2017 年 5 月 23 日，星期二

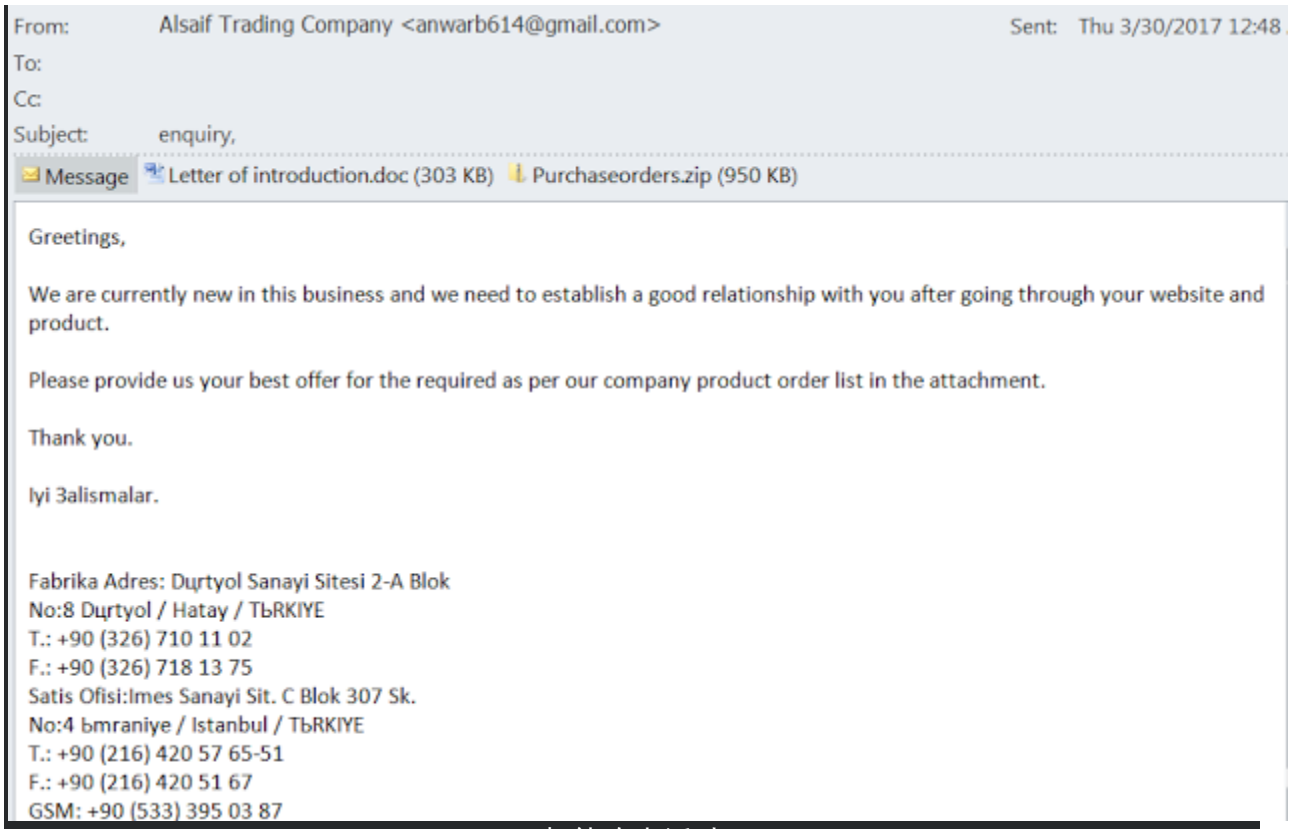
来自印度的修改版 Zyklon 和插件

简介

Talos 每天检查的大量恶意邮件通常包括活跃的垃圾邮件攻击活动，这些攻击活动来自各种勒索软件系列、网络钓鱼攻击活动，以及银行木马和僵尸程序等常见的可疑恶意软件系列。然而，分析量级较小的攻击活动通常更有意义，因为它们可能包含更值得关注的恶意软件。几周前，我对这样一种攻击活动产生了兴趣，它会循环发送少量邮件。第一封邮件的提交地点是中东，声称来自一家土耳其贸易公司，这可能进一步说明此类攻击活跃的地理区域。分析恶意软件通常像玩拼图游戏，必须一块一块地去拼才能得到最终的图像。在本案例中，分析攻击活动花费的时间超过了我的最初计划。该攻击活动包含许多感染链阶段，在到达最终的有效负载级别之前需要对每个阶段进行拆解。此外，每个阶段使用不同的开发平台，并以不同的方式进行混淆处理。不过，我们需要从头开始。

第 1 阶段 - 邮件

邮件包含两个附件。第一个是 Office Open XML 文件格式的 Word 文档，第二个是 Zip 文件 PurchaseOrders.zip，其中包含一个可执行文件 PurchaseOrders.exe。相对而言，这是一种不寻常的邮件攻击活动策略，因为更为常见的情形是恶意邮件包含一个附件，而不是两个或两个以上。攻击者似乎想要确保收件人会至少打开其中一个附件。



From: Alsaif Trading Company <anwarb614@gmail.com> Sent: Thu 3/30/2017 12:48
To:
Cc:
Subject: enquiry,
Message Letter of introduction.doc (303 KB) Purchaseorders.zip (950 KB)

Greetings,

We are currently new in this business and we need to establish a good relationship with you after going through your website and product.

