近期中文钓鱼邮件攻击事件分析报告

——针对我国的 NanoCore RAT 恶意软件钓鱼邮件攻击事件分析报告

安天 CERT

初稿完成时间：2019 年 03 月 05 日 13 时 27 分

本版更新时间：2019 年 05 月 16 日 11 时 24 分

首次发布时间：2019 年 05 月 17 日 09 时 00 分

扫二维码获取最新版报告

目 录

1 概述

2019 年 2 月起，安天 CERT 发现大量由境外 IP 向我国用户邮箱发送的钓鱼邮件，邮件主题涉及“发票”、“采购”、“订单”等关键字，并且在邮件中包含同样关键字的恶意附件。经分析，还发现了大量相关类似的钓鱼邮件，但多数以英文“invoice”为邮件关键字。我们认为，该类攻击事件可能是全球范围内进行的黑产活动，其针对不同国家的目标时可能会编写对应语言文字的钓鱼邮件。

攻击者通过邮件传播恶意附件，最终载荷为.Net 语言编写并进行混淆的“NanoCore”[1]远控木马。“NanoCore”是一款功能强大的远程控制程序（RAT），可以对目标主机的文件、屏幕、进程等进行操作，还支持扩展功能插件。该木马由美国阿肯色州的 Taylor Huddleston 编写并出售（目前可在互联网上下载），该木马作者已于 2018 年 2 月被美国当局以创建和销售恶意软件罪判入狱 33 个月[2]。

2 攻击分析

2.1 攻击源（发件地址）

针对国内的钓鱼邮件主要有两类，一类的邮件主题为：“****采购订单”，附件名：“采购订单.7z”；另一类的邮件主题为“确认_发票****”，附件名：“发票支付.7z”。攻击者主要使用 juliet@goldwick.com.au 和 daniel@splashcad.com 作为发件地址。通过分析这两个邮箱所属公司网站的注册信息及页面内容来看，两个公司网站均为合法网站，均归属澳大利亚。攻击者使用的这两个邮箱，很可能是通过盗用、假冒或入侵网站后利用的邮箱。

goldwick.com.au 是一家澳大利亚的珠宝批发商网站，目前网站运营正常。

splashcad.com 是一家经营 CAD 产品的公司，网站位置和注册信息均在澳大利亚，网站状态正常。

2.2 攻击目标

该事件攻击的国内目标主要为电商平台、银行、高校等机构。其中收件人的邮箱地址基本是在网上公开过的邮箱，如公司的联系邮箱、客服邮箱、公开的个人邮箱等。这些邮箱疑似通过网页爬取而来，推测是大范围的撒网式攻击。

3 样本分析

该事件相关邮件较多，邮件内容类似，投递的恶意载荷只是名称和哈希不同，其主要功能行为都完全一致，因此我们提取其中一个典型样本进行分析。

3.1 样本标签

表 3-1 采购订单.exe 样本标签

病毒名称	Trojan[PSW]/MSIL.Heye
原始文件名	采购订单.exe
MD5	6786606813fb6fcf9e0828392215f4ba
处理器架构	Intel 386 or later processors and compatible processors
文件大小	333KB
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2019-02-20 00:57:22
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C#
VT 首次上传时间	2019-02-20 11:14:12
VT 检测结果	21/71

3.2 功能分析

样本是一个.Net 程序，它对部分字符串进行了混淆。程序入口点在 MyApplication，其中调用了 Form09，Form09 中解密了资源文件 w22B7azvmB2JvCA7N6HIBm8oMX…，该资源文件伪装成 Bitmap 格式。样本通过解密该资源文件，得到另一个.Net 程序并执行，程序再次解密自身的资源文件，得到最终的 NanoCore (1.2.2.0)版本的远控木马。

