



COORDINATION CENTER
FOR TLD RU/PФ

Proactive methods of malicious domain registration detection

Vadim A. Mikhaylov
APTLD`83

cctld.ru | кц.рф



Problem



Problem



Solution



Solution



— registrant contact information analysis

— registrant contact information analysis

Name: qwertyuiop

Address: 000000, Ajdlkjaslkdfjalkjd

Methods

– registrant contact information analysis

Name: qwertyuiop

Address: 000000, Ajdlkjaslkdfjalkjd

Phone: +000000000000

E-mail: attacker@proton.me

Methods

- registrant contact information analysis
- **delegation parameters analysis**

Methods

- registrant contact information analysis
- **delegation parameters analysis**

IPv4
IPv6

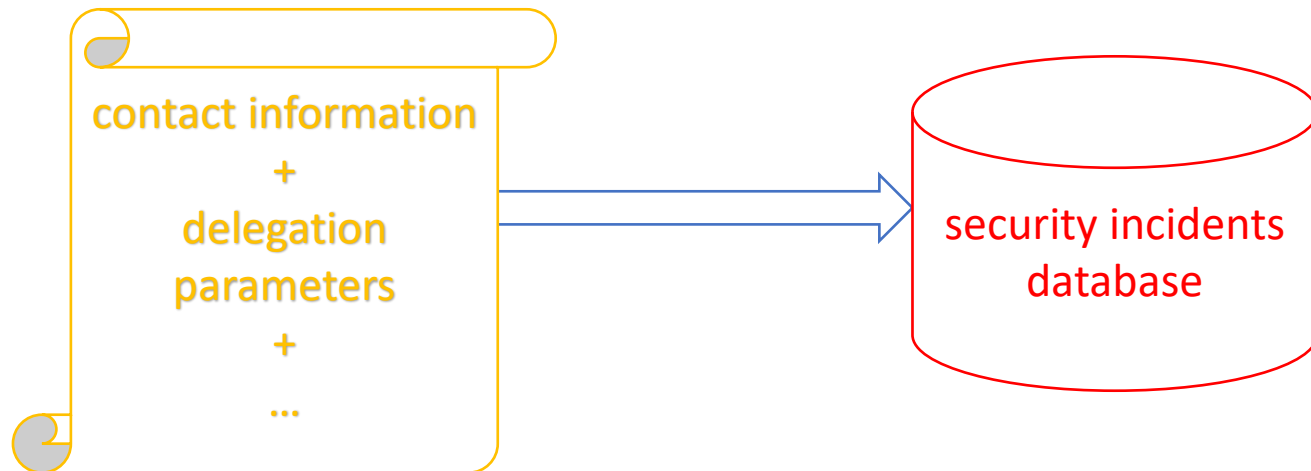


Bulletproof hosting

- registrant contact information analysis
- delegation parameters analysis
- **domain parameters history analysis**

Methods

- registrant contact information analysis
- delegation parameters analysis
- **domain parameters history analysis**



Methods

- registrant contact information analysis
- delegation parameters analysis
- domain parameters history analysis
- **domain string analysis**

Methods

- registrant contact information analysis
- delegation parameters analysis
- domain parameters history analysis
- **domain string analysis**

b	a	d
b	a	t

distance = 1

k	i	t	t	e	n	
s	i	t	t	i	n	g

distance = 3

Methods

- registrant contact information analysis
- delegation parameters analysis
- domain parameters history analysis
- **domain string analysis**

o	o	Identical	и	й	Low	w	vv	High
0	O	High	e	ë	Low	m	rn	High
1	1	High	d	ḍ	High	ffl	ffl	Low
l	l	High	a	ā	Low	л̣	л̣	Low
simple			diacritic			composite		

Methods

- registrant contact information analysis
- delegation parameters analysis
- domain parameters history analysis
- **domain string analysis**
 - *bank*, *loan*, *credit*, *pay*...
 - *corona*, *covid*, *vaccin*, ...
 - + DGA

Methods

- registrant contact information analysis
- delegation parameters analysis
- domain parameters history analysis
- domain string analysis
- **registrar reputation level**

Conclusion

- The more methods used together, the better the result

Conclusion

- The more methods used together, the better the result
- Setting up weight coefficients it's individual challenge

Conclusion

- The more methods used together, the better the result
- Setting up weight coefficients it's individual challenge
- Difficulties with suspicious domains checking

Conclusion

- The more methods used together, the better the result
- Setting up weight coefficients it's individual challenge
- Difficulties with suspicious domains checking
- Important role of actual security incident information sharing

Conclusion

- The more methods used together, the better the result
- Setting up weight coefficients it's individual challenge
- Difficulties with suspicious domains checking
- Important role of actual security incident information sharing
- ML-tech growth gives new opportunities and new challenges

*«Prevention is better than cure»
Desiderius Erasmus*



COORDINATION CENTER
FOR TLD RU/PФ

Thank you!

Vadim A. Mikhaylov

mva@cctld.ru | мва@кц.рф



cctld.ru | кц.рф

,RU

,PФ