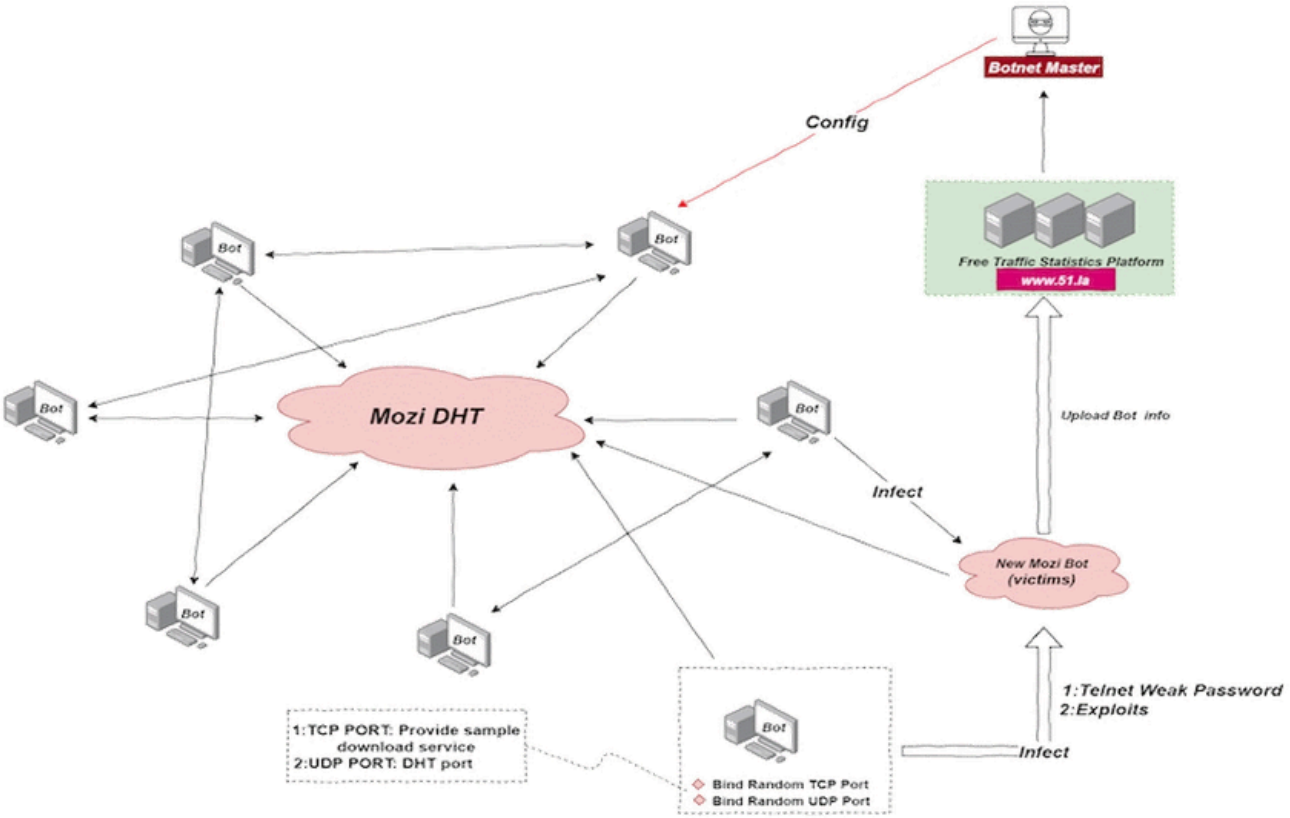
Raport consolidat eveniment cibernetic

MOZI BOTNET

Mozi botnet a fost observat folosind CMDi pentru a obține accesul inițial la un dispozitiv vulnerabil folosind comanda shell "wget", apoi schimbând permisiunile pentru a permite actorului de amenințare să interacționeze cu sistemul. Mozi ar putea compromite un dispozitiv Linux încorporat cu un serviciu Telnet expus. Acesta vizează în principal routerele și DVR-urile care sunt fie neactualizate, fie configurate în mod lax sau a căror credențiale Telnet sunt cu parole slabe/implicite.

