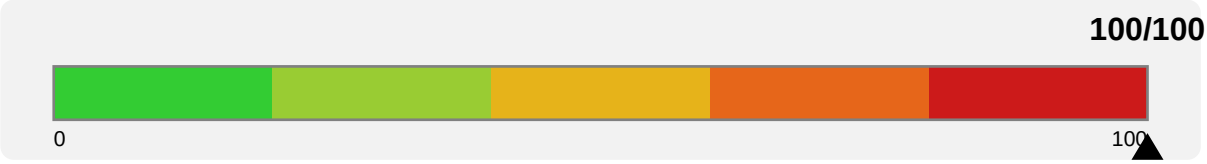
MALWARE ANALYSIS REPORT

Subject: simple_backdoor.exe

THREAT CLASSIFICATION:

MALICIOUS

Threat Score:



File Size	58.5 KB
SHA-256	8a304256092f0cbfb24b4204ce785ed9...
Analysis Date	2026-01-18 10:20 UTC
Report ID	20260118-102026

1. EXECUTIVE SUMMARY

The analyzed file has been classified as **MALICIOUS** with a threat score of **100/100**. This file exhibits characteristics consistent with malware and poses a significant security risk. Immediate containment and remediation actions are recommended.

Key Findings:

• YARA signature matches: 36 total (19 critical, 8 high severity)
• ML Classification: BENIGN (73.2% confidence)

Recommendations:

• Immediately quarantine the file and prevent execution
• Isolate affected systems from the network
• Conduct full system scan with updated antivirus software
• Preserve the file for forensic analysis
• Review system logs for signs of compromise
• Report incident to security team

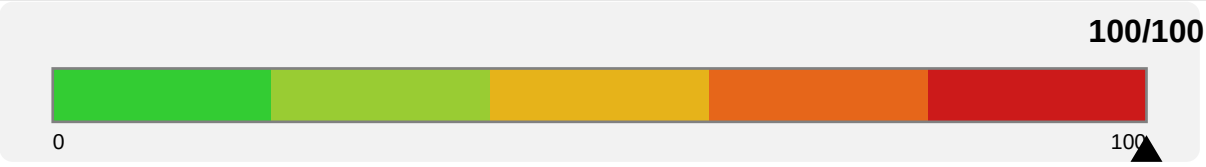
2. FILE INFORMATION

Property	Value
Filename	simple_backdoor.exe
File Size	58.5 KB
File Type	Unknown
Architecture	AMD64
Subsystem	Windows Console
Entry Point	0x000013F0
Image Base	0x140000000
Compile Time	2026-01-15T12:52:08+00:00
Is DLL	No
Is .NET	No
Is Driver	No

3. CRYPTOGRAPHIC HASHES

Algorithm	Hash Value
MD5	`a14bee091e1ac71b7e8c1cd505488142`
SHA-1	`af5b966cd98fe4c9a6519c665f394598b5179318`
SHA-256	`8a304256092f0cbfb24b4204ce785ed9f42ee0c240f4d5edb96c45eaef4c3882`
SHA-512	`4f09e54f7d61c8c199dc2103ce882cda4a97ef9f9c496f7c1c2ea6935c5d7b87...`
Import Hash	`2cbba2623ef4e20d1316b8e959a5dcdf`
Rich Header Hash	`N/A`
SSDEEP	

4. THREAT SCORE BREAKDOWN



No detailed breakdown available.

5. DIGITAL SIGNATURE & LEGITIMACY

Signature Status: ✗ NO DIGITAL SIGNATURE

Property	Value
Is Legitimate	No
Confidence	19.5%
Publisher	N/A
Reason	No legitimacy indicators found
Signer	N/A

6. YARA SIGNATURE MATCHES

Total Matches: 36 (19 critical, 8 high, 8 medium, 1 low)

Rule Name	Category	Severity	Description
Shellcode_Patterns	N/A	CRITICAL	Shellcode patterns
Backdoor_Generic	N/A	CRITICAL	Generic backdoor indicators
RevengeRAT	N/A	CRITICAL	RevengeRAT
Serverless_Function_Backdoor	N/A	CRITICAL	Serverless function backdoor
ExploitKit_Terror	N/A	CRITICAL	Terror Exploit Kit
Generic_C2_Communication	N/A	CRITICAL	Generic C2 communication
Insider_Sabotage_Tool	N/A	CRITICAL	System sabotage tool
Linux_SSH_Backdoor	N/A	CRITICAL	Linux SSH backdoor
SocGholish_FakeUpdate	N/A	CRITICAL	SocGholish fake update loader
Memory_Stack_Pivot	N/A	CRITICAL	Stack pivot technique
Memory_EggHunter	N/A	CRITICAL	Egg hunter shellcode
POS_ChewBacca	N/A	CRITICAL	ChewBacca POS Trojan
Ransomware_REvil_Sodinokibi	N/A	CRITICAL	REvil/Sodinokibi ransomware
Shellcode_x64_Common	N/A	CRITICAL	x64 shellcode patterns
Shellcode_Metasploit	N/A	CRITICAL	Metasploit shellcode patterns
Lumma_Stealer	N/A	CRITICAL	Lumma Stealer
Rhadamanthys_Stealer	N/A	CRITICAL	Rhadamanthys Stealer
Tor_Data_Exfiltration	N/A	CRITICAL	Data exfiltration via Tor

ZeroDay_Integer_Overflow	N/A	CRITICAL	Integer overflow exploit
BlueTool_Seatbelt	N/A	HIGH	Seatbelt enumeration
Obfuscation_API_Hashing	N/A	HIGH	API hashing technique
Obfuscation_XOR_Rolling	N/A	HIGH	Rolling XOR encoding
Crypter_Generic	N/A	HIGH	Generic crypter indicators
Quantum_Shor_Algorithm	N/A	HIGH	Shor's algorithm implementation
Exploit_Heap_Spray	N/A	HIGH	Heap spray pattern
SupplyChain_Typosquatting	N/A	HIGH	Typosquatting package indicators
Sandbox_Evasion_Sleep	N/A	HIGH	Sleep-based sandbox evasion
Suspicious_Strings	N/A	MEDIUM	Suspicious strings - lowered threshold
PUP_System_Optimizer	N/A	MEDIUM	Fake system optimizer
Network_Activity	N/A	MEDIUM	Suspicious network activity
Obfuscation_String_Encryption	N/A	MEDIUM	String encryption/obfuscation
Obfuscation_XOR_Single_Byte	N/A	MEDIUM	Single-byte XOR encoding
Obfuscation_Indirect_Call	N/A	MEDIUM	Indirect function calls
Obfuscation_Time_Based	N/A	MEDIUM	Time-based obfuscation
High_Entropy_Section	N/A	MEDIUM	High entropy section (possible packing/encryption)
Obfuscation_Garbage_Bytes	N/A	LOW	Garbage byte insertion

7. BEHAVIORAL ANALYSIS

Risk Level: CRITICAL (Score: 95.0)

✓ No suspicious behavioral indicators detected.

8. PE STRUCTURE ANALYSIS

Detected Anomalies:

■ Suspicious section: .bss
■ TLS callbacks present

PE Sections:

Name	Virtual Size	Raw Size	Entropy	Flags
.text	7616	7680	5.95	EXEC
.data	160	512	0.60	WRITE
.rdata	2232	2560	4.23	

.pdata	600	1024	2.55	
.xdata	492	512	3.88	
.bss	384	0	0.00	WRITE ■SUSPICIOUS
.idata	2684	3072	3.62	
.tls	16	512	0.00	WRITE
.reloc	100	512	1.30	
/4	80	512	0.23	
/19	4518	4608	5.20	
/31	181	512	2.21	
/45	164	512	1.49	
/57	72	512	0.70	
/70	163	512	2.48	
/81	504	512	4.90	

Import Summary:

Total DLLs: 11, Total Functions: 55

DLL	Function Count
api-ms-win-crt-runtime-l1-1-0.dll	14
KERNEL32.dll	10
WS2_32.dll	10
api-ms-win-crt-stdio-l1-1-0.dll	8
api-ms-win-crt-heap-l1-1-0.dll	4
api-ms-win-crt-string-l1-1-0.dll	3
api-ms-win-crt-private-l1-1-0.dll	2
api-ms-win-crt-convert-l1-1-0.dll	1
api-ms-win-crt-environment-l1-1-0.dll	1
api-ms-win-crt-locale-l1-1-0.dll	1
api-ms-win-crt-math-l1-1-0.dll	1

9. ENTROPY ANALYSIS

Overall Entropy: 0.5696 bits/byte
Assessment: NORMAL

Normal entropy levels consistent with standard executable code and data.

10. VIRUSTOTAL SCAN RESULTS

VirusTotal results not available. File may not be in VT database or API not configured.

11. MACHINE LEARNING CLASSIFICATION

Prediction: **BENIGN**
Confidence: 73.2%
Method: Unknown

12. STRINGS ANALYSIS

Total Strings Extracted: 1549

13. DISASSEMBLY ANALYSIS

Total Instructions Analyzed: 23,222

Call Instructions Summary: 83 calls found

Address	Target
0x00000A01	0x610
0x00000A99	0x2040
0x00000ACA	0x2288
0x00000AE5	rax
0x00000AF2	rax
0x00000B00	0x20c0
0x00000B26	rax
0x00000B40	rax
0x00000B4E	0x20c0
0x00000B67	0x2288
0x00000B7D	rax
0x00000BA0	rax
0x00000BC3	0x20c0
0x00000BE6	rax
0x00000BF6	0x2288
0x00000C0C	rax
0x00000C15	rax
0x00000C2B	0x2288
0x00000C57	rax
0x00000C7B	0x2288
0x00000CA6	0x20c0
0x00000CC2	0x2240
0x00000CE7	rax
0x00000D07	0x2238
0x00000D2C	rax
0x00000D44	0x2280
0x00000D5F	rax
0x00000D78	rax
0x00000D81	rax
0x00000DA3	0x2288
0x00000DB4	rax
0x00000DC0	0x2288
0x00000DDE	0x2288
0x00000DF9	0x1020
0x00000E0F	0x2288
0x00000E1E	0x2288
0x00000E2D	0x2288
0x00000E3C	0x2288

0x00000E4B	0x2288
0x00000E5A	0x2288
0x00000E88	0xa40
0x00000EA5	0x2230
0x00000EBE	0x2350
0x00000EC6	0xd91
0x00000ED5	0x2288
0x00000EE4	0xa93
0x00000EF3	0x2288
0x00000F78	rax
0x00000FD0	qword ptr [rbx]
0x000010C0	rax

...showing 50 of 83 call instructions

Entry Point Disassembly (First 200 Instructions):

Complete disassembly starting from the executable's entry point:

Address	Bytes	Instruction
0x000009F0	48 83 ec 28	sub rsp, 0x28
0x000009F4	48 8b 05 e5 32 00 00	mov rax, qword ptr [rip + 0x32e5]
0x000009FB	c7 00 00 00 00 00	mov dword ptr [rax], 0
0x00000A01	e8 0a fc ff ff	call 0x610
0x00000A06	90	nop
0x00000A07	90	nop
0x00000A08	48 83 c4 28	add rsp, 0x28
0x00000A0C	c3	ret
0x00000A0D	0f 1f 00	nop dword ptr [rax]
0x00000A10	e9 9b 18 00 00	jmp 0x22b0
0x00000A15	90	nop
0x00000A16	90	nop
0x00000A17	90	nop
0x00000A18	90	nop
0x00000A19	90	nop
0x00000A1A	90	nop
0x00000A1B	90	nop
0x00000A1C	90	nop
0x00000A1D	90	nop
0x00000A1E	90	nop
0x00000A1F	90	nop
0x00000A20	48 8d 0d 09 00 00 00	lea rcx, [rip + 9]
0x00000A27	e9 e4 ff ff ff	jmp 0xa10
0x00000A2C	0f 1f 40 00	nop dword ptr [rax]
0x00000A30	c3	ret
0x00000A31	90	nop

