Jan 12 2024

NETMANAGEIT

Intelligence Report

DreamBus Unleashes Metabase Mayhem With New Exploit Module

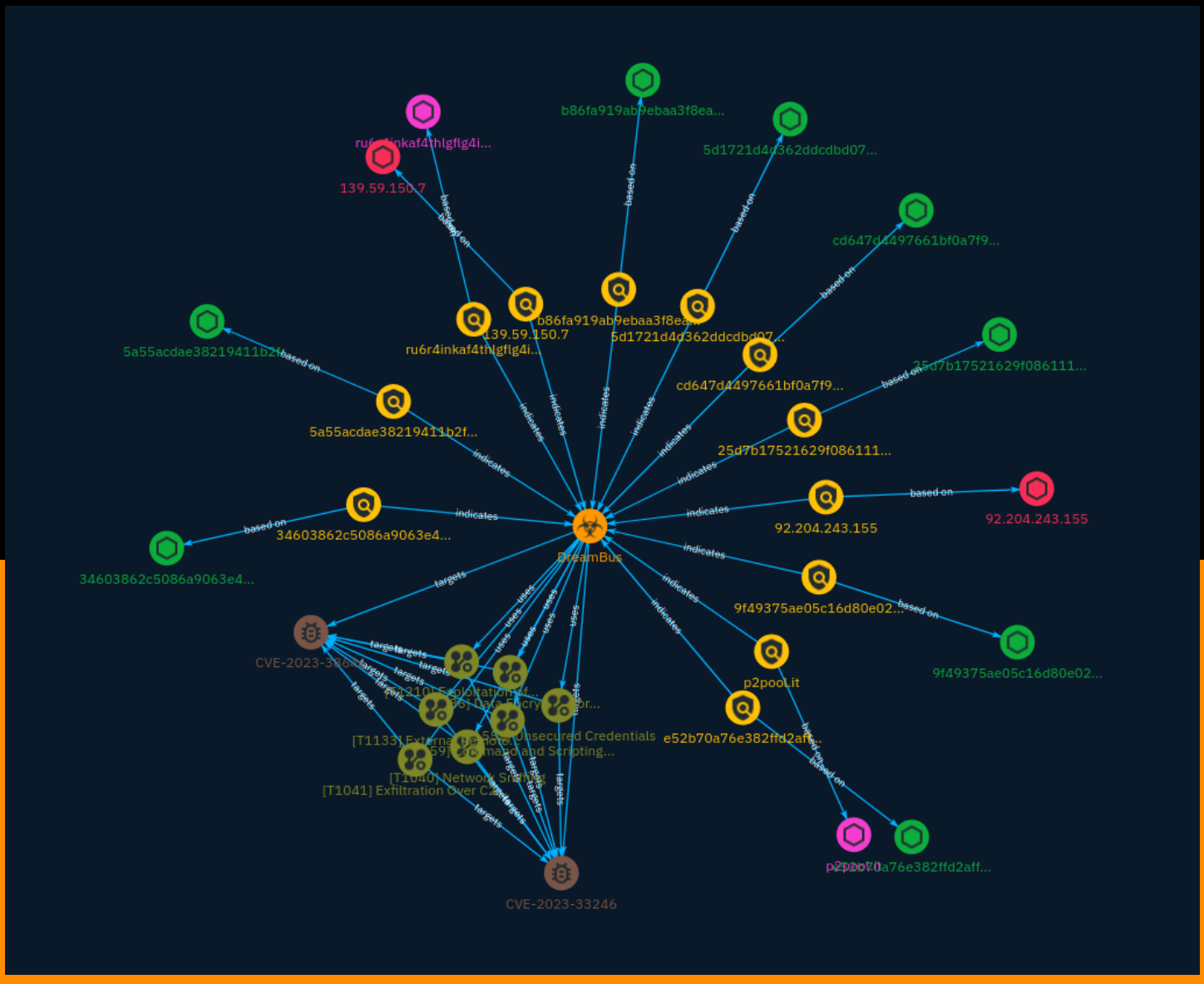

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Zscaler's ThreatLabz research team has been tracking the Linux-based malware family known as DreamBus. Not much has changed in the last few years other than minor bug fixes, and slight modifications to evade detection from security software. However, in the last 6 months, the threat actor operating DreamBus has introduced two new modules to target vulnerabilities in Metabase and Apache RocketMQ. This is likely in response to a decrease in new infections stemming from exploits utilized by DreamBus, many of which are dated and have been in use for several years. DreamBus also continues to use techniques that exploit implicit trust and weak passwords including Secure Shell (SSH), IT administration tools, cloud-based applications, and databases. The primary monetization vector for DreamBus infections is still through mining Monero cryptocurrency.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Network Sniffing
ID
T1040
Description
Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data. Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay] (https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary. Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities. In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)(Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use

exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring) On network devices, adversaries may perform network captures using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `monitor capture`.(Citation: US-CERT-TA18-106A)(Citation: capture_embedded_packet_on_software)

Name

Exploitation of Remote Services

ID

T1210

Description

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

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

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management]

(https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

Unsecured Credentials

ID

T1552

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name
5d1721d4d362ddcdbd0762eccdb4e07b0cc1c26c7d69da30e024e70c7063c519
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5d1721d4d362ddcdbd0762eccdb4e07b0cc1c26c7d69da30e024e70c7063c519']
Name
9f49375ae05c16d80e02c21f178429602f726ce87295b9dfd9458f37956392e3
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9f49375ae05c16d80e02c21f178429602f726ce87295b9dfd9458f37956392e3']
Name

