PROVEX: Detecting Botnets with Encrypted C&C Channels

Christian Rossow
Christian J. Dietrich

Presentation at DIMVA 2013, Berlin, July 2013

Introduction & Acknowledgements

- Research assistant at if(is), Gelsenkirchen
  - In collaboration with Chris Dietrich

- PostDoc at
  - VU Amsterdam
  - Ruhr University Bochum

- Twitter: @christianrossow

- Funded by

Botnet Detection Challenges

Challenge 1: Custom C&C Traffic Encryption

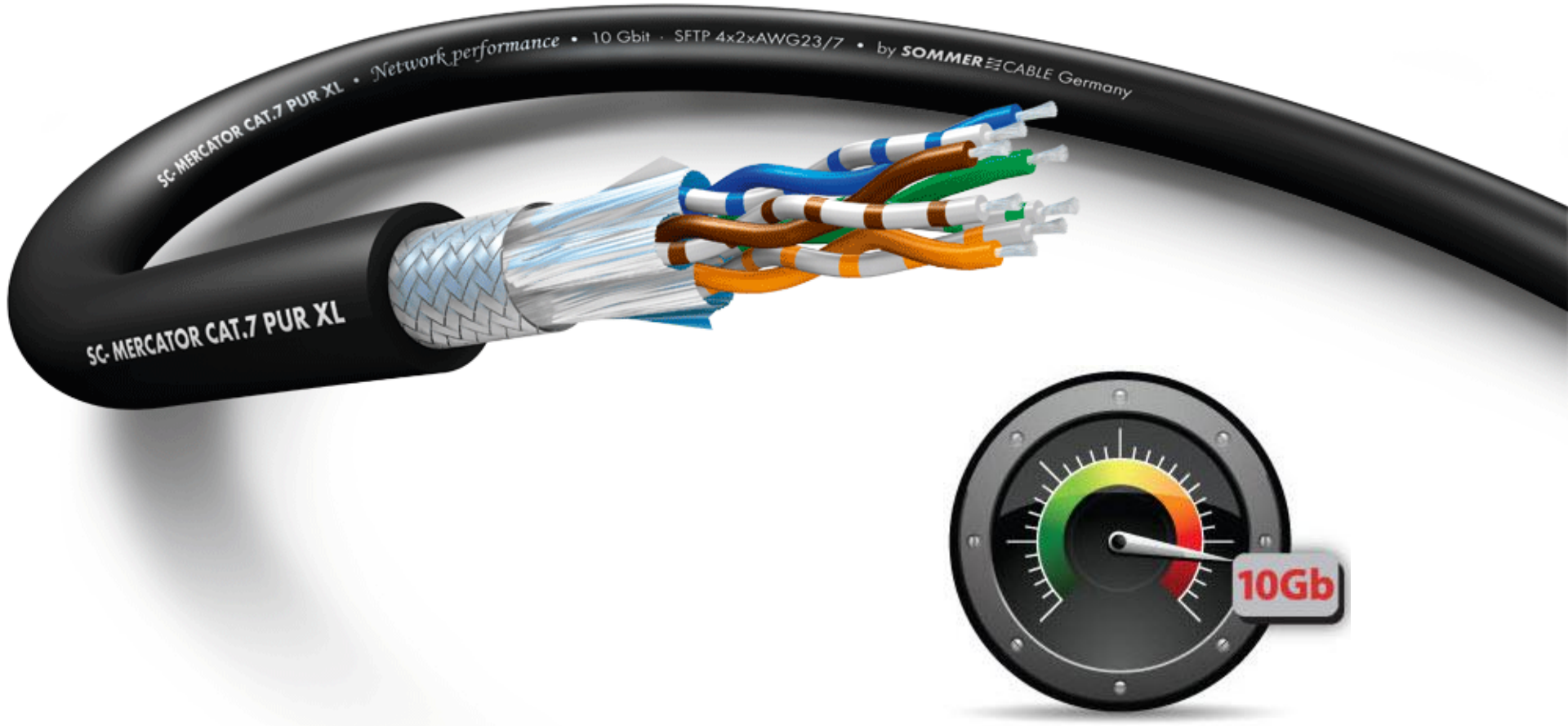
(1998)

