2016 DANGER ZONE INCIDENT RETORT

THE CURRENT STATE OF INTERNET THREATY THREATS

PRESENTED BY THREATBUTT

THREATBUTT DZIR

SCARY APTS

2016 Danger Zone Incident Retort

99% of breaches involved the Internet.

2016 DZIR Introduction

The world's leading Threaty Threat sub-Genius company, now in 10th year (in dog years), is reluctant to release it's first DZIR report. Working in close partnership with Kenny Loggins Security and their unique Intrusion Detection Highway platform.

In the usual ground breaking and innovative way you've come to expect from Threatbutt, this year's data set is available online in full. Over at 170gb torrent.

We hope you enjoy this report and we look forward to forcing some intern in to copy and pasting another one next year.

Who got owned

In analysing the data and using our industry leading Internet Hacking Attribution Map data, we've been able to plot a definite trend. Using our Machine Learning Actually Quite Small Data Super Computer we've been able to neatly summarize this research in to the following PR friendly sound bite:

> *The majority of attacks come from and target population centers or places with a lot of computers.*

For the first time we are able to reveal to the world that the majority of Internet Cyber Attacks do not come from Africa or Antarctica, but do in fact focus on America and Eastern Asia.

We believe, armed with this new knowledge, enterprises are better able to defend themselves by requiring "Data Passports" for all their traffic.

THREATBUTT DZIR

CHINA DID IT NO MATTER WHAT

Incidents vs. Breaches

> *Incidentals: A charge for room service, or a bottle of champagne on your business class flight.*
> *Breach: A mere trip of any of the up to date IDS rules from [Cisco's Cyber Secure GenX Sourcefire IPS]*

Beach Trends

I hear ShakaCon is nice, they even pay flights and hotels. You should CFP there next time. You just missed Infiltrate too.

