

# Evasion of High-End IDPS Devices in the Age of IPv6

Antonios Atlasis

*secfu.net*

*aatlasis@secfu.net*

Enno Rey

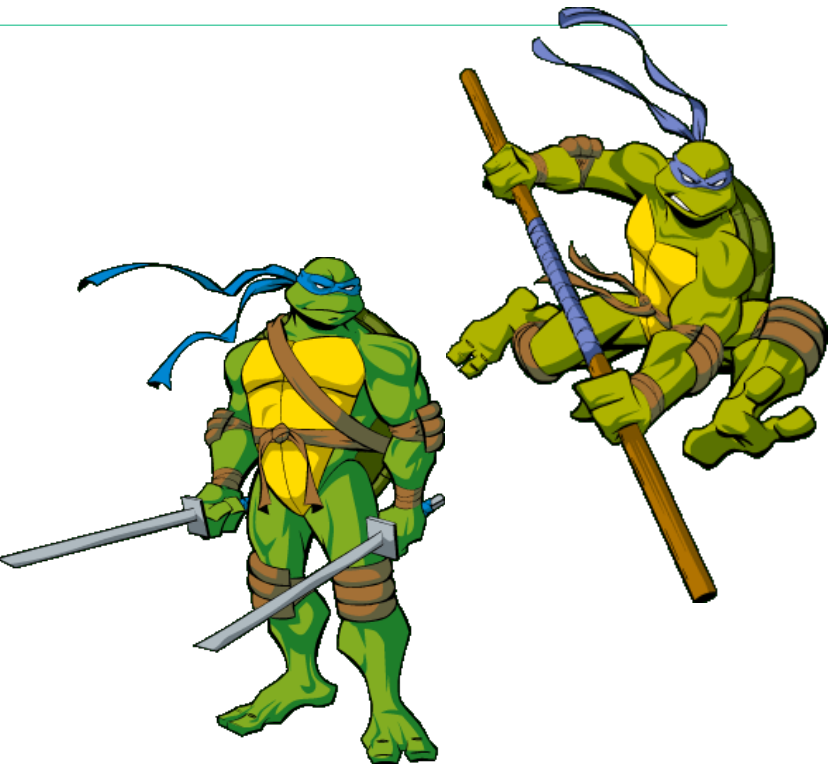
*ERNW GmbH*

*erey@ernw.de*



# Who We Are

---



- Enno Rey
  - Old school network security guy. Back in 2001 founder of ERNW & still proudly running the team.
- Antonios Atlasis
  - IT Security enthusiast.
  - Researching security issues for fun.

# Outline of the Presentation

---

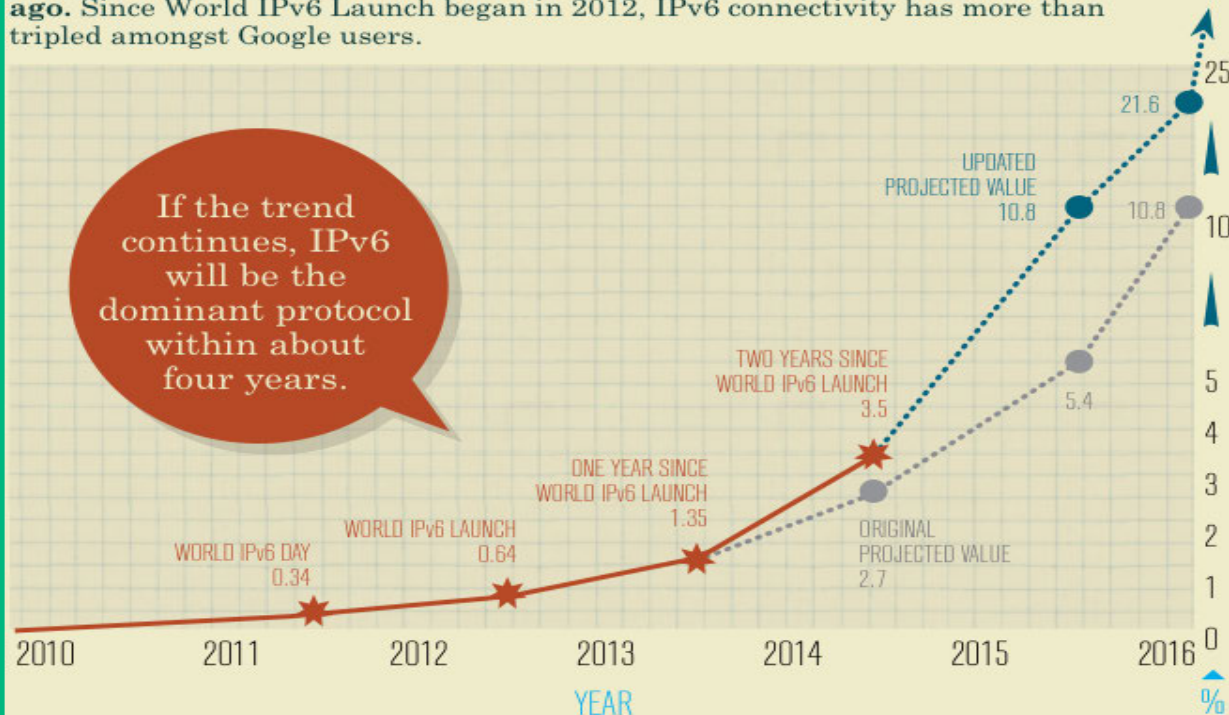
- Introduction
  - IPv6 is here
  - What IPv6 brings with it:  
The extension headers
- Problem Statement – Describe the Mess
- Overview of Test Results
  - Suricata
  - HP TippingPoint
  - (Snort/Sourcefire)
- Mitigation & Conclusions



