

The background features a complex network of thin grey lines and dots, forming a web-like structure. Several triangles of various sizes are scattered across the image, some with solid black dots at their vertices. The overall aesthetic is minimalist and technical.

# **Gotta Catch 'Em All**

## **Domain Generation Algorithms**

---

Nathaniel Beckstead - Security Unprofessional

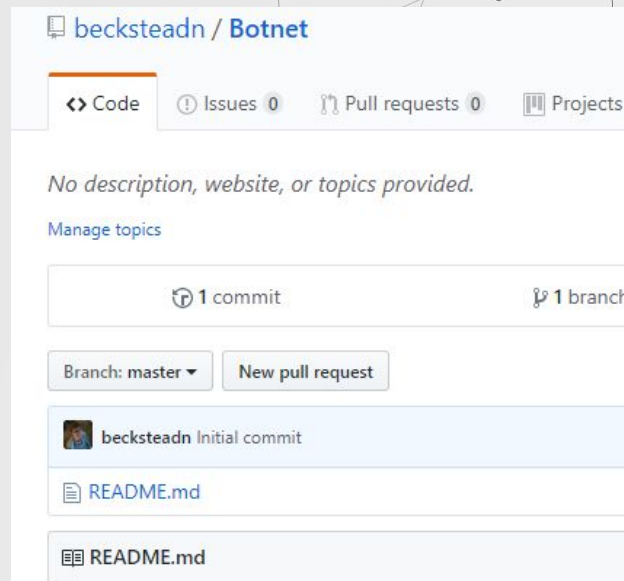


# Nathaniel Beckstead

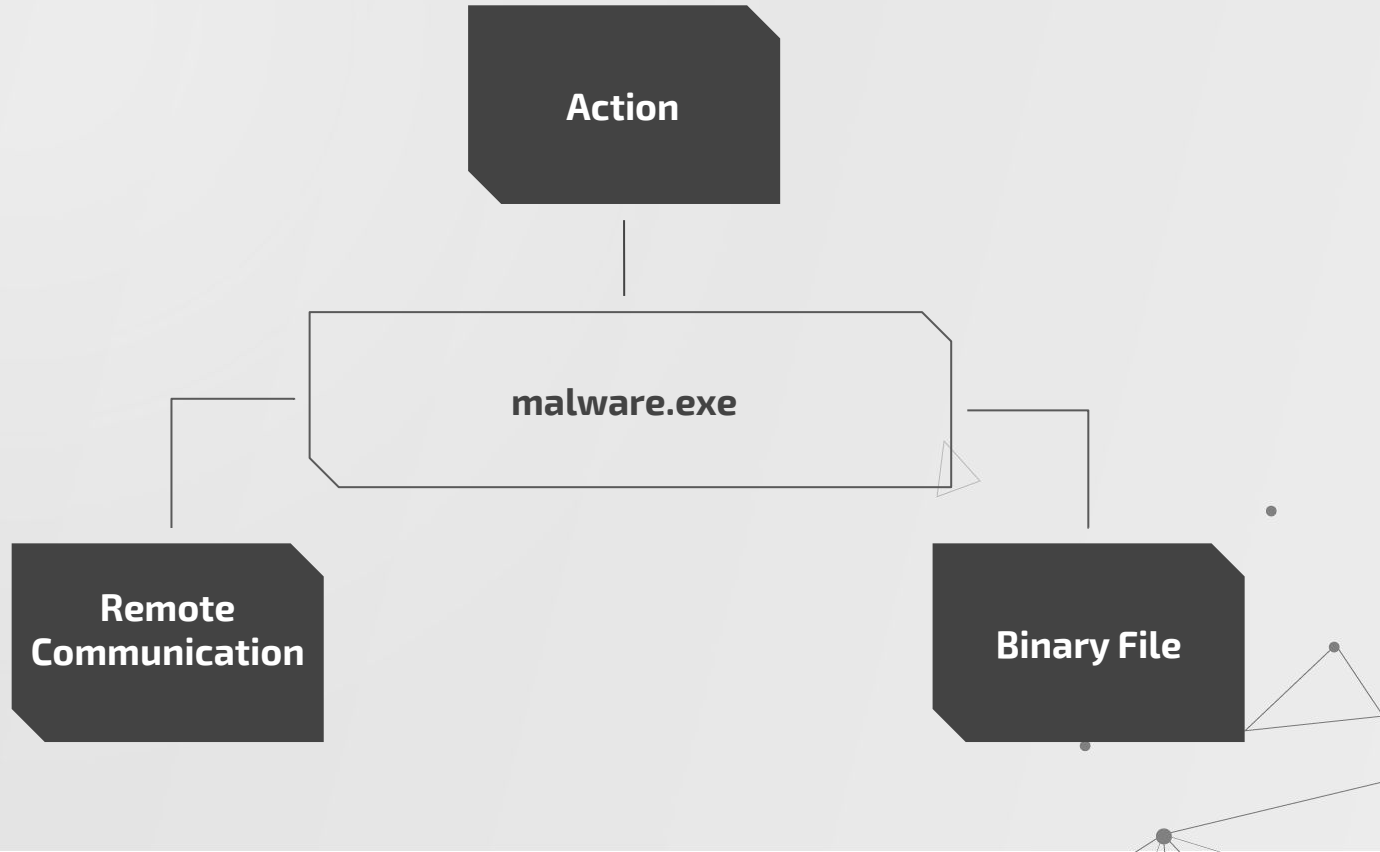
Blue teamer by day

Red teamer by night

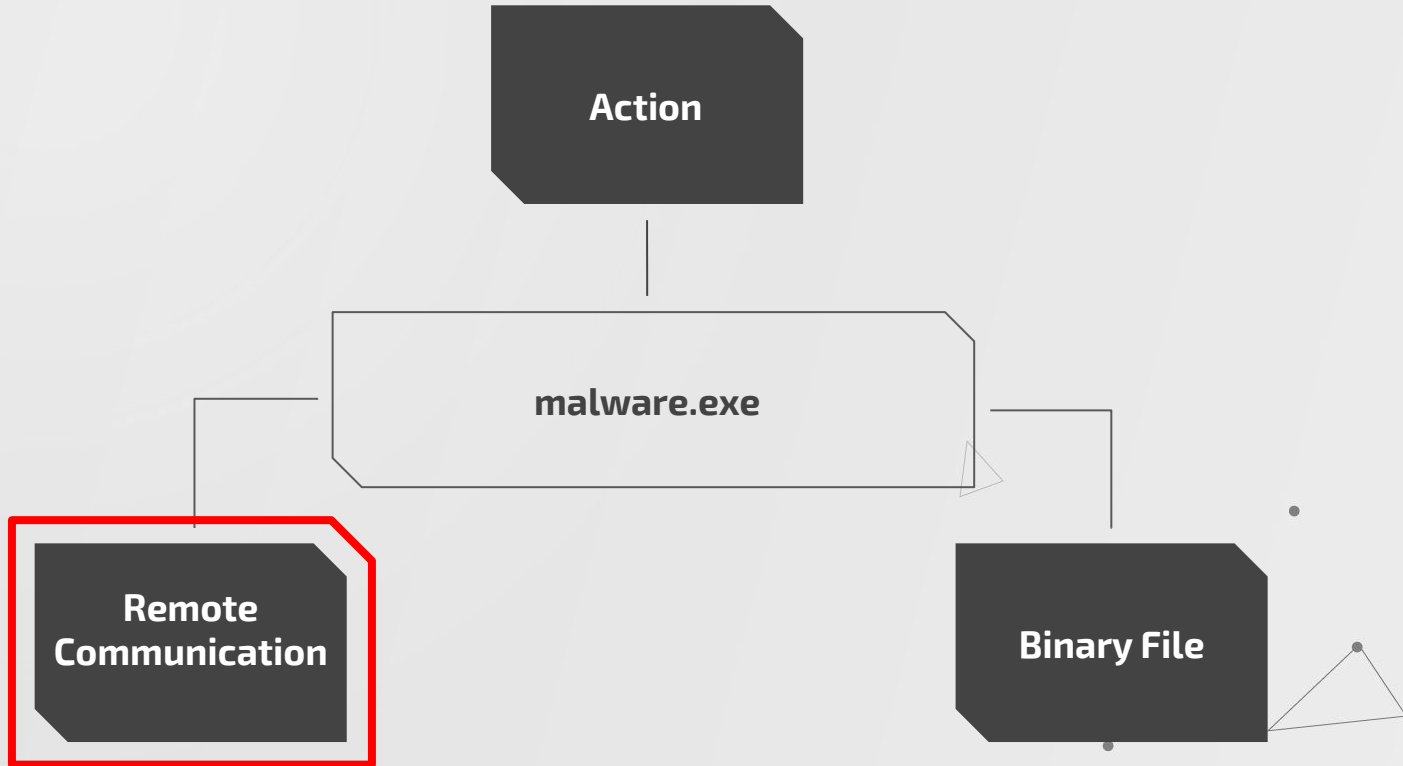
@scriptingislife  
<https://scriptingis.life>



