

JOESandbox Cloud BASIC



ID: 516930

Sample Name:

dngqoAXyDd.exe

Cookbook: default.jbs

Time: 15:02:51

Date: 06/11/2021

Version: 34.0.0 Boulder Opal

Table of Contents

| | |
|--|----|
| Table of Contents | 2 |
| Windows Analysis Report dngqoAXyDd.exe | 3 |
| Overview | 3 |
| General Information | 3 |
| Detection | 3 |
| Signatures | 3 |
| Classification | 3 |
| Process Tree | 3 |
| Malware Configuration | 3 |
| Threatname: Trickbot | 3 |
| Yara Overview | 4 |
| Memory Dumps | 4 |
| Sigma Overview | 4 |
| Jbx Signature Overview | 4 |
| AV Detection: | 4 |
| Malware Analysis System Evasion: | 4 |
| Anti Debugging: | 4 |
| HIPS / PFW / Operating System Protection Evasion: | 4 |
| Stealing of Sensitive Information: | 4 |
| Remote Access Functionality: | 4 |
| Mitre Att&ck Matrix | 4 |
| Behavior Graph | 5 |
| Screenshots | 5 |
| Thumbnails | 5 |
| Antivirus, Machine Learning and Genetic Malware Detection | 6 |
| Initial Sample | 6 |
| Dropped Files | 6 |
| Unpacked PE Files | 6 |
| Domains | 6 |
| URLs | 7 |
| Domains and IPs | 7 |
| Contacted Domains | 7 |
| Contacted IPs | 7 |
| General Information | 7 |
| Simulations | 7 |
| Behavior and APIs | 7 |
| Joe Sandbox View / Context | 8 |
| IPs | 8 |
| Domains | 8 |
| ASN | 8 |
| JA3 Fingerprints | 8 |
| Dropped Files | 8 |
| Created / dropped Files | 8 |
| Static File Info | 8 |
| General | 8 |
| File Icon | 8 |
| Static PE Info | 9 |
| General | 9 |
| Entrypoint Preview | 9 |
| Rich Headers | 9 |
| Data Directories | 9 |
| Sections | 9 |
| Resources | 9 |
| Imports | 9 |
| Version Infos | 9 |
| Possible Origin | 9 |
| Network Behavior | 10 |
| Code Manipulations | 10 |
| Statistics | 10 |
| Behavior | 10 |
| System Behavior | 10 |
| Analysis Process: dngqoAXyDd.exe PID: 4872 Parent PID: 912 | 10 |
| General | 10 |
| Analysis Process: wermgr.exe PID: 5784 Parent PID: 4872 | 10 |
| General | 10 |
| Analysis Process: cmd.exe PID: 6396 Parent PID: 4872 | 11 |
| General | 11 |
| Disassembly | 11 |
| Code Analysis | 11 |

Windows Analysis Report dngqoAXyDd.exe

Overview

General Information

| | |
|------------------------------|---------------------|
| Sample Name: | dngqoAXyDd.exe |
| Analysis ID: | 516930 |
| MD5: | 0afbb383c5cea9f.. |
| SHA1: | 148266112b2508.. |
| SHA256: | 6a910ec8055b38.. |
| Tags: | exe top147 TrickBot |
| Infos: | |
| Most interesting Screenshot: | |

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

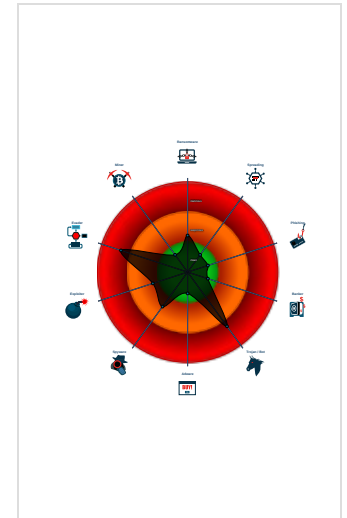
TrickBot

| | |
|--------------|---------|
| Score: | 80 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

Signatures

- Found malware configuration
- Yara detected Trickbot
- Multi AV Scanner detection for subm...
- Writes to foreign memory regions
- Tries to detect virtualization through...
- Found potential dummy code loops (...)
- Found evasive API chain (trying to d...
- Creates a DirectInput object (often fo...
- Uses 32bit PE files
- Found inlined nop instructions (likely...
- Queries the volume information (nam...
- Sample file is different than original ...

