Real-Time Detection of Fast Flux Service Networks

Cybersecurity Applications and Technology Conference for Homeland Security

March 3, 2009

Washington, DC

milcord

Alper Caglayan
Mike Toothaker
Dan Drapeau
Dustin Burke
Gerry Eaton

milcord

info@milcord.com (781) 839-7138

Presentation Outline

- Problem
- Need
- Solution
- Results
- Related work
- Conclusions

News

- Waledac **botnet** is active again with malicious money saving website **...**

  SC Magazine UK - 1 hour ago

- Conficker **botnet** ready to be split, sold

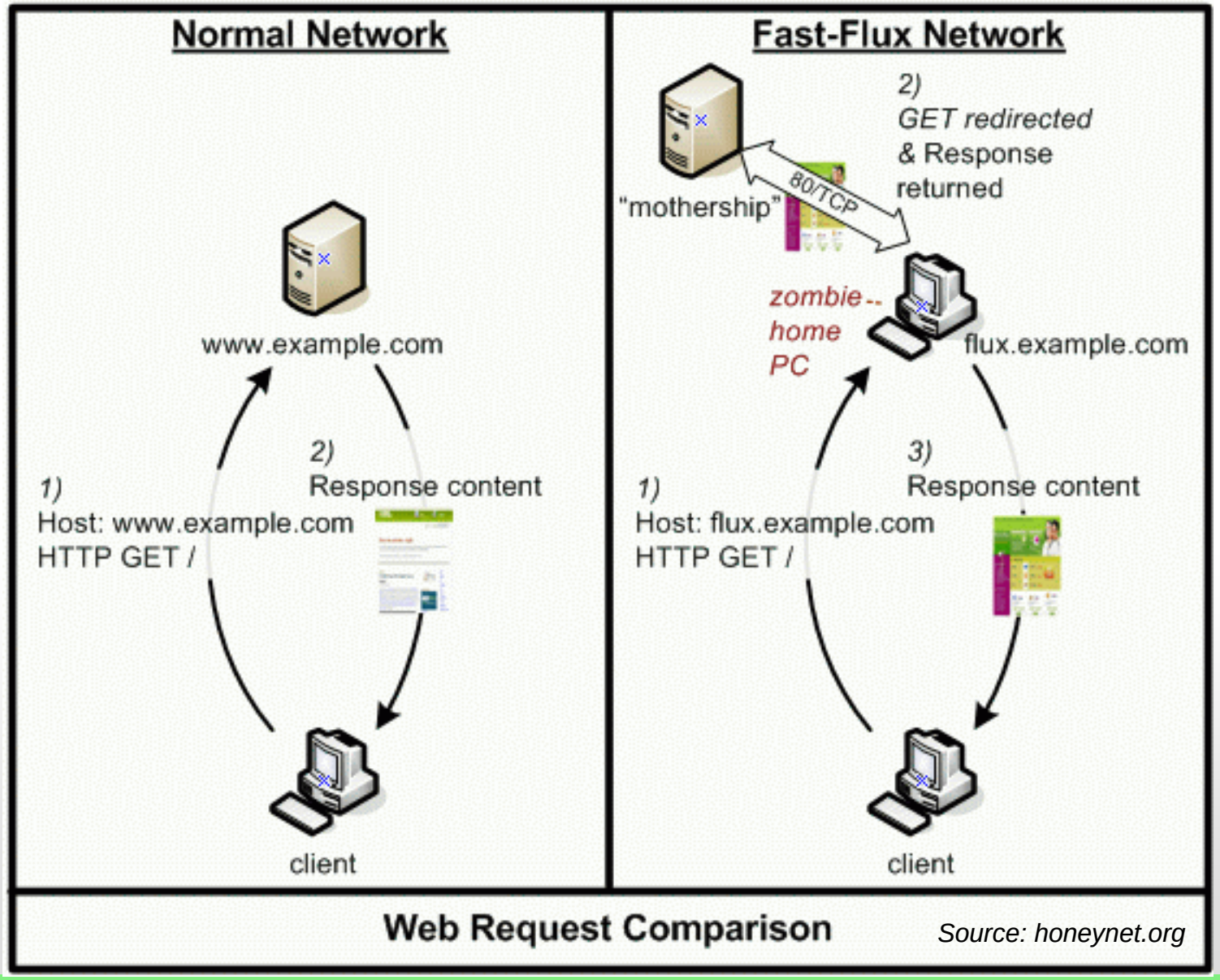
  SearchSecurity.com - Feb 26, 2009