## IPv6 MOMENTUM

IPv6 usage is increasing more rapidly than predicted just two years ago. Since World IPv6 Launch began in 2012, IPv6 connectivity has more than tripled amongst Google users.

If the trend continues, IPv6 will be the dominant protocol within about four years.



Source: <http://www.worldipv6launch.org/infographic/>

→ To make matters more urgent...

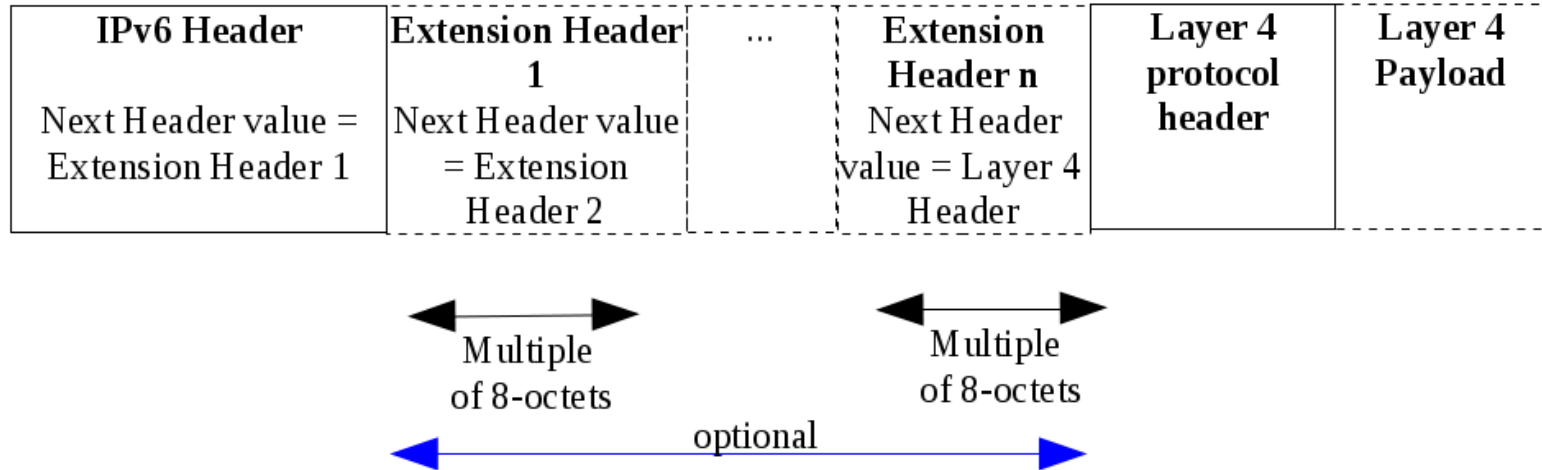


is coming.

