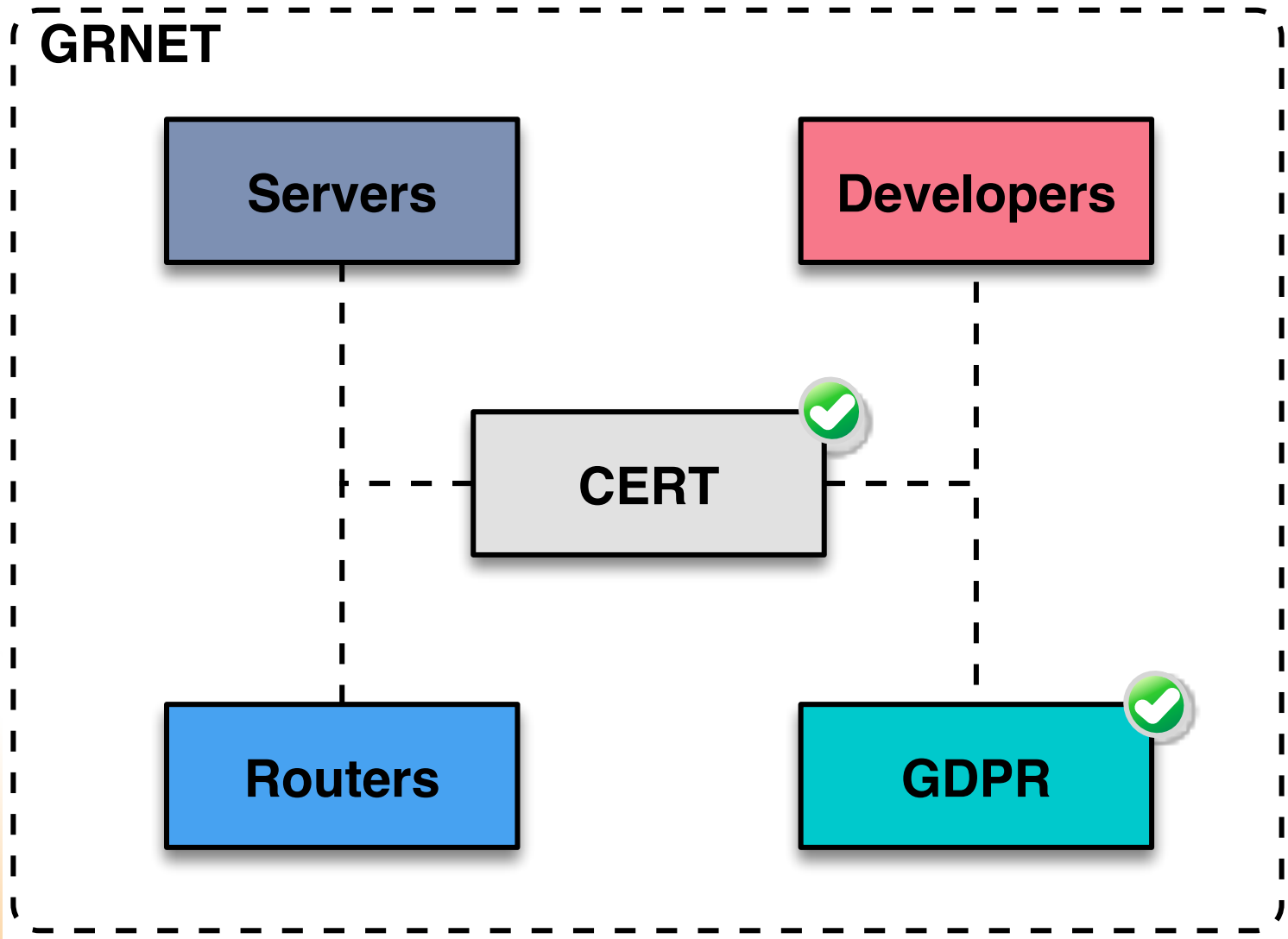
GRNET-CERT
ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΩΝ, ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ

Δημήτρης Μητρόπουλος
dimitro@grnet.gr

https://cert.grnet.gr/

Δράσεις

- **Διαχείριση** κινδύνων και απειλών σε όλο το εύρος του ΕΔΕΤ.
- **Αξιολόγηση** υποδομών, υπηρεσιών και εφαρμογών σε σχέση με την ασφάλεια.
- **Υποστήριξη** των διαφόρων ομάδων του οργανισμού.
- **Εκπαίδευση** και **Ενημέρωση** του προσωπικού.
- **Συμμετοχή** σε ερευνητικά προγράμματα, ασκήσεις κυβερνοπολέμου κ.α.
- **Συνεργασία** με ακαδημαϊκά ιδρύματα.