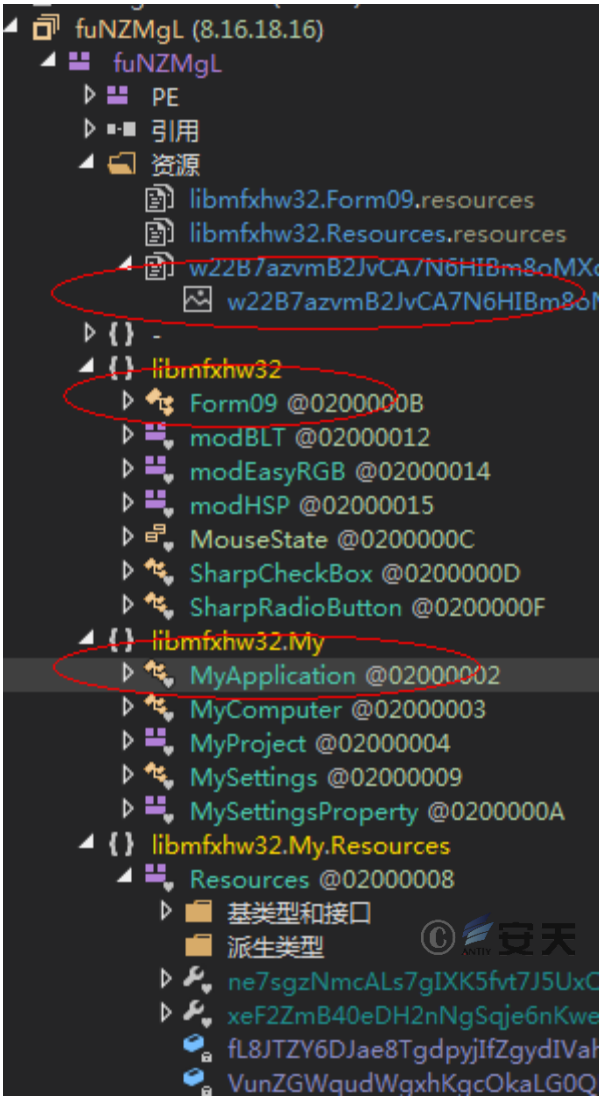

图 3-1 程序入口点 MyApplication

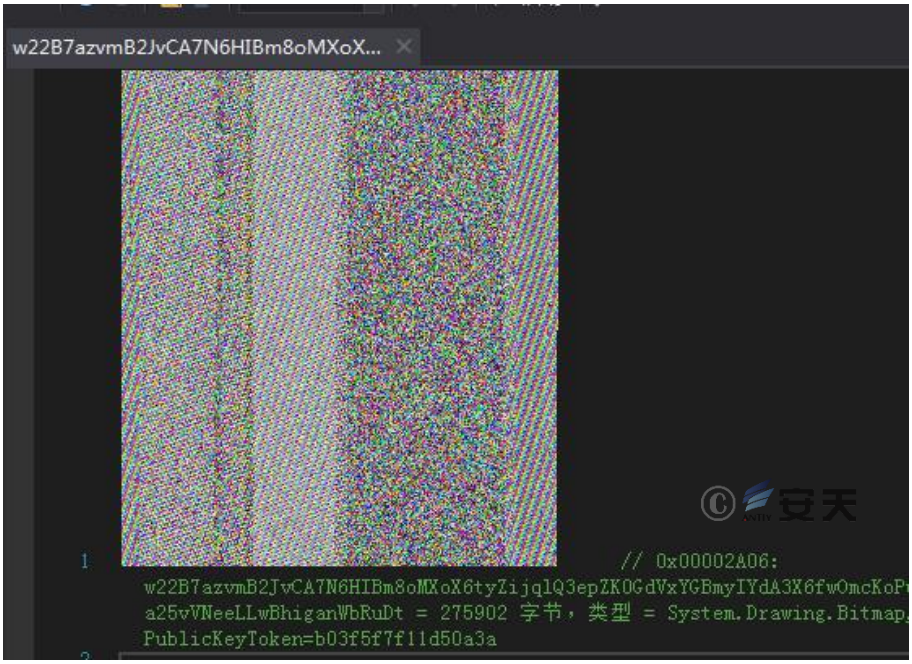

图 3-2 加密的资源文件

解密并运行资源文件的具体流程如下：

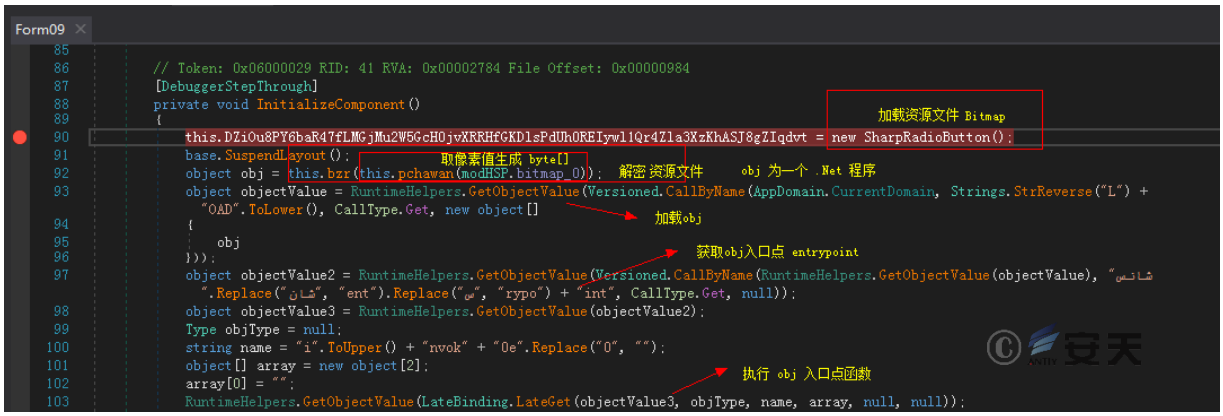

图 3-3 解密资源文件

解密算法为循环异或固定 key：

```
public byte[] bzr(byte[] n6QO4JGxfg7vHDZuhQqGG35n2R3LUcIDHonr5Uawd)
{
    checked
    {
        byte[] array = new byte[n6QO4JGxfg7vHDZuhQqGG35n2R3LUcIDHonr5Uawd.Length - 16 - 1 + 1];
        Array.Copy(n6QO4JGxfg7vHDZuhQqGG35n2R3LUcIDHonr5Uawd, 16, array, 0, array.Length);
        int num = array.Length - 1;
        for (int i = 0; i <= num; i++)
        {
            array[i] ^= n6QO4JGxfg7vHDZuhQqGG35n2R3LUcIDHonr5Uawd[i % 16];
        }
        return array;
    }
```

图 3-4 解密算法代码

从资源文件中提取出来的 obj 是一个.Net 程序，原名 CyaX.exe，样本标签如下：

表 3-2 CyaX.exe 样本标签

病毒名称	Trojan/Win32.Agent
原始文件名	CyaX.exe
MD5	C5F14514A290E31DAE7A0083A156B4E0
处理器架构	Intel 386 or later processors and compatible processors
文件大小	333KB
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2019-02-20 00:57:22
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C#
VT 首次上传时间	无
VT 检测结果	无

