原文地址:http://drops.wooyun.org/papers/11046

http://researchcenter.paloaltonetworks.com/2015/11/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/>

0x00 前言

Unit42近期公布了一份关于最新木马Bookworm的研究文章，文章中讨论了这个木马的架构和功能。泰国是这次攻击活动的主要攻击目标。

在本文中，我们会讨论目前的攻击活动，以及相关的威胁基础设施和攻击策略，技术和过程（TTPs）。在下面的列表中，提供了一份TTP总结，在本文中，我们都会涵盖到：

- 主要攻击目标都分布在泰国，尤其是政府机构。
- 使用Bookworm作为攻击载体。
- 能够访问遭攻击的服务器，这些服务器用于下载Bookworm。
- 已知利用钓鱼攻击作为渗透目标的攻击途径，但是能够访问遭入侵的web服务器，以便支持未来利用战略web渗透（SWC）作为攻击途径。
- 使用独立的FlashPlayer来播放幻灯片，这些幻灯片以泰国实事作为诱饵文档，但是有时候，还会使用合法的Flash Player安装程序作为诱饵。
- 使用日期代码来跟踪攻击行动或木马版本。如果日期代码确实用作了行动标识符，然后，攻击者会利用攻击活动6到18天之前的事件作为诱饵文档的内容，从中我们可以稍微了解某个小组的开发和行动节奏。
- 使用大型的C2基础设施，这些C2服务器非常喜欢利用动态DNS域名。部署了Poison Ivy，PlugX，FFRAT 和 Scieron木马家族。

0x01 Bookworm 攻击活动

攻击者利用Bookworm作为攻击载体来打击泰国的目标。对这些活动感兴趣的读者可以首先读一读我们的第一篇文章，在文章中我们介绍了木马的整体功能和木马的各种组件。

Unit 42并没有掌握到关于所有已知Bookworm样本的详细目标信息，但是我们发现至少有两处泰国政府分支机构遭到了攻击。根据相关诱饵文档的内容以及几个用于托管C2服务器的动态DNS域名，我们怀疑，其他涉及Bookworm的攻击活动也在攻击泰国的组织，在这些C2服务器中出现了“泰”、“泰国”等字样。我们分析发现，遭到入侵的系统出现在了Backworm的C2服务器中，这也证实了我们所猜测的主要的目标系统都出现在泰国。

0x02 静态日期代码和诱饵

我们在上一篇Bookworm文章中提到过，这个木马会向C2服务器发送一个静态的日期字符串，我们认为这个日期字符串代表的就是活动代码。我们认为攻击者会利用这个日期代码来跟踪其攻击活动；但是，在继续分析了木马后，我们认为这些静态日期可以作为木马的创建标识符。凭借当前的数据，我们还很难确定这些静态日期代码的确切目的，但是，我们会在下一部分讲解。虽然，目前我们更支持这些日期是活动代码的理论，我们从所有已知的Bookworm中提取出了下面的这些日期代码，从中可以看出他们的活动开始时间可能是2015年6月或7月：

• 20150626 • 20150716 • 20150801 • 20150818 • 20150905 • 20150920

0x03 木马创建日期

攻击者可能会使用硬编码到Bookworm样本中的数据字符串作为一个创建标识符。很常见的就是，一个木马把一个创建标识符发送到它的服务器上，因为这个标识符能提示攻击者确切的木马版本。我们在上一篇博客中说过，因为其模块化框架，Bookworm相当复杂，也就表明攻击者需要了解他们正在与哪个版本的木马通讯，以便安装合适的补充模块。

虽然有一个合理的前提，但是我们掌握的数据还是无法证实Bookworm样本中的硬编码日期就是创建标识符。为了尝试证实这些日期就是创建ID，我们提取出了每个Bookworm样本中的所有模块。然后，我们比较了日期值相同的Bookworm样本中的各个模块。大多数使用相同模块的Bookworm中 都使用了相同的日期字符串，但是有几个样本中虽然模块不同但是也有相同的日期字符串。例如，表1中列出了两种Bookworm样本，日期代码有“20150716”和“20150818”，这些样本使用了完全不同的Leader.dll模块。

Date Code	Leader.dll Module	Compile Date
20150716	e602a12e8173ca17ba4a0c6c12a094c1	2015-07-18
20150716	4537257cb69a467a63c5a561825571f9	2015-07-23
20150818	e6cb32805bc5d758a5ea1dcd3c05beb8	2015-08-24
20150818	7065c709dd9dc7072dd5a5e2904c2d78	2015-08-31

