索伦之眼

09月09, 2016

核心安全事业部-追日团队

报告更新相关时间节点:

- 2016年6月27日，形成样本分析报告
- 2016年7月15日，形成攻击行动报告简版
- 2016年8月10日，剔除修改部分内容
- 2016年9月7日，添加补充相关内容
- 2016年9月18日，修改部分内容

文章目录

披露申明

本报告中出现的IOC（Indicators of Compromise，

威胁指标），进一步包括涉及到相关攻击事件的样本文件MD5等哈希值、域名、IP、URL、邮箱等威胁情报信息，由于其相关信息的敏感性和特殊性，所以在本报告中暂不对外披露，在报告中呈现的相关内容（文字、图片等）均通过打码隐藏处理。

若您对本报告的内容感兴趣，需要了解报告相关细节或相关IOC，可与360追日团队通过电子邮件进行联系，另外我们目前只提供电子邮件联系方式：360zhuiri@360.cn，敬请谅解！

一、 概述

索伦之眼组织（APT-C-16），又称Sauron、Strider。该组织主要针对中国、俄罗斯等多个国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到2010年，至今还非常活跃。

索伦之眼组织攻击中使用了大量的恶意代码，截止到目前360已捕获到291个。在攻击过程中通过利用Windows域和劫持某安全软件升级程序来实现横向移动。

该组织整个攻击过程中是高度隐蔽，且针对性极强，对特定目标采用定制的恶意程序或通信设施，不会重复使用相关攻击资源。相关恶意代码复杂度可以与方程式（Equation）媲美，其综合能力不弱于震网（Stuxnet）、火焰（Flame）等APT组织。该组织是我们今年披露的APT组织中综合能力最高的一个。

关于索伦之眼组织目前已公开相关报告信息汇总：

公开时间	报告名称	公司

公开时间	报告名称	公司
2016年8月7日	Strider: Cyberespionage group turns eye of Sauron on targets [1]	Symantec
2016年8月8日	ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms [2]	Kaspersky

表 1安全厂商针对索伦之眼发布的相关报告汇总列表

二、 中国受影响情况

我们将统计索伦之眼组织从2010年开始至今的活跃情况。

1. 行业分布：主要针对政府机构、科研教育

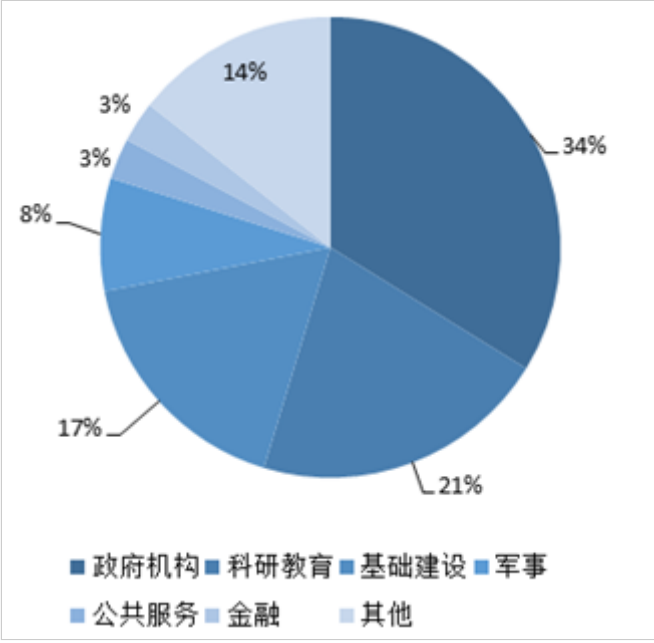

图 2主要针对行业分布

索伦之眼组织主要关注科研教育和军事领域，其中值得我们注意的是该组织还特别关注基础建设相关领域，如：水利、海洋等。

2. 目的：窃取敏感数据

窃取指定文件扩展名的文件，在针对中国地区的攻击中，其中以窃取文档文件为主，进一步主要包括微软Office、OpenOffice和中国本土的WPS Office。

另外是收集目标环境基本信息，其意图主要是为了后续攻击收集情报信息。相关基础信息主要包括驱动器卷信息，当前用户信息，当前所有的进程，所有已安装程序，服务，用户列表，网络信息和状态，开放端口以及本机外网IP等。