+

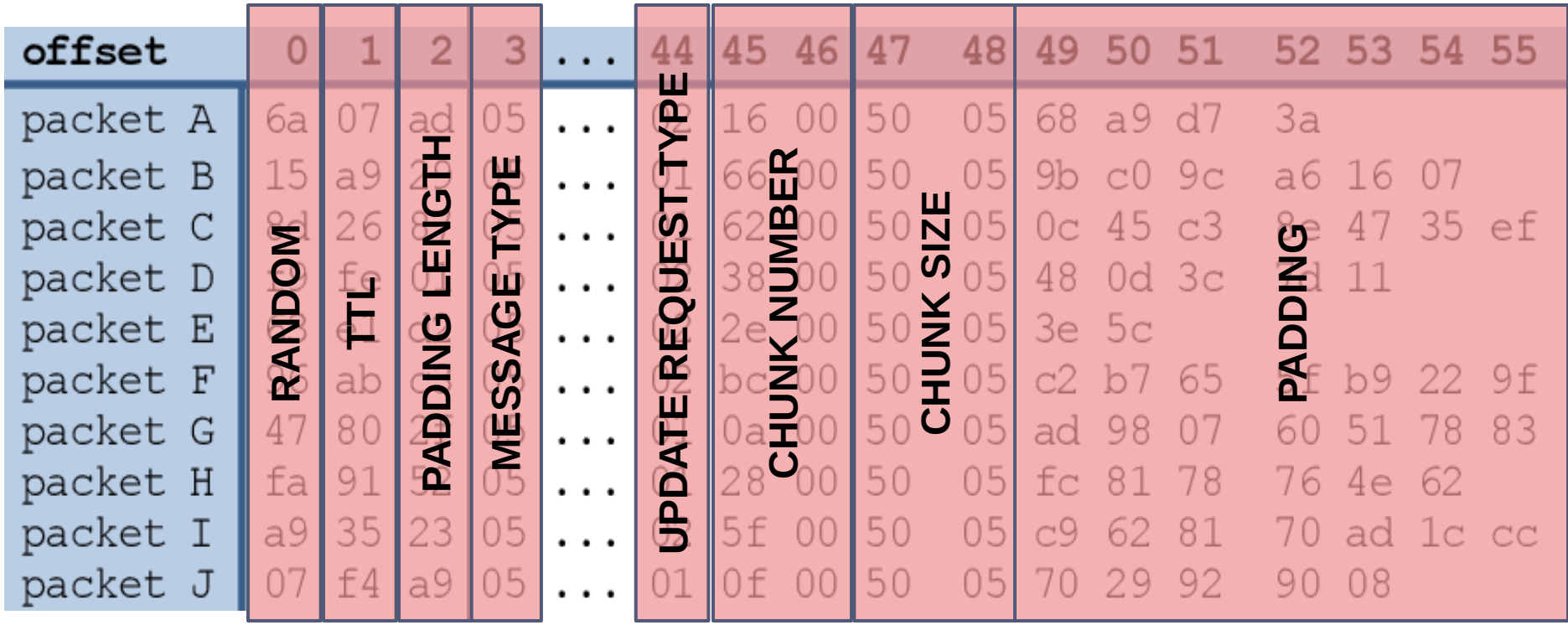
(2010)


```
cmd[0] = random();
for(i = 1; i < len; i++) {
  cmd[i] ^= cmd[i - 1];
}
```