- Malware Writers Use Multiple **Botnets** to Spread Valentine's Day **...**

  eWeek - Feb 11, 2009

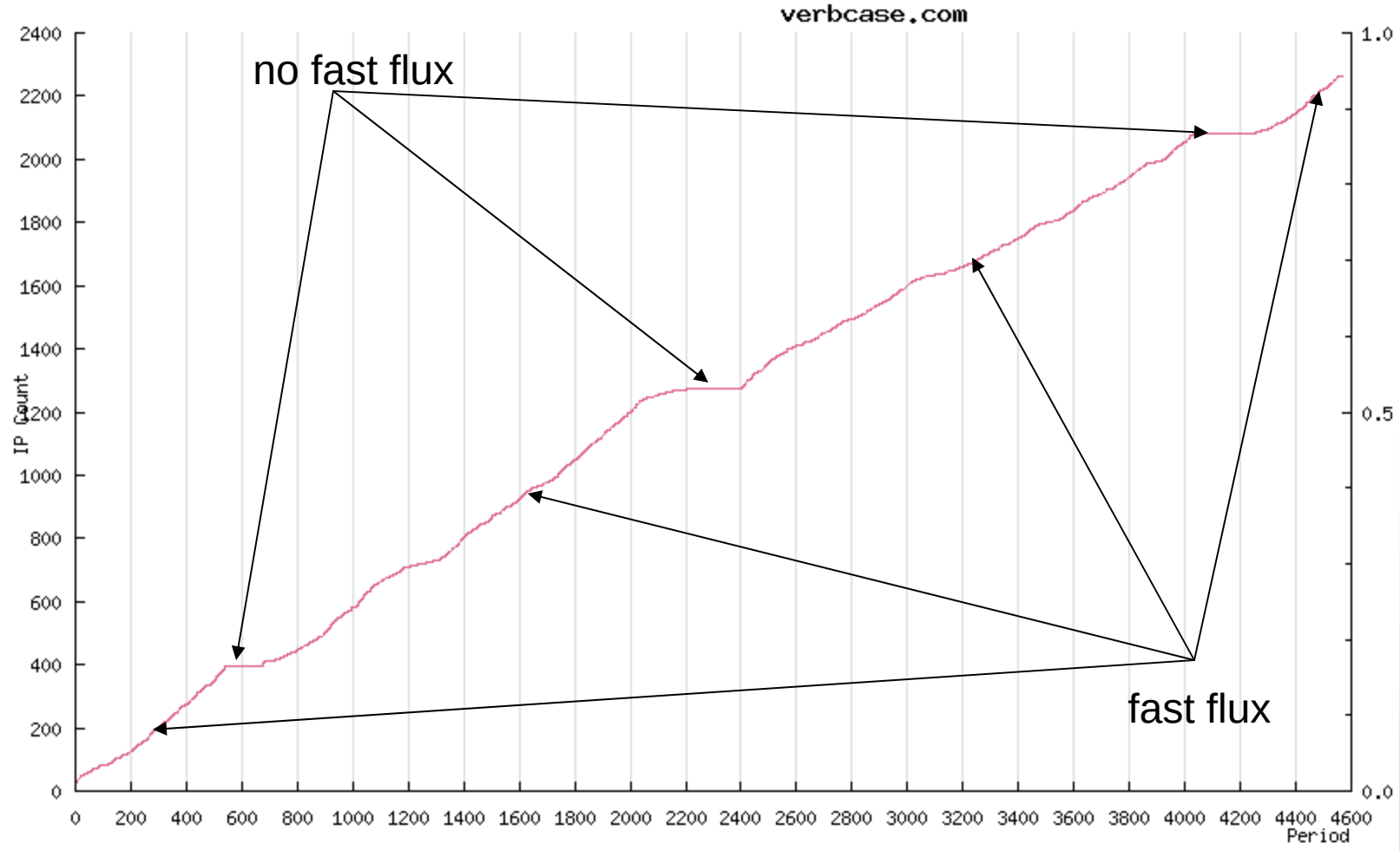
Fast Flux Problem

- ICANN GNSO definition:
  - rapid and repeated changes to host and/or name server resource records, which result in rapidly changing the IP address to which the domain name of an Internet host or name server resolves
- Malicious use:
  - Spam campaigns, phishing, malware delivery, DDoS attacks
- Technical challenge:
  - monitoring changes to DNS records
  - classification of historical behavior
  - real time detection
  - differentiation from legitimate behavior