最后还会收集浏览器相关信息，如浏览器历史记录。另外还会收集浏览器相关设置信息，如默认主页、安全策略等。

类型	产品	扩展名	360	卡巴斯基
密钥类	PuTTY	.ppk	✓	✓
		.rsa	×	✓
		.key	×	✓
文档类	Microsoft Office	.doc	✓	✓
		.docx	✓	✓
		.ppt	✓	✓
		.pptx	✓	✓
		.xls	✓	✓
		.xlsx	✓	✓
		.vsd	✓	✓
		.vsdx	✓	×
		.rtf	✓	✓
		.one	×	✓
	OpenOffice	**.ods**	✓	×
		.odt	✓	×
		.odp	✓	×
	Adobe Reader	.pdf	×	✓
	WPS Office	**.wps**	✓	×
		.txt	✓	✓
压缩包类		.rar	×	✓
邮箱类	Microsoft Outlook Express	.wab	×	✓
其他		.dst	×	✓
		.FTS	×	✓
		.rpt	×	✓
		.conf	×	✓
		.cfg	×	✓
		.pk2	×	✓
		.nct	×	✓
		.psw	×	✓
		~WPL*.tmp	×	✓

表 2相关窃取文件的扩展名汇总列表

```
ILP_TAG_PATTERN = "arsex%sxauto"
EXTENSIONS = "rtf|txt|ods|odt|odp|ppk|wps|doc|docx|xls|xlsx|ppt|pptx|vsd|vsdx"
STATE_FILE = "~FHAFFG.tmp"
```

图 3 VFS（类型6）的Lua脚本部分截图

三、 索伦之眼攻击平台

索伦之眼攻击平台是非常高端的模块化平台，其技术复杂度可与方程式（Equation）等顶级APT媲美。

1. 整体结构

索伦之眼将各种功能模块都封装成为一个Blob，高度组件化，并利用多种方式进行传输，比如：以一个单独文件的方式，将shellcode写入某个注册表的表项中，或者利用管道和各种通讯协议进行传输。所有的模块都使用强加密算法进行加密，比如：RC4、RC5、RC6、AES、Salsa20等。Blob被调用时会在内存中释放出一个预编译的脚本和数量不定的模块dll，这些模块dll的命令和Unix/Linux上的命令的风格很相似。开发者还通过修改Lua脚本引擎对字符串统一使用Unicode编码，平台的核心模块通过执行释放出的预编译Lua脚本来调用各个模块dll实现具体功能。

Blob作为攻击平台的一种组件格式，实际就是二进制数据,通常用来封装具体的功能，在其内部采用VFS进行管理组织。

下面是一个Blob从传输到最后释放出真正的功能模块的过程，以及Lua脚本和dll的调度关系：

图 4具体执行过程

图 5调度关系

2. 持续攻击

索伦组织针对中国地区的攻击，最早可以追溯到2010年。

3. 横向移动

1) 利用Windows域服务器

什么是Active Directory域服务[3]

使用 Active Directory(R) 域服务 (AD DS) 服务器角色，可以创建用于用户和资源管理的可伸缩、安全及可管理的基础机构，并可以提供对启用目录的应用程序（如 Microsoft(R) Exchange Server）的支持。

AD DS 提供了一个分布式数据库，该数据库可以存储和管理有关网络资源的信息，以及启用了目录的应用程序中特定于应用程序的数据。 运行 AD DS 的服务器称为域控制器。 管理员可以使用 AD DS 将网络元素（如用户、计算机和其他设备）整理到层次内嵌结构。 内嵌层次结构包括Active Directory林、林中的域以及每个域中的组织单位 (OU)。

安全性通过登录身份验证以及对目录中资源的访问控制与 AD DS 集成。 借助单点网络登录，管理员可以管理其整个网络中的目录数据和组织。 授权网络用户还可以使用单点网络登录访问网络中任意位置的资源。

攻击流程

图 7 攻击流程

- 步骤a：攻击者首先攻陷域服务器，获得相关读写权限；
- 步骤b：将thumb.db,iphlpapi.dll放入域共享SYSVOL目录：“SystemRoot\SYSVOL\Sysvol\DomainName\Scripts”，将logon.exe,logoff.exe放入：

