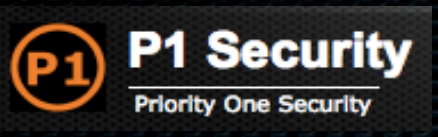


Intrusions

Experiences terrains pour le défensif et l'offensif

Philippe Langlois

P1 Security Inc.

V4.2

APT & orfèvrerie

- Aurora, TJX, …
- L'époque "mythique" est révolue.
- "Commodification" du hacking
- Les "orfèvres" de l'intrusion se font rare (statistiquement)
- Place à l'industrie de masse…

Citation de forums “hostiles”

P1 Security
Priority One Security

My favorite quote:

Чтобы заработь на Интернете не нужно ничего и даже мозгов

“To make money on Internet you don’t need much, not even brain” - from online tutorial on how to make money

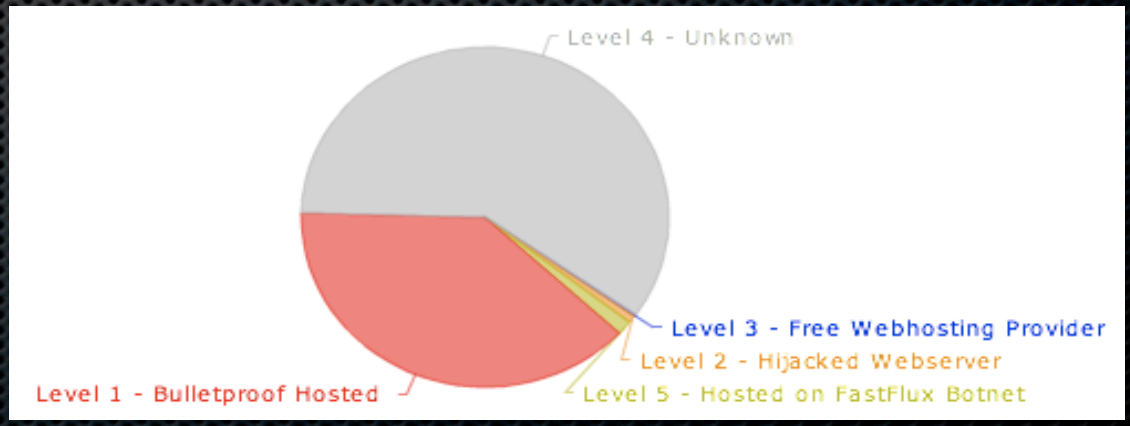
Industrie de l'intrusion

P1 Security
Priority One Security

- Editeurs, Competition
- Protection logicielle
- Hosting, abuse resist
- Intermédiaires
- Exploit packs, SEO Poisoning, 3rdP
- Prix, Monétisation, (X/43)
- CPs, monitoring

Dateadded	Host	IP address	Level	Status	Files Online	SBL	Country	AS number	Uptime
2010-11-23	delaciudadfm.com.ar	64.22.110.26	2	online	2	Not listed		AS3595	07:45:33
2010-11-23	develstate.com	91.217.249.16	4	online	1	SBL97861		AS51554	07:48:37
2010-11-22	tomatoo.in	178.63.149.150	4	online	2	Not listed		AS24940	40:36:03
2010-11-22	securelayer.in	91.211.117.38	4	online	2	Not listed		AS48587	40:36:37
2010-11-22	database-upgrade.net	92.241.190.128	1	online	1	SBL60370		AS41947	40:41:27
2010-11-22	92.241.190.128	92.241.190.128	1	unknown	4	SBL60370		AS41947	-
2010-11-21	88.198.40.111	88.198.40.111	4	unknown	2	Not listed		AS24940	-
2010-11-21	lanlabs.net	87.255.51.229	4	online	1	Not listed		AS38930	63:28:58
2010-11-20	backorderru.com	213.155.29.56	4	online	2	Not listed		AS41665	75:08:08
2010-11-19	193.104.146.55	193.104.146.55	1	unknown	0	SBL91085		AS50134	-
2010-11-19	bizwaxxxonline.com		4	offline	0	Not listed	-		00:00:00
2010-11-19	colcolcolcol.com		4	offline	0	Not listed	-		00:00:00
2010-11-19	rorolord.net		4	offline	0	Not listed	-		00:00:00
2010-11-19	98up.com		4	offline	0	Not listed	-		37:02:43
2010-11-19	futondrop.com	109.196.142.18	1	online	0	SBL92047		AS39150	112:15:46
2010-11-19	bxpartner.com	213.155.12.144	4	online	0	Not listed		AS41665	113:44:29
2010-11-19	boltizdeh.com	122.224.4.132	1	online	2	Not listed		AS4134	113:45:16
2010-11-18	pihksdf469kjsdfkhsdf.co.cc	FastFlux Botnet	5	online	0	Not listed	-		123:03:50
2010-11-16	esim.raciborz.pl	78.31.91.122	2	online	0	Not listed		AS30813	169:50:54
2010-11-16	x188188x.su	62.109.3.105	4	online	1	Not listed		AS29182	169:52:01
2010-11-16	dscodec.com		4	offline	0	Not listed	-		34:31:34
2010-11-16	govnozhest.cz.cc	194.8.250.10	4	online	0	SBL90325			170:02:22
2010-11-16	adm.jazteberabim.de	212.117.178.176	4	online	0	Not listed		AS5577	182:33:09
2010-11-16	fastertraders.net	173.244.194.237	4	online	2	Not listed		AS36351	184:00:54
2010-11-16	fenieneec.info	195.242.161.86	1	online	2	Not listed		AS47434	184:02:00
2010-11-16	healthbeas.com	91.204.48.99	4	online	0	Not listed		AS24965	184:02:48
2010-11-16	kerero.info		4	offline	0	Not listed	-		13:54:40
2010-11-16	moun1r.co.cc	66.96.249.117	4	online	0	Not listed		AS21788	184:05:58
2010-11-16	svetodioduk.net	81.176.236.12	4	online	2	Not listed		AS8342	184:09:33
2010-11-16	webpatrol.com.tw	91.204.48.121	4	online	0	Not listed		AS24965	184:10:48