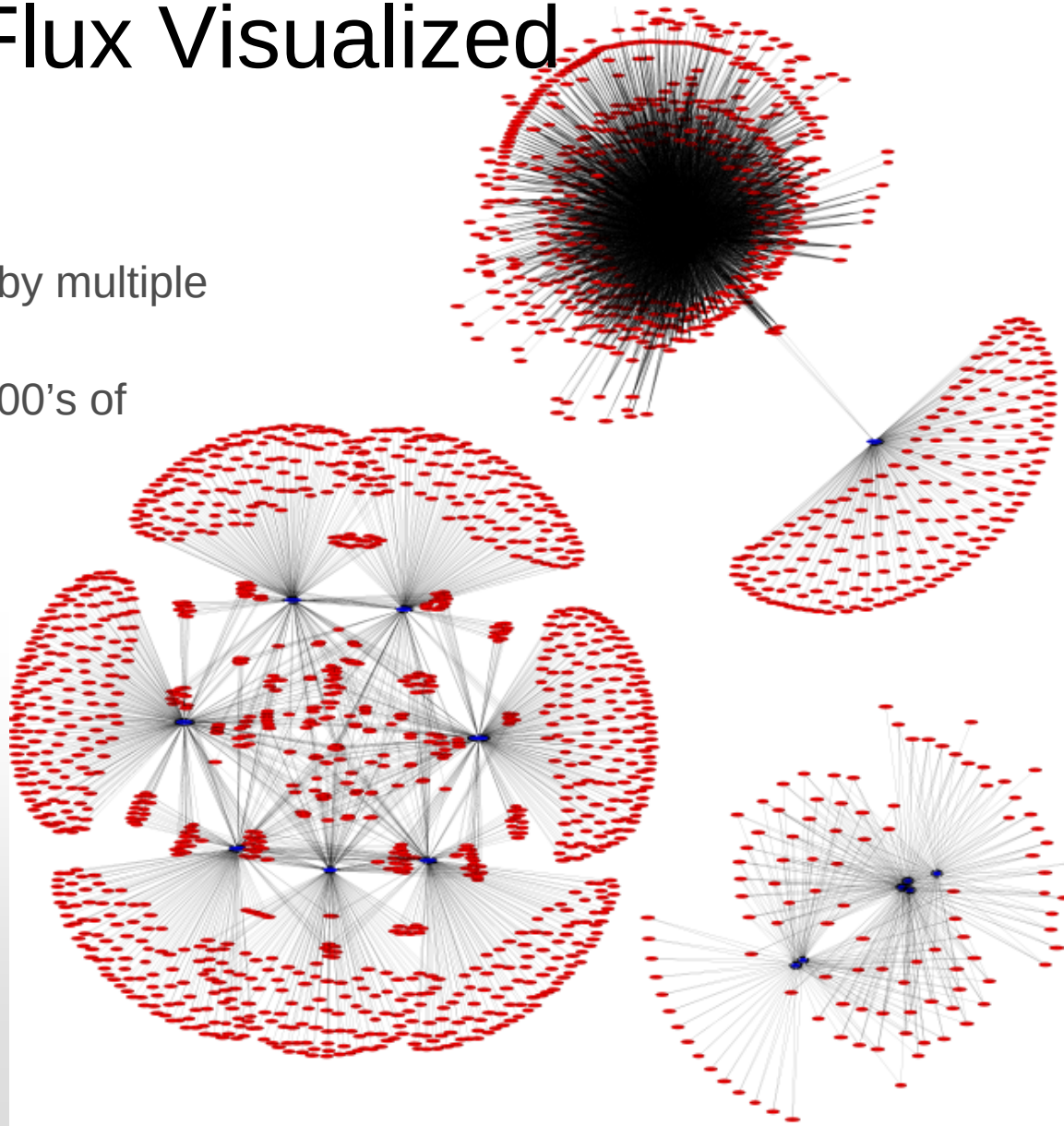
Source: honeynet.org

Fast Flux Behavior



FastFlux Visualized

- "*Guilt-by-association*"
  - Infected nodes are shared by multiple FastFlux domains
  - Drones participate 10's – 100's of domains