La executare, botnetul **Mozi** încearcă să se lege la portul local UDP 14737. Eșantionul citește /**proc/net/tcp** sau /**proc/net/raw** pentru a găsi și a închide procesele care folosesc **porturile 1536 și 5888.** De asemenea, verifică dacă există fișierul **/usr/bin/python.** Dacă acesta există, eșantionul își schimbă numele de proces în **"sshd".** În caz contrar, își schimbă numele în **"dropbear**



Informații sumare

TIP	BOTNET
MD5	• eda730498b3d0a97066807a2d98909f3 • 849b165f28ae8b1cebe0c7430f44aff3 • b9e122860983d035a21f6984a92bfb22
File Hash	**mozi.m,** 4dde761681684d7edad4e5e1ffdb940b 5738f1bc69e78d234dd04e2fbfcfb4b86403fc9117b133cf1bb7cda67e7aef0a, 86d42d968d3d12c36722e16c78e49ffb **mozi.a,** 9a111588a7db15b796421bd13a949cd4 83441d77abb6cf328e77e372dc17c607fb9c4a261722ae80d83708ae3865053d, dd4b6f3216709e193ed9f06c37bcc3890
CVE exploatate	**CVE-2014–8361, CVE-2017–17215, CVE-2018–10561, CVE-2018–10562**
Măsuri preventive	1. Utilizatorii sunt sfătuiți să își actualizeze dispozitivele cu patch-uri atunci când acestea sunt eliberate de către producătorii OEM ai dispozitivelor. 2. În cazul în care dispozitivele sunt infectate, se recomandă resetarea firmware-ului dispozitivului sau restaurarea acestuia dintr-un backup de încredere. 3. Monitorizați sau blocați traficul UDP de la dispozitiv către nodurile de pornire BitTorrent DHT. 4. Blocați traficul TCP de ieșire cu porturile destinație 22, 23, 2323, 80, 81, 5555, 7574, 8080, 8443, 37215, 49152 și 52869, în cazul în care acestea nu sunt utilizate. 5. Evaluați în mod regulat securitatea rețelei și revizuiți politicile de securitate pentru a vă asigura protecția continuă împotriva amenințărilor.
Măsuri de tratare post incident	• **Izolarea dispozitivului infectat**: Izolați dispozitivul infectat de restul rețelei pentru a preveni răspândirea infecției. • **Scanare antivirus și anti-malware**: Rulați scanări complete folosind programe antivirus și anti-malware actualizate pentru a identifica și elimina orice fișiere malware asociate cu botnetul Mozi. • **Actualizarea firmware-ului și a software-ului**: Asigurați-vă că firmware-ul și software-ul dispozitivului sunt actualizate la cele mai recente versiuni pentru a remedia eventualele vulnerabilități care ar putea fi exploatate de către botnet. • **Resetarea la setările implicite de fabrică**: Dacă nu puteți elimina complet infecția sau nu sunteți siguri de integritatea sistemului, este recomandabil să resetați dispozitivul la setările implicite de fabrică. Asigurați-vă că faceți o copie de siguranță a datelor importante înainte de a efectua această acțiune. • **Monitorizarea traficului de rețea**: Monitorizați traficul de rețea pentru a identifica și bloca orice comunicare neobișnuită sau suspectă către adrese IP asociate cu botnetul Mozi. • **Schimbarea tuturor credențialelor**: Schimbați toate parolele și credențialele asociate cu dispozitivul infectat pentru a preveni accesul neautorizat în viitor.

Resurse externe

	https://blog.netlab.360.com/mozi-another-botnet-using-dht/
	https://www.hybrid-analysis.com/sample/4790754ccd895626c67f0d63736577d363de7e7684b624d584615d83532d1414