“SystemRoot\SYSVOL\Sysvol\DomainName\Policies{GUID}\MACHINE\Scripts\Startup\”

- 步骤c：用户登录域控制器所管理的机器时，自动执行logon.exe。logon.exe的主要功能是如果“%temp%\MpCmdRun.dat”不存在，则将“\{DomainName}\SYSVOL{DomainName}\scripts\thumb.db”添加为计划任务后立即执行，且只执行一次。如果“%temp%\MpCmdRun.dat”存在，则直接退出。thumb.db与iphlpapi.dll功能相同，可以认为thumb.db是iphlpapi.dll更新替代版本。
- 步骤d：用户注销域控制器所管理的机器时，自动执行logoff.exe。logoff.exe首先判断“%temp%\MpCmdRun.dat”是否存在，如果不存在，则通过rundll32.exe执行thumb.db的GUID导出函数。如果“%temp%\MpCmdRun.dat”存在，则直接退出。

thumb.db和iphlpapi.dll的主要功能是查找域共享目录下以下文件，并解密执行窃取用户信息的主要模块：

```
\\{ DomainName}\SYSVOL\{DomainName}\Policies\Gpt.ini
 \\{ DomainName}\SYSVOL\{DomainName}\scripts\GptTmpl.ini
```

另外由于缺失部分文件，所以相关攻击细节无法确认，下表是缺失的文件列表：

相关文件	推测相关功能
%temp%\MpCmdRun.dat	未知
policies\Gpt.ini	窃取用户信息主要模块
scripts\GptTmpl.ini	窃取用户信息主要模块

表 4缺失文件列表

2) 劫持某安全软件升级服务器

索伦组织至少从2010年开始至2014年，就一直通过劫持某安全软件网络版升级程序进行横向移动攻击， 通过对相关攻击事件的分析，我们推测出了可能的攻击流程。

攻击流程

- 步骤a：攻击者首先需要获得目标内网环境的A服务器权限，该A服务器是作为安全软件服务端，主要对内网其他客户端进行更新升级。
- 步骤b（服务端）：攻击者会将A服务器上的更新程序替换为恶意程序，进一步修改升级配置文件“index.dat”，需要和恶意程序的信息匹配，以便通过客户端的升级校验。最后攻击者可以选择目标客户端机器进行定向安装升级，升级成功后恶意代码下发并执行。
- 步骤b（客户端）：当恶意代码成功植入之后，会修改客户端的配置文件“Svr.ini”，将升级地址修改为指定地址，我们推测该地址与A服务器内网地址一致。
- 步骤c：注入进程winlogon.exe实现监听指定地址，该地址有可能是A服务器的地址，也有可能是另外一台内网服务器，也有可能直接指向外网C&C地址。
- 步骤d：在部分恶意代码中，会收集客户端系统信息，并将相关信息写入index.dat或index.ini，并上传到A服务器。

4. 具体功能模块

1) VFS

一个Blob模块通常包括Payload和VFS Data 两部分，VFS Data中存放着实际的功能模块，通过虚拟文件系统（VFS）进行管理，这样攻击者就可以非常方便的管理各个功能模块，而将其他通用的固定功能都存放在Payload中。

在VFS中主要包括了预编译的Lua脚本和要使用到的各个功能DLL模块，某些样本中还保存着一个或多个Blob模块。VFS采用了RC4或Salsa20加密并用Zlib进行了压缩，每个VFSFILE拥有独立的密钥。作者修改了Lua解释器对其中的字符串统一使用Unicode编码。在这个模块中各个具体的功能都被作为插件封装到一个模块dll中然后通过Lua脚本进行调用执行，Lua脚本在整个攻击组件中处于核心组织者的地位。

图 16 VFS的结构

目前已知的功能插件总共85个，其中以下15个是我们首次发现，其他厂商尚未披露的。

插件名称	功能描述
battery	获取电池信息
cmdump	获取密钥信息
drives	获取磁盘盘符列表
iehist	获取IE浏览历史记录
injchk2	获取装的杀软列表
ip	获取当前IP列表
modini	修改配置文件
nc	通过使用TCP或UDP协议的网络连接去读写数据
pipe pipe	管道读写
printer	枚举可用的打印机
set	设置环境变量
shortcut	遍历目录如果是.lnk的则直接输出源路径