GRNET
Servers
Developers
CERT
Routers
GDPR

ABUSEIO

Open Source abuse management

https://abuseio.cert.grnet.gr/

Netblocks

New Netblock | CSV Export

Show 10 entries

Search:

First IP	Last IP	Contact	Action
139.91.0.0	139.91.255.255	Ίδρυμα Τεχνολογίας και Έρευνας	Show Edit Delete
143.233.0.0	143.233.255.255	ΕΚΕΦΕ-Δημόκριτος	Show Edit Delete
143.233.141.0	143.233.141.255	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών	Show Edit Delete
143.233.169.0	143.233.169.255	ΤΕΙ Πειραιά	Show Edit Delete
143.233.172.0	143.233.175.255	Okeanos Helpdesk	Show Edit Delete
143.233.176.0	143.233.176.255	ΤΕΙ Πειραιά	Show Edit Delete
143.233.182.0	143.233.183.255	Γεωπονικό Πανεπιστήμιο Αθηνών	Show Edit Delete
143.233.184.0	143.233.187.255	Γεωπονικό Πανεπιστήμιο Αθηνών	Show Edit Delete
143.233.188.0	143.233.189.255	Γεωπονικό Πανεπιστήμιο Αθηνών	Show Edit Delete

Tickets

New event | CSV Export

Show 10 entries

Search:

Ticket Id	IP	Domain	Type	Classification	Events	Notes	Status	Action
1909	195.251.201.		Escalation	Botnet infection	990	0	Open	Show
8968	147.52.1.		Escalation	Botnet infection	472	1	Open	Show
1970	195.130.120.		Escalation	Botnet infection	443	0	Open	Show
1966	195.130.95		Escalation	Botnet infection	440	0	Open	Show
1969	143.233.5.		Escalation	Botnet infection	423	0	Open	Show
1972	192.104.147.		Escalation	Botnet infection	396	0	Open	Show
9070	195.130.87		Escalation	Compromised website	251	0	Closed	Show
9589	83.212.32.		Escalation	Botnet infection	199	0	Closed	Show
1907	155.207.176.		Escalation	Botnet infection	197	1	Closed	Show
1922	195.134.64.		Escalation	Botnet infection	193	0	Closed	Show

