ID: 830303
Sample Name: rocroc.exe
Cookbook: default.jbs
Time: 08:46:27
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

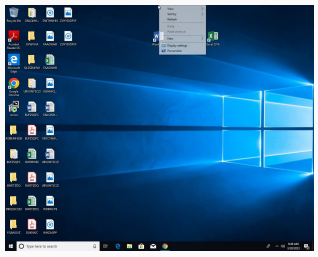
Windows Analysis Report

rocroc.exe

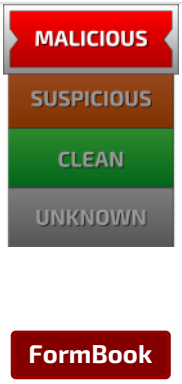
Overview

General Information

Sample Name:	rocroc.exe
Analysis ID:	830303
MD5:	b7e5425d0dae…
SHA1:	505084085e1a…
SHA256:	06fbb80f37ae3…
Tags:	exe Formbook
Infos:	



Detection

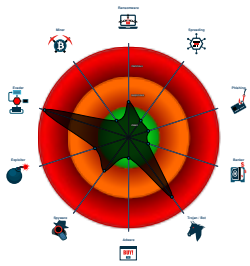


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- rocroc.exe (PID: 6124 cmdline: C:\Users\user\Desktop\rocroc.exe MD5: B7E5425D0DAEA66FC85E360A0B0D760D)
  - nmtargerx.exe (PID: 5260 cmdline: "C:\Users\user\AppData\Local\Temp\nmtargerx.exe" C:\Users\user\AppData\Local\Temp\rimgurbkmm.edy MD5: 5DDE2B26DE7E8B448EDCED428AF8E385)
    - nmtargerx.exe (PID: 3140 cmdline: C:\Users\user\AppData\Local\Temp\nmtargerx.exe MD5: 5DDE2B26DE7E8B448EDCED428AF8E385)
      - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cscript.exe (PID: 1788 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
          - cmd.exe (PID: 4648 cmdline: /c del "C:\Users\user\AppData\Local\Temp\nmtargerx.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 2604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	**http://** blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

Threatname: FormBook


```
{
  "C2 list": [
    "www.senriki.net/re29/"
  ],
  "decoy": [
    "barnstorm-music.com",
    "gazzettadellapuglia.com",
    "baratieistore.space",
    "cdrjdkj.com",
    "carlissablog.com",
    "langlalang.com",
    "2886365.com",
    "aq993.cyou",
    "jwjwjwjw.com",
    "car-deals-80304.com",
    "dikevolesas.info",
    "buycialistablets.online",
    "theplantgranny.net",
    "detoxshopbr.store",
    "imans.biz",
    "fightingcock.co.uk",
    "loveforfurbabies.com",
    "eastcoastbeveragegroup.com",
    "alaaeldinsoft.com",
    "microshel.com",
    "deal-markt.com",
    "hypothetical.systems",
    "baxhakutrade.com",
    "chiehhsikaoportfolio.com",
    "brandsmania.net",
    "follred.com",
    "6566x14.app",
    "defi88.com",
    "h-skyseo.com",
    "imagina-onshop.com",
    "bambooleavescompany.com",
    "cmojohnny.com",
    "1whxgd.top",
    "infernaljournal.app",
    "kk156.net",
    "chokolatk.com",
    "guoshan-0800777216.com",
    "funparty.rsvp",
    "helenfallon.com",
    "digitalmagazine.online",
    "idealcutandtrim.com",
    "bricoitalia.net",
    "ecwid-store-copy.net",
    "iljamusic.com",
    "uvcon.africa",
    "hoodiesupplycol.com",
    "iilykt.top",
    "continuousvoltage.com",
    "josephajaogo.africa",
    "baba-robot.ru",
    "1wsfcg.top",
    "hagfiw.xyz",
    "firstcitizncb.com",
    "calamitouscrochet.shop",
    "829727.com",
    "eleonorasdaycare.com",
    "lafourmiprovencal.ch",
    "corollacompany.africa",
    "acorsgroup.com",
    "jabberglotty.com",
    "akhlit.com",
    "kompetenceboersen.online",
    "fxtcb8.site",
    "whetegeneralprojects.africa"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9bf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C

Click to see the 33 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.nmtargerx.exe.1330000.1.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
1.2.nmtargerx.exe.1330000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.nmtargerx.exe.1330000.1.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bbf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14aa7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
1.2.nmtargerx.exe.1330000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.nmtargerx.exe.1330000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C

Click to see the 15 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 192.185.52.247	
Timestamp:	192.168.2.6192.185.52.24749707802031412 03/20/23-08:48:38.899953
SID:	2031412