# Anatomy of Malware



# Anatomy of Malware



---



# Creative Seeds

- US dollar to Japanese yen exchange rate
- Top hashtag on Twitter
- Temperature in Rio de Janeiro



# Why?

- Diversion
  - ◀ Overload blue teamers with domains to block
- Hide from static analysis
  - ◀ Can't just run `strings` and find the C2 domain



# Conficker

## Conficker.a & Conficker.b

- Computer worm in 2008
  - ◀ Spread via MS08-67
- 250 domains a day
  - ◀ 5 TLDs

## Conficker.c

- 50,000 domains a day
  - ◀ 110 TLDs
  - ◀ Shortened to 4-9 characters to avoid heuristics
    - ◀ Could collide with legit domains causing a DDOS
- Attempt to contact 500 domains a day

## Response

- Registrars blocked registration of possible domains





# Defense

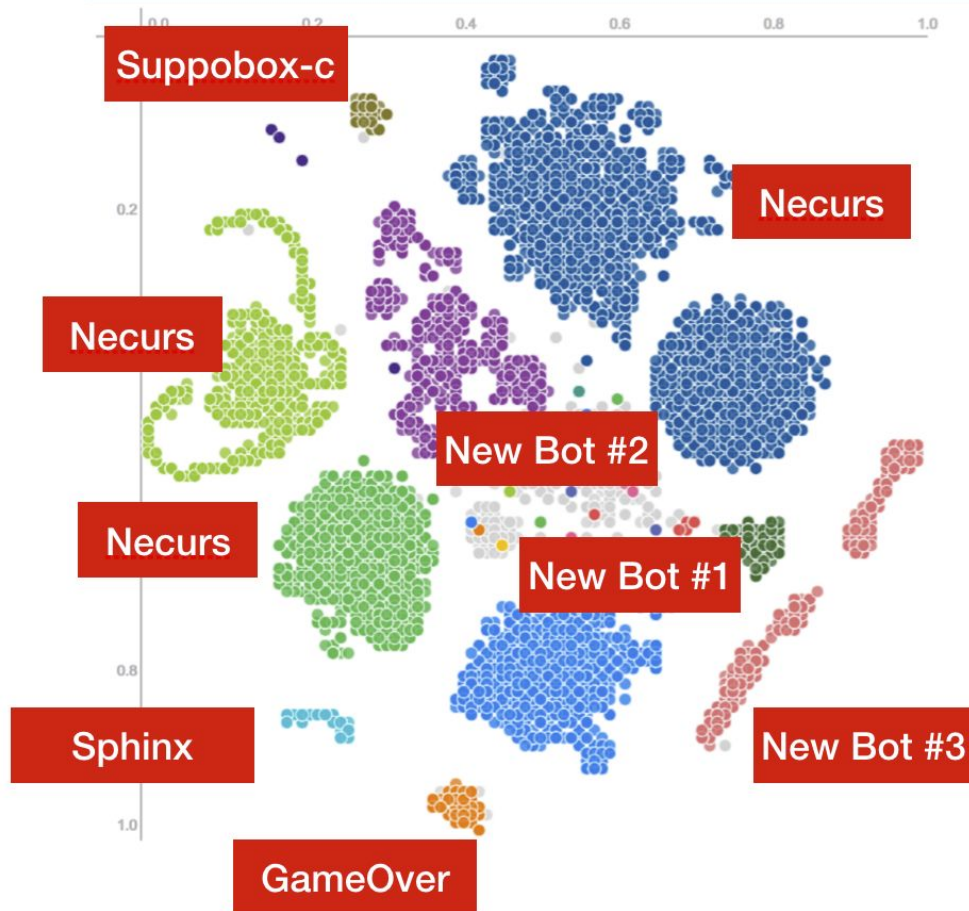
**Network Intrusion Prevention** - Detect C2 signatures