0x00000A32	90	nop
0x00000A33	90	nop
0x00000A34	90	nop
0x00000A35	90	nop
0x00000A36	90	nop
0x00000A37	90	nop
0x00000A38	90	nop
0x00000A39	90	nop
0x00000A3A	90	nop
0x00000A3B	90	nop
0x00000A3C	90	nop
0x00000A3D	90	nop
0x00000A3E	90	nop
0x00000A3F	90	nop
0x00000A40	55	push rbp
0x00000A41	48 89 e5	mov rbp, rsp
0x00000A44	48 83 ec 10	sub rsp, 0x10
0x00000A48	48 89 4d 10	mov qword ptr [rbp + 0x10], rcx
0x00000A4C	89 55 18	mov dword ptr [rbp + 0x18], edx
0x00000A4F	44 89 c0	mov eax, r8d
0x00000A52	88 45 20	mov byte ptr [rbp + 0x20], al
0x00000A55	c7 45 fc 00 00 00 00	mov dword ptr [rbp - 4], 0
0x00000A5C	eb 25	jmp 0xa83
0x00000A5E	8b 45 fc	mov eax, dword ptr [rbp - 4]
0x00000A61	48 98	cdqe
0x00000A63	48 8b 55 10	mov rdx, qword ptr [rbp + 0x10]
0x00000A67	48 01 d0	add rax, rdx
0x00000A6A	0f b6 00	movzx eax, byte ptr [rax]
0x00000A6D	8b 55 fc	mov edx, dword ptr [rbp - 4]
0x00000A70	48 63 d2	movsxd rdx, edx
0x00000A73	48 8b 4d 10	mov rcx, qword ptr [rbp + 0x10]
0x00000A77	48 01 ca	add rdx, rcx
0x00000A7A	32 45 20	xor al, byte ptr [rbp + 0x20]
0x00000A7D	88 02	mov byte ptr [rdx], al
0x00000A7F	83 45 fc 01	add dword ptr [rbp - 4], 1
0x00000A83	8b 45 fc	mov eax, dword ptr [rbp - 4]
0x00000A86	3b 45 18	cmp eax, dword ptr [rbp + 0x18]
0x00000A89	7c d3	jl 0xa5e
0x00000A8B	90	nop
0x00000A8C	90	nop
0x00000A8D	48 83 c4 10	add rsp, 0x10
0x00000A91	5d	pop rbp
0x00000A92	c3	ret
0x00000A93	55	push rbp

0x00000A94	b8 f0 13 00 00	mov eax, 0x13f0
0x00000A99	e8 a2 15 00 00	call 0x2040
0x00000A9E	48 29 c4	sub rsp, rax
0x00000AA1	48 8d ac 24 80 00 00	lea rbp, [rsp + 0x80]
0x00000AA9	48 89 8d 80 13 00 00	mov qword ptr [rbp + 0x1380], rcx
0x00000AB0	89 95 88 13 00 00	mov dword ptr [rbp + 0x1388], edx
0x00000AB6	c7 85 6c 13 00 00 00	mov dword ptr [rbp + 0x136c], 0x200
0x00000AC0	48 8d 05 39 2b 00 00	lea rax, [rip + 0x2b39]
0x00000AC7	48 89 c1	mov rcx, rax
0x00000ACA	e8 b9 17 00 00	call 0x2288
0x00000ACF	48 8d 85 b0 11 00 00	lea rax, [rbp + 0x11b0]
0x00000AD6	48 89 c2	mov rdx, rax
0x00000AD9	b9 02 02 00 00	mov ecx, 0x202
0x00000ADE	48 8b 05 e3 6f 00 00	mov rax, qword ptr [rip + 0x6fe3]
0x00000AE5	ff d0	call rax
0x00000AE7	85 c0	test eax, eax
0x00000AE9	74 24	je 0xb0f
0x00000AEB	48 8b 05 ce 6f 00 00	mov rax, qword ptr [rip + 0x6fce]
0x00000AF2	ff d0	call rax
0x00000AF4	89 c2	mov edx, eax
0x00000AF6	48 8d 05 1f 2b 00 00	lea rax, [rip + 0x2b1f]
0x00000AFD	48 89 c1	mov rcx, rax
0x00000B00	e8 bb 15 00 00	call 0x20c0
0x00000B05	b8 01 00 00 00	mov eax, 1
0x00000B0A	e9 79 02 00 00	jmp 0xd88
0x00000B0F	41 b8 00 00 00 00	mov r8d, 0
0x00000B15	ba 01 00 00 00	mov edx, 1
0x00000B1A	b9 02 00 00 00	mov ecx, 2
0x00000B1F	48 8b 05 da 6f 00 00	mov rax, qword ptr [rip + 0x6fda]
0x00000B26	ff d0	call rax
0x00000B28	48 89 85 60 13 00 00	mov qword ptr [rbp + 0x1360], rax
0x00000B2F	48 83 bd 60 13 00 00	cmp qword ptr [rbp + 0x1360], -1
0x00000B37	75 24	jne 0xb5d
0x00000B39	48 8b 05 80 6f 00 00	mov rax, qword ptr [rip + 0x6f80]
0x00000B40	ff d0	call rax
0x00000B42	89 c2	mov edx, eax
0x00000B44	48 8d 05 ed 2a 00 00	lea rax, [rip + 0x2aed]
0x00000B4B	48 89 c1	mov rcx, rax
0x00000B4E	e8 6d 15 00 00	call 0x20c0
0x00000B53	b8 01 00 00 00	mov eax, 1
0x00000B58	e9 2b 02 00 00	jmp 0xd88
0x00000B5D	48 8d 05 f5 2a 00 00	lea rax, [rip + 0x2af5]
0x00000B64	48 89 c1	mov rcx, rax
0x00000B67	e8 1c 17 00 00	call 0x2288

0x00000B6C	48 8b 85 80 13 00 00	mov rax, qword ptr [rbp + 0x1380]
0x00000B73	48 89 c1	mov rcx, rax
0x00000B76	48 8b 05 6b 6f 00 00	mov rax, qword ptr [rip + 0x6f6b]
0x00000B7D	ff d0	call rax
0x00000B7F	89 85 a4 11 00 00	mov dword ptr [rbp + 0x11a4], eax
0x00000B85	66 c7 85 a0 11 00 00	mov word ptr [rbp + 0x11a0], 2
0x00000B8E	8b 85 88 13 00 00	mov eax, dword ptr [rbp + 0x1388]
0x00000B94	0f b7 c0	movzx eax, ax
0x00000B97	89 c1	mov ecx, eax
0x00000B99	48 8b 05 40 6f 00 00	mov rax, qword ptr [rip + 0x6f40]
0x00000BA0	ff d0	call rax
0x00000BA2	66 89 85 a2 11 00 00	mov word ptr [rbp + 0x11a2], ax
0x00000BA9	8b 8d 88 13 00 00	mov ecx, dword ptr [rbp + 0x1388]
0x00000BAF	48 8b 95 80 13 00 00	mov rdx, qword ptr [rbp + 0x1380]
0x00000BB6	48 8d 05 b0 2a 00 00	lea rax, [rip + 0x2ab0]
0x00000BBD	41 89 c8	mov r8d, ecx
0x00000BC0	48 89 c1	mov rcx, rax
0x00000BC3	e8 f8 14 00 00	call 0x20c0
0x00000BC8	48 8d 85 a0 11 00 00	lea rax, [rbp + 0x11a0]
0x00000BCF	48 8b 8d 60 13 00 00	mov rcx, qword ptr [rbp + 0x1360]
0x00000BD6	41 b8 10 00 00 00	mov r8d, 0x10
0x00000BDC	48 89 c2	mov rdx, rax
0x00000BDF	48 8b 05 f2 6e 00 00	mov rax, qword ptr [rip + 0x6ef2]
0x00000BE6	ff d0	call rax
0x00000BE8	85 c0	test eax, eax
0x00000BEA	79 35	jns 0xc21
0x00000BEC	48 8d 05 96 2a 00 00	lea rax, [rip + 0x2a96]
0x00000BF3	48 89 c1	mov rcx, rax
0x00000BF6	e8 8d 16 00 00	call 0x2288
0x00000BFB	48 8b 85 60 13 00 00	mov rax, qword ptr [rbp + 0x1360]
0x00000C02	48 89 c1	mov rcx, rax
0x00000C05	48 8b 05 c4 6e 00 00	mov rax, qword ptr [rip + 0x6ec4]
0x00000C0C	ff d0	call rax
0x00000C0E	48 8b 05 a3 6e 00 00	mov rax, qword ptr [rip + 0x6ea3]
0x00000C15	ff d0	call rax
0x00000C17	b8 01 00 00 00	mov eax, 1
0x00000C1C	e9 67 01 00 00	jmp 0xd88
0x00000C21	48 8d 05 78 2a 00 00	lea rax, [rip + 0x2a78]
0x00000C28	48 89 c1	mov rcx, rax
0x00000C2B	e8 58 16 00 00	call 0x2288
0x00000C30	8b 95 6c 13 00 00	mov edx, dword ptr [rbp + 0x136c]
0x00000C36	48 8d 85 a0 0f 00 00	lea rax, [rbp + 0xfa0]
0x00000C3D	48 8b 8d 60 13 00 00	mov rcx, qword ptr [rbp + 0x1360]
0x00000C44	41 b9 00 00 00 00	mov r9d, 0

0x00000C4A	41 89 d0	mov r8d, edx
0x00000C4D	48 89 c2	mov rdx, rax
0x00000C50	48 8b 05 99 6e 00 00	mov rax, qword ptr [rip + 0x6e99]
0x00000C57	ff d0	call rax
0x00000C59	89 85 5c 13 00 00	mov dword ptr [rbp + 0x135c], eax
0x00000C5F	83 bd 5c 13 00 00 ff	cmp dword ptr [rbp + 0x135c], -1
0x00000C66	74 09	je 0xc71
0x00000C68	83 bd 5c 13 00 00 00	cmp dword ptr [rbp + 0x135c], 0
0x00000C6F	75 14	jne 0xc85
0x00000C71	48 8d 05 37 2a 00 00	lea rax, [rip + 0x2a37]
0x00000C78	48 89 c1	mov rcx, rax
0x00000C7B	e8 08 16 00 00	call 0x2288
0x00000C80	e9 e2 00 00 00	jmp 0xd67
0x00000C85	8b 85 5c 13 00 00	mov eax, dword ptr [rbp + 0x135c]
0x00000C8B	48 98	cdqe
0x00000C8D	c6 84 05 a0 0f 00 00	mov byte ptr [rbp + rax + 0xfa0], 0
0x00000C95	48 8d 85 a0 0f 00 00	lea rax, [rbp + 0xfa0]
0x00000C9C	48 8d 0d 23 2a 00 00	lea rcx, [rip + 0x2a23]
0x00000CA3	48 89 c2	mov rdx, rax
0x00000CA6	e8 15 14 00 00	call 0x20c0
0x00000CAB	48 8d 15 2e 2a 00 00	lea rdx, [rip + 0x2a2e]
0x00000CB2	48 8d 85 a0 0f 00 00	lea rax, [rbp + 0xfa0]
0x00000CB9	41 b8 04 00 00 00	mov r8d, 4
0x00000CBF	48 89 c1	mov rcx, rax
0x00000CC2	e8 79 15 00 00	call 0x2240
0x00000CC7	85 c0	test eax, eax
0x00000CC9	0f 84 97 00 00 00	je 0xd66
0x00000CCF	48 8d 15 0f 2a 00 00	lea rdx, [rip + 0x2a0f]
0x00000CD6	48 8d 85 a0 0f 00 00	lea rax, [rbp + 0xfa0]
0x00000CDD	48 89 c1	mov rcx, rax
0x00000CE0	48 8b 05 91 6d 00 00	mov rax, qword ptr [rip + 0x6d91]
0x00000CE7	ff d0	call rax
0x00000CE9	48 89 85 50 13 00 00	mov qword ptr [rbp + 0x1350], rax
0x00000CF0	48 83 bd 50 13 00 00	cmp qword ptr [rbp + 0x1350], 0
0x00000CF8	0f 84 32 ff ff ff	je 0xc30
0x00000CFE	eb 2e	jmp 0xd2e
0x00000D00	48 8d 45 a0	lea rax, [rbp - 0x60]
0x00000D04	48 89 c1	mov rcx, rax
0x00000D07	e8 2c 15 00 00	call 0x2238
0x00000D0C	89 c2	mov edx, eax
0x00000D0E	48 8d 45 a0	lea rax, [rbp - 0x60]
0x00000D12	48 8b 8d 60 13 00 00	mov rcx, qword ptr [rbp + 0x1360]

Extended Disassembly (Instructions 201-1000):