Please provide us your best offer for the required as per our company product order list in the attachment.

Thank you.

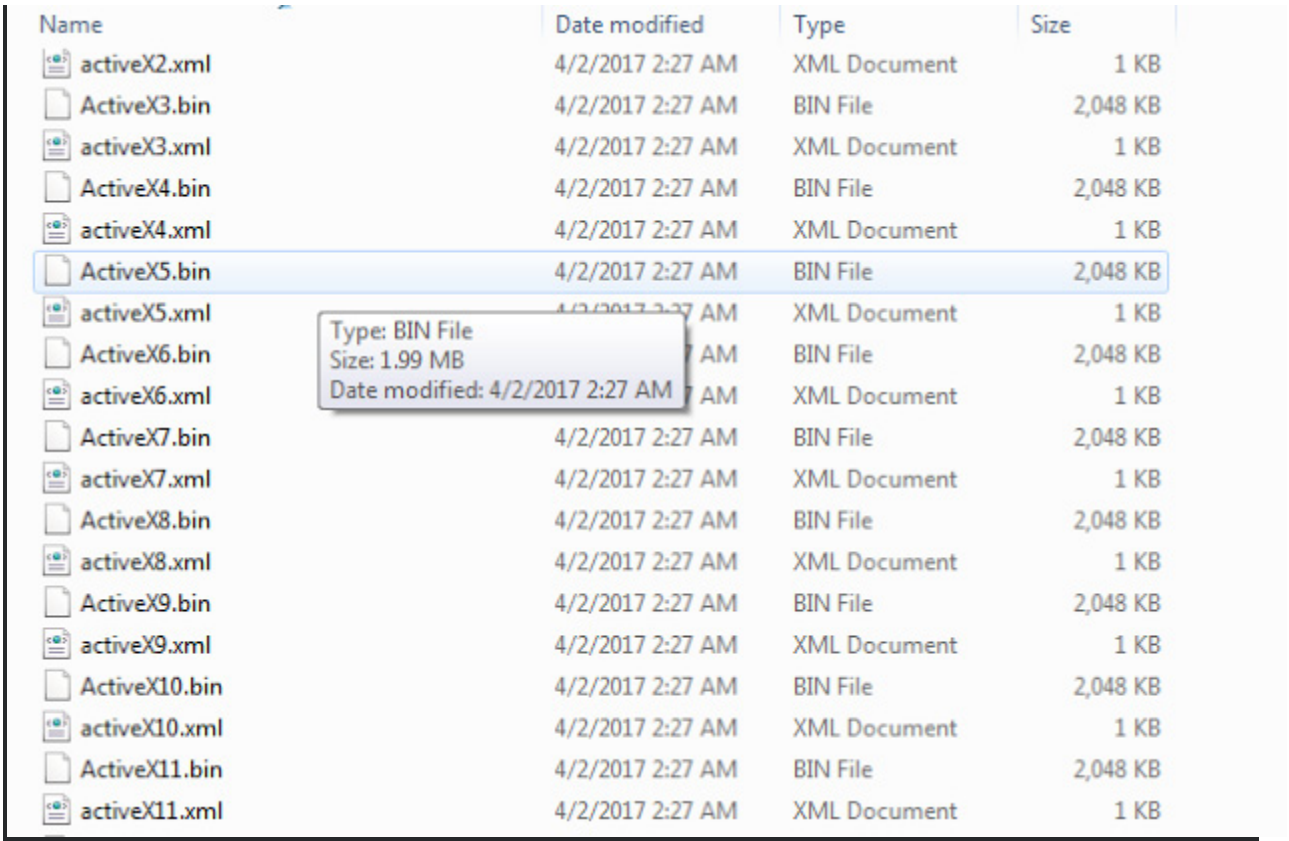
Iyi 3alismalar.