插件名称	功能描述
who	获取用户的SID
wtc2	端口转发，将本地端口转发至远程服务器端口
start	创建进程

表 8部分功能插件列表

2) Pipe_RPCHlpr

该模块是一个名称为RPCHlpr的系统服务主要用来进行管道通讯。

首先会检测SID判断权限，当符合条件后会继续运行创建一个线程在这个线程中创建名为” \.\pipe\rpchlp_0”的命名管道等待连接，当成功连接后会再次创建线程进行通信,接收命令。然后会继续创建3个管道分别为：“\.\pipe\rpchlp_1”，“\.\pipe\rpchlp_2”和“\.\pipe\rpchlp_3”等待连接；根据获取的命令远程加载执行Blob或创建相应的进程

图 17功能分支图

3) pipe_NullSession

检测[HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters] NullSessionPipes 是否已经存在键值{2A37B052-7AB2-4fde-9536-D1DD8D4A8260}，如果在这个配置列表中没有则会更新进去。

主要功能是读取，根据条件删除、写入、遍历目录、删除文件和加载Blob并执行等。

4) NetListener

该模块解密后一般会解密出1-3个dll，其中包括一个主模块和1-2个插件模块。主模块解密配置文件，创建一个socket并创建线程监控路由和IP地址的变化，接着调用插件模块监听网络，插件将接收到数据包交给核心模块来处理，核心模块会用public key对数据包头进行解密校验，如果符合条件才会解密剩下的部分并用CRC32进行校验。根据接收的命令该模块可以执行文件，加载插件或进行网络通讯；该模块可以支持PcapUdp、PcapTcp、Pcap、 Icmp、Dns、Raw、Pipe、Http等协议

5) Backdoor_A

通过样本文件的导出函数,推断该模块应该通常伪装为Security Providers ,在这个模块中shellcode中主要包含两个功能模块。第一个模块就是一个后门组件，通过根据配置文件中的内容和远程CC服务器进行HTTP通信，进行上传下载数据操作。第二个模块的主要功能就是进行删除清理操作。

6) Blob加载器

通常伪装为系统dll（例如：wtsapi32.dll,iphpapi.dll）进行dll劫持，读取事先在指定目录中存放的Blob文件进行解密，然后进行校验如果条件符合就会加载此Blob并运行。

图 18伪装wtsapi32.dll

7) 其他类型

以下类型我们目前暂未发现，相关功能卡巴斯基曾报告过。

5. C&C

外网

为每个被攻击目标单位配备专属C&C，不同单位之间不会存在C&C共用的情况。进一步针对同一单位的不同的计算机终端，大部分也采用不同的C&C，少量会存在C&C复用的情况。

内网

这里主要是横向移动环节，利用Windows域和某安全软件升级服务器的相关恶意代码，其中的Lua脚本一般都内置内网IP。进一步还存在不同网段的内网IP之间进行通信。

四、 关联分析

1. 与方程式、Regin对比

表 20 索伦与其他APT对比分析

2. 样本同源性分析

Blob 是恶意攻击平台的一种组件格式，在索伦中我们发现的Blob有两中版本一个是版本1.0，一个是版本2.0。主要以2.0的为主，具体格式如下：

VFS其中第4类Lua脚本的升级迭代。

表 21版本迭代

3. 同一目标被多个APT组织攻击

索伦之眼组织攻击的目标中，其中有一个目标曾经被APT-C-06组织攻击，该目标在被APT-C-06组织攻击后3个月，遭受索伦之眼组织的攻击。

另外一个被索伦之眼组织攻击的目标，曾经是被APT-C-12组织攻击。

同一个目标被不同APT组织攻击，我们推测有以下可能性：首先该目标是高价值目标，不同APT组织都关注；另外一种可能性或许是APT组织之间有合作关系，或者从其他第三方渠道获得该目标相关信息或权限；最后有可能相关组织幕后原本就是同一个组织，而采用截然不同的TTPs发动的相关攻击行动。