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 192.185.52.247	
Timestamp:	192.168.2.6192.185.52.24749707802031453 03/20/23-08:48:38.899953
SID:	2031453
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 192.185.52.247	
Timestamp:	192.168.2.6192.185.52.24749707802031449 03/20/23-08:48:38.899953
SID:	2031449
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

Yara detected FormBook

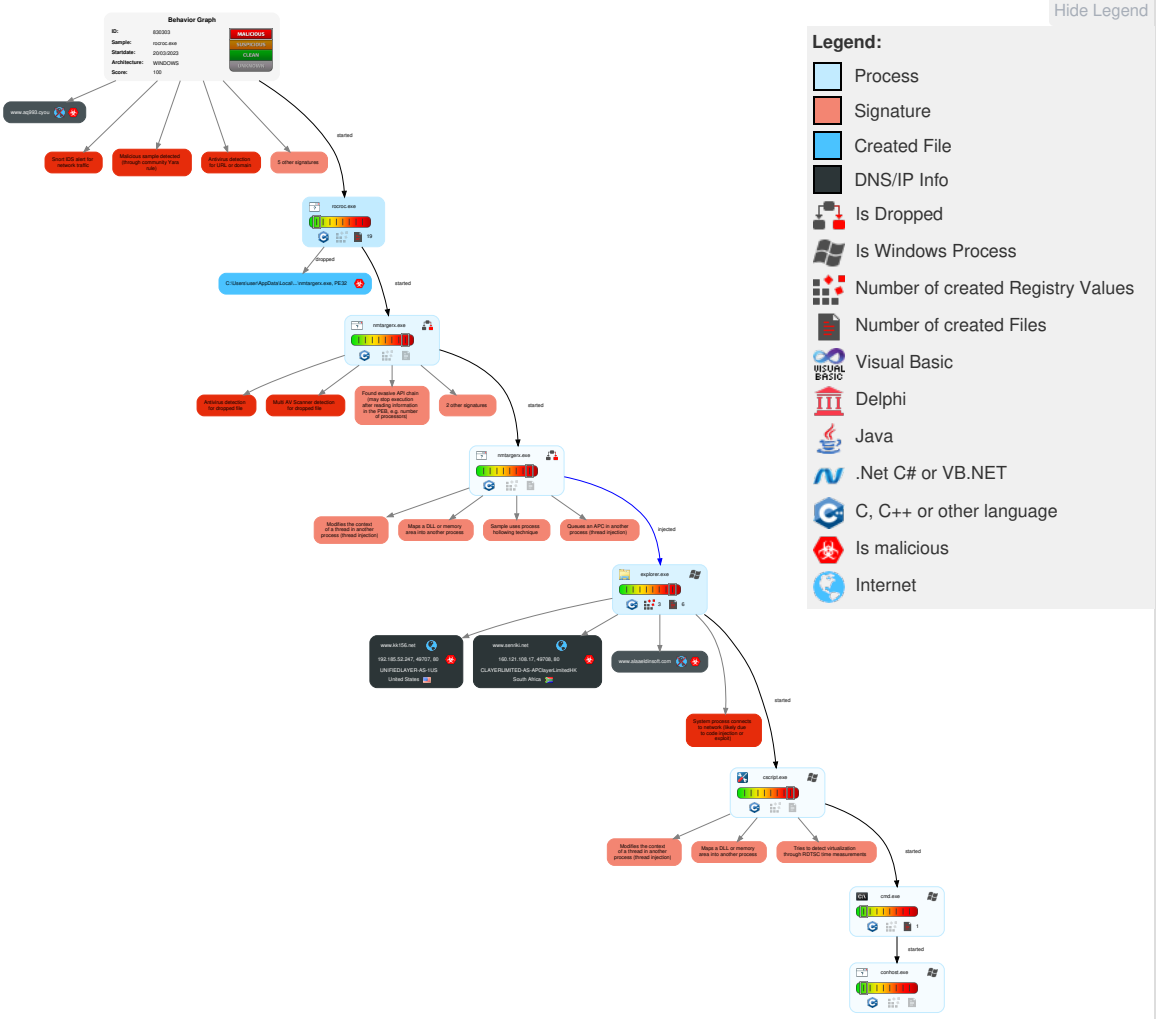
Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	5 1 2 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph

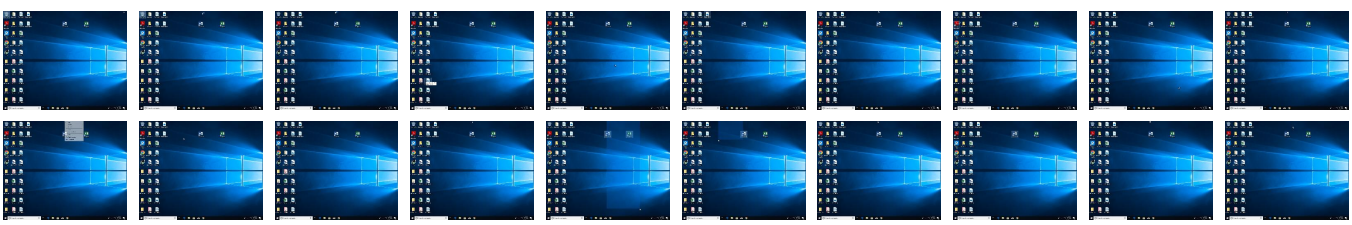
Hide Legend



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
rocroc.exe	74%	ReversingLabs	Win32.Trojan.Leonem	
rocroc.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nmtargerx.exe	100%	Avira	HEUR/AGEN.1242497	
C:\Users\user\AppData\Local\Temp\nmtargerx.exe	31%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
1.2.nmtargerx.exe.1330000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.nmtargerx.exe.b0000.0.unpack	100%	Avira	HEUR/AGEN.1242497		Download File
2.2.nmtargerx.exe.b0000.0.unpack	100%	Avira	HEUR/AGEN.1242497		Download File
2.2.nmtargerx.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nmtargerx.exe.b0000.0.unpack	100%	Avira	HEUR/AGEN.1242497		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.senriki.net	0%	Avira URL Cloud	safe	
http://www.barnstorm-music.com/re29/www.1whxgd.top	100%	Avira URL Cloud	malware	
http://www.langlalang.com	0%	Avira URL Cloud	safe	
http://www.aq993.cyou/re29/www.barnstorm-music.com	0%	Avira URL Cloud	safe	
http://www.fxtcb8.site	0%	Avira URL Cloud	safe	
http://www.kk156.net/re29/	0%	Avira URL Cloud	safe	
http://www.dikevolesas.infoReferer:	0%	Avira URL Cloud	safe	
http://www.hagfiw.xyz/re29/www.langlalang.com	100%	Avira URL Cloud	malware	
http://www.detoxshopbr.store	0%	Avira URL Cloud	safe	
http://www.acorsgroup.com	100%	Avira URL Cloud	malware	
http://www.1whxgd.topReferer:	0%	Avira URL Cloud	safe	
http://www.corollacompany.africa	100%	Avira URL Cloud	malware	
http://www.senriki.net/re29/?0DK4Qn=yRhazfKsHirG6nKYYl6mAz5vTQUNqz4sZ9ZrGGOS+9vLvJ0EFUwbGotar2l3eQhiIGPXkjmVOg==&nPW=WdYdbB1p3b2H7x	100%	Avira URL Cloud	malware	
http://www.jabberglotty.com/re29/www.acorsgroup.com	0%	Avira URL Cloud	safe	
http://www.hagfiw.xyz	100%	Avira URL Cloud	malware	
http://www.barnstorm-music.com	100%	Avira URL Cloud	malware	
http://www.barnstorm-music.com/re29/	100%	Avira URL Cloud	malware	
http://www.acorsgroup.com/re29/	100%	Avira URL Cloud	malware	
http://www.detoxshopbr.store/re29/	100%	Avira URL Cloud	malware	
http://www.hagfiw.xyz/re29/	100%	Avira URL Cloud	malware	
http://www.defi88.com	0%	Avira URL Cloud	safe	
http://www.dikevolesas.info/re29/www.follred.com	0%	Avira URL Cloud	safe	
http://www.defi88.com/re29/www.corollacompany.africa	0%	Avira URL Cloud	safe	
http://www.aq993.cyou	0%	Avira URL Cloud	safe	
http://www.follred.com/re29/R	0%	Avira URL Cloud	safe	
http://www.follred.comReferer:	0%	Avira URL Cloud	safe	
http://www.alaaeldinsoft.com/re29/www.aq993.cyou	0%	Avira URL Cloud	safe	
http://www.detoxshopbr.store/re29/www.jabberglotty.com	100%	Avira URL Cloud	malware	
http://www.kk156.netReferer:	0%	Avira URL Cloud	safe	
http://www.alaaeldinsoft.com	0%	Avira URL Cloud	safe	
http://www.langlalang.com/re29/www.defi88.com	0%	Avira URL Cloud	safe	
http://www.1whxgd.top/re29/	100%	Avira URL Cloud	malware	
http://www.kk156.net/re29/www.senriki.net	0%	Avira URL Cloud	safe	
http://www.aq993.cyou/re29/	0%	Avira URL Cloud	safe	
http://www.senriki.net/re29/www.alaaeldinsoft.com	100%	Avira URL Cloud	malware	
http://www.1whxgd.top/re29/www.hagfiw.xyz	100%	Avira URL Cloud	malware	
http://www.senriki.netReferer:	0%	Avira URL Cloud	safe	
http://www.langlalang.com/re29/	0%	Avira URL Cloud	safe	
http://www.hagfiw.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.detoxshopbr.storeReferer:	0%	Avira URL Cloud	safe	
