HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Shell over DTMF

Alambix

Nicolas Collignon
<Nicolas.Collignon@hsc.fr>

Alambix ?

- Backdoor pour se connecter sur un IPBX déjà compromis
- Permet d'exécuter des commandes sur un IPBX inaccessible depuis Internet
  ► attaques sur le réseau interne
- Se présente sous la forme d'un module Asterisk

Spécifications

- Entrée ► DTMF
- Sortie ► Voix
  - Épelle les lettres avec le moteur interne d'Asterisk
  - Lit les résultats avec festival
- Compatible avec les différentes versions de l'API Asterisk
- Fonctionne sur CPU Intel et ARM
- Asterisk tourne en root sur certaines box ADSL ...

Du côté Asterisk

- Un SDA est attribué à la backdoor
- Installation en modifiant la configuration (`extensions.conf`)
- Inutile de redémarrer Asterisk
- Dans les rares cas où la configuration Asterisk est intelligible, un rootkit peut aider à cacher le module

```
exten => 1234,1,Answer()
exten => 1234,n,Macro(blacklist,${CALLERID(num)})
exten => 1234,n,Macro(reception-SDA,665,SIP/665,0)
exten => 1234,n,Hangup()
```

```
exten => 666,1,Alambix()
exten => _1XXX,2,Dial(SIP/${EXTEN},20)
exten => _1XXX,3,VoiceMail(${EXTEN}@hsc)
```

Fonctionnement général

1) Numéro de téléphone composé
2) Alambix décroche et demande le code PIN
3) Menu principal
4) Commande shell encodée en DTMF
5) Alambix décode et exécute la commande
6) Alambix lit le résultat

Menu / Clavier

- Menu Alambix
  - 1 ► exécute une commande
  - 2 ► exécute une commande et épelle le résultat
  - 3 ► exécute une commande et lit le résultat
- Clavier « SMS »

0	/	|	$	*	+	
1		.	,	-	_	
2	a	b	c	'	"	
3	d	e	f	(	)	
4	g	h	i	[	]	
5	j	k	l	:	;	
6	m	n	o	@	!	
7	p	q	r	s	{	}
8	t	u	v	&	~	
9	w	x	y	z	?	