Source: abuse.ch



P1 Security
Priority One Security

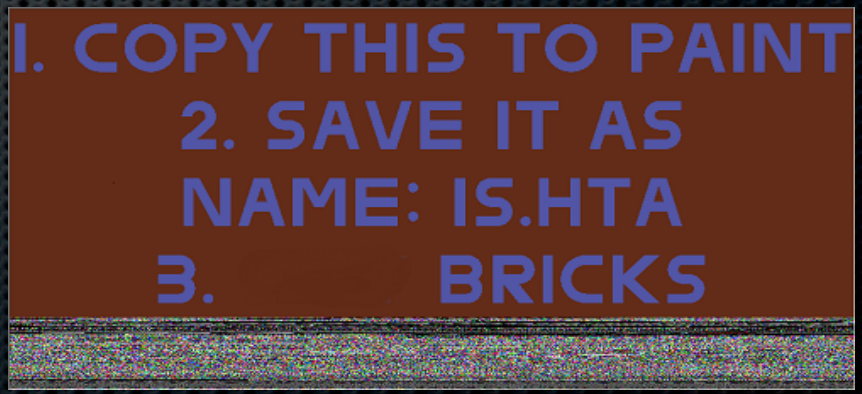
Du point de vue technique

- Builders, configs, chiffrement
- Administration: du C&C au C4I
- Furtivité: Fast Flux, Hosting “Abuse resistant”, P2P, Tor, VMprotect
- Loader, Pack d’Exploits, “Drive by downloads”, Emails de masse, marché des exploits, Faux antivirus
- Fonctionnalités financières

Top ten ZeuS hosting countries (by ZeuS hosts)