表1-这两种Bookworm样本都共用了一个静态日期代码，但是使用了不同的Leader模块。

如果Bookworm开发者使用这些日期代码作为创建标识符，这就表明使用新Leader模块的样本也添加了新的日期代码。由于这些变化没有新的日期字符串，我们认为这些日期代码适用于行动追踪，而不是Bookworm的创建标识符。Unit 42会在未来的样本中继续比较Bookworm模块与这些日期代码。如果有证据表明这些日期字符串的确是创建标识符，我们还会修改我们的评定。

0x04 行动代码

我们认为Bookworm样本使用的静态日期字符串用作活动代码，我们会根据这些字符串来判断我们尚不清楚的攻击活动的大致日期。我们还比较了这些行动代码与攻击活动发生的日期和诱饵文档中的事件日期。有大量的Bookworm样本中会包括一个诱饵，这个诱饵会在木马安装过程中打开，尝试伪装入侵活动。目前攻击者使用了两种诱饵文件：一个合法的Flash Player安装程序和一个独立的Flash应用，用于播放照片幻灯片。图1中就是使用的Flash Player安装程序，从中可以看出，攻击者正在使用社会工程来控制受害者更新或安装Flash Player应用。在所有与这些合法Flash Player 安装程序相关的样本中都使用了代号“20150818”作为行动代码。

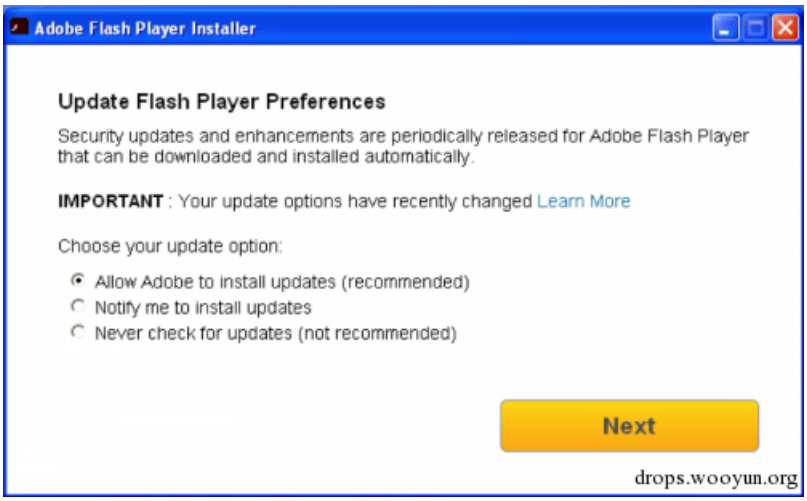

图1-Adobe Flash Player用作诱饵

Unit 42自己就遇到了6个幻灯片诱饵，攻击者在一起Bookworm行动中利用这些诱饵攻击了泰国。所有这六个幻灯片诱饵中都包含有与泰国相关的图片。在一个已知的诱饵中，有一幅漫画，描述了一些小孩前往寺庙的情形（图2），攻击者在2015年6月27日的一次钓鱼攻击中利用这个诱饵攻击了一处泰国政府的分支机构。这个诱饵的文件名是“wankaophansa.exe”，从这个文件名中可以看出这幅漫画与守夏节相关，守夏节指的是3个月漫长雨季的第一天。守夏节是泰国的国家性节日，2015年的守夏节从6月31日开始。此次攻击活动在守夏节前四天开始，行动代码是“20150716”，比实际攻击活动提前了11天。

图2-泰国儿童庆祝守夏节

我们目前还不清楚，投放另外5个诱饵的攻击活动都攻击了哪些具体的目标。为了判断大致的攻击时间，我们对比了与每个幻灯片诱饵关联的行动代码，我们发现这些活动与诱饵文档中的事件日期一致。 其中的三个诱饵与2015年8月27日在曼谷发生的四面佛爆炸案由关系，图3、4、5。与幻灯片诱饵关联的行动代码是“20150801”，其中的照片显示的就是四面佛的爆照情况（图3），这个日期实际是爆炸事件发生的前16天。

图3-幻灯片诱饵中的图片，显示的是曼谷四面佛爆炸情况 (http://metro.co.uk/2015/08/17/huge-explosion-in-central-bangkok-near-major-tourist-attraction-5347076/)