Fabrika Adres: Dųrtyol Sanayi Sitesi 2-A Blok
No:8 Dųrtyol / Hatay / TЬRKIYE
T.: +90 (326) 710 11 02
F.: +90 (326) 718 13 75
Satis Ofisi:Imes Sanayi Sit. C Blok 307 Sk.
No:4 Ьmraniye / Istanbul / TЬRKIYE
T.: +90 (216) 420 57 65-51
F.: +90 (216) 420 51 67
GSM: +90 (533) 395 03 87

邮件攻击活动

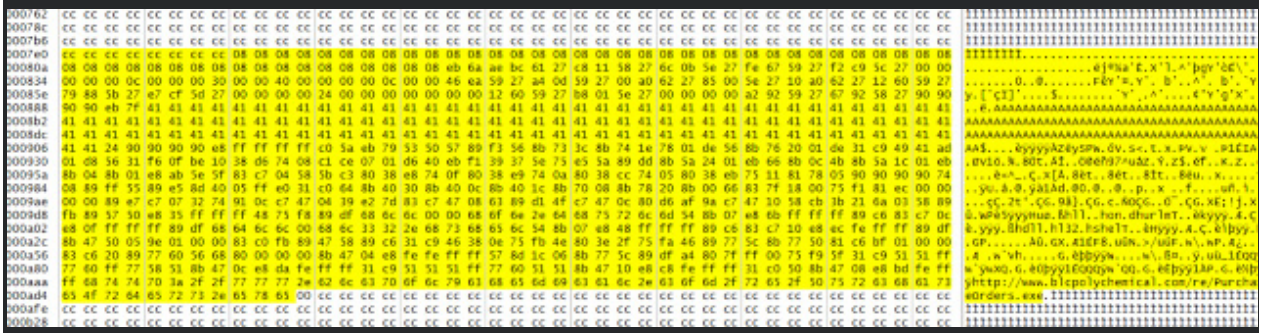
第 2a 阶段 - Word 文档 - CVE-2013-3906

Word 文档附件“Letter of introduction.doc”包含一个用于解析漏洞的 CVE-2013-3906 TIFF 图像文件。该文档包含多个 TabStrip (classid: {1EFB6596-857C-11D1-B16A-00C0F0283628}) ActiveX 控件，CVE-2012-1856 中也使用这些控件。



用于堆喷射的嵌入式 ActiveX 控件

嵌入式 TabStrip ActiveX 控件用于堆喷射，而名为 image1.jpeg 的嵌入式 TIFF 文件可触发 CVE-2013-3906 漏洞。嵌入式 ActiveX 控件有 40 个，每个映射到 2MB 的已分配内存空间。在本案例中，漏洞攻击需要一些时间，但漏洞最终会导致易受攻击的 Word 版本崩溃，并启动 Shellcode。Shellcode 会立即显示在 ActiveX OLE2 文件的十六进制转储编码中，并在被利用的 Word 进程内存中喷射。



ActiveXn.bin 文件中发生堆喷射的 Shellcode

SHELLCODE - 避开挂钩

Shellcode 本身相对简单，长度大约为 450 个字节，不包括用于下载有效负载的 URL。通常情况下，它通过解析进程环境块 (PEB) 并遍历链接的已加载模块列表及其各自的导出函数来找到 API。

值得注意的是，在调用所需的 API 之前，Shellcode 会检查是否存在内联挂钩（通常由终端安全产品安装），并跳过已安装的挂钩代码，以避免在相应的行为检测窗口中被发现。

```
.text:0040107F
.text:00401080
.text:00401080 ; =============== S U B R O U T I N E =======================================
.text:00401080
.text:00401080
.text:00401080 EvadeHookCall   proc near               ; CODE XREF: sub_4010A7+69↓p
.text:00401080                                         ; sub_4010A7+8C↓p ...
.text:00401080                 cmp     byte ptr [eax], 0E8h ; Is it a call?
.text:00401083                 jz      short loc_401094
.text:00401085                 cmp     byte ptr [eax], 0E9h ; Or a long jump?
.text:00401088                 jz      short loc_401094
.text:0040108A                 cmp     byte ptr [eax], 0CCh ; Or a breakpoint?
.text:0040108D                 jz      short loc_401094
.text:0040108F                 cmp     byte ptr [eax], 0EBh ; Or short jump?
.text:00401092                 jnz     short loc_4010A5
.text:00401094
.text:00401094 loc_401094:                             ; CODE XREF: EvadeHookCall+3↑j
.text:00401094                                         ; EvadeHookCall+8↑j ...
.text:00401094                 cmp     dword ptr [eax+5], 90909090h ; Legit Windows hook (Win7+ )
.text:0040109B                 jz      short loc_4010A5
.text:0040109D                 mov     edi, edi
.text:0040109F                 push    ebp
.text:004010A0                 mov     ebp, esp
.text:004010A2                 lea     eax, [eax+5]
.text:004010A5
.text:004010A5 loc_4010A5:                             ; CODE XREF: EvadeHookCall+12↑j
.text:004010A5                                         ; EvadeHookCall+18↑j
.text:004010A5                 jmp     eax
.text:004010A5 EvadeHookCall   endp ; sp-analysis failed
.text:004010A5
.text:004010A7
.text:004010A7 ; =============== S U B R O U T I N E =======================================
```

