

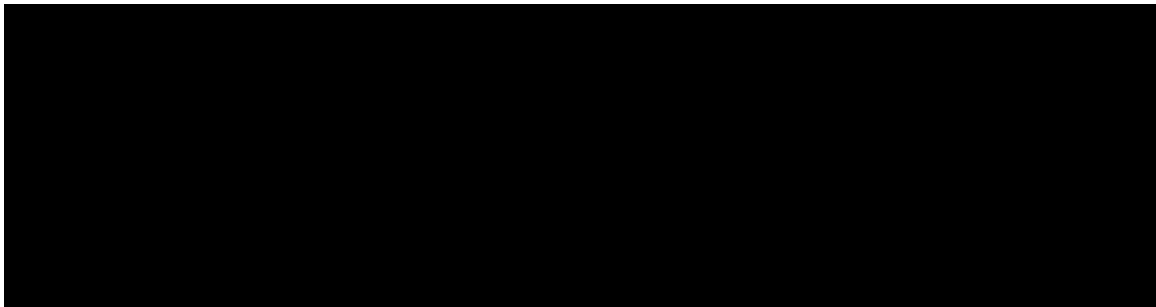


W

W

W

W

[illegible]

W

W



W

W

W

W

W

W



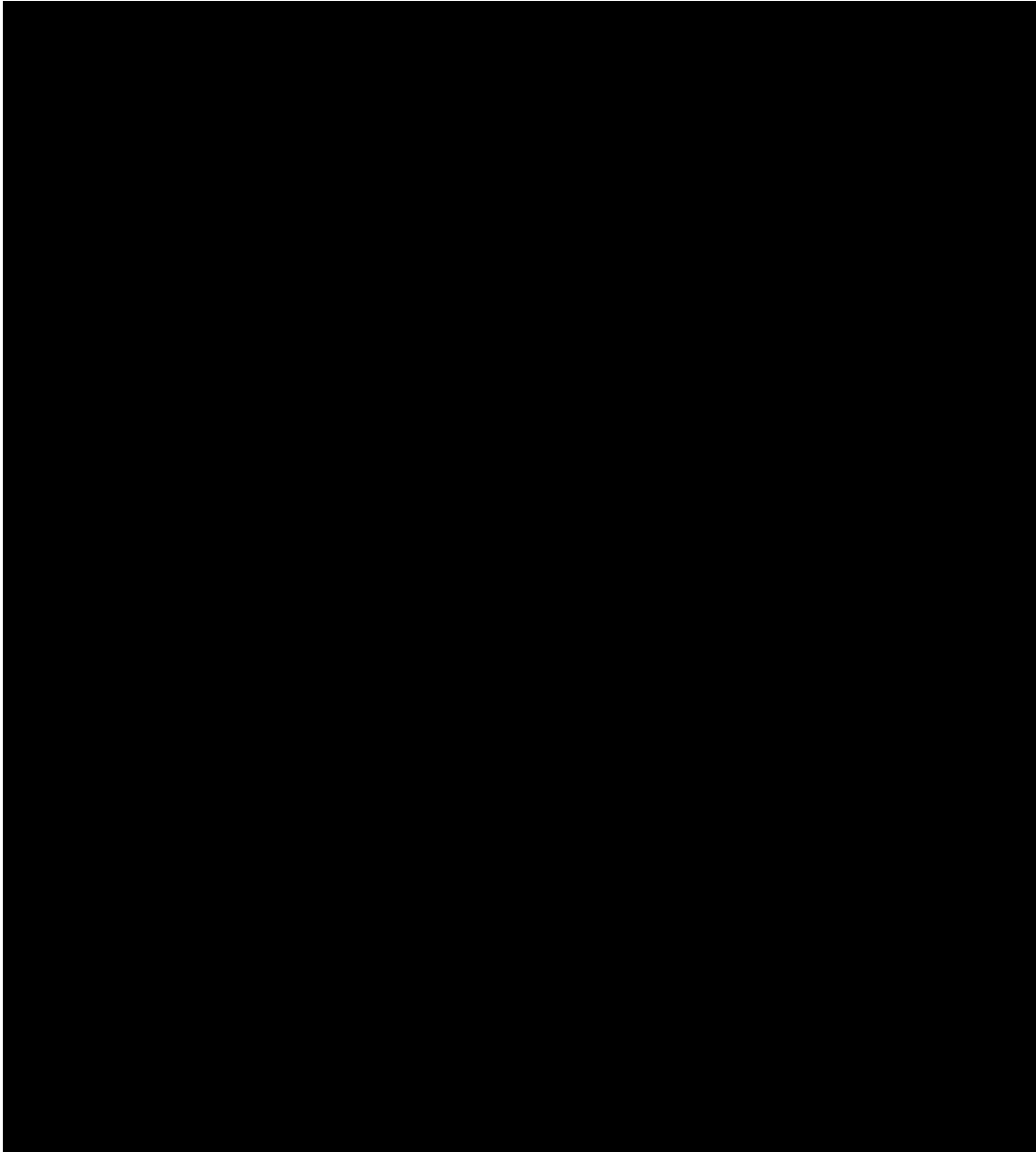
Э

Ю

Ш

Ш

Ш



Ш

1. [https://www.rosstat.gov.ru/](#) - официальный сайт Росстата

Ш







|          |          |                              |
|----------|----------|------------------------------|
| 026A5F40 | 026A5F44 |                              |
| 026A5F44 | 6B5AB522 | EPSIMP32.6B5AB522            |
| 026A5F48 | 6B5E9E30 | EPSIMP32.6B5E9E30            |
| 026A5F4C | 00000000 |                              |
| 026A5F50 | 00000000 |                              |
| 026A5F54 | 6B5E9E2F | EPSIMP32.6B5E9E2F            |
| 026A5F58 | 76ED5F18 | ntdll.ZwProtectVirtualMemory |
| 026A5F5C | 026A6140 |                              |
| 026A5F60 | FFFFFFFF |                              |
| 026A5F64 | 026A6040 |                              |

三

|          |                |                                            |
|----------|----------------|--------------------------------------------|
| 6B5D1218 | E8 46B0F0FF    | call EPSIMP32.6B5AC263                     |
| 6B5D121D | C745 D8 170000 | mov dword ptr ss:[ebp-0x28],0x17           |
|          |                | call XEPSIMP32.6B5D11EF                    |
|          |                | mov dword ptr ss:[ebp-0x28],0x17           |
|          |                | mov dword ptr ds:[026A5F54],0x17           |
|          |                | call EPSIMP32.6B5E9E25                     |
|          |                | cmp eax,edi                                |
| 6B5D1230 | 7F 03          | je XEPSIMP32.6B5D1235                      |
| 6B5D1232 | 83C8 FF        | or eax,0xFFFFFFFF                          |
|          |                | ds:[026A5F54]=6B5E9E2F (EPSIMP32.6B5E9E2F) |



|          |               |                            |
|----------|---------------|----------------------------|
| 026B682C | 8D9B 00000000 | mov ebx,edx                |
| 026B6834 | BA 4D5A0000   | lea ebx,dword ptr ds:[ebx] |
| 026B683D | 66 120412     | mov edx,0x5A4D             |
| 026B6845 | 66 120412     | cmp word ptr ds:[ebx],dx   |

|          |      |                |
|----------|------|----------------|
| 026B6857 | 5B0C | short 026B6834 |
| 026B6857 | 5B0C | ecx, -0x1      |

dx=5A4D  
ds:[026B6D17]=5A4D

| ASCII                                           | 地址       | HEX         | 数据            |