FastFlux domain

Infected drone IP

Source: December 31st, 2008 by Jaime Blasco

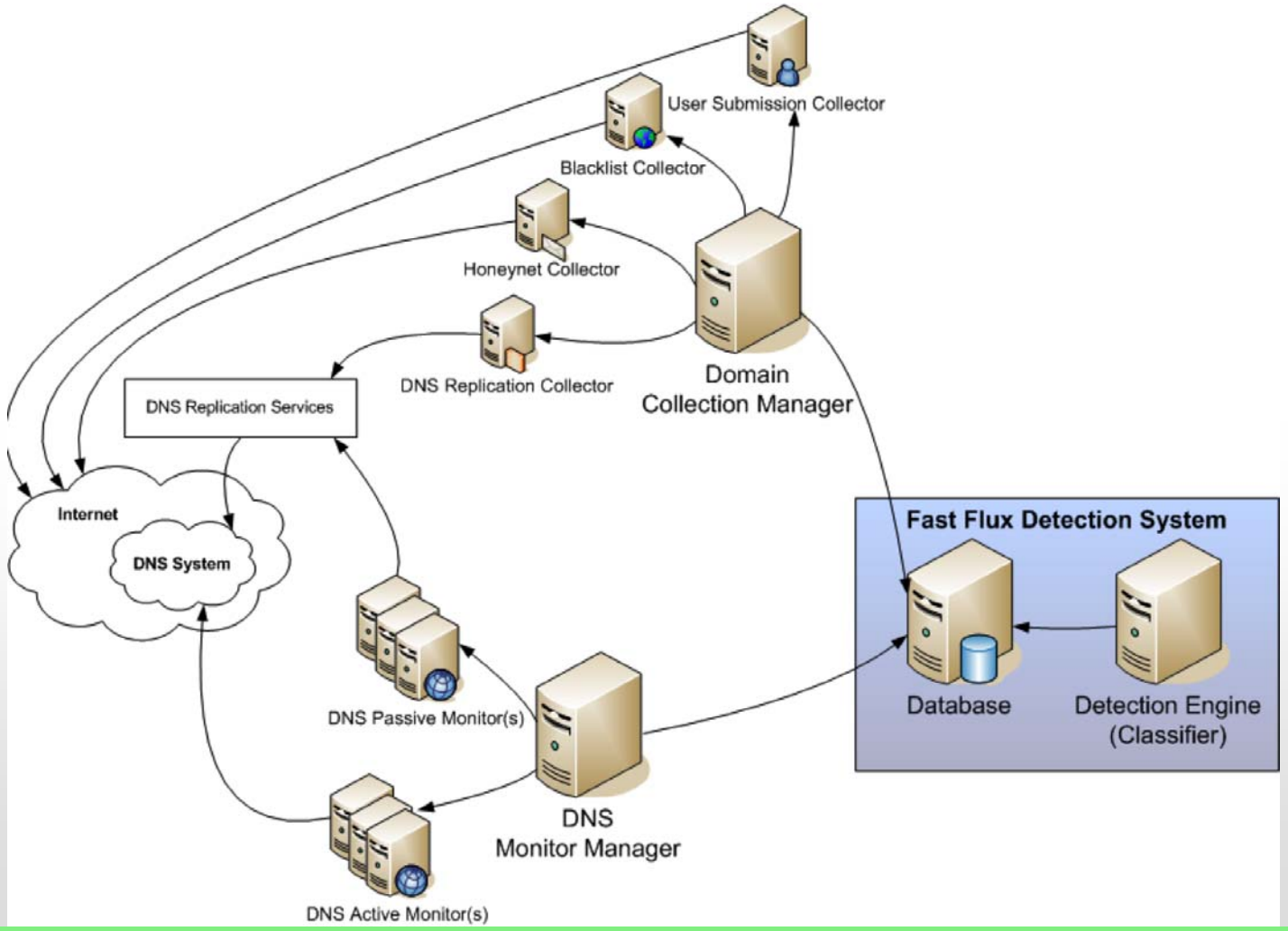
Need

- Blacklists
  - faster detection before disappearance
- Registrars
  - evidence for domain removal
- ISPs
  - mitigation support for customers
- Enterprise
  - alerts for security event management
- Law enforcement
  - solid evidence for prosecution

FastFlux Service Monitor

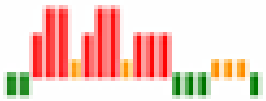
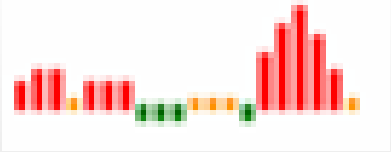
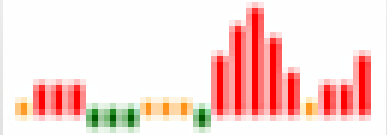
- Scheduler
  - Supports multiple concurrent processes for domain testing
- Detection and classification
  - Behavioral indicators from DNS records
  - Bayesian classifier domain IPs → single flux
  - Bayesian classifier nameserver IPs → double flux
- Application logic
  - Analytics, reporting, domain management (e.g. dead domains) …
- Notification services
  - RSS …
- Distributed Architecture Design
  - Support batch processing and incremental learning automation