Details for ticket: 10825

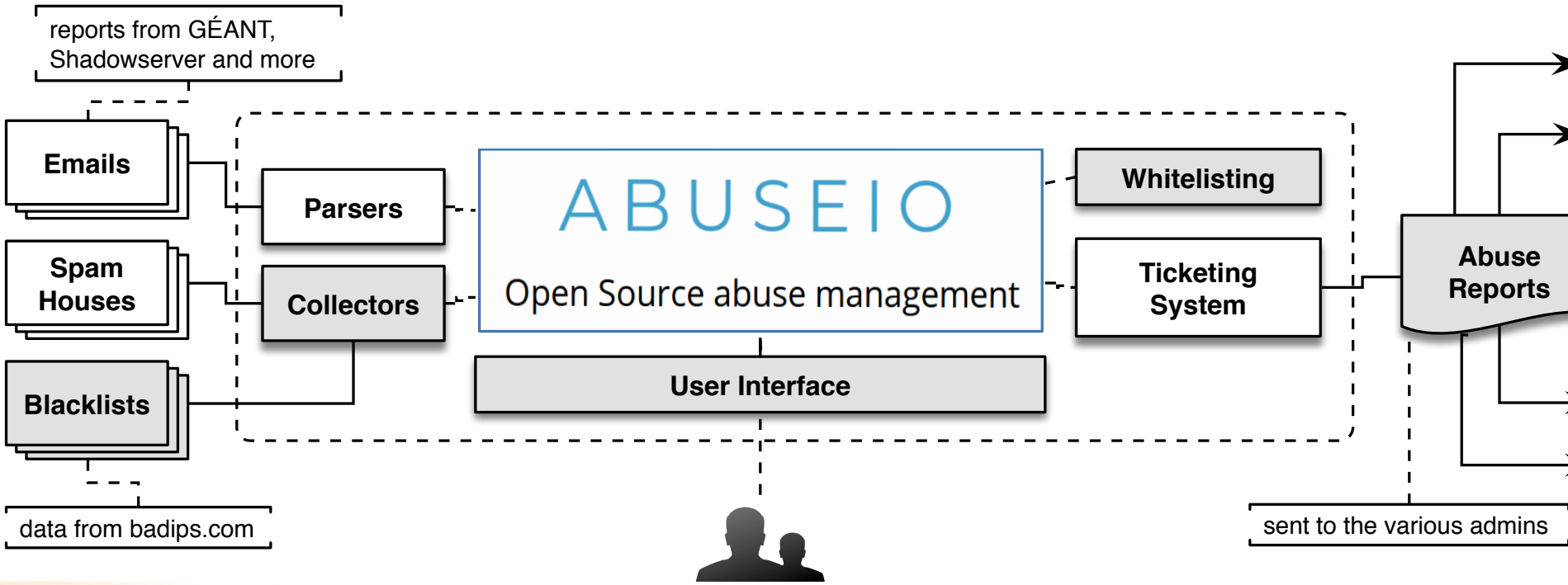
Update contact ▾ | Send notification ▾ | Ticket Status ▾

Information | Evidence | Communication

IP Address	[redacted]
Classification	Botnet infection
Type	Abuse
Action required	We require you to resolve this matter swiftly or we are required to intervene
First seen	[redacted]8-2[redacted]06:13:01 +03:00
Last seen	[redacted]0-2[redacted]05:54:17 +03:00
Events	25
Status	Open
Contact Status	Open
Ticket created	[redacted]10:20:13 +03:00
Ticket modified	[redacted]10:45:03 +03:00
Last notification	[redacted]10:45:03 +03:00 (event: 25)
IP notifications	25
Domain notifications	0
ASH link IP	http://abuseio.cert.grnet.gr/ash/collect/10825/[redacted]

IP Contact:

Reference	[redacted]
Name	[redacted]
E-Mail	[redacted]
API Host	


reports from GÉANT, Shadowserver and more
Emails
Spam Houses
Blacklists
Parsers
Collectors
ABUSEIO
Open Source abuse management
User Interface
Whitelisting
Ticketing System
Abuse Reports
data from badips.com
sent to the various admins


bad IPs

AbuseIO Αρχική Επαφές Netblocks Domains Δελτία Στατιστικά Εξαιρέσεις Ρυθμίσεις System Admin (Default)

Εξαιρέσεις

Προσθήκη Νέας

Προσθήκη

Ενημέρωση

IP Address/Subnet	
31[redacted]1[redacted]	Διαγραφή
14[redacted]7[redacted]	Διαγραφή
17[redacted]1[redacted]	Διαγραφή
19[redacted]239[redacted]	Διαγραφή