图4是第二个与爆炸案相关的诱饵，这里面的照片是被捕的爆炸案嫌疑人Adem Karadag。这次逮捕事件是在2015年8月29日发生的，比与幻灯片诱饵关联的行动代码“20150818”晚了11天。

图4来自一个幻灯片诱饵，显示的是曼谷爆炸案犯罪嫌疑人的被捕画面

第三个和最后一个与爆炸案相关的幻灯片诱饵中包含有Adem Karadag向经常描述自己在爆炸案中所扮演的角色（图5）。案情重现是泰国警方办案的一个标准程序，这起案例发生于2015年9月26日。与这个诱饵关联的行动代码是“20150920”，比真实事件早六天。

图5-幻灯片诱饵中的照片，显示的是犯罪嫌疑人在现场的照片

在另一个与Bookworm活动相关的诱饵中，包含有关于Bike for Dad 2015事件的照片。Bike for Dad是一次骑行事件，将会在2015年12月11日举行， 旨在纪念泰国国王Bhumibol Adulyadej的88岁诞辰。许多泰国的重要人物都会出席此次活动，比如 泰国总统帕拉育就出现在了幻灯片诱饵中的多张照片中（图6）。

图6-幻灯片诱饵中与Bike for Dad事件相关的照片(http://www.m-society.go.th/ewt_news.php?nid=15002)

与这个诱饵关联的行动代码是“20150920”，也就是媒体报道泰国王储Maha Vajiralongkorn会主持Bike for Dad 2015的一周前。首先，我们认为Bike for Dad 2015事件与先前的曼谷爆炸案诱饵并没有关联。根据同一篇文章中的报道，王储称骑行路线会通过拉差帕颂路口，也就是爆炸案的发生位置。因此，攻击者在社会工程中利用这次事件是为了继续吸引注意，因为先前的爆炸事件还牵动着泰国人民的心。

最后一个诱饵中出现了Chitpas Tant Kridakon的照片（图7），这个人是泰国最大啤酒厂的女继承人。Chitpas积极参与泰国政治，并且是人民民主委员会（PCAD）的一名核心领导人，这个组织在2013年和2014年的时候举行了反政府活动。在2015年9月，Chitpas由于尝试加入泰国行家警方而登上报纸头条，因为她的政治观点引起了抗议活动。幻灯片中的两张照片是在2015年9月20日发表的一篇文章上刊登的。这些图片都与代号为“20150905”的Bookworm活动有关。

图7-在一个幻灯片诱饵中出现的Chitpas Tant Kridakon照片

通过对比与未知攻击活动相关的活动代码和诱饵中相关的事件日期，我们发现这些活动代码都会遭遇攻击或事件发生的6到18天。这点可以表明，攻击者首先会利用工具来部署行动，然后再选择诱饵。这些诱饵文档还表明，攻击者会积极地追踪当前的新闻事件，并利用媒体报道中的图片来创建幻灯片诱饵。

0x05 遭到入侵的主机

Unit42分析了与Bookworm C2进行通讯的系统，并发现了大量存IP地址是来自于泰国的自治系统（ASN）。图8中的饼图显示大量的（73%）的主机位于泰国，符合这个攻击小组的攻击目标。我们认为来自加拿大、俄罗斯和挪威的IP属于杀毒公司和安全研究员。很有意思的是来自韩国的IP，这说明攻击者也可能攻击过韩国。但是，我们还没有发现其

