Homeland Defense & Security
Information Analysis Center

Defining the Profile of Potential Cyber Criminals

COL Thomas Hyslip, Ph.D.

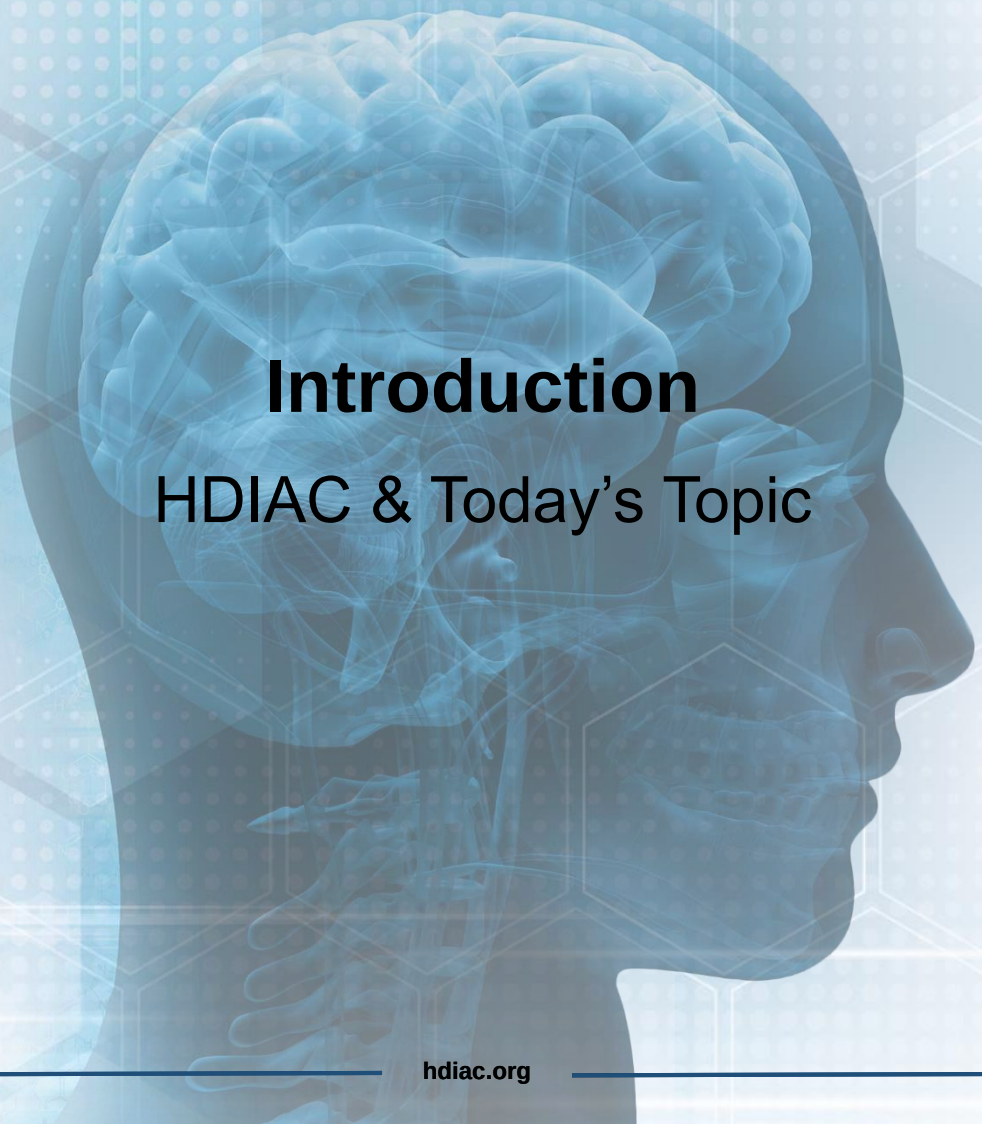
HDIAC Subject Matter Expert
Adjunct Professor, Norwich University
Resident Agent in Charge, Cyber Field Office,
Defense Criminal Investigative Service

Thomas J. Holt, Ph.D.

HDIAC Subject Matter Expert
Professor, Michigan State University

May 15, 2018

The views presented are those of the speaker and do not necessarily represent the views of DoD or its components.



Introduction

HDIAC & Today's Topic

HDIAC Overview

What is the Homeland Defense & Security Information Analysis Center (HDIAC)?

One of three Department of Defense Information Analysis Centers

Responsible for acquiring, analyzing, and disseminating relevant scientific and technical information, in each of its eight focus areas, in support of the DoD and U.S. government R&D activities

HDIAC's Mission

Our mission is to be the go-to R&D/S&T and RDT&E leader within the homeland defense and security (HDS) community, by providing timely and relevant information, superior technical solutions, and quality products to the DoD and HDS Communities of Interest/Communities of Practice.

HDIAC Overview

HDIAC Subject Matter Expert (SME) Network

HDIAC SMEs are experts in their field(s), and, typically, have been published in technical journals and publications.

SMEs are involved in a variety of HDIAC activities

- Authoring HDIAC Journal articles
- Answering HDIAC Technical Inquiries
- Engaging in active discussions in the HDIAC community
- Assisting with HDIAC Core Analysis Tasks
- Presenting webinars

If you are interested in applying to become a SME, please visit HDIAC.org or email info@hdiac.org.

Overview: Hacking (For) the Department of Defense

- **DoD's efforts in cyberdefense and cyber capabilities are growing in prominence**
  - 2000 – "full spectrum dominance" / "information" as a warfighting domain
  - 2009 – "cyberspace" as a domain
  - 2018 – NDS stresses cyberspace-related investments / U.S. Cyber Command officially elevated to Unified Combatant Command status
- **The operative word regarding this study is "potential" cyber criminals**
- **DoD—as well as private groups—are turning to crowdsourced hackers to test and identify system vulnerabilities**
  - DoD's "Hack the Pentagon" program, 2016–present
- **This study sheds critical light on both individual and group dynamics of a major hacking subculture**
- **In turn, this informs DoD & the government's efforts to both prevent cybercrime and work collaboratively with "white hat" hackers**

COL Thomas Hyslip, Ph.D.

Adjunct Professor, Norwich University

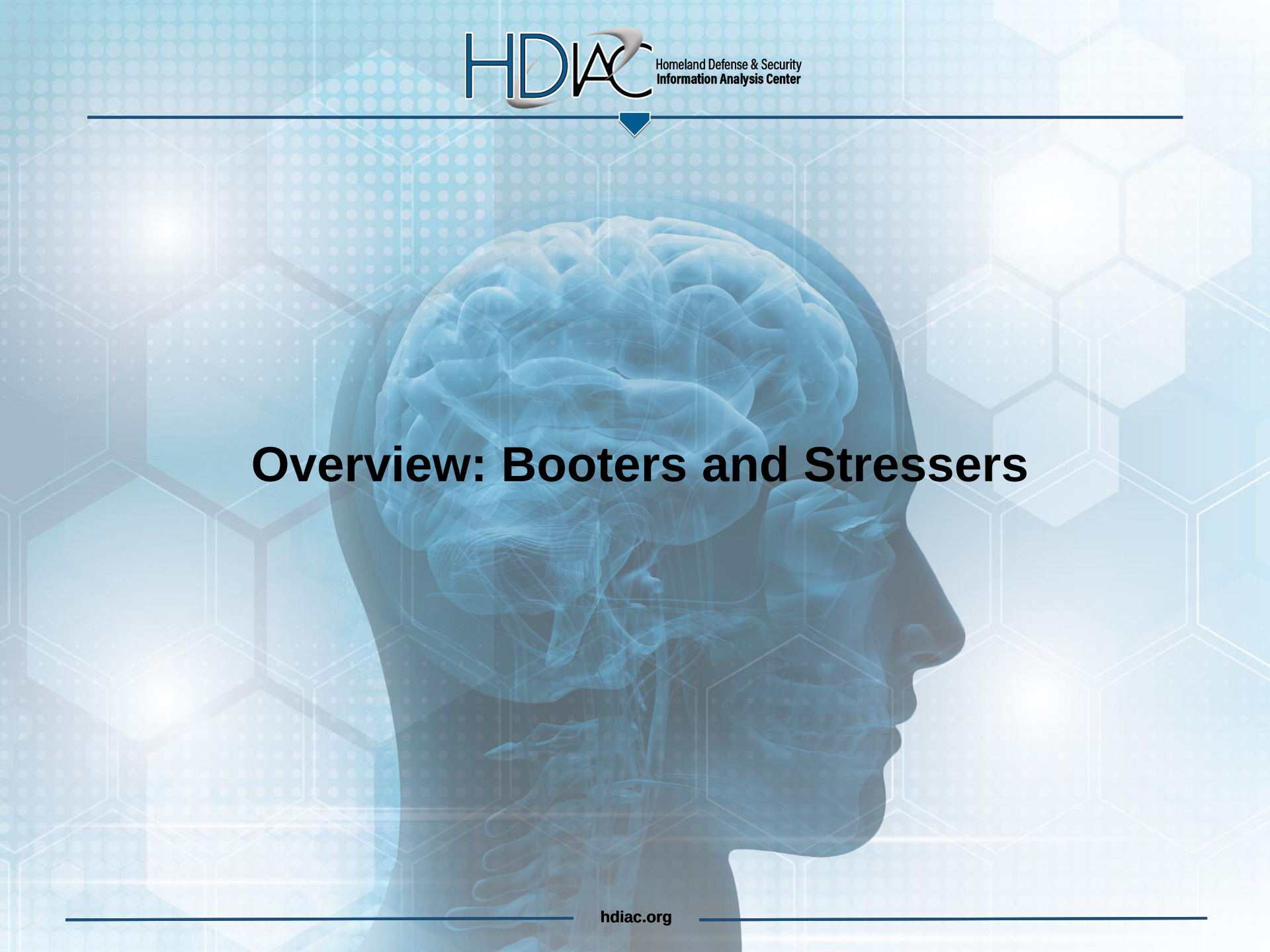
Resident Agent in Charge, Cyber Field Office, Defense Criminal Investigative Service

Thomas S. Hyslip is an adjunct professor in the College of Graduate and Continuing Studies at Norwich University specializing in cybersecurity, cybercrime, and critical infrastructure protection (Ph.D., Capitol College). Hyslip works full time as federal agent specializing in cybercrime investigations and forensics, and is also a Colonel in the U.S. Army Reserve.

Thomas J. Holt, Ph.D.

