Aug 31 2023

NETMANAGEIT

Intelligence Report

DreamBus Botnet Exploiting execution Flaw in RocketMQ servers

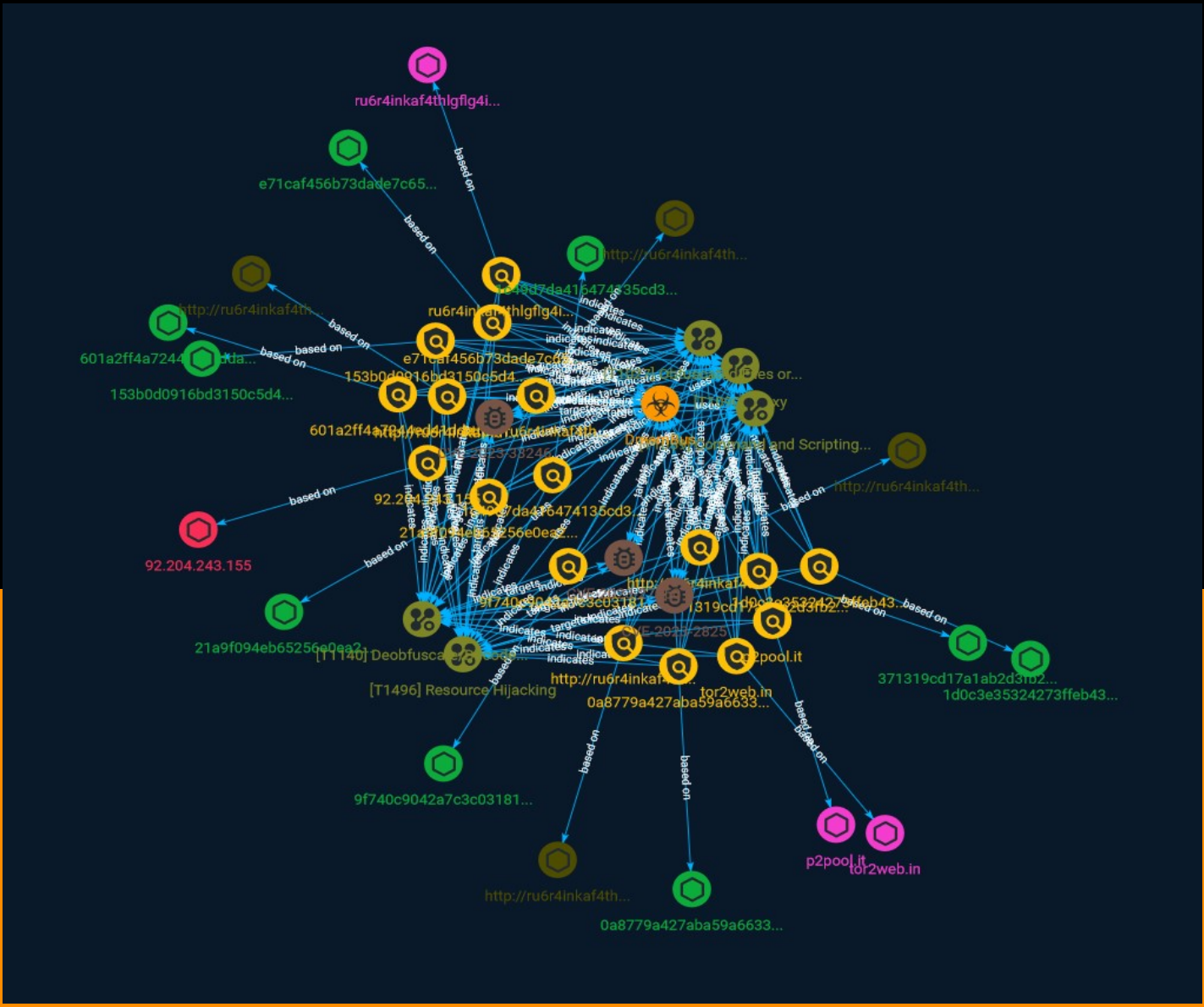

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/ping
Pattern Type
stix
Pattern
[url:value = 'http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/ping']
Name
http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/cmd1
Pattern Type
stix
Pattern
[url:value = 'http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/cmd1']
Name

9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f']

Name

tor2web.in

Pattern Type

stix

Pattern

[domain-name:value = 'tor2web.in']

Name

601a2ff4a7244ed41dda1c1fc71b10d3cfefa34e2ef8ba71598f41f73c031443

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '601a2ff4a7244ed41dda1c1fc71b10d3cfefa34e2ef8ba71598f41f73c031443']

Name

http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/mine

Pattern Type

stix

Pattern

[url:value = 'http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/mine']

Name

21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417']

Name

http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/kill

Pattern Type

stix

Pattern

[url:value = 'http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/kill']

Name

1c49d7da416474135cd35a9166f2de0f8775f21a27cd47d28be48a2ce580d58d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c49d7da416474135cd35a9166f2de0f8775f21a27cd47d28be48a2ce580d58d']