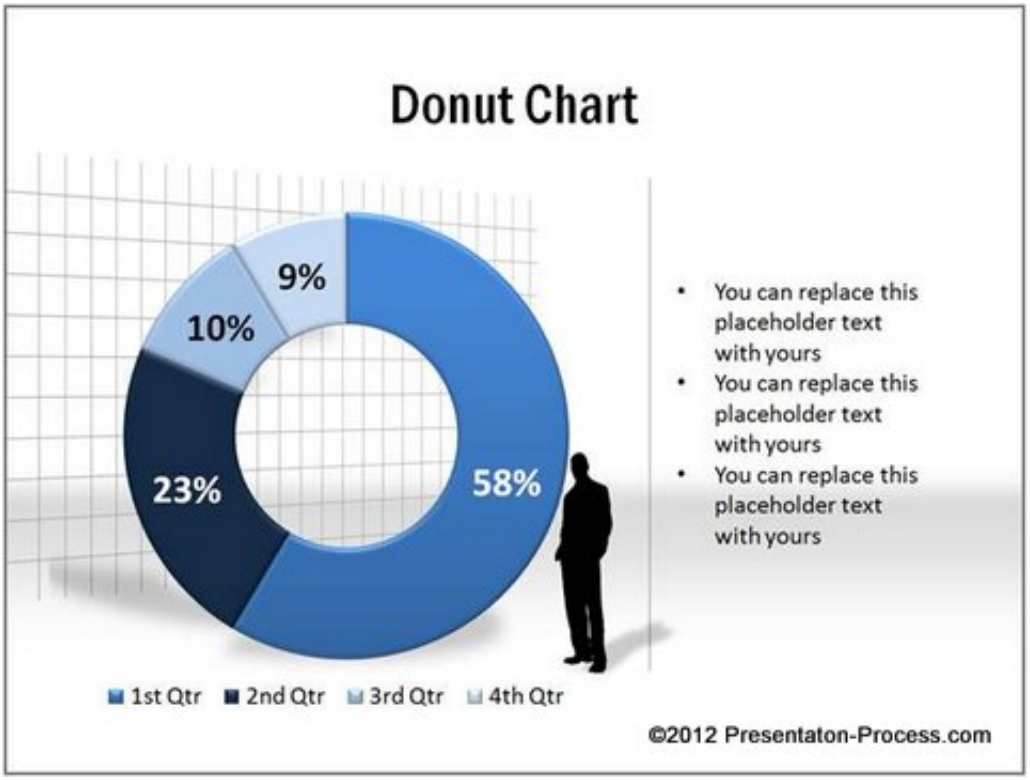
Breach Trends

Coming up with yet more analogies for war makes me feel like a real man, which is empowering, especially when compared to the fact I spend all day typing and making PowerPoint presentations about compliance and which firewall vendor is cheapest. What has my life become. My wife is threatening to leave me, my children hate the fact all I want to do is play golf at the weekends and during the week I'm so consumed with work that this is my only outlet. I want to see fear in the attackers eyes, I want them to know that I am all powerful and not to be messed with. I want the little paracord bracelet I have show them that I am ready. I'm basically a marine, just with no training or combat experience, but other than that, a 100% like a marine, only more badass, as I have a Matrix t-shirt that a friend bought me from DefCon years ago and I know someone that knows someone that is a Goon.

I will now drop in references to American Civil war heroes to show I both a true Patriot and well educated.

And now, on with the pie charts!

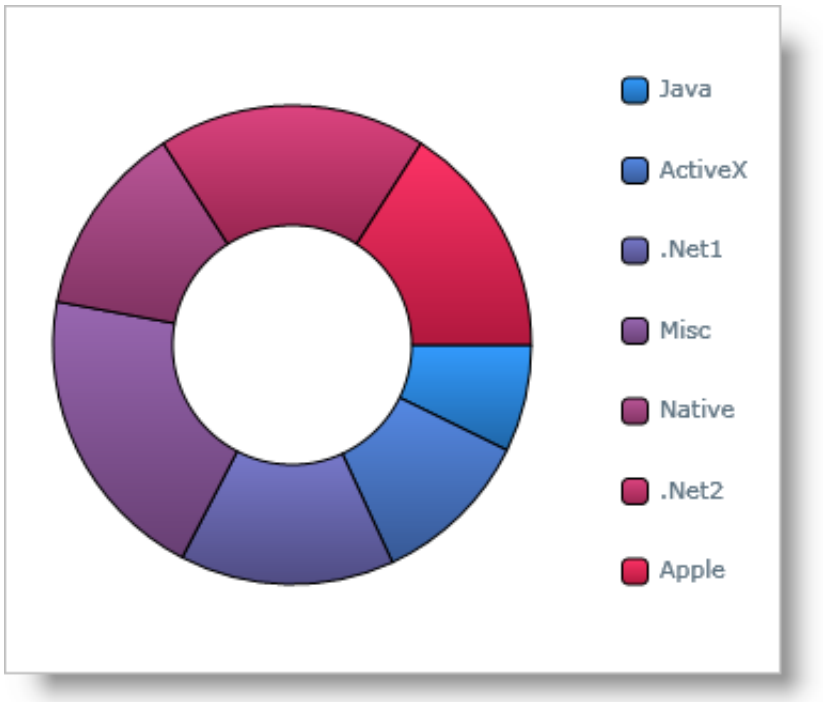
Number of people who can understand what a stupid graph has to do with securing their cybers