# What an IPv6 Datagrams Looks Like...



# What an IPv6 Datagrams Looks Like...



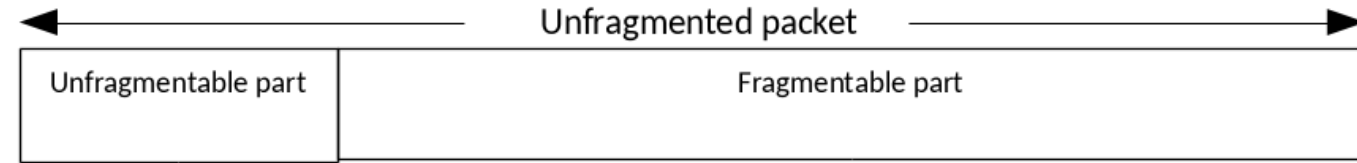
- This is the root of 3 significant problems...

# Problem 1: Too Many Things to Vary

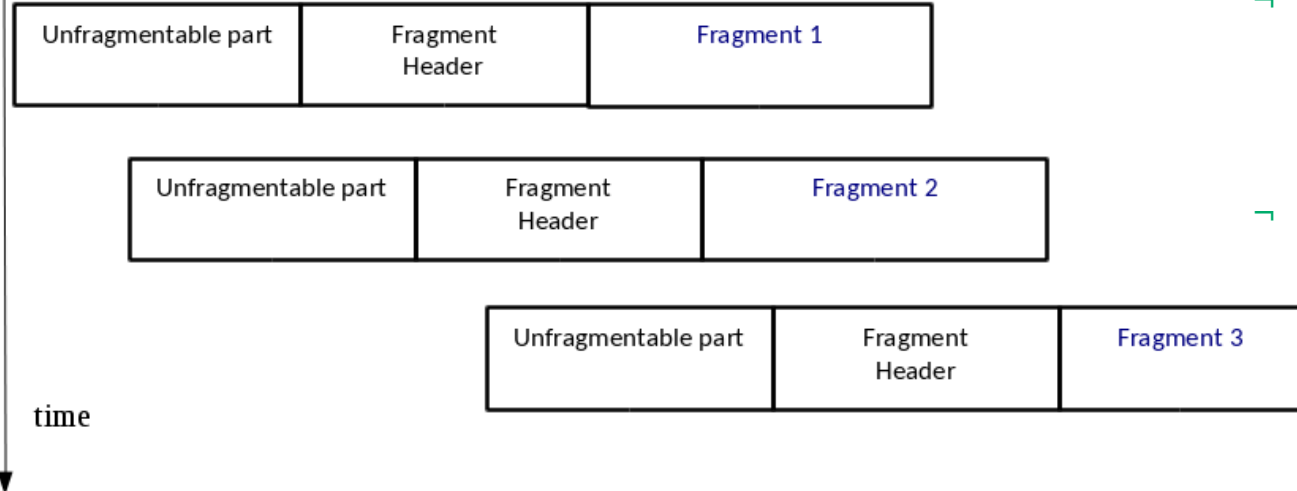
- Variable types
- Variable sizes
- Variable order
- Variable number of occurrences of each one.
- Variable fields



$IPv6 = f(v,w,x,y,z,)$



IPv6 header + some of the extension headers



## Problem 2: Fragmentation

- Both the *Fragmentable* and the *Unfragmentable* parts may contain any IPv6 Extension headers.
- Problem 1 becomes more complicated.



## Problem 3: How IPv6 Extension Headers are Chained?

|   |   |  |                                 |
|---|---|--|---------------------------------|
| <b>IPv6 header</b><br><br>Next Header<br>Value = 43 | <b>IPv6 Routing<br/>Extension header</b><br><br>Next Header<br>Value = 60 | <b>IPv6 Destination<br/>Options header</b><br><br>Next Header<br>Value = 6 | <b>TCP header + payload ...</b> |
|---|---|--|---------------------------------|

### → Next header fields:

- Contained in IPv6 headers, identify the type of header immediately following the current one.
- They use the same values as the IPv4 Protocol field.



# Why IPv6 Header Chaining is a Problem?

Fragmentable part

|  |                                 |
|--|---------------------------------|
| <b>IPv6 Destination Options header</b><br>Next Header<br>Value = 6 | <b>TCP header + payload ...</b> |
|--|---------------------------------|

Fragment 1

|   |   |  |  |
|---|---|--|--|
| <b>IPv6 header</b><br>Next Header<br>Value = 43 | <b>IPv6 Routing Extension header</b><br>Next Header<br>Value = 44 | <b>IPv6 Fragment Extension header</b><br>Next Header<br>Value = 60 | (part 1 out of 2 of the fragmentable part) |
|---|---|--|--|

Fragment 2

|   |   |  |  |
|---|---|--|--|
| <b>IPv6 header</b><br>Next Header<br>Value = 43 | <b>IPv6 Routing Extension header</b><br>Next Header<br>Value = 44 | <b>IPv6 Fragment Extension header</b><br>Next Header<br>Value = 60 | (part 2 out of 2 of the fragmentable part) |
|---|---|--|--|

## Did You Notice?



- When designing/writing IPv6 protocols & parsers they didn't pay too much attention to #LANGSEC.
- Please visit [www.langsec.org](http://www.langsec.org).