Classification



Process Tree

- System is w10x64
- dngqoAXyDd.exe (PID: 4872 cmdline: "C:\Users\user\Desktop\dngqoAXyDd.exe" MD5: 0AFBB383C5CEA9F11202D572141BB0F4)
 - wermgr.exe (PID: 5784 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
 - cmd.exe (PID: 6396 cmdline: C:\Windows\system32\cmd.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- cleanup

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "100019",
  "gtag": "top147",
  "servs": [
    "65.152.201.203:443",
    "185.56.175.122:443",
    "46.99.175.217:443",
    "179.189.229.254:443",
    "46.99.175.149:443",
    "181.129.167.82:443",
    "216.166.148.187:443",
    "46.99.188.223:443",
    "128.201.76.252:443",
    "62.99.79.77:443",
    "60.51.47.65:443",
    "24.162.214.166:443",
    "45.36.99.184:443",
    "97.83.40.67:443",
    "184.74.99.214:443",
    "103.105.254.17:443",
    "62.99.76.213:443",
    "82.159.149.52:443"
  ],
  "autorun": [
    "pwgrabb",
    "pwgrabc"
  ],
  "ecc_key": "RUNTMzAAAAbfmkJRvwyw7iFKx40hL2HwsUe0SZZZ0FRRWGkY6J1+gf3YKq13Ee4sY3Jb9/0myCr0MwzNK1K2L5yuY87nW290/yjMJG0ISDj0HNBC3G+ZGta60i9Qk;JCwnNGbw2hQ4="
}
```

Yara Overview


Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|------------------------|------------------------|--------------|---------|
| 00000000.00000002.374239555.0000000000B3 1000.00000040.00000001.sdmp | JoeSecurity_TrickBot_4 | Yara detected Trickbot | Joe Security | |

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 [Click to jump to signature section](#)

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Malware Analysis System Evasion:



Tries to detect virtualization through RDTS time measurements

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Anti Debugging:



Found potential dummy code loops (likely to delay analysis)

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Stealing of Sensitive Information:



Yara detected Trickbot

Remote Access Functionality:



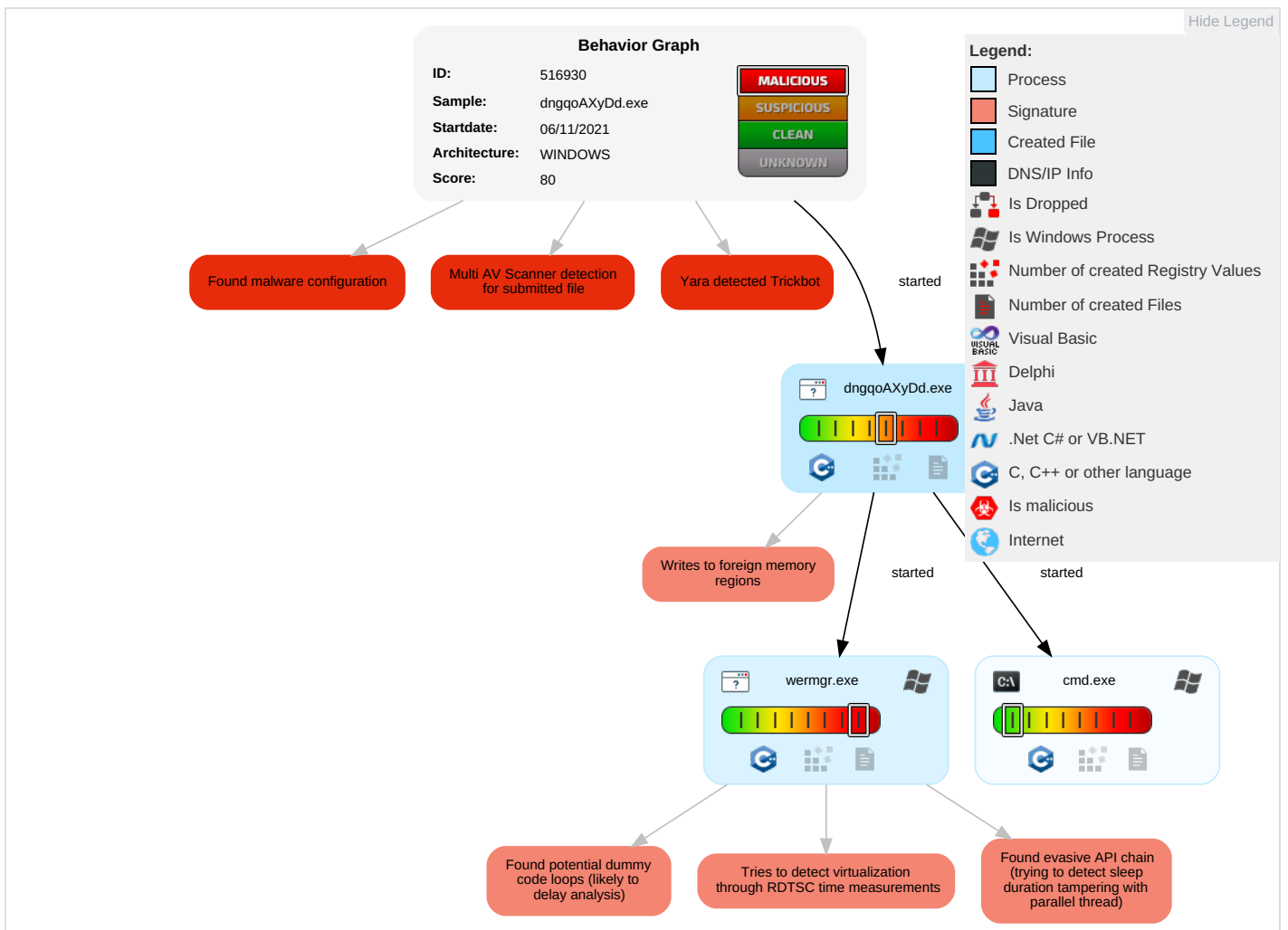
Yara detected Trickbot

Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|----------------|-----------|-------------|----------------------|-----------------|-------------------|-----------|------------------|------------|--------------|---------------------|-----------------|
|----------------|-----------|-------------|----------------------|-----------------|-------------------|-----------|------------------|------------|--------------|---------------------|-----------------|

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|-------------------------------------|--------------------|--------------------------------------|-----------------------------|---|---------------------------|--|------------------------------------|--------------------------------|--|-------------------------|--|