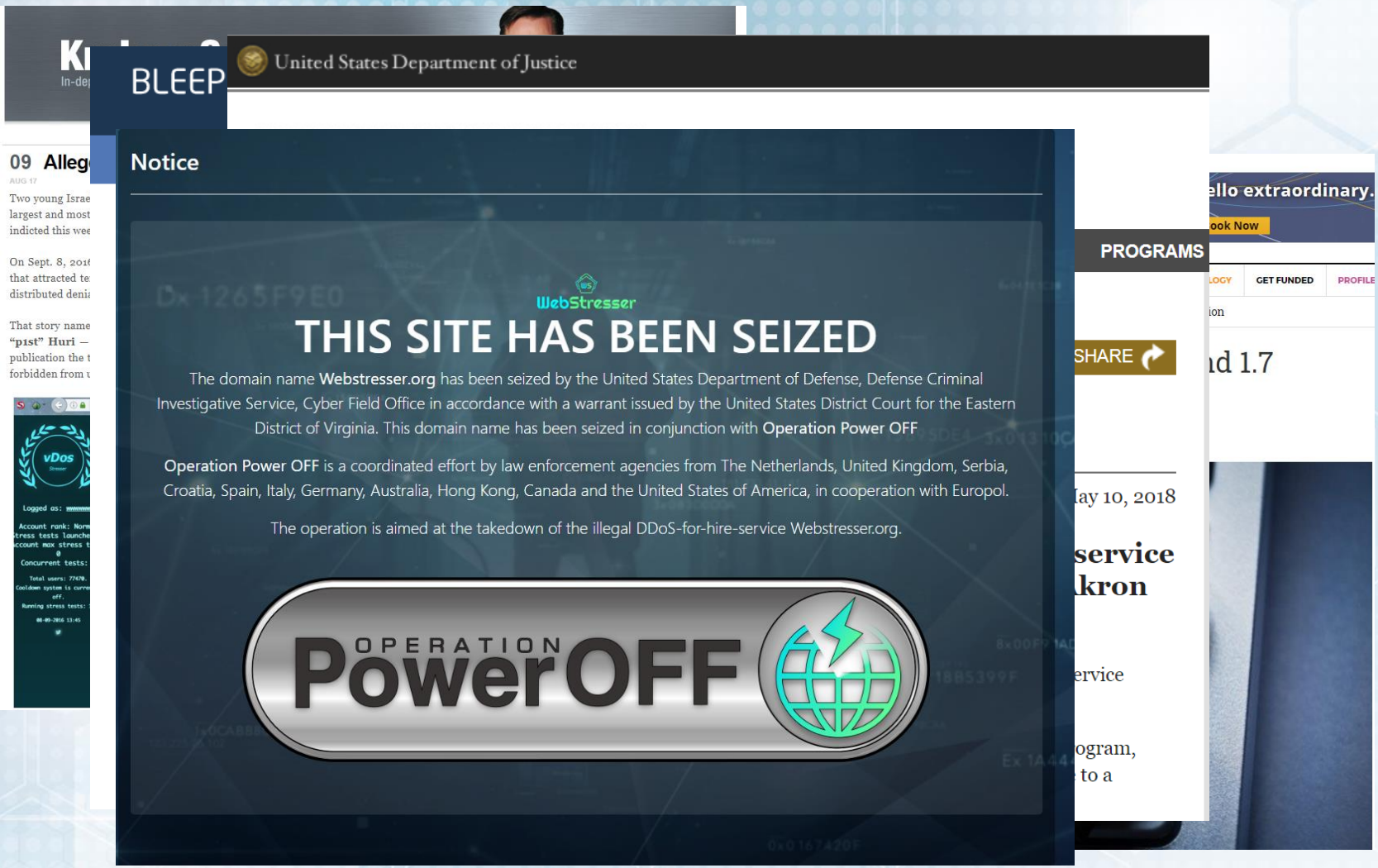
Professor, Michigan State University

Thomas J. Holt is a professor in the School of Criminal Justice at Michigan State University, specializing in cybercrime, cyberterrorism, and policy responses to these threats (Ph.D., University of Missouri-Saint Louis). His work has appeared in numerous academic journals, including *British Journal of Criminology, Crime & Delinquency, Deviant Behavior* and *Terrorism & Political Violence*. He is also the author of multiple books and has presented his work in various academic and practitioner conferences around the world.



Overview: Booters and Stressers

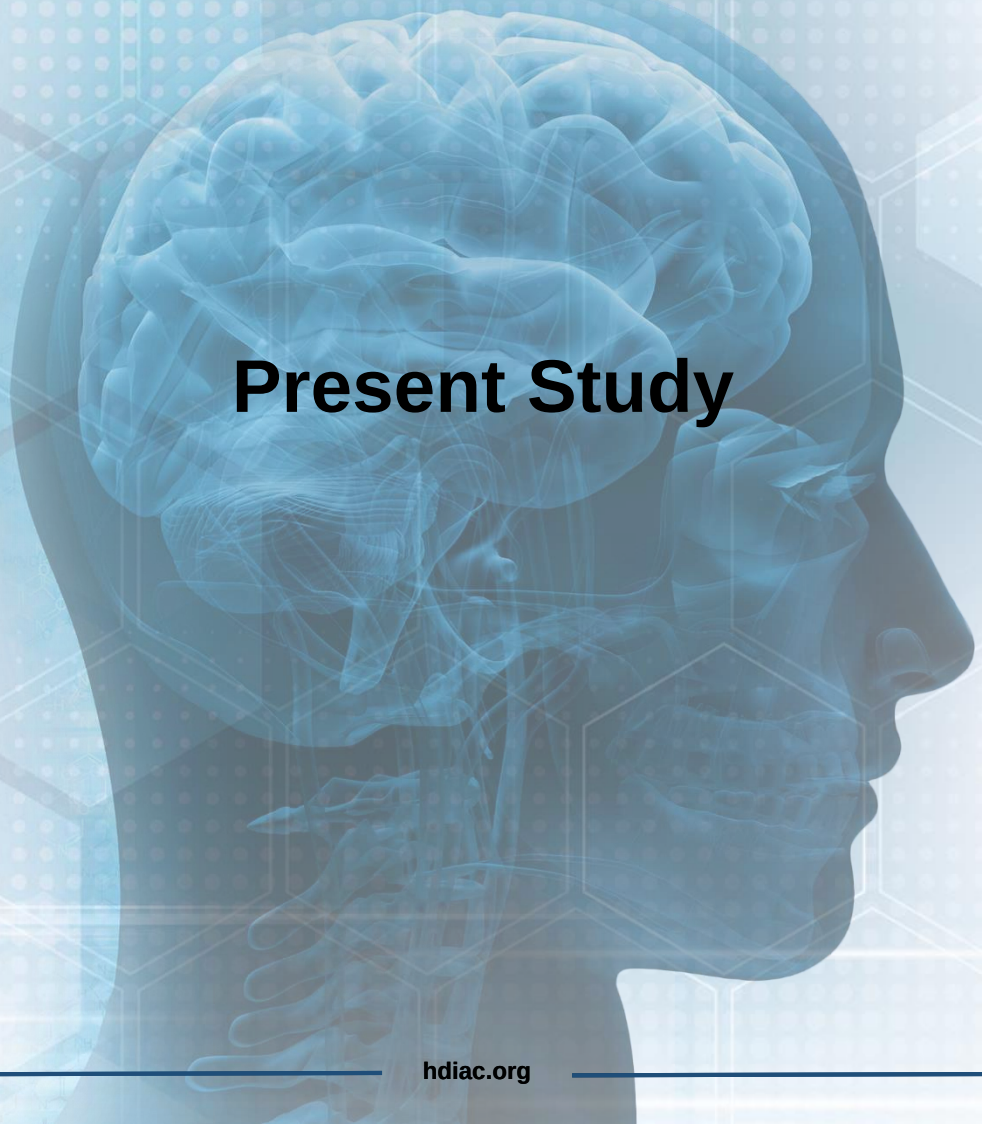

Stresser Operator Website
bitcoin
ACCEPTED HERE
PayPal
Payment
Attacker
1
2
3
4
5
6
Backend Servers
Reflection / Amplifiers
Target


BLEEP
United States Department of Justice
Notice
WebStresser
THIS SITE HAS BEEN SEIZED
The domain name Webstresser.org has been seized by the United States Department of Defense, Defense Criminal Investigative Service, Cyber Field Office in accordance with a warrant issued by the United States District Court for the Eastern District of Virginia. This domain name has been seized in conjunction with Operation Power OFF
Operation Power OFF is a coordinated effort by law enforcement agencies from The Netherlands, United Kingdom, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada and the United States of America, in cooperation with Europol.
The operation is aimed at the takedown of the illegal DDoS-for-hire-service Webstresser.org.
OPERATION
PowerOFF
PROGRAMS
SHARE
GET FUNDED
PROFILE
vDos

Booter and Stresser Services

- Hutchings & Clayton (2016) surveyed Booter operators
- Karami, Park and McCoy (2015) examined the business structure of booter and stresser services by intervening with the payment processors, such as Paypal
- Santanna, Rijswijk-Deij, Hofstede and Sperotto (2014) measured the bandwidth and packets size of booter and stresser DDoS attacks
- Rossow (2014) identified 14 protocols for amplification attacks and millions of vulnerable amplification servers.

[1]



Present Study

15 Stressers

- DDOS City
- Device Stresser
- Galaxy Booter
- Hostiles Booter
- Jays Stresser
- Legion Booter
- Lizard Stresser
- Network Stresser
- Nulled Booter
- P0wned Stresser
- Phantom Stresser
- Quantum Stresser
- Rage Booter
- Space Booter
- Unknown Stresser

[1]

Email Address Analysis

- **51,909 User Email Addresses**

  - Gmail: 18,571: 36%
  - Hotmail: 11,540: 22%
  - Yahoo: 5,273: 10%

  68%

  - Live: 1,590
  - AOL: 878
  - Outlook: 833
  - GMX: 384
  - Mail.ru: 372
  - Yandex.ru: 202

[1]

Survey of Users

- 43,891 Emails sent (Dec. 2016)
- 5,226 verified as received and viewed
- N = 821 respondents
- 84 Follow up requests

- 23 Questions
- Skill level
- Usage
- Payments
- Targets
- Attack Types
- Demographics

Hypotheses

- **Users:** Young, white males, USA
- **Accounts:** 1 or 2 stresser accounts
  - Based on email analysis
- **Targets:** Gaming competition (other users), self
- **Motivation:** Impact games, test systems

[1]

Recent Examples

- **Adam Mudd, Titanium Stresser**

Teen UK hacker pleads guilty after earning $385k from DDoS tool

Cops say net crims launched 1.7 million attacks from 15 year-old's creation.