Challenge 2: High-Speed Networks

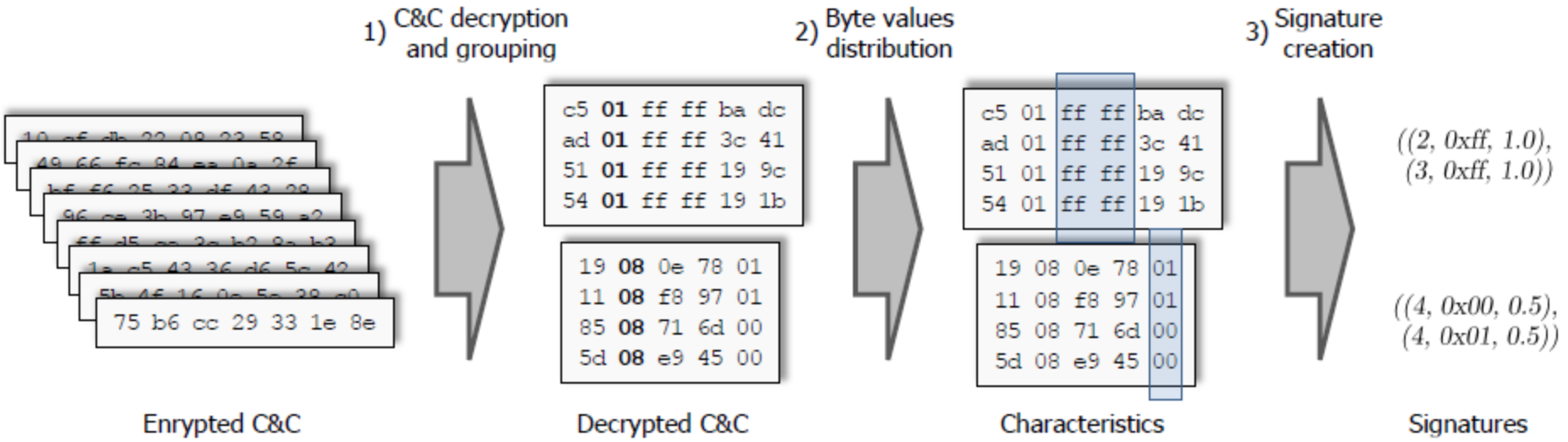


Challenge 3: Custom Binary C&C Protocols



ProVeX

ProVeX: Signature Generation



ProVeX: Signature Generation

- Prerequisites
  - Decrypt recorded C&C traffic with known crypto material
  - Identify message type field within C&C protocol

	offset	0	1	2	3	...	44	45	46	47	48	49	50	51	52	53	54	55
Update	packet A	6a	07	34	05	...	02	16	00	50	05	68	a9	d7	3a			
	packet B	15	a9	36	05	...	01	66	00	50	05	9b	c0	9c	a6	16	07	
	packet C	8d	26	37	05	...	01	62	00	50	05	0c	45	c3	8e	47	35	ef
	packet D	f9	fe	35	05	...	02	38	00	50	05	48	0d	3c	7d	11		
	packet E	63	e1	32	05	...	02	2e	00	50	05	3e	5c					
	packet F	96	ab	37	05	...	02	bc	00	50	05	c2	b7	65	5f	b9	22	9f
Version!	packet G	47	80	37	01	...	7a	0a	a7	9a	3d	ad	98	07	60	51	78	83
Peerlist?	packet H	fa	91	36	02	...	fe	28	d3	19	17	fc	81	78	76	4e	62	
Peerlist!	packet I	a9	35	37	03	...	89	5f	b1	a7	f1	c9	62	81	70	ad	1c	cc
Version!	packet J	07	f4	35	01	...	c5	0f	a7	9b	5c	70	29	92	90	08		

