Oct 15 2023

NETMANAGEIT

Intelligence Report

ShellBot DDoS Malware Installed Through Hexadecimal Notation Addresses

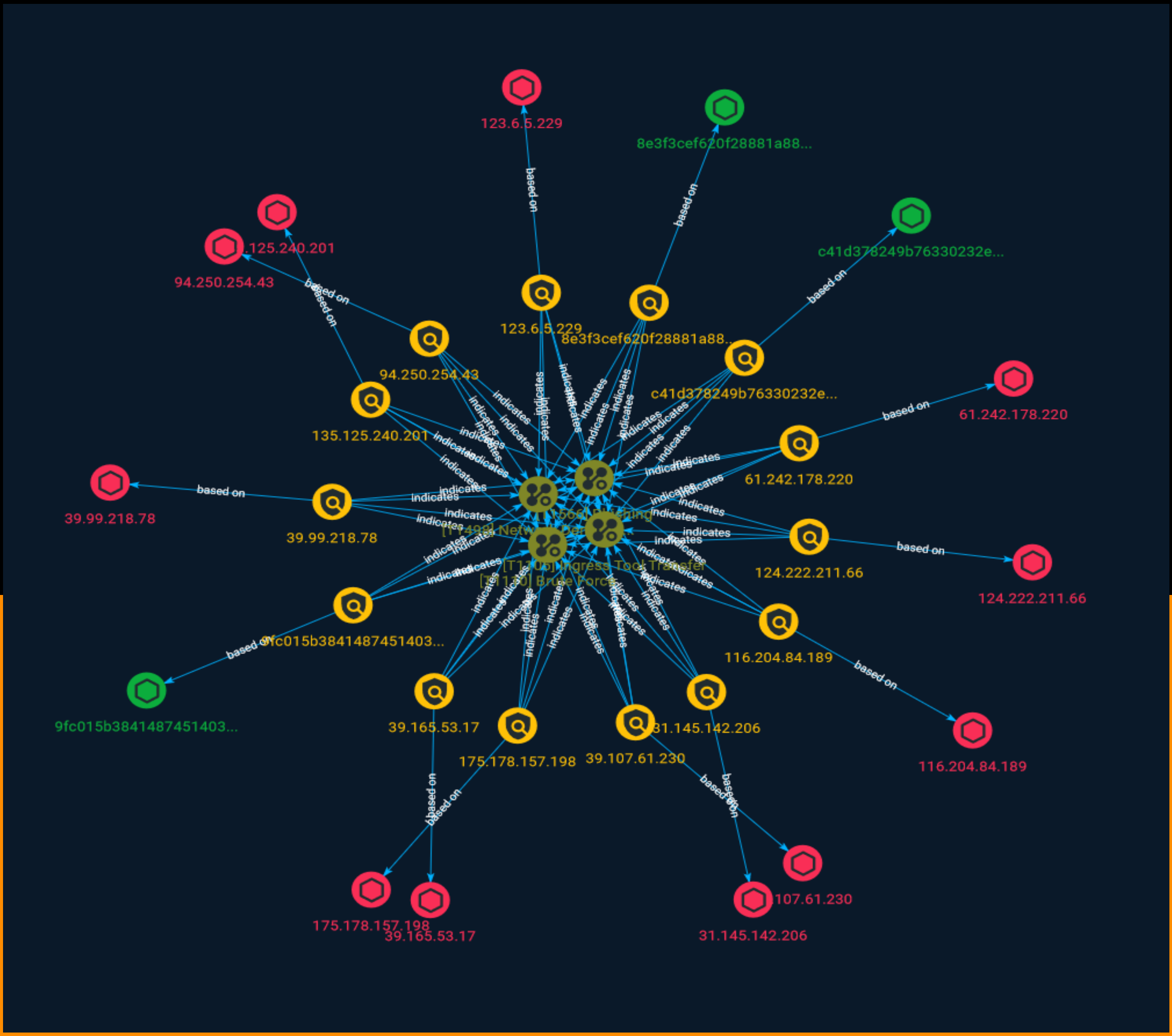

Table of contents

Overview

- Description 3
- Confidence 3
- Content 4

Entities

- Attack-Pattern 5
- Indicator 9

Observables

- StixFile 18
- IPv4-Addr 19

External References

- External References 20

Overview

Description

AhnLab Security Emergency response Center (ASEC) has recently discovered a change in the distribution method of the ShellBot malware, which is being installed on poorly managed Linux SSH servers. The overall flow remains the same, but the download URL used by the threat actor to install ShellBot has changed from a regular IP address to a hexadecimal value.

Confidence

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

15 / 100

Content

4

N/A

Name

Network Denial of Service

ID

T1498

Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Indicator

Name

123.6.5.229

Description

CC=CN ASN=AS4837 CHINA UNICOM China169 Backbone

Pattern Type

stix

Pattern

[ipv4-addr:value = '123.6.5.229']

Name

116.204.84.189

Description

ISP: Huawei Cloud Service data center **OS:** None -------------------------- Hostnames: - ecs-116-204-84-189.compute.hwclouds-dns.com -------------------------- Domains: - hwclouds-dns.com -------------------------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Sat, 16 Sep 2023 03:21:30 GMT Content-Type: text/html Content-Length: 1326 Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "59005463-52e" Accept-Ranges: bytes ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '116.204.84.189']

Name

9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97

Description

Win.Trojan.IRCBot-785 SHA256 of 8853bb0aef4a3dfe69b7393ac19ddf7f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97']

Name

c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140

Description

Win.Trojan.IRCBot-785 SHA256 of a92559ddace1f9fa159232c1d72096b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140']