Login with **your organization credentials**

Shib Login

Login

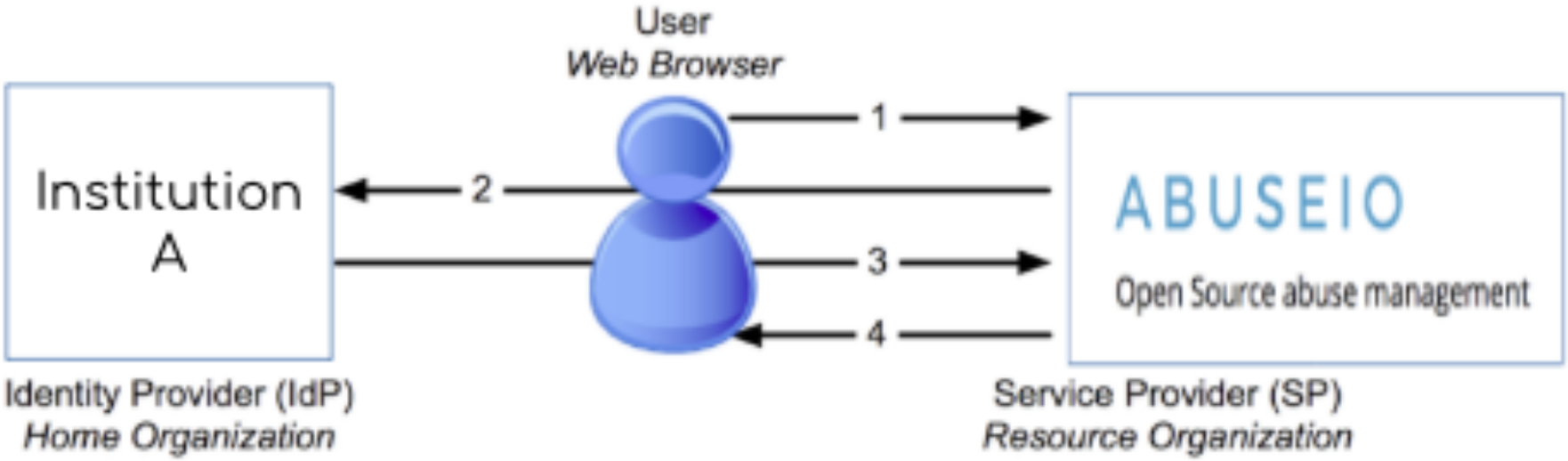
Email addres

Password

Remember me

Login

Forgot Your Password?


User
Web Browser
1
2
3
4
Institution
A
ABUSEIO
Open Source abuse management
Identity Provider (IdP)
Home Organization
Service Provider (SP)
Resource Organization


HONEY

DinoTools / **dionaea**

Watch 32 | Star 255 | Fork 81

Code | Issues 32 | Pull requests 6 | Projects 0 | Insights

Home of the dionaea honeypot https://dionaea.readthedocs.io/

honeypot dionaea security

1,671 commits | **7** branches | **11** releases | **12** contributors | GPL-2.0

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

phibos git - Merge pull request #236 from DinoTools/improve_config_parsing ... Latest commit 4159025 on Sep 13

.github	github - Add actual result section to issue template	2 years ago
ci	ci - Add Ubuntu 18.04	6 months ago
cmake	dionaea - Detect support for IPv4 mapped IPv6	5 months ago
conf	python/hpfeeds - Improve port parsing	4 months ago
doc	doc - Fix warning with missing include file	3 months ago
include	build - remove autotools config	5 months ago
modules	python - load yaml config with safe_load()	2 months ago
share/python/http/template/nginx	python/http - Add initial templates for nginx	2 years ago

DinoTools / **dionaea**

Watch 32 | Star 255 | Fork 81

Code | Issues 32 | Pull requests 6 | Projects 0 | Insights

Home of the dionaea honeypot https://dionaea.readthedocs.io/

honeypot dionaea security

1,671 commits | **7** branches | **11** releases | **12** contributors | GPL-2.0

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

phibos git - Merge pull request #236 from DinoTools/improve_config_parsing ... Latest commit 4159025 on Sep 13