FFM Architecture



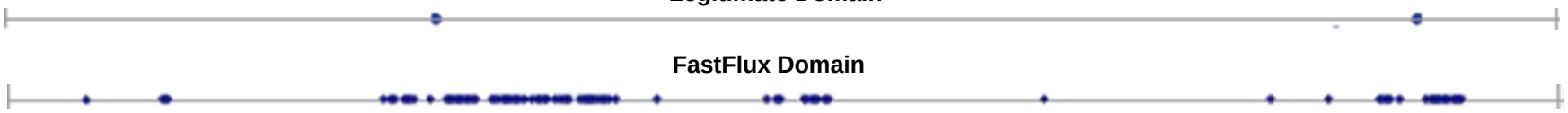
Fast Flux Activity Index

safecause.com

1:55 pm	
1:58 pm	
2:01 pm	
2:04 pm	
2:07 pm	

Footprint Index

Legitimate Domain



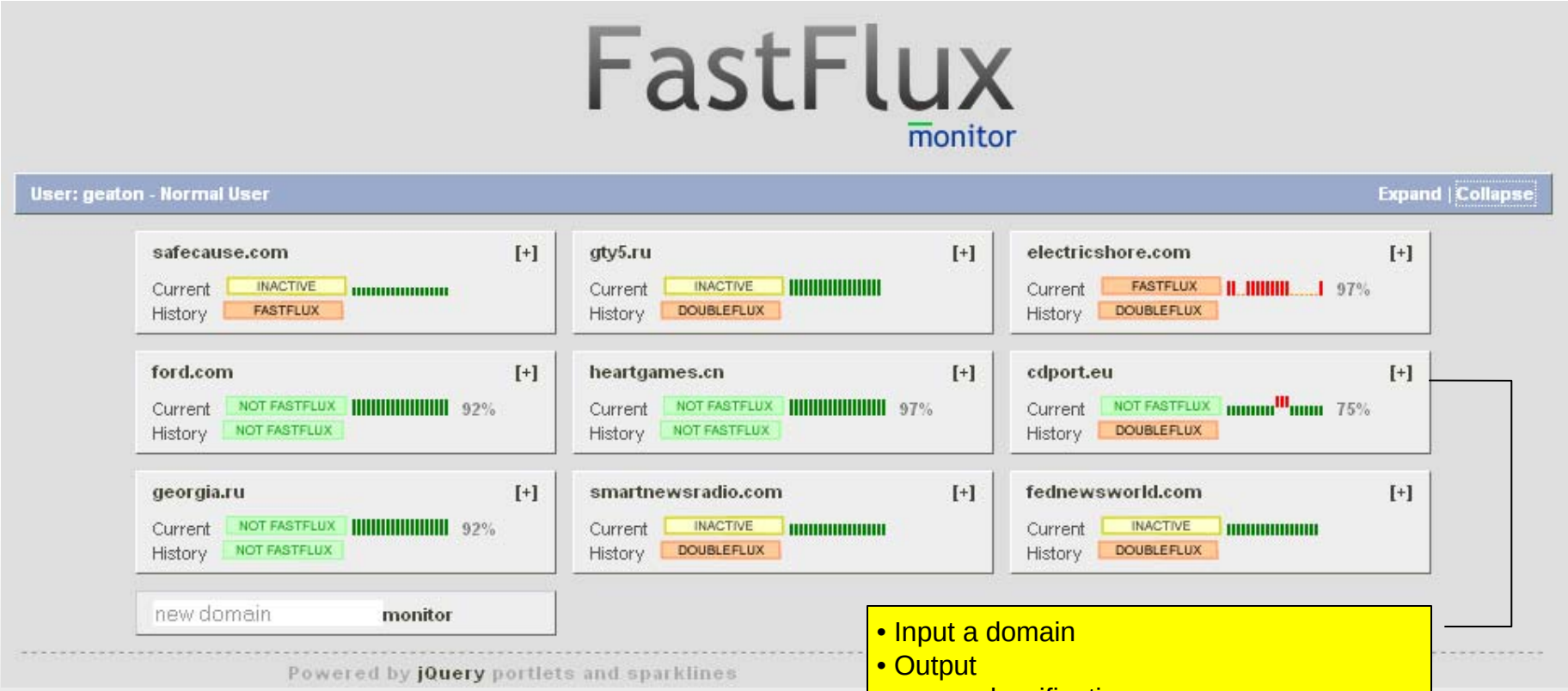
FastFlux Domain

FastFlux Domain's Geographic Footprint

TTL Index

TTL	Fast Flux Domain	High Availability Site
20		ironport.com
60	mp3for-you.com	att.com
120	safecause.com, electricshore.com, towardplain.com	
180		akamai.net
300	entryrxshop.com	google.com, yahoo.com
600	gty5.ru	
3600		microsoft.com

FF Monitor



- Input a domain
- Output
  - classification
  - confidence score
  - summary visualization
  - details
- Real-time and Database support

Nameserver Report for
electricshore.com

Nameservers

Current

Nameserver	Activity	Activity Index	Confidence
ns0.justlikehollywood.com	NOT FASTFLUX		98.5 %
ns0.greatniceprice.com	NOT FASTFLUX		98.5 %
ns0.wholikeguide.com	NOT FASTFLUX		66.1 %
ns0.likenewautosdirect.com	NOT FASTFLUX		98.5 %

History

Nameserver	Activity	Confidence History	Fast Flux Observed
ns0.justlikehollywood.com	FASTFLUX		26.3 %
ns0.greatniceprice.com	FASTFLUX		31.1 %
ns0.wholikeguide.com	FASTFLUX		51.4 %
ns0.likenewautosdirect.com	FASTFLUX		26.6 %
ns3.electricshore.com	FASTFLUX		99.8 %
ns2.electricshore.com	FASTFLUX		99.8 %
ns1.electricshore.com	FASTFLUX		99.8 %
ns4.electricshore.com	FASTFLUX		99.8 %

