Gotta Catch ‘Em All

Domain Generation Algorithms

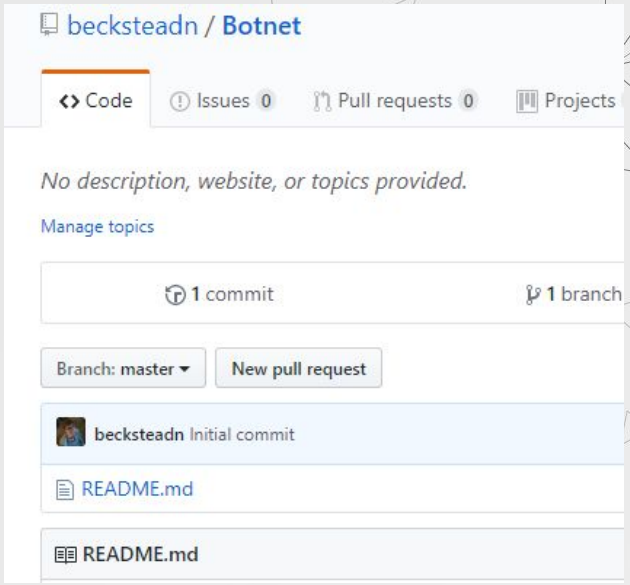
Nathaniel Beckstead - Security Unprofessional

