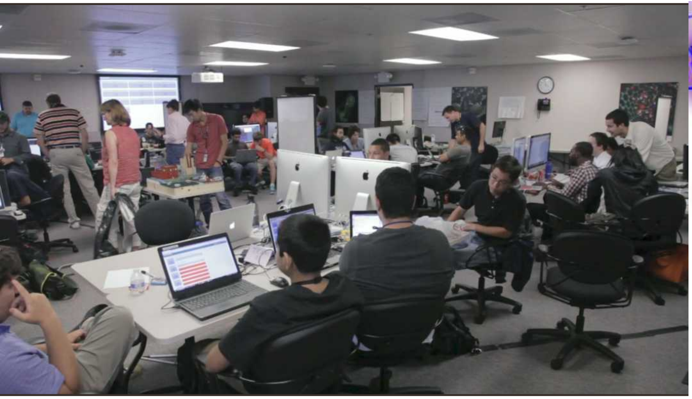
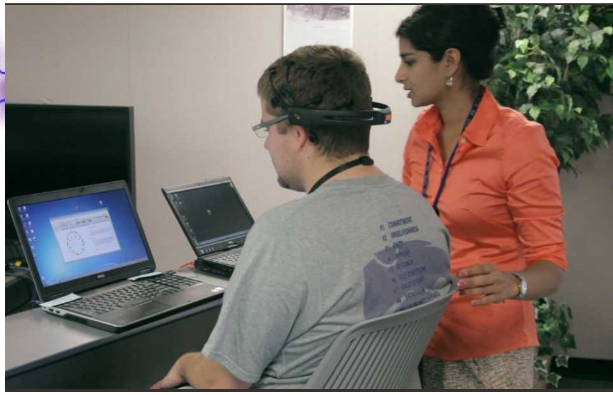
SAND2015-6237C

Exceptional service in the national interest





Measuring Expert and Novice Performance within Computer Security Incident Response Teams

Austin Silva, Glory Aviña, Jonathan T. McClain, Laura Matzen, Chris Forsythe

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Introduction

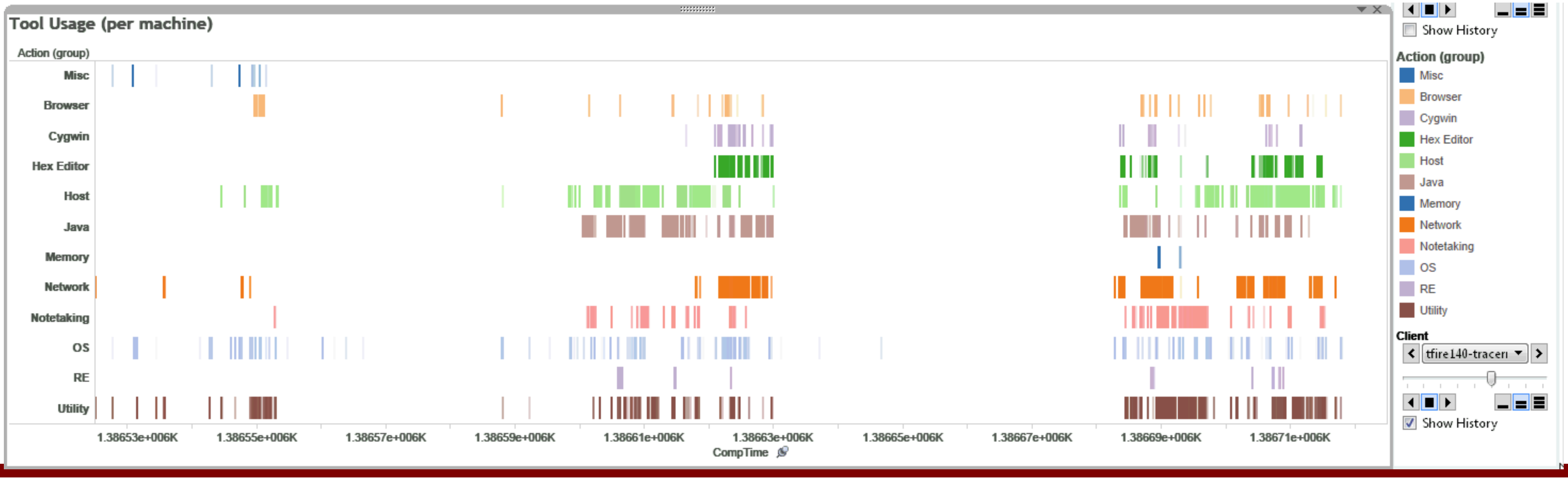
- Cyber threats are increasing and not going away
- There is a need to understand the the characteristics of high-performing individuals in cybersecurity, as well as their impact on incident outcomes .
- This methodology seeks to advance:
  - The ability to **identify individuals with a high aptitude** to excel in the cybersecurity domain in order to inform recruiting and enhance training.
  - The ability to **build a better cybersecurity workforce** that will directly contribute to the crucial task of protecting organizations' information and infrastructure.