CyaX.exe 运行后，再次解密自身资源文件 YI3KSdM，得到 NanoCore 远控木马的 PE 文件，之后通过解析 PE 文件格式，取得入口点并执行：

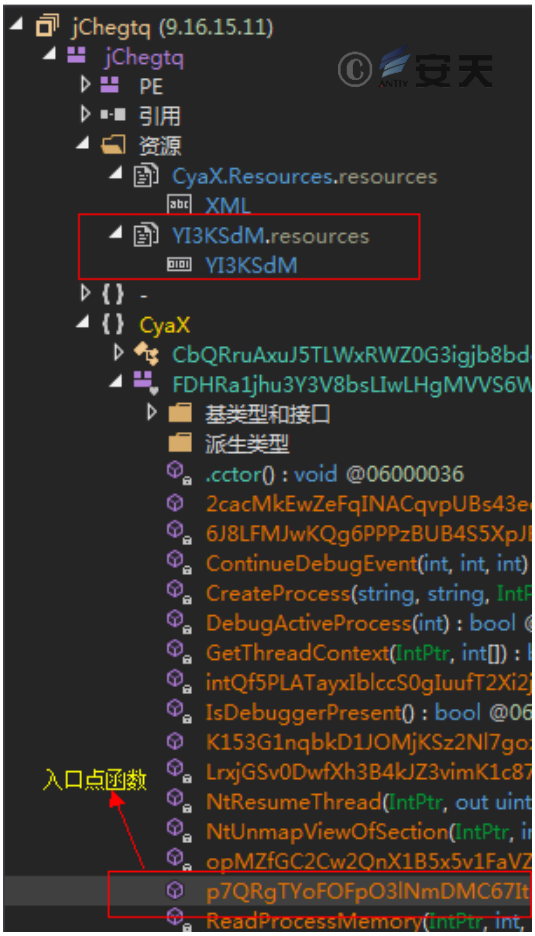

图 3-5 CyaX.exe 反编译代码

vjYpuWOAjMO8sjLffqr4ri2 是对 YI3KSdM 解密后，得到的 PE 文件：

```
private static byte[] vjYpuWOAjMO8sjLffqr4ri2 =
    syOQ5aJUJjhRdob556zKbZ83WJpBt24AATggh1KXBWE7OAux.AMFJ1iD45OSd2SUVMIdLw4ANtirAkiSWCxmpgtsh
    (syOQ5aJUJjhRdob556zKbZ83WJpBt24AATggh1KXBWE7OAux.eUnZiOKH5oRBFI6OpRxSOt0OUm3qoXYN1jFRhxdlUBGcCtzx5Y3e8TE4("YI3KSdM"));
```

图 3-6 资源解密函数

解密函数的算法与图 3-4 一样：

```
public static byte[] AMFJ1iD45OSd2SUVMIdLw4ANtirAkiSWCxmpgtsh(byte[]
  TNjj7UMaCPR7N1cHgNDZreFN5pmOdvOXc5fsFxMUj1BKFFD27Z4nQQdEsWzNuk7mqKS1Gaw37u)
{
    checked
    {
        byte[] array = new byte[TNjj7UMaCPR7N1cHgNDZreFN5pmOdvOXc5fsFxMUj1BKFFD27Z4nQQdEsWzNuk7mqKS1Gaw37u.Length - 16 - 1 +
          1];
        Buffer.BlockCopy(TNjj7UMaCPR7N1cHgNDZreFN5pmOdvOXc5fsFxMUj1BKFFD27Z4nQQdEsWzNuk7mqKS1Gaw37u, 16, array, 0,
          array.Length);
        int num = array.Length - 1;
        for (int i = 0; i <= num; i++)
        {
            array[i] ^= TNjj7UMaCPR7N1cHgNDZreFN5pmOdvOXc5fsFxMUj1BKFFD27Z4nQQdEsWzNuk7mqKS1Gaw37u[i % 16];
        }
        return array;
    }
}
```

图 3-7 解密算法与第一次解密相同

对 YI3KSdM 解密后，就会得到 Nanocore Client.exe 远控木马， 它被作为参数层层传递，最终在以下位置对它进行 PE 解析，找到入口点执行。