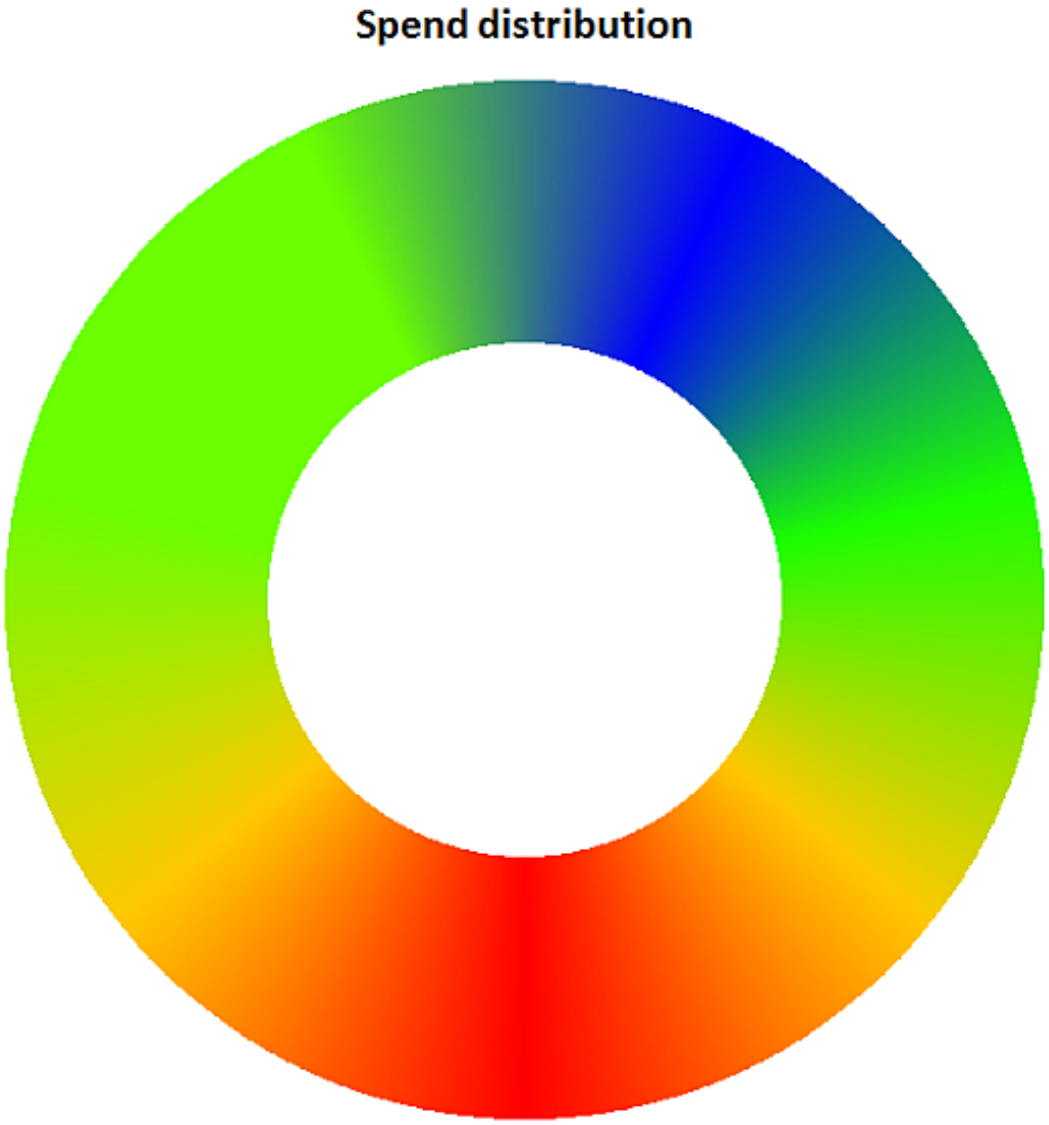
THREATBUTT DZIR

BOOTH BABES

Internet protocol used in breaches, attempted breaches and thought about but never executed breaches