避开安全挂钩

如果用户受到 Word 文档附件感染，Shellcode 就会从合法的受感染服务器下载和执行可执行文件。最终有效负载的 C2 服务器提取自以加密方式存储在下载的有效负载主体中的配置 Blob。

第 2b 阶段 - PurchaseOrders.exe

Shellcode 下载的可执行文件与邮件附带的可执行文件具有完全相同的功能，因此我们最终会来到 PurchaseOrder.exe 这一阶段，无论用户打开文档附件，还是立即去启动 PurchaseOrder.exe，最终都会执行该文件。该可执行文件有一个 PDF 文档图标，用户无法辨认出它是可执行文件有情可原，因为 Windows 默认隐藏已知文件类型的文件扩展名。

PurchaseOrder.exe 使用的图标文件。

该可执行文件本身的大小略大于 1.4MB，对于在邮件攻击活动中使用的附件而言，这是个相当大的文件。文件本身是一个可自提取的 CAB 归档文件，包含三个随机命名的文件。

第 3 阶段 - AutoIt 脚本

第一个文件一眼即可认出，它是一个合法的 Autoit 脚本解释器。第二个文件是一个以 UTF-16 编码的 Unicode 文件，大小超过 110MB，这样的大小起初几乎足以让分析者望而却步。实际脚本代码在文件深处启动，攻击者借此能够混淆脚本代码，使得调查人员无法立即发现。

Talos 以前编写过一个类似的传送方法，该攻击活动似乎使用类似的混淆 Autoit 脚本生成器。幸运的是，删除所有的垃圾字符并将待分析代码的大小降至更便于管理的 41KB 相对比较容易。

还原混淆的 Autoit 阶段

Autoit 脚本本身在用户的配置文件文件夹中创建一个目录，并将其属性设置为“系统”和“隐藏”。然后，它创建 RegSvcs.exe .NET 服务安装工具的副本，或将现有的

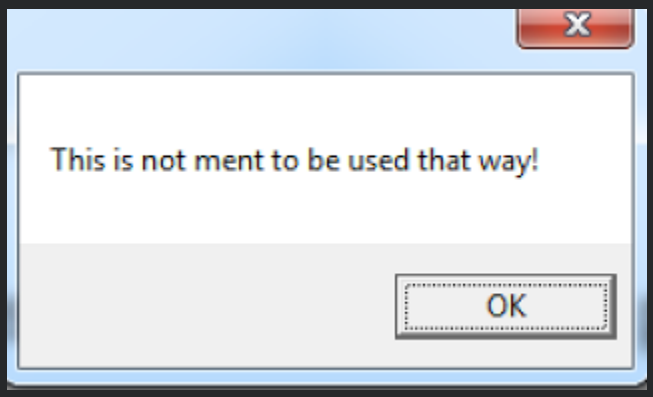
RegSvcs.exe 复制为文件 splwow64.exe，以设置下一阶段。Regscvcs.exe 用于在其进程空间内注入和启动远程线程。该线程使用 RC4 解密由原始自提取 CAB 归档文件植入的第三个文件，并将其读取到 regsvcs.exe 的进程空间中。这将我们带到下一阶段：使用以 C/C++ 开发的可执行文件。该阶段在内存中仅以可执行文件格式存在，但在磁盘上是一个 RC4 加密数据 Blob。

第 4 阶段 - Zyklon 注入程序

该阶段注入 RegSvcs.exe 中，是最终有效负载的另一个还原混淆注入程序。可执行文件从 PE 文件的资源部分解压有效负载，找到并启动 Windows 资源管理器可执行文件（该文件根据 Windows 平台（32 或 64 位）的不同而位于不同文件夹），然后启动用于加载和运行 .NET 可执行文件的远程线程，这是该攻击活动的最终负载，在本案例中是一个 Zyklon HTTP 僵尸程序样本。

将托管代码加载到非托管空间并不完全是一个简单的过程。攻击活动策划者显然已经预料到有人会尝试诱骗感染链从命令行启动 Zyklon 僵尸程序，因此更改了 Zyklon 类主函数，以向任何试图以这种方式启动它的人显示文本消息。

版本 1.0.0.0 的原始 Zyklon 代码似乎不包含这种机制，该机制可确保运行有效负载的特定加载程序不会调用 Zyklon 类主函数，而是调用不同的入口点。