ProVeX: Signature Generation

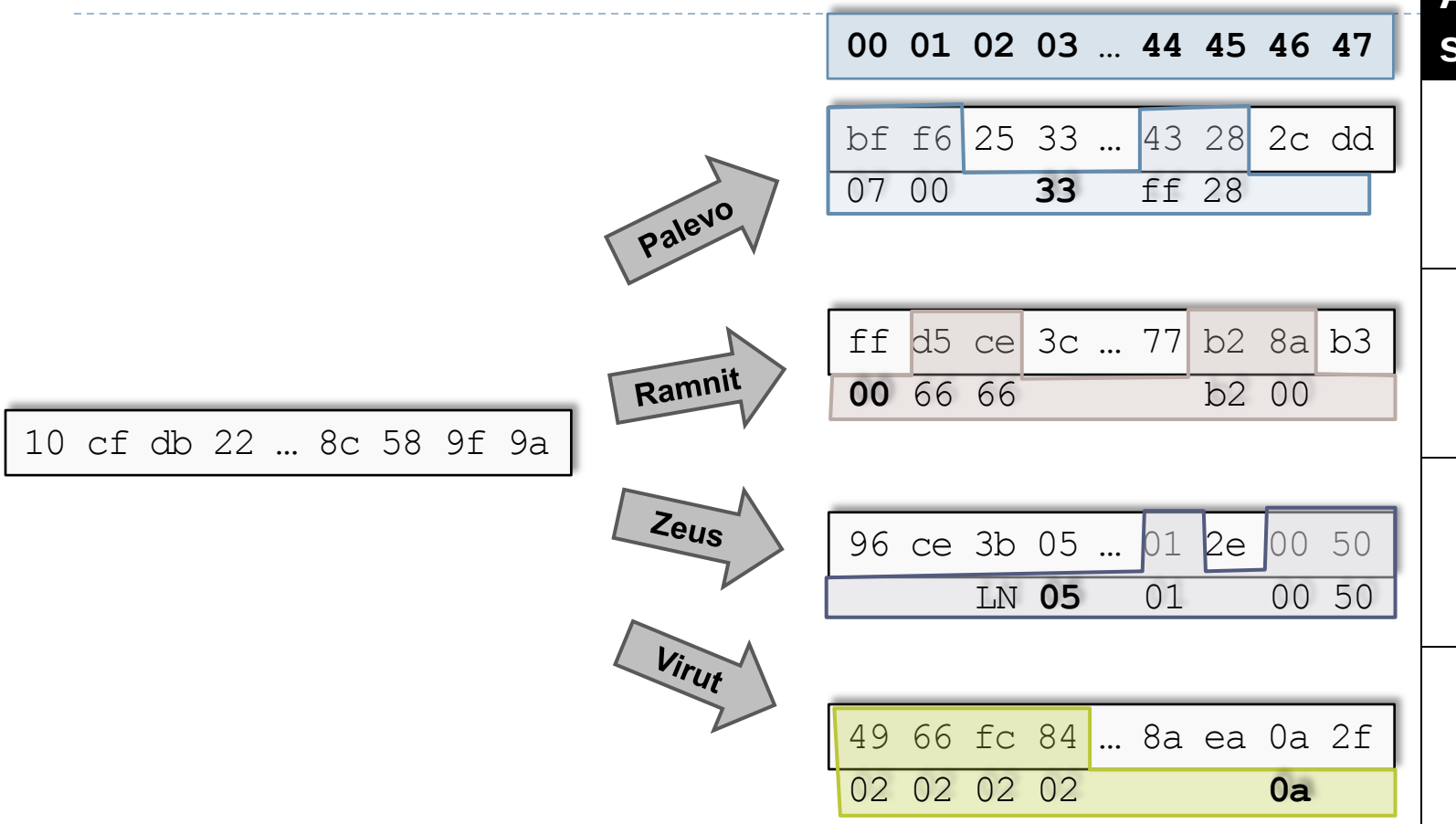
offset	0	1	2	3	...	44	45	46	47	48	49	50	51	52	53	54	55
packet A	6a	07	34	05	...	02	16	00	50	05	68	a9	d7	3a			
packet B	15	a9	36	05	...	01	66	00	50	05	9b	c0	9c	a6	16	07	
packet C	8d	26	37	05	...	01	62	00	50	05	0c	45	c3	8e	47	35	ef
packet D	f9	fe	35	05	...	02	38	00	50	05	48	0d	3c	7d	11		
packet E	63	e1	32	05	...	02	2e	00	50	05	3e	5c					
packet F	96	ab	37	05	...	02	bc	00	50	05	c2	b7	65	5f	b9	22	9f