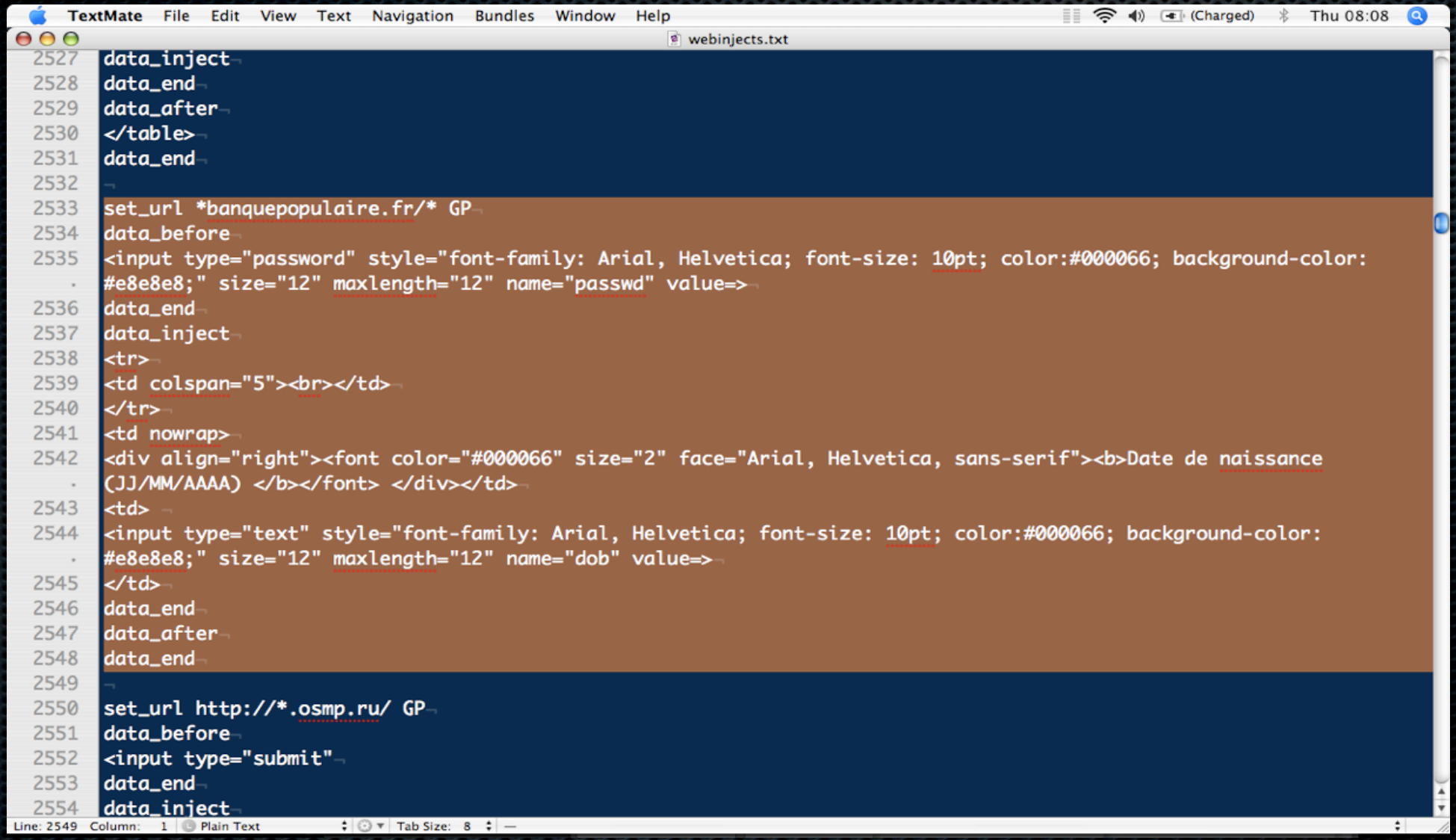
ZeuS C&C count	country
78	United States (US)
71	Ukraine (UA)
62	Russian Federation (RU)
42	Czech Republic (CZ)
17	China (CN)
9	Romania (RO)
8	Netherlands (NL)
7	United Kingdom (GB)
6	Bosnia and Herzegovina (BA)
5	Europe (EU)

Source: abuse.ch



WebInjects

P1 Security
Priority One Security



P1 Security
Priority One Security

Et maintenant nos expériences directes…

CAS CONCRETS

P1 Security
Priority One Security

Cas #1: Attaque Massive

- Réutilisation des mêmes méthodes “brutes”
- Mass mailing
- Brute forcing
- Social Engineering
- “Scoring” précis des utilisateurs & employés
- Suivi d’une “compétition jeu” interne
- Bons résultats, formation continuelle des reflexes et suivi des menaces.

