Tracking Ransomware

Austin Zhang

Brief Rundown on Ransomware

- Encrypts files and demands payment
- Delivery: via malicious email attachments, pay-per-install networks
- Execution: silently encrypts valuable files, displays ransom note
- Payment: includes bitcoin purchase guide, addresses
- Initially demanded via online cash payment instruments
- Adopted Bitcoin and other cryptocurrencies

The Article

Government

The murky ecosystem of ransomware payments comes into focus in new research led by Damon McCoy, an assistant professor of computer science and engineering at the NYU Tandon School of Engineering. Ransomware attacks, which encrypt and hold a computer user's files hostage in exchange for payment, extort millions of dollars from individuals each month, and comprise one of the fastest-growing forms of cyber attack.

In a paper slated for presentation at the IEEE Symposium on Security and Privacy in May, McCoy and a team including researchers from the University of California, San Diego; Princeton University; Google; and the blockchain analytics firm Chainalysis provide the first detailed account of the ransomware payment ecosystem, from initial attack to cash-out.

Key findings include the discovery that South Koreans are disproportionately impacted by ransomware campaigns, with analysis revealing that $2.5 million of the $16 million in ransomware payments tracked by

The Paper

Tracking Ransomware End-to-end

Danny Yuxing Huang[1], Maxwell Matthaios Aliapoulios[2], Vector Guo Li[3]
Luca Invernizzi[4], Kylie McRoberts[4], Elie Bursztein[4], Jonathan Levin[5]
Kirill Levchenko[3], Alex C. Snoeren[3], Damon McCoy[2]

[1] Princeton University [2] New York University [3] University of California, San Diego [4] Google Inc [5] Chainalysis

***Abstract*—Ransomware is a type of malware that encrypts the files of infected hosts and demands payment, often in a cryptocurrency such as Bitcoin. In this paper, we create a measurement framework that we use to perform a large-scale, two-year, end-to-end measurement of ransomware payments, victims, and operators. By combining an array of data sources, including ransomware binaries, seed ransom payments, victim telemetry from infections, and a large database of Bitcoin addresses annotated with their owners, we sketch the outlines of this burgeoning ecosystem and associated third-party infrastructure. In particular, we trace the financial transactions, from the moment victims acquire bitcoins, to when ransomware operators cash them out. We find that many ransomware operators cashed out using BTC-e, a now-defunct Bitcoin exchange. In total we are able to track over $16 million in likely ransom payments made by 19,750 potential victims during a two-year period. While**

In this paper, we perform a large-scale, two-year measurement study of ransomware payments, victims, and operators. While prior studies have estimated the revenue for a single ransomware operation [6] or reverse engineered the technical inner works of particular ransomware binaries [11], [12], our study is the first to perform an end-to-end analysis of a large portion of the ransomware ecosystem, including its revenue, affiliate schemes, and infrastructure.

To do so, we combine multiple data sources, including labeled ransomware binaries, victims' ransom payments, victim telemetry (collected through an IP sinkhole we deploy), and a large database of Bitcoin addresses annotated with their owners (provided by Chainalysis[1]). This wealth of data allows us to follow the money trail from the moment a victim

TL;DR

- Research led by Damon McCoy reveals ecosystem of ransomware payments
- Traced Bitcoin transactions
- Executed real ransomware binaries in a controlled setting
- Estimated $16 million in ransoms from 19,750 potential victims
- South Koreans disproportionately impacted: $2.5m/$16m
- Identified BTC-e as a key cash-out point

Benefits

- Helps us better understand a threat that is challenging by nature to measure
- Identified BTC-e as a key cash out point.
- Conservatively estimate the amount of money extorted and number of victims affected

Challenges

- Coverage limitations on some ransomware families
- Intervention can be risky
- Must consider impact of victims

Final Thoughts

- Impressive, practical results
- Study limited by the nature of its subject
- No clear solution

Works Cited

1. “Exposed: The Path Of Ransomware Payments.” *Electronic Component News*, NYU Tandon School of Engineering, 23 Mar. 2018, www.ecnmag.com/news/2018/03/exposed-path-ransomware-payments.
2. Huang, Danny YuXing, et al. *Tracking Ransomware End-to-End*, San Francisco, CA, May 2018.