The D.E.A.D. Pool

A collection of disposable email address domain registrations

Alex Valdivia
Senior Threat Intel Research Engineer
ThreatConnect, Inc.

June 16, 2016

Agenda

- Disposable Email Addresses (DEAs)
- DEA Domain Registrations
- D.E.A.D. Pool Concept
- Rombertik Case Study
- D.E.A.D. Pool in ThreatConnect

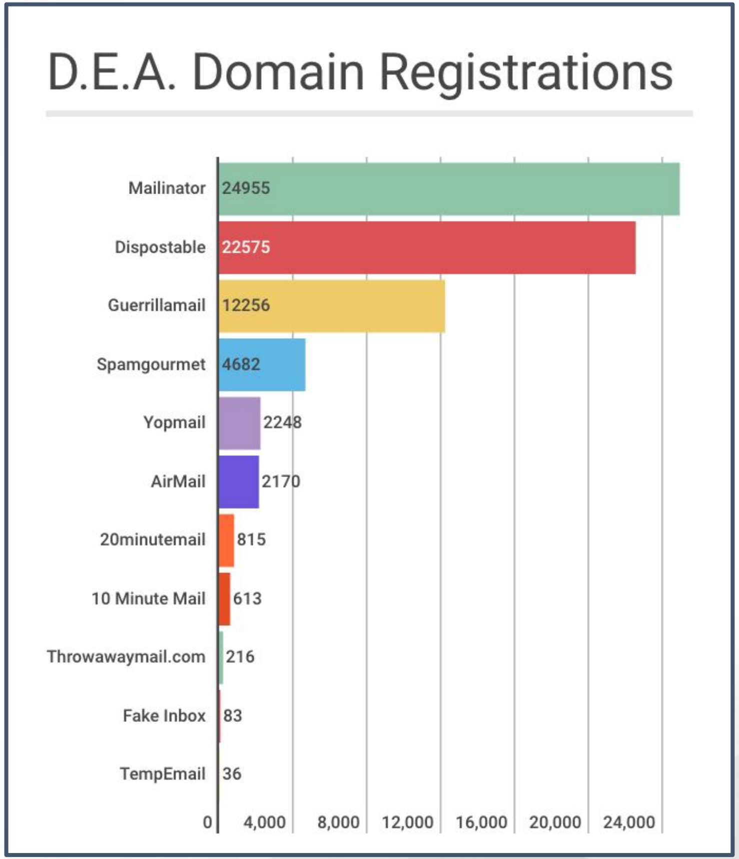
Disposable Email Addresses

- Anonymous P.O. boxes of the internet
- Fast and easy
- Can be used and abused

DEA Domain Registrations

- Domain abuse
  - Dedicated phishing websites
  - Malware delivery
  - C2 Infrastructure

- Registration records
  - Captured in WHOIS
  - DomainTools
    - Reverse Whois
    - Registrant Monitor