Amount spent by attackers, versus ROI across vertices



THREATBUTT DZIR

EXISTENTIAL CRISIS

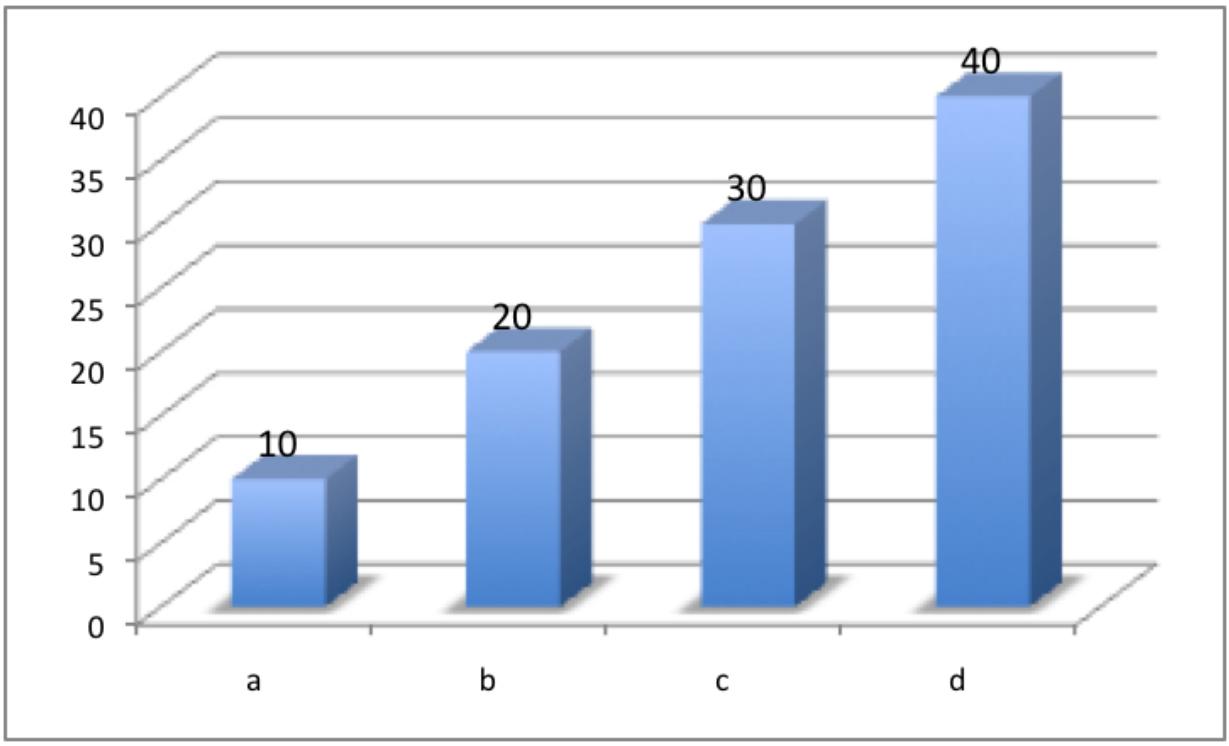
Favorite color of threat actor

THREATBUTT DZIR

SHODAN IS THE BEST HACKER TOOL FOR TOOLS

The Highway to the "Mad" "Oh" "Day" zone

CVEs exploited in the wild.



Vulnerability top 10.