Address	Bytes	Instruction
0x00000D19	41 b9 00 00 00 00	mov r9d, 0
0x00000D1F	41 89 d0	mov r8d, edx
0x00000D22	48 89 c2	mov rdx, rax
0x00000D25	48 8b 05 cc 6d 00 00	mov rax, qword ptr [rip + 0x6dcc]
0x00000D2C	ff d0	call rax
0x00000D2E	48 8b 95 50 13 00 00	mov rdx, qword ptr [rbp + 0x1350]
0x00000D35	48 8d 45 a0	lea rax, [rbp - 0x60]
0x00000D39	49 89 d0	mov r8, rdx
0x00000D3C	ba 00 10 00 00	mov edx, 0x1000
0x00000D41	48 89 c1	mov rcx, rax
0x00000D44	e8 37 15 00 00	call 0x2280
0x00000D49	48 85 c0	test rax, rax
0x00000D4C	75 b2	jne 0xd00
0x00000D4E	48 8b 85 50 13 00 00	mov rax, qword ptr [rbp + 0x1350]
0x00000D55	48 89 c1	mov rcx, rax
0x00000D58	48 8b 05 11 6d 00 00	mov rax, qword ptr [rip + 0x6d11]
0x00000D5F	ff d0	call rax
0x00000D61	e9 ca fe ff ff	jmp 0xc30
0x00000D66	90	nop
0x00000D67	48 8b 85 60 13 00 00	mov rax, qword ptr [rbp + 0x1360]
0x00000D6E	48 89 c1	mov rcx, rax
0x00000D71	48 8b 05 58 6d 00 00	mov rax, qword ptr [rip + 0x6d58]
0x00000D78	ff d0	call rax
0x00000D7A	48 8b 05 37 6d 00 00	mov rax, qword ptr [rip + 0x6d37]
0x00000D81	ff d0	call rax
0x00000D83	b8 00 00 00 00	mov eax, 0
0x00000D88	48 81 c4 f0 13 00 00	add rsp, 0x13f0
0x00000D8F	5d	pop rbp
0x00000D90	c3	ret
0x00000D91	55	push rbp
0x00000D92	48 89 e5	mov rbp, rsp
0x00000D95	48 83 ec 20	sub rsp, 0x20
0x00000D99	48 8d 05 48 29 00 00	lea rax, [rip + 0x2948]
0x00000DA0	48 89 c1	mov rcx, rax
0x00000DA3	e8 e0 14 00 00	call 0x2288
0x00000DA8	b9 e8 03 00 00	mov ecx, 0x3e8
0x00000DAD	48 8b 05 7c 6b 00 00	mov rax, qword ptr [rip + 0x6b7c]
0x00000DB4	ff d0	call rax
0x00000DB6	48 8d 05 4e 29 00 00	lea rax, [rip + 0x294e]
0x00000DBD	48 89 c1	mov rcx, rax
0x00000DC0	e8 c3 14 00 00	call 0x2288
0x00000DC5	90	nop
0x00000DC6	48 83 c4 20	add rsp, 0x20
0x00000DCA	5d	pop rbp
0x00000DCB	c3	ret
0x00000DCC	55	push rbp
0x00000DCD	48 89 e5	mov rbp, rsp
0x00000DD0	48 83 ec 20	sub rsp, 0x20

0x00000DD4	48 8d 05 4d 29 00 00	lea rax, [rip + 0x294d]
0x00000DDB	48 89 c1	mov rcx, rax
0x00000DDE	e8 a5 14 00 00	call 0x2288
0x00000DE3	90	nop
0x00000DE4	48 83 c4 20	add rsp, 0x20
0x00000DE8	5d	pop rbp
0x00000DE9	c3	ret
0x00000DEA	55	push rbp
0x00000DEB	48 89 e5	mov rbp, rsp
0x00000DEE	48 83 ec 40	sub rsp, 0x40
0x00000DF2	89 4d 10	mov dword ptr [rbp + 0x10], ecx
0x00000DF5	48 89 55 18	mov qword ptr [rbp + 0x18], rdx
0x00000DF9	e8 22 02 00 00	call 0x1020
0x00000DFE	c7 45 fc 5c 11 00 00	mov dword ptr [rbp - 4], 0x115c
0x00000E05	48 8d 05 5c 29 00 00	lea rax, [rip + 0x295c]
0x00000E0C	48 89 c1	mov rcx, rax
0x00000E0F	e8 74 14 00 00	call 0x2288
0x00000E14	48 8d 05 75 29 00 00	lea rax, [rip + 0x2975]
0x00000E1B	48 89 c1	mov rcx, rax
0x00000E1E	e8 65 14 00 00	call 0x2288
0x00000E23	48 8d 05 8e 29 00 00	lea rax, [rip + 0x298e]
0x00000E2A	48 89 c1	mov rcx, rax
0x00000E2D	e8 56 14 00 00	call 0x2288
0x00000E32	48 8d 05 a7 29 00 00	lea rax, [rip + 0x29a7]
0x00000E39	48 89 c1	mov rcx, rax
0x00000E3C	e8 47 14 00 00	call 0x2288
0x00000E41	48 8d 05 c0 29 00 00	lea rax, [rip + 0x29c0]
0x00000E48	48 89 c1	mov rcx, rax
0x00000E4B	e8 38 14 00 00	call 0x2288
0x00000E50	48 8d 05 f9 29 00 00	lea rax, [rip + 0x29f9]
0x00000E57	48 89 c1	mov rcx, rax
0x00000E5A	e8 29 14 00 00	call 0x2288
0x00000E5F	48 8d 45 e0	lea rax, [rbp - 0x20]
0x00000E63	48 ba 31 32 37 2e 30	movabs rdx, 0x2e302e302e373231
0x00000E6D	48 89 10	mov qword ptr [rax], rdx
0x00000E70	66 c7 40 08 31 00	mov word ptr [rax + 8], 0x31
0x00000E76	48 8d 45 e0	lea rax, [rbp - 0x20]
0x00000E7A	41 b8 00 00 00 00	mov r8d, 0
0x00000E80	ba 09 00 00 00	mov edx, 9
0x00000E85	48 89 c1	mov rcx, rax
0x00000E88	e8 b3 fb ff ff	call 0xa40
0x00000E8D	83 7d 10 01	cmp dword ptr [rbp + 0x10], 1
0x00000E91	7e 17	jle 0xeaa
0x00000E93	48 8b 45 18	mov rax, qword ptr [rbp + 0x18]
0x00000E97	48 83 c0 08	add rax, 8
0x00000E9B	48 8b 10	mov rdx, qword ptr [rax]
0x00000E9E	48 8d 45 e0	lea rax, [rbp - 0x20]
0x00000EA2	48 89 c1	mov rcx, rax
0x00000EA5	e8 86 13 00 00	call 0x2230
0x00000EAA	83 7d 10 02	cmp dword ptr [rbp + 0x10], 2

0x00000EAE	7e 16	jle 0xec6
0x00000EB0	48 8b 45 18	mov rax, qword ptr [rbp + 0x18]
0x00000EB4	48 83 c0 10	add rax, 0x10
0x00000EB8	48 8b 00	mov rax, qword ptr [rax]
0x00000EBB	48 89 c1	mov rcx, rax
0x00000EBE	e8 8d 14 00 00	call 0x2350
0x00000EC3	89 45 fc	mov dword ptr [rbp - 4], eax
0x00000EC6	e8 c6 fe ff ff	call 0xd91
0x00000ECB	48 8d 05 be 29 00 00	lea rax, [rip + 0x29be]
0x00000ED2	48 89 c1	mov rcx, rax
0x00000ED5	e8 ae 13 00 00	call 0x2288
0x00000EDA	8b 55 fc	mov edx, dword ptr [rbp - 4]
0x00000EDD	48 8d 45 e0	lea rax, [rbp - 0x20]
0x00000EE1	48 89 c1	mov rcx, rax
0x00000EE4	e8 aa fb ff ff	call 0xa93
0x00000EE9	48 8d 05 cb 29 00 00	lea rax, [rip + 0x29cb]
0x00000EF0	48 89 c1	mov rcx, rax
0x00000EF3	e8 90 13 00 00	call 0x2288
0x00000EF8	b8 00 00 00 00	mov eax, 0
0x00000EFD	48 83 c4 40	add rsp, 0x40
0x00000F01	5d	pop rbp
0x00000F02	c3	ret
0x00000F03	90	nop
0x00000F04	90	nop
0x00000F05	90	nop
0x00000F06	90	nop
0x00000F07	90	nop
0x00000F08	90	nop
0x00000F09	90	nop
0x00000F0A	90	nop
0x00000F0B	90	nop
0x00000F0C	90	nop
0x00000F0D	90	nop
0x00000F0E	90	nop
0x00000F0F	90	nop
0x00000F10	ff 25 ea 6b 00 00	jmp qword ptr [rip + 0x6bea]
0x00000F16	90	nop
0x00000F17	90	nop
0x00000F18	ff 25 da 6b 00 00	jmp qword ptr [rip + 0x6bda]
0x00000F1E	90	nop
0x00000F1F	90	nop
0x00000F20	ff 25 ca 6b 00 00	jmp qword ptr [rip + 0x6bca]
0x00000F26	90	nop
0x00000F27	90	nop
0x00000F28	ff 25 ba 6b 00 00	jmp qword ptr [rip + 0x6bba]
0x00000F2E	90	nop
0x00000F2F	90	nop
0x00000F30	ff 25 aa 6b 00 00	jmp qword ptr [rip + 0x6baa]
0x00000F36	90	nop
0x00000F37	90	nop

0x00000F38	ff 25 9a 6b 00 00	jmp qword ptr [rip + 0x6b9a]
0x00000F3E	90	nop
0x00000F3F	90	nop
0x00000F40	ff 25 8a 6b 00 00	jmp qword ptr [rip + 0x6b8a]
0x00000F46	90	nop
0x00000F47	90	nop
0x00000F48	ff 25 7a 6b 00 00	jmp qword ptr [rip + 0x6b7a]
0x00000F4E	90	nop
0x00000F4F	90	nop
0x00000F50	ff 25 6a 6b 00 00	jmp qword ptr [rip + 0x6b6a]
0x00000F56	90	nop
0x00000F57	90	nop
0x00000F58	ff 25 5a 6b 00 00	jmp qword ptr [rip + 0x6b5a]
0x00000F5E	90	nop
0x00000F5F	90	nop
0x00000F60	48 83 ec 28	sub rsp, 0x28
0x00000F64	48 8b 05 95 16 00 00	mov rax, qword ptr [rip + 0x1695]
0x00000F6B	48 8b 00	mov rax, qword ptr [rax]
0x00000F6E	48 85 c0	test rax, rax
0x00000F71	74 22	je 0xf95
0x00000F73	0f 1f 44 00 00	nop dword ptr [rax + rax]
0x00000F78	ff d0	call rax
0x00000F7A	48 8b 05 7f 16 00 00	mov rax, qword ptr [rip + 0x167f]
0x00000F81	48 8d 50 08	lea rdx, [rax + 8]
0x00000F85	48 8b 40 08	mov rax, qword ptr [rax + 8]
0x00000F89	48 89 15 70 16 00 00	mov qword ptr [rip + 0x1670], rdx
0x00000F90	48 85 c0	test rax, rax
0x00000F93	75 e3	jne 0xf78
0x00000F95	48 83 c4 28	add rsp, 0x28
0x00000F99	c3	ret
0x00000F9A	66 0f 1f 44 00 00	nop word ptr [rax + rax]
0x00000FA0	56	push rsi
0x00000FA1	53	push rbx
0x00000FA2	48 83 ec 28	sub rsp, 0x28
0x00000FA6	48 8b 15 a3 2c 00 00	mov rdx, qword ptr [rip + 0x2ca3]
0x00000FAD	48 8b 02	mov rax, qword ptr [rdx]
0x00000FB0	83 f8 ff	cmp eax, -1
0x00000FB3	89 c1	mov ecx, eax
0x00000FB5	74 39	je 0xff0
0x00000FB7	85 c9	test ecx, ecx
0x00000FB9	74 20	je 0xfdb
0x00000FBB	89 c8	mov eax, ecx
0x00000FBD	83 e9 01	sub ecx, 1
0x00000FC0	48 8d 1c c2	lea rbx, [rdx + rax*8]
0x00000FC4	48 29 c8	sub rax, rcx
0x00000FC7	48 8d 74 c2 f8	lea rsi, [rdx + rax*8 - 8]
0x00000FCC	0f 1f 40 00	nop dword ptr [rax]
0x00000FD0	ff 13	call qword ptr [rbx]
0x00000FD2	48 83 eb 08	sub rbx, 8
0x00000FD6	48 39 f3	cmp rbx, rsi

