



Sicurezza delle
reti

Monga

Fast-flux
service
network

FluXOR

Risultati
sperimentali

L'autentica-
zione in
rete

Sicurezza dei sistemi e delle reti¹

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

¹© 2011–15 M. Monga. Creative Commons Attribuzione — Condividi allo stesso modo 4.0 Internazionale. <http://creativecommons.org/licenses/by-sa/4.0/deed.it>. Derivato con permesso da © 2010 M. Cremonini.

1



Sicurezza delle
reti

Monga

Fast-flux
service
network

FluXOR

Risultati
sperimentali

L'autentica-
zione in
rete

Lezione XIV: Botnet Fast-Flux

277



Sicurezza delle
reti

Monga

Fast-flux
service
network

FluXOR

Risultati
sperimentali

L'autentica-
zione in
rete

Botnet

Botnet

- una rete di macchine infette (bot, zombie) controllate da un unico attaccante (bot-master, mother-ship)
- usate per: spam, DDoS, phishing, scam, SQL injection massivi, ...

278



Sicurezza delle
reti

Monga

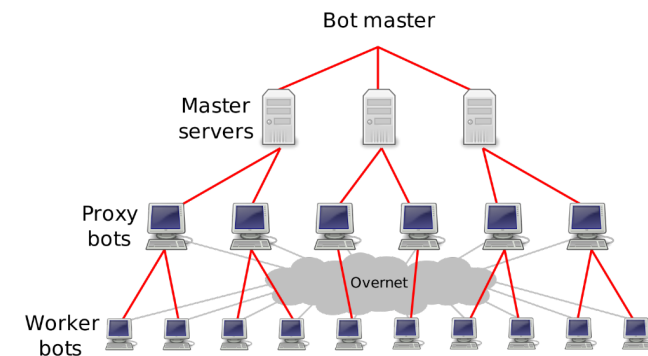
Fast-flux
service
network

FluXOR

Risultati
sperimentali

L'autentica-
zione in
rete

Botnet



279

Botnet

Non solo spam...



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Analisi di 10 giorni di traffico di rete generato da Torpig:

Unique IP Count	1.148.264
Unique Torpig keys (machines)	180.835
POP accounts	415.206
Email addresses	1.235.122
Passwords	411.039
Unique credit cards	875
Unique ATM pins	141
Unique social security numbers	21

280

Tecniche di propagazione



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Propagation mechanisms	Percentage
File sharing executables	40%
File transfer/email attachment	32%
File transfer/CIFS	28%
File sharing/P2P	19%
Remotely exploitable vulnerability	17%
SQL	3%
Back door/Kuang2	3%
Back door/SubSeven	3%
File transfer/embedded HTTP URI/Yahoo! Messenger	2%
Web	1%

Symantec, 2007

281

Botnet Fast-flux



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Fast-flux service network

- una tecnica (~ 2007) utilizzata per aumentare la robustezza della botnet, rendendola più difficile da identificare.
- l'idea è semplice: si aggiunge un livello di indirettezza fra vittime e attaccante.