五、 组织特点

索伦之眼组织的攻击体系庞大，相关恶意代码均为模块化，其复杂度可与方程式（Equation）等顶级APT媲美。以下是索伦之眼组织相关攻击手法高级和特别的地方：

- 改造Lua引擎作为恶意代码运行平台。
- 相关功能模块达到几十种。
- 攻击中使用域服务器或邮件服务器进行横向移动。
- 采用VFS（虚拟文件系统），相关功能模块均无实体文件。
- 相关模块或通信协议采用了多种强加密算法，如RC6、RC5、RC4、AES。并使用单独密钥加密。
- 针对不同的目标进行量身定制的攻击，有极强的针对性。

1. 极强针对性

为每个单位配备专属C&C，不同单位之间不会存在C&C共用的情况。进一步针对同一单位的不同的计算机终端，大部分也采用不同的C&C，少量会存在C&C复用的情况。

2. 组织描述

六、 总结

重点攻击领域：政府机构

我们在今年年初发布的《2015年中国高级持续性威胁（APT）研究报告》 中指出“针对科研教育机构发起的攻击次数最多，占到了所有APT攻击总量的37%；其次是政府机构，占27%；”。另外今年8月披露的摩诃草组织（APT-C-09） 和本次披露的索伦之眼组织（APT-C-16），其中政府机构都是被重点攻击的领域，尤其在索伦之眼相关攻击行动中，政府机构被攻击的次数最多，占到了整体攻击总量的34%。

由此可见政府机构是绝大多数APT组织首要关注的攻击领域，这也是由于其背景和最终意图所决定的。在我们捕获的APT攻击中，更有针对政府机构领域对同一高价值目标，先后会被不同的APT组织所攻击。

APT实为大国博弈

随着信息技术的快速发展，网络空间成为大国博弈的制高点，网络安全进入国家安全的范畴。网络安全不仅涵盖数据安全、技术安全等常规领域，对政治安全、经济安全、文化安全、军事安全也有深刻影响。

从2010年针对伊朗核电站的震网蠕虫被曝光，到2013年美国国家安全局（NSA）的棱镜计划被斯诺登公诸于世，以及2015年末针对乌克兰工业领域的网络攻击导致乌克兰某地区大规模停电事件。越来越多的APT组织或攻击行动不断地被披露曝光，从中我们可以看出，当前世界范围内网络监听、网络攻击、网络犯罪等问题此起彼伏，并向国防、经济、文化等多领域渗透。网络空间作为国家继陆海空天电之后的“第六疆域”，需严守以待。

协同联动应对顶尖的APT

与索伦之眼攻击水准类似的还有方程式（Equation）、震网（Stuxnet）、火焰（Flame）等APT攻击，这类攻击的共性是相应幕后组织，属于全球已披露的数百个APT组织或行动中最为顶尖的精英部队。这批精英APT组织发动的攻击一般针对性极强、高隐蔽性、代码复杂度高，这也是持续攻击多年而不被发现的主要原因。面对这类顶尖的APT，我们除了需要从技术手段方面加强防御检测，还需协同联动各方一并应对。

我们认为协同分为数据协同、产业协同和智能协同三个层面，第一个层面是数据协同，是希望能够打破数据的孤岛和数据的鸿沟,数据的协同和共享，是数据驱动安全体系里最关键性的基石。第二个层面是产业联动、产业协同。产业协同需要政府和企业共同推进，达成政府间、企业间包括政府和企业间透明的互信的协同，从而形成更安全的产业生态。第三个层面是智能协同，这是一种更高层面的协同。从世界范围内发生的多起安全事件看，还需要更多领域的专家参与到协同里来，不同的领域、设备、行业之间都需要进行不同维度的协同。这个协同，是超过企业层面、行业层面、领域层面、区域层面的协同，甚至超越国家层面的协同。

1. http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets
2. https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/
3. https://msdn.microsoft.com/zh-cn/library/hh831484(v=ws.11).aspx

本文链接：https://blogs.360.cn/post/APT-C-16.html

-- EOF --

作者 `heliosteam` 发表于 *2016-09-09 11:35:43*，添加在分类 `APT` 下，最后修改于 *2020-06-15 14:47:29*

« 分享一款失败的国产加密勒索软件

Android系统新权限模型剖析与预警 »

360 核心安全技术博客

Comments