0x00000FD9	75 f5	jne 0xfd0
0x00000FDB	48 8d 0d 7e ff ff ff	lea rcx, [rip - 0x82]
0x00000FE2	48 83 c4 28	add rsp, 0x28
0x00000FE6	5b	pop rbx
0x00000FE7	5e	pop rsi
0x00000FE8	e9 23 fa ff ff	jmp 0xa10
0x00000FED	0f 1f 00	nop dword ptr [rax]
0x00000FF0	31 c0	xor eax, eax
0x00000FF2	66 66 2e 0f 1f 84 00	nop word ptr cs:[rax + rax]
0x00000FFD	0f 1f 00	nop dword ptr [rax]
0x00001000	44 8d 40 01	lea r8d, [rax + 1]
0x00001004	89 c1	mov ecx, eax
0x00001006	4a 83 3c c2 00	cmp qword ptr [rdx + r8*8], 0
0x0000100B	4c 89 c0	mov rax, r8
0x0000100E	75 f0	jne 0x1000
0x00001010	eb a5	jmp 0xfb7
0x00001012	66 66 2e 0f 1f 84 00	nop word ptr cs:[rax + rax]
0x0000101D	0f 1f 00	nop dword ptr [rax]
0x00001020	8b 05 0a 56 00 00	mov eax, dword ptr [rip + 0x560a]
0x00001026	85 c0	test eax, eax
0x00001028	74 06	je 0x1030
0x0000102A	c3	ret
0x0000102B	0f 1f 44 00 00	nop dword ptr [rax + rax]
0x00001030	c7 05 f6 55 00 00 01	mov dword ptr [rip + 0x55f6], 1
0x0000103A	e9 61 ff ff ff	jmp 0xfa0
0x0000103F	90	nop
0x00001040	31 c0	xor eax, eax
0x00001042	c3	ret
0x00001043	90	nop
0x00001044	90	nop
0x00001045	90	nop
0x00001046	90	nop
0x00001047	90	nop
0x00001048	90	nop
0x00001049	90	nop
0x0000104A	90	nop
0x0000104B	90	nop
0x0000104C	90	nop
0x0000104D	90	nop
0x0000104E	90	nop
0x0000104F	90	nop
0x00001050	83 fa 03	cmp edx, 3
0x00001053	74 0b	je 0x1060
0x00001055	85 d2	test edx, edx
0x00001057	74 07	je 0x1060
0x00001059	c3	ret
0x0000105A	66 0f 1f 44 00 00	nop word ptr [rax + rax]
0x00001060	e9 ab 0a 00 00	jmp 0x1b10
0x00001065	66 66 2e 0f 1f 84 00	nop word ptr cs:[rax + rax]
0x00001070	56	push rsi

0x00001071	53	push rbx
0x00001072	48 83 ec 28	sub rsp, 0x28
0x00001076	48 8b 05 b3 2b 00 00	mov rax, qword ptr [rip + 0x2bb3]
0x0000107D	83 38 02	cmp dword ptr [rax], 2
0x00001080	74 06	je 0x1088
0x00001082	c7 00 02 00 00 00	mov dword ptr [rax], 2
0x00001088	83 fa 02	cmp edx, 2
0x0000108B	74 13	je 0x10a0
0x0000108D	83 fa 01	cmp edx, 1
0x00001090	74 46	je 0x10d8
0x00001092	48 83 c4 28	add rsp, 0x28
0x00001096	5b	pop rbx
0x00001097	5e	pop rsi
0x00001098	c3	ret
0x00001099	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x000010A0	48 8d 1d 09 2e 00 00	lea rbx, [rip + 0x2e09]
0x000010A7	48 8d 35 02 2e 00 00	lea rsi, [rip + 0x2e02]
0x000010AE	48 39 f3	cmp rbx, rsi
0x000010B1	74 df	je 0x1092
0x000010B3	0f 1f 44 00 00	nop dword ptr [rax + rax]
0x000010B8	48 8b 03	mov rax, qword ptr [rbx]
0x000010BB	48 85 c0	test rax, rax
0x000010BE	74 02	je 0x10c2
0x000010C0	ff d0	call rax
0x000010C2	48 83 c3 08	add rbx, 8
0x000010C6	48 39 f3	cmp rbx, rsi
0x000010C9	75 ed	jne 0x10b8
0x000010CB	48 83 c4 28	add rsp, 0x28
0x000010CF	5b	pop rbx
0x000010D0	5e	pop rsi
0x000010D1	c3	ret
0x000010D2	66 0f 1f 44 00 00	nop word ptr [rax + rax]
0x000010D8	48 83 c4 28	add rsp, 0x28
0x000010DC	5b	pop rbx
0x000010DD	5e	pop rsi
0x000010DE	e9 2d 0a 00 00	jmp 0x1b10
0x000010E3	66 66 2e 0f 1f 84 00	nop word ptr cs:[rax + rax]
0x000010EE	66 90	nop
0x000010F0	31 c0	xor eax, eax
0x000010F2	c3	ret
0x000010F3	90	nop
0x000010F4	90	nop
0x000010F5	90	nop
0x000010F6	90	nop
0x000010F7	90	nop
0x000010F8	90	nop
0x000010F9	90	nop
0x000010FA	90	nop
0x000010FB	90	nop
0x000010FC	90	nop

0x000010FD	90	nop
0x000010FE	90	nop
0x000010FF	90	nop
0x00001100	56	push rsi
0x00001101	53	push rbx
0x00001102	48 83 ec 78	sub rsp, 0x78
0x00001106	0f 29 74 24 40	movaps xmmword ptr [rsp + 0x40], xmm6
0x0000110B	0f 29 7c 24 50	movaps xmmword ptr [rsp + 0x50], xmm7
0x00001110	44 0f 29 44 24 60	movaps xmmword ptr [rsp + 0x60], xmm8
0x00001116	83 39 06	cmp dword ptr [rcx], 6
0x00001119	0f 87 cd 00 00 00	ja 0x11ec
0x0000111F	8b 01	mov eax, dword ptr [rcx]
0x00001121	48 8d 15 3c 29 00 00	lea rdx, [rip + 0x293c]
0x00001128	48 63 04 82	movsxd rax, dword ptr [rdx + rax*4]
0x0000112C	48 01 d0	add rax, rdx
0x0000112F	ff e0	jmp rax
0x00001131	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x00001138	48 8d 1d 20 28 00 00	lea rbx, [rip + 0x2820]
0x0000113F	48 8b 71 08	mov rsi, qword ptr [rcx + 8]
0x00001143	f2 44 0f 10 41 20	movsd xmm8, qword ptr [rcx + 0x20]
0x00001149	f2 0f 10 79 18	movsd xmm7, qword ptr [rcx + 0x18]
0x0000114E	f2 0f 10 71 10	movsd xmm6, qword ptr [rcx + 0x10]
0x00001153	b9 02 00 00 00	mov ecx, 2
0x00001158	e8 f3 10 00 00	call 0x2250
0x0000115D	f2 44 0f 11 44 24 30	movsd qword ptr [rsp + 0x30], xmm8
0x00001164	49 89 f1	mov r9, rsi
0x00001167	49 89 d8	mov r8, rbx
0x0000116A	f2 0f 11 7c 24 28	movsd qword ptr [rsp + 0x28], xmm7
0x00001170	48 89 c1	mov rcx, rax
0x00001173	f2 0f 11 74 24 20	movsd qword ptr [rsp + 0x20], xmm6
0x00001179	48 8d 15 b8 28 00 00	lea rdx, [rip + 0x28b8]
0x00001180	e8 9b 0f 00 00	call 0x2120
0x00001185	90	nop
0x00001186	0f 28 74 24 40	movaps xmm6, xmmword ptr [rsp + 0x40]
0x0000118B	31 c0	xor eax, eax
0x0000118D	0f 28 7c 24 50	movaps xmm7, xmmword ptr [rsp + 0x50]
0x00001192	44 0f 28 44 24 60	movaps xmm8, xmmword ptr [rsp + 0x60]
0x00001198	48 83 c4 78	add rsp, 0x78
0x0000119C	5b	pop rbx
0x0000119D	5e	pop rsi
0x0000119E	c3	ret
0x0000119F	90	nop
0x000011A0	48 8d 1d 99 27 00 00	lea rbx, [rip + 0x2799]
0x000011A7	eb 96	jmp 0x113f
0x000011A9	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x000011B0	48 8d 1d e9 27 00 00	lea rbx, [rip + 0x27e9]
0x000011B7	eb 86	jmp 0x113f
0x000011B9	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x000011C0	48 8d 1d b9 27 00 00	lea rbx, [rip + 0x27b9]
0x000011C7	e9 73 ff ff ff	jmp 0x113f

0x000011CC	0f 1f 40 00	nop dword ptr [rax]
0x000011D0	48 8d 1d 19 28 00 00	lea rbx, [rip + 0x2819]
0x000011D7	e9 63 ff ff ff	jmp 0x113f
0x000011DC	0f 1f 40 00	nop dword ptr [rax]
0x000011E0	48 8d 1d e1 27 00 00	lea rbx, [rip + 0x27e1]
0x000011E7	e9 53 ff ff ff	jmp 0x113f
0x000011EC	48 8d 1d 33 28 00 00	lea rbx, [rip + 0x2833]
0x000011F3	e9 47 ff ff ff	jmp 0x113f
0x000011F8	90	nop
0x000011F9	90	nop
0x000011FA	90	nop
0x000011FB	90	nop
0x000011FC	90	nop
0x000011FD	90	nop
0x000011FE	90	nop
0x000011FF	90	nop
0x00001200	56	push rsi
0x00001201	53	push rbx
0x00001202	48 83 ec 38	sub rsp, 0x38
0x00001206	48 8d 44 24 58	lea rax, [rsp + 0x58]
0x0000120B	48 89 cb	mov rbx, rcx
0x0000120E	b9 02 00 00 00	mov ecx, 2
0x00001213	4c 89 44 24 60	mov qword ptr [rsp + 0x60], r8
0x00001218	4c 89 4c 24 68	mov qword ptr [rsp + 0x68], r9
0x0000121D	48 89 54 24 58	mov qword ptr [rsp + 0x58], rdx
0x00001222	48 89 44 24 28	mov qword ptr [rsp + 0x28], rax
0x00001227	e8 24 10 00 00	call 0x2250
0x0000122C	48 8d 15 4d 28 00 00	lea rdx, [rip + 0x284d]
0x00001233	48 89 c1	mov rcx, rax
0x00001236	e8 e5 0e 00 00	call 0x2120
0x0000123B	48 8b 74 24 28	mov rsi, qword ptr [rsp + 0x28]
0x00001240	b9 02 00 00 00	mov ecx, 2
0x00001245	e8 06 10 00 00	call 0x2250
0x0000124A	48 89 da	mov rdx, rbx
0x0000124D	48 89 c1	mov rcx, rax
0x00001250	49 89 f0	mov r8, rsi
0x00001253	e8 28 0e 00 00	call 0x2080
0x00001258	e8 83 10 00 00	call 0x22e0
0x0000125D	90	nop
0x0000125E	66 90	nop
0x00001260	57	push rdi
0x00001261	56	push rsi
0x00001262	53	push rbx
0x00001263	48 83 ec 50	sub rsp, 0x50
0x00001267	48 63 35 36 54 00 00	movsxd rsi, dword ptr [rip + 0x5436]
0x0000126E	85 f6	test esi, esi
0x00001270	48 89 cb	mov rbx, rcx
0x00001273	0f 8e 17 01 00 00	jle 0x1390
0x00001279	48 8b 05 28 54 00 00	mov rax, qword ptr [rip + 0x5428]
0x00001280	45 31 c9	xor r9d, r9d