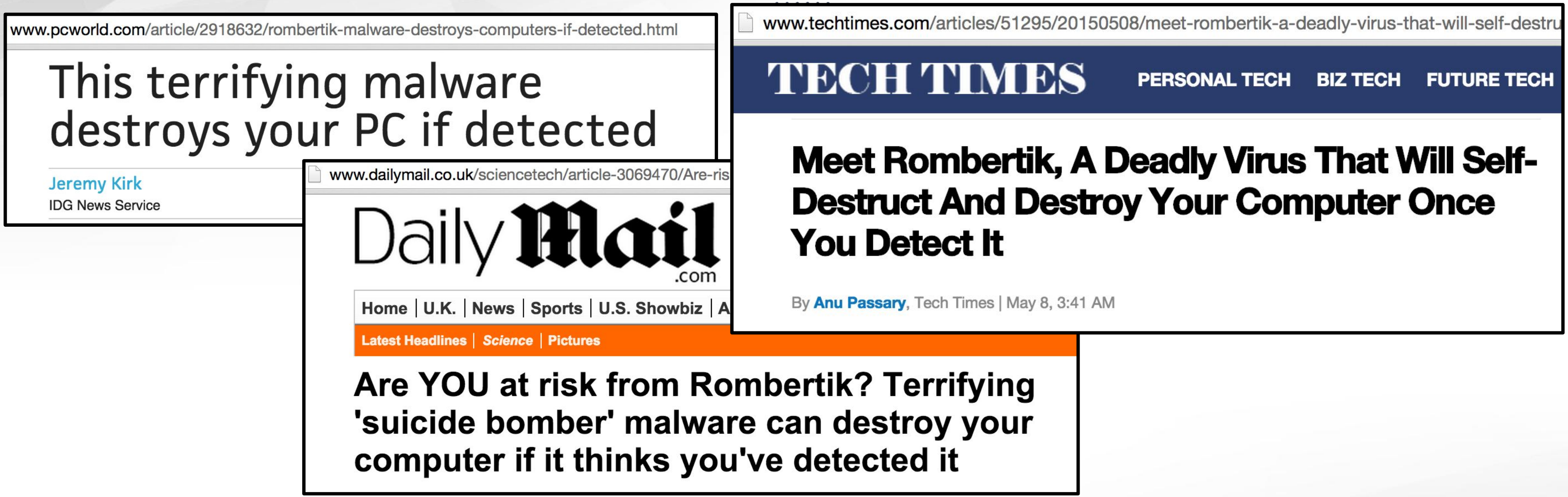


DOMAINTOOLS

D.E.A.D.Pool Concept

- Internal resource for ThreatConnect Research Team
- Data partnership: DomainTools
- Objectives:
  - Create collection of domains registered using DEAs
  - Track WHOIS changes
  - Alert on DNS resolution changes
  - Provide context to other indicators in ThreatConnect
- Approach:
  - Compile reverse WHOIS reports for DEA domains
  - Import domains to ThreatConnect Source
  - Set up DomainTools registrant alerts
  - Parse alert emails and feed to ThreatConnect Source

Rombertik Case Study



www.pcworld.com/article/2918632/rombertik-malware-destroys-computers-if-detected.html

This terrifying malware destroys your PC if detected

Jeremy Kirk
IDG News Service

www.dailymail.co.uk/sciencetech/article-3069470/Are-ris

Daily Mail .com

Home | U.K. | News | Sports | U.S. Showbiz | A
Latest Headlines | Science | Pictures

Are YOU at risk from Rombertik? Terrifying 'suicide bomber' malware can destroy your computer if it thinks you've detected it

www.techtimes.com/articles/51295/20150508/meet-rombertik-a-deadly-virus-that-will-self-destru

