Overview

The Andariel gang is classified by the Korean Financial Security Institute as a subgroup of the Lazarus APT group. The group mainly attacks South Korean organizations, especially financial institutions, for financial gain and cyber espionage.

Recently, the Red Raindrop team of Qi'anxin Threat Intelligence Center captured a batch of Andariel-related attack samples in daily threat hunting, all of which are PE executable files. According to the time when this batch of samples was uploaded to VT, it can be seen that the related attack activities have been launched since at least February this year.

Attack samples can be divided into two categories: one is a loader that decrypts and loads subsequent payloads in memory, and the loaded content includes backdoors and browser stealing programs; the other is a downloader written in Go language, which sends back to the C2 server The collected host information then downloads the PE file and executes it. Most Go downloaders currently still have low single-digit detections on VT, which may be one reason why attackers choose Go to develop their malware.

Sample information

The information of malicious samples of the loader class captured this time is as follows.

MD5	file type	VT first upload time
079b4588eaa99a1e802adf5e0b26d8aa	pe exe 64-bit	2022-04-20 03:59:13 UTC
47791bf9e017e3001ddc68a7351ca2d6	pe exe 64-bit	2022-04-21 08:37:27 UTC
1875f6a68f70bee316c8a6eda9ebf8de	pe exe 64-bit	2022-04-22 04:43:01 UTC

The downloader malicious sample information is as follows.

MD5	file name	file type	VT first upload time
5be1e382cd9730fbe386b69bd8045ee7	iexplore.exe	pe exe 64-bit	2022-04-22 02:10:17 UTC
2e18350194e59bc6a2a3f6d59da11bd8	-	pe exe 32-bit	2022-02-04 18:48:06 UTC
3bd22e0ac965ebb6a18bb71ba39e96dc	scsetup_original.exe	pe exe 32-bit	2022-02-05 07:10:11 UTC
17c46ed7b80c2e4dbea6d0e88ea0827c	OneNoteAuth.exe	pe exe 32-bit	2022-02-08 09:40:17 UTC
85f6e3e3f0bdd0c1b3084fc86ee59d19	OneNoteAuth.exe	pe exe 32-bit	2022-02-18 08:06:41 UTC

Sample analysis

Loader

Taking the sample 079b4588eaa99a1e802adf5e0b26d8aa as an example for analysis, the core functions of the loader are as follows.

The API string and subsequent payloads are decrypted by the methods of the CryptoXor class in the program, and the decryption operation is completed by the function sub_140001220.

The encrypted subsequent payload is placed at the end of the file, and is located by summing the length of the original file header and the length of each segment. Taking this sample as an example, the data of the last segment of the sample ends at 0x26800, and the 4 bytes starting from the file offset 0x26800 indicate the length of the subsequent payload, here is 0x41e00, followed by the encrypted payload.

Subsequent payload decryption to obtain PE file

Call the function sub_140004AA0 to load and execute the PE file in memory.

PE is a backdoor program, and DES decrypts three strings to obtain the IP address of the C2 server. The actual effective IP is 109.248.144.155, and the ports are 8443 and 8080.

The backdoor has 7 functions, each of which is implemented as a C++ class. The names of each class and the corresponding main functions are as follows.

Backdoor function class name	The main function
ModuleUpdate	self delete
ModuleInformation	Get all kinds of information about the host
ModuleShell	Remote shell, command execution
ModuleFileManager	file management
ModuleKeyLogger	keylogging
ModuleSocksTunnel	Create proxy relay
ModuleScreenCapture	screenshot

样本1875f6a68f70bee316c8a6eda9ebf8de内存加载的PE同样也是后门，C2服务器为“mail.usengineergroup.com”，连接端口为8443，域名解析的IP为109.248.144.136，与前面提到的C2服务器IP地址在一个C段网络中，后门功能包括除ModuleKeyLogger之外的6种。

样本47791bf9e017e3001ddc68a7351ca2d6加载的PE主要功能为窃取Opera和Chrome浏览器中保存的密码。

下载器

通过C2服务器109.248.144.155，我们发现了另一个与之通信的攻击样本，该样本为Go语言开发的PE文件，样本信息如下。

文件名	iexplore.exe
MD5	5be1e382cd9730fbe386b69bd8045ee7
C2	hxxp://109.248.144.155/login.php

样本首先隐藏程序的控制台窗口，检查互斥量"obtaink_shrimp"。设置全局变量main_gstrIniFilePath为”thumbcache_2022.db”的文件路径，该文件用来保存样本采集的主机信息。