Address	Bytes	Instruction
0x00001283	48 83 c0 18	add rax, 0x18
0x00001287	66 0f 1f 84 00 00 00	nop word ptr [rax + rax]
0x00001290	4c 8b 00	mov r8, qword ptr [rax]
0x00001293	4c 39 c3	cmp rbx, r8
0x00001296	72 13	jb 0x12ab
0x00001298	48 8b 50 08	mov rdx, qword ptr [rax + 8]
0x0000129C	8b 52 08	mov edx, dword ptr [rdx + 8]
0x0000129F	49 01 d0	add r8, rdx
0x000012A2	4c 39 c3	cmp rbx, r8
0x000012A5	0f 82 8a 00 00 00	jb 0x1335
0x000012AB	41 83 c1 01	add r9d, 1
0x000012AF	48 83 c0 28	add rax, 0x28
0x000012B3	41 39 f1	cmp r9d, esi
0x000012B6	75 d8	jne 0x1290
0x000012B8	48 89 d9	mov rcx, rbx
0x000012BB	e8 a0 0a 00 00	call 0x1d60
0x000012C0	48 85 c0	test rax, rax
0x000012C3	48 89 c7	mov rdi, rax
0x000012C6	0f 84 e6 00 00 00	je 0x13b2
0x000012CC	48 8b 05 d5 53 00 00	mov rax, qword ptr [rip + 0x53d5]
0x000012D3	48 8d 1c b6	lea rbx, [rsi + rsi*4]
0x000012D7	48 c1 e3 03	shl rbx, 3
0x000012DB	48 01 d8	add rax, rbx
0x000012DE	48 89 78 20	mov qword ptr [rax + 0x20], rdi
0x000012E2	c7 00 00 00 00 00	mov dword ptr [rax], 0
0x000012E8	e8 b3 0b 00 00	call 0x1ea0
0x000012ED	8b 57 0c	mov edx, dword ptr [rdi + 0xc]
0x000012F0	41 b8 30 00 00 00	mov r8d, 0x30
0x000012F6	48 8d 0c 10	lea rcx, [rax + rdx]
0x000012FA	48 8b 05 a7 53 00 00	mov rax, qword ptr [rip + 0x53a7]
0x00001301	48 8d 54 24 20	lea rdx, [rsp + 0x20]
0x00001306	48 89 4c 18 18	mov qword ptr [rax + rbx + 0x18], rcx
0x0000130B	ff 15 37 66 00 00	call qword ptr [rip + 0x6637]
0x00001311	48 85 c0	test rax, rax
0x00001314	0f 84 7d 00 00 00	je 0x1397
0x0000131A	8b 44 24 44	mov eax, dword ptr [rsp + 0x44]
0x0000131E	8d 50 fc	lea edx, [rax - 4]
0x00001321	83 e2 fb	and edx, 0xfffffffb
0x00001324	74 08	je 0x132e
0x00001326	8d 50 c0	lea edx, [rax - 0x40]
0x00001329	83 e2 bf	and edx, 0xffffffbf
0x0000132C	75 12	jne 0x1340
0x0000132E	83 05 6f 53 00 00 01	add dword ptr [rip + 0x536f], 1
0x00001335	48 83 c4 50	add rsp, 0x50
0x00001339	5b	pop rbx
0x0000133A	5e	pop rsi
0x0000133B	5f	pop rdi
0x0000133C	c3	ret
0x0000133D	0f 1f 00	nop dword ptr [rax]

0x00001340	83 f8 02	cmp eax, 2
0x00001343	41 b8 40 00 00 00	mov r8d, 0x40
0x00001349	b8 04 00 00 00	mov eax, 4
0x0000134E	48 8b 4c 24 20	mov rcx, qword ptr [rsp + 0x20]
0x00001353	44 0f 44 c0	cmove r8d, eax
0x00001357	48 8b 54 24 38	mov rdx, qword ptr [rsp + 0x38]
0x0000135C	48 03 1d 45 53 00 00	add rbx, qword ptr [rip + 0x5345]
0x00001363	49 89 d9	mov r9, rbx
0x00001366	48 89 4b 08	mov qword ptr [rbx + 8], rcx
0x0000136A	48 89 53 10	mov qword ptr [rbx + 0x10], rdx
0x0000136E	ff 15 cc 65 00 00	call qword ptr [rip + 0x65cc]
0x00001374	85 c0	test eax, eax
0x00001376	75 b6	jne 0x132e
0x00001378	ff 15 92 65 00 00	call qword ptr [rip + 0x6592]
0x0000137E	48 8d 0d 73 27 00 00	lea rcx, [rip + 0x2773]
0x00001385	89 c2	mov edx, eax
0x00001387	e8 74 fe ff ff	call 0x1200
0x0000138C	0f 1f 40 00	nop dword ptr [rax]
0x00001390	31 f6	xor esi, esi
0x00001392	e9 21 ff ff ff	jmp 0x12b8
0x00001397	48 8b 05 0a 53 00 00	mov rax, qword ptr [rip + 0x530a]
0x0000139E	48 8d 0d 1b 27 00 00	lea rcx, [rip + 0x271b]
0x000013A5	8b 57 08	mov edx, dword ptr [rdi + 8]
0x000013A8	4c 8b 44 18 18	mov r8, qword ptr [rax + rbx + 0x18]
0x000013AD	e8 4e fe ff ff	call 0x1200
0x000013B2	48 8d 0d e7 26 00 00	lea rcx, [rip + 0x26e7]
0x000013B9	48 89 da	mov rdx, rbx
0x000013BC	e8 3f fe ff ff	call 0x1200
0x000013C1	90	nop
0x000013C2	66 66 2e 0f 1f 84 00	nop word ptr cs:[rax + rax]
0x000013CD	0f 1f 00	nop dword ptr [rax]
0x000013D0	55	push rbp
0x000013D1	41 57	push r15
0x000013D3	41 56	push r14
0x000013D5	41 55	push r13
0x000013D7	41 54	push r12
0x000013D9	57	push rdi
0x000013DA	56	push rsi
0x000013DB	53	push rbx
0x000013DC	48 83 ec 48	sub rsp, 0x48
0x000013E0	48 8d 6c 24 40	lea rbp, [rsp + 0x40]
0x000013E5	8b 35 b5 52 00 00	mov esi, dword ptr [rip + 0x52b5]
0x000013EB	85 f6	test esi, esi
0x000013ED	74 11	je 0x1400
0x000013EF	48 8d 65 08	lea rsp, [rbp + 8]
0x000013F3	5b	pop rbx
0x000013F4	5e	pop rsi
0x000013F5	5f	pop rdi
0x000013F6	41 5c	pop r12
0x000013F8	41 5d	pop r13

0x000013FA	41 5e	pop r14
0x000013FC	41 5f	pop r15
0x000013FE	5d	pop rbp
0x000013FF	c3	ret
0x00001400	c7 05 96 52 00 00 01	mov dword ptr [rip + 0x5296], 1
0x0000140A	e8 d1 09 00 00	call 0x1de0
0x0000140F	48 98	cdqe
0x00001411	48 8d 04 80	lea rax, [rax + rax*4]
0x00001415	48 8d 04 c5 0f 00 00	lea rax, [rax*8 + 0xf]
0x0000141D	48 83 e0 f0	and rax, 0xfffffffffffffff0
0x00001421	e8 1a 0c 00 00	call 0x2040
0x00001426	4c 8b 25 43 28 00 00	mov r12, qword ptr [rip + 0x2843]
0x0000142D	48 8b 1d 4c 28 00 00	mov rbx, qword ptr [rip + 0x284c]
0x00001434	48 29 c4	sub rsp, rax
0x00001437	c7 05 63 52 00 00 00	mov dword ptr [rip + 0x5263], 0
0x00001441	48 8d 44 24 30	lea rax, [rsp + 0x30]
0x00001446	48 89 05 5b 52 00 00	mov qword ptr [rip + 0x525b], rax
0x0000144D	4c 89 e0	mov rax, r12
0x00001450	48 29 d8	sub rax, rbx
0x00001453	48 83 f8 07	cmp rax, 7
0x00001457	7e 96	jle 0x13ef
0x00001459	48 83 f8 0b	cmp rax, 0xb
0x0000145D	0f 8f 85 01 00 00	jg 0x15e8
0x00001463	8b 03	mov eax, dword ptr [rbx]
0x00001465	85 c0	test eax, eax
0x00001467	0f 85 73 02 00 00	jne 0x16e0
0x0000146D	8b 43 04	mov eax, dword ptr [rbx + 4]
0x00001470	85 c0	test eax, eax
0x00001472	0f 85 68 02 00 00	jne 0x16e0
0x00001478	8b 53 08	mov edx, dword ptr [rbx + 8]
0x0000147B	83 fa 01	cmp edx, 1
0x0000147E	0f 85 d1 02 00 00	jne 0x1755
0x00001484	48 83 c3 0c	add rbx, 0xc
0x00001488	48 8b 3d d1 27 00 00	mov rdi, qword ptr [rip + 0x27d1]
0x0000148F	41 be ff ff ff ff	mov r14d, 0xffffffff
0x00001495	4c 39 e3	cmp rbx, r12
0x00001498	72 7c	jb 0x1516
0x0000149A	e9 50 ff ff ff	jmp 0x13ef
0x0000149F	90	nop
0x000014A0	83 fa 08	cmp edx, 8
0x000014A3	0f 84 d7 01 00 00	je 0x1680
0x000014A9	83 fa 10	cmp edx, 0x10
0x000014AC	0f 85 7b 02 00 00	jne 0x172d
0x000014B2	41 0f b7 45 00	movzx eax, word ptr [r13]
0x000014B7	41 81 e0 c0 00 00 00	and r8d, 0xc0
0x000014BE	66 85 c0	test ax, ax
0x000014C1	79 06	jns 0x14c9
0x000014C3	48 0d 00 00 ff ff	or rax, 0xffffffffffff0000
0x000014C9	4c 29 d0	sub rax, r10
0x000014CC	4c 01 c8	add rax, r9

0x000014CF	45 85 c0	test r8d, r8d
0x000014D2	48 89 45 f8	mov qword ptr [rbp - 8], rax
0x000014D6	75 18	jne 0x14f0
0x000014D8	48 3d ff ff 00 00	cmp rax, 0xffff
0x000014DE	0f 8f 5d 02 00 00	jg 0x1741
0x000014E4	48 3d 00 80 ff ff	cmp rax, -0x8000
0x000014EA	0f 8c 51 02 00 00	jl 0x1741
0x000014F0	4c 8d 7d f8	lea r15, [rbp - 8]
0x000014F4	4c 89 e9	mov rcx, r13
0x000014F7	e8 64 fd ff ff	call 0x1260
0x000014FC	41 b8 02 00 00 00	mov r8d, 2
0x00001502	4c 89 fa	mov rdx, r15
0x00001505	4c 89 e9	mov rcx, r13
0x00001508	e8 eb 0d 00 00	call 0x22f8
0x0000150D	48 83 c3 0c	add rbx, 0xc
0x00001511	4c 39 e3	cmp rbx, r12
0x00001514	73 7a	jae 0x1590
0x00001516	44 8b 43 08	mov r8d, dword ptr [rbx + 8]
0x0000151A	44 8b 13	mov r10d, dword ptr [rbx]
0x0000151D	8b 4b 04	mov ecx, dword ptr [rbx + 4]
0x00001520	41 0f b6 d0	movzx edx, r8b
0x00001524	49 01 fa	add r10, rdi
0x00001527	83 fa 20	cmp edx, 0x20
0x0000152A	4d 8b 0a	mov r9, qword ptr [r10]
0x0000152D	4c 8d 2c 39	lea r13, [rcx + rdi]
0x00001531	0f 84 d9 00 00 00	je 0x1610
0x00001537	0f 86 63 ff ff ff	jbe 0x14a0
0x0000153D	83 fa 40	cmp edx, 0x40
0x00001540	0f 85 e7 01 00 00	jne 0x172d
0x00001546	49 8b 45 00	mov rax, qword ptr [r13]
0x0000154A	4c 29 d0	sub rax, r10
0x0000154D	4c 01 c8	add rax, r9
0x00001550	41 81 e0 c0 00 00 00	and r8d, 0xc0
0x00001557	48 89 45 f8	mov qword ptr [rbp - 8], rax
0x0000155B	75 09	jne 0x1566
0x0000155D	48 85 c0	test rax, rax
0x00001560	0f 89 db 01 00 00	jns 0x1741
0x00001566	4c 8d 7d f8	lea r15, [rbp - 8]
0x0000156A	4c 89 e9	mov rcx, r13
0x0000156D	48 83 c3 0c	add rbx, 0xc
0x00001571	e8 ea fc ff ff	call 0x1260
0x00001576	41 b8 08 00 00 00	mov r8d, 8
0x0000157C	4c 89 fa	mov rdx, r15
0x0000157F	4c 89 e9	mov rcx, r13
0x00001582	e8 71 0d 00 00	call 0x22f8
0x00001587	4c 39 e3	cmp rbx, r12
0x0000158A	72 8a	jb 0x1516
0x0000158C	0f 1f 40 00	nop dword ptr [rax]
0x00001590	8b 05 0e 51 00 00	mov eax, dword ptr [rip + 0x510e]
0x00001596	31 db	xor ebx, ebx