FF Monitor Analytics Report

Analytics

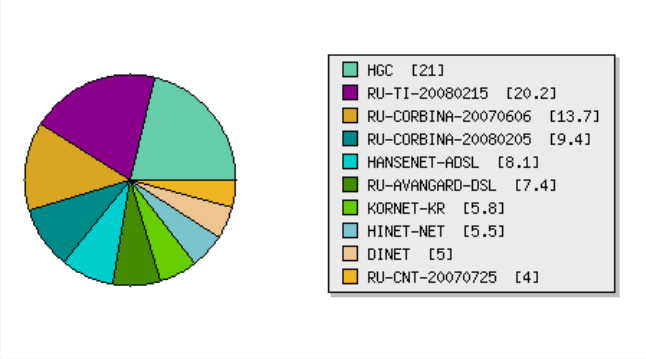
Analysis of electricshore.com's IP Addresses

This section analyzes the attributes of all IP addresses that have at least on one occasion been associated with the domain electricshore.com.These IP addresses are likely to be botnet drones (i.e. zombies).

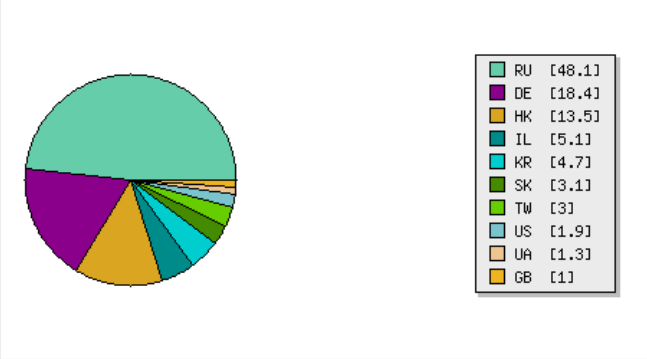
This is a medium fast flux service network with a fast rate of growth.

The charts below show the ISPs and countries hosting the drones used by this fast flux service network and the network's growth over the surveillance period.

Top 10 ISPs hosting electricshore.com's drone IPs



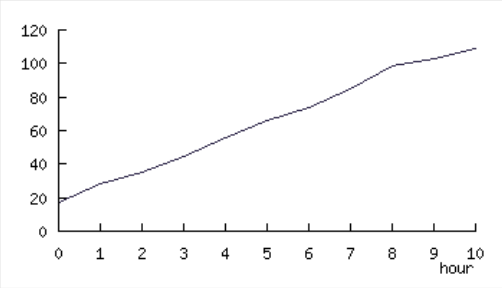
Top 10 Countries hosting electricshore.com's drone IPs



FACT SHEET

Network Size: 5427 unique IP addresses
Growth Rate: 4788.5 unique IP addresses/month
Days Monitored: 34
Domains Sharing IP Addresses: 195
Nameserver Count: 16
Domains Sharing Nameservers: 0

Growth of electricshore.com's fast flux drone IP addresses for the last day.



Total History | Last Year| Last Month| Last Week| Last Day| Last Hour

Detection Accuracy

- Average empirical probability of detection = 96.6%
  - Based on tests performed every 10 minutes
  - probability of false alarm rate to 5% on the weekly training data
- Effective probability of detection → 100%
  - as more and more10-minute monitoring windows are accumulated
- Verifying the assertion of long term monitoring research reported in related work

