MOZI BotNet Malware
(CSB21-10)

September 8, 2021

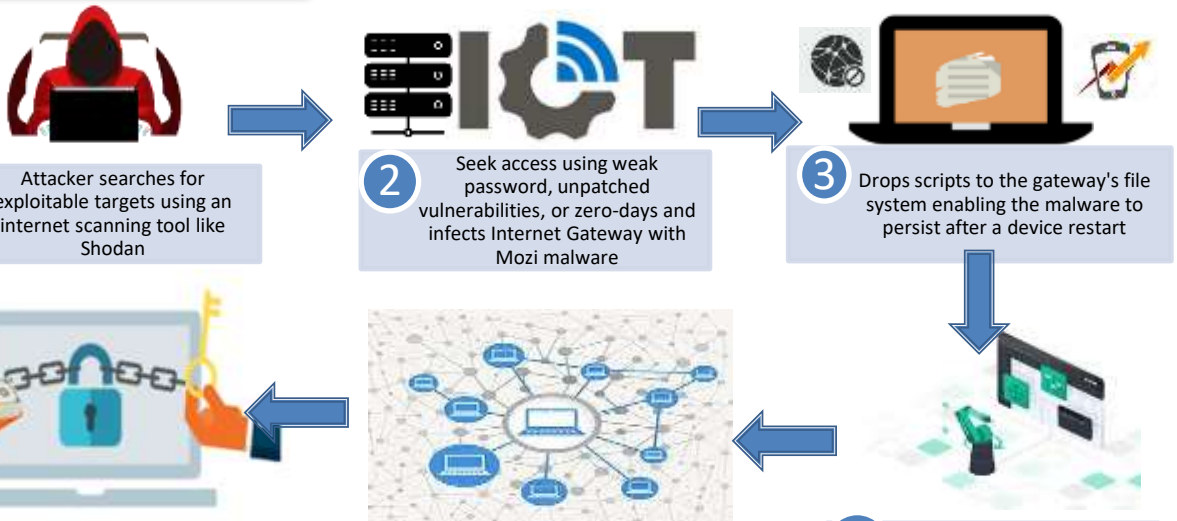
Mozi is a peer-to-peer (P2P) botnet that uses a BitTorrent-like network to infect IoT devices such as network gateways and digital video records (DVRs). It works by exploiting weak telnet passwords and nearly a dozen unpatched IoT vulnerabilities and has been used to conduct distributed denial-of service (DDoS) attacks, data exfiltration, and command or payload execution.

Mozi has evolved to achieve persistence on network gateways manufactured by Netgear, Huawei, and ZTE, using clever persistence techniques that are specifically adapted to each gateway's particular architecture.

The malware now takes specific actions to increase its chances of survival upon reboot or any other attempt by other malware or responders to interfere with its operation.

The malware blocks TCP ports (23, 2323, 7547, 35000, 50023 and 58000) and use it to gain remote access to the device. Shutting them increases the malware's chances of survival.

HOW IT WORKS



1. Attacker searches for exploitable targets using an internet scanning tool like Shodan
2. Seek access using weak password, unpatched vulnerabilities, or zero-days and infects Internet Gateway with Mozi malware
3. Drops scripts to the gateway's file system enabling the malware to persist after a device restart
4. Impedes the gateway's configuration from being altered by configuration servers
5. if the attack is discovered, it prevents remote access to the gateway to hinder remediation actions
6. HTTP requests passing through the gateway are altered and silently redirected users to exploit websites that install ransomware
7. Infected gateway scales out the attack and deploys ransomware to all user devices
8. the data on targeted devices are ransomed impacting IT endpoints and when present, Industrial/OT infrastucture

ITMS ISSD Computer Security Incident Response Team
2nd Floor ITMS Bldg Camp Crame, Quezon City
723-0401 loc 4225

www.itms.pnp.gov.ph
issd.itms@pnp.gov.ph

IMPACT

- Compromise endpoints/devices that communicates back and forth within the network.
- Performs TELNET brute force attack on exposed IoT Devices.
- Exploits hardcoded passwords in IoT devices.
- Capable of targeting the hardware which may lead to hardware-damage.
- Disrupts internet connectivity, affects device performance and possibly wipe files on the compromised IoT Devices.
- Blocks SSH and TELNET protocols to prevent future access to the infected IoT Device.

MITIGATIONS

- Changing the device default remote access passphrases.
- Updating devices to the supported latest firmware and software version.
- Segmenting IoT devices from the rest of your internal network.
- Making IoT devices not accessible from public use on the Internet.
- Ensure all passwords used on the device are created using strong password best practices;
- Ensure devices are patched and up-to-date
- Regularly update IoT devices firmware and software version.
- Regularly change IoT devices passphrase for remote access.
- Segment IoT devices from internal network.
- Do not put access IoT devices on public network which can be used publicly.

REFERENCES

- https://portswigger.net/daily-swig/mozi-malware-modified-to-present-a-more-potent-threat-to-industrial-control-systems
- https://www.elastic.co/blog/collecting-and-operationalizing-threat-data-from-the-mozi-botnet
- https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/