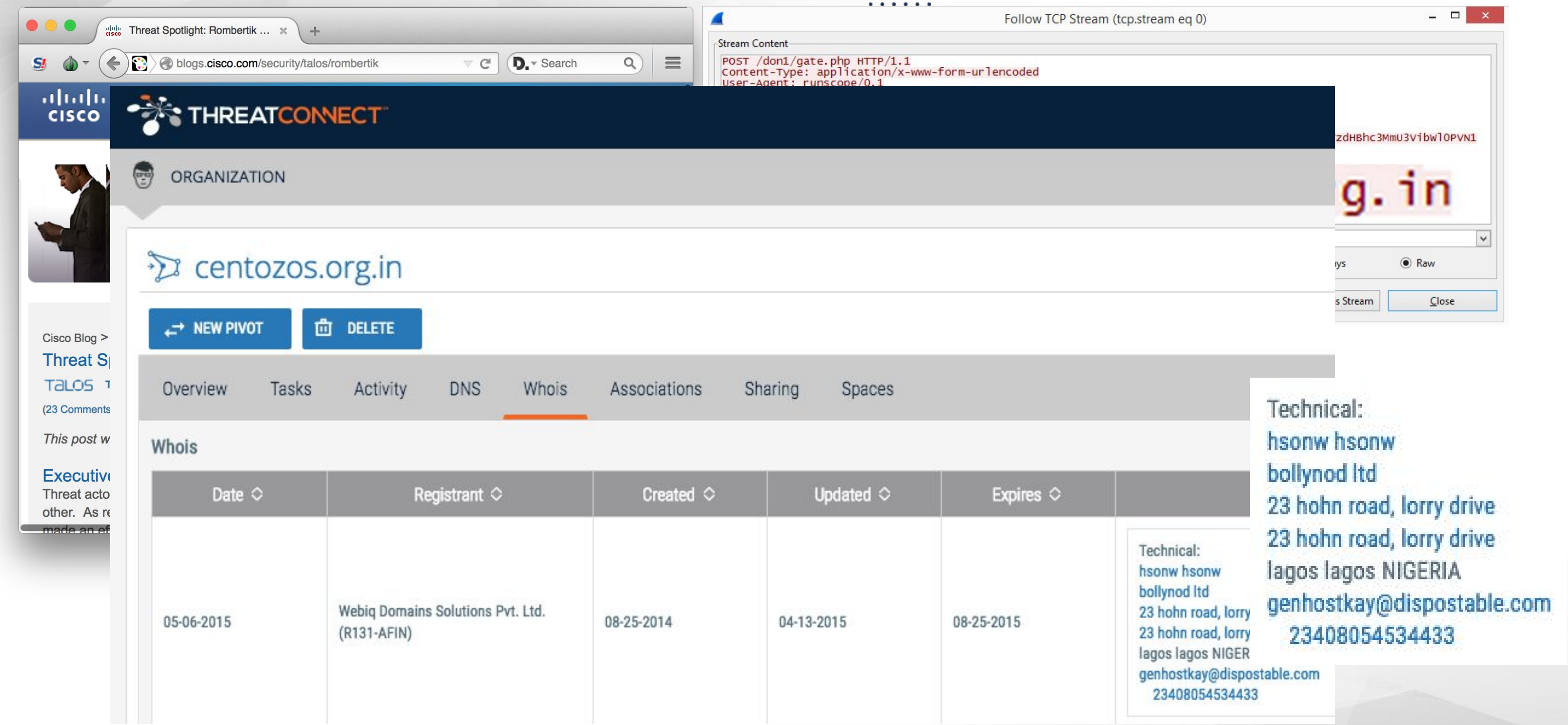
TECH TIMES

Meet Rombertik, A Deadly Virus That Will Self-Destruct And Destroy Your Computer Once You Detect It

By Anu Passary, Tech Times | May 8, 3:41 AM

In May 2015, a single Rombertik malware sample signaled the end of the internet. EVERYBODY PANIC!

Rombertik Case Study



Threat Spotlight: Rombertik ...
blogs.cisco.com/security/talos/rombertik
Search
cisco

Cisco Blog >
Threat S
TALOS T
(23 Comments
This post w

Executive
Threat acto
other. As re
made an ef

Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
POST /don1/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: runscope/0.1
```