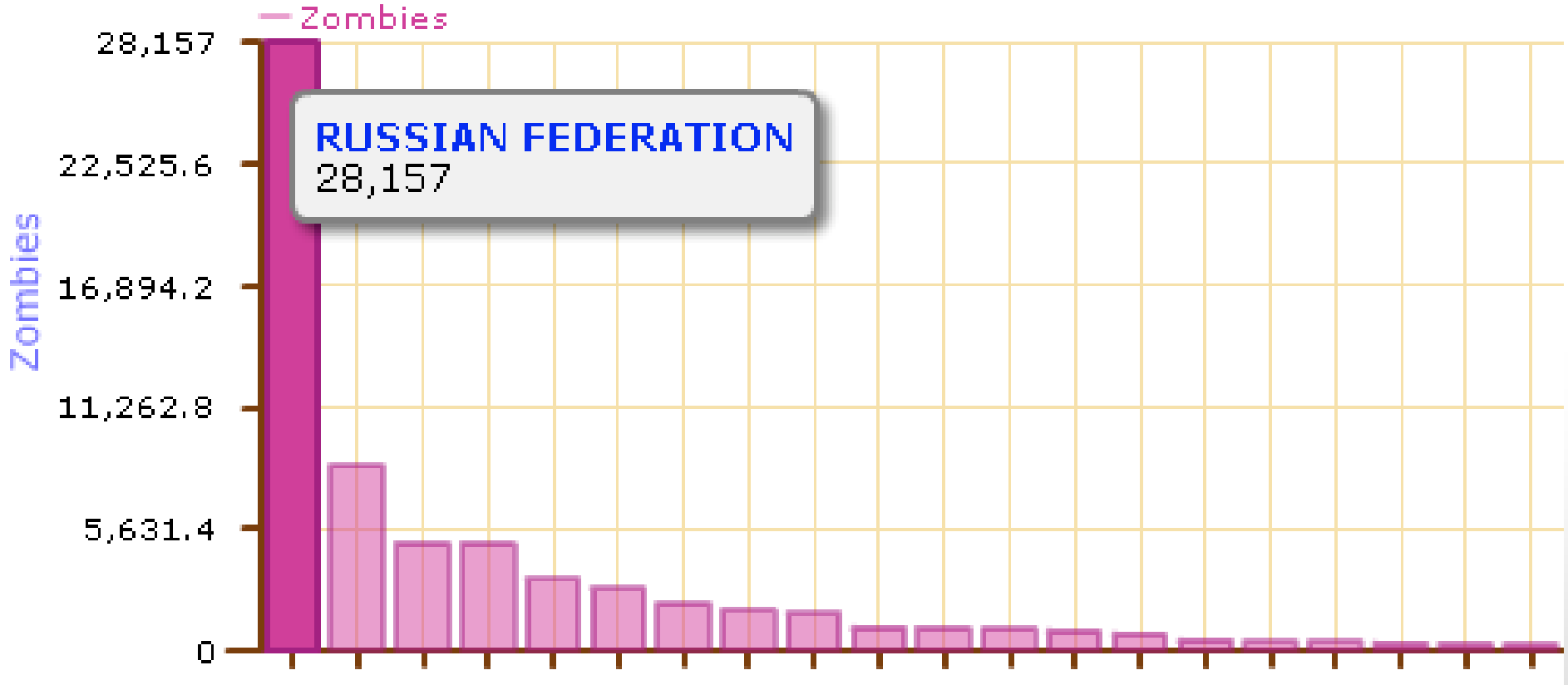
Related Work

- University of Mannheim
  - Holz, T. Gorecki, C. Rieck, C. Freiling, F. "Measuring and Detecting Fast-Flux Service Networks." Presented at NDSS Symposium (2008).
- The University of Milan
  - Passerini, E. Paleari, R. Martignoni, L. Bruschi, D. "FluXOR: detecting and monitoring fast-flux service networks." Detection of Intrusions and Malware, and Vulnerability Assessment (2008), pp. 186-206.
- Shadowserver.org
  - www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotnetsA
- Arbor
  - Active Threat Level Analysis System (ATLAS)

FFM Current Status

- Currently FFM monitors 1,000 active botnet domains and 40,000 zombies
- FFM database has 3,000 botnet domains including inactive ones
- Distributed monitors at Milcord and Sandia
- Active beta service
- Commercial FFM subscription service to be launched this month

Top 20 Infected Countries



Top 10 Infected Countries

Country	Zombie Count	Corruption Index	No of Zombies per 1M PC's
Russia	28,157	147	1,489
Germany	8,545	14	160
USA	4,956	18	20
Israel	4,953	33	2,503
EU	3,294		
Hong Kong	2,878	12	651
Ukraine	2,160	134	1,015
Taiwan	1,850	39	726
Korea	1,695	40	65
Slovakia	1,070	52	460

Conclusions

- FastFlux Monitor
  - detects domain and name server flux in real time
  - tracks zombie IP's, ISPs, countries
  - provides evidence for take-down
  - generates reports, alerts and blacklists
- Visit our demo booth at the Expo this evening
- Evaluate beta: bot@milcord.com
- Coming soon: fastfluxmonitor.com

Thank You.

Any Questions?

milcord

info@milcord.com (781) 839-7138