Payload bytes — Msg type — Payload len

$$psig = \langle (o_1, b_1, p_1), ..., (o_n, b_n, p_n), \quad (o_t, b_t), \quad (o_{pl}, l_{pl}, e_{pl}) \rangle$$

- ((44, 0x01, 50%), (44, 0x02, 50%), (46, 0x00, 100%), (47, 0x50, 100%), (48, 0x05, 100%),)

ProVeX: Signature Matching



S: Abs. score	R: Relat. score
1	25%
discard	
4	100%
0	0%

- Signature matches if S ≥ 4.0 and R ≥ 75%

Evaluation

True Positive Evaluation

- Cross folds to test for generality of signatures
- Cross environments – learn at A, apply at B

Family	# sigs	CV TPR
Cutwail	1	100%
Fynloski	11	78%
Palevo	5	87%
Pramro	1	81.5%
Ramnit	5	97%
Sality	2	100%
Tofsee	1	100%
Virut	1	100%
ZeroAccess	3	100%
Zeus P2P	5	100%

False Positive Evaluation

- Probabilistic:

	$S = 4, R = 0.5$		$S = 4, R = 0.75$		$S = 4, R = 0.9$	
family	P_{fam}	*matches*	P_{fam}	*matches*	P_{fam}	*matches*
Cutwail	$2^{-34.5}$	6118	$2^{-52.6}$	1118	$2^{-67.7}$	43
Fynloski	$2^{-36.6}$	6518	$2^{-45.4}$	1426	$2^{-54.4}$	69
Palevo	$2^{-39.4}$	900	$2^{-47.0}$	186	$2^{-47.0}$	7
Pramro	$2^{-40.0}$	1	$2^{-40.0}$	1	$2^{-40.0}$	1
Ramnit	$2^{-34.4}$	3556	$2^{-43.8}$	649	$2^{-54.4}$	40
Sality	$2^{-39.9}$	638	$2^{-53.1}$	139	$2^{-69.2}$	10
Tofsee	$2^{-41.0}$	512	$2^{-64.5}$	56	$2^{-80.0}$	1
Virut	$2^{-41.0}$	256	$2^{-58.8}$	46	$2^{-80.0}$	1
ZeroAccess	$2^{-39.4}$	768	$2^{-57.2}$	138	$2^{-78.4}$	3
Zeus P2P	$2^{-38.4}$	1536	$2^{-56.2}$	276	$2^{-72.0}$	7

- Live network: 3 FPs for Palevo in 24h
- Packet fuzzing: 123 FPs for Virut in 2^{35} random packets

Qualitative Evaluation

- What do the signatures cover?
  - *Zeus*: IP version type field in peer lists
  - *ZeroAccess*: Age attribute in peer lists
  - *Cutwail*: Message length and `addr` payload substring
  - *Sality*: Padding of NULL-bytes
  - …
- Efficiency
  - With 50 families: 418MBit/s (not optimized, single core)
  - Straightforward to parallelize!

Conclusion

- Payload detection fails for crypted C&C channels
- ProVeX can detect even encrypted C&C traffic
  - Semi-automatically learn probabilistic vectorized sigs
  - Apply sigs on decrypted network traffic
- Evaluation promising

PROVEX: Detecting Botnets with Encrypted C&C Channels

Christian Rossow
@christianrossow
Christian J. Dietrich

Presentation at DIMVA 2013, Berlin, July 2013