http://www.kk156.net	0%	Avira URL Cloud	safe	
http://www.langlalang.comReferer:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fxtcb8.site/re29/www.dikevolesas.info	0%	Avira URL Cloud	safe	
http://https://www.zoty1116.com:30120/register/?i_code=4627044	0%	Avira URL Cloud	safe	
http://www.fxtcb8.site/re29/	0%	Avira URL Cloud	safe	
http://www.fxtcb8.siteReferer:	0%	Avira URL Cloud	safe	
http://www.corollacompany.africa/re29/www.detoxshopbr.store	100%	Avira URL Cloud	malware	
http://www.corollacompany.africa/re29/	100%	Avira URL Cloud	malware	
http://www.alaaeldinsoft.com/re29/	0%	Avira URL Cloud	safe	
http://https://47.116.3.86:29920/kok/logo.png	0%	Avira URL Cloud	safe	
http://www.1whxgd.top	0%	Avira URL Cloud	safe	
http://www.barnstorm-music.comReferer:	0%	Avira URL Cloud	safe	
http://www.defi88.com/re29/	0%	Avira URL Cloud	safe	
http://www.jabberglotty.com/re29/	0%	Avira URL Cloud	safe	
http://www.kk156.net/re29/?0DK4Qn=GULsnGSHMoQzF5BSBaA7IgErJIrC6IG18OGrAG0wV2/PJUf48ccOVKgRcy3msHjKmovQQ592kQ==&nPW=WdYdbB1p3b2H7x	0%	Avira URL Cloud	safe	
http://www.jabberglotty.comReferer:	0%	Avira URL Cloud	safe	
http://www.corollacompany.africaReferer:	0%	Avira URL Cloud	safe	
http://www.follred.com/re29/	0%	Avira URL Cloud	safe	
http://www.acorsgroup.com/re29/www.fxtcb8.site	100%	Avira URL Cloud	malware	
http://www.dikevolesas.info/re29/	0%	Avira URL Cloud	safe	
http://www.dikevolesas.info	0%	Avira URL Cloud	safe	
http://www.follred.com	0%	Avira URL Cloud	safe	
http://www.aq993.cyouReferer:	0%	Avira URL Cloud	safe	
www.senriki.net/re29/	100%	Avira URL Cloud	malware	
http://www.defi88.comReferer:	0%	Avira URL Cloud	safe	
http://www.jabberglotty.com	0%	Avira URL Cloud	safe	
http://www.alaaeldinsoft.comReferer:	0%	Avira URL Cloud	safe	
http://www.senriki.net/re29/	100%	Avira URL Cloud	malware	
http://www.acorsgroup.comReferer:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.senriki.net	160.121.108.17	true	true		unknown
www.kk156.net	192.185.52.247	true	true		unknown
www.aq993.cyou	unknown	unknown	true		unknown
www.alaaeldinsoft.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.senriki.net/re29/?0DK4Qn=yRhazfKsHirG6nKYYI6mAz5vTQUNqz4sZ9ZrGGOS+9vLvJ0EFUwbGotar2l3eQhiIGPXkjmVOg==&nPW=WdYdbB1p3b2H7x	true	• Avira URL Cloud: malware	unknown
http://www.kk156.net/re29/?0DK4Qn=GULsnGSHMoQzF5BSBaA7IgErJIrC6IG18OGrAG0wV2/PJUf48ccOVKgRcy3msHjKmovQQ592kQ==&nPW=WdYdbB1p3b2H7x	true	• Avira URL Cloud: safe	unknown
www.senriki.net/re29/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.barnstorm-music.com/re29/www.1whxgd.top	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.barnstorm-music.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.barnstorm-music.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.acorsgroup.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.senriki.net	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.langlalang.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fxtcb8.site	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aq993.cyou/re29/www.barnstorm-music.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hagfiw.xyz/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.kk156.net/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hagfiw.xyz	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hagfiw.xyz/re29/www.langlalang.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.acorsgroup.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.dikevolesas.infoReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.detoxshopbr.store	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.1whxgd.topReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.corollacompany.africa	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.detoxshopbr.store/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.jabberglotty.com/re29/www.acorsgroup.