|-------------------------------------------------|----------|-------------|---------------|
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 00412035 | 56          | push esi      |
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 00412036 | 57          | push edi      |
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 00412037 | E8 FE010000 | call 00412F3A |
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 0041203C | 83F8 01     | cmp eax,0x1   |

三

|          |         |                                |
|----------|---------|--------------------------------|
| 026B6CD4 | 33D2    | xor edx,edx                    |
| 026B6CD6 | 6A 00   | push 0x0                       |
| 026B6CD8 | FFD2    | call edx                       |
| 026B6CDA | 8B45 FC | mov eax,dword ptr ss:[ebp-0x4] |
| 026B6CDD | 83C4 04 | add esp,0x4                    |
| 026B6CE0 | 6A 00   | push 0x0                       |
| 026B6CE2 | 6A 00   | push 0x0                       |

|          |       |          |
|----------|-------|----------|
| 026B6CE2 | 6A 00 | push 0x0 |
| 026B6CE2 | 6A 00 | push 0x0 |

0x8000

三

|          |             |               |
|----------|-------------|---------------|
| 00412D35 | 56          | push esi      |
| 00412D36 | 57          | push edi      |
| 00412D37 | E8 FE010000 | call 00412F3A |
| 00412D3C | 83F8 01     | cmp eax,0x1   |

|          |         |             |
|----------|---------|-------------|
| 00412D3C | 83F8 01 | cmp eax,0x1 |
| 00412D3C | 83F8 01 | cmp eax,0x1 |

short 00412D40  
ecx,0x436C68

三

|          |       |                   |
|----------|-------|-------------------|
| 00412DB8 | 74 1D | je short 00412DD7 |
| 00412DBA | 6A 00 | push 0x0          |
| 00412DBC | 6A 01 | push 0x1          |
| 00412DBE | 57    | push edi          |
| 00412DBF | FFD0  | call eax          |

|          |      |          |
|----------|------|----------|
| 00412DBF | FFD0 | call eax |
| 00412DBF | FFD0 | call eax |

short 00412DD7  
00412DCB E8 11F6FFFF 00412DE1

三

 **金睛**  
VenusEye

W

© 2006 The Authors  
Journal compilation © 2006 Blackwell Publishing Ltd

W

```

62     // 将dll文件保存到临时目录
63     if (sub_1000153C((int)v1, i))
64     {
65     }
66     // 判断是否通过rundll32执行dll
67     if ( *(BYTE *) (v13 + 0x18) && !(unsigned_int8)sub_1000158B((int)v1, i))

```

W

W

[illegible]