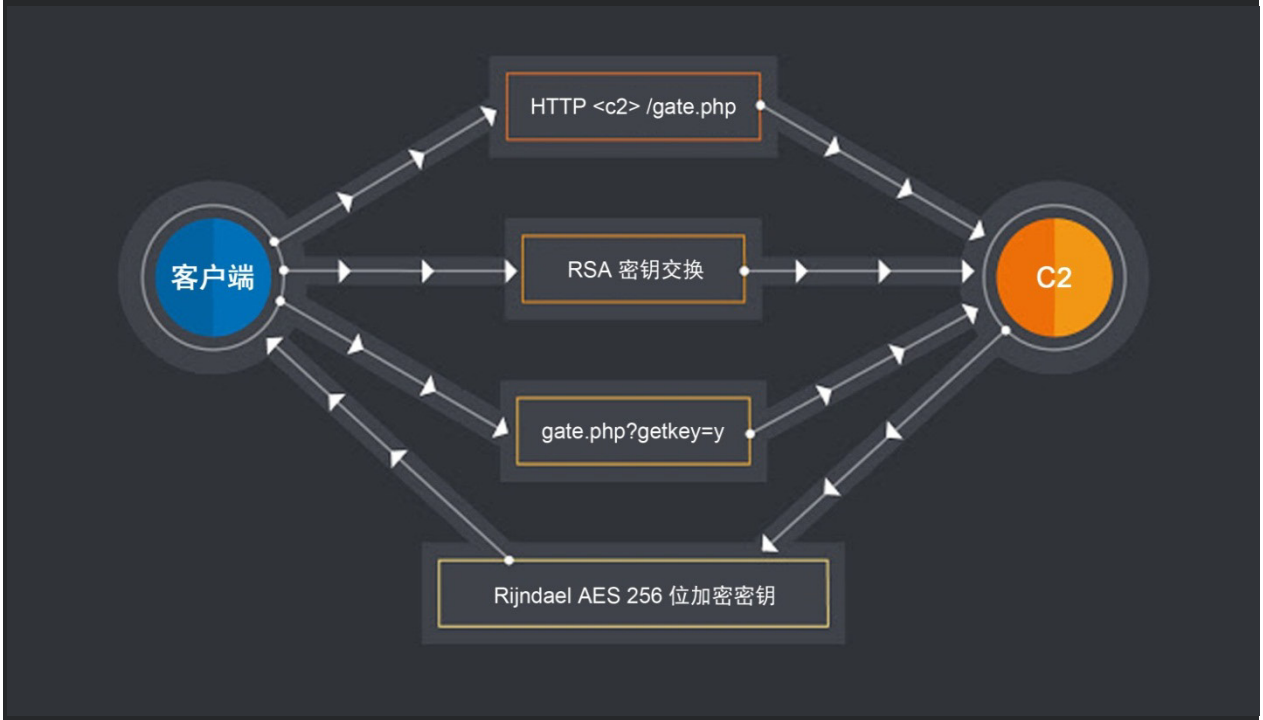
您不应以此方式运行程序

有效负载是使用 Crypto Obfuscator 和一个附加代码生成器进行混淆处理的。代码使用 xor 运算设置开关语句中使用的变量值来引导程序流，在使用非常有用的 .NET 还原混淆实用程序 de4dot 删除 Crypto Obfuscator 代码转换后，就可以相对轻松地跟踪这些代码。事实上，在 VirusTotal 上发现的 Zyklon Builder 使用相同的 dnlib 库（de4dot 和 dnspy 分析工具也使用该库），向 Zyklon 僵尸程序在其资源部分嵌入的恶意 .NET 程序集基类添加配置文件。

删除混淆器后，很快就可以意识到，为了进行分析，我们可以手动修改 Zyklon 类主函数，以调用包含僵尸代码的入口点函数，并使用 dnspy 调试程序调试 Zyklon。

C2 通信（加密）

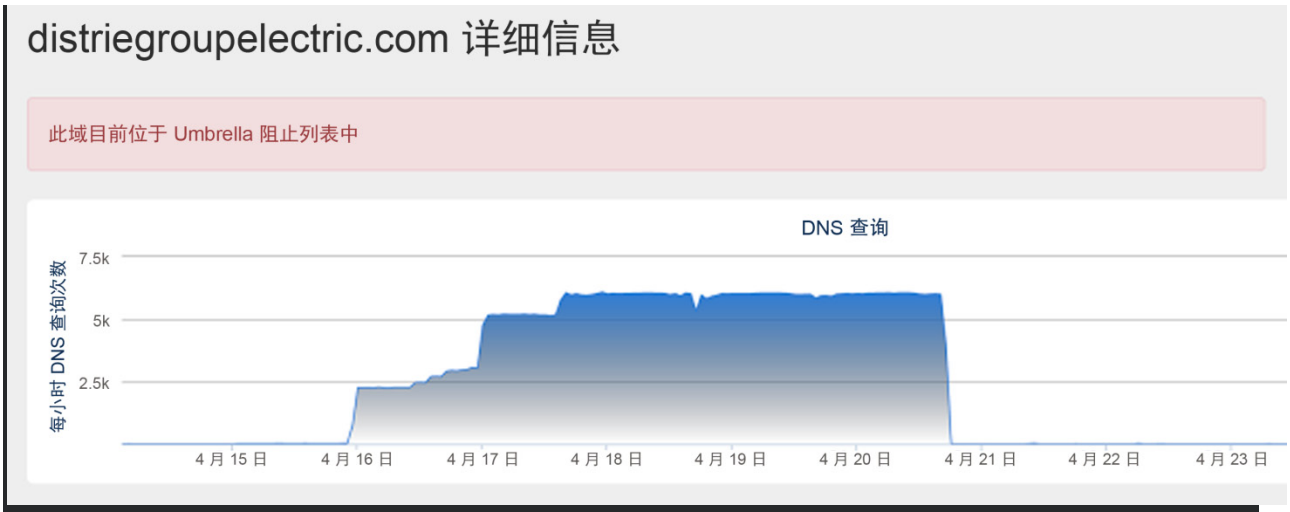
Zyklon 的“正式”名称为“Zyklon H.T.T.P bot”，可以在指向作为编译过程剩余部分保留下来的 PDB 文件的链接中看到。僵尸程序经过精心编写，并采取预防措施防止流量被基于网络的检测引擎发现，甚至通过加密所有通信来拦截代理。