Name

92.204.243.155

Description

ISP: Host Europe GmbH **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **4369:** ``` Erlang Port Mapper Daemon: nodes: rabbit: 25672 ``` ---------- **5672:** ``` AMQP: Protocol Version: 0-9 Product: RabbitMQ Product Version: 3.11.7 Platform: Erlang/OTP 25.2.1 Capabilities: Exchange Exchange Bindings: True Connection.blocked: True Authentication Failure Close: True Direct Reply To: True Basic.nack: True Per Consumer Qos: True Consumer Priorities: True Consumer Cancel Notify: True Publisher Confirms: True ``` ---------- **6379:** ``` # Server redis_version:6.2.5 redis_git_sha1:00000000 redis_git_dirty:0 redis_build_id:f272b47bc83a1122 redis_mode:standalone os:Linux 5.11.0-25-generic x86_64 arch_bits:64 multiplexing_api:epoll atomicvar_api:c11-builtin gcc_version:9.3.0 process_id:2112077 process_supervised:systemd run_id:a73a80fe3f94e53a2679e3fc61b17c6ea76395f4 tcp_port:6379 server_time_usec:1693024673307265 uptime_in_seconds:32754233 uptime_in_days:379 hz:10 configured_hz:10 lru_clock:15303073 executable:/usr/bin/redis-server config_file:/etc/redis/redis.conf io_threads_active:0 # Clients connected_clients:5 cluster_connections:0 maxclients:10000 client_recent_max_input_buffer:32 client_recent_max_output_buffer:0 blocked_clients:0 tracking_clients:0

clients_in_timeout_table:0 # Memory used_memory:1067312 used_memory_human:1.02M used_memory_rss:5013504 used_memory_rss_human:4.78M used_memory_peak:6585544 used_memory_peak_human:6.28M used_memory_peak_perc:16.21% used_memory_overhead:896600 used_memory_startup:810192 used_memory_dataset:170712 used_memory_dataset_perc:66.39% allocator_allocated:1257144 allocator_active:1822720 allocator_resident:4636672 total_system_memory:14674329600 total_system_memory_human:13.67G used_memory_lua:70656 used_memory_lua_human:69.00K used_memory_scripts:4376 used_memory_scripts_human:4.27K number_of_cached_scripts:11 maxmemory:0 maxmemory_human:0B maxmemory_policy:allkeys-lru allocator_frag_ratio:1.45 allocator_frag_bytes:565576 allocator_rss_ratio:2.54 allocator_rss_bytes:2813952 rss_overhead_ratio:1.08 rss_overhead_bytes:376832 mem_fragmentation_ratio:5.44 mem_fragmentation_bytes:4091792 mem_not_counted_for_evict:0 mem_replication_backlog:0 mem_clients_slaves:0 mem_clients_normal:82032 mem_aof_buffer:0 mem_allocator:jemalloc-5.1.0 active_defrag_running:0 lazyfree_pending_objects:0 lazyfreed_objects:0 # Persistence loading:0 current_cow_size:0 current_cow_size_age:0 current_fork_perc:0.00 current_save_keys_processed:0 current_save_keys_total:0 rdb_changes_since_last_save:8478 rdb_bgsave_in_progress:0 rdb_last_save_time:1690743986 rdb_last_bgsave_status:err rdb_last_bgsave_time_sec:0 rdb_current_bgsave_time_sec:-1 rdb_last_cow_size:528384 aof_enabled:0 aof_rewrite_in_progress:0 aof_rewrite_scheduled:0 aof_last_rewrite_time_sec:-1 aof_current_rewrite_time_sec:-1 aof_last_bgrewrite_status:ok aof_last_write_status:ok aof_last_cow_size:0 module_fork_in_progress:0 module_fork_last_cow_size:0 # Stats total_connections_received:5211485 total_commands_processed:982135326 instantaneous_ops_per_sec:143 total_net_input_bytes:68471920824 total_net_output_bytes:1813276829172 instantaneous_input_kbps:9.77 instantaneous_output_kbps:235.98 rejected_connections:0 sync_full:0 sync_partial_ok:0 sync_partial_err:0 expired_keys:71 expired_stale_perc:0.00 expired_time_cap_reached_count:0 expire_cycle_cpu_milliseconds:111 evicted_keys:0 keyspace_hits:7771333 keyspace_misses:1421 pubsub_channels:1 pubsub_patterns:0 latest_fork_usec:471 total_forks:3699452 migrate_cached_sockets:0 slave_expires_tracked_keys:0 active_defrag_hits:0 active_defrag_misses:0 active_defrag_key_hits:0 active_defrag_key_misses:0 tracking_total_keys:0 tracking_total_items:0 tracking_total_prefixes:0 unexpected_error_replies:0 total_error_replies:72908 dump_payload_sanitizations:0 total_reads_processed:64696916 total_writes_processed:132675384 io_threaded_reads_processed:0 io_threaded_writes_processed:0 # Replication role:slave master_host:92.204.243.156 master_port:6379 master_link_status:down master_last_io_seconds_ago:-1 master_sync_in_progress:0 slave_repl_offset:1 master_link_down_since_seconds:-1 slave_priority:100 slave_read_only:0 replica_announced:1 connected_slaves:0 master_failover_state:no-failover master_replid:5d4ab1d097172eba5d8285b5eff71c4ad8472aa2 master_replid2:a2cf02ab56d9badbb680805bc8139494db7ff632 master_repl_offset:6617104233 second_repl_offset:6617104234 repl_backlog_active:0 repl_backlog_size:1048576 repl_backlog_first_byte_offset:6616055658 repl_backlog_histlen:1048576 # CPU