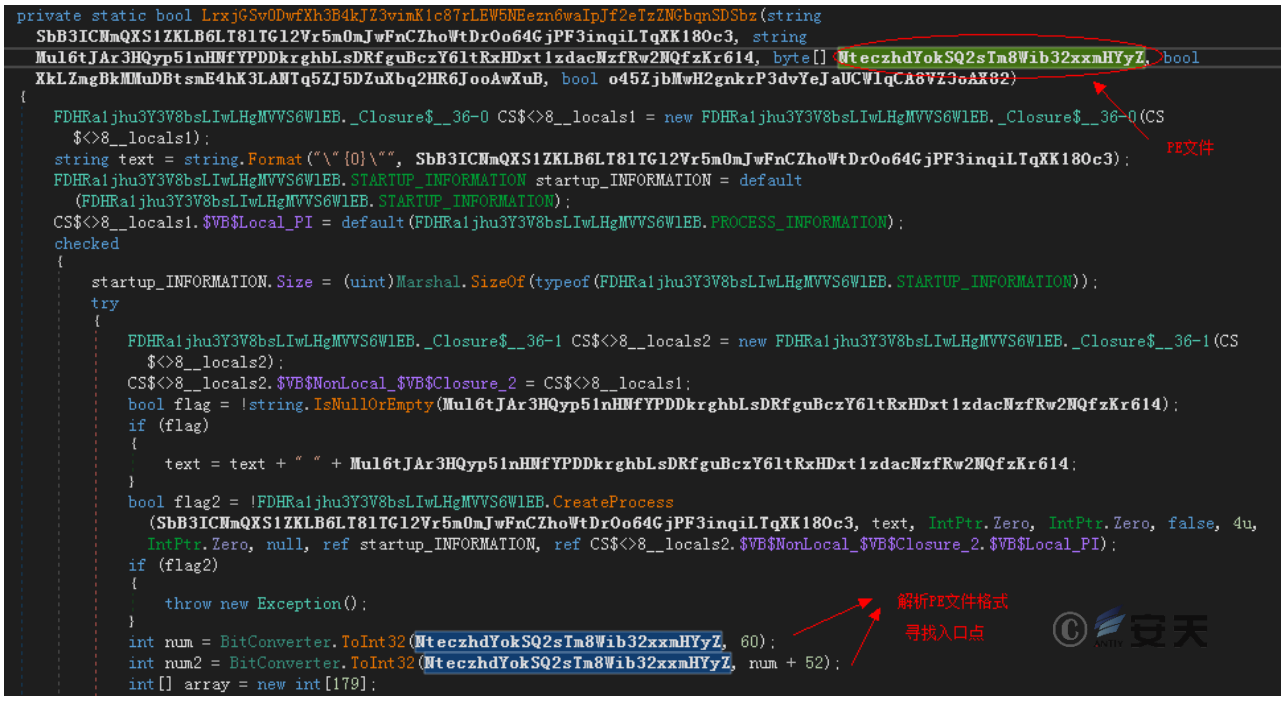

图 3-8 解密后的 Nanocore 木马

最终的 Nanocore 程序代码经过完全混淆以对抗逆向分析。通过原始项目名称可以看到木马版本号为 1.2.2.0，木马最终连接远程 C2：194.68.59.60:717。

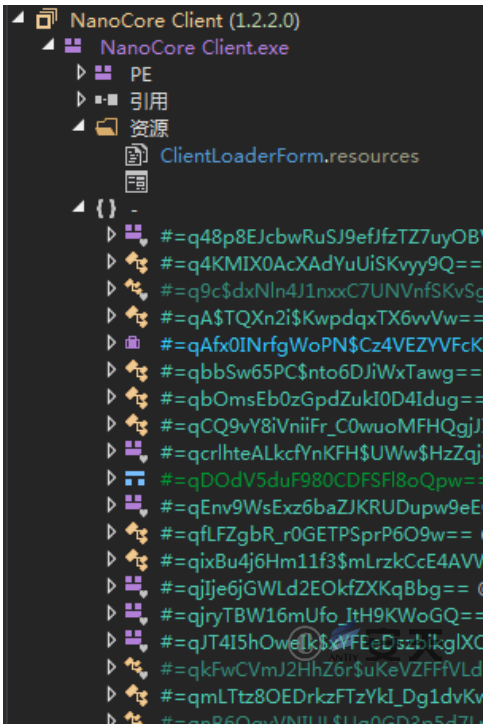

图 3-9 解密后的 NanoCore 远控木马反编译代码

3.3 植入特征

被植入此木马的机器会出现以下文件特征：

1. 在“%AppData%”目录下创建以本机 GUID 命名的文件夹，然后在该文件夹下创建两个子文件夹和几个文件。其中一个文件夹的命名随机生成，如“DHCP Manager”或“DSL Service”或“Manager”等，另一个文件夹为“Logs”。

2. 复制样本自身到的“DSL Service”文件夹下，重命名为“dslsv.exe”，并在注册表中添加启动项，设置该程序开机自启动。

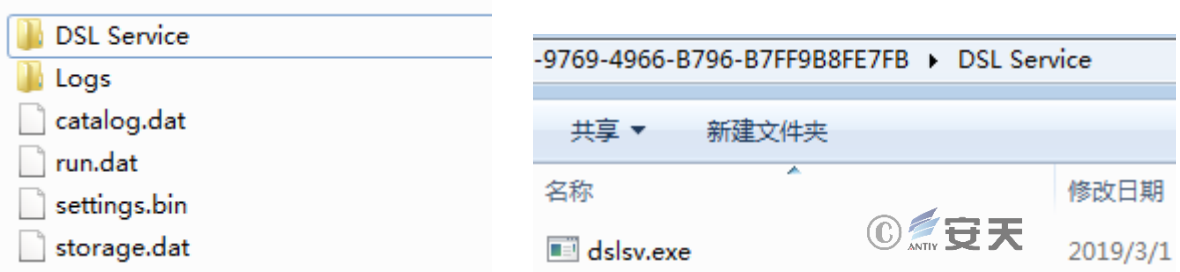

图 3-10 感染特征——衍生文件

3. “Logs”文件夹下会生成以当前登录用户命名的子文件夹，在该文件夹下有一个伪装成 Windows 更新日志文件的 KB_xxxxx.log ，此文件用来记录用户键盘输入的数据信息。