- **Vincent Omari, Lizard Squad "Spokesman"**

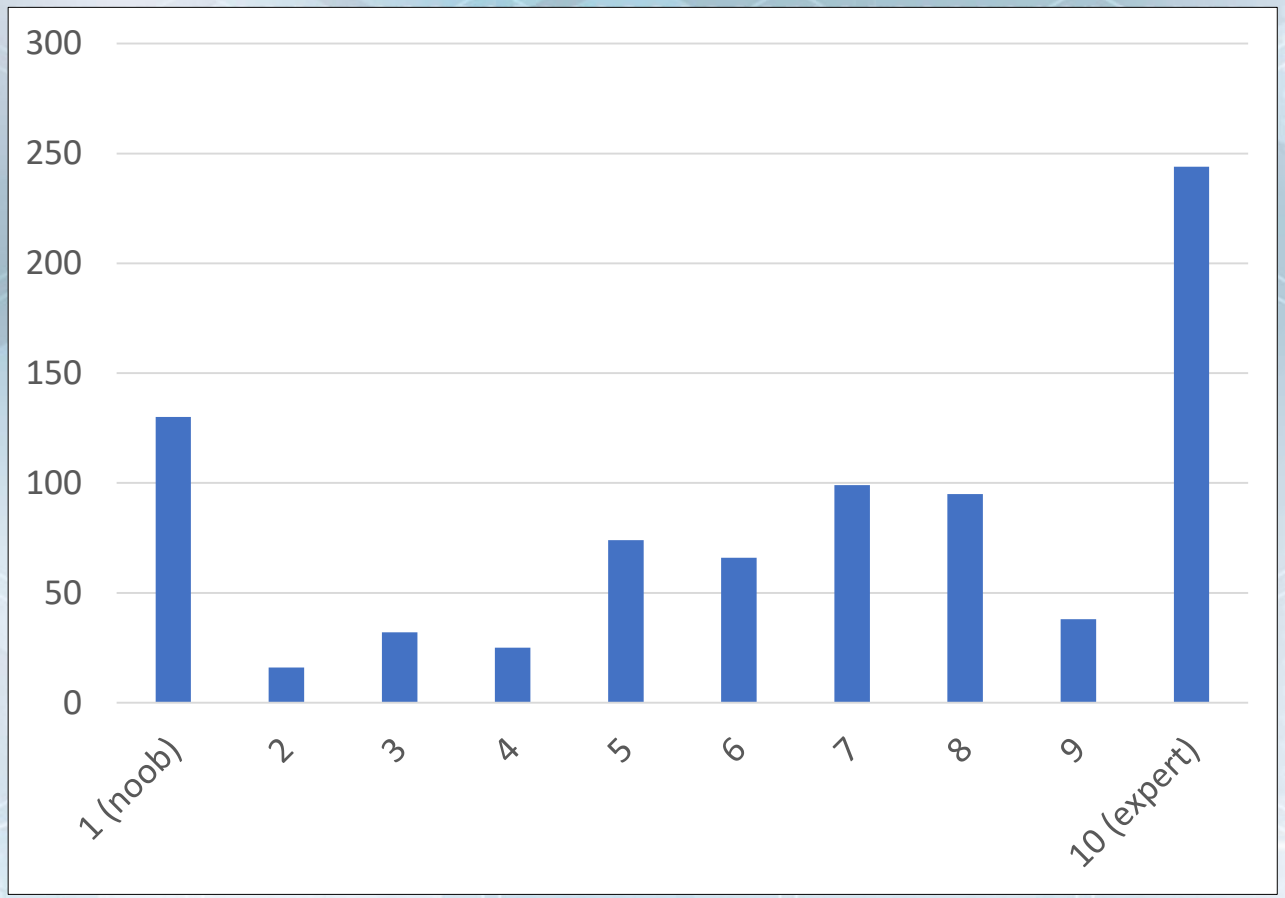
6 UK teenagers arrested for allegedly using Lizard Squad's Lizard Stresser DDoS service

If law enforcement can't hunt down and arrest Lizard Squad members, then it settles for arresting teenage Lizard Stressor customers accused of launching DDoS attacks on Microsoft, Amazon, Sony, and others.

[1]

Survey Results

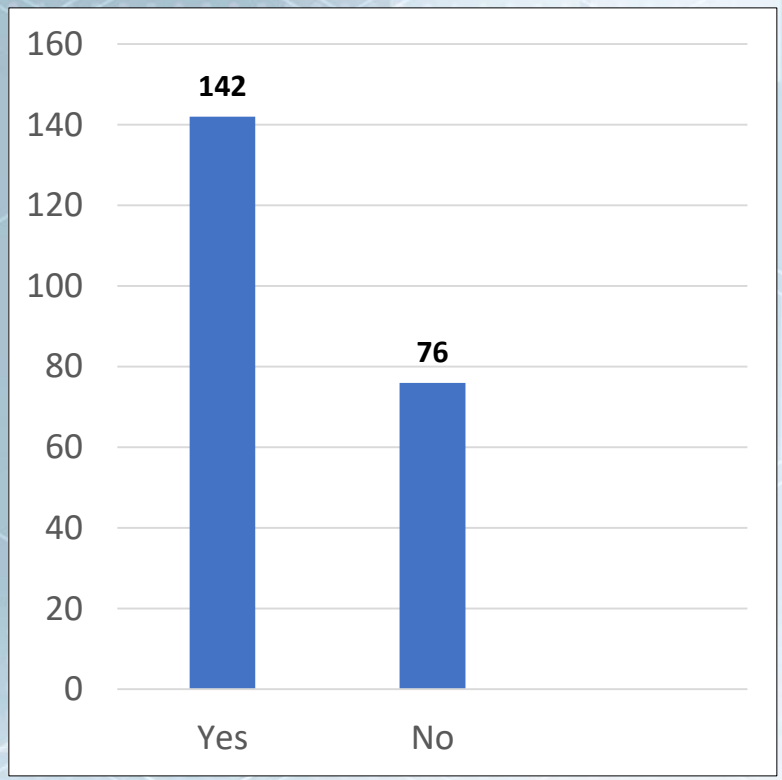
What is your knowledge and skill level with stresser/booter tools and services?



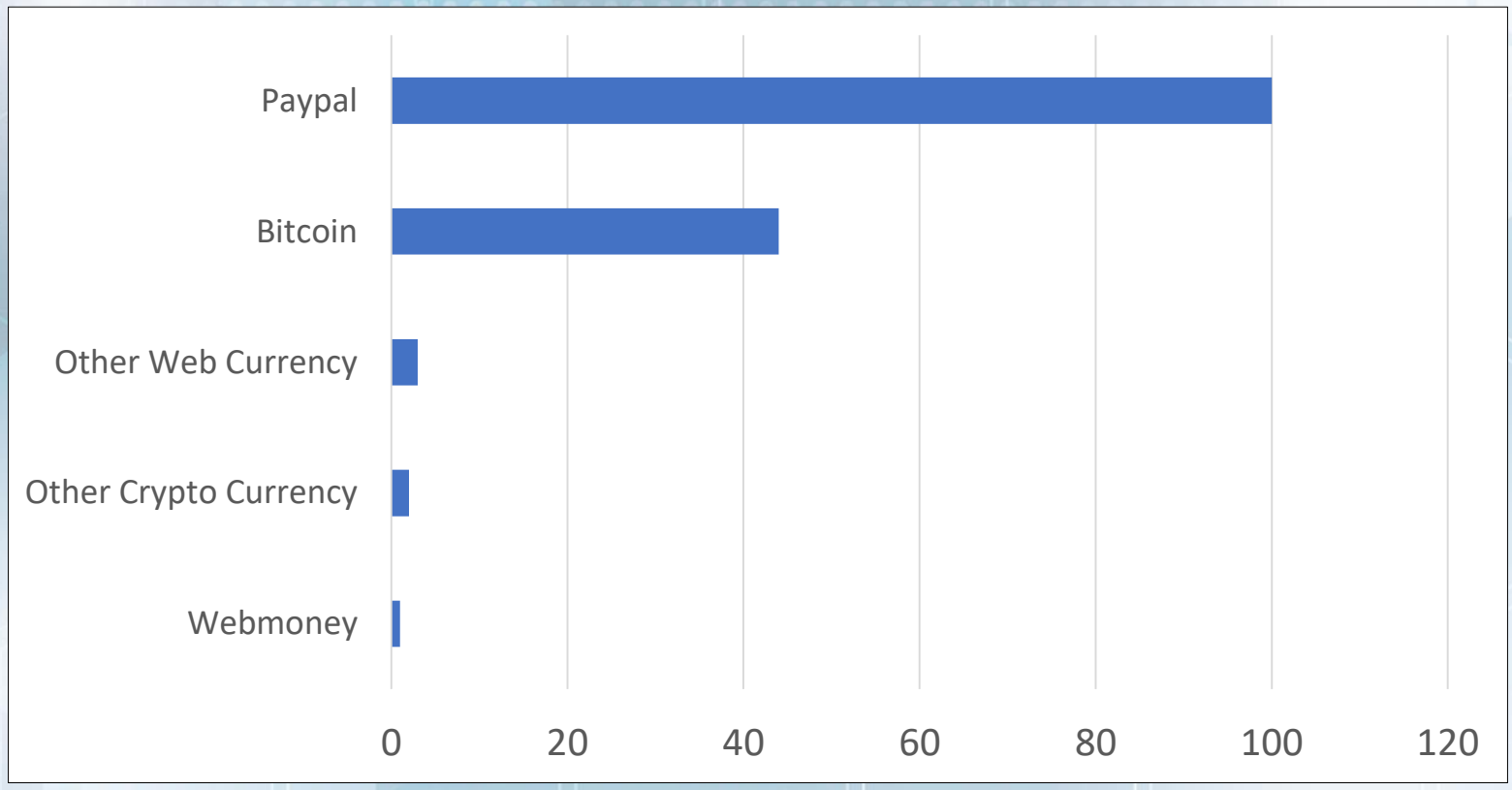
30% Experts
16% Noob

Have you ever used a booter or stresser?

Did you pay a fee to use the booter or stresser?

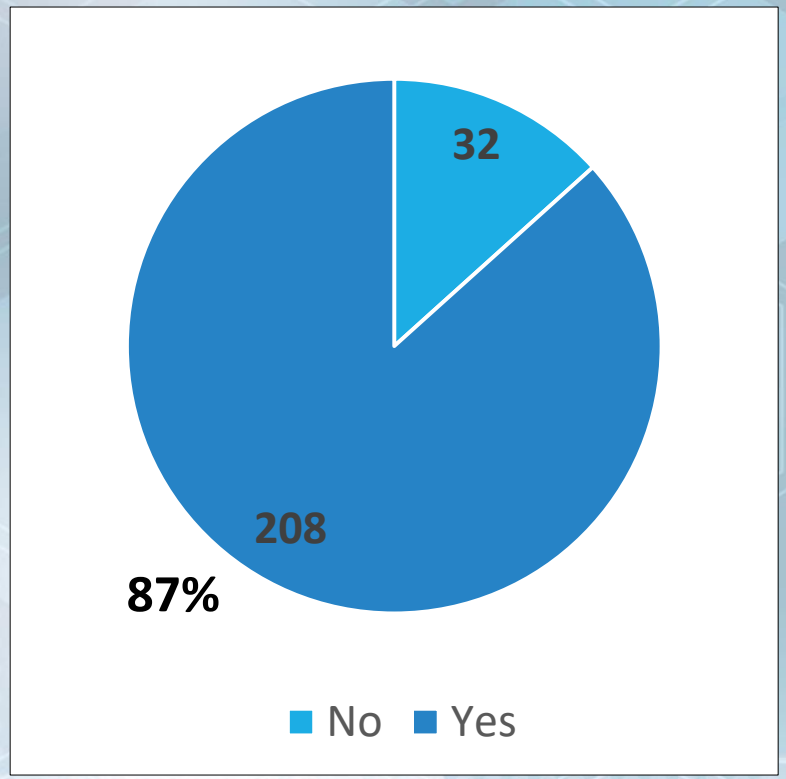


How did you pay for the stresser?