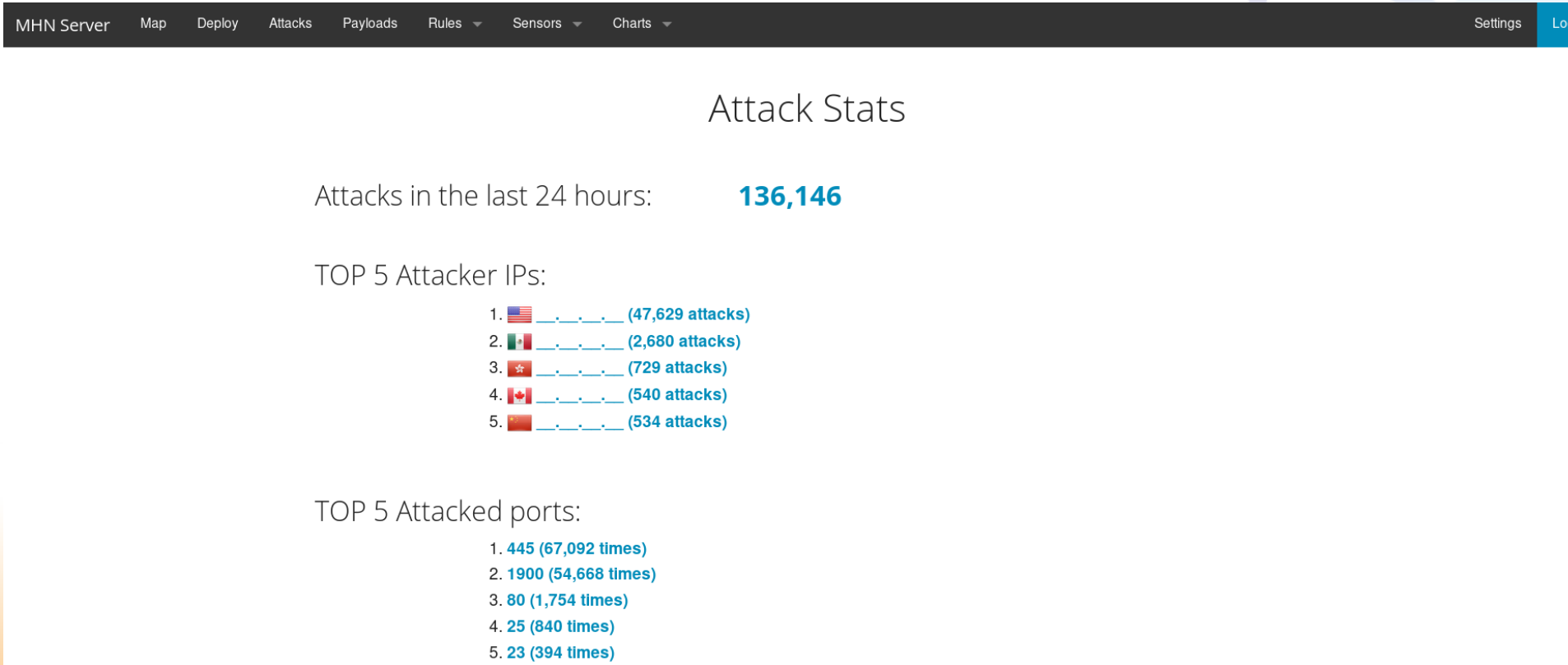
.github	github - Add actual result section to issue template	2 years ago
ci	ci - Add Ubuntu 18.04	6 months ago
cmake	dionaea - Detect support for IPv4 mapped IPv6	5 months ago
conf	python/hpfeeds - Improve port parsing	4 months ago
doc	doc - Fix warning with missing include file	3 months ago
include	build - remove autotools config	5 months ago
modules	python - load yaml config with safe_load()	2 months ago
share/python/http/template/nginx	python/http - Add initial templates for nginx	2 years ago