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.defi88.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dikevolesas.info/re29/www.follred.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.alaaeldinsoft.com/re29/www.aq993.cyou	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.follred.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.detoxshopbr.store/re29/www.jabberglotty.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.alaaeldinsoft.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.follred.com/re29/R	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.langlalang.com/re29/www.defi88.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aq993.cyou	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kk156.netReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.defi88.com/re29/www.corollacompany.africa	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kk156.net/re29/www.senriki.net	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

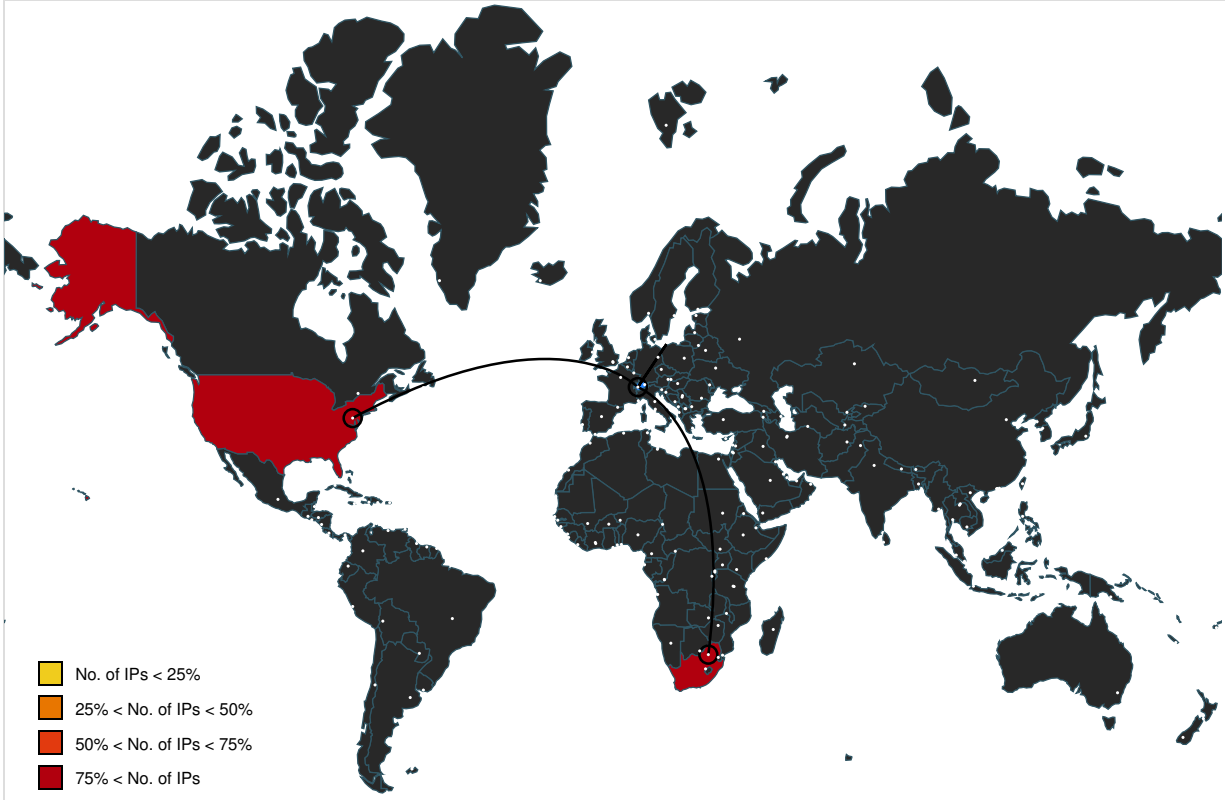
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.1whxgd.top/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.aq993.cyou/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.1whxgd.top/re29/www.hagfiw.xyz	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.27016983 2.0000000008442000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.262086599.0000000000AC8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000003.00000002.511875749.000000 0000AC8000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.462968225.0000000008442000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000002.520408845.00000000084420 00.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.hagfiw.xyzReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.senriki.net/re29/www.alaaeldinsoft.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.detoxshopbr.storeReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.senriki.netReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.langlalang.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kk156.net	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.langlalang.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.zoty1116.com:30120/register/?i_code=4627044	explorer.exe, 00000003.00000002.52515007 8.0000000013A0F000.00000004.80000000.000 40000.00000000.sdmp, cscript.exe, 000000 08.00000002.513850777.00000000052EF000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fxtcb8.site/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fxtcb8.site/re29/www.dikevolesas.info	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.corollacompany.africa/re29/www.detoxshopbr.store	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.fxtcb8.siteReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.alaaeldinsoft.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://47.116.3.86:29920/kok/logo.png	explorer.exe, 00000003.00000002.52515007 8.0000000013A0F000.00000004.80000000.000 40000.00000000.sdmp, cscript.exe, 000000 08.00000002.513850777.00000000052EF000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	rocroc.exe	false		high
http://www.corollacompany.africa/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.1whxgd.top	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.barnstorm-music.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.defi88.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jabberglotty.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.corollacompany.africaReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dikevolesas.info/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jabberglotty.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.follred.com/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acorsgroup.com/re29/www.fxtcb8.site	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.dikevolesas.info	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.follred.