如果thumbcache_2022.db文件存在，则样本直接从文件中提取主机信息，否则收集主机信息，并保存在该文件中。

样本通过调用bcdedit程序的执行结果判断当前用户是否具备管理员权限。该系统程序只有具备管理员权限的用户才能正常运行。

如果用户具备管理员权限则通过添加计划任务实现持久化，计划任务的名称为"Microsoft\\Windows\\Nahimic Interface Coperation"。对于普通用户则调用powershell在开机自启动目录下添加链接文件实现持久化，链接文件名称为“OneNoteAuth.lnk”。

收集的主机信息包括：主机名和用户名、操作系统版本与位数、杀软信息、MAC地址、局域网IP地址。每种信息经过base64编码之后再用”|”分隔从而拼接在一起，拼接后的字符串保存在全局变量main_gstrPCInfo中，写入thumbcache_2022.db文件中的主机信息用换行符分隔。

在函数main_GetVaccineInfo中，杀软信息通过释放的powershell脚本“detectav1.ps1”获取。

获取到主机相关信息后，进入循环，通过main_ClientThrea函数与C2通信。向hxxp://109.248.144.155/login.php发送POST请求回传主机信息，主机信息拼接在”mem_id=1260&data=”之后。

从C2获取后续载荷写入全局变量main_gstrSecondTroyPath指向的文件路径，文件名为“NahimicInterface.exe”，并修改文件开头两字节为”MZ”，然后执行该文件。由于URL现已无法访问，故无法获取到后续载荷进行分析。

溯源关联

根据代码相似性，可以将这批攻击样本归属到Lazarus组织下属团体Andariel。加载器样本对应Kaspersky在2021年6月披露Andariel攻击活动报告[1]中的第三阶段载荷，不过解密内嵌载荷的方式有些不同。

在本次捕获的下载器样本所加载的后门中，C2地址通过DES解密得到，后门以TCP连接C2通信时，会发送字符串”HTTP 1.1 /index.php?member=sbi2009 SSL3.3.7”，可能是为了伪装为https流量。

Kaspersky在报告中提到Andariel所用后门的三个C2地址通过DES解密得到，在连接C2时会发送字符串”HTTP 1.1 /member.php SSL3.4”，这些都与此次捕获到的下载器样本相符，并且也有相同的后门指令。

另外，本次捕获的下载器样本也与Anlab在2021年11月披露Lazarus攻击工具的报告[2]中提到的一类下载器相似。该下载器回传给C2的数据格式同样是将收集的各类主机信息经过base64编码后再用”|”符号拼接起来。

总结

基于代码相似性，可以认为本次捕获到的加载器和下载器攻击样本来自Lazarus APT组织，攻击者开始借助Go语言编写恶意软件以避开安全软件的检测，不过目前暂不清楚相关攻击活动针对的具体目标和发起初始攻击的入口点。

APT组织攻击一直以来对于国家和企业来说都是一个巨大的网络安全威胁，通常由某些人员精心策划，针对特定的目标。出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性进行攻击。

因此，奇安信红雨滴团队在此提醒广大用户，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行夸张标题的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁。

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOCs

MD5

079b4588eaa99a1e802adf5e0b26d8aa

47791bf9e017e3001ddc68a7351ca2d6

1875f6a68f70bee316c8a6eda9ebf8de

5be1e382cd9730fbe386b69bd8045ee7

2e18350194e59bc6a2a3f6d59da11bd8

3bd22e0ac965ebb6a18bb71ba39e96dc

17c46ed7b80c2e4dbea6d0e88ea0827c

85f6e3e3f0bdd0c1b3084fc86ee59d19

bdece9758bf34fcad9cba1394519019b

d0e203e8845bf282475a8f816340f2e8

5130888a0ad3d64ad33c65de696d3fa2

b1c1d28dc7da1d58abab73fa98f60a83

5c6f9c83426c6d33ff2d4e72c039b747

C2

109.248.144.155: {8443, 8080}

mail[.]usengineergroup.com (109.248.144.136:8443)

hxxp://109.248.144.155/login.php

hxxp://155.94.210.11/covid/login.php

hxxp://45.57.245.17/member/login.php

hxxp://193.56.28.32/voris/view.php

Reference link

[1] https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

[2] https://asec.ahnlab.com/wp-content/uploads/2021/11/Lazarus-%EA%B7%B8%EB%A3%B9%EC%9D%98-NukeSped-%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84 %9C.pdf

Click to read the original text to ALPHA 5.0

Immediately assist in threat analysis