# The Mess in IPv6



- └ Vary:
  - The types of the IPv6 Extension headers
  - The order of the IPv6 Extension headers
  - The number of their occurrences.
  - Their size.
  - Their fields.
  - The Next Header values of the IPv6 Fragment Extension headers in each fragment.
  - Fragmentation (where to split the datagram)
  
- └ And combine them.

# We May Have a Fundamental Problem Here...

- There is too much flexibility and freedom...
- Which is usually inverse proportional to security :-)
- And it can potentially lead to a complete chaos...



# So, What Can Possibly Go Wrong With Them?

- Detection Signatures, e.g. used by IDPS rules, etc. are based on blacklisting traffic.
- What if we confuse their parsers by abusing IPv6 Extension headers in an unusual / unexpected way?





### 1st version of Chiron - An all-in-one IPv6 Pen Testing Framework

The first version (v0.1) of Chiron, an all-in-one IPv6 Penetration Testing Framework has been released. Still many things remain to do, but it is already useful for various IPv6 testing purposes. For instance, this was used to conduct the RISC (Researching IPv6 Security Capabilities) Project, a combined effort with the ERNW (<https://www.ernw.de/>) guys.

The main advantage of this tool is that it can be used to easily craft arbitrary IPv6 header chains combined by several IPv6 Extension headers.

The framework is actually a Scapy-wrapper, so you need Python, a patched version of Scapy (provided), which offers some bug fixes and a Fake IPv6 Extension header, and of course, Chiron.

More will follow soon. Stay tuned :-)

chiron.tar.gz

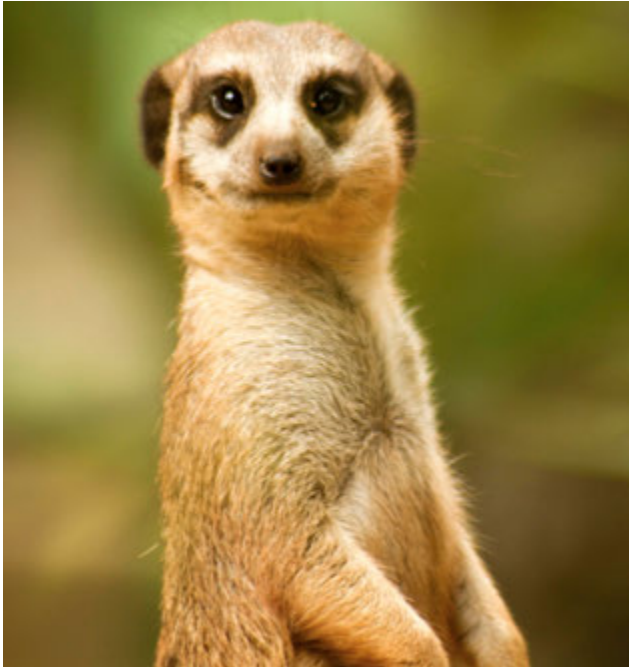
GNU Compressed Tar Archive File [3.9 MB]

[Download](#)

All this Is not just Theory

<http://www.secfu.net/tools-scripts/>

# Case 1: Evading Suricata



- Version 2.0.1, with Emerging Threats ETOpen Ruleset, 03 June, 2014
- It can be evaded when:
  - An IPv6 Destination Option header is used a part of the fragmentable piece of the IPv6 datagram.
  - The IPv6 Destinations Option header is padded with six (6) octets of bytes (at least).
  - The IPv6 datagram is fragmented in at least 7 fragments, which are sent mis-ordered.



# Suricata Developers Reacted really Fast



**June 25, 2014**

by [inliniac](#)

in [news](#), [release](#)

2 Comments

## Suricata 2.0.2 Available!

The OISF development team is proud to announce Suricata 2.0.2. This release fixes a number of issues in the 2.0 series.