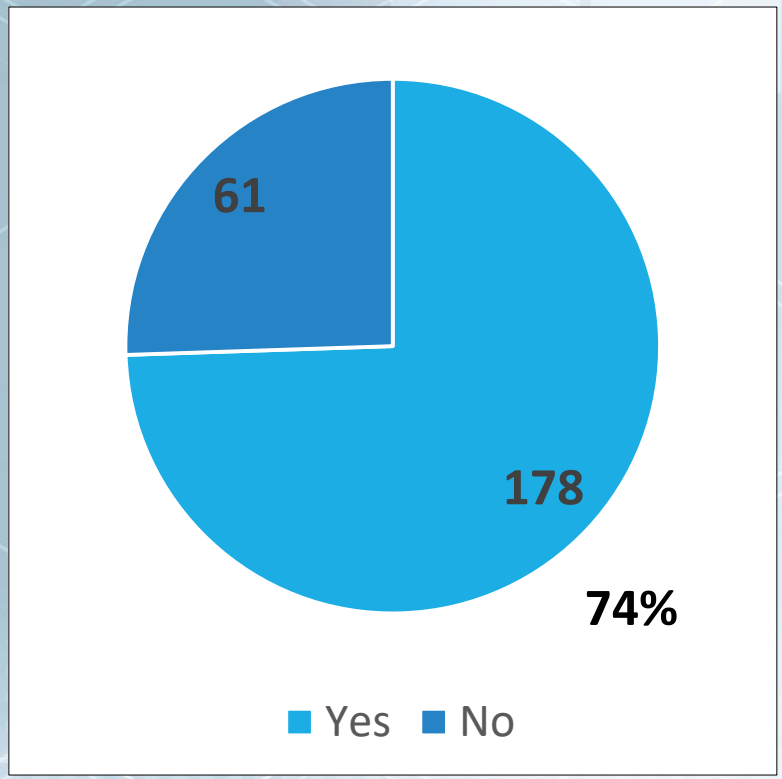


[1]

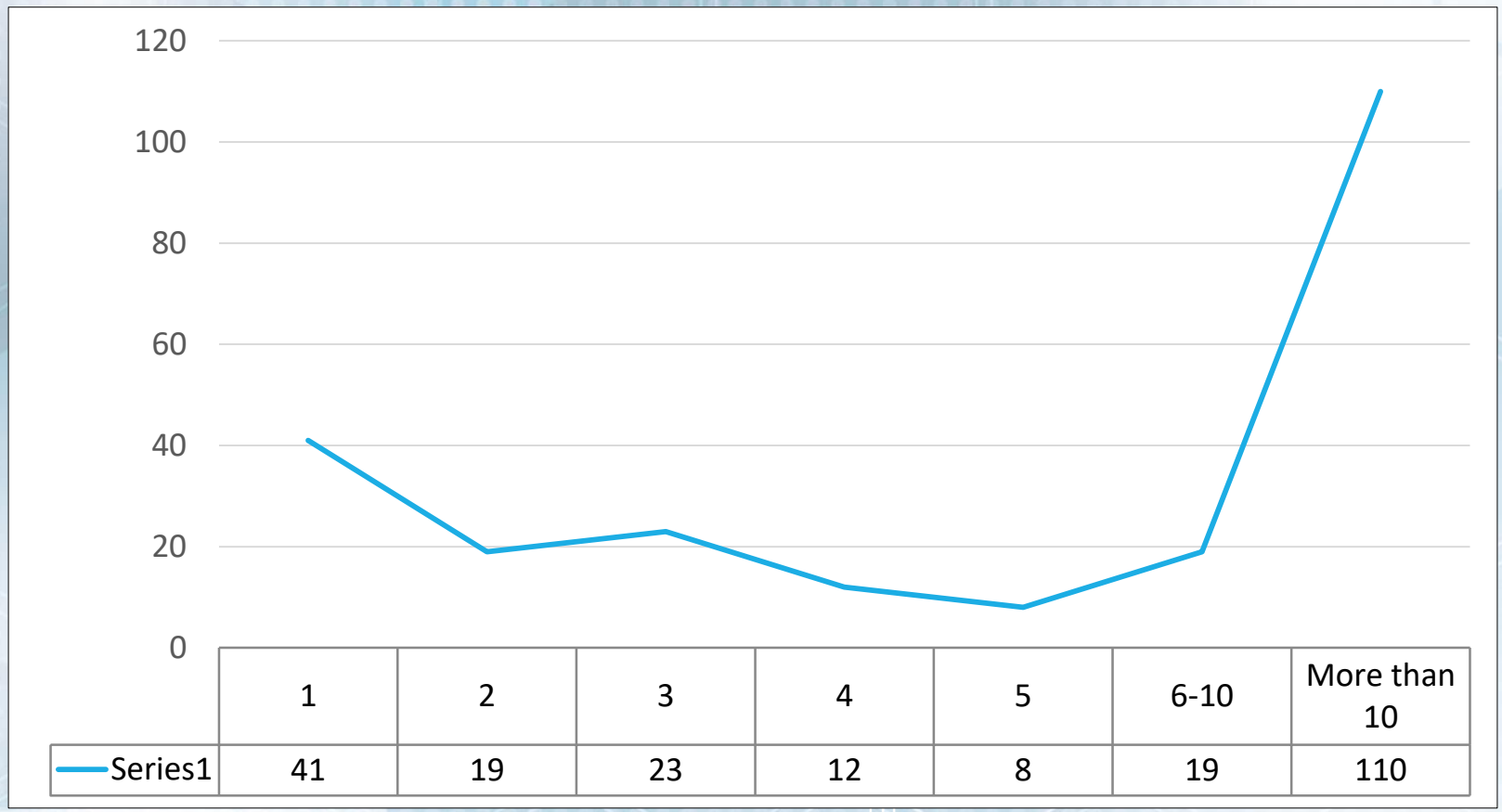
Were you able to use the stresser or booter to test systems?



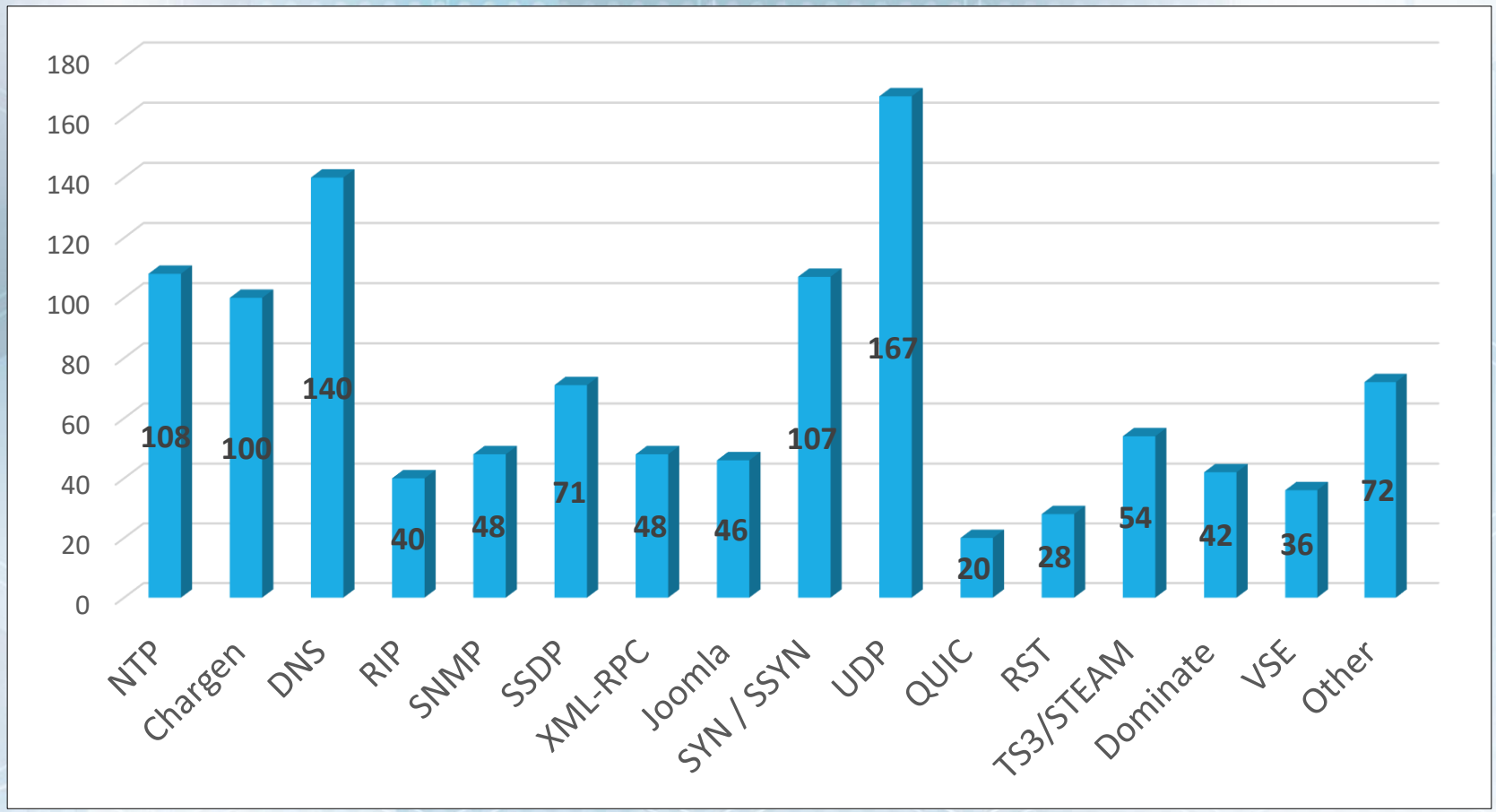
Did the booter or stresser work as advertised?