5a55acdae38219411b2f3350db425d8883d6238e465d07a71cadfe89877df6ac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a55acdae38219411b2f3350db425d8883d6238e465d07a71cadfe89877df6ac']

Name

25d7b17521629f0861113b1e9f7653dc19c40b1d8f3de685ba29108a0d9fa7aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25d7b17521629f0861113b1e9f7653dc19c40b1d8f3de685ba29108a0d9fa7aa']

Name

e52b70a76e382ffd2aff02d1d26269036c589676ba1f2086051c11cb7997a5a5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e52b70a76e382ffd2aff02d1d26269036c589676ba1f2086051c11cb7997a5a5']

Name

b86fa919ab9ebaa3f8ead4f7ef6ee0bb94a3a1b7d9583e99598893f2738a1c71

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b86fa919ab9ebaa3f8ead4f7ef6ee0bb94a3a1b7d9583e99598893f2738a1c71']

Name

92.204.243.155

Description

Mirai botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.204.243.155']

Name

34603862c5086a9063e42d79fb094e8d89e3aeef6f8eadf23c6925c6a4201a9c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '34603862c5086a9063e42d79fb094e8d89e3aeef6f8eadf23c6925c6a4201a9c']

Name

139.59.150.7

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_6.6.1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCos4kFYOSKc02n2pfgsthdOg+22KnsQdGajWnJvDQDsM6p sav9jPkFZYmjqJsD/jcm1pwiMY33OM/4/EDaHxzn3nNNnr92SH/C+kZPummUeMvgudEdoNI2WdA8 EfcvriEvvfg3DKQDGa5BxvSfn8fUNjvmgi+RMTCes6w77IoR9vhHoCjMaV7/YzEHe+sNWq8ef8oM jSFFAfeGo2NTPkKaPbqCGsUyGDmMzCHmV7kkaZ+zAXW19OcCJahTwedlVsJyWCmzDsQi/hzr1rqn YuWmlkvVOKbjUchAwTBBDutx7zII8Yj9l1hWVlydDPxNPQHeOJ4Wz+QQZjSCR77CJyaZ Fingerprint: fd:5b:63:f8:43:f5:15:e4:33:5b:36:24:51:89:82:45 Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5-etm@openssh.com hmac-sha1-etm@openssh.com umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-ripemd160-etm@openssh.com hmac-sha1-96-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-md5 hmac-sha1 umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Wed, 10 Jan 2024 22:45:10 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Wed, 05 Jan 2022 13:20:17 GMT ETag: "51c-5d4d59d602640" Accept-

Ranges: bytes Content-Length: 1308 Content-Type: text/html; charset=UTF-8 ``` ---------- **443:** ``` HTTP/1.0 404 Not Found Date: Sun, 07 Jan 2024 16:03:42 GMT Connection: close Content-type: text/html

404 Not Found

The requested URL was not found ``` ---------- **3306:** ``` MariaDB: Error Message: Host '224.255.187.125' is not allowed to connect to this MariaDB server Error Code: 1130 ``` ---------- **8080:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express X-RateLimit-Limit: 2000 X-RateLimit-Remaining: 1999 set-cookie: session=s%3AtDJqE2pFuJU8SJHiiM5d4jKULoGrNcf5.6CDfPXuGVF%2F2XLawKOZEl2%2BNEOoeXw9xHBgTrNXRLCE; Path=/; HttpOnly Date: Mon, 25 Dec 2023 08:03:10 GMT Connection: keep-alive Content-Length: 0 ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '139.59.150.7']

Name
p2pool.it

Pattern Type
stix

Pattern

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

Name

ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion

Description

Mirai botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

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

Name

cd647d4497661bf0a7f9a11fd5ca84d52f49d4cca74941a31cf631c8f6bc88d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd647d4497661bf0a7f9a11fd5ca84d52f49d4cca74941a31cf631c8f6bc88d2']

Malware

Name
DreamBus

Vulnerability

Name
CVE-2023-33246

Description
Several components of Apache RocketMQ, including NameServer, Broker, and Controller, are exposed to the extranet and lack permission verification. An attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as or achieve the same effect by forging the RocketMQ protocol content.

Name
CVE-2023-38646

Domain-Name

Value
p2pool.it
ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad.onion

StixFile

Value
b86fa919ab9ebaa3f8ead4f7ef6ee0bb94a3a1b7d9583e99598893f2738a1c71
e52b70a76e382ffd2aff02d1d26269036c589676ba1f2086051c11cb7997a5a5
5a55acdae38219411b2f3350db425d8883d6238e465d07a71cadfe89877df6ac
5d1721d4d362ddcdbd0762eccdb4e07b0cc1c26c7d69da30e024e70c7063c519
9f49375ae05c16d80e02c21f178429602f726ce87295b9dfd9458f37956392e3
cd647d4497661bf0a7f9a11fd5ca84d52f49d4cca74941a31cf631c8f6bc88d2
25d7b17521629f0861113b1e9f7653dc19c40b1d8f3de685ba29108a0d9fa7aa
34603862c5086a9063e42d79fb094e8d89e3aeef6f8eadf23c6925c6a4201a9c

IPv4-Addr

Value
92.204.243.155
139.59.150.7

External References

- https://otx.alienvault.com/pulse/65a11e3746e6adfeb24af445
- https://www.zscaler.com/blogs/security-research/dreambus-unleashes-metabase-mayhem-new-exploit-module