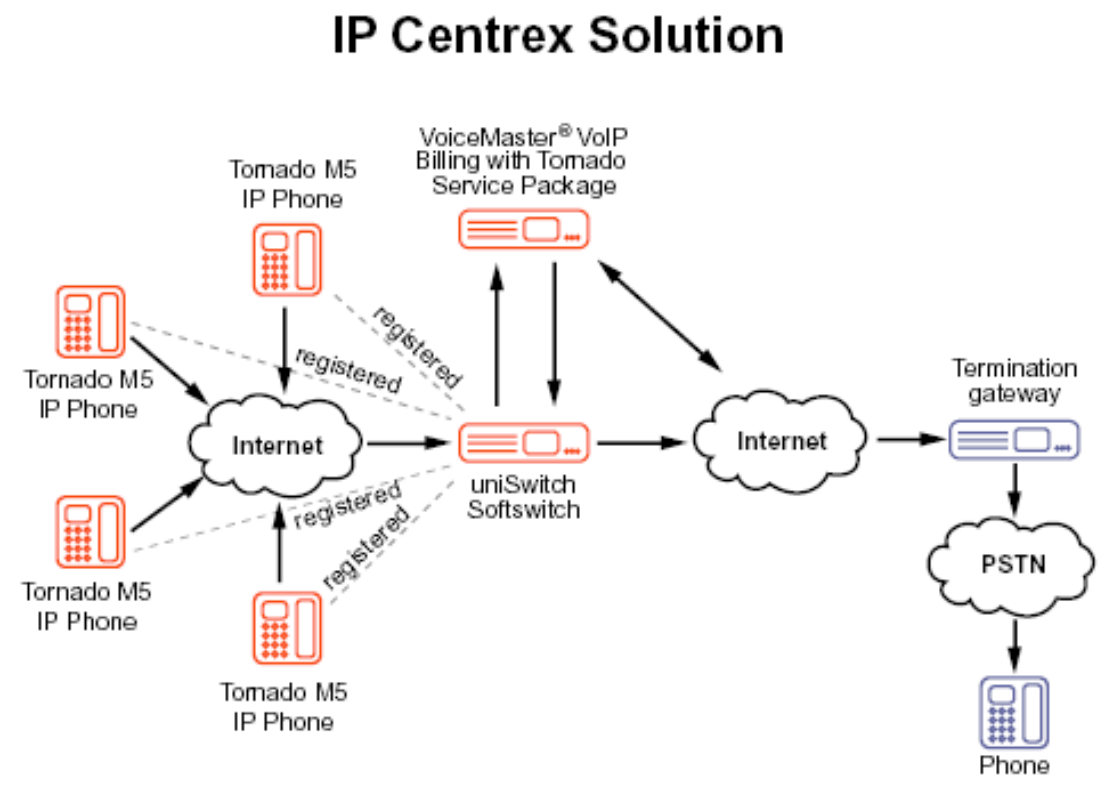
P1 Security
Priority One Security

Cas #2: Legacy Sandwich

- Pentest dans un grand groupe (B2C, 7 millions de clients)
- “Total Information Outsourcing”
- Pentest sur leur infrastructure
- “Mais nous n’avons pas de telle infrastructure” (!)
- Conséquences

Cas #3: fraude VoIP

- Défense
- 3-4 jours
- 100k EUR en communications
- Manquements du côté fournisseurs
- Problème technologique mais aussi en terme d' "éveil".



P1 Security
Priority One Security

Cas #4: Démo intrusion telecom SS7 & 3G

Démo!

(Démonstration de cartographie et attaques SS7 sur réseau télécom mobile 3G)

P1 Security
Priority One Security

Cas #5: Combinaisons infernales

- Série de bugs minimes
- SNMP v2 obscur (port source)
- IPv6 activé par défaut
- Leaks via Mail
- Informations glanées sur Facebook
- Web App vulnérable
- Filtrage imparfait
- == Intrusion à distance

P1 Security
Priority One Security

Protection: Defense active

- Paradigme “Firewall + Antivirus”, dépassé?
- Nouvelles architectures, “haute interaction”, industrialisation de la réaction, CERT interne, …
- Quelle courbe d’apprentissage de l’organisation?
- Double problème de la commodification pour l’obtention de ressources
  - “Mon ingénieur est certifié Cxxxx” ou isolement
- Course R&D, course organisationnelle, course sur le “Threat intelligence”

Protection: Et l'offensif?

- Face à la réalité
- "Un pentest ne sert à rien"
- Sensibilisation, déblocage
- Taille = difficulté
- Expertise = difficulté
- Problème des "modes"

Conclusion

P1 Security
Priority One Security

- Approche “Massive” et approche “Experte” en même temps
- Règle 80/20
- Cloud infrastructure, mobile apps, gmail apps & extensions
- Threat intelligence, CERTs, monitoring interne et global
- Maturité de la sécurité
- Approche “aggressive” autant pour la défense que l’attaque
- Parfois, nécessité de “preuves”, de déblocages
- Entrainement, formation, exercices, workshops, information

Merci.

P1 Security
Priority One Security

Questions?

Philippe.Langlois@p1sec.com

http://www.p1security.com

Merci à Fyodor Yarochkin, P1 Labs, TCERT, HNP TSIG, Telecom Security Task Force, FUSR-U