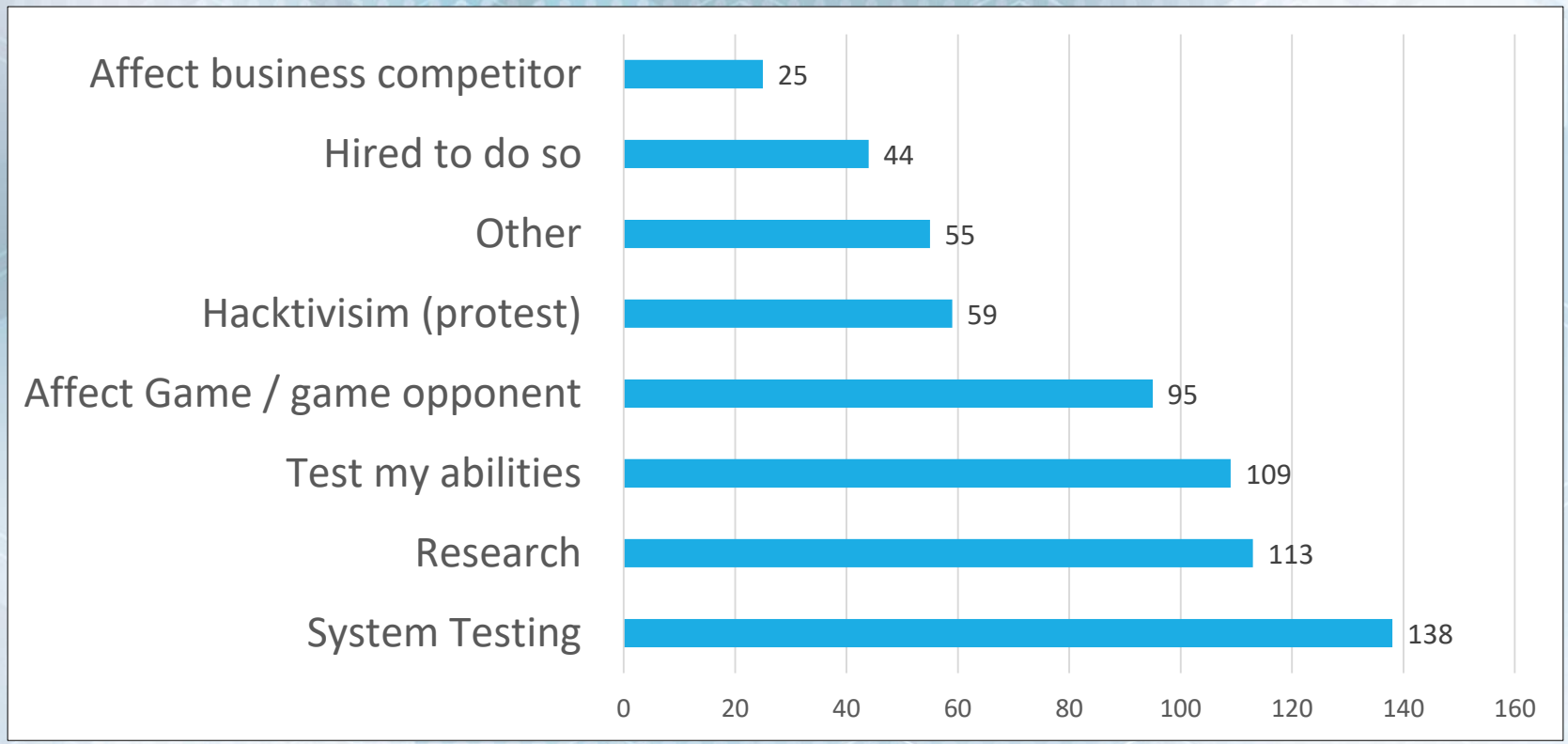
How many systems/servers did you test?



Type of Attack Utilized

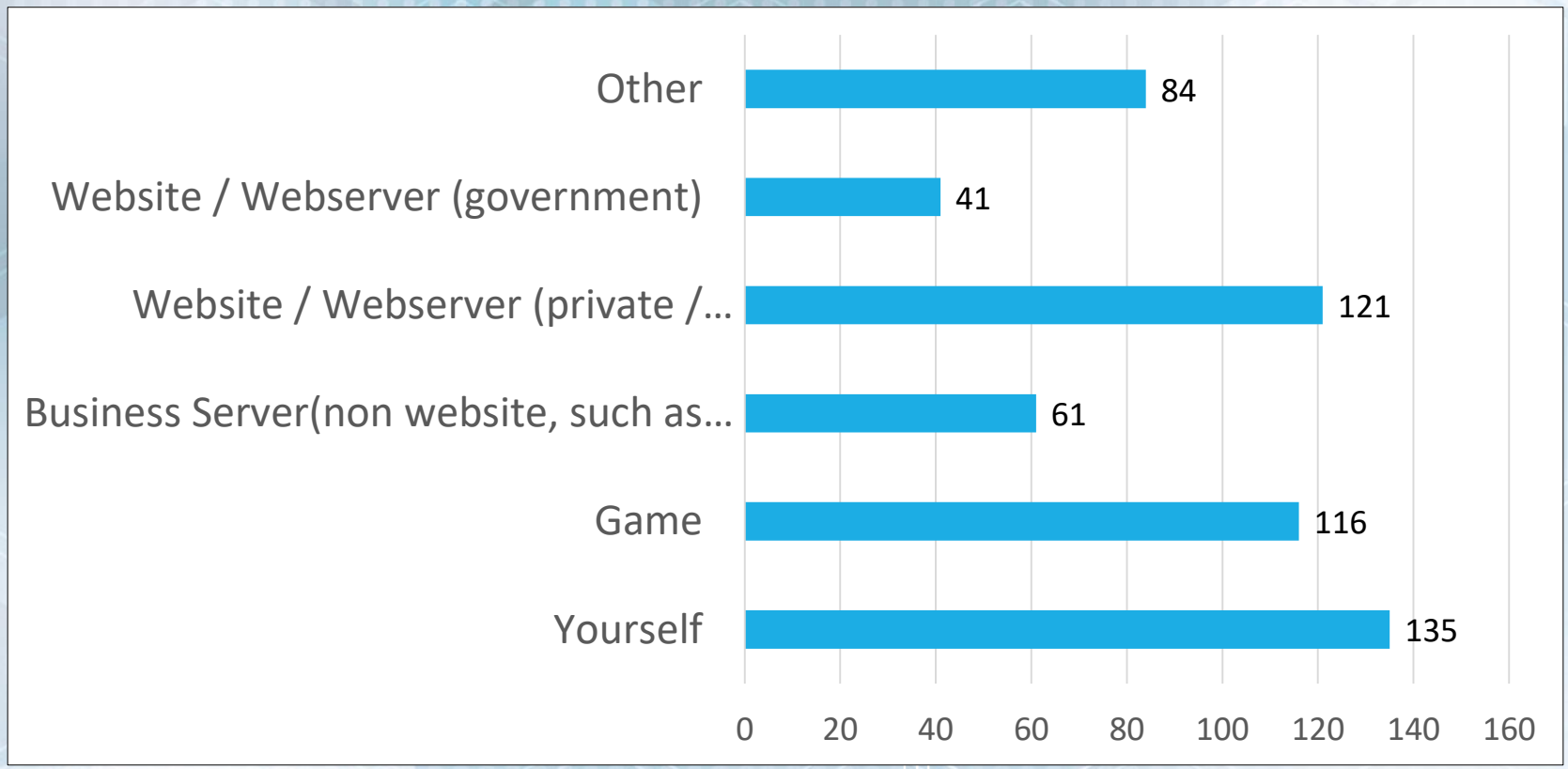


What was the motivation behind your use of the booter/stresser?

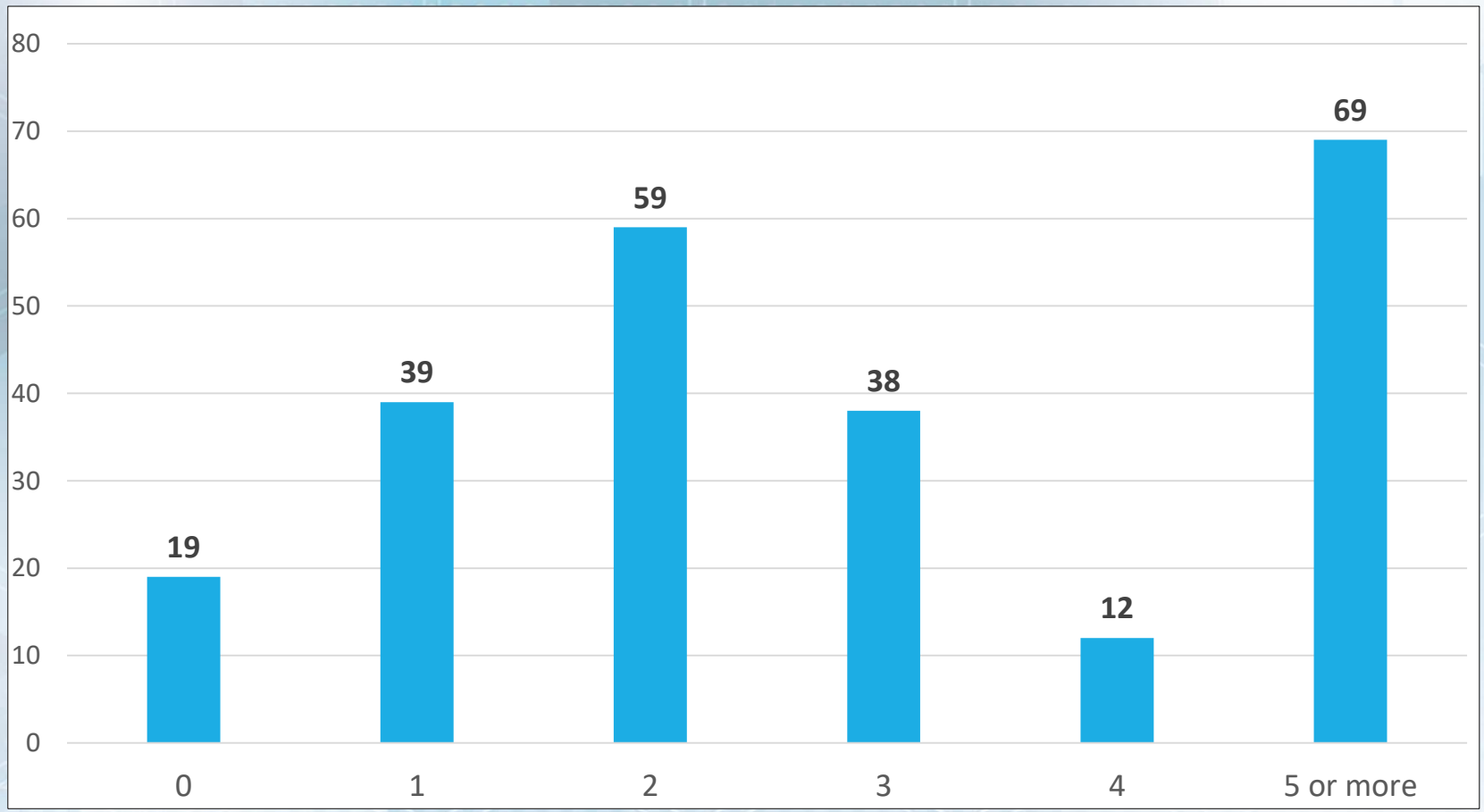


[1]