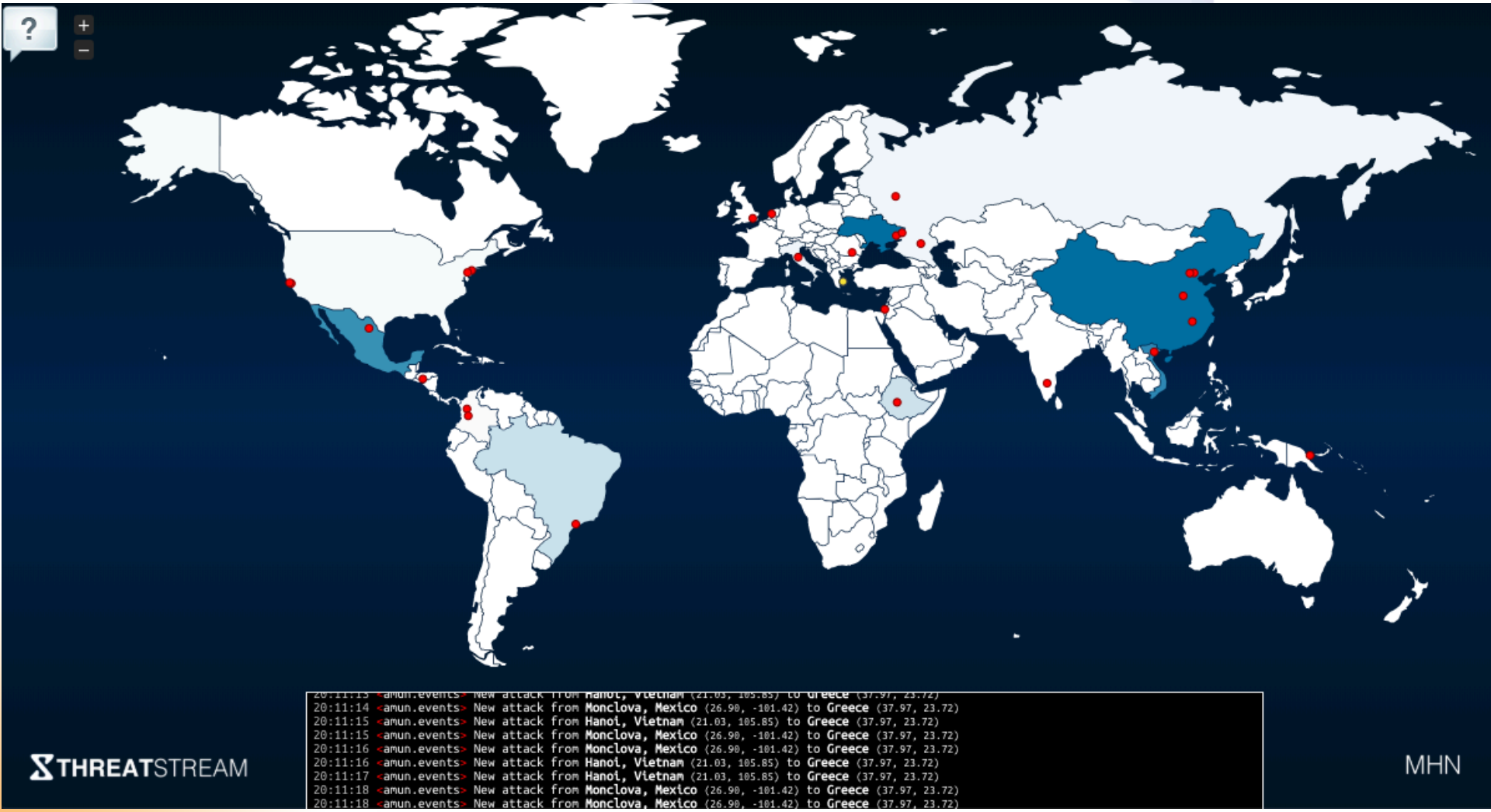
Dionaea Services / Protocols

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	filtered	smtp
42/tcp	open	nameserver
53/tcp	open	domain
80/tcp	open	http
135/tcp	open	msrpc
443/tcp	open	https
445/tcp	open	microsoft-ds
1433/tcp	open	ms-sql-s
1723/tcp	open	pptp
3306/tcp	open	mysql
5060/tcp	open	sip
5061/tcp	open	sip-tls
10000/tcp	open	snet-sensor-mgmt