Nathaniel Beckstead

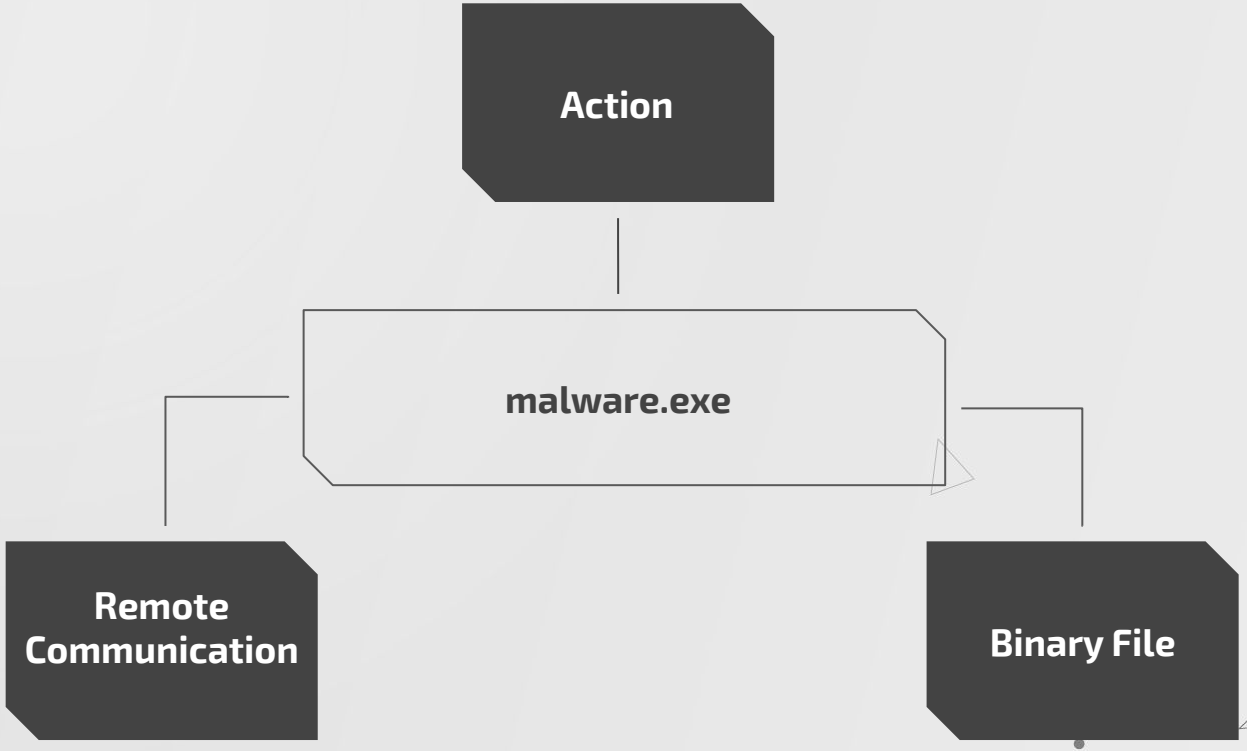
Blue teamer by day

Red teamer by night

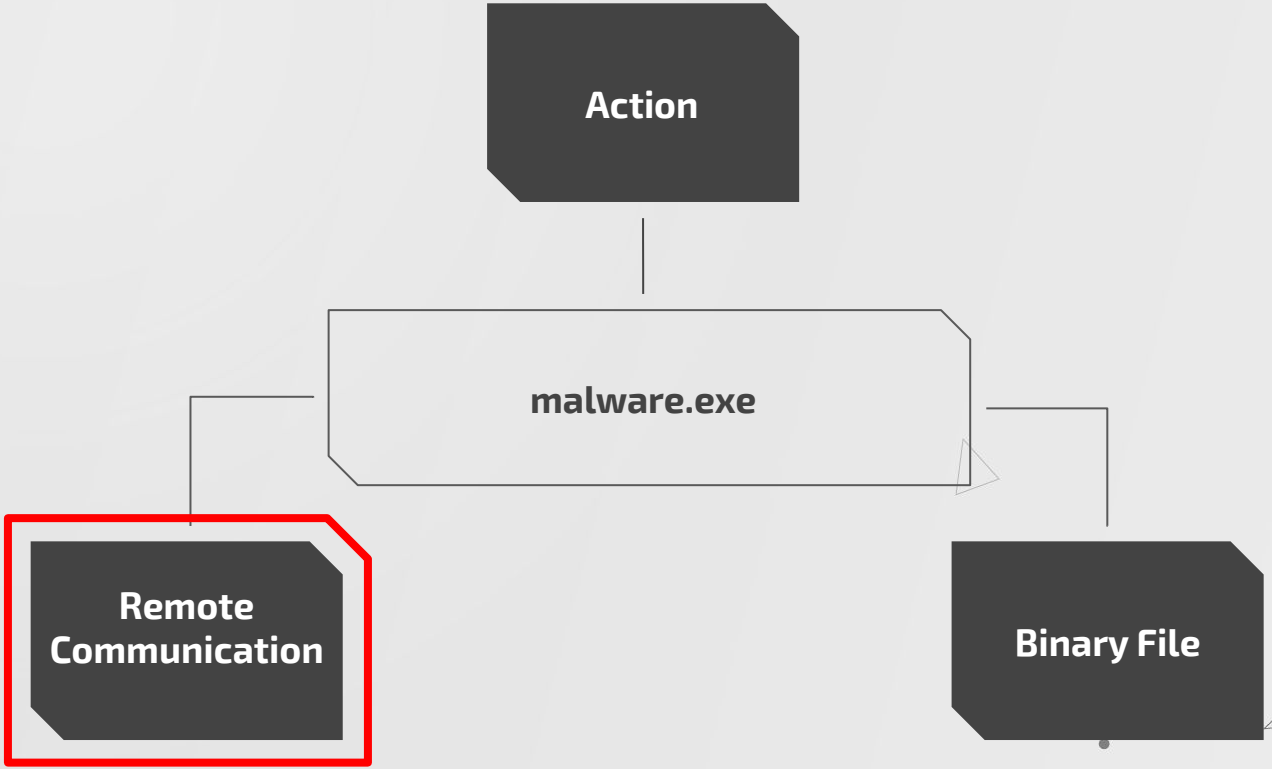
@scriptingislife
https://scriptingis.life



Anatomy of Malware



Anatomy of Malware



Domain Generation Algorithm

Routinely calculate the domain to use for C2 communication.