与 C2 服务器建立通信

僵尸程序连接到三个可能的 C2 服务器之一，从其配置中指定的第一个服务器开始。服务器发送一个证书，通信首先使用 RSA 加密，然后使用长度为 256 位的 AES 加密，服务器生成初始化媒介和密钥，并在客户端发出以查询 gate.php?getkey=y 结束的 POST 请求后发回客户端。

对于在整个攻击活动中持续保持活跃的 C2 服务器，当查看其中一个服务器的 DNS 请求时，可能会看到该攻击活动活跃的时间。



C2 DNS 域活动

僵尸程序的初始配置嵌入在文件的资源部分中，一同嵌入的还有僵尸程序在与 C2 服务器通信时使用的用户代理字符串列表。恶意的 .NET 程序集还包含一个加密的 Blob，成为其暂留模块注入程序。该程序经解密并加载到内存中后，其功能是确保如果主要可执行文件被作为进程终止，僵尸程序可以从远程线程重新启动。

客户端随后发送包含受感染系统信息的请求，并从设置内部僵尸程序参数的 C2 服务器接收配置字符串。此外，恶意程序会启动多个线程，以下载并执行所需的其他插件。

主要命令循环会休眠 60 秒，然后向 C2 服务器发送命令请求。该僵尸程序的主要目的似乎是实施 DDoS 攻击，但或多或少还有其他可用的标准命令，例如从用户指定的 URL 下载并执行其他有效负载，或记录用户按键并将记录发回 C2 服务器。

令人好奇的是，Zyklon 还可能尝试枚举 Windows 注册表中通常的自动启动位置，以发现潜在的竞争文件，并将其提交至 VirusTotal 进行扫描。所谓的云恶意软件检测用于根据 VirusTotal 的扫描结果终止进程。该僵尸程序还对某些已知的竞争性僵尸程序名称和文件扩展名进行初步启发式检查，并在发现后尝试将其从系统中删除。坏人从不欢迎竞争对手出现。

Zyklon 网站

宣传 Zyklon 的网站托管在一个 .onion 域上，也可以通过 Web 转 Tor 代理从明网进行访问。所有者正在为出售的两个不同版本做宣传，一个可以连接到基于 Tor 的 C2 服务器，而另一个标准版则不具备此功能。

Zyklon 网站中最有趣的页面或许是其“服务条款”，制作者似乎认为这可以使其免于可能的控诉。据称，用户（也称为攻击者）对因此导致的损害单独承担法律责任，至少 Zyklon 制作者是这样规定的：

您理解并特此确认和同意，您不得且保证不会：

1. 将 Zyklon H.T.T.P 远程管理软件用于任何非法目的或违反任何法律（包括但不限于管理知识产权、数据保护和隐私以及进出口控制的法律）的行为；

2. 删除、规避、禁用、损坏或以其他方式干预 Zyklon H.T.T.P 远程管理软件的安全相关功能，阻止或限制使用或者复制可通过 Zyklon H.T.T.P 远程管理软件访问的任何内容的功能，或者对使用 Zyklon H.T.T.P 远程管理软件加以限制的功能；