```
zdHBhc3MmU3VibWlOPVN1
g.in
```

THREATCONNECT

ORGANIZATION

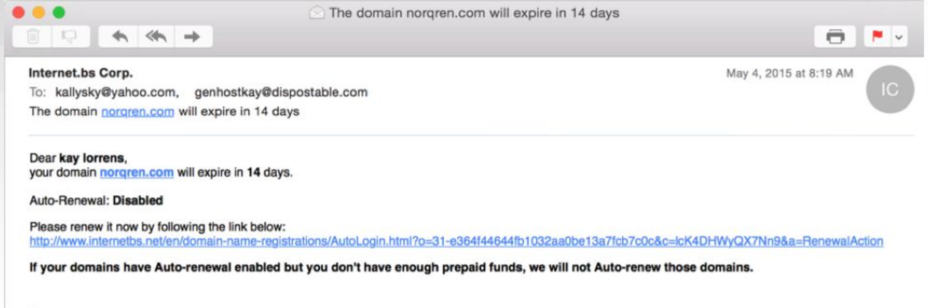
centozos.org.in

Whois

Date ◇	Registrant ◇	Created ◇	Updated ◇	Expires ◇	
05-06-2015	Webiq Domains Solutions Pvt. Ltd. (R131-AFIN)	08-25-2014	04-13-2015	08-25-2015	Technical: hsonw hsonw bollynod ltd 23 hohn road, lorry 23 hohn road, lorry lagos lagos NIGER genhostkay@dispostable.com 23408054534433

Technical:
hsonw hsonw
bollynod ltd
23 hohn road, lorry drive
23 hohn road, lorry drive
lagos lagos NIGERIA
genhostkay@dispostable.com
23408054534433

Rombertik Case Study



The domain norqren.com will expire in 14 days

Internet.bs Corp.
To: kallysky@yahoo.com, genhostkay@dispostable.com
The domain norqren.com will expire in 14 days

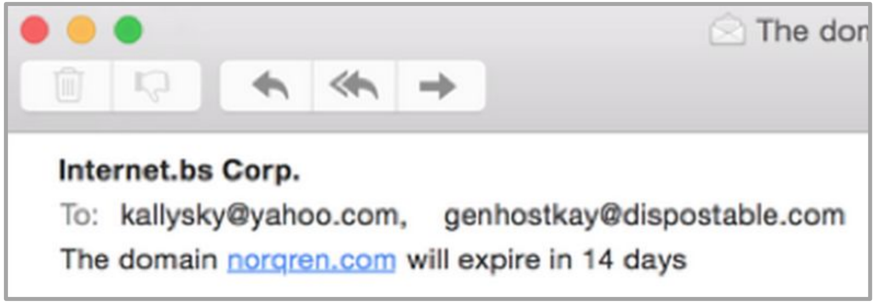
May 4, 2015 at 8:19 AM

Dear **kay lorrens**,
your domain norqren.com will expire in **14** days.

Auto-Renewal: **Disabled**

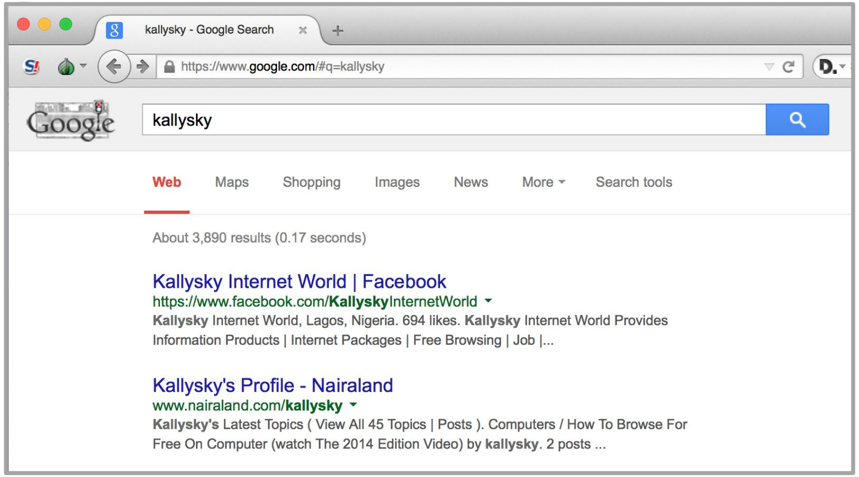
Please renew it now by following the link below:
http://www.internetbs.net/en/domain-name-registrations/AutoLogin.html?o=31-e364f44644fb1032aa0be13a7fcb7c0c&c=IcK4DHWyQX7Nn9&a=RenewalAction

If your domains have Auto-renewal enabled but you don't have enough prepaid funds, we will not Auto-renew those domains.



The dor

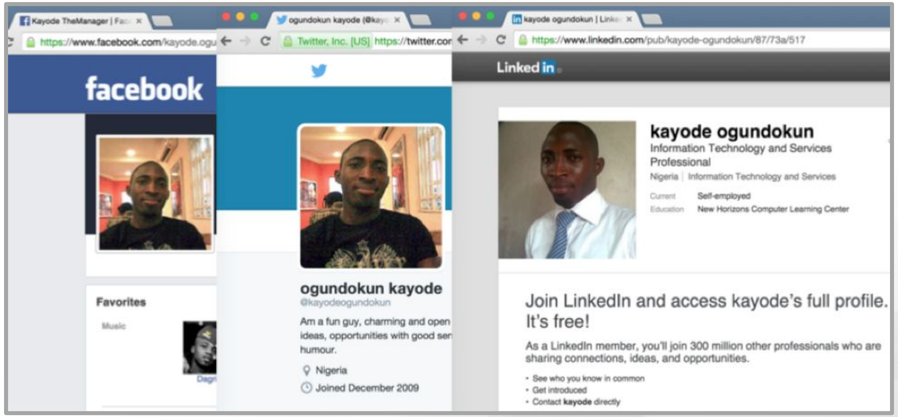
Internet.bs Corp.
To: kallysky@yahoo.com, genhostkay@dispostable.com
The domain norqren.com will expire in 14 days



About 3,890 results (0.17 seconds)

Kallysky Internet World | Facebook
https://www.facebook.com/**Kallysky**InternetWorld