What is Tracer FIRE?

- A game-based training environment for incident responders (IRs)
- Teams compete in a variety of challenges related to various aspects of cybersecurity
- As teams solve individual puzzles in the the game, they unlock new pieces of the narrative.

Methodology

- Performance Data
  - Computer instrumentation (from TracerFIRE)
    - Correct submissions
    - Tools used
    - # of submissions
    - Who submitted answers



□ Show History

Client: tfire140-traceri

☑ Show History

Methodology

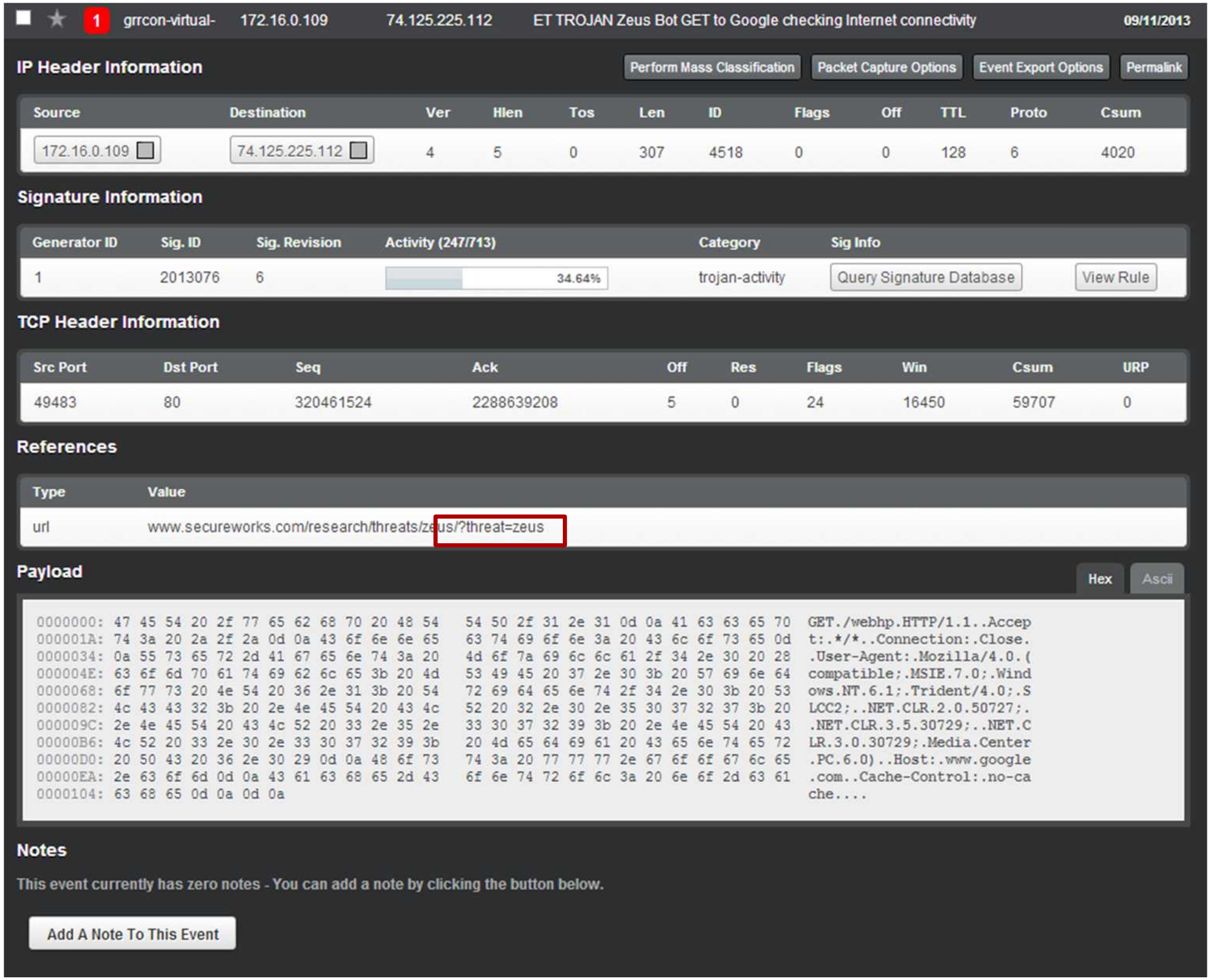
- Cognitive/Behavioral Data
  - Eye Tracking
    - Domain-general task
    - Domain-specific task
  - Electroencephalography
    - Recognition memory test
  - Self-report measures
    - Big Five Personality Inventory
    - Need for Cognition Scale
    - General Decision-Making Style