3. 以任何方式（包括上传或传播病毒、蠕虫或其他恶意代码）故意干预或破坏 Zyklon H.T.T.P 远程管理软件的操作，或对用户使用该软件进行干预或破坏；

4. 发布、存储、发送、传输或传播侵犯专利、商标、商业机密、版权或任何其他专利或知识产权的信息或资料；或者

5. 在不具备明确权限的任何计算机上安装和/或使用 Zyklon H.T.T.P 远程管理软件；

6. 通过互联网分发 Zyklon H.T.T.P 文件，意图感染/危害他人设备；

下载的凭证收集模块（邮件、浏览器，ftp）

Zyklon 制作者还推出大量有用的插件，用于收集用户凭证和窃取机密信息，例如比特币、莱特币和 DodgeCoin 等各种加密数字货币的钱包详细信息。对于一名潜在客户而言，功能列表肯定十分具有吸引力，但并非所有功能都像乍看起来那样理想。

在所分析的攻击活动中，Zyklon 的主要可执行文件仅按照 C2 服务器的指示下载三个插件，其目的均为从最常用的网络浏览器以及邮件和 ftp 客户端的密码缓存中窃取用户凭证。

CI=False|KT=1|UAC=False|S5=False|ER=False|UPNP=False|RP=True|RW=False|
AK=False|BK_CYCLE=|BK_RUN_ONCE=False|SOCKS_PORT=3128|SOCKS_AUTH=False|
SOCKS_USERNAME=Nothing|SOCKS_PASSWORD=Nothing|KLI=1|KLM=500|EKL=True|
WC=False|BA=MyBtc|LA=MyLtc|KLF=False|BR=True|FTR=True|EMR=True|SFR=False|
GR=False|AU=False|UF=N/A|

从 C2 服务器发送到 Zyklon 的配置命令

插件下载 URL 采用 plugin/index.php?plugin=<pluginname> 格式，可能的插件包括

/plugin/index.php?plugin=browser
/plugin/index.php?plugin=email
/plugin/index.php?plugin=ftp!
/plugin/index.php?plugin=software
/plugin/index.php?plugin=games
/plugin/index.php?plugin=cuda
/plugin/index.php?plugin=minerd

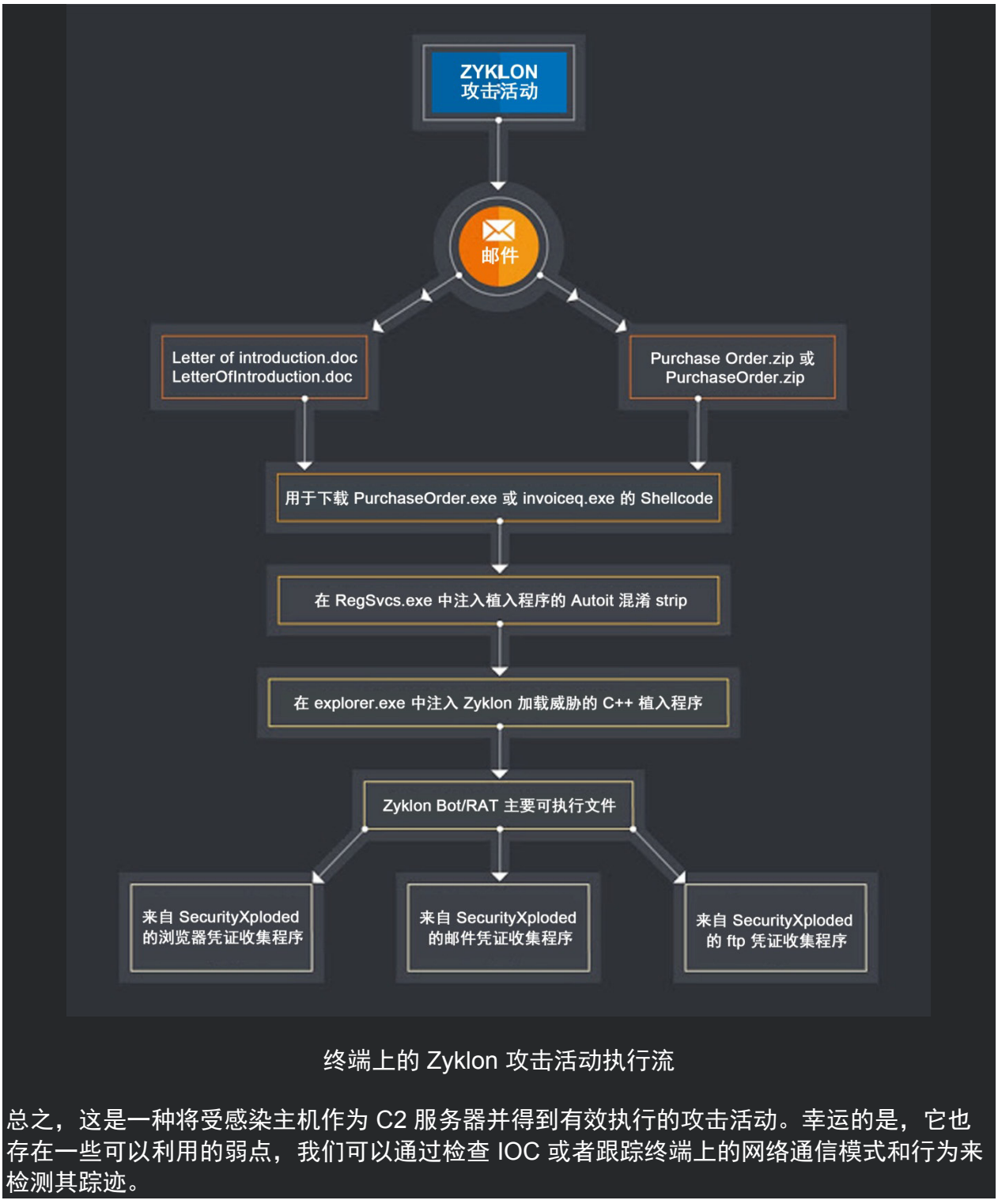
/plugin/index.php?plugin=sgminer
/plugin/index.php?plugin=socks
可用的 Zyklon 插件