Kallysky Internet World, Lagos, Nigeria. 694 likes. **Kallysky** Internet World Provides Information Products | Internet Packages | Free Browsing | Job |...

Kallysky's Profile - Nairaland
www.nairaland.com/**kallysky**
Kallysky's Latest Topics (View All 45 Topics | Posts). Computers / How To Browse For Free On Computer (watch The 2014 Edition Video) by **kallysky**. 2 posts ...



Kayode TheManager | Fac
https://www.facebook.com/kayode.ogu
facebook
Favorites
Music
Dagr
ogundokun kayode (@kay
Twitter, Inc. [US] https://twitter.com
kayode ogundokun | Linke
https://www.linkedin.com/pub/kayode-ogundokun/87/73a/517
Linked in

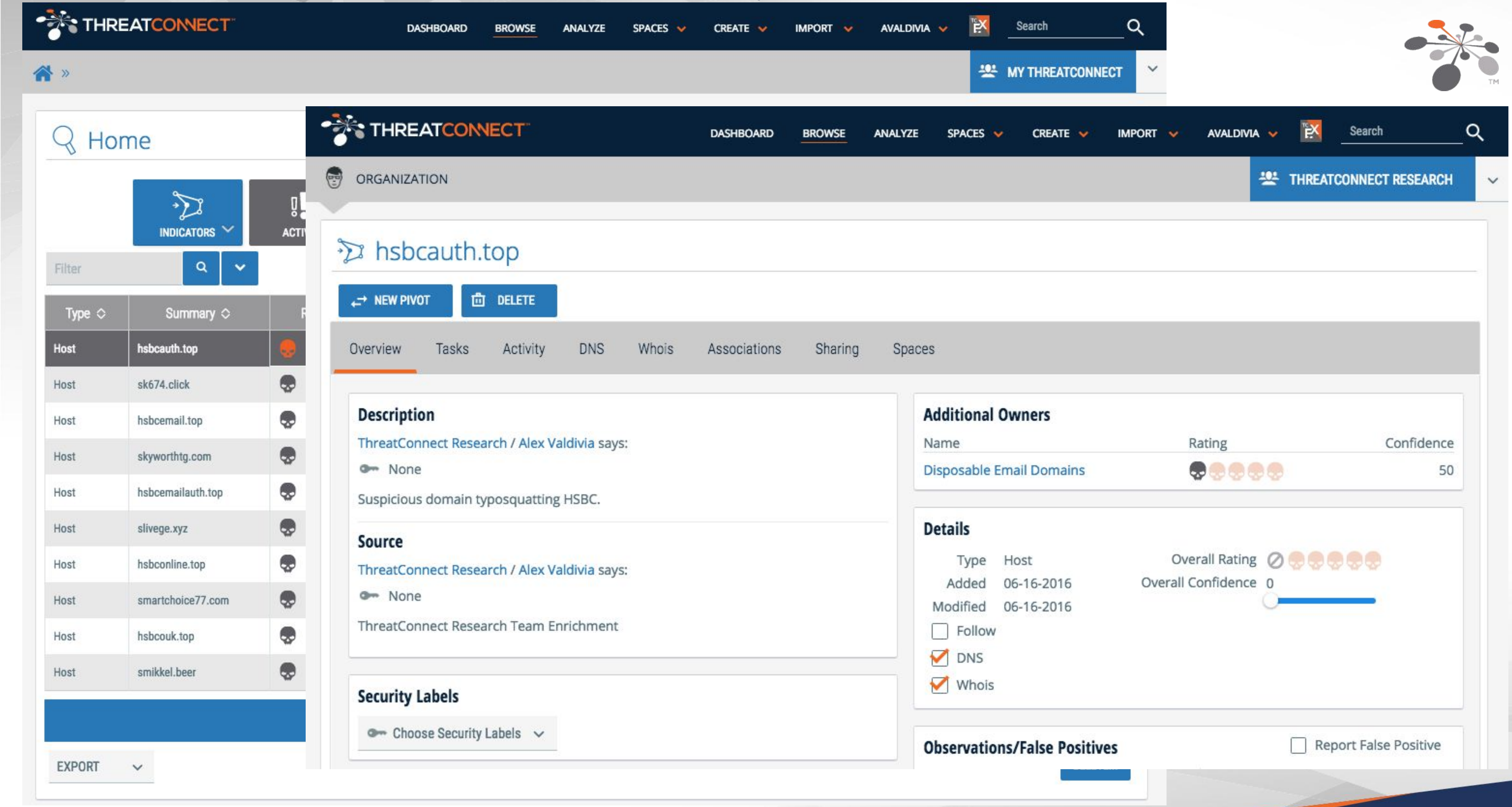
ogundokun kayode
@kayodeogundokun
Am a fun guy, charming and open ideas, opportunities with good ser humour.
Nigeria
Joined December 2009

kayode ogundokun
Information Technology and Services Professional
Nigeria | Information Technology and Services
Current Self-employed
Education New Horizons Computer Learning Center

Join LinkedIn and access kayode's full profile. It's free!

As a LinkedIn member, you'll join 300 million other professionals who are sharing connections, ideas, and opportunities.

- See who you know in common
- Get introduced
- Contact **kayode** directly



Type	Summary
Host	hsbcauth.top
Host	sk674.click
Host	hsbcemail.top
Host	skyworthtg.com
Host	hsbcemailauth.top
Host	slivege.xyz
Host	hsbconline.top
Host	smartchoice77.com
Host	hsbcouk.top
Host	smikkel.beer

hsbcauth.top

Description

ThreatConnect Research / Alex Valdivia says:

None