**DNS Sinkhole** - Respond NXDomain all possible domains

**Threat Intelligence** - Block newly registered domains

**Machine Learning** - N-grams, linguistics, probability????





< 2017-07-01 00:00 > ☒ AD / Emerging

First available: 2016-03-27 00:00

Last available: 2017-07-21 16:00

Domain  Search

#### Domain info:

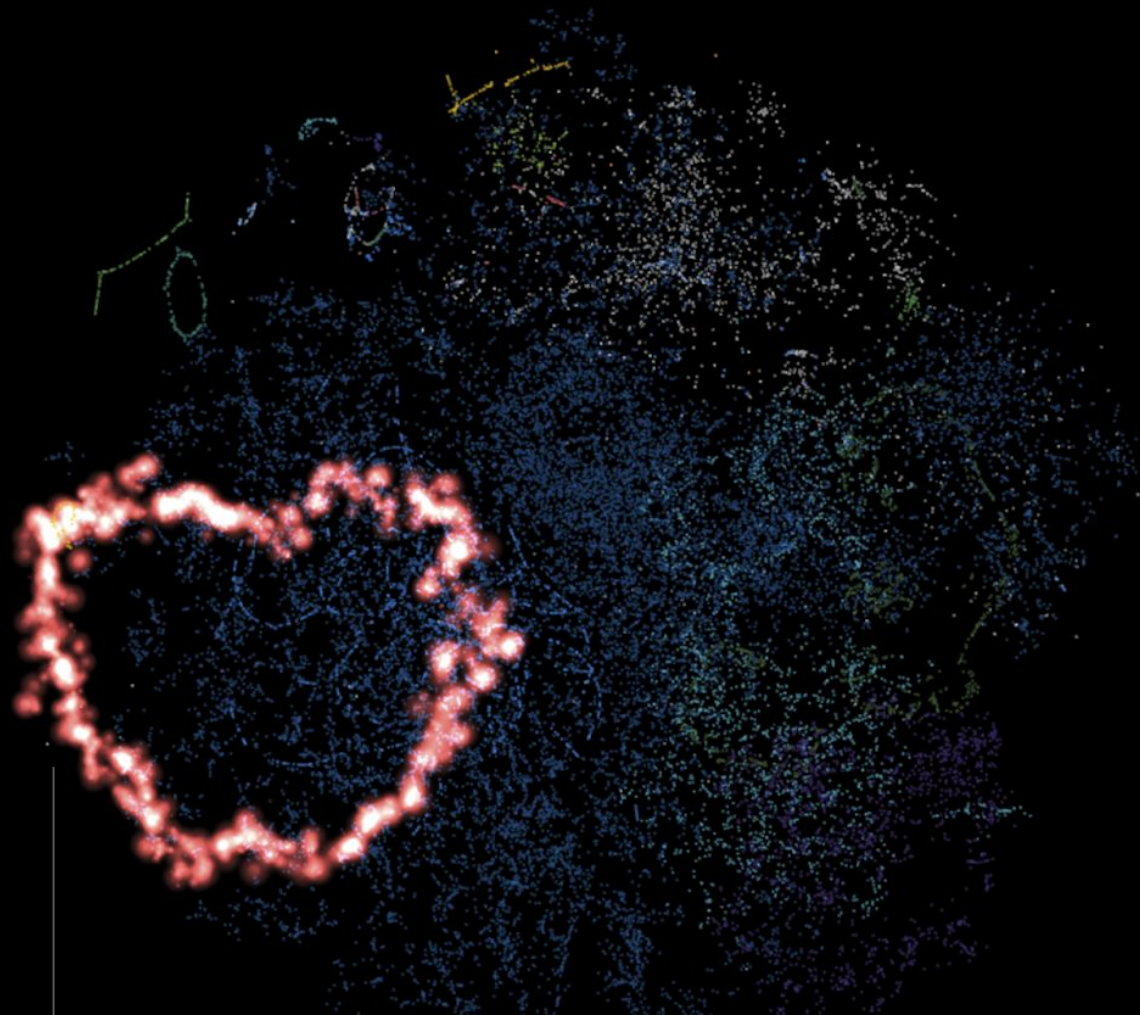
Domain: thisthousand.ru.,1  
Cluster: 4 Query count: 4 ISP count: 2