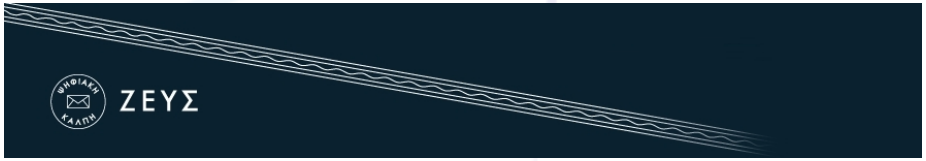
```
logsql dionaea/logsql.py:665: accepted connection from 1[redacted]8.[redacted]42[redacted]2 to 1[redacted]68.[redacted]12[redacted] (id=1048)
SMB dionaea/smb/smb.py:574: Possible DoublePulsar connection attempts..
SMB dionaea/smb/smb.py:587: DoublePulsar request opcode: 23 command: ping
SMB dionaea/smb/smb.py:574: Possible DoublePulsar connection attempts..
SMB dionaea/smb/smb.py:587: DoublePulsar request opcode: c8 command: exec
SMB dionaea/smb/smb.py:574: Possible DoublePulsar connection attempts..
SMB dionaea/smb/smb.py:587: DoublePulsar request opcode: c8 command: exec
SMB dionaea/smb/smb.py:574: Possible DoublePulsar connection attempts..
SMB dionaea/smb/smb.py:587: DoublePulsar request opcode: c8 command: exec
SMB dionaea/smb/smb.py:599: DoublePulsar payload receiving..
SMB dionaea/smb/smb.py:604: DoublePulsar payload - MD5 (before XOR decryption): 9f7d3bf2a55c2408b8b5441f4bcbfb27
SMB dionaea/smb/smb.py:606: DoublePulsar payload - MD5 (after XOR decryption ): 4ca644b546bf1efba65468bb100e6c7e
SMB dionaea/smb/smb.py:620: DoublePulsar payload - MZ header found...
SMB dionaea/smb/smb.py:626: DoublePulsar payload - MD5 final: 83941ad4f15637eeb228000ce8ad9de2. Save to disk
logsql dionaea/logsql.py:757: complete for attackid 1048
logsql dionaea/logsql.py:730: attackid 1047 is done
```

MHN (Modern Honey Network Server)




20:11:14 <amun.events> New attack from Monclova, Mexico (26.90, -101.42) to Greece (37.97, 23.72)
20:11:15 <amun.events> New attack from Hanoi, Vietnam (21.03, 105.85) to Greece (37.97, 23.72)
20:11:15 <amun.events> New attack from Monclova, Mexico (26.90, -101.42) to Greece (37.97, 23.72)
20:11:16 <amun.events> New attack from Monclova, Mexico (26.90, -101.42) to Greece (37.97, 23.72)
20:11:16 <amun.events> New attack from Hanoi, Vietnam (21.03, 105.85) to Greece (37.97, 23.72)
20:11:17 <amun.events> New attack from Hanoi, Vietnam (21.03, 105.85) to Greece (37.97, 23.72)
20:11:18 <amun.events> New attack from Monclova, Mexico (26.90, -101.42) to Greece (37.97, 23.72)
20:11:18 <amun.events> New attack from Monclova, Mexico (26.90, -101.42) to Greece (37.97, 23.72)
THREATSTREAM
MHN

Αξιολόγηση Υπηρεσιών



okeanos

MOTORCYCLE ACCIDENT CAUSE FACTORS AND IDENTIFICATION OF COUNTERMEASURES VOLUME I: TECHNICAL REPORT

H.H. Hurt, Jr.
J.V. Ouellet
D.R. Thom

Traffic Safety Center
University of Southern California
Los Angeles, California 90007