0x00001598	48 8b 3d a1 63 00 00	mov rdi, qword ptr [rip + 0x63a1]
0x0000159F	85 c0	test eax, eax
0x000015A1	0f 8e 48 fe ff ff	jle 0x13ef
0x000015A7	66 0f 1f 84 00 00 00	nop word ptr [rax + rax]
0x000015B0	48 8b 05 f1 50 00 00	mov rax, qword ptr [rip + 0x50f1]
0x000015B7	48 01 d8	add rax, rbx
0x000015BA	44 8b 00	mov r8d, dword ptr [rax]
0x000015BD	45 85 c0	test r8d, r8d
0x000015C0	74 0d	je 0x15cf
0x000015C2	48 8b 50 10	mov rdx, qword ptr [rax + 0x10]
0x000015C6	4d 89 f9	mov r9, r15
0x000015C9	48 8b 48 08	mov rcx, qword ptr [rax + 8]
0x000015CD	ff d7	call rdi
0x000015CF	83 c6 01	add esi, 1
0x000015D2	48 83 c3 28	add rbx, 0x28
0x000015D6	3b 35 c8 50 00 00	cmp esi, dword ptr [rip + 0x50c8]
0x000015DC	7c d2	jl 0x15b0
0x000015DE	e9 0c fe ff ff	jmp 0x13ef
0x000015E3	0f 1f 44 00 00	nop dword ptr [rax + rax]
0x000015E8	8b 13	mov edx, dword ptr [rbx]
0x000015EA	85 d2	test edx, edx
0x000015EC	0f 85 ee 00 00 00	jne 0x16e0
0x000015F2	8b 43 04	mov eax, dword ptr [rbx + 4]
0x000015F5	89 c7	mov edi, eax
0x000015F7	0b 7b 08	or edi, dword ptr [rbx + 8]
0x000015FA	0f 85 70 fe ff ff	jne 0x1470
0x00001600	48 83 c3 0c	add rbx, 0xc
0x00001604	e9 5a fe ff ff	jmp 0x1463
0x00001609	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x00001610	41 8b 45 00	mov eax, dword ptr [r13]
0x00001614	41 81 e0 c0 00 00 00	and r8d, 0xc0
0x0000161B	85 c0	test eax, eax
0x0000161D	79 0d	jns 0x162c
0x0000161F	48 b9 00 00 00 00 ff	movabs rcx, 0xffffffff00000000
0x00001629	48 09 c8	or rax, rcx
0x0000162C	4c 29 d0	sub rax, r10
0x0000162F	4c 01 c8	add rax, r9
0x00001632	45 85 c0	test r8d, r8d
0x00001635	48 89 45 f8	mov qword ptr [rbp - 8], rax
0x00001639	75 1c	jne 0x1657
0x0000163B	4c 39 f0	cmp rax, r14
0x0000163E	0f 8f fd 00 00 00	jg 0x1741
0x00001644	48 b9 ff ff ff 7f ff	movabs rcx, 0xffffffff7fffffff
0x0000164E	48 39 c8	cmp rax, rcx
0x00001651	0f 8e ea 00 00 00	jle 0x1741
0x00001657	4c 8d 7d f8	lea r15, [rbp - 8]
0x0000165B	4c 89 e9	mov rcx, r13
0x0000165E	e8 fd fb ff ff	call 0x1260
0x00001663	41 b8 04 00 00 00	mov r8d, 4
0x00001669	4c 89 fa	mov rdx, r15

0x0000166C	4c 89 e9	mov rcx, r13
0x0000166F	e8 84 0c 00 00	call 0x22f8
0x00001674	e9 94 fe ff ff	jmp 0x150d
0x00001679	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x00001680	41 0f b6 45 00	movzx eax, byte ptr [r13]
0x00001685	41 81 e0 c0 00 00 00	and r8d, 0xc0
0x0000168C	84 c0	test al, al
0x0000168E	79 06	jns 0x1696
0x00001690	48 0d 00 ff ff ff	or rax, 0xffffffffffffff00
0x00001696	4c 29 d0	sub rax, r10
0x00001699	4c 01 c8	add rax, r9
0x0000169C	45 85 c0	test r8d, r8d
0x0000169F	48 89 45 f8	mov qword ptr [rbp - 8], rax
0x000016A3	75 16	jne 0x16bb
0x000016A5	48 3d ff 00 00 00	cmp rax, 0xff
0x000016AB	0f 8f 90 00 00 00	jg 0x1741
0x000016B1	48 83 f8 80	cmp rax, -0x80
0x000016B5	0f 8c 86 00 00 00	jl 0x1741
0x000016BB	4c 8d 7d f8	lea r15, [rbp - 8]
0x000016BF	4c 89 e9	mov rcx, r13
0x000016C2	e8 99 fb ff ff	call 0x1260
0x000016C7	41 b8 01 00 00 00	mov r8d, 1
0x000016CD	4c 89 fa	mov rdx, r15
0x000016D0	4c 89 e9	mov rcx, r13
0x000016D3	e8 20 0c 00 00	call 0x22f8
0x000016D8	e9 30 fe ff ff	jmp 0x150d
0x000016DD	0f 1f 00	nop dword ptr [rax]
0x000016E0	4c 39 e3	cmp rbx, r12
0x000016E3	0f 83 06 fd ff ff	jae 0x13ef
0x000016E9	4c 8b 2d 70 25 00 00	mov r13, qword ptr [rip + 0x2570]
0x000016F0	4c 8d 7d f8	lea r15, [rbp - 8]
0x000016F4	0f 1f 40 00	nop dword ptr [rax]
0x000016F8	8b 7b 04	mov edi, dword ptr [rbx + 4]
0x000016FB	48 83 c3 08	add rbx, 8
0x000016FF	8b 43 f8	mov eax, dword ptr [rbx - 8]
0x00001702	4c 01 ef	add rdi, r13
0x00001705	03 07	add eax, dword ptr [rdi]
0x00001707	48 89 f9	mov rcx, rdi
0x0000170A	89 45 f8	mov dword ptr [rbp - 8], eax
0x0000170D	e8 4e fb ff ff	call 0x1260
0x00001712	41 b8 04 00 00 00	mov r8d, 4
0x00001718	4c 89 fa	mov rdx, r15
0x0000171B	48 89 f9	mov rcx, rdi
0x0000171E	e8 d5 0b 00 00	call 0x22f8
0x00001723	4c 39 e3	cmp rbx, r12
0x00001726	72 d0	jb 0x16f8
0x00001728	e9 63 fe ff ff	jmp 0x1590
0x0000172D	48 8d 0d 24 24 00 00	lea rcx, [rip + 0x2424]
0x00001734	48 c7 45 f8 00 00 00	mov qword ptr [rbp - 8], 0
0x0000173C	e8 bf fa ff ff	call 0x1200

0x00001741	48 89 44 24 20	mov qword ptr [rsp + 0x20], rax
0x00001746	48 8d 0d 3b 24 00 00	lea rcx, [rip + 0x243b]
0x0000174D	4d 89 e8	mov r8, r13
0x00001750	e8 ab fa ff ff	call 0x1200
0x00001755	48 8d 0d c4 23 00 00	lea rcx, [rip + 0x23c4]
0x0000175C	e8 9f fa ff ff	call 0x1200
0x00001761	90	nop
0x00001762	90	nop
0x00001763	90	nop
0x00001764	90	nop
0x00001765	90	nop
0x00001766	90	nop
0x00001767	90	nop
0x00001768	90	nop
0x00001769	90	nop
0x0000176A	90	nop
0x0000176B	90	nop
0x0000176C	90	nop
0x0000176D	90	nop
0x0000176E	90	nop
0x0000176F	90	nop
0x00001770	48 83 ec 58	sub rsp, 0x58
0x00001774	48 8b 05 35 4f 00 00	mov rax, qword ptr [rip + 0x4f35]
0x0000177B	48 85 c0	test rax, rax
0x0000177E	66 0f 14 d3	unpcklpd xmm2, xmm3
0x00001782	74 25	je 0x17a9
0x00001784	f2 0f 10 84 24 80 00	movsd xmm0, qword ptr [rsp + 0x80]
0x0000178D	89 4c 24 20	mov dword ptr [rsp + 0x20], ecx
0x00001791	48 8d 4c 24 20	lea rcx, [rsp + 0x20]
0x00001796	48 89 54 24 28	mov qword ptr [rsp + 0x28], rdx
0x0000179B	0f 29 54 24 30	movaps xmmword ptr [rsp + 0x30], xmm2
0x000017A0	f2 0f 11 44 24 40	movsd qword ptr [rsp + 0x40], xmm0
0x000017A6	ff d0	call rax
0x000017A8	90	nop
0x000017A9	48 83 c4 58	add rsp, 0x58
0x000017AD	c3	ret
0x000017AE	66 90	nop
0x000017B0	48 89 0d f9 4e 00 00	mov qword ptr [rip + 0x4ef9], rcx
0x000017B7	e9 44 0b 00 00	jmp 0x2300
0x000017BC	90	nop
0x000017BD	90	nop
0x000017BE	90	nop
0x000017BF	90	nop
0x000017C0	53	push rbx
0x000017C1	48 83 ec 20	sub rsp, 0x20
0x000017C5	48 8b 11	mov rdx, qword ptr [rcx]
0x000017C8	8b 02	mov eax, dword ptr [rdx]
0x000017CA	48 89 cb	mov rbx, rcx
0x000017CD	89 c1	mov ecx, eax
0x000017CF	81 e1 ff ff ff 20	and ecx, 0x20ffffff

0x000017D5	81 f9 43 43 47 20	cmp ecx, 0x20474343
0x000017DB	0f 84 8f 00 00 00	je 0x1870
0x000017E1	3d 96 00 00 c0	cmp eax, 0xc0000096
0x000017E6	77 47	ja 0x182f
0x000017E8	3d 8b 00 00 c0	cmp eax, 0xc000008b
0x000017ED	76 61	jbe 0x1850
0x000017EF	05 73 ff ff 3f	add eax, 0x3fffff73
0x000017F4	83 f8 09	cmp eax, 9
0x000017F7	77 6b	ja 0x1864
0x000017F9	48 8d 15 e0 23 00 00	lea rdx, [rip + 0x23e0]
0x00001800	48 63 04 82	movsxd rax, dword ptr [rdx + rax*4]
0x00001804	48 01 d0	add rax, rdx
0x00001807	ff e0	jmp rax
0x00001809	0f 1f 80 00 00 00 00	nop dword ptr [rax]
0x00001810	31 d2	xor edx, edx
0x00001812	b9 08 00 00 00	mov ecx, 8
0x00001817	e8 cc 0a 00 00	call 0x22e8
0x0000181C	48 83 f8 01	cmp rax, 1
0x00001820	0f 84 3e 01 00 00	je 0x1964
0x00001826	48 85 c0	test rax, rax
0x00001829	0f 85 01 01 00 00	jne 0x1930
0x0000182F	48 8b 05 9a 4e 00 00	mov rax, qword ptr [rip + 0x4e9a]
0x00001836	48 85 c0	test rax, rax
0x00001839	74 45	je 0x1880
0x0000183B	48 89 d9	mov rcx, rbx
0x0000183E	48 83 c4 20	add rsp, 0x20
0x00001842	5b	pop rbx
0x00001843	48 ff e0	jmp rax
0x00001846	66 2e 0f 1f 84 00 00	nop word ptr cs:[rax + rax]
0x00001850	3d 05 00 00 c0	cmp eax, 0xc0000005
0x00001855	0f 84 a5 00 00 00	je 0x1900
0x0000185B	77 33	ja 0x1890
0x0000185D	3d 02 00 00 80	cmp eax, 0x80000002
0x00001862	75 cb	jne 0x182f
0x00001864	b8 ff ff ff ff	mov eax, 0xffffffff
0x00001869	48 83 c4 20	add rsp, 0x20
0x0000186D	5b	pop rbx
0x0000186E	c3	ret
0x0000186F	90	nop
0x00001870	f6 42 04 01	test byte ptr [rdx + 4], 1
0x00001874	0f 85 67 ff ff ff	jne 0x17e1
0x0000187A	eb e8	jmp 0x1864
0x0000187C	0f 1f 40 00	nop dword ptr [rax]
0x00001880	31 c0	xor eax, eax
0x00001882	48 83 c4 20	add rsp, 0x20
0x00001886	5b	pop rbx
0x00001887	c3	ret
0x00001888	0f 1f 84 00 00 00 00	nop dword ptr [rax + rax]
0x00001890	3d 08 00 00 c0	cmp eax, 0xc0000008
0x00001895	74 cd	je 0x1864

0x00001897	3d 1d 00 00 c0	cmp eax, 0xc000001d
0x0000189C	75 91	jne 0x182f
0x0000189E	31 d2	xor edx, edx

Note: Showing 1,000 of 23,222 total instructions. Full disassembly available in raw analysis data.