他的证据能说明这一推论。

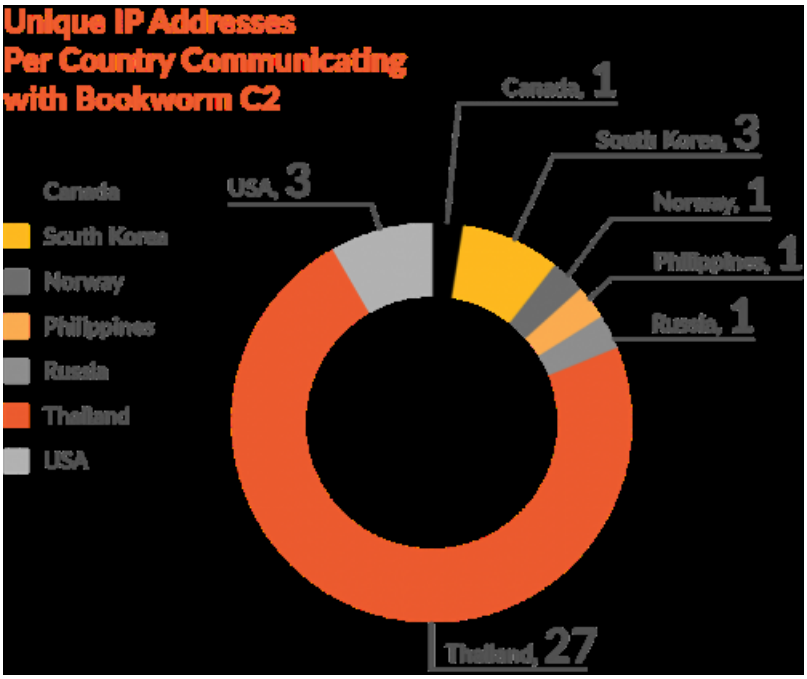

图8-与Bookworm C2通讯的IP地址印证了攻击目标位于泰国

我们提取出了这些与Bookworm C2服务器通讯的IP地址，并利用IP地理位置数据库确定了这些IP的地理坐标，标记在了地图上，如图9。大量的IP地址都位于泰国曼谷的城市区域，有一个位于Pattini南部小镇，一个位于Chonburi省的 Phanat Nikhom街。IP位置确定系统并不是绝对准确的，但是，数据表明大多数遭到入侵的足迹都在曼谷周围。这也符合攻击者的主要攻击目标，大部分泰国政府机构都分布在曼谷和暖武里府。

图9-GeoIP位置显示遭到攻击的主机大都分布在曼谷城市区域

0x06 Bookworm的威胁基础设施

攻击者创建的Bookworm基础设施大都使用了动态域名，但是，早期的样本使用了攻击者持有的一个完全限定域名（FQDN）。攻击者还利用了合法的服务来托管Bookworm和其他相关的攻击工具。总而言之，Bookworm的基础设施与攻击工具的C2服务器出现了重合，包括FFRAT，Poison Ivy，PlugX等。

0x07 遭到入侵的Web服务器

Unit 42发现攻击者在合法的网站上托管Bookworm和其他相关的工具，这就表明攻击者非法入侵了这些服务器。我们发现一些Bookworm样本托管在了属于下列组织的服务器上：

• 泰国的两处政府分支机构 • 泰国军方 • 台湾工会

在这四个遭到入侵的web服务器中，有3个网站早就在 Zone-h上列出来了遭到了篡改，而根据从2015年11月11日之间的Google cacge来看，另一个网站遭到了TURKHACKTEAM的篡改。我们不清楚攻击者具体是如何入侵了这些网站，但是，其中一个网站允许访客通过表单上传文件到web服务器上（图8）。Unit 42认为攻击者知道可以通过表单向这个服务器上传Bookworm。很可能，攻击者会上传ASP shell来进一步控制这个服务器。我们怀疑这些攻击者可能会借助对web服务器的非法访问在以后使用策略性web渗透（SWC）作为攻击途径。

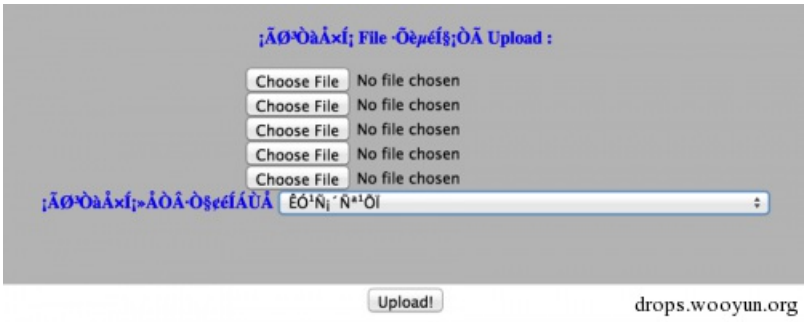

图10-利用表单上传文件到服务器上托管Bookworm木马

托管这个文件的网站上传了一个属于Bookworm攻击目标的表单。这就说明攻击者可能利用了这个websever来入侵其内部网络。

0x08 基础设施和相关的工具

托管Bookworm C2的域名（参照我们Bookworm博客中的入侵标识）连接到了一个大型服务器，攻击者还利用这个服务器作为了其他一些工具的C2。目前为止，Unit 42发现Bookworm的基础设施也是一些木马的C2服务器，包括FFRAT, PlugX, Poison Ivy和 Scieron木马，这就表明攻击者会使用这些工具作为攻击载体。

