

一、 暗网情报

分类	发现时间	暗网交易标题
互联网	2019-12-29 21:38	2018 年 8 月某贷款网贷借款数据 78663 条
互联网	2019-12-29 21:15	简历数据某招聘网站个人简历数据 373G
金融	2019-12-29 21:23	股民数据 26 万条上市公司证券股民数据
金融	2019-12-29 21:24	股民数据 2019 年 3 月份到 5 月份各大证券股民数据 22 万条
互联网	2019-12-29 21:29	网贷数据 2019 年 5 月 某借贷款审核用户数据 3W 条
互联网	2019-12-29 09:29	某社交平台 3100w+5000 游戏行业通讯录
互联网	2020-01-01 10:55	某财经网注册用户 72W 条，包含股民金融投资理财数据

*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

二、 热点资讯

1. 2019 Botnet 趋势报告

【概述】

通过对 Botnet 的持续研究和追踪，绿盟科技伏影实验室发布《2019 Botnet 趋势报告》，从入侵、传播方式和威胁种类及方式等方面深度剖析 2019 年 Botnet 威胁趋势。入侵与传播方面，弱口令、远程漏洞利用和钓鱼邮件依然是三种主要手段；Go 语言恶意软件组成的 Botnet 不断发展，爆破型家族 GoBrut 便是其中之一；DDoS 恶意家族进一步集中于少数几个家族，UDP 泛洪攻击比例有所上升；勒索家族持续谋取暴利，效仿者不断涌现，产业化程度不断加强；银行木马与勒索家族之间合作更加频繁，使得受害者同时面临多重安全风险；广告捆绑软件持续通过静默安装获利，同时也是传播恶意软件的重要渠道。

【参考链接】

http://blog.nsfocus.net/2019-botnet-nsfocus/

2. 移动恶意软件与 APT 活动

【概述】

BlackBerry 发布《移动恶意软件与 APT 活动》报告，报告分析 APT 威胁组织利用移动设备开展的网络间谍活动情况。按照地域划分，分析了已知和新发现的威胁组织进行的几次攻击活动。

【参考链接】

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/mobile-malware-and-apt-espionage-report.pdf

3. 微软诉讼与朝鲜有关的威胁组织

【概述】

近日微软起诉威胁组织 Thallium，并接到法院命令使其能够控制 Thallium 组织用于开展业务的 50 个域。通过次操作，这些站点将不再被用来执行攻击。Thallium 是一个来自朝鲜的威胁组织，以窃取敏感信息为目的，受害者包含政府人员、大学工作人员、关注世界和平和人权组织成员，主要针对美国、日本和韩国。

【参考链接】

https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercrime/

4. Maze 勒索软件攻击美国电线电缆制造商

【概述】

2019 年 12 月，美国电线和电缆制造商被攻击，攻击者非法访问其网络、窃取数据、加密计算机并在公布未支付赎金的数据，活动中利用 Maze 勒索软件窃取 120GB 的数据并加密了 878 台设备。

【参考链接】

https://www.bleepingcomputer.com/news/security/maze-ransomware-sued-for-publishing-victims-stolen-data/

5. BRONZE PRESIDENT 组织针对非政府机构的攻击

【概述】

BRONZE PRESIDENT 是一个与中国有关的威胁组织，至少从 2014 年开始活跃，该组织近期针对非政府组织以及东南亚国家的政治和执法组织进行网络间谍活动，攻击活动中同时使用专有和公开可用的工具，包括 PlugX、Cobalt Strike、ORat、RCSession、Nbtscan、Wmiexec 等。

【参考链接】

https://www.secureworks.com/research/bronze-president-targets-ngos

6. 新木马 Lampion 利用钓鱼邮件传播

【概述】

近期发现钓鱼邮件攻击活动传播名为 Lampion 的木马，邮件伪装成葡萄牙政府财政税收部门、以税收申报为主题诱导用户，一旦用户点击邮件中链接，就会下载包含 Lampion 木马的恶意压缩文件，该木马可收集计算机磁盘、打开的窗口、剪贴板和银行凭证的详细信息。

【参考链接】

https://seguranca-informatica.pt/targeting-portugal-a-new-trojan-lampion-has-spread-using-template-emails-from-the-portuguese-government-finance-tax/

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