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aq993.cyouReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.alaaeldinsoft.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.defi88.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jabberglotty.com	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.senriki.net/re29/	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.acorsgroup.comReferer:	explorer.exe, 00000003.00000002.52446528 5.000000000F4B5000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.461212385.000000000F4B5000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.462613362.000000 000F4B5000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
160.121.108.17	www.senriki.net	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	true
192.185.52.247	www.kk156.net	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830303
Start date and time:	2023-03-20 08:46:27 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	rocroc.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/5@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.1% (good quality ratio 40.4%) • Quality average: 78.9% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: rocroc.exe

Simulations

Behavior and APIs

Time	Type	Description
08:47:43	API Interceptor	698x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat

Process:	C:\Windows\explorer.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.204081515204597
Encrypted:	false
SSDEEP:	24:Yq6CUXyhmQmnbNdB6hmxjmnz0JahmemnHZ6T06MhmDmnbxdB6hmktmn7KTdB6hm0:YqDUXyctnbNdUcAnz0JacPnHZ6T06McW
MD5:	160494591DCB3DD4E2C36F71207A87F3
SHA1:	D611935CA91C155B10A449DB72B3D5C8308A6EB7
SHA-256:	B82EC6928AAA7C30ABBE26DF13CA514DC4508C704F03EB28A4B2ABE40F60DF6E
SHA-512:	301BD7B6A4B7B2D3261C3A10FE98B2B4B811B861FCA077AF8732B7FCDFB2D106FFE82F0072CD859A4436E2EBD9347EACF44539E11AEAD2CA83703737B3030881
Malicious:	false
Preview:	{"RecentItems":[{"AppID":"Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim","PenUsageSec":15,"LastSwitchedLowPart":3648731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.WindowsMaps_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":3638731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint","PenUsageSec":15,"LastSwitchedLowPart":3628731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","PenUsageSec":15,"LastSwitchedLowPart":3618731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.Windows.Photos_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":3608731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.Getstarted_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":3598731648,"LastSwitchedHighPart":30747937,"PrePopulated":true}]}

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

Process:	C:\Users\user\Desktop\rocroc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	6.265679032611912
Encrypted:	false
SSDEEP:	768:JXJxBLApCDxvhqBrcbQdYPaPfhJAx1oZakLSO0OYCiPBjgFSd+ChG5Xev3P:JXBdxsBwfaPJJtZFLkPay+V5Xe/
MD5:	5DDE2B26DE7E8B448EDCED428AF8E385
SHA1:	AC9033CA6155232ED5250DA70B7622D797A41C36
SHA-256:	2423D7CB2BE18902BCDB5C9C5AE88B32F9F4D97C920A429AAF4AE1FF70D70B01
SHA-512:	DBBA75DDA90E4A47948F27D41EC6D55B3B7270134DAC211A3DBBF55F680BBE0F43D36F7703C1761456FD406ED8C30F3FD43D0C4F63EF1EFD47B35C79D8FDB79
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......??..{^..{^..{^....j.z^..e.x.[^..e.i.k^..e....^..\...n^..{^...^..e.u.z^..e.n.z^..e.m.z^..Rich{^..........................PE..L...Y..d....................d...................@..........................0...........@............................#...\|.............................. ....text............................. ..`.rdata...$.......&.................@..@.data...,.........................@....reloc....... ....@..B..

