TO PAY OR NOT TO PAY: AN ANALYSIS OF SERVER RANSOMWARE AND SERVER RANSOM SCAMS

Kevin van Liebergen
kevin.liebergen@imdea.org

Gibrán Gómez
gibran.gomez@imdea.org

Juan Caballero
juan.caballero@imdea.org

institute IMDEA software

(1) INTRODUCTION

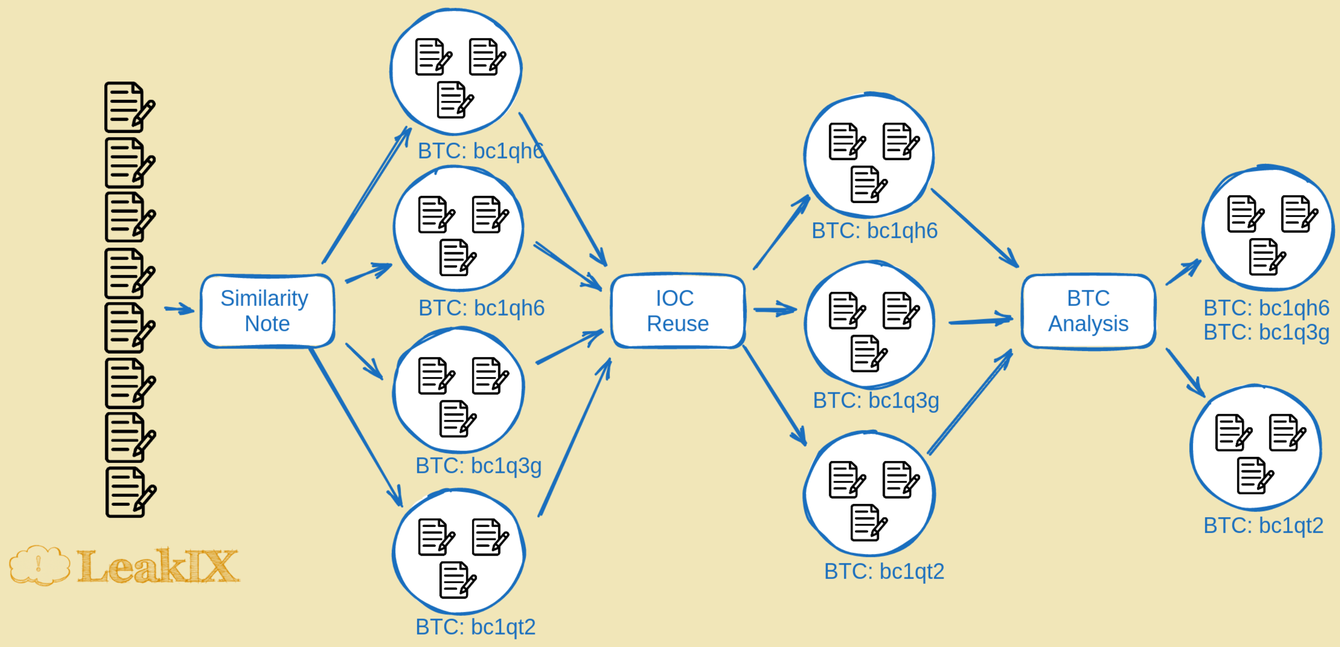
- *Server ransom* differs from **desktop** ransom by scanning the Internet for victim servers
- Server ransom easy to confuse with **ransom scam** where **data cannot be recovered**

(2) CONTRIBUTIONS

- We perform the **first study** of server ransomware and server ransom scams
- Three-step automated **clustering** to **group infections** of the **same campaign**
- We **quantify** the (lack of) **coverage** on the **DeadBolt** ransomware by Internet scanners

(3) CLUSTERING

- We get the dataset of **infected devices** collected from Internet-wide scanners, that scan the IPv4 address space on selected ports



- Clustered 40K events into 120 clusters

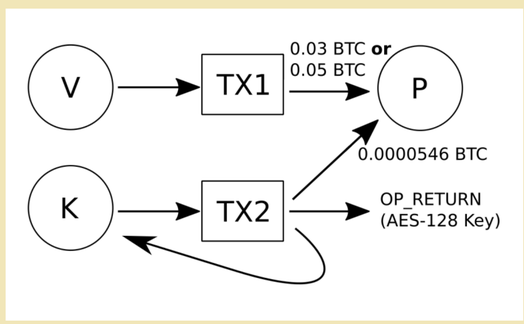
(4) FINANCIAL IMPACT

- **Low** estimated **revenue** (354K USD)
- How much higher is the real revenue?

	Direct Deposits on Seeds				Direct Deposits on MI clusters			
CID	Addr.	Seeds	BTC	USD	MI Cl.	MI Addr.	BTC	USD
BC1	141	65	5.53759499	164,405.24	55	77	5.71522320	168,174.62
BC95	2	2	5.90752362	36,676.31	1	9	10.13022872	59,842.66
BC1039	38	7	5.23605537	44,189.99	6	9	5.44936636	46,141.00
BC1848	1	1	0.21471800	8,320.08	1	3	0.22760200	8,816.07
BC896	1	1	0.14829752	1,363.85	1	3	0.64939752	6,402.47
Total	263	127	19.46058512	311,995.45	112	176	25.87318893	354,444.75

(5) DEADBOLT RANSOMWARE

- Key release transactions



(6) COVERAGE IMPACT

Collection	Coverage	Seeds	Addr.	Dep.	BTC	USD
Censys	2.0%	49	49	104	2.48620746	54,136.66
Shodan	2.6%	64	64	114	2.82608808	63,077.10
Censys+Shodan	2.6%	64	64	114	2.82608808	63,077.10
Key-release	99.3%	2,482	2,483	2,596	97.83718238	2,453,532.39
Oracle	100.0%	2,500	2,501	2,615	98.35008368	2,472,845.02

- Shodan and Censys only observe 2.6% of the addresses with payments
- **Real estimation** is $2.4M, **39** times **higher**

(7) FUTURE WORK

- Automatically **differentiate** server ransomware and server ransom scams clusters
- Explore which **organizations** are being **targeted**
- Do attacker **leverage Internet scanners** to discover victims?