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

![ThreatConnect Page Screenshot](image)

**Organization**

**Domain Name:** centozos.org.in

<table>
<thead>
<tr>
<th>Date</th>
<th>Registrant</th>
<th>Created</th>
<th>Updated</th>
<th>Expires</th>
</tr>
</thead>
</table>

**Technical Information:**

- hsonw hsonw
- bollynod ltd
- 23 hohn road, lorry drive
- 23 hohn road, lorry drive
- Lagos Lagos NIGERIA
- genhostkay@dispostable.com
  - 23408054534433

© 2016 ThreatConnect, Inc. All Rights Reserved | All material confidential and proprietary
Rombertik Case Study

Internet.bs Corp.
To: kallysky@yahoo.com, genhostskay@disposable.com
The domain norgren.com will expire in 14 days

Dear kay lorryn,
your domain norgren.com will expire in 14 days.
Auto-Renewal: Disabled
Please renew it now by following the link below:
http://www.internetservices.com/main-name-registrations/AutoLogin.html?ts=1522129404&1032a8b51a7f677b70c0a-kK4D69WQ7N66k=k=RenewalAction
If your domains have Auto-renew enabled but you don't have enough prepaid funds, we will not Auto-renew those domains.

Internet.bs Corp.
To: kallysky@yahoo.com, genhostskay@disposable.com
The domain norgren.com will expire in 14 days

Kallysky Internet World | Facebook
https://www.facebook.com/KallyskyInternetWorld
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...
 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

Details
Type: Host
Added: 06-16-2016
Modified: 06-16-2016

Overall Rating
Overall Confidence

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