C:\Users\user\AppData\Local\Temp\nsoFB77.tmp

Process:	C:\Users\user\Desktop\rocroc.exe
File Type:	data
Category:	dropped
Size (bytes):	290468
Entropy (8bit):	7.686066118581011
Encrypted:	false
SSDEEP:	6144:N4ctNUinAsuMC58arHZJS68nS9beVPRHPSsd+6NVrNbnj1rf7UH3:bFWSmHZJSPS9bQpHP5dTxtrYH
MD5:	B7088F21084BA05718C30F38A65C1962
SHA1:	88AF4651DF9CB248B7287A44EDE4D4590BD1B850
SHA-256:	51095185AD751296C86254BE081B3AB5CE9AA450A4C89C5BF08325DC7C79C1DD
SHA-512:	5EE7619D6D733A957D5AD2183BA98502482B9E76CA468490346F4DE1CD0CED789C09D4CB09E7D43728B97503C590462F753662E491FB41FA0E310FEF47FF588
Malicious:	false
Preview:	R3......,........................!......p2......:3..0..G...................j...i...........Q..

C:\Users\user\AppData\Local\Temp\rimgurbkmm.edy

Process:	C:\Users\user\Desktop\rocroc.exe
File Type:	data
Category:	dropped
Size (bytes):	5585
Entropy (8bit):	7.178232710885884
Encrypted:	false
SSDEEP:	96:Farc6oYV7OWg/DrYuTk2XO5oSwYRH1VaNvI5dMS8+FCV76RdoT1uHDfRnTomtC8h:FarcRQyJLhX1S9jgNIMSZMVWQ8JDtC8h
MD5:	1D60216105868CAAA0F06B608139D885
SHA1:	610D96D5761A623D0F3F12E137320486DEE13AFE
SHA-256:	4B276576113FA41BD67EC015F38C8AC857B4ED637C2FAF1B86914B307EAF6AA2
SHA-512:	1E2A7CE5C46DBCE5CF1516AED8FF99653564F9E3D2991EC937BFA3AFC6753AE292DFC88D4096E4B0C19B071357453230237B410965824EFE2B0C673C96DDEF 5
Malicious:	false
Preview:	.005m..f.F<...05o.:......?v>.3.3.<......M.knl.02a..c.E<...42c. ......4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r.D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX.....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4......F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058.q..v..l.0A..q..34.q.p.}..u.{.w....}.p013......u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M......v.ZXK.J.E.....}.]..O.F.....u.X_.M.M......H...X...K.D.....}.\&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.;.q%..5M%.}.;.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0.m...D4...B358.q.0342.}.e......dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\scrzuow.py

Process:	C:\Users\user\Desktop\rocroc.exe
File Type:	data
Category:	dropped
Size (bytes):	210289
Entropy (8bit):	**7.991537261695156**
Encrypted:	**true**
SSDEEP:	6144:wtNUinAsuMC58arHZJS68nS9beVPRHPSsd+6NVrNbnjK:8FWSmHZJSPS9bQpHP5dTxi
MD5:	C6281DBF1E7F8D63CDBB6FBA7E32FC55
SHA1:	F53EC938F3090E49CEC933B5E126F9F2C695CADA
SHA-256:	FD25DD08024DA860BE53CD4653004E8568A523E548673C0A3FFFC5F778150778
SHA-512:	338FFC8BCA62AE71DD537DAED9FFE701E7641DC14494B781DC64B61E9A753D81E7A32EFEFF00928349002C0CFC859A45B0693FFD9FE5C94E0B062F52733FC2 2
Malicious:	false
Preview:	.(..bv..f....BJ..qx.....v...&..k.i...U..$..x...=..!.f..72.!.W..+3'.. 1l.S..F]....:DY.\.....h.:.......]t.\>...z.+..fs.si__L=$.....{.da=8..q...."_.JW..z......%oR.5A#[n.`.....T.0..r.K.S.d.%...<..52.A.g....Oq.P..r..H......]..B.S.|{..<c....z...3...g....v..X.$r.f`....H......F....k.i.s.U..$..x...=#.!.f..7..!.....31r.b...fab....a..a...9.]...d)`/&{.....)........#s.si__L...p>.].=$...xX.)g....\W.}p.....Pd.:.d..b..`.....T~...W.K.X&..q......<2_A.g...LO.QYQOrm..L.....].<n..S?\|{.K.c....z...3... ....v..f.:r.f`...........J...k.i...U..$..x...=..!.f..7..!.....31r.b...fab....a..a...9.]...d)`/&{.....)........#s.si__L...p>.].=$...xX.)g....\W.}p.....Pd.:.d..b..`.....T.0..r.K.7.d.q....!.<2.A.g...LO.QYQOr........].<n..S?\|{.K.c....z...3... ....v..f.:r.f`...........J...k.i...U..$..x...=..!.f..7..!.....31r.b...fab....a..a...9.]...d)`/&{.....)........#s.si__L...p>.].=$...xX.)g....\W.}p.....Pd.:.d..b..`.....T.0..r.K.7.d.q....!.<2.A.g...LO.QYQOr........].

