The Digital Cockroach Bait Station

How to Build Spam Honeypots
Who am I?

Sr. Threat Intelligence Researcher

ThreatConnect, Inc.
Intelligence Research Team (TCIRT)

@MalwareUtkonos
Problems

• Requirements:
  • Fresh:
    • Malware samples
    • Malicious links
    • Advanced fee fraud scams

• Goal:
  • Actionable Threat Intelligence
A Rose by Any Other Name

Spam Trap = Spam Honeypot
Definition

“Spamtraps are usually e-mail addresses that are created not for communication, but rather to lure spam.”

https://en.wikipedia.org/wiki/Spamtrap
Spam Honeypot Diagram

Mailserver

Python Script

SPAM

JSON

ElasticSearch
Definitions

- **Postfix**
  - General purpose mail server (FreeBSD 10.2)
  - http://www.postfix.org/

- **JSON** (JavaScript Object Notation)
  - Machine and human readable data interchange format
  - http://json.org/

- **ElasticSearch**
  - Full-text search engine accessible via RESTful API and stores documents in JSON
  - https://www.elastic.co/products/elasticsearch
Mailserver Configuration

- Accept email sent to:
  - Any username
  - Any domain

- Prevent:
  - Bounce messages
  - All outbound email
Mailserver Configuration

1. Process all inbound email with a custom Python script
2. Store a copy of all messages for backup
Python Script

- Uses `email.parser` core module
- https://docs.python.org/3.4/library/email.parser.html
- Translates all email into JSON format
Important Email Components

Email Components

- Email
  - Header
    - Date timezone
    - Received-SPF:
    - DKIM
    - HELO/ELHO String
    - Originating IP
    - Reply-To:
    - Subject:
    - From:
    - Envelope Sender
    - Return-path:
    - X-Mailer:
    - Mailer URL
    - MIME Boundary String
    - Simhash
  - Body
    - Phone Number
    - Attachment
    - URL
    - Simhash
    - Rendered Simhash
    - Email Address
    - Text

All material confidential and proprietary
ElasticSearch

- Easy to find the data you require
- Great visualizations
Time to Bait the Trap!

- Register a domain
  - Turn on privacy!
- Configure DNS
  - Assign three IP addresses to your server
  - Create a primary and two “backup” hostnames
  - Create three DNS MX records with increasing priorities
- Generate email addresses
  - Seed them across the internet
  - Seed them on your website
  - Give them to friends to help seed
  - Maintain a database or spreadsheet of emails created and where they were seeded or to whom they were given
Registering a Domain

• Many free services - the adversary uses them, why can’t we?
• Make sure to protect your identity by using free:
  • Email service
  • Domain registration
  • DNS service
• Verify the WHOIS and DNS records don’t contain your info before seeding
• Make your username on the new server generic
DNS Records

; example.com Dumped Sun Apr 12 14:18:42 2015
;
example.com. 86400 IN SOA ns1.example.net. hostmaster.example.net. (;
               2015041212 ;serial
               10800 ;refresh
               1800 ;retry
               604800 ;expire
               86400 ;minimum
)
example.com. 86400 IN NS ns1.example.net.
example.com. 86400 IN NS ns2.example.net.
example.com. 86400 IN NS ns3.example.net.
example.com. 86400 IN NS ns4.example.net.
example.com. 86400 IN NS ns5.example.net.
mail1.example.com. 86400 IN A 123.123.123.123
mail1.example.com. 86400 IN MX 10 mail1.example.com.
mail2.example.com. 86400 IN A 125.125.125.125
mail3.example.com. 86400 IN A 127.127.127.127
mail2.example.com. 86400 IN MX 20 mail2.example.com.
mail3.example.com. 86400 IN MX 30 mail3.example.com.
Generate Email Addresses

• Random Name Generators
  • http://www.behindthename.com/random/
  • http://random-name-generator.info/
  • http://www.namemesh.com/company-name-generator
  • http://online-generator.com/name-generator/business-name-generator.php

• Scrabble word finders
  • http://www.wordfind.com/
  • http://wordfinder.yourdictionary.com/

• Anagram solvers
  • http://wordsmith.org/anagram/
  • http://www.wordplays.com/anagram-solver
Now You Have Spam!

あなたのお気に入りの女性からのメールを受け取る!!


あとは、2人が決める待ち合わせの場所まで一直線です！
あなたも人生が変わるような出会いを体験してください！！

All material confidential and proprietary
http://www.threatconnect.com/blog/

Thanks!

@MalwareUtkonos

@ThreatConnect