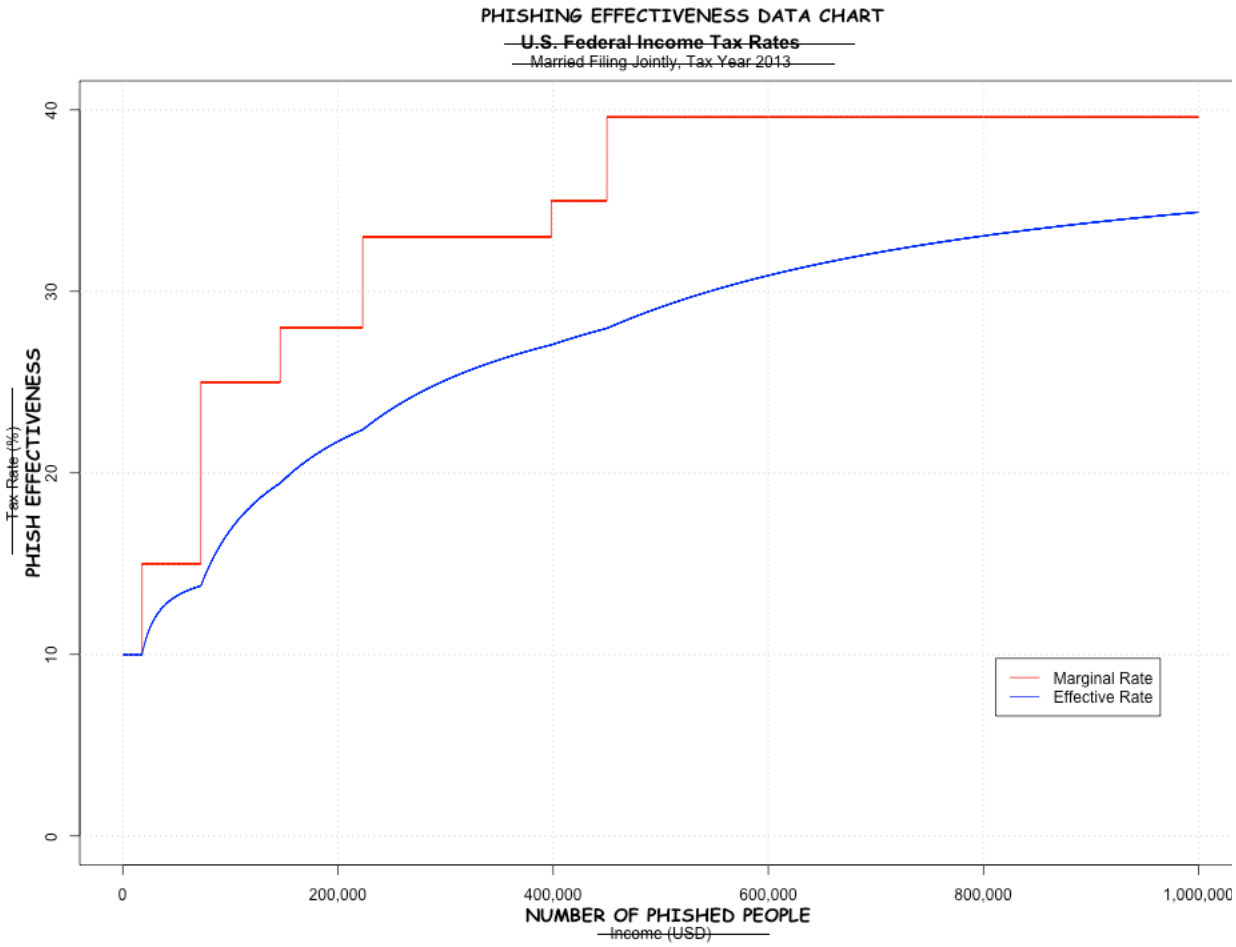
Vuln	CVE	Arbitrary number
Badlock	CVE-1999-0179	0
Classified	CVE-1999-1597	:symbol:
Full remote code execute in global database software	CVE-2002-0649	W32
Internet standard FTP server compromise	CVE-2000-0761	2
Password compromise on core networking equipment	CVE-2005-3196	DB9
Attacks able to disrupt critical networking infrastructure	CVE-1999-0290	1080
Use of Shodan	*pending*	80
Full browser sandbox escape	CVE-2002-0371	70
Kinetic weaponized injection attack via bluetooth	CVE-2015-2247	7
No idea, it just seemed to keep happening in our dataset	CVE-2003-0033	191

THREATBUTT DZIR

SHRIMP AND WHITE WINE

Phishing

Is super effective. Here is another chart to prove it.



Rap Up

> *Revvin' up your engine*
> *Listen to her howlin' roar*
> *Metal under tension*
> *Beggin' you to touch and go*

If you've made it this far I hope you're being billed by the hour.

We at the world's leading Threaty Threat Untelligence plagiariser, hope you've enjoyed this report or at least paid for it. Figuring out how to self publish it on Amazon turned out to be really hard, so there's every chance this is just a series of BMP screenshots cut and pasted in to a Word document and then printed to a PDF. If so, I hope we closed our browser when we took the caps...

We'd also like to take this opportunity to thanks Kenny Logins Security, who are probably a pioneer and leader of a new category of IT security solutions, that of soft rock solid security solutioneering.

The story, all names, characters, and incidents portrayed in this production are fictitious. No identification with actual persons, places, buildings, and products is intended or should be inferred.

To recap, everything is terrible, and heck, we are literally just phoning this one in. See you at the 19th hole!

Your friend,

Tomas Krapier

THREATBUTT DZIR

THOSE POOR VIKINGS

Special note from our CEO, Richard Derriere

Please buy more licenses so we can buy more strip-, I mean, dru-, er...lambo-. Er. You get the drift. It's your loss if you don't have the best® protection™...

Namaste.