Name

39.107.61.230

Description

ISP: Hangzhou Alibaba Advertising Co.,Ltd. **OS:** None -------------------------- Hostnames: -------------------------- Domains: -------------------------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.14.1 Date: Sat, 30 Sep 2023 14:32:25 GMT Content-Type: text/html Content-Length: 12 Last-Modified: Fri, 15 Sep 2023 13:41:41 GMT Connection: keep-alive ETag: "65045f15-c" Accept-Ranges: bytes ``` ------------------ **3306:** ``` MySQL: Protocol Version: 10 Version: 8.0.33 Capabilities: 65535 Server Language: 255 Server Status: 2 Extended Server Capabilities: 57343 Authentication Plugin: caching_sha2_password ``` ------------------ **6001:** ``` HTTP/1.1 400 Content-Type: text/html;charset=utf-8 Content-Language: en Content-Length: 435 Date: Wed, 11 Oct 2023 09:17:10 GMT Connection: close

HTTP Status 400 – Bad Request

``` ------------------

**Pattern Type**

stix

**Pattern**
```

[ipv4-addr:value = '39.107.61.230']

Name

135.125.240.201

Description

Agressive IP known malicious on AbuseIPDB - countryCode: DE - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-12T15:15:22+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '135.125.240.201']

Name

124.222.211.66

Description

Agressive IP known malicious on AbuseIPDB - countryCode: CN - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-13T15:00:11+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '124.222.211.66']

Name

39.165.53.17

Description

CC=CN ASN=AS24445 Henan Mobile Communications Co.,Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '39.165.53.17']

Name

8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a

Description

Win.Trojan.IRCBot-785 SHA256 of 7bc4c22b0f34ef28b69d83a23a6c88c5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a']

Name

31.145.142.206

Description

Agressive IP known malicious on AbuseIPDB - countryCode: TR - abuseConfidenceScore: 100 - lastReportedAt: 2023-08-05T09:16:23+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.145.142.206']

Name

39.99.218.78

Description

ISP: Hangzhou Alibaba Advertising Co.,Ltd. **OS:** None -------------------------- Hostnames: -------------------------- Domains: -------------------------- Services: **80:** ``` HTTP/1.1 403 Forbidden Date: Sun, 01 Oct 2023 10:20:06 GMT Server: Apache/2.4.6 (CentOS) Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` ------------------ **3306:** ``` MySQL: Protocol Version: 10 Version: 8.0.19 Capabilities: 65535 Server Language: 255 Server Status: 2 Extended Server Capabilities: 51199 Authentication Plugin: caching_sha2_password ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '39.99.218.78']

Name

61.242.178.220

Description

ISP: CHINA UNICOM China169 Backbone **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDHkqako1gS+tjY/P9U4RAY0sYSSSpcY1jVRF7iruXCYcS8 ILCPmGNSkafaoErUGqL/w62tzkdLnSoVGjtFMUm7aSvgqD/s02XhsN4tHe/j44AgGmBx+5u6Dir0 m6juEmzzdcjs1oSx1u//4zu39+JURl28fLk+TFMTdG0gVdnA3ycX/wcXe8UOCUgvlf2+KJCNla7B AcBAJ5KTnhoWBk4bOYUK3HalqmzYtv1G3ikUvYEiMTpqJ363iPH73gwxthQF2j0Cq0lAX0M7MN1x xNyD230bNWPMV6mvJxUqOVhNbTz/rAlbu9vlAvfoDybdP7lKmQ09drK95JIHd1sJnCCN Fingerprint: 02:2a:fa:36:bf:75:0d:da:35:ec:21:5d:7b:b3:e3:89 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------ **9999:** ``` HTTP/1.1 200 OK Accept-Ranges: bytes Content-Length: 1266 Content-Type: text/html Last-Modified: Wed, 06 Sep 2023 02:40:55 GMT Server: MinIO Console X-Content-Type-Options: nosniff X-Frame-Options: DENY X-Xss-Protection: 1; mode=block Date: Wed, 06 Sep 2023 02:40:55 GMT Connection: close ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '61.242.178.220']

Name

175.178.157.198

Description

ISP: Shenzhen Tencent Computer Systems Company Limited **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC/09CDltG4hdlCcJRWH7P/+3/M5jv+NIPsWbNFpU30hEpP ZttAQo+nYhKDVgqWt04OgrECzGVo1A9w2A27KdVQltTijRyTc90Fgq8dCk4Sjp6c/ncBShktFLIy R+Lov0gCakRYP8NKGfof/Jahqbsf2jLEbDPz5YlRwGGY3nXsssu8K/uxmgOJh6UcxklkmFJ2pZOG jqIj+DPn2XN01MH/5L/p92lzanpiZs+HrJaKqhmnAwX0DmMLPiPpM5uveSFSa4S3IyG8id4RB1tP IcT1z/d61kyZFWJBHkNG3WyrhfD7w5JpE0eLi1uDlN9DvkEPOkv5lmuFTvoRz6JbCIRL Fingerprint: c9:9c:60:94:89:4c:d5:62:d3:c5:5e:4c:b0:1c:ea:85 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------ **3306:** ``` MySQL: Error Message: Host '224.133.101.29' is not allowed to connect to this MySQL server Error Code: 1130 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '175.178.157.198']

Name

94.250.254.43

Description

CC=RU ASN=AS29182 JSC IOT

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.250.254.43']

StixFile

Value
9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97
8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a
c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140

IPv4-Addr

Value
61.242.178.220
94.250.254.43
39.107.61.230
116.204.84.189
39.99.218.78
39.165.53.17
124.222.211.66
175.178.157.198
123.6.5.229
31.145.142.206
135.125.240.201

External References

- https://otx.alienvault.com/pulse/652847937abbfd5f6e9087a9
- https://asec.ahnlab.com/en/57635/