下载的插件注入之前启动并挖空的合法进程，名称为“%windir%\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe”，实际上，这些插件只是以 C/C++ 编写的免费软件命令行工具，可从网站 http://www.securityxploded.com 中获取。

Zyklon 制作者可能意识到，在主要的 Zyklon 僵尸程序中完整开发所有功能将需要大量时间，因而决定加入现成的免费密码转储实用程序，以使其 RAT 在残酷的远程管理工具地下市场中更具竞争力。

结论

Zyklon 是一个臭名昭著的僵尸网络攻击包，今年一直非常猖獗。在我们分析的这一数量较少但可能更具针对性的攻击活动中，我们发现其用户利用大量不同的技术和混淆方法来提高成功几率，包括通过 Autoit 脚本和 .NET 可执行文件利用 Microsoft Word 中的漏洞，以及将免费软件实用程序用作插件，从浏览器缓存、邮件和 ftp 客户端中收集凭证。



终端上的 Zyklon 攻击活动执行流

总之，这是一种将受感染主机作为 C2 服务器并得到有效执行的攻击活动。幸运的是，它也存在一些可以利用的弱点，我们可以通过检查 IOC 或者跟踪终端上的网络通信模式和行为来检测其踪迹。

防护

产品	生产
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

具备高级安全功能的网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella 可防止对与恶意活动相关的域进行 DNS 解析。

StealthWatch 可以检测网络扫描活动、网络传播和与 CnC 基础设施的连接，从而与此活动建立联系，通知管理员。

IOC

文档漏洞
ac944374d5f50ecbdd3b9e7151d5a4b055ec18ea26482c2301ccc439164b25be

996b19658cffedc9395243693c3ca1d12a2c2a2c986e35a877f1ae2a2b595a6d

漏洞文档下载的 PE 可执行文件
4bce73a29ee1b9840cd82d8c08e107179cd74dc1aed488f6d16772ce12092c69
bcf8dbbc78883b2d84511819123cf39b1c2ffe3cd9763d08fe1544c89084cadf

ZIP 附件
e67db2e2ebd3c540489dd4844b066b45f31b2d879a085eabda1f63926ddc0688
b1906c1d23f62df7f63a06030f27c3249414d027a9deb62d27f65ec6f3a61adb

ZIP 中的 PE 可执行文件
b7101462507a8cf5bf91b62b641ef1ac3d268115d6dfca54a1625efb07fccf0d
4bce73a29ee1b9840cd82d8c08e107179cd74dc1aed488f6d16772ce12092c69

浏览器插件
e5d2c3a7ddd219ab361af4a709999a492387e3aaf8380187a7699895fc383e40

FTP 插件
6a32a0d83a5c955822502444833283a3fde8e1893f1490fac1ae5b84a00db5c6

邮件插件
bbcc07baaa00bb30de43a39a04dc66754fe805630f155fde47ab259fdbd03748

Zyklon Builder v1.0.0
682d5d60d6fc0e1d5810e9cd9d8b1c6b6fa154d5a790da944177074d28846d66

下载 URL
http://wszystkozmetalu[.]pl/Invoiceq.exe
http://www.blcpolychemical[.]com/re/PurchaseOrders.exe
http://barkliaytire[.]com
http://distriegroupelectric[.]com
http://extreime-net[.]com
http://distriegroupelectric[.]com:80/plugin/index[.]php?plugin=ftp
http://distriegroupelectric[.]com:80/plugin/index[.]php?plugin=email
http://distriegroupelectric[.]com:80/plugin/index[.]php?plugin=browser

C2

http://distriegroupelectric.com:80/gate[.]php
http://distriegroupelectric.com:80/login[.]php - Control Panel

发布者：VANJA SVAJCER；发布时间：9:05
标签：AUTOIT、僵尸网络、键盘记录器、VBA、漏洞、ZYKLON