| Valid Accounts | Native API 1 1 | Path Interception | Access Token Manipulation 1 | Disable or Modify Tools 1 | Input Capture 1 | System Time Discovery 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communicator |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Process Injection 1 1 2 | Virtualization/Sandbox Evasion 1 1 1 | LSASS Memory | Security Software Discovery 2 2 1 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Access Token Manipulation 1 | Security Account Manager | Virtualization/Sandbox Evasion 1 1 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 1 2 | NTDS | Process Discovery 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Deobfuscate/Decode Files or Information 1 | LSA Secrets | System Network Configuration Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicator |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 3 | Cached Domain Credentials | System Information Discovery 1 2 3 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |

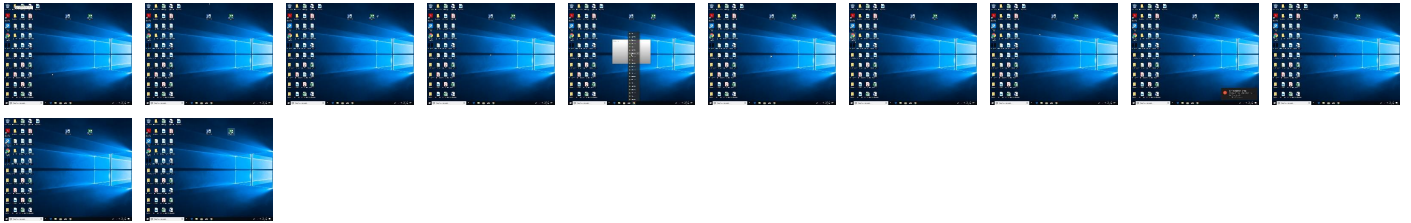
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

| Source | Detection | Scanner | Label | Link |
|----------------|-----------|---------------|-----------------------|------|
| dngqoAXyDd.exe | 29% | ReversingLabs | Win32.Trojan.Trickpak | |

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

| | |
|--|--|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 516930 |
| Start date: | 06.11.2021 |
| Start time: | 15:02:51 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 52s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | dngqoAXyDd.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 21 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | <ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal80.troj.evad.winEXE@5/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | <ul style="list-style-type: none">• Successful, ratio: 18.1% (good quality ratio 16.9%)• Quality average: 83.1%• Quality standard deviation: 28.2% |
| HCA Information: | <ul style="list-style-type: none">• Successful, ratio: 67%• Number of executed functions: 0• Number of non-executed functions: 0 |
| Cookbook Comments: | <ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe |
| Warnings: | Show All |

Simulations

Behavior and APIs

| Time | Type | Description |
|----------|-----------------|--|
| 15:04:04 | API Interceptor | 1x Sleep call for process: dngqoAXyDd.exe modified |
| 15:04:04 | API Interceptor | 1x Sleep call for process: wermgr.exe modified |

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

| General | |
|-----------------------|--|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 6.167416806599989 |
| TrID: | <ul style="list-style-type: none"> Win32 Executable (generic) a (10002005/4) 99.96% Generic Win/DOS Executable (2004/3) 0.02% DOS Executable Generic (2002/1) 0.02% Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | dngqoAXyDd.exe |
| File size: | 652800 |
| MD5: | 0afbb383c5cea9f11202d572141bb0f4 |
| SHA1: | 148266112b25087f10ac1124ea32630e48fb0bd9 |
| SHA256: | 6a910ec8055b3844e3dd14c7af08a68110abc9395a88ab9199e69ed07be27210 |
| SHA512: | 702447b6e1313224d4c8084f716d8d838090c7bd9fb355fc6ab4553ce3676bb5fe1c2ebde61e4ed8b7bb6d3d7f1dfd11c434e5e0f9b7baa2511a12fd1c501880 |
| SSDEEP: | 12288:AjX3XdmePk2BSPkno2voTFa24aZZTUQxlpTLYOE5pM:2HXgASPMNvoTFfJT8tLYNH |
| File Content Preview: | MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$......1...u...u. ..u.....b.....&..... ...r...u...#.....'.G.....t..u...t.....t..Richu..PE.L....(a..... |