Raw Disassembly Code Dump:

Complete text dump of disassembled code for detailed analysis:

```
0x000009F0: sub rsp, 0x28
0x000009F4: mov rax, qword ptr [rip + 0x32e5]
0x000009FB: mov dword ptr [rax], 0
0x00000A01: call 0x610
0x00000A06: nop
0x00000A07: nop
0x00000A08: add rsp, 0x28
0x00000A0C: ret
0x00000A0D: nop dword ptr [rax]
0x00000A10: jmp 0x22b0
0x00000A15: nop
0x00000A16: nop
0x00000A17: nop
0x00000A18: nop
0x00000A19: nop
0x00000A1A: nop
0x00000A1B: nop
0x00000A1C: nop
0x00000A1D: nop
0x00000A1E: nop
0x00000A1F: nop
0x00000A20: lea rcx, [rip + 9]
0x00000A27: jmp 0xa10
0x00000A2C: nop dword ptr [rax]
0x00000A30: ret
0x00000A31: nop
0x00000A32: nop
0x00000A33: nop
0x00000A34: nop
0x00000A35: nop
0x00000A36: nop
0x00000A37: nop
0x00000A38: nop
0x00000A39: nop
0x00000A3A: nop
0x00000A3B: nop
0x00000A3C: nop
0x00000A3D: nop
0x00000A3E: nop
0x00000A3F: nop
0x00000A40: push rbp
0x00000A41: mov rbp, rsp
0x00000A44: sub rsp, 0x10
0x00000A48: mov qword ptr [rbp + 0x10], rcx
0x00000A4C: mov dword ptr [rbp + 0x18], edx
0x00000A4F: mov eax, r8d
0x00000A52: mov byte ptr [rbp + 0x20], al
0x00000A55: mov dword ptr [rbp - 4], 0
0x00000A5C: jmp 0xa83
0x00000A5E: mov eax, dword ptr [rbp - 4]

0x00000A61: cdqe
0x00000A63: mov rdx, qword ptr [rbp + 0x10]
0x00000A67: add rax, rdx
0x00000A6A: movzx eax, byte ptr [rax]
0x00000A6D: mov edx, dword ptr [rbp - 4]
```

```
0x00000A70: movsxd rdx, edx
0x00000A73: mov rcx, qword ptr [rbp + 0x10]
0x00000A77: add rdx, rcx
0x00000A7A: xor al, byte ptr [rbp + 0x20]
0x00000A7D: mov byte ptr [rdx], al
0x00000A7F: add dword ptr [rbp - 4], 1
0x00000A83: mov eax, dword ptr [rbp - 4]
0x00000A86: cmp eax, dword ptr [rbp + 0x18]
0x00000A89: jl 0xa5e
0x00000A8B: nop
0x00000A8C: nop
0x00000A8D: add rsp, 0x10
0x00000A91: pop rbp
0x00000A92: ret
0x00000A93: push rbp
0x00000A94: mov eax, 0x13f0
0x00000A99: call 0x2040
0x00000A9E: sub rsp, rax
0x00000AA1: lea rbp, [rsp + 0x80]
0x00000AA9: mov qword ptr [rbp + 0x1380], rcx
0x00000AB0: mov dword ptr [rbp + 0x1388], edx
0x00000AB6: mov dword ptr [rbp + 0x136c], 0x200
0x00000AC0: lea rax, [rip + 0x2b39]
0x00000AC7: mov rcx, rax
0x00000ACA: call 0x2288
0x00000ACF: lea rax, [rbp + 0x11b0]
0x00000AD6: mov rdx, rax
0x00000AD9: mov ecx, 0x202
0x00000ADE: mov rax, qword ptr [rip + 0x6fe3]
0x00000AE5: call rax
0x00000AE7: test eax, eax
0x00000AE9: je 0xb0f
0x00000AEB: mov rax, qword ptr [rip + 0x6fce]
0x00000AF2: call rax
0x00000AF4: mov edx, eax
0x00000AF6: lea rax, [rip + 0x2b1f]
0x00000AFD: mov rcx, rax
0x00000B00: call 0x20c0
0x00000B05: mov eax, 1
0x00000B0A: jmp 0xd88
0x00000B0F: mov r8d, 0
0x00000B15: mov edx, 1
0x00000B1A: mov ecx, 2
0x00000B1F: mov rax, qword ptr [rip + 0x6fda]
0x00000B26: call rax
0x00000B28: mov qword ptr [rbp + 0x1360], rax
0x00000B2F: cmp qword ptr [rbp + 0x1360], -1
0x00000B37: jne 0xb5d
0x00000B39: mov rax, qword ptr [rip + 0x6f80]
0x00000B40: call rax
0x00000B42: mov edx, eax
0x00000B44: lea rax, [rip + 0x2aed]
0x00000B4B: mov rcx, rax
0x00000B4E: call 0x20c0
0x00000B53: mov eax, 1
0x00000B58: jmp 0xd88
0x00000B5D: lea rax, [rip + 0x2af5]
```

```
0x00000B64: mov rcx, rax
0x00000B67: call 0x2288
0x00000B6C: mov rax, qword ptr [rbp + 0x1380]
0x00000B73: mov rcx, rax
0x00000B76: mov rax, qword ptr [rip + 0x6f6b]
0x00000B7D: call rax
0x00000B7F: mov dword ptr [rbp + 0x11a4], eax
0x00000B85: mov word ptr [rbp + 0x11a0], 2
0x00000B8E: mov eax, dword ptr [rbp + 0x1388]
0x00000B94: movzx eax, ax
0x00000B97: mov ecx, eax
0x00000B99: mov rax, qword ptr [rip + 0x6f40]
0x00000BA0: call rax
0x00000BA2: mov word ptr [rbp + 0x11a2], ax
0x00000BA9: mov ecx, dword ptr [rbp + 0x1388]
0x00000BAF: mov rdx, qword ptr [rbp + 0x1380]
0x00000BB6: lea rax, [rip + 0x2ab0]
0x00000BBD: mov r8d, ecx
0x00000BC0: mov rcx, rax
0x00000BC3: call 0x20c0
0x00000BC8: lea rax, [rbp + 0x11a0]
0x00000BCF: mov rcx, qword ptr [rbp + 0x1360]
0x00000BD6: mov r8d, 0x10
0x00000BDC: mov rdx, rax
0x00000BDF: mov rax, qword ptr [rip + 0x6ef2]
0x00000BE6: call rax
0x00000BE8: test eax, eax
0x00000BEA: jns 0xc21
0x00000BEC: lea rax, [rip + 0x2a96]
0x00000BF3: mov rcx, rax
0x00000BF6: call 0x2288
0x00000BFB: mov rax, qword ptr [rbp + 0x1360]
0x00000C02: mov rcx, rax
0x00000C05: mov rax, qword ptr [rip + 0x6ec4]
0x00000C0C: call rax
0x00000C0E: mov rax, qword ptr [rip + 0x6ea3]
0x00000C15: call rax
0x00000C17: mov eax, 1
0x00000C1C: jmp 0xd88
0x00000C21: lea rax, [rip + 0x2a78]
0x00000C28: mov rcx, rax
0x00000C2B: call 0x2288
0x00000C30: mov edx, dword ptr [rbp + 0x136c]
0x00000C36: lea rax, [rbp + 0xfa0]
0x00000C3D: mov rcx, qword ptr [rbp + 0x1360]
0x00000C44: mov r9d, 0
0x00000C4A: mov r8d, edx
0x00000C4D: mov rdx, rax
0x00000C50: mov rax, qword ptr [rip + 0x6e99]
0x00000C57: call rax
0x00000C59: mov dword ptr [rbp + 0x135c], eax
0x00000C5F: cmp dword ptr [rbp + 0x135c], -1
0x00000C66: je 0xc71
0x00000C68: cmp dword ptr [rbp + 0x135c], 0
0x00000C6F: jne 0xc85
0x00000C71: lea rax, [rip + 0x2a37]
0x00000C78: mov rcx, rax
```

```
0x00000C7B: call 0x2288
0x00000C80: jmp 0xd67
0x00000C85: mov eax, dword ptr [rbp + 0x135c]
0x00000C8B: cdqe
0x00000C8D: mov byte ptr [rbp + rax + 0xfa0], 0
0x00000C95: lea rax, [rbp + 0xfa0]
0x00000C9C: lea rcx, [rip + 0x2a23]
0x00000CA3: mov rdx, rax
0x00000CA6: call 0x20c0
0x00000CAB: lea rdx, [rip + 0x2a2e]
0x00000CB2: lea rax, [rbp + 0xfa0]
0x00000CB9: mov r8d, 4
0x00000CBF: mov rcx, rax
0x00000CC2: call 0x2240
0x00000CC7: test eax, eax
0x00000CC9: je 0xd66
0x00000CCF: lea rdx, [rip + 0x2a0f]
0x00000CD6: lea rax, [rbp + 0xfa0]
0x00000CDD: mov rcx, rax
0x00000CE0: mov rax, qword ptr [rip + 0x6d91]
0x00000CE7: call rax
0x00000CE9: mov qword ptr [rbp + 0x1350], rax
0x00000CF0: cmp qword ptr [rbp + 0x1350], 0
0x00000CF8: je 0xc30
0x00000CFE: jmp 0xd2e
0x00000D00: lea rax, [rbp - 0x60]
0x00000D04: mov rcx, rax
0x00000D07: call 0x2238
0x00000D0C: mov edx, eax
0x00000D0E: lea rax, [rbp - 0x60]
0x00000D12: mov rcx, qword ptr [rbp + 0x1360]
0x00000D19: mov r9d, 0
0x00000D1F: mov r8d, edx
0x00000D22: mov rdx, rax
0x00000D25: mov rax, qword ptr [rip + 0x6dcc]
0x00000D2C: call rax
0x00000D2E: mov rdx, qword ptr [rbp + 0x1350]
0x00000D35: lea rax, [rbp - 0x60]
0x00000D39: mov r8, rdx
0x00000D3C: mov edx, 0x1000
0x00000D41: mov rcx, rax
0x00000D44: call 0x2280
0x00000D49: test rax, rax
0x00000D4C: jne 0xd00
0x00000D4E: mov rax, qword ptr [rbp + 0x1350]
0x00000D55: mov rcx, rax
0x00000D58: mov rax, qword ptr [rip + 0x6d11]
0x00000D5F: call rax
0x00000D61: jmp 0xc30
0x00000D66: nop
0x00000D67: mov rax, qword ptr [rbp + 0x1360]
0x00000D6E: mov rcx, rax
0x00000D71: mov rax, qword ptr [rip + 0x6d58]
0x00000D78: call rax
0x00000D7A: mov rax, qword ptr [rip + 0x6d37]
0x00000D81: call rax
0x00000D83: mov eax, 0
```

```
0x00000D88: add rsp, 0x13f0
0x00000D8F: pop rbp
0x00000D90: ret
0x00000D91: push rbp
0x00000D92: mov rbp, rsp
0x00000D95: sub rsp, 0x20
0x00000D99: lea rax, [rip + 0x2948]
0x00000DA0: mov rcx, rax
0x00000DA3: call 0x2288
0x00000DA8: mov ecx, 0x3e8
0x00000DAD: mov rax, qword ptr [rip + 0x6b7c]
0x00000DB4: call rax
0x00000DB6: lea rax, [rip + 0x294e]
0x00000DBD: mov rcx, rax
0x00000DC0: call 0x2288
0x00000DC5: nop
0x00000DC6: add rsp, 0x20
0x00000DCA: pop rbp
0x00000DCB: ret
0x00000DCC: push rbp
0x00000DCD: mov rbp, rsp
0x00000DD0: sub rsp, 0x20
0x00000DD4: lea rax, [rip + 0x294d]
0x00000DDB: mov rcx, rax
0x00000DDE: call 0x2288
0x00000DE3: nop
0x00000DE4: add rsp, 0x20
0x00000DE8: pop rbp
0x00000DE9: ret
0x00000DEA: push rbp
0x00000DEB: mov rbp, rsp
0x00000DEE: sub rsp, 0x40
0x00000DF2: mov dword ptr [rbp + 0x10], ecx
0x00000DF5: mov qword ptr [rbp + 0x18], rdx
0x00000DF9: call 0x1020
0x00000DFE: mov dword ptr [rbp - 4], 0x115c
0x00000E05: lea rax, [rip + 0x295c]
0x00000E0C: mov rcx, rax
0x00000E0F: call 0x2288
0x00000E14: lea rax, [rip + 0x2975]
0x00000E1B: mov rcx, rax
0x00000E1E: call 0x2288
0x00000E23: lea rax, [rip + 0x298e]
0x00000E2A: mov rcx, rax
0x00000E2D: call 0x2288
0x00000E32: lea rax, [rip + 0x29a7]
0x00000E39: mov rcx, rax
0x00000E3C: call 0x2288
0x00000E41: lea rax, [rip + 0x29c0]
0x00000E48: mov rcx, rax
0x00000E4B: call 0x2288
0x00000E50: lea rax, [rip + 0x29f9]
0x00000E57: mov rcx, rax
0x00000E5A: call 0x2288
0x00000E5F: lea rax, [rbp - 0x20]
0x00000E63: movabs rdx, 0x2e302e302e373231
0x00000E6D: mov qword ptr [rax], rdx
```

```
0x00000E70: mov word ptr [rax + 8], 0x31
0x00000E76: lea rax, [rbp - 0x20]
0x00000E7A: mov r8d, 0
0x00000E80: mov edx, 9
0x00000E85: mov rcx, rax
0x00000E88: call 0xa40
0x00000E8D: cmp dword ptr [rbp + 0x10], 1
0x00000E91: jle 0xeaa
0x00000E93: mov rax, qword ptr [rbp + 0x18]
0x00000E97: add rax, 8
0x00000E9B: mov rdx, qword ptr [rax]
0x00000E9E: lea rax, [rbp - 0x20]
0x00000EA2: mov rcx, rax
0x00000EA5: call 0x2230
0x00000EAA: cmp dword ptr [rbp + 0x10], 2
0x00000EAE: jle 0xec6
0x00000EB0: mov rax, qword ptr [rbp + 0x18]
0x00000EB4: add rax, 0x10
0x00000EB8: mov rax, qword ptr [rax]
0x00000EBB: mov rcx, rax
0x00000EBE: call 0x2350
0x00000EC3: mov dword ptr [rbp - 4], eax
0x00000EC6: call 0xd91
0x00000ECB: lea rax, [rip + 0x29be]
0x00000ED2: mov rcx, rax
0x00000ED5: call 0x2288
0x00000EDA: mov edx, dword ptr [rbp - 4]
0x00000EDD: lea rax, [rbp - 0x20]
0x00000EE1: mov rcx, rax
0x00000EE4: call 0xa93
0x00000EE9: lea rax, [rip + 0x29cb]
0x00000EF0: mov rcx, rax
0x00000EF3: call 0x2288
0x00000EF8: mov eax, 0
0x00000EFD: add rsp, 0x40
0x00000F01: pop rbp
0x00000F02: ret
0x00000F03: nop
0x00000F04: nop
0x00000F05: nop
0x00000F06: nop
0x00000F07: nop
0x00000F08: nop
0x00000F09: nop
0x00000F0A: nop
0x00000F0B: nop
0x00000F0C: nop
0x00000F0D: nop
0x00000F0E: nop
0x00000F0F: nop
0x00000F10: jmp qword ptr [rip + 0x6bea]
0x00000F16: nop
0x00000F17: nop
0x00000F18: jmp qword ptr [rip + 0x6bda]
0x00000F1E: nop
0x00000F1F: nop
0x00000F20: jmp qword ptr [rip + 0x6bca]
```

```
0x00000F26: nop
0x00000F27: nop
0x00000F28: jmp qword ptr [rip + 0x6bba]
0x00000F2E: nop
0x00000F2F: nop
0x00000F30: jmp qword ptr [rip + 0x6baa]
0x00000F36: nop
0x00000F37: nop
0x00000F38: jmp qword ptr [rip + 0x6b9a]
0x00000F3E: nop
0x00000F3F: nop
0x00000F40: jmp qword ptr [rip + 0x6b8a]
0x00000F46: nop
0x00000F47: nop
0x00000F48: jmp qword ptr [rip + 0x6b7a]
0x00000F4E: nop
0x00000F4F: nop
0x00000F50: jmp qword ptr [rip + 0x6b6a]
0x00000F56: nop
0x00000F57: nop
0x00000F58: jmp qword ptr [rip + 0x6b5a]
0x00000F5E: nop
0x00000F5F: nop
0x00000F60: sub rsp, 0x28
0x00000F64: mov rax, qword ptr [rip + 0x1695]
0x00000F6B: mov rax, qword ptr [rax]
0x00000F6E: test rax, rax
0x00000F71: je 0xf95
0x00000F73: nop dword ptr [rax + rax]
0x00000F78: call rax
0x00000F7A: mov rax, qword ptr [rip + 0x167f]
0x00000F81: lea rdx, [rax + 8]
0x00000F85: mov rax, qword ptr [rax + 8]
0x00000F89: mov qword ptr [rip + 0x1670], rdx
0x00000F90: test rax, rax
0x00000F93: jne 0xf78
0x00000F95: add rsp, 0x28
0x00000F99: ret
0x00000F9A: nop word ptr [rax + rax]
0x00000FA0: push rsi
0x00000FA1: push rbx
0x00000FA2: sub rsp, 0x28
0x00000FA6: mov rdx, qword ptr [rip + 0x2ca3]
0x00000FAD: mov rax, qword ptr [rdx]
0x00000FB0: cmp eax, -1
0x00000FB3: mov ecx, eax
0x00000FB5: je 0xff0
0x00000FB7: test ecx, ecx
0x00000FB9: je 0xfdb
0x00000FBB: mov eax, ecx
0x00000FBD: sub ecx, 1
0x00000FC0: lea rbx, [rdx + rax*8]
0x00000FC4: sub rax, rcx
0x00000FC7: lea rsi, [rdx + rax*8 - 8]
0x00000FCC: nop dword ptr [rax]
0x00000FD0: call qword ptr [rbx]
0x00000FD2: sub rbx, 8
```

```
0x00000FD6: cmp rbx, rsi
0x00000FD9: jne 0xfd0
0x00000FDB: lea rcx, [rip - 0x82]

0x00000FE2: add rsp, 0x28
0x00000FE6: pop rbx
0x00000FE7: pop rsi
0x00000FE8: jmp 0xa10
0x00000FED: nop dword ptr [rax]
0x00000FF0: xor eax, eax
0x00000FF2: nop word ptr cs:[rax + rax]
0x00000FFD: nop dword ptr [rax]
0x00001000: lea r8d, [rax + 1]
0x00001004: mov ecx, eax
0x00001006: cmp qword ptr [rdx + r8*8], 0
0x0000100B: mov rax, r8
0x0000100E: jne 0x1000
0x00001010: jmp 0xfb7
0x00001012: nop word ptr cs:[rax + rax]
0x0000101D: nop dword ptr [rax]
0x00001020: mov eax, dword ptr [rip + 0x560a]
0x00001026: test eax, eax
0x00001028: je 0x1030
0x0000102A: ret
0x0000102B: nop dword ptr [rax + rax]
0x00001030: mov dword ptr [rip + 0x55f6], 1
0x0000103A: jmp 0xfa0
0x0000103F: nop
0x00001040: xor eax, eax
0x00001042: ret
0x00001043: nop
0x00001044: nop
0x00001045: nop
0x00001046: nop
0x00001047: nop
0x00001048: nop
0x00001049: nop
0x0000104A: nop
0x0000104B: nop
0x0000104C: nop
0x0000104D: nop
0x0000104E: nop
0x0000104F: nop
0x00001050: cmp edx, 3
0x00001053: je 0x1060
0x00001055: test edx, edx
0x00001057: je 0x1060
0x00001059: ret
0x0000105A: nop word ptr [rax + rax]
0x00001060: jmp 0x1b10
0x00001065: nop word ptr cs:[rax + rax]
0x00001070: push rsi
0x00001071: push rbx
0x00001072: sub rsp, 0x28

0x00001076: mov rax, qword ptr [rip + 0x2bb3]
0x0000107D: cmp dword ptr [rax], 2
0x00001080: je 0x1088
0x00001082: mov dword ptr [rax], 2
```

```
0x00001088: cmp edx, 2
0x0000108B: je 0x10a0
0x0000108D: cmp edx, 1
0x00001090: je 0x10d8
0x00001092: add rsp, 0x28
0x00001096: pop rbx
0x00001097: pop rsi
0x00001098: ret
0x00001099: nop dword ptr [rax]
0x000010A0: lea rbx, [rip + 0x2e09]
0x000010A7: lea rsi, [rip + 0x2e02]
0x000010AE: cmp rbx, rsi
0x000010B1: je 0x1092
0x000010B3: nop dword ptr [rax + rax]
0x000010B8: mov rax, qword ptr [rbx]
0x000010BB: test rax, rax
0x000010BE: je 0x10c2
0x000010C0: call rax
0x000010C2: add rbx, 8
0x000010C6: cmp rbx, rsi
0x000010C9: jne 0x10b8
0x000010CB: add rsp, 0x28
0x000010CF: pop rbx
0x000010D0: pop rsi
0x000010D1: ret
0x000010D2: nop word ptr [rax + rax]
0x000010D8: add rsp, 0x28
0x000010DC: pop rbx
0x000010DD: pop rsi
0x000010DE: jmp 0x1b10
0x000010E3: nop word ptr cs:[rax + rax]
0x000010EE: nop
0x000010F0: xor eax, eax
0x000010F2: ret
0x000010F3: nop
0x000010F4: nop
0x000010F5: nop
0x000010F6: nop
0x000010F7: nop
0x000010F8: nop
0x000010F9: nop
0x000010FA: nop
0x000010FB: nop
0x000010FC: nop
0x000010FD: nop
0x000010FE: nop
```