Unit 42列出了所有与Bookworm相关的基础设施，以及与这个攻击小组相关的当前攻击活动。其基础设施相当复杂，并且与其他工具集出现了重合。图11中就是一部分基础设施与Bookworm, FFRAT, PlugX 和Poison Ivy之间的关联。

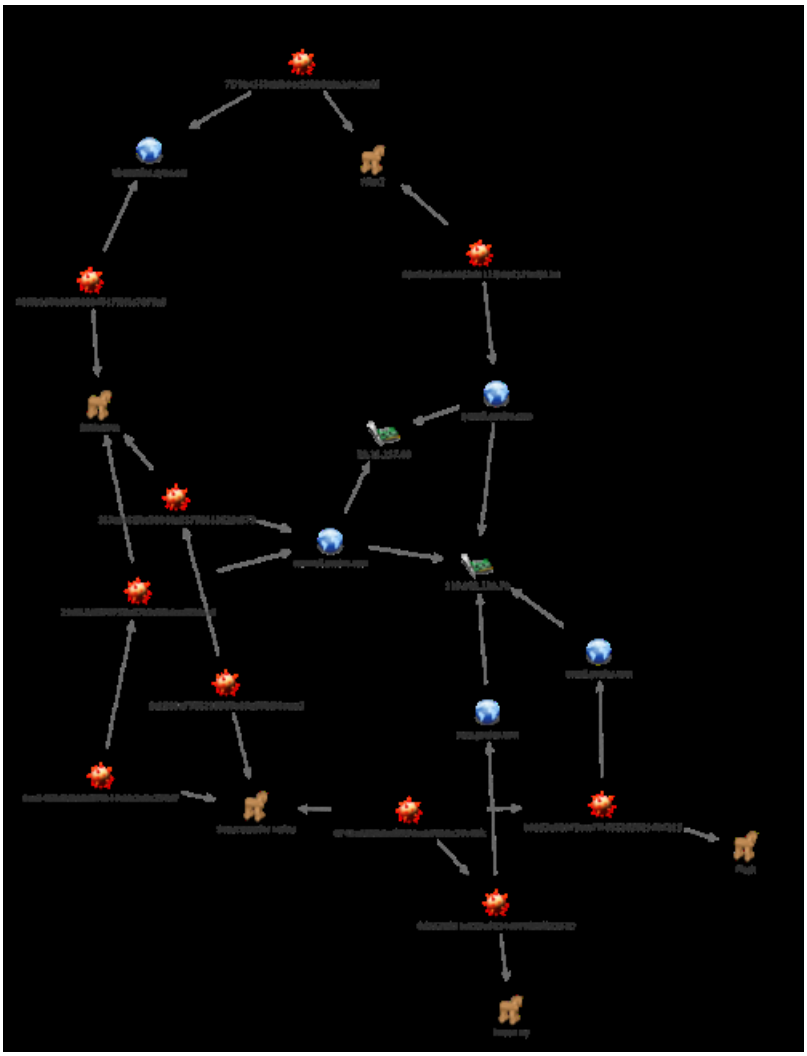

图11-Bookworm，PlugX, Poison Ivy 和FFRAT木马之间使用的基础设施

Bookworm，PlugX和Poison Ivy样本都使用了Smart Installer Maker，这是攻击小组经常使用的一种技术。在一次案例中，一个Smart Installer Maker（MD5: 6741ad202dcef693dceb98b0a10c49fc）安装了PlugX和Poison Ivy木马，与木马通讯的域名会解析到IP地址(119.205.158.70)，这个IP同样解析到了一个Bookworm的C2域名(sswmail.gotdns[.]com)。另一个木马FFRAT同样使用了这个IP，解析到了qemail.gotdns[.]com。我们观察到Bookworm和FFRAT都使用了另外一个C2域名(ubuntudns.sytes[.]net)。