Contract No. DOT HS-5-01160
Contract Amount $501,814.00

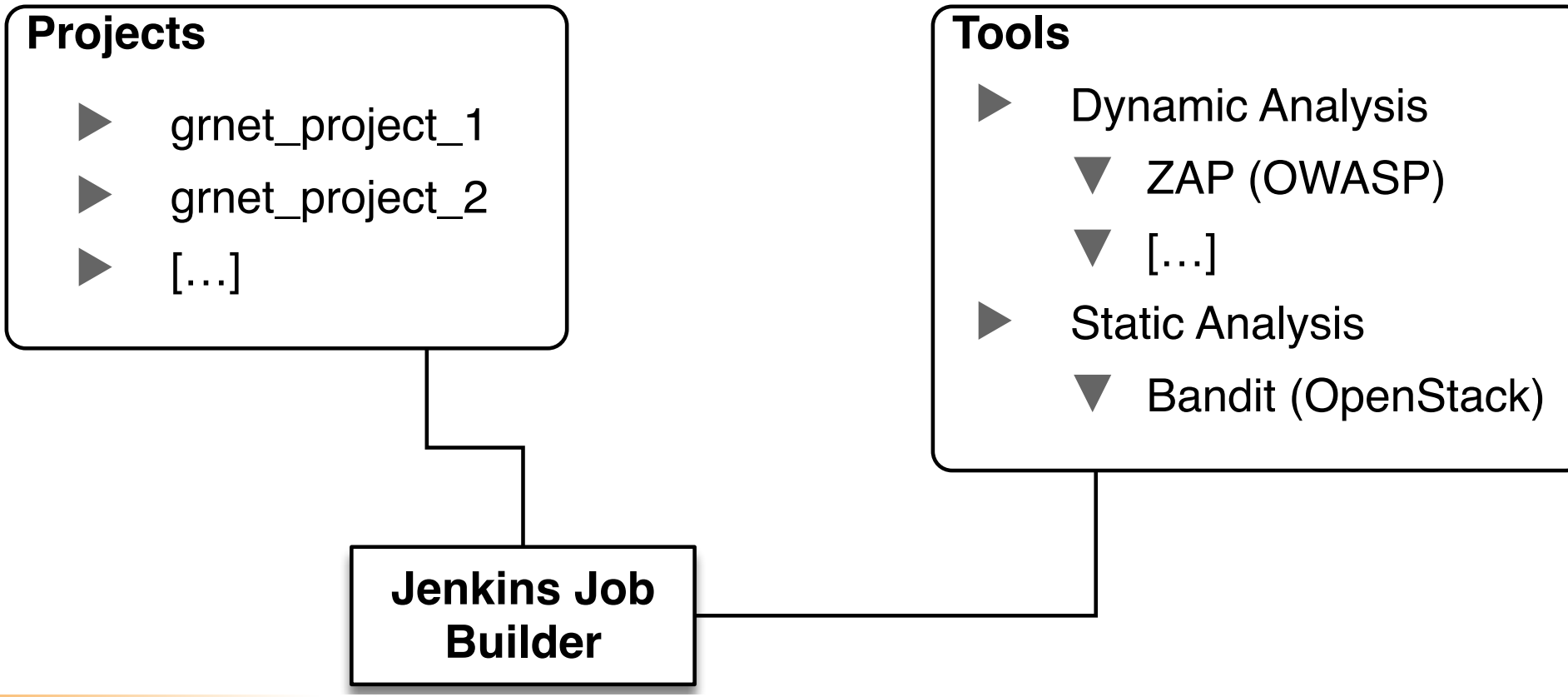
JANUARY 1981
FINAL REPORT

This document is available to the US. public through the National Technical Information Service, Springfield, Virginia 22161

Prepared For
U.S. DEPARTMENT OF TRANSPORTATION
National Highway Traffic Safety Administration
Washington, D.C. 20590

tASE

(Automated Security Assessments)



Συμμετοχή σε Ευρωπαϊκά Έργα

CERTCOOP

https://www.certcoop.eu/

Συμμετοχή σε Ασκήσεις Κυβερνοπολέμου

Συνεργασίες

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
1988 — 2018
χρόνια δημιουργίας

FORTH

ΕΘΝ·ΜΕΤΣΟΒ·ΠΟΛΥΤΕΧΝΕΙΟΝ
ΠΡΟΜΗΘΕΥΣ ΠΥΡΦΟΡΟΣ

Ευχαριστούμε!

Βιβλιογραφία

- N. Brownlee and E. Guttman. RFC 2350. June 1998. Available Online: https://www.ietf.org/rfc/rfc2350.txt
- Jan Gobel. Amun: A Python Honeypot. Technical Report. 2009. Available online: https://ub-madoc.bib.uni-mannheim.de/2595/1/amunhoneypot2.pdf
- Konstantinos Stroggylos, Dimitris Mitropoulos, Zacharias Tzermias, Panagiotis Papadopoulos, Fotios Rafailidis, Diomidis Spinellis, Sotiris Ioannidis, and Panagiotis Katsaros. TRACER: a platform for securing legacy code. *In TRUST '14: Proceedings of 7th International Conference on Trust & Trustworthy Computing - Poster Presentation Track*, 218–219. Springer, June 2014.

Πηγές Εικόνων

- https://www.prlog.org/11932740-cmc-government-supply-showcases-new-armor-tactical-gear-and-emergency-response-bags-and-backpacks.html
- https://opensource.org/
- https://abuse.io/
- https://www.badips.com/
- https://www.drupal.org/project/honeypotr
- https://www.honeynet.org/node/1353
- http://code-epicenter.com/the-biggest-software-bugs-in-the-history/