Suspicious domain typosquatting HSBC.

Source

ThreatConnect Research / Alex Valdivia says:

None

ThreatConnect Research Team Enrichment

Security Labels

Choose Security Labels

Additional Owners

Name	Rating	Confidence
Disposable Email Domains	●	50

Details

Type Host

Added 06-16-2016

Modified 06-16-2016

Overall Rating ⊘

Overall Confidence 0

□ Follow

☑ DNS

☑ Whois

Observations/False Positives

□ Report False Positive

Thank you!

Alex Valdivia

Twitter: @AXValdivia (#deadpool)

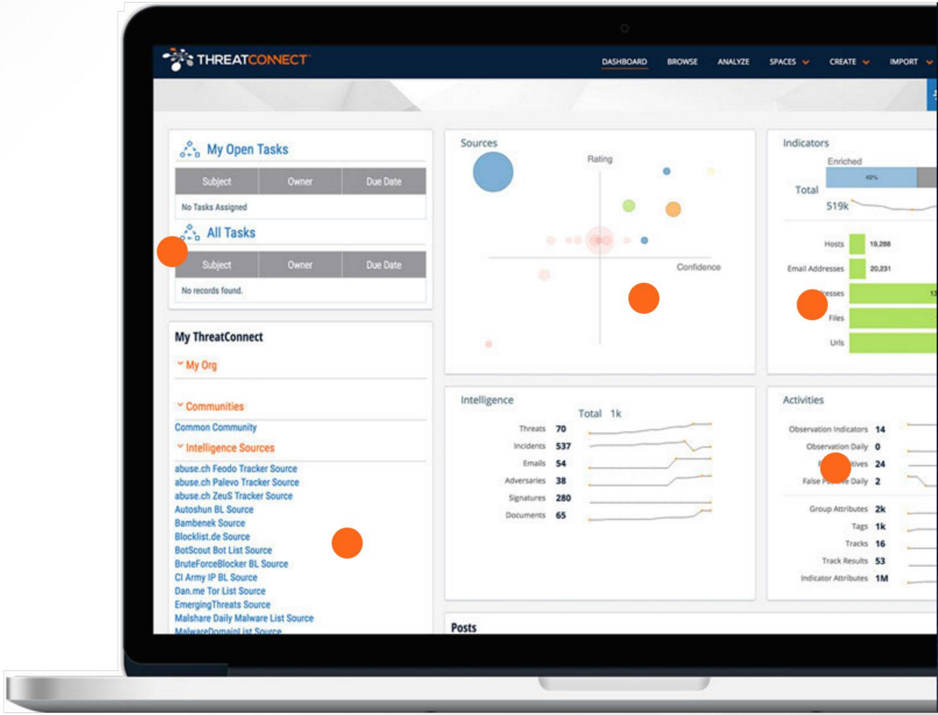
LinkedIn: linkedin.com/in/axvaldivia

ThreatConnect

https://www.threatconnect.com/free/

Twitter: @ThreatConnect

youtube.com/threatconnect1



My Open Tasks

Subject	Owner	Due Date
No Tasks Assigned		

All Tasks

Subject	Owner	Due Date
No records found.		

My ThreatConnect

My Org

Communities

Common Community

Intelligence Sources

abuse.ch Feodo Tracker Source
abuse.ch Palevo Tracker Source
abuse.ch ZeuS Tracker Source
Autoshun BL Source
Bambenek Source
Blocklist.de Source
BotScout Bot List Source
BruteForceBlocker BL Source
CI Army IP BL Source
Dan.me Tor List Source
EmergingThreats Source
Malshare Daily Malware List Source
MalwareDomainList Source

Sources

Indicators

Total 519k

Hosts	19,288
Email Addresses	20,231
...esses	
Files	
Urls	

Intelligence

Total 1k

Threats	70
Incidents	537
Emails	54
Adversaries	38
Signatures	280
Documents	65

Activities

Observation Indicators	14
Observation Daily	0
...ives	24
False Po... Daily	2
Group Attributes	2k
Tags	1k
Tracks	16
Track Results	53
Indicator Attributes	1M

Posts