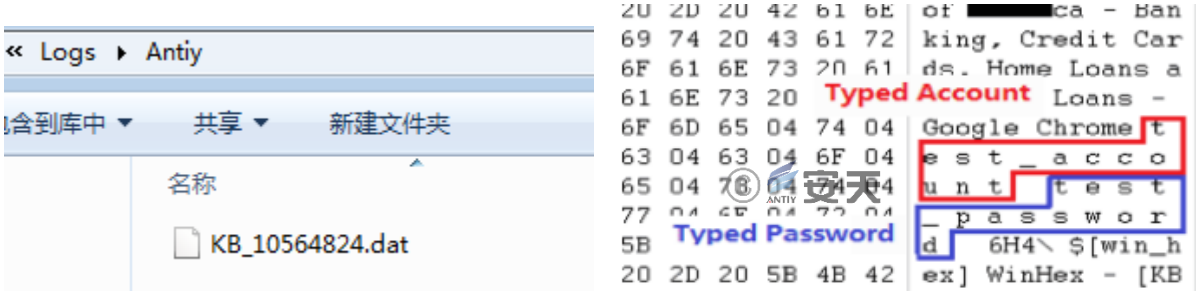

图 3-11 键盘记录存储文件

4. 定期尝试连接 C2 服务器 194.68.59.60:717，连接成功后接收指令进行相应操作。

3.4 NanoCore RAT

NanoCore 是一个.Net framework 编写的 RAT，首次出现于 2012 年，当前最新版本为 1.2.2.0。NanoCore RAT 的功能十分强大，它能够执行多种恶意操作，比如：文件操控、注册表编辑、进程控制、文件传输、远程命令执行、键盘记录、口令恢复等。

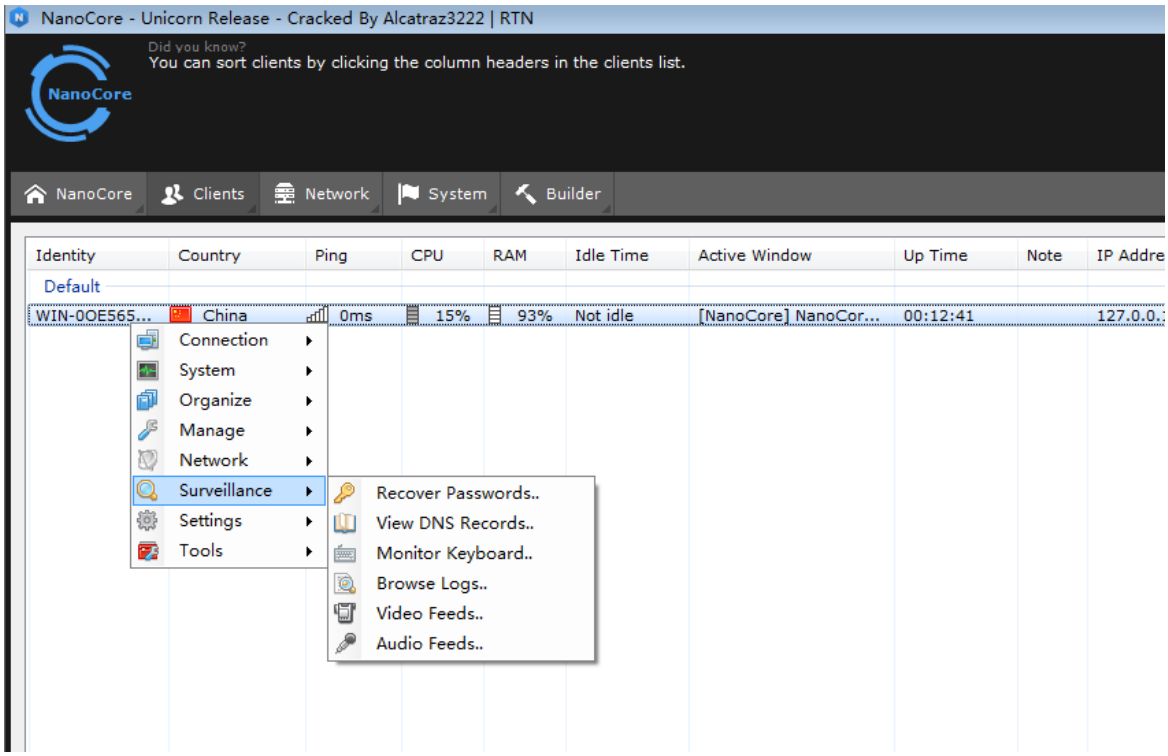

图 3-12NanoCore 控制端界面

4 关联分析

攻击者使用的 C2 服务器为 194.68.59.60，通过关联分析发现新的样本和域名，经分析确认与此事件属于同一组织/行动所为，这些样本应为通用性全球范围传播的样本（英文文件名），从样本的生成时间和域名

