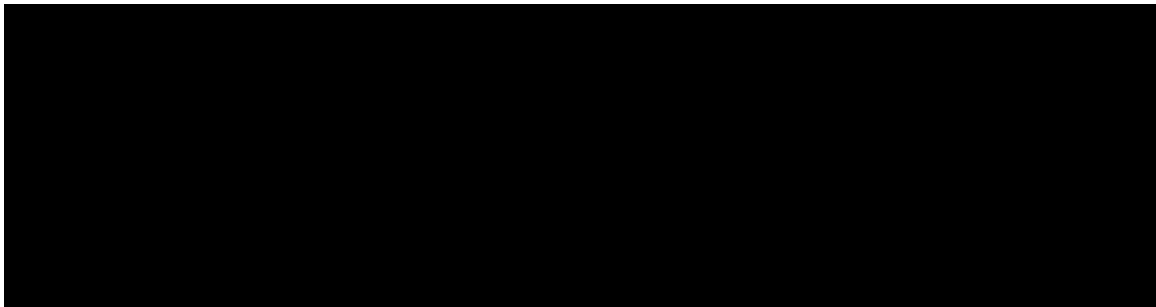


W

W

W

W

[illegible]

W

W



W

W

W

栈基地址

参数个数



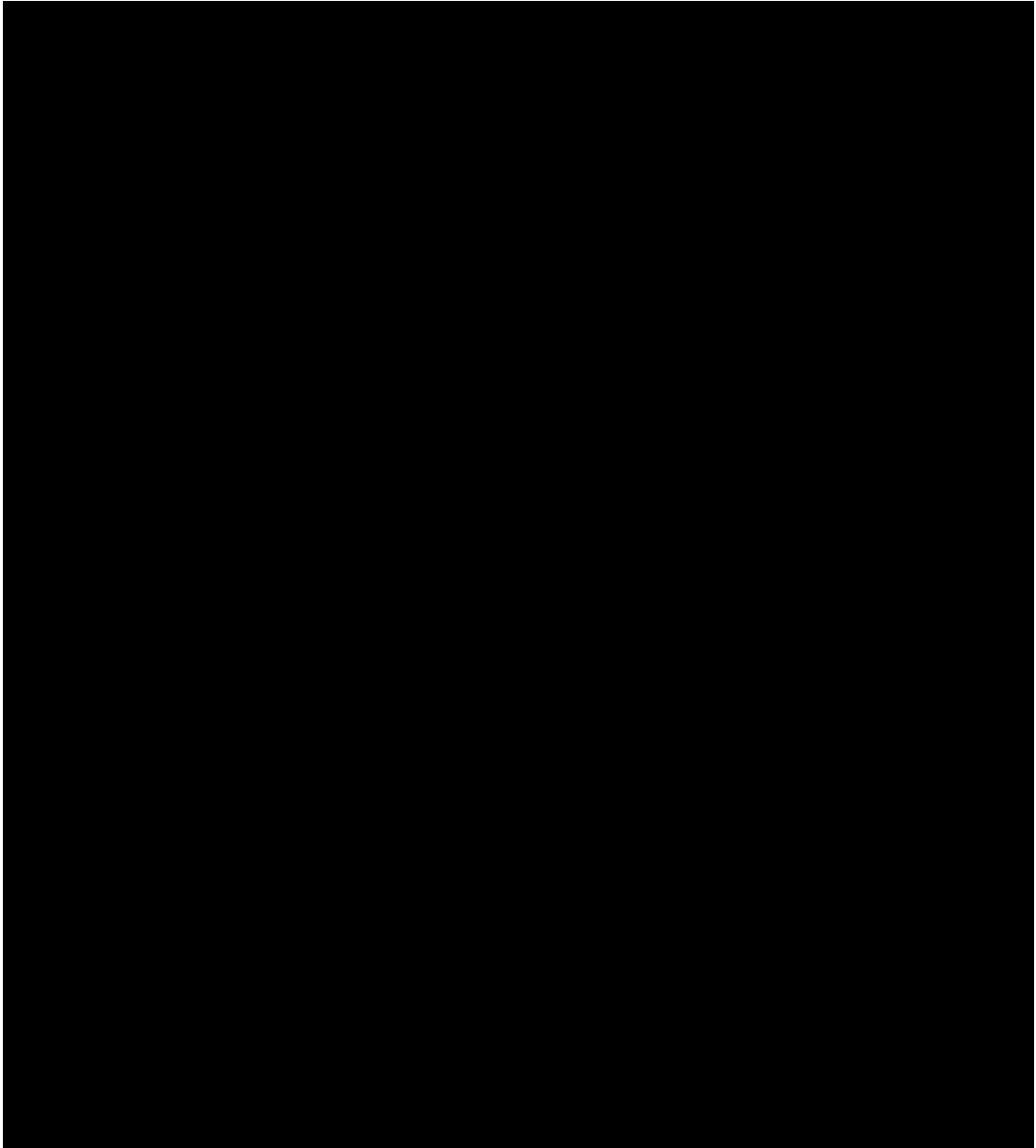
Э

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	

W

```
6B5D1218 E8 46B0FDFF call XEPSIMP32.6B5AC263  
6B5D121D C745 D8 170000 mov_dword_ptr_ss:[ebp-0x28],0x17  
  
[X] XEPSIMP32_6B5D11EF  
mov_eax, dword_ptr_ss:[ebp-0x8]  
mov_dword_ptr_ds:[ecx],eax  
[X] XEPSIMP32_6B5F9E25  
cmp_eax.edi  
[X] XEPSIMP32.6B5D1235  
or_eax,0xFFFFFFFF  
ds:[026A5F54]=6B5E9E2F (XEPSIMP32.6B5E9E2F)  
  
[X] [X] [X]  
[X] [X] [X]
```


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
026B6857	5B0C	ecx, ebx

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

0x8000

三

00412D35	56	push esi
00412D36	57	push edi
00412D37	E8 FE010000	call 00412F3A
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

short 00412DD7
00412DCB E8 11F6FFFF
00412DCB 0000

三

00412E41	6A 01	push 0x1	
00412E43	33D2	xor edx,edx	
00412E45	B9 E8974200	mov ecx,0x4297E8	WINWORD.exe
00412E4A	E8 82FEFFFF	call 00412CD1	
00412E4F	59	pop ecx	0041348C
00412E50	8BC8	mov ecx,eax	
00412E52	E8 14FDFFFF	call 00412B6B	
00412E57	85C0	test eax,eax	
00412E59	EB 04	jne 00412E5F	
00412E5A	8ACB	mov cl,byte ptr [eax]	
00412E61	E8 5CFDFFFF	call 00412B62	
00412E65	8B52	mov edx,dword ptr [edx]	