Eye Tracking Collection

12 Novice Subjects:

- Domain-specific task
- T/L visual discrimination task
- Sandia Progressive Matrices task

Sample Domain-specific Task



1 grrcon-virtual- 172.16.0.109 74.125.225.112 ET TROJAN Zeus Bot GET to Google checking Internet connectivity 09/11/2013

IP Header Information

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
172.16.0.109	74.125.225.112	4	5	0	307	4518	0	0	128	6	4020

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (247/713)	Category	Sig Info	
1	2013076	6	34.64%	trojan-activity	Query Signature Database	View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
49483	80	320461524	2288639208	5	0	24	16450	59707	0

References

Type	Value
url	www.secureworks.com/research/threats/zeus/?threat=zeus

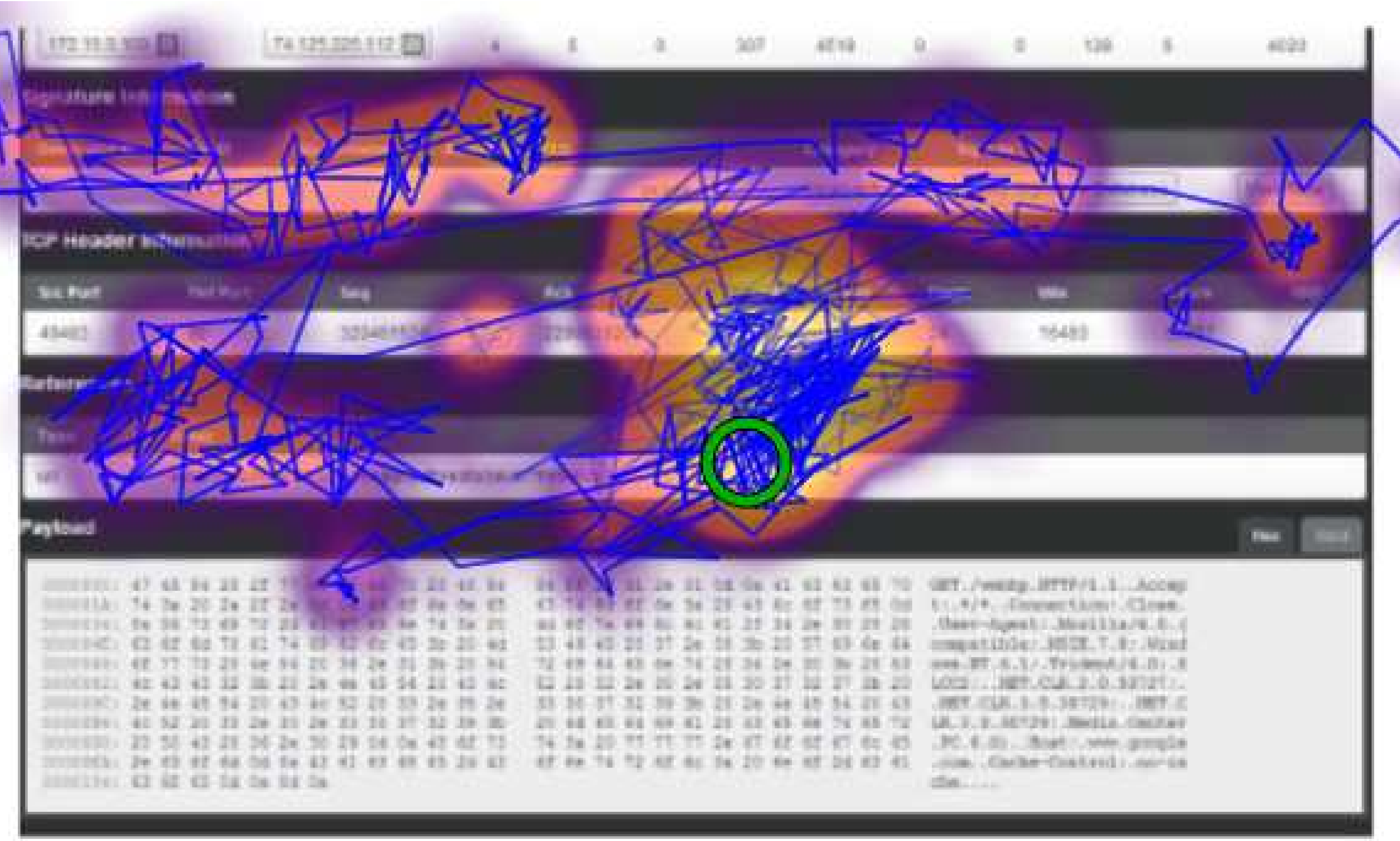
Payload

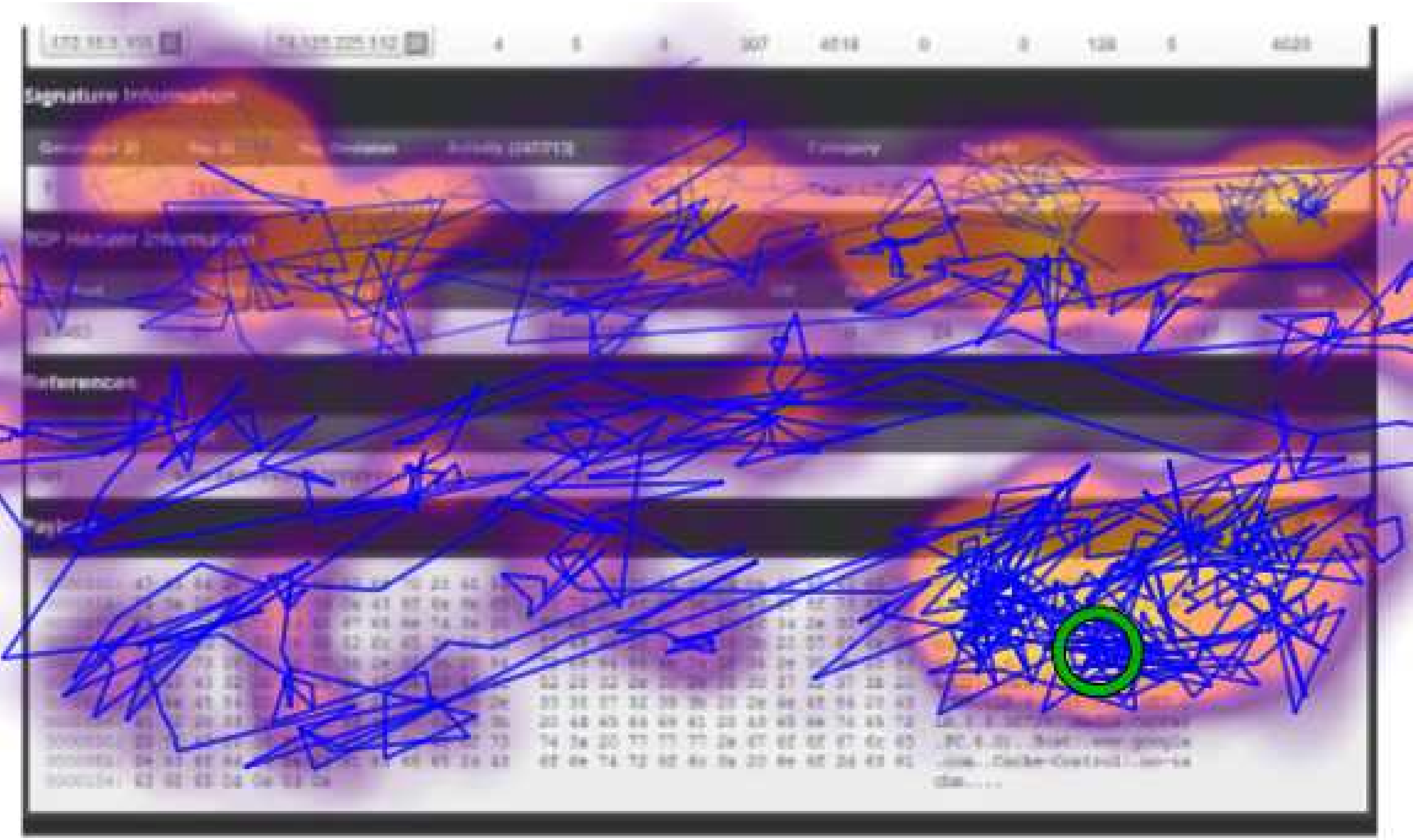
```
0000000: 47 45 54 20 2f 77 65 62 68 70 20 48 54   54 50 2f 31 2e 31 0d 0a 41 63 63 65 70   GET./webhp.HTTP/1.1..Accep
000001A: 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 6e 65   63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d   t:.*/*..Connection:.Close.
0000034: 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20   4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28   .User-Agent:.Mozilla/4.0.(
000004E: 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d   53 49 45 20 37 2e 30 3b 20 57 69 6e 64   compatible;.MSIE.7.0;.Wind
0000068: 6f 77 73 20 4e 54 20 36 2e 31 3b 20 54   72 69 64 65 6e 74 2f 34 2e 30 3b 20 53   ows.NT.6.1;.Trident/4.0;.S
0000082: 4c 43 43 32 3b 20 2e 4e 45 54 20 43 4c   52 20 32 2e 30 2e 35 30 37 32 37 3b 20   LCC2;..NET.CLR.2.0.50727;.
000009C: 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e   33 30 37 32 39 3b 20 2e 4e 45 54 20 43   .NET.CLR.3.5.30729;..NET.C
00000B6: 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b   20 4d 65 64 69 61 20 43 65 6e 74 65 72   LR.3.0.30729;.Media.Center
00000D0: 20 50 43 20 36 2e 30 29 0d 0a 48 6f 73   74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65   .PC.6.0)..Host:.www.google
00000EA: 2e 63 6f 6d 0d 0a 43 61 63 68 65 2d 43   6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61   .com..Cache-Control:.no-ca
0000104: 63 68 65 0d 0a 0d 0a                                                                che....
```