的解析时间可以看出该组织的攻击行动在持续活跃；从文件名称来看，其攻击活动可能是普适性（传统邮件钓鱼）而不是针对性的。

表 4-1 相关域名

解析时间	域名	IP/端口	检测结果
2019-02-07	mehkhan.ddns.net	194.68.59.60	C2
2019-04-25	podzz.ddns.net	194.68.59.60	C2

表 4-2 相关样本

原始名称	MD5	时间戳	域名/IP	类型
invoice.exe	17c67ffd368b3820d1aab2ed9d960d74	2019-02-05 21:32:06	mehkhan.ddns.net:3210	Nanocore 远控
invoice.exe	79fd9a76ac2a880c916b51ec416ab990	2019-02-14 13:24:47	194.68.59.60:717	Nanocore 远控
未知	1303b57d5e966270b2de73c8c0b599f4	SFX 默认时间	podzz.ddns.net:54984	Nanocore 远控
Text Twist.exe	5641d0712d7377d546ee640df32487e6	2019-03-19 04:12:35	194.68.59.60:333	Nanocore 远控
wetransfer.exe	243a188da9af32414b0fa254c62e77af	2019-03-24 22:59:45	194.68.59.60:333	Nanocore 远控
NJ.EXE	263fabec8661aebb4529813f099a6fd2	2019-02-27 23:19:00	podzz.ddns.net	Nanocore 远控
libmfxhw32.exe	1b65a1d91cc3618b24b3ddaca8398692	2019-02-21 02:05:55	194.68.59.60:717	Nanocore 远控
invoice19.exe	02a3b528e494ffedb36e6da635e6f230	2019-03-20 00:10:35	194.68.59.60:333	Nanocore 远控
vmkbd.exe	a6d19fdbc3f04c9b554e388dcb765246	2019-02-14 13:24:47	194.68.59.60:717	Nanocore 远控
invoice18-03-19.exe	6dab8c73b6cdf15c92fdc4f86da1c67b	2019-03-17 23:47:25	194.68.59.60:333	Nanocore 远控

5 小结

此系列攻击事件虽然与传统钓鱼邮件攻击手法类似，但其对国内的攻击目标单独构造了中文内容和文件名，且投递的样本是功能强大的远控木马，攻击成功后可能会产生严重威胁。同时需要我们警惕的是，不排除该事件可能像“乌克兰停电事件”[3]一样采用“黑色能量”作为后续攻击的前期预置环节，我方应予以重视，做好排查防范工作，谨防后续攻击。

附录一：参考资料

[1]. Stratosphere Lab：What do we know about NanoCore RAT? A review.

https://www.stratosphereips.org/blog/2018/9/7/what-do-we-know-about-nanocore-rat-a-review

[2]. Bleepingcomputer：Nanocore RAT Author Gets 33 Months in Prison

https://www.bleepingcomputer.com/news/security/nanocore-rat-author-gets-33-months-in-prison/

[3]. 安天：乌克兰电力系统遭受攻击事件综合分析报告

https://www.antiy.com/response/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage.html

[4]. Symantec：NanoCore: Another RAT tries to make it out of the gutter

https://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter

[5]. Palo Alto Networks：Operation Comando: How to Run a Cheap and Effective Credit Card Business

https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/

附录二：关于安天

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户筑起可对抗高级威胁的网络安全防线。

安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。参与了 2005 年后历次国家重大政治社会活动的安保工作，并多次获得杰出贡献奖、安保先进集体等称号。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。其中，安天的移动检测引擎是第一个获得权威国际评测奖项的中国产品。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情

想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天实验室更多信息请访问： *http://www.antiy.com*（*中文*）

http://www.antiy.net（*英文*）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*