如前文提到的，与Bookworm相关的基础设施相当复杂，与其他工具的C2域名存在诸多关联。相关的基础设施和木马都列在了下表中。

Domain	Malware Family/Cluster
web12.nhknews[.]hk	Bookworm
systeminfothai.gotdns[.]ch	Bookworm
bkmail.blogdns[.]com	Bookworm
thailandbbs.ddns[.]net	Bookworm
blog.nhknews[.]hk	Bookworm
news.nhknews[.]hk	Bookworm
sysnc.sytes[.]net	Bookworm
debain.servehttp[.]com	Bookworm
sswmail.gotdns[.]com	Bookworm
sswwmail.gotdns[.]com	Bookworm
ubuntudns.sytes[.]net	Bookworm, FFRAT
linuxdns.sytes[.]net	Bookworm, FFRAT
www.chinabztech[.]com	FFRAT
www.tibetonline[.]info	FFRAT
3h01.dwy[.]cc	FFRAT
www.vxea[.]com	FFRAT
bdimg.s.dwy[.]cc	FFRAT
nine.alltosec[.]com	FFRAT
www.rooter[.]tk	FFRAT
wucy08.eicp[.]net	FFRAT
welcome.dnsd[.]info	FFRAT
www.ifilmone[.]com	FFRAT
pcal2.dwy[.]cc	FFRAT
luotuozhizhu.blog.163[.]com	FFRAT
office.alltosec[.]com	FFRAT

ftpseck.ftp21[.]net	FFRAT
wuzhiting.3322[.]org	FFRAT
qemail.gotdns[.]com	FFRAT
googleupdating[.]com	FFRAT
welcometohome.strangled[.]net	FFRAT
zz.alltosec[.]com	FFRAT
back.rooter[.]tk	FFRAT
products.alltosec[.]com	FFRAT
windowsupdating[.]net	FFRAT
app.rooter[.]tk	FFRAT
hkemail.f3322[.]org	FFRAT
pcal2.yahoolive[.]us	FFRAT
happy.tftpd[.]net	PlugX
weather.webhop[.]me	PlugX
ns1.vancouversun[.]us	PlugX
n5579a.voanews[.]hk	PlugX
hope.jumpingcrab[.]com	PlugX
news.nowpublic[.]us	PlugX
web.vancouversun[.]us	PlugX
news.voanews[.]hk	PlugX
bugatti.from-wa[.]com	PlugX
web.voanews[.]hk	PlugX
ns3.yomiuri[.]us	PlugX
tree.crabdance[.]com	PlugX
supercat.strangled[.]net	PlugX
webupdate.strangled[.]net	PlugX

breaknews.mefound[.]com	PlugX
succ.gotdns[.]com	Poison Ivy, PlugX
imail.gotdns[.]com	Poison Ivy, PlugX
wmail.gotdns[.]com	Poison Ivy, PlugX
xxcase.gotdns[.]com	Poison Ivy
romadc.homelinux[.]com	Poison Ivy
3389temp.dyndns[.]org	Poison Ivy
ahcase.gotdns[.]com	Poison Ivy
kcase.gotdns[.]com	Poison Ivy
3389pi.servegame[.]org	Poison Ivy
flashcard.gotdns[.]com	Poison Ivy
kr-update.homelinux[.]com	Poison Ivy
3389.homeunix[.]org	Poison Ivy
flashgame.gotdns[.]com	Poison Ivy
anhei.gotdns[.]com	Poison Ivy
xcase.gotdns[.]com	Poison Ivy
education.suroot[.]com	Scieron
server.organiccrap[.]com	Scieron
pricetag.deaftone[.]com	Scieron
apple.dynamic-dns[.]net	Scieron
williamsblog.dtdns[.]net	Scieron
will-smith.dtdns[.]net	Scieron
durant.dumb1[.]com	Scieron

表2-与Bookworm相关的基础设施

我们通过代码签名证书，PE创建共性，被动DNS数据和重复的C2郁闷确定了表2中的域名关系。通过被动DNS确定联系的域名都共用同样的IP地址来解析到域名。通过重合的被动DNS数据，确定了下面的IP地址存在联系：

- 103.226.127.47
- 104.156.239.105
- 112.167.143.179
- 115.144.107.22
- 115.144.107.46
- 115.144.107.52
- 115.144.107.53
- 115.144.107.134
- 115.144.166.209
- 119.205.158.70
- 43.248.8.249

0x09 总结

攻击者从2015年6月开始攻击泰国政府并投放了最新发现的Bookworm木马。攻击者似乎定好了作战计划，因为我们观察到攻击者的技战术相当统一。攻击者还在利用Flash Player安装程序和Flash幻灯片来作为诱饵。诱饵幻灯片中的照片都是在泰国很有意义的事件或个人，这表明攻击者还在利用有影响力的事件来伪装他们的攻击活动。

大量与Bookworm C2服务器通讯的系统都位于曼谷的城市区域，在这里有大量的泰国政府机构。虽然目前的攻击活动都是以泰国政府为目标，但是Unit42认为攻击者还会在未来的活动中利用Bookworm来攻击其它政府。