Анализа случаја Малоне Лам: Социјални инжењеринг и прање новца

Лука Колаковић
Број индекса: 25100

17. јануар 2026.

Садржај

1 Увод

Случај Малоне Лам представља типичан пример person-to-person крађе криптовалута, у којој нападач не експлоатише техничку рањивост система већ понашање самог корисника. Циљ овог кратког рада је да, на основу јавних података, прикаже основне фазе напада, модел вероватноће успеха и основне импликације по сајбер безбедност.

Фокус је на *социјалном инжењерингу* као механизму за стицање почетног приступа, затим на праћу новца кроз више блокчејн мрежа и на улози формалних модела у разумевању ризика.

2 Теоријски оквир

2.1 Социјални инжењеринг

Дефиниција 1. *Социјални инжењеринг је контролисана психолошка манипулација људи са циљем да открију поверљиве информације или изврше радње које иду у корист нападача, а на штету сопствене безбедности.*

У контексту криптовалута, циљ нападача је да дође до *приватних кључева* или других акредитива (налог на берзи, резервне копије новчаника). Техничке мере заштите су често снажне, али корисник остаје најслабија карика.

2.2 Модел вероватноће успеха

Нека је $P(s)$ вероватноћа успеха напада, n број покушаја контакта са метом (телефонски позиви, поруке), а I мера квалитета информација о мети (контакт подаци, навике, финансијски профил). Једноставан модел гласи

$$P(s) = 1 - e^{-k \cdot n \cdot I}, \tag{1}$$

где је $k > 0$ параметар ефикасности нападачког тима.

Теорема 1. *За фиксно k, вероватноћа успеха $P(s)$ је монотоно растућа у односу на n и I.*

Лема 1. *Ако је $I = 0$, односно нападач нема никакве информације о мети, тада је $P(s) = 0$ без обзира на број покушаја n.*

Ови резултати формално потврђују интуицију да су систематично прикупљање информација и упорност кључни фактори успеха напада.

3 Анализа случаја Малоне Лам

3.1 Фазе напада и прања новца

У јавним материјалима о овом случају може се уочити неколико типичних фаза:

1. иницијални контакт и представљање као техничка подршка (нпр. *Google* или крипто берза),
2. стицање контроле над налозима корисника (мејл, облак, берза),
3. пренос средстава на новчанике које контролише нападач,
4. прање новца кроз више платформи и криптовалута.

Прање новца често укључује тзв. *chain hopping*, односно секвенцијалну конверзију из једне криптовалуте у другу:

- Bitcoin → Ethereum,
- Ethereum → Litecoin,
- Litecoin → Monero, криптовалута са појачаним механизмима приватности.

У поједностављеној табеларној форми, ток средстава се може приказати као:

Фаза	**Опис**	**Приближни износ (USD)**
1	Иницијална крађа са берзе	4 500 000
2	Касније трансакције и допуне	50 000 000+
3	Укупно опрана средства	230 000 000
4	Заплењена имовина (FBI)	59 000 000

3.2 Безбедносне импликације

Случај Малоне Лам показује да и релативно зрела инфраструктура као што је blockchain није довољна ако су процеси аутентикације и верификације корисника слабо дефинисани. Посебно је критично ослањање на један канал комуникације (телефон) и на неформалне процедуре ресетовања налога.

4 Закључак

У овом кратком раду приказан је сажет теоријски оквир за разумевање *person-to-person* напада на криптовалуте, као и примена тог оквира на случај Малоне Лам. Комбинација социјалног инжењеринга и вишестепеног прања новца доводи до напада велике финансијске вредности, при чему људски фактор остаје централна слабост.

Практична поука је да мере заштите морају обухватити не само техничке механизме (попут шифровања), већ и стандардизоване процедуре за рад са корисницима, обуку запослених и континуирано праћење аномалија у понашању налога.

Слика 1: Лого крипто менјачнице Gemini