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9138695436616
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	rocroc.exe
File size:	271915
MD5:	b7e5425d0daea66fc85e360a0b0d760d
SHA1:	505084085e1ae2666b7b6d15ea82e4d249cbf85c
SHA256:	06fbb80f37ae3534d8d87fe5444da0a09f10e45b8f2882c9e9fe89e879d380c7
SHA512:	c15d0e2e88c6a10c70f2d70d453ebd3f51fbe978fef94ff200e0b98962b6a44c447c0dbc889625ad486e90397af7ab0b61c1dbcce7faf1c828f4610489c5b1b5
SSDEEP:	6144:/Ya6muRXRMsFsHZ2mRKkxZDu772pFxRwy/qLSsgsrzFCvs0eKUW6/f3Ss:/Yw6XRMFHMmRKkxZa776TwKvsgkxaVD6
TLSH:	914412489BF4C1A7F5628B320C3AD66A5EB65A221C79774F5BA01F0C7631382DC1F396
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx

Instruction
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F736C3663CAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F736C36639Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xcf0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0xcf0	0xe00	False	0.4243861607142857	data	4.2499257400572805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b1d8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x3b4c0	0x100	data	English	United States
RT_DIALOG	0x3b5c0	0x11c	data	English	United States
RT_DIALOG	0x3b6e0	0x60	data	English	United States
RT_GROUP_ICON	0x3b740	0x14	data	English	United States
RT_VERSION	0x3b758	0x258	data	English	United States
RT_MANIFEST	0x3b9b0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

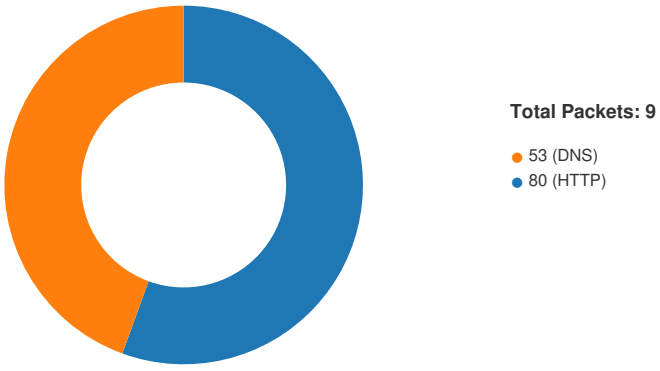
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6192.185.52.24749707802031412 03/20/23-08:48:38.899953	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.6	192.185.52.247
192.168.2.6192.185.52.24749707802031453 03/20/23-08:48:38.899953	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.6	192.185.52.247
192.168.2.6192.185.52.24749707802031449 03/20/23-08:48:38.899953	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.6	192.185.52.247

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 08:48:38.758335114 CET	49707	80	192.168.2.6	192.185.52.247
Mar 20, 2023 08:48:38.885831118 CET	80	49707	192.185.52.247	192.168.2.6
Mar 20, 2023 08:48:38.886101961 CET	49707	80	192.168.2.6	192.185.52.247
Mar 20, 2023 08:48:38.899952888 CET	49707	80	192.168.2.6	192.185.52.247
Mar 20, 2023 08:48:39.024099112 CET	80	49707	192.185.52.247	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 08:48:39.039813042 CET	80	49707	192.185.52.247	192.168.2.6
Mar 20, 2023 08:48:39.039846897 CET	80	49707	192.185.52.247	192.168.2.6
Mar 20, 2023 08:48:39.039869070 CET	80	49707	192.185.52.247	192.168.2.6
Mar 20, 2023 08:48:39.040052891 CET	49707	80	192.168.2.6	192.185.52.247
Mar 20, 2023 08:48:39.040132999 CET	49707	80	192.168.2.6	192.185.52.247
Mar 20, 2023 08:48:39.164454937 CET	80	49707	192.185.52.247	192.168.2.6
Mar 20, 2023 08:48:58.525475025 CET	49708	80	192.168.2.6	160.121.108.17
Mar 20, 2023 08:48:58.802179098 CET	80	49708	160.121.108.17	192.168.2.6
Mar 20, 2023 08:48:58.802460909 CET	49708	80	192.168.2.6	160.121.108.17
Mar 20, 2023 08:48:58.802561998 CET	49708	80	192.168.2.6	160.121.108.17
Mar 20, 2023 08:48:59.081161022 CET	80	49708	160.121.108.17	192.168.2.6
Mar 20, 2023 08:48:59.081218958 CET	80	49708	160.121.108.17	192.168.2.6
Mar 20, 2023 08:48:59.081574917 CET	49708	80	192.168.2.6	160.121.108.17
Mar 20, 2023 08:48:59.081809998 CET	49708	80	192.168.2.6	160.121.108.17
Mar 20, 2023 08:48:59.358578920 CET	80	49708	160.121.108.17	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 08:48:37.582377911 CET	49786	53	192.168.2.6	8.8.8.8
Mar 20, 2023 08:48:37.772387028 CET	53	49786	8.8.8.8	192.168.2.6
Mar 20, 2023 08:48:58.182288885 CET	58595	53	192.168.2.6	8.8.8.8
Mar 20, 2023 08:48:58.524323940 CET	53	58595	8.8.8.8	192.168.2.6
Mar 20, 2023 08:49:19.683146954 CET	56331	53	192.168.2.6	8.8.8.8
Mar 20, 2023 08:49:19.737277031 CET	53	56331	8.8.8.8	192.168.2.6
Mar 20, 2023 08:49:38.430727959 CET	50506	53	192.168.2.6	8.8.8.8
Mar 20, 2023 08:49:38.689497948 CET	53	50506	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 08:48:37.582377911 CET	192.168.2.6	8.8.8.8	0x6bee	Standard query (0)	www.kk156.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 08:48:58.182288885 CET	192.168.2.6	8.8.8.8	0xb1bd	Standard query (0)	www.senriki.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 08:49:19.683146954 CET	192.168.2.6	8.8.8.8	0x33d1	Standard query (0)	www.alaael dinsoft.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 08:49:38.430727959 CET	192.168.2.6	8.8.8.8	0x5b3e	Standard query (0)	www.aq993.cyou	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 08:48:37.772387028 CET	8.8.8.8	192.168.2.6	0x6bee	No error (0)	www.kk156.net		192.185.52.247	A (IP address)	IN (0x0001)	false
Mar 20, 2023 08:48:58.524323940 CET	8.8.8.8	192.168.2.6	0xb1bd	No error (0)	www.senriki.net		160.121.108.17	A (IP address)	IN (0x0001)	false
Mar 20, 2023 08:49:19.737277031 CET	8.8.8.8	192.168.2.6	0x33d1	Server failure (2)	www.alaael dinsoft.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 08:49:38.689497948 CET	8.8.8.8	192.168.2.6	0x5b3e	Name error (3)	www.aq993.cyou	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.kk156.net
- www.senriki.net

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

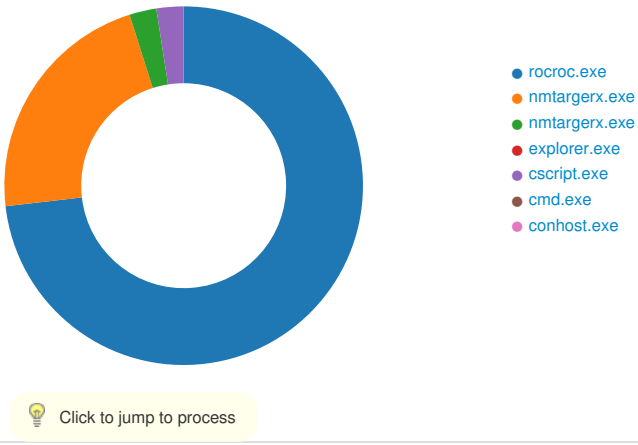