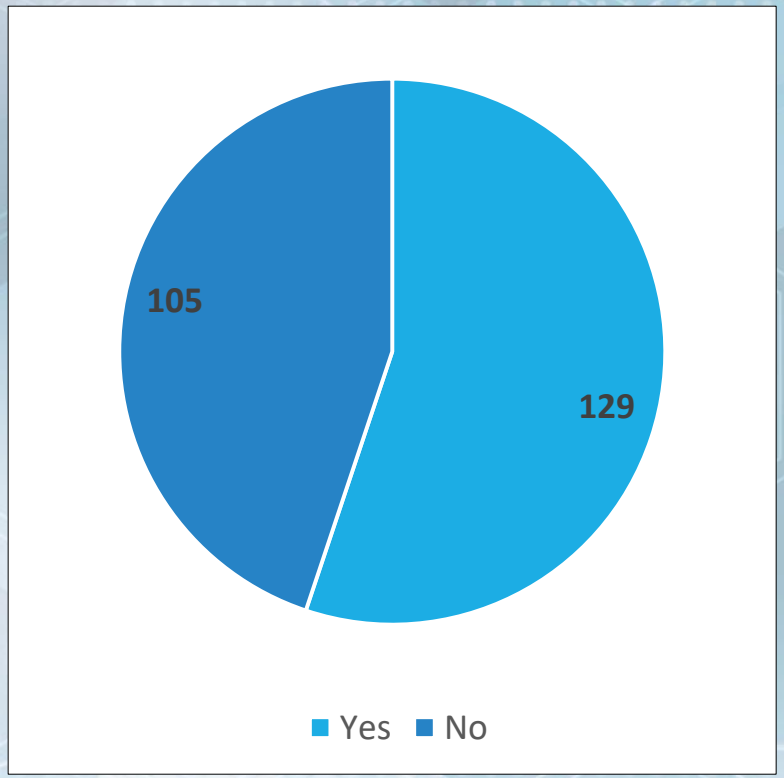
What did you use the stresser on?



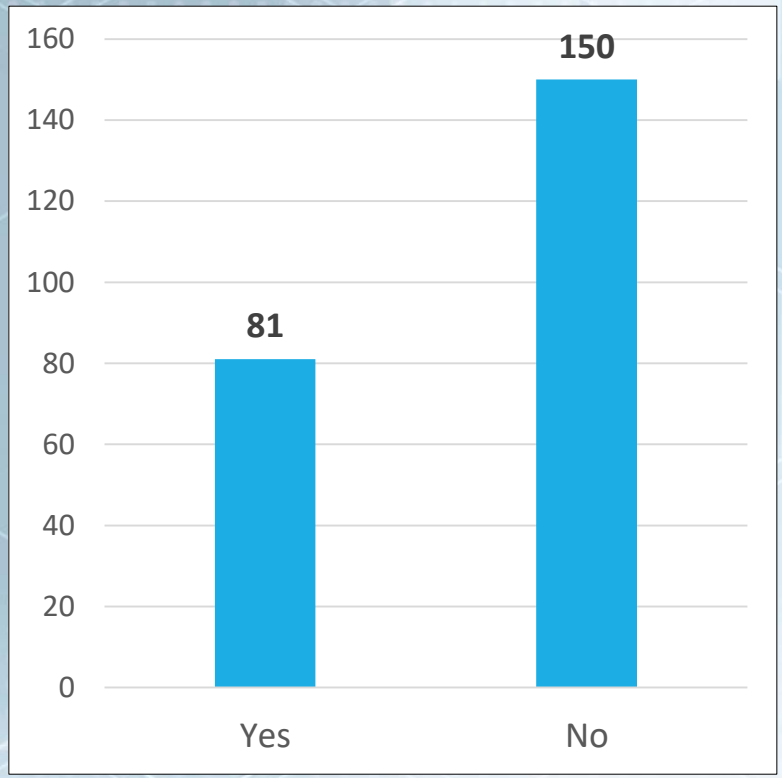
How many different stressers/booters did you use or have accounts with?



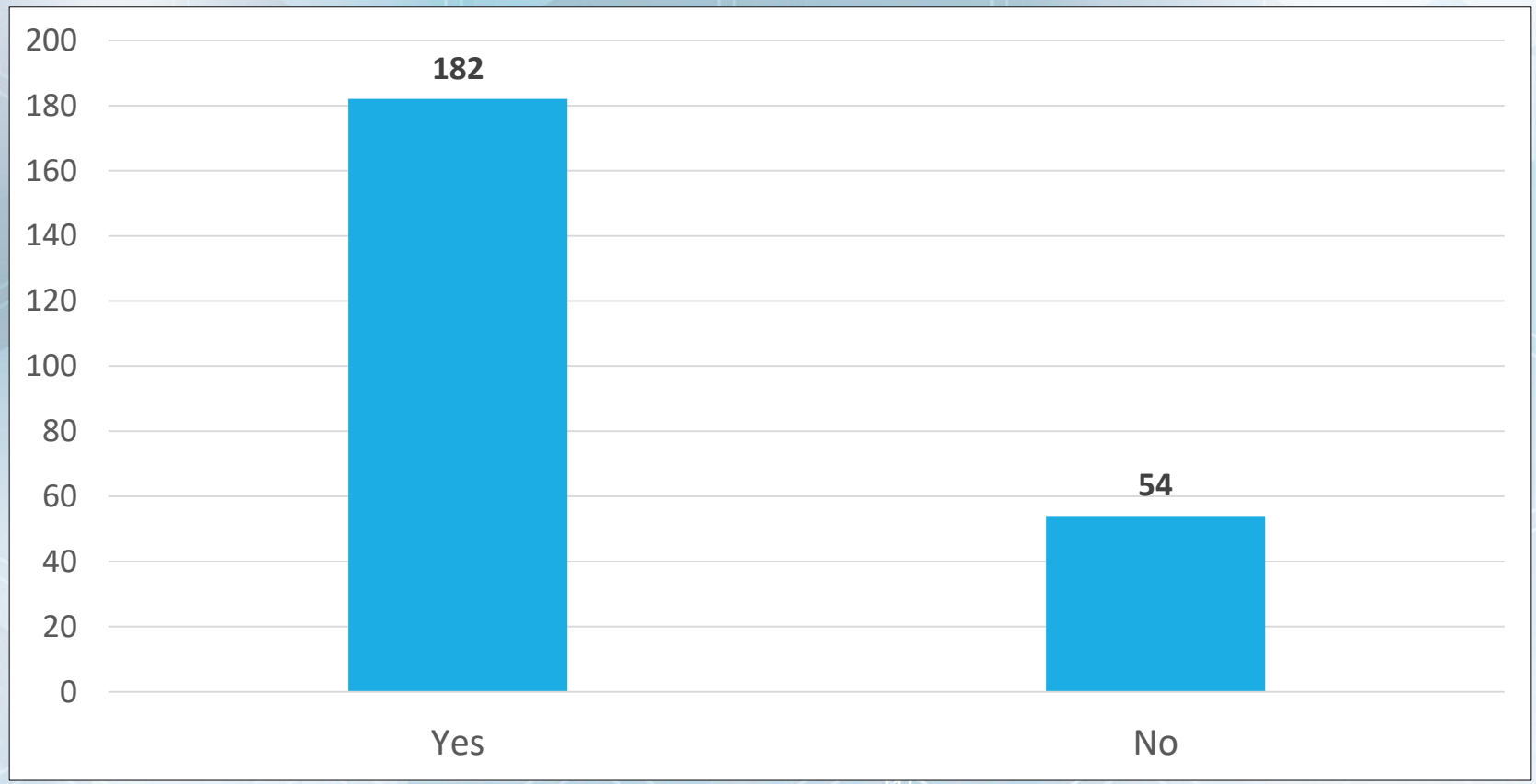
Have you ever operated your own stresser/booter?



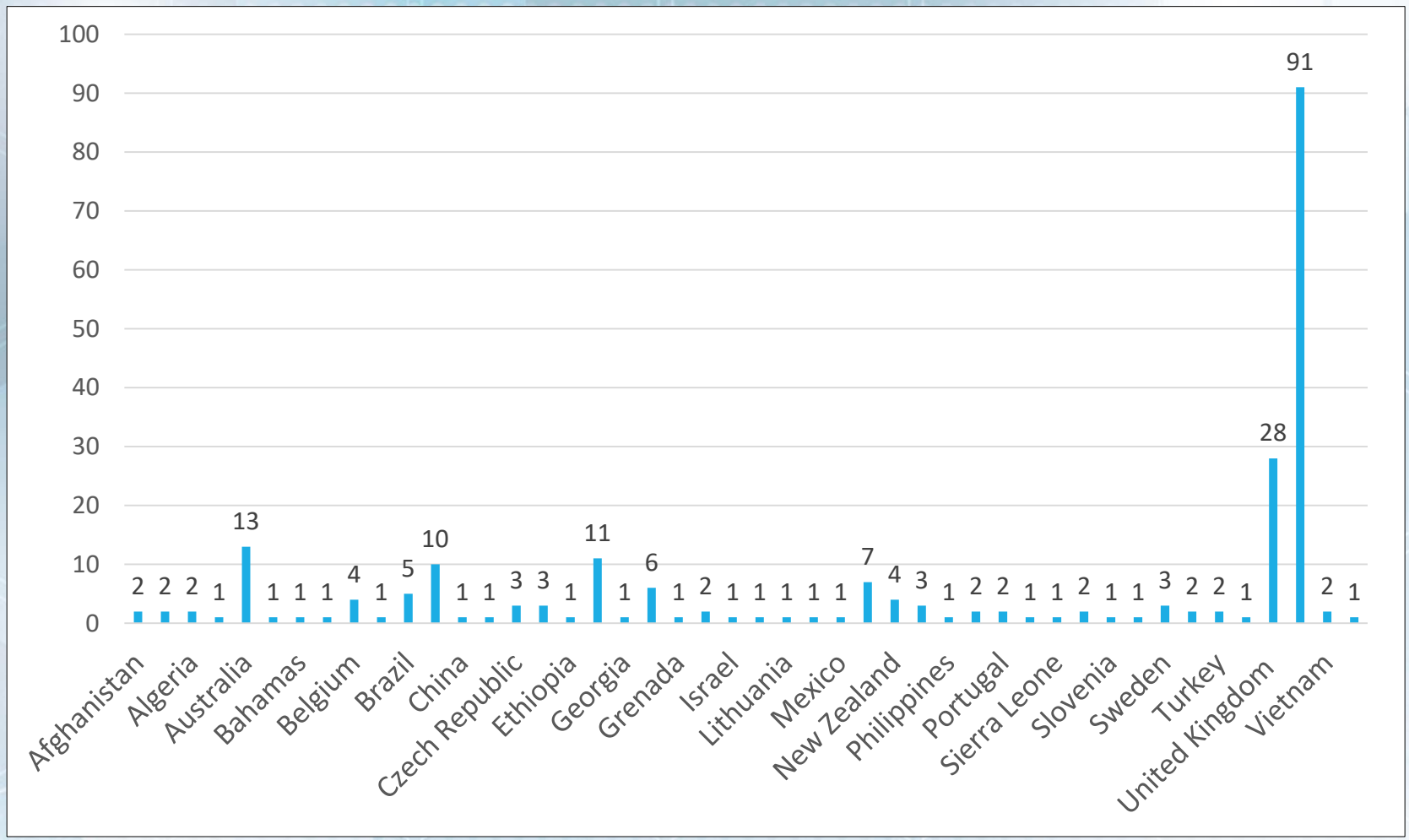
Have you assisted with the operation of a booter or stresser, or recruited members, posted ads?