File Icon



Icon Hash:

0000000000000000

Static PE Info

General

| | |
|-----------------------------|--|
| Entrypoint: | 0x40cfee |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x618528F1 [Fri Nov 5 12:52:01 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 1 |
| File Version Major: | 5 |
| File Version Minor: | 1 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 1 |
| Import Hash: | 2a49715e49b2891839bf716e121ca434 |

Entrypoint Preview

Rich Headers

Data Directories

Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|--------|-----------------|--------------|----------|----------|-----------------|-----------|---------------|---|
| .text | 0x1000 | 0x382bb | 0x38400 | False | 0.395729166667 | data | 5.67953550398 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x3a000 | 0x8082 | 0x8200 | False | 0.237379807692 | data | 3.46352247423 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x43000 | 0x4598 | 0x2000 | False | 0.2734375 | data | 3.48353069957 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .idata | 0x48000 | 0xc7b | 0xe00 | False | 0.318080357143 | data | 4.19163051635 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x49000 | 0x59689 | 0x59800 | False | 0.644514883031 | data | 6.09524824059 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xa3000 | 0x25c6 | 0x2600 | False | 0.625616776316 | data | 5.79339854832 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

Resources

Imports

Version Infos

Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|--------------------------------|----------------------------------|-----|
| English | United States | |


Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: dngqoAXyDd.exe PID: 4872 Parent PID: 912

General

| | |
|-------------------------------|---|
| Start time: | 15:03:52 |
| Start date: | 06/11/2021 |
| Path: | C:\Users\user\Desktop\dngqoAXyDd.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\dngqoAXyDd.exe" |
| Imagebase: | 0x180000 |
| File size: | 652800 bytes |
| MD5 hash: | 0AFBB383C5CEA9F11202D572141BB0F4 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | <ul style="list-style-type: none">Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000000.00000002.374239555.000000000B31000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

Analysis Process: wermgr.exe PID: 5784 Parent PID: 4872

General

| | |
|-------------------------------|----------------------------------|
| Start time: | 15:03:58 |
| Start date: | 06/11/2021 |
| Path: | C:\Windows\System32\wermgr.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\wermgr.exe |
| Imagebase: | 0x7ff7ae910000 |
| File size: | 209312 bytes |
| MD5 hash: | FF214585BF10206E21EA8EBA202FACFD |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

General

| | |
|-------------------------------|----------------------------------|
| Start time: | 15:04:00 |
| Start date: | 06/11/2021 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\cmd.exe |
| Imagebase: | 0x7ff7180e0000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

Disassembly

Code Analysis