ハニーポット簡易調査報告書（日次）

作成日時：2023/02/26 (日) 00:00

Twitter：@MMWR_Security

概要

- Amazon Lightsail上に設置してあるT-Potが受けた攻撃のうち、 1 日間の計測結果をまとめます。
- 計測期間は 2023/02/25 (土) 00:00 - 2023/02/26 (日) 00:00 です。

詳細内容

【攻撃を受けたハニーポット Top10】

ハニーポットの種類	攻撃を受けた回数
Cowrie	3,331
Ddospot	2,642
Dionaea	636
Adbhoney	402
Redishoneypot	128
Honeytrap	119
CitrixHoneypot	53
Tanner	52
ConPot	33
Ciscoasa	19

送信元AS Top10

送信元AS番号	送信元AS名	送信された回数
4134	No.31,Jin-rong Street	913
3269	Telecom Italia	256
17762	Tata Teleservices Maharashtra Ltd	233
5438	Agence Tunisienne d'Internet	218
30722	Vodafone Italia S.p.A.	215
15475	NOL	211
14061	DigitalOcean, LLC	209
27831	Colombia Móvil	130
4766	Korea Telecom	129
8708	RCS & RDS	121

【送信元IPアドレス Top10】

送信元IPアドレス	送信回数
49.248.155.173	233
197.5.145.150	218
87.15.210.210	218
93.148.246.51	214
62.193.68.91	211
222.81.35.186	176
181.206.14.42	129
86.105.27.140	118
159.223.135.216	113
128.199.58.12	109

【送信元IPアドレスの評価 Top3】

送信元IPアドレスの評価	区分
known attacker	2,714
mass scanner	45
tor exit node	6

【攻撃を仕掛けてきた国 Top10】

攻撃を仕掛けてきた国	攻撃を受けた回数
United States	1,517
China	1,256
Italy	493
India	306
Japan	270
Egypt	227
Singapore	224
Tunisia	220
South Korea	218
Colombia	186

攻撃を仕掛けてきた国Top5中の送信先ポート Top5

攻撃を仕掛けてきた国	送信先ポート	攻撃を仕掛けた回数
United States	123	1,136
United States	22	25
United States	5555	18
United States	25	16
United States	445	13
China	123	274
China	1433	179
China	6379	86
China	23	73

攻撃を仕掛けてきた国	送信先ポート	攻撃を仕掛けた回数
China	1521	12
Italy	22	64
Italy	123	34
Italy	23	1
India	445	235
India	123	26
India	23	7
India	5555	6
India	6379	6
Japan	123	145
Japan	22	10
Japan	23	6
Japan	6379	3
Japan	445	2

【送信元OS Top10】

送信元OS	送信された回数
Linux 2.2.x-3.x	3,039
Windows 7 or 8	570
Linux 3.11 and newer	490
Windows NT kernel	479
Linux 2.2.x-3.x (barebone)	148
Linux 3.1-3.10	76
Linux 2.2.x-3.x (no timestamps)	43
Linux 2.6.x	35
Linux 2.4.x-2.6.x	11
Linux 3.x	10

Suricataアラート署名 Top10

ID	説明	回数
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	7,068
2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read	1,488
2200094	SURICATA zero length padN option	1,488
2017162	ET SCAN SipCLI VOIP Scan	323
2002752	ET POLICY Reserved Internal IP Traffic	296
2010935	ET SCAN Suspicious inbound to MSSQL port 1433	223
2009582	ET SCAN NMAP -sS window 1024	210
2001219	ET SCAN Potential SSH Scan	158
2100402	GPL ICMP_INFO Destination Unreachable Port Unreachable	113
2001978	ET POLICY SSH session in progress on Expected Port	102

【利用を試みられたCVE Top10】

利用を試みられたCVE	利用を試みられた回数
CVE-2020-11899	1,488
CVE-2022-27255 CVE-2022-27255	21
CVE-2019-11500 CVE-2019-11500	16
CVE-2002-0013 CVE-2002-0012	7
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	6
CVE-2001-0414	4
CVE-2005-4050	2

【侵入を試みられたユーザID Top50】

侵入を試みられたユーザID	侵入を試みられた回数
root	188
sa	186
admin	62
ubuntu	16
345gs5662d34	14
test	14
user	8
postgres	7
super	5
administrator	4
git	4
testuser	4
ftptest	3
guest	3
john	3
mother	3
nagios	3
service	3
supervisor	3
test01	3
(empty)	2
admin1	2
crayadm	2
default	2
gitlab-runner	2
luis	2
oracle	2
pi	2

侵入を試みられたユーザID	侵入を試みられた回数
sysadmin	2
test002	2
666666	1
888888	1
Admin	1
Administrator	1
MODTEST	1
alan	1
ali	1
alin	1
alpine	1
amg	1
anonymous	1
ansible	1
avianto	1
brian	1
cf	1
chart	1
cistest	1
dadmin	1
daemon	1
datac	1

【侵入を試みられたパスワード Top50】

侵入を試みられたパスワード	侵入を試みられた回数
(empty)	25
admin	17
1234	15
3245gs5662d34	14
345gs5662d34	14
123456	13
password	12
12345	10
root	9
123	8
1	7
1234567890	7
test123	7
123123	6
12345678	6
1qaz2wsx	6
pass	6
test	6
1988	5
7ujMko0admin	5
1111	4
666666	4
888888	4
abc123	4
ipcam_rt5350	4
ivdev	4
qwertyuiop	4
saadmin	4

侵入を試みられたパスワード	侵入を試みられた回数
zhongxing	4
zlxx.	4
0	3
111111	3
1111111	3
112233	3
123321	3
123456789	3
123qwe	3
1q2w3e4r	3
admin123	3
admin1234	3
admin@123	3
aquario	3
dreambox	3
football	3
fucker	3
service	3
supervisor	3
xc3511	3
!@#$%^&*	2
!QAZ2wsx	2

参考情報

- 2019年10月のハニーポット観察記録。100万回を超えるMySQLへの攻撃を観測