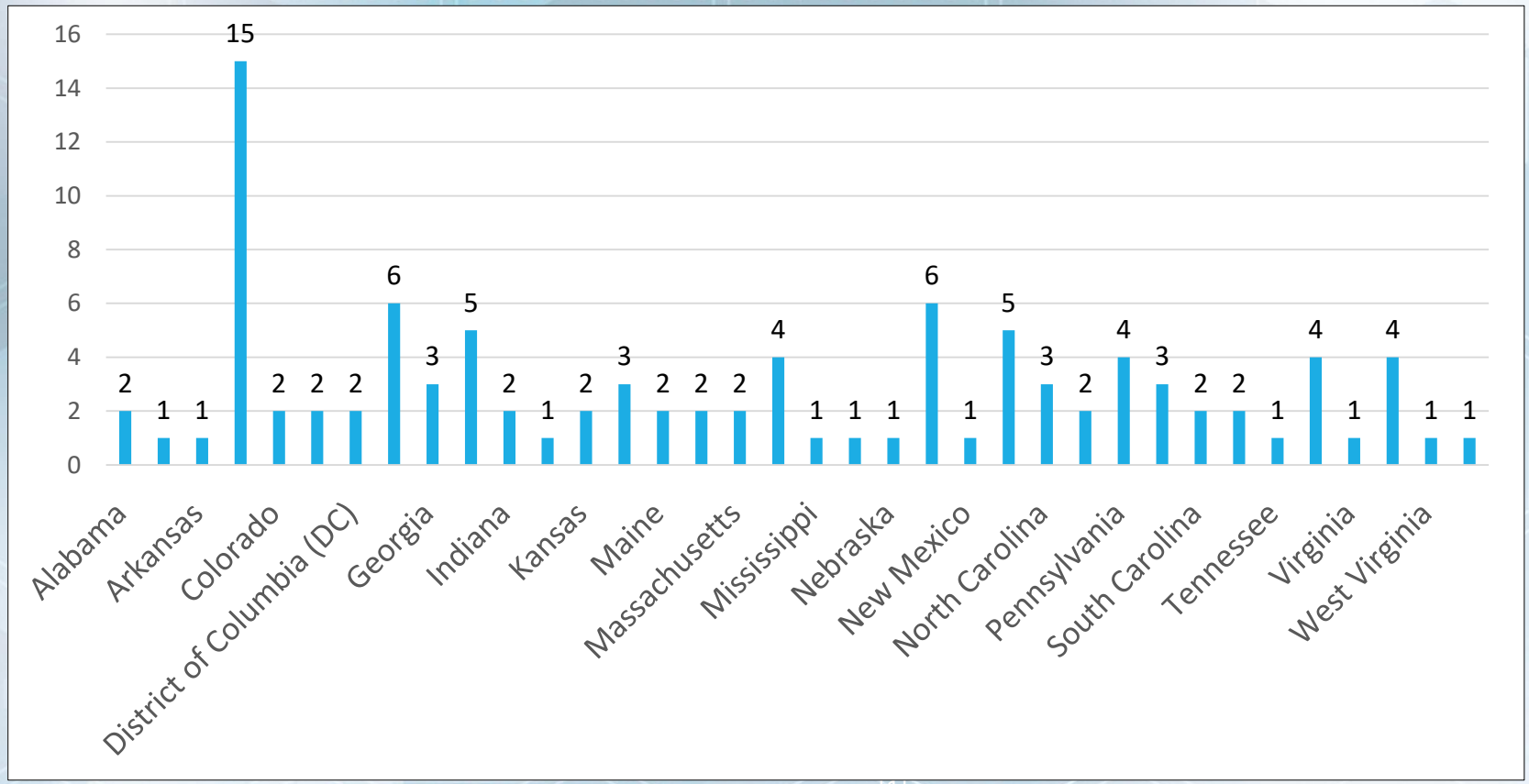
Have you ever been the target of a stresser?



In what country do you live?

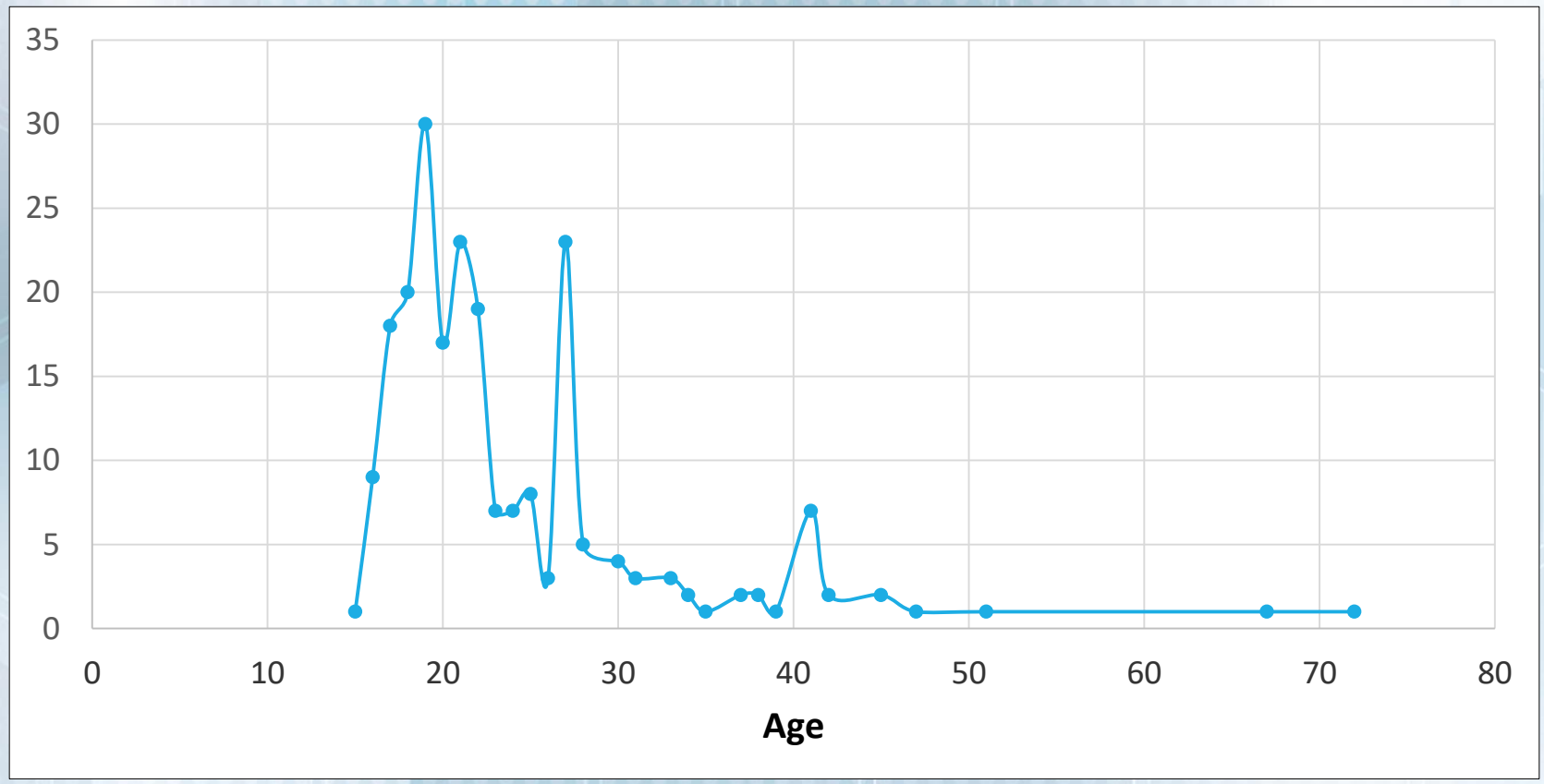


If USA, what state do you reside in?