282

Fast-flux service network



Sicurezza delle reti

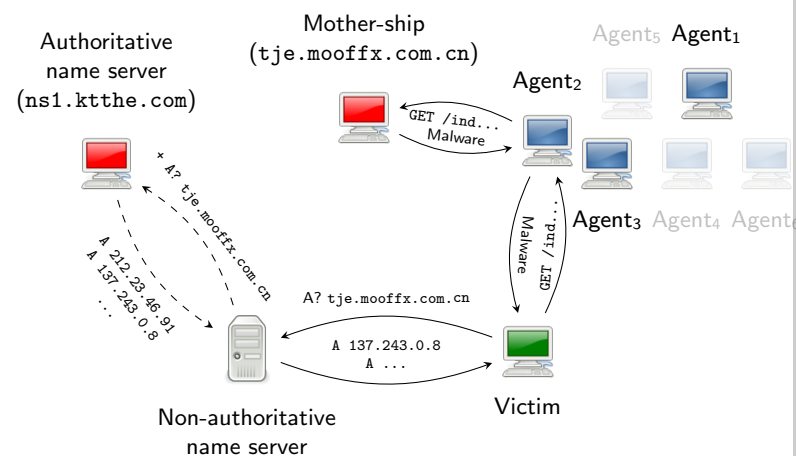
Monga

Fast-flux service network

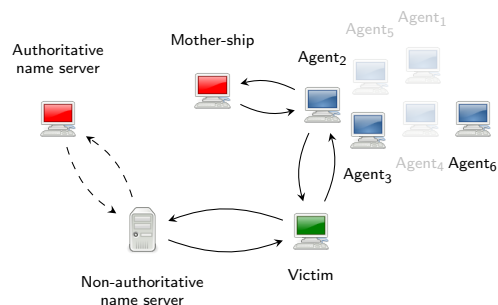
FluXOR

Risultati sperimentali

L'autenticazione in rete



283



- I bot offline, disinfettati o problematici vengono immediatamente rimpiazzati da altri
- Composta da milioni di agenti (Nostri esperimenti: ~121.000 fast-flux FQDN ~360.000 host)
- Più domini vengono utilizzati dalla stessa botnet (non basta chiudere un dominio)

284

Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Come identificare una FFSN?

- Ci sono moltissime caratteristiche misurabili...
- ... ma nessuna è sufficiente per identificare una FFSN

285



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

FluXOR

- si monitora un hostname sospetto, fingendosi una vittima
- si raccolgono dati e si identificano le FFSN tramite classificazione complessa
- si tengono sotto controllo le FFSN per elencare il maggior numero di agenti infetti

286

Features of fast-flux service network



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

● Domain				
● Domain age	Benign			
	avast.com	539	12	3600
	adriaticobishkek.com	65	21	1200
	google.com	542	3	300
	mean	493.27	2.86	4592.53
	std. dev.	289.27	3.89	7668.74
● Availability				
● # of DNS records of type A				
● TTL of DNS records				
● Heterogeneity	Malicious			
	eveningher.com	18	127	300
	factvillage.com	2	117	300
	doacasino.com	2	33	180
	mean	4.85	98.13	261.49
	std. dev.	4.9	37.27	59.64
	# of organisations			

287



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Collector

Raccoglie nomi di dominio **sospetti** da sonde informative (e.g, spam ...)

Monitor

- per ogni DN **sospetto** raccoglie info sulle caratteristiche
- per ogni DN **malevolo** (classificato dal Detector) raccoglie gli IP degli agenti infetti

Detector

- classifica i sospetti in **malevoli** e **benevoli** tramite un classificatore bayesiano
- Training set di partenza: 50 benevoli + 58 malevoli

Riassumendo



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Le botnet Fast-flux

- nascondono la propria topologia grazie a registrar "compiacenti"
- sono rilevabili con tecniche di data mining



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Descrizione	#
Email processate	144952
URL estratti	34466
FQDN attivi	29368
<i>Fast-flux service network</i>	<i>9988</i>
<i>Agenti Fast-flux</i>	<i>162855</i>
<i>Botnet Fast-flux</i>	<i>25</i>

Botnet	# agenti	# FFSN
European Pharmacy	65043	3950
Halifax Online Banking	46772	1
Digital Shop	20069	17
Royal Casino	15078	34
Royal VIP Casino	8665	16
Euro Dice Casino	7667	28

Botnet	# spam email	% spam (rispetto al totale)
European Pharmacy	12056	8.32%
SwissWatchesDirect	3330	2.30%
RXNET	2558	1.76%
MaxHerbal	1897	1.31%
Altre FFSN	6395	4.41%
Totale	144952	18.10%

289

Protezione dei servizi critici



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

L'accesso ai servizi critici è controllato

- Autenticazione:** chi è l'agente (che opera in nome di un *principal*)
- Autorizzazione:** l'agente autenticato ha il permesso?



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Autenticazione

Autenticare significa verificare **l'identità** di un soggetto (non necessariamente umano)

292



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete



Modalità di base per l'autenticazione (di Alice) tramite rete:

- ① **password** (ossia la conoscenza di un segreto)
- ② **locazione** (logica o fisica) da cui proviene la richiesta di autenticazione
- ③ per mezzo di operazioni crittografiche su dati forniti dall'autenticatore (Bob).

293



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Alcune vulnerabilità sono intrinseche:

- Le password possono essere **indovinate**
- Le locazioni possono essere **millantate**
- I dati crittografici possono essere **intercettati e riutilizzati** (replay attack)

294



Sicurezza delle reti

Monga

Fast-flux service network

FluXOR

Risultati sperimentali

L'autenticazione in rete

Queste minacce possono essere mitigate

- Aumentando la cardinalità delle password possibili
- Controlli di coerenza
- Crittografia a chiave pubblica e protocolli articolati

L'autorizzazione conseguita con l'autenticazione dura un intervallo temporale detto sessione.

295