used_cpu_sys:27084.688546 used_cpu_user:34313.894106 used_cpu_sys_children:477.090970 used_cpu_user_children:2351.089249 used_cpu_sys_main_thread:26266.760528 used_cpu_user_main_thread:33933.784614 # Modules # Errorstats errorstat_ERR:count=71726 errorstat_MISCONF:count=1181 errorstat_WRONGTYPE:count=1 # Cluster cluster_enabled:0 # Keyspace # Keys # Connected Clients id=5215935 addr=92.204.243.155:51873 laddr=92.204.243.155:6379 fd=10 name=sentinel-1aec94f8-pubsub age=53 idle=1 flags=P db=0 sub=1 psub=0 multi=-1 qbuf=0 qbuf-free=0 argv-mem=0 obl=0 oll=0 omem=0 tot-mem=20504 events=r cmd=subscribe user=default redir=-1 id=5215936 addr=92.204.243.156:50657 laddr=92.204.243.155:6379 fd=11 name=sentinel-b0267c85-pubsub age=53 idle=1 flags=P db=0 sub=1 psub=0 multi=-1 qbuf=0 qbuf-free=0 argv-mem=0 obl=0 oll=0 omem=0 tot-mem=20504 events=r cmd=subscribe user=default redir=-1 id=5215940 addr=92.204.243.156:45619 laddr=92.204.243.155:6379 fd=12 name=sentinel-b0267c85-cmd age=11 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=0 qbuf-free=0 argv-mem=0 obl=0 oll=0 omem=0 tot-mem=20496 events=r cmd=ping user=default redir=-1 id=5215941 addr=92.204.243.155:36973 laddr=92.204.243.155:6379 fd=14 name=sentinel-1aec94f8-cmd age=1 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=0 qbuf-free=0 argv-mem=0 obl=0 oll=0 omem=0 tot-mem=20496 events=r cmd=ping user=default redir=-1 id=5215942 addr=224.143.82.8:52730 laddr=92.204.243.155:6379 fd=9 name= age=0 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=26 qbuf-free=40928 argv-mem=10 obl=0 oll=0 omem=0 tot-mem=61466 events=r cmd=client user=default redir=-1 ``` ---------- **8500:** ``` Consul agent: Datacenter: qa-b NodeName: vmb02 NodeID: 1aba8cc6-1cc4-9cc7-4d8d-c2d60e93ab45 Server: True PrimaryDatacenter: qa-b Version: 1.14.3 BuildDate: 2022-12-13T17:13:55Z Revision: bd257019 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.204.243.155']

Name

e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d']

Name

371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c']

Name

153b0d0916bd3150c5d4ab3e14688140b34fdd34caac725533adef8f4ab621e2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '153b0d0916bd3150c5d4ab3e14688140b34fdd34caac725533adef8f4ab621e2']

Name

p2pool.it

Pattern Type

stix

Pattern

[domain-name:value = 'p2pool.it']

Name

0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f']

Name

ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion

Pattern Type

stix

Pattern

[domain-name:value = 'ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion']

Name

1d0c3e35324273ffeb434f929f834b59dcc6cdd24e9204abd32cc0abefd9f047

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d0c3e35324273ffeb434f929f834b59dcc6cdd24e9204abd32cc0abefd9f047']

Malware

Name
DreamBus

Vulnerability

Name
CVE-2023-2825
Name
CVE-2023-33246
Name
CVE-2023-27350

Attack-Pattern

Name
Proxy
ID
T1090
Description
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.
Name
Resource Hijacking
ID
T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary.

(Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.

(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Domain-Name

Value
p2pool.it
ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion
tor2web.in

StixFile

Value
601a2ff4a7244ed41dda1c1fc71b10d3cfefa34e2ef8ba71598f41f73c031443
1d0c3e35324273ffeb434f929f834b59dcc6cdd24e9204abd32cc0abefd9f047
9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f
1c49d7da416474135cd35a9166f2de0f8775f21a27cd47d28be48a2ce580d58d
0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f
e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d
371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c
153b0d0916bd3150c5d4ab3e14688140b34fdd34caac725533adef8f4ab621e2
21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417

IPv4-Addr

Value
92.204.243.155

Url

Value
http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/mine
http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/ping
http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/cmd1
http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion/kill

External References

- https://cybersecuritynews.com/dreambus-botnet-rocketmq-servers/
- https://otx.alienvault.com/pulse/64ee0767ef32a83bd953ff02
- https://blogs.juniper.net/en-us/threat-research/dreambus-botnet-resurfaces-targets-rocketmq-vulnerability