三

00412E04	57	push edi	
00412E05	58	pop edi	
00412E06	59	pop ecx	
00412E07	5A	pop edx	
00412E08	5B	pop ebx	
00412E09	5C	pop esi	
00412E0A	5D	pop ebp	
00412E0B	5E	pop esi	
00412E0C	5F	pop edi	
00412E0D	58	pop edi	
00412E0E	59	pop ecx	
00412E0F	5A	pop edx	
00412E10	5B	pop ebx	
00412E11	5C	pop esi	
00412E12	5D	pop ebp	
00412E13	5E	pop esi	
00412E14	5F	pop edi	
00412E15	58	pop edi	
00412E16	59	pop ecx	
00412E17	5A	pop edx	
00412E18	5B	pop ebx	
00412E19	5C	pop esi	
00412E1A	5D	pop ebp	
00412E1B	5E	pop esi	
00412E1C	5F	pop edi	
00412E1D	58	pop edi	
00412E1E	59	pop ecx	
00412E1F	5A	pop edx	
00412E20	5B	pop ebx	
00412E21	5C	pop esi	
00412E22	5D	pop ebp	
00412E23	5E	pop esi	
00412E24	5F	pop edi	
00412E25	58	pop edi	
00412E26	59	pop ecx	
00412E27	5A	pop edx	
00412E28	5B	pop ebx	
00412E29	5C	pop esi	
00412E2A	5D	pop ebp	
00412E2B	5E	pop esi	
00412E2C	5F	pop edi	
00412E2D	58	pop edi	
00412E2E	59	pop ecx	
00412E2F	5A	pop edx	
00412E30	5B	pop ebx	
00412E31	5C	pop esi	
00412E32	5D	pop ebp	
00412E33	5E	pop esi	
00412E34	5F	pop edi	
00412E35	58	pop edi	
00412E36	59	pop ecx	
00412E37	5A	pop edx	
00412E38	5B	pop ebx	
00412E39	5C	pop esi	
00412E3A	5D	pop ebp	
00412E3B	5E	pop esi	
00412E3C	5F	pop edi	
00412E3D	58	pop edi	
00412E3E	59	pop ecx	
00412E3F	5A	pop edx	
00412E40	5B	pop ebx	
00412E41	5C	pop esi	
00412E42	5D	pop ebp	
00412E43	5E	pop esi	
00412E44	5F	pop edi	
00412E45	58	pop edi	
00412E46	59	pop ecx	
00412E47	5A	pop edx	
00412E48	5B	pop ebx	
00412E49	5C	pop esi	
00412E4A	5D	pop ebp	
00412E4B	5E	pop esi	
00412E4C	5F	pop edi	
00412E4D	58	pop edi	
00412E4E	59	pop ecx	
00412E4F	5A	pop edx	
00412E50	5B	pop ebx	
00412E51	5C	pop esi	
00412E52	5D	pop ebp	
00412E53	5E	pop esi	
00412E54	5F	pop edi	
00412E55	58	pop edi	
00412E56	59	pop ecx	
00412E57	5A	pop edx	
00412E58	5B	pop ebx	
00412E59	5C	pop esi	
00412E5A	5D	pop ebp	
00412E5B	5E	pop esi	
00412E5C	5F	pop edi	
00412E5D	58	pop edi	
00412E5E	59	pop ecx	
00412E5F	5A	pop edx	
00412E60	5B	pop ebx	
00412E61	5C	pop esi	
00412E62	5D	pop ebp	
00412E63	5E	pop esi	
00412E64	5F	pop edi	
00412E65	58	pop edi	
00412E66	59	pop ecx	
00412E67	5A	pop edx	
00412E68	5B	pop ebx	
00412E69	5C	pop esi	
00412E6A	5D	pop ebp	
00412E6B	5E	pop esi	
00412E6C	5F	pop edi	
00412E6D	58	pop edi	
00412E6E	59	pop ecx	
00412E6F	5A	pop edx	
00412E70	5B	pop ebx	
00412E71	5C	pop esi	
00412E72	5D	pop ebp	
00412E73	5E	pop esi	
00412E74	5F	pop edi	
00412E75	58	pop edi	
00412E76	59	pop ecx	
00412E77	5A	pop edx	
00412E78	5B	pop ebx	
00412E79	5C	pop esi	
00412E7A	5D	pop ebp	
00412E7B	5E	pop esi	
00412E7C	5F	pop edi	
00412E7D	58	pop edi	
00412E7E	59	pop ecx	
00412E7F	5A	pop edx	
00412E80	5B	pop ebx	
00412E81	5C	pop esi	
00412E82	5D	pop ebp	
00412E83	5E	pop esi	
00412E84	5F	pop edi	
00412E85	58	pop edi	
00412E86	59	pop ecx	
00412E87	5A	pop edx	
00412E88	5B	pop ebx	
00412E89	5C	pop esi	
00412E8A	5D	pop ebp	
00412E8B	5E	pop esi	
00412E8C	5F	pop edi	
00412E8D	58	pop edi	
00412E8E	59	pop ecx	
00412E8F	5A	pop edx	
00412E90	5B	pop ebx	
00412E91	5C	pop esi	
00412E92	5D	pop ebp	
00412E93	5E	pop esi	
00412E94	5F	pop edi	
00412E95	58	pop edi	
00412E96	59	pop ecx	
00412E97	5A	pop edx	
00412E98	5B	pop ebx	
00412E99	5C	pop esi	
00412E9A	5D	pop ebp	
00412E9B	5E	pop esi	
00412E9C	5F	pop edi	
00412E9D	58	pop edi	
00412E9E	59	pop ecx	
00412E9F	5A	pop edx	
00412EA0	5B	pop ebx	
00412EA1	5C	pop esi	
00412EA2	5D	pop ebp	
00412EA3	5E	pop esi	
00412EA4	5F	pop edi	
00412EA5	58	pop edi	
00412EA6	59	pop ecx	
00412EA7	5A	pop edx	
00412EA8	5B	pop ebx	
00412EA9	5C	pop esi	
00412EAA	5D	pop ebp	
00412EAB	5E	pop esi	
00412EAC	5F	pop edi	
00412EAD	58	pop edi	
00412EAE	59	pop ecx	
00412EAF	5A	pop edx	
00412EB0	5B	pop ebx	
00412EB1	5C	pop esi	
00412EB2	5D	pop ebp	
00412EB3	5E	pop esi	
00412EB4	5F	pop edi	
00412EB5	58	pop edi	
00412EB6	59	pop ecx	
00412EB7	5A	pop edx	
00412EB8	5B	pop ebx	
00412EB9	5C	pop esi	
00412EBA	5D	pop ebp	
00412EBB	5E	pop esi	
00412EBC	5F	pop edi	
00412EBD	58	pop edi	
00412EBE	59	pop ecx	
00412EBF	5A	pop edx	
00412EC0	5B	pop ebx	
00412EC1	5C	pop esi	
00412EC2	5D	pop ebp	
00412EC3	5E	pop esi	
00412EC4	5F	pop edi	
00412EC5	58	pop edi	
00412EC6	59	pop ecx	
00412EC7	5A	pop edx	
00412EC8	5B	pop ebx	
00412EC9	5C	pop esi	
00412ECA	5D	pop ebp	
00412ECB	5E	pop esi	
00412ECC	5F	pop edi	
00412ECD	58	pop edi	
00412ECE	59	pop ecx	
00412ECF	5A	pop edx	
00412ED0	5B	pop ebx	
00412ED1	5C	pop esi	
00412ED2	5D	pop ebp	
00412ED3	5E	pop esi	
00412ED4	5F	pop edi	
00412ED5	58	pop edi	
00412ED6	59	pop ecx	
00412ED7	5A	pop edx	
00412ED8	5B	pop ebx	
00412ED9	5C	pop esi	
00412EDA	5D	pop ebp	
00412EDB	5E	pop esi	
00412EDC	5F	pop edi	
00412EDD	58	pop edi	
00412EDE	59	pop ecx	
00412EDF	5A	pop edx	
00412EE0	5B	pop ebx	
00412EE1	5C	pop esi	
00412EE2	5D	pop ebp	
00412EE3	5E	pop esi	
00412EE4	5F	pop edi	
00412EE5	58	pop edi	
00412EE6	59	pop ecx	
00412EE7	5A	pop edx	
00412EE8	5B	pop ebx	
00412EE9	5C	pop esi	
00412EEA	5D	pop ebp	
00412EEB	5E	pop esi	
00412EEC	5F	pop edi	
00412EED	58	pop edi	
00412EEF	59	pop ecx	
00412EF0	5A	pop edx	
00412EF1	5B	pop ebx	
00412EF2	5C	pop esi	
00412EF3	5D	pop ebp	
00412EF4	5E	pop esi	
00412EF5	5F	pop edi	
00412EF6	58	pop edi	
00412EF7	59	pop ecx	
00412EF8	5A	pop edx	
00412EF9	5B	pop ebx	
00412EFA	5C	pop esi	
00412EFB	5D	pop ebp	
00412EFC	5E	pop esi	
00412EFD	5F	pop edi	
00412EFE	58	pop edi	
00412EFF	59	pop ecx	
00412F00	5A	pop edx	
00412F01	5B	pop ebx	
00412F02	5C	pop esi	
00412F03	5D	pop ebp	
00412F04	5E	pop esi	
00412F05	5F	pop edi	
00412F06	58	pop edi	
00412F07	59	pop ecx	
00412F08	5A	pop edx	
00412F09	5B	pop ebx	
00412F0A	5C	pop esi	
00412F0B	5D	pop ebp	
00412F0C	5E	pop esi	
00412F0D	5F	pop edi	
00412F0E	58	pop edi	
00412F0F	59	pop ecx	
00412F10	5A	pop edx	
00412F11	5B	pop ebx	
00412F12	5C	pop esi	
00412F13	5D	pop ebp	
00412F14	5E	pop esi	
00412F15	5F	pop edi	
00412F16	58	pop edi	
00412F17	59	pop ecx	
00412F18	5A	pop edx	
00412F19	5B	pop ebx	
00412F1A	5C	pop esi	
00412F1B	5D	pop ebp	
00412F1C	5E	pop esi	