14. INDICATORS OF COMPROMISE (IOCs)

The following indicators can be used for threat hunting and detection rule creation:

File Hashes:

Type	Value
MD5	a14bee091e1ac71b7e8c1cd505488142
SHA-1	af5b966cd98fe4c9a6519c665f394598b5179318
SHA-256	8a304256092f0cbfb24b4204ce785ed9f42ee0c240f4d5edb96c45eaef4c3882

Matched YARA Rules:

- Shellcode_Patterns
- Backdoor_Generic
- Suspicious_Strings
- PUP_System_Optimizer
- RevengeRAT
- BlueTool_Seatbelt
- Serverless_Function_Backdoor
- ExploitKit_Terror
- Generic_C2_Communication
- Insider_Sabotage_Tool
- Linux_SSH_Backdoor
- SocGholish_FakeUpdate
- Network_Activity
- Memory_Stack_Pivot
- Memory_EggHunter
- Obfuscation_String_Encryption
- Obfuscation_API_Hashing
- Obfuscation_XOR_Single_Byte
- Obfuscation_XOR_Rolling
- Obfuscation_Indirect_Call

APPENDIX A: ANALYSIS METADATA

Analysis Configuration:

Parameter	Value
Report Generated	2026-01-18 10:20:26 UTC
Report ID	20260118-102026
Analyzer Version	1.0.0
YARA Rules Loaded	True
ML Model	N/A
VirusTotal API	Not Available

Disclaimer:

This report is generated by automated analysis tools and should be used as part of a comprehensive security assessment. The classification and threat scores are based on heuristic analysis, signature matching, and machine learning models. False positives and false negatives may occur. Manual verification by qualified security analysts is recommended for critical decisions.

This document contains confidential information and is intended for authorized personnel only. Unauthorized distribution or use is prohibited.