#### Cluster 4 info:

|                            |  |
|----------------------------|--|
| TLD Dist: ru.:71           | Predicted DGA: suppobox-c                    |
| Max Core Length: 21        | Found DGA count: 71                          |
| Median Core Length: 13     | Query Type Dist: 1:71                        |
| Average Core Length: 14.06 | NZRC Average: 0.99                           |
| Min Core Length: 8         | NZRC Median: 1                               |
| Member Count: 71           | Guess DGA: suppobox-c:1.00000 necurs:1.00000 |
| Query Count: 12071         | locky_v1:0.64789                             |
| Client Count: 172          | locky:0.64789 necurs-v2:0.63380              |
| ISP Count: 7               | gameover-p2p:0.56338                         |
|                            | vawtrak:0.49296                              |
|                            | prosliekfan:0.49296                          |
|                            | modpack:0.43662                              |
|                            | nymaim:0.43662                               |
|                            | feedo:0.12676                                |
|                            | rovnix:0.12676                               |

#### Members:

alexandrinaanastasia.ru.,1  
ariveloud.ru.,1  
arivestock.ru.,1  
bartholomewandriana.ru.,1  
bartholomewethelbert.ru.,1  
beauregardandriana.ru.,1  
beauregardethelbert.ru.,1  
beauregardmontgomery.ru.,1  
christiananormanson.ru.,1  
christianasherwood.ru.,1  
dreamnews.ru.,1  
dreamread.ru.,1  
dulcehellakingslev.ru.,1



**Cluster name:** `gameover_p2p`

**Cluster ID:** 14

**Cluster size:** 1,001 domains

**Primary usage:** Financial fraud

**Sample cluster domain names:**

|                                    |   |
|------------------------------------|---|
| ucxopzovsgifwcamsgzdhmptljce.biz.  | A |
| ijmducsxfyauybmfmtwbyor.com.       | A |
| qslrcdatmbdmwgpxgihltu.net.        | A |
| dyqclknkfbibiaudmprylvgpjfixg.com. | A |
| pbkjhhwkvCIFUWAEUOLJYTHQNZFI.NET.  | A |
| pgiswwgswbukkfwfedcap.com.         | A |
| rkmzdaqmhqdlvyhinschjvoznvd.ru.    | A |
| hmcqhtglswdmkvqjneagakndzhxk.org.  | A |
| gugqvzdhaprzpgqxlfgecydyht.com.    | A |
| swqpboqovqgbxoxkmbdhrwnr.biz.      | A |

A high-contrast, black and white photograph of a computer circuit board. The central focus is a large, square integrated circuit (chip) with a textured surface. To its right, a multi-pin connector is visible. The board is populated with various other components, including smaller chips and capacitors. The background shows the complex layout of the board with numerous traces and connectors. The word "Demo" is overlaid in a bold, white, sans-serif font on the left side of the image.

**Demo**

The background of the slide is a light gray with a complex network of thin black lines and dots. These lines and dots form various geometric shapes, including triangles and polygons, some of which are filled with a darker gray. The overall effect is a modern, tech-inspired geometric pattern.

# Thanks!

# RESOURCES

## Websites

- [MITRE ATT&CK Technique](#)
- [Unit 42 - Threat Brief: Understanding Domain Generation Algorithms \(DGA\)](#)
- [Akamai - A Death Match of Domain Generation Algorithms](#)
- [SRI International - An Analysis of Conficker](#)

## PDFs

- [Cybereason Lab Analysis - Dissecting Domain Generation Algorithms, Eight Real World DGA Variants](#)
- [DGAs in the Hands of Cyber-Criminals - Examining The State of The Art In Malware Evasion Techniques](#)

## Twitter Accounts

- [@DGAFeedAlerts](#)