### Download

Get the new release here:



<http://www.openinfosecfoundation.org/download/suricata-2.0.2.tar.gz>

### Notable changes

- IP defrag issue leading to evasion. Bug discovered by Antonios Alias working with ERNW GmbH

Unfortunately, there's More to Come (Suricata)

**ANOTHER DEMO**



# Evading TippingPoint, “The Old Way” (Mar 2014)

|   |                          |
|---|--------------------------|
| <b>IPv6 Destination Options header</b><br>Next Header Value = 6 | TCP header + payload ... |
|---|--------------------------|

|  |   |  |
|--|---|--|
| <b>IPv6 header</b><br>Next Header Value = 43 | <b>IPv6 Fragment Extension header</b><br>Next Header Value = 60 | (part 1 out of 2 of the fragmentable part) |
|--|---|--|



|  |  |  |
|--|--|--|
| <b>IPv6 header</b><br>Next Header Value = 43 | <b>IPv6 Fragment Extension header</b><br>Next Header Value = 6 | (part 2 out of 2 of the fragmentable part) |
|--|--|--|

## That One Was Patched...

But Again We Have a New One ;-)



|                        |            |
|------------------------|------------|
| <b>Model Number</b>    | 110        |
| <b>Serial Number</b>   | U110C-50F  |
| <b>TOS Version</b>     | 3.6.2.4109 |
| <b>Digital Vaccine</b> | 3.2.0.8565 |

- For demo configured to:
  - Operate inline at Layer 2.
  - Block any HTTP traffic.
  - Additional XSS rules (to test attacks at the payload too).

## Evading TP After Patching



- Currently this is a 0-day.
- Vendor has built a patch, which is currently under testing, but not yet released publicly.

# Mitigations



- RFCs should strictly define the exact legitimate usage.
  - “Loose” specifications result in ambiguities and so they introduce potential attack vectors.
  - Functionality and flexibility are definitely good things, but security is non-negotiable.
  
- Vendors should definitely make fully-compliant products and test them thoroughly before claiming IPv6-readiness.
  
- For the time being: Configure your devices to drop IPv6 Extension headers not used in your environment.

# The Most Important Take Away



- These are just some of the IPv6 “grey areas”. Other may also exist.
  - Hint: MLD comes to mind...
- IPv6 Security awareness.
  - Meet the protocol, play with it, test it in your lab and in your environment, study thoroughly potential configurations and finally, use it.
  - You will have to do it, sooner or later. The earlier you will be familiarised with it, the better.

There's never enough time...

**THANK YOU...**



**...for yours!**

Tool & Slides:

<https://www.insinuator.net>

<http://www.secfu.net/tools-scripts/>


(..soon)




## Questions?

---

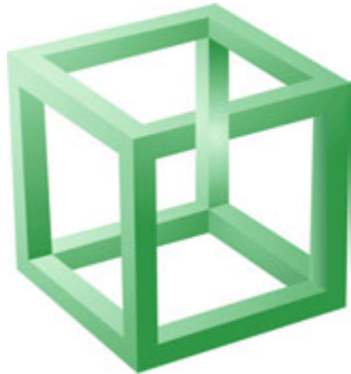


- You can reach us at: 
  - [aatlasis@secfu.net](mailto:aatlasis@secfu.net), [www.secfu.net](http://www.secfu.net)
  - [erey@ernw.de](mailto:erey@ernw.de), [www.insinuator.net](http://www.insinuator.net),  
[www.ernw.de](http://www.ernw.de)

- Follow us at: 
  - @AntoniosAtlasis
  - @Enno\_Insinuator

## Some Links

---



- RFC 2460
  - <https://www.ietf.org/rfc/rfc2460.txt>
- Antonios' Tools & Papers
  - <http://www.secfu.net/>
- "Why IPv6 Security is so Hard" from *IPv6 Security Summit 2014*:
  - [https://www.troopers.de/wp-content/uploads/2013/11/TROOPERS14-Why\\_IPv6\\_Security\\_is\\_so\\_hard-Structural\\_Deficits\\_of\\_IPv6\\_and\\_their\\_Implications-Enno\\_Rey.pdf](https://www.troopers.de/wp-content/uploads/2013/11/TROOPERS14-Why_IPv6_Security_is_so_hard-Structural_Deficits_of_IPv6_and_their_Implications-Enno_Rey.pdf)
- Enno & Antonios' blog posts on IPv6 sec
  - <http://www.insinuator.net/tag/ipv6/>

There are few things to know about TROOPERS:

March, 16-20 2015  
Heidelberg, Germany  
Make the world a safer place.



**REGISTRATION OPEN:** [www.troopers.de](http://www.troopers.de)