Notes

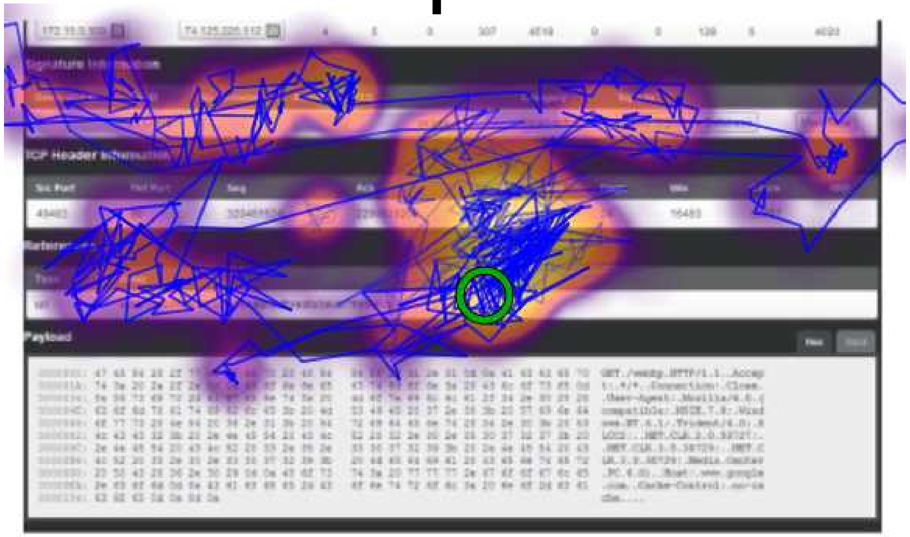
This event currently has zero notes - You can add a note by clicking the button below.

Question: What is the common name of the malware reported by the IDS alert provided?

172.15.3.103
74.125.225.112
4
5
3
307
4519
0
0
128
5
4023
Signature Information
TCP Header Information
Src Port
Seq
Ack
Win
43482
15483
Payload
Hex
GET./webhp.HTTP/1.1..Accep
t:.*/*..Connection:.Close.
.User-Agent:.Mozilla/4.0.(
compatible;.MSIE.7.0;.Wind
ows.NT.6.1;.Trident/4.0;.S
LCC2;..NET.CLR.2.0.50727;.
.NET.CLR.3.5.30729;..NET.C
LR.3.0.30729;.Media.Center
.PC.6.0)..Host:.www.google
.com..Cache-Control:.no-ca
che....

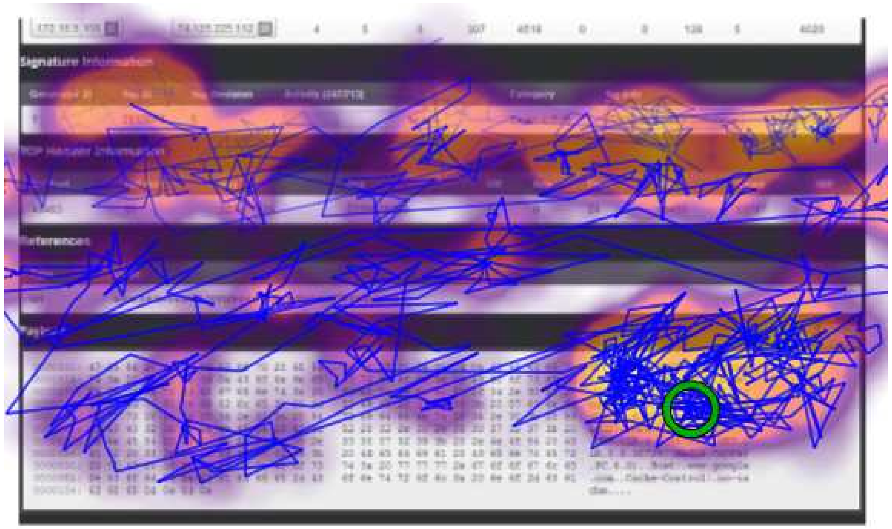

Signature Information
TCP Header Information
References
Payload

Expert



6 Sec

Novice



20 Sec

Cognitive Measures

- Self report measures are hypothesized to show:
  - High performers that fell within the ROI quickly would have higher reported need for cognition scores
  - High performers that answered soon after entering the ROI would be rational-intuitive decision makers
  - Low performers and those with high levels of avoidance would not answer without investigating the screen in its entirety.

Future Work

- Acquire more data from domain experts
- Help alleviate problems due to attribution within the teams
- Use a dynamic cyber domain task for more operational relevance

Conclusion

- It is possible to perform complex in-situ testing in the cyber domain to identify differences between expert and novice individuals and teams
- Differences in skill can be detected using the eye trackers but more data is needed for more robust results
- Cognitive measures and behavioral game data can be leveraged alongside eye tracking information to understand expertise in topical space or tool.