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

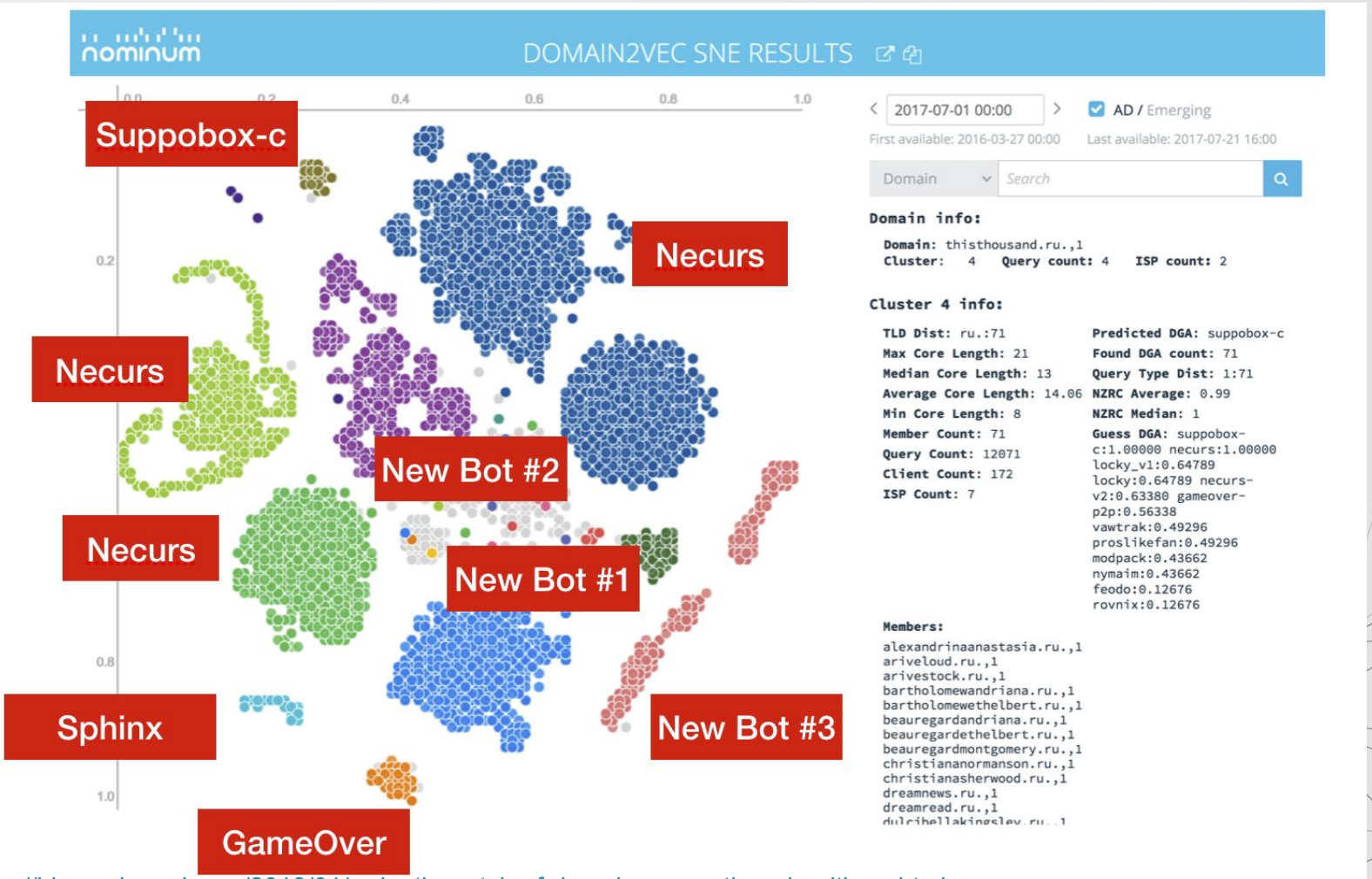
Defense

Network Intrusion Prevention - Detect C2 signatures

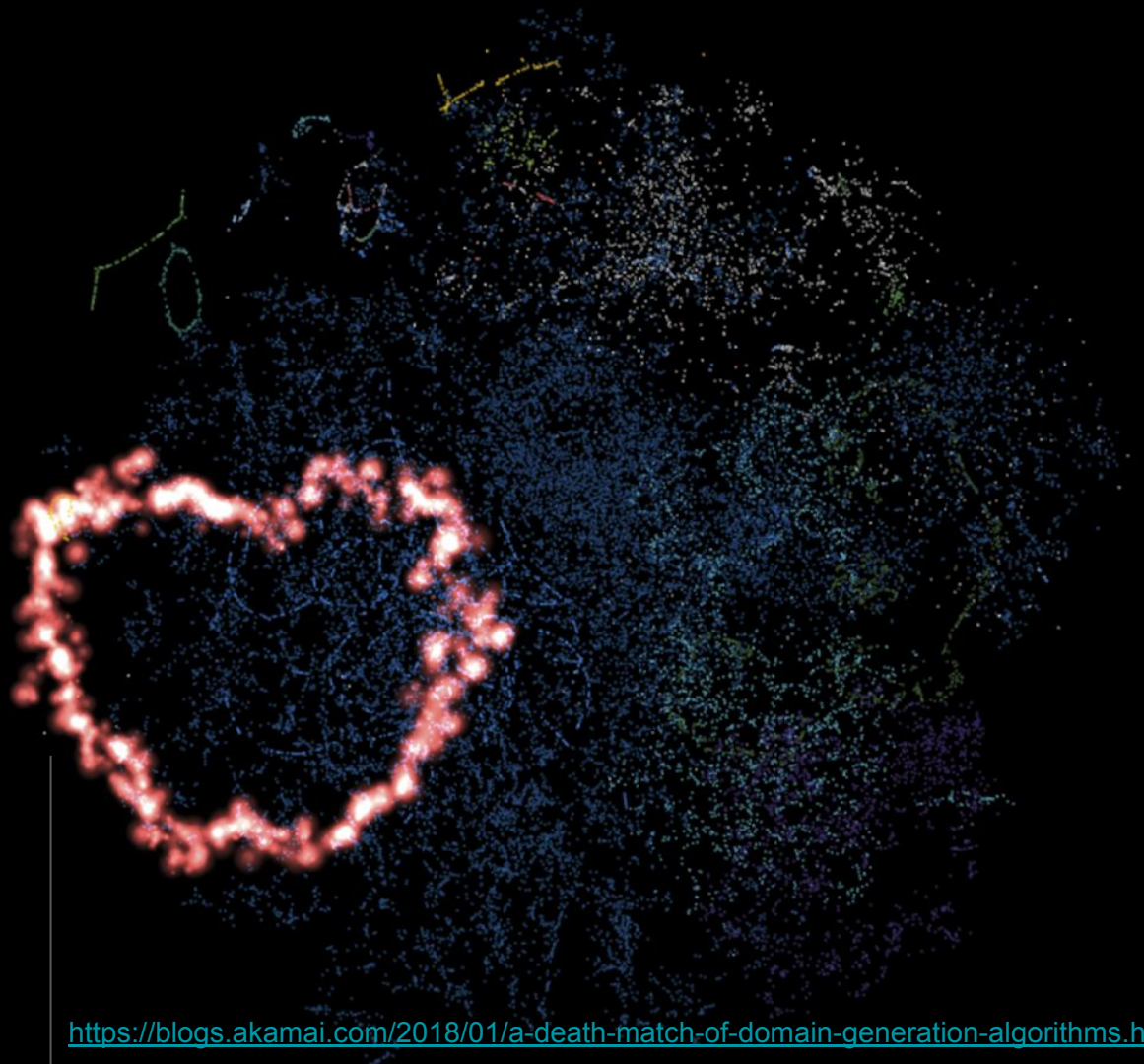
DNS Sinkhole - Respond NXDomain all possible domains

Threat Intelligence - Block newly registered domains

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



https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html



Cluster name: gameover_p2p

Cluster ID: 14
Cluster size: 1,001 domains
Primary usage: Financial fraud

Sample cluster domain names:

ucxopzovsgifwcamsgzdhhmptljce.biz.	A
ijmducsxfyauybmfmtwbyor.com.	A
qslrcmdatmbdmwgpxgihltu.net.	A
dyqclknkfbebiaudmprylvgpjfixg.com.	A
pbkjhhwkvcifuwaeuouljythqnzfi.net.	A
pgiswwgswbukkfwfedcap.com.	A
rkmzdqamhqdlvyhinschjvoznvd.ru.	A
hmcqhtglswdmkvqjneagakndzhxk.org.	A
gugqvozdhaprzpgqxlfgecydyyht.com.	A
swqpboqoqvgpbxoxkmbdhqrwnr.biz.	A

https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html

Demo

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