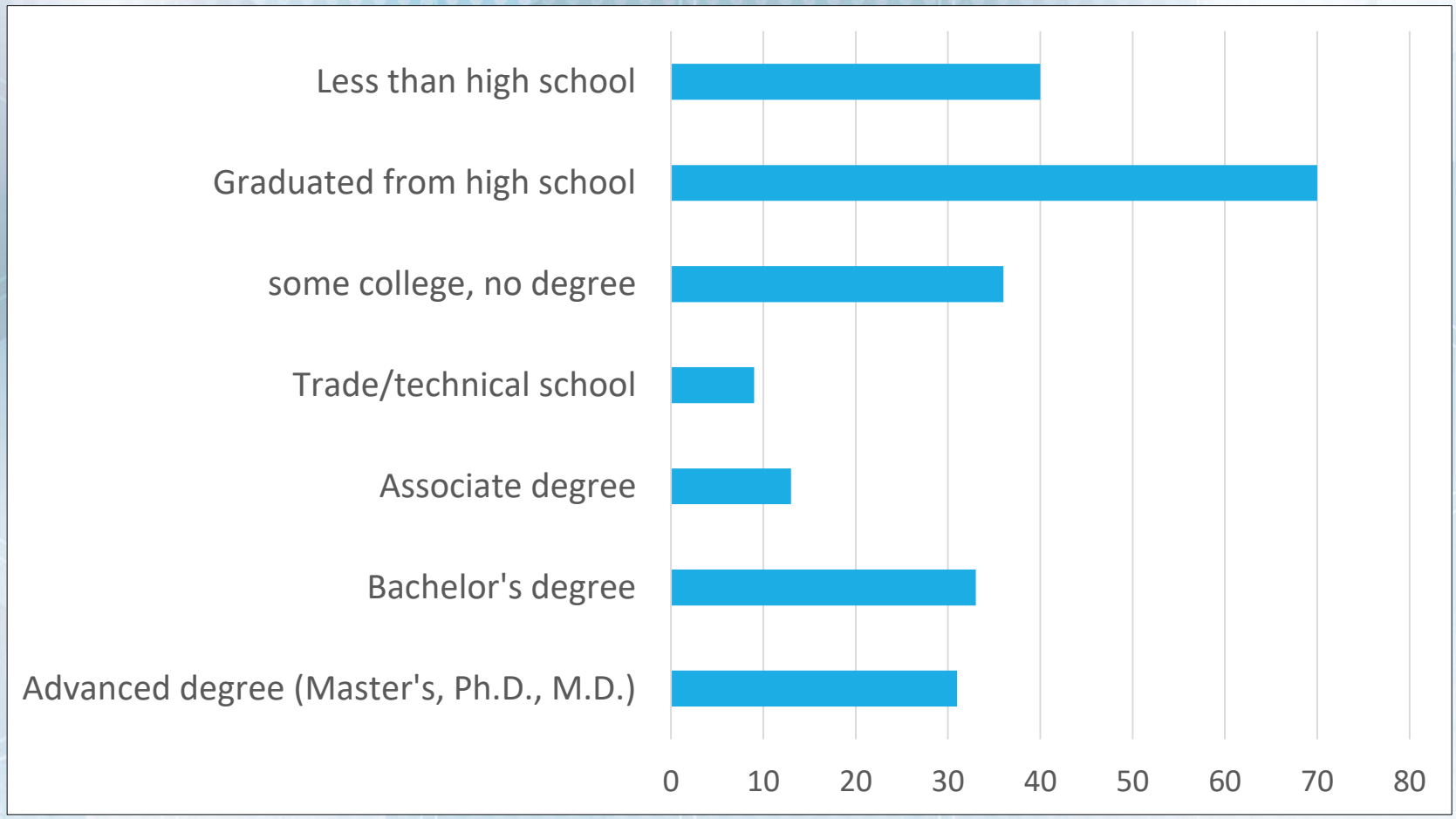
[1]

What is your age?

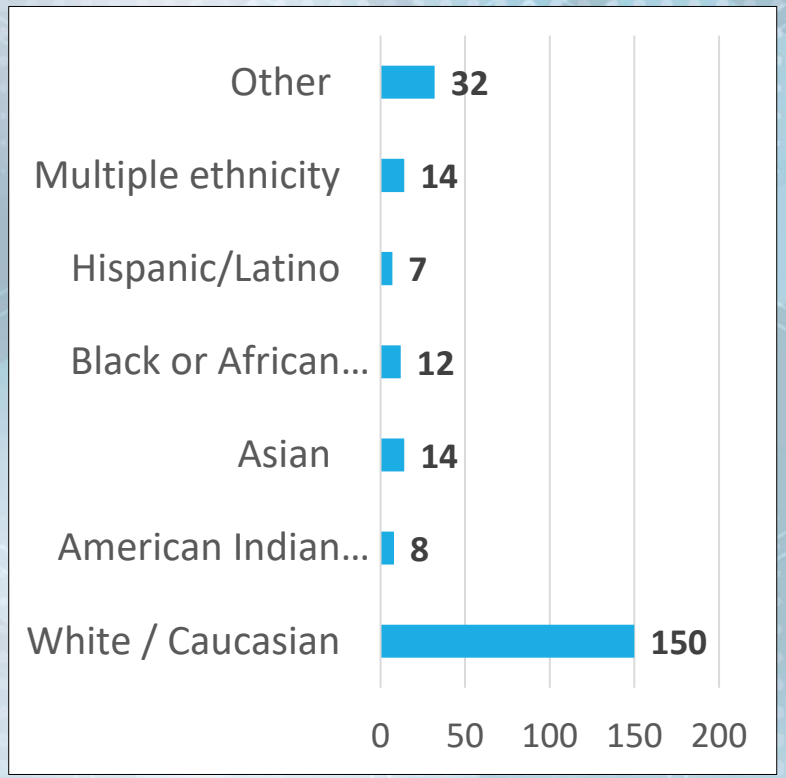


[1]

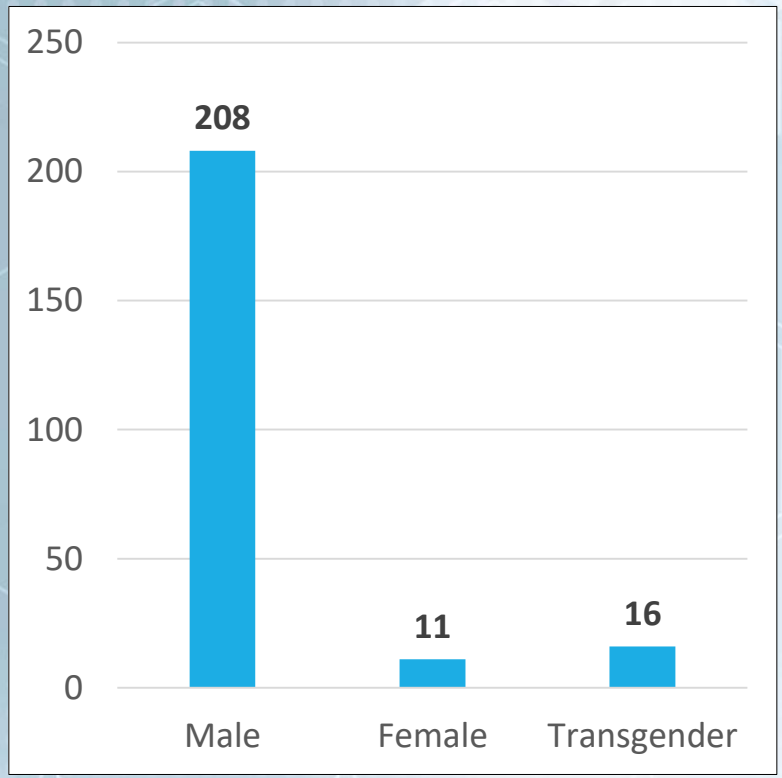
What is the highest level of education?



Race/Ethnicity



Gender



Demographic Breakdown

	Native Indian or Alaskan Native	Asian	Native Hawaiian or other Pacific Islander	Black or African American	Hispanic/ Latino	White/ Caucasian	Multiple Ethnicity	Other	Total
Male	5	11	0	6	6	**143**	11	25	207
Female	1	3	0	3	0	2	1	1	11
Transgender	4	0	0	2	1	4	1	5	17
	10	14	0	11	7	149	13	31	235

[1]

		What is your knowledge and skill level with stressers?										
Have you ever operated your own stresser?		1 (Noob)	2	3	4	5	6	7	8	9	10 (Expert)	Total
	Yes	3	0	1	0	5	8	14	10	7	**56**	104
	No	5	2	6	7	21	15	17	25	6	25	129
	Total	8	2	7	7	26	23	31	35	13	81	233

		What is your gender?			
		Female	Male	Transgender	Total
Have you ever operated your own stresser?	Yes	8	88	9	105
	No	3	117	6	126
	Total	11	205	15	231

What was the motivation behind the use of the stresser?	How many systems/servers did you test?							
	1	2	3	4	5	6-10	Over 10	Total
System Testing	19	17	14	6	6	12	67	141
Research	15	11	11	4	4	11	61	117
Test My Abilities	13	6	10	8	4	10	58	109
Affect Game/Opponent	7	2	4	7	4	7	61	92
Hactivisim/Protest	2	2	4	2	2	5	41	58
Other	7	1	5	3	3	4	32	55
Hired to Do So	3	1	0	3	1	2	33	43
Affect Business Competitor	0	1	0	1	2	1	20	25

What did you use the stresser on?	What is your knowledge and skill level with stressers?										
	1 (Noob)	2	3	4	5	6	7	8	9	10 (Expert)	Total
Yourself	6	0	3	2	17	15	12	23	8	49	135
Game	0	0	2	2	11	9	15	16	6	52	113
Business Server (non website, such as email or file server)	0	0	2	1	4	3	5	6	6	**33**	60
Website/Webserver (Private/Commerical)	0	0	1	0	12	9	**13**	**24**	**10**	**47**	116
Website/Webserver (Gov't)	0	1	0	0	3	2	2	3	9	**25**	45
Other	2	0	2	3	7	6	9	8	5	**40**	82

What was the motivation behind the use of the stresser?	What is your knowledge and skill level with stressers?										
	1	2	3	4	5	6	7	8	9	10	Total
System Testing	2	0	2	2	19	12	19	23	11	49	139
Research	4	0	2	1	14	13	14	14	7	46	115
Test My Abilities	3	0	2	2	12	11	18	12	9	39	108
Affect Game/Opponent	1	1	2	2	2	9	15	14	6	36	88
Hactivisim/Protest	0	0	1	1	4	5	6	12	5	24	58
Other	2	0	1	1	5	5	5	7	3	25	54
Hired to Do So	1	0	0	0	2	1	6	5	8	20	43
Affect Business Competitor	0	0	0	0	1	1	2	1	4	15	24

What did you use the stresser on?	What was your motivation?								
	Research	System Testing	Affect Game/ Opponent	Hactivisim/ Protest	Affect Business Competitor	Test Abilities	Hired to Do So	Other	Total
Yourself	84	106	42	35	17	69	31	33	417
Game	54	64	73	41	20	65	30	35	382
Business Server (non website, such as email or file server)	42	48	30	27	19	37	28	25	256
Website/Webserver (Private/Commerical)	64	78	56	50	21	68	32	41	410
Website/Webserver (Gov't)	27	28	24	24	15	28	20	18	184
Other	42	49	44	30	19	47	24	42	297

Conclusion

Going Forward

- **Exploratory analysis**
  - Did the stresser work as advertised (Binary Logistic Regression Model)?
  - Predicting motivation
  - Predicting target
  - Predicting whether the person operated their own stresser
- **Follow up survey or interview of 84 respondents**

HDIAC Services

Technical Inquiry Service

- HDIAC provides up to 4 free hours of information services:
  - Literature searches
  - Document/bibliography requests
  - Analysis within our eight focus areas – Alternative Energy, Biometrics, CBRN Defense, Critical Infrastructure Protection, Cultural Studies, Homeland Defense and Security, Medical, Weapons of Mass Destruction

Core Analysis Task (CAT)

- Challenging technical problems requiring more than 4 hours of research can be solved by initiating a CAT:
  - Pre-competed and pre-awarded
  - Work can begin on a project approximately two months after the statement of work has been approved
  - Cap of $500,000 (through August 31, 2018)
  - Must be completed within 12 months

For more information: https://www.hdiac.org/technical_services

Questions?