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE1
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE1

Statistics

Behavior



System Behavior

Analysis Process: rocroc.exe PID: **6124**, Parent PID: **3452**

General

Target ID:	0
Start time:	08:47:23
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\rocroc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rocroc.exe
Imagebase:	0x400000
File size:	271915 bytes
MD5 hash:	B7E5425D0DAEA66FC85E360A0B0D760D

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

File Activities

Analysis Process: nmtargerx.exe PID: **5260**, Parent PID: **6124**

General

Target ID:	1
Start time:	08:47:23
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\nmtargerx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\nmtargerx.exe" C:\Users\user\AppData\Local\Temp\rimgurbkmm.edy
Imagebase:	0xb0000
File size:	61440 bytes
MD5 hash:	5DDE2B26DE7E8B448EDCED428AF8E385
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.256878457.0000000001330000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.256878457.0000000001330000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.256878457.0000000001330000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.256878457.0000000001330000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.256878457.0000000001330000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 31%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rimgurbkmm.edy	unknown	4096	success or wait	1	B3DE9	ReadFile
C:\Users\user\AppData\Local\Temp\rimgurbkmm.edy	unknown	4096	success or wait	1	B3DE9	ReadFile
C:\Users\user\AppData\Local\Temp\scrzuow.py	unknown	189440	success or wait	1	2F533A5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F53772	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F53772	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F53772	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F53772	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F53772	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F53772	ReadFile

Analysis Process: nmtargerx.exe PID: **3140**, Parent PID: **5260**

General

Target ID:	2
Start time:	08:47:24
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\nmtargerx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\nmtargerx.exe
Imagebase:	0xb0000
File size:	61440 bytes

MD5 hash:	5DDE2B26DE7E8B448EDCED428AF8E385
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.297641452.0000000001400000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.297641452.0000000001400000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.297641452.0000000001400000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.297641452.0000000001400000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.297641452.0000000001400000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.297541015.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.297541015.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.297541015.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.297541015.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.297541015.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.297615381.00000000013D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.297615381.00000000013D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.297615381.00000000013D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.297615381.00000000013D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.297615381.00000000013D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **3140**

General

Target ID:	3
Start time:	08:47:29
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Formbook_772cc62d, Description: unknown, Source: 00000003.00000002.516554082.0000000005840000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cscript.exe PID: **1788**, Parent PID: **3452**

General

Target ID:	8
Start time:	08:47:43
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xd90000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.512168370.0000000000D60000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.511623036.0000000000830000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.511623036.0000000000830000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.511623036.0000000000830000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.511623036.0000000000830000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.511623036.0000000000830000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.512093073.0000000000D30000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.512093073.0000000000D30000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.512093073.0000000000D30000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.512093073.0000000000D30000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.512093073.0000000000D30000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	84A447	NtReadFile

Analysis Process: cmd.exe PID: **4648**, Parent PID: **1788**

General	
Target ID:	14
Start time:	08:47:49
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\nmtargerx.exe"
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2604**, Parent PID: **4648**

General	
Target ID:	15
Start time:	08:47:49
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly