# Ransomware early detection by the analysis of file sharing traffic

Daniel Morato, Eduardo Berrueta, Eduardo Magaña, Mikel Izal

PII: S1084-8045(18)30300-X
DOI: 10.1016/j.jnca.2018.09.013
Reference: YJNCA 2213

To appear in: *Journal of Network and Computer Applications*

Received Date: 21 February 2018
Revised Date: 21 June 2018
Accepted Date: 21 September 2018

Please cite this article as: Morato, D., Berrueta, E., Magaña, E., Izal, M., Ransomware early detection by the analysis of file sharing traffic, *Journal of Network and Computer Applications* (2018), doi: https://doi.org/10.1016/j.jnca.2018.09.013.

# Ransomware early detection by the analysis of file sharing traffic

Daniel Morato[b], Eduardo Berrueta[a], Eduardo Magaña[a,c], Mikel Izal[a]

[a]*Public University of Navarre, Department of Automatics and Computing, Campus Arrosadia, 31006 Pamplona, Spain*
[b]*Institute of Smart Cities, calle Tajonar 22, 31006 Pamplona, Spain*
[c]*Naudit High Performance Computing and Networking S.L., calle Faraday 7, 28049 Madrid, Spain*

**Abstract**

Crypto ransomware is a type of malware that locks access to user files by encrypting them and demands a ransom in order to obtain the decryption key. This type of malware has become a serious threat for most enterprises. In those cases where the infected computer has access to documents in network shared volumes, a single host can lock access to documents across several departments in the company. We propose an algorithm that can detect ransomware action and prevent further activity over shared documents. The algorithm is based on the analysis of passively monitored traffic by a network probe. 19 different ransomware families were used for testing the algorithm in action. The results show that it can detect ransomware activity in less than 20 seconds, before more than 10 files are lost. Recovery of even those files was also possible because their content was stored in the traffic monitored by the network probe. Several days of traffic from real corporate networks were used to validate a low rate of false alarms. This paper offers also analytical models for the probability of early detection and the probability of false alarms for an arbitrarily large population of users.

*Keywords:* ransomware, malware detection, traffic analysis, network security

*Email addresses:* `daniel.morato@unavarra.es` (Daniel Morato), `eduardo.berrueta@unavarra.es` (Eduardo Berrueta), `eduardo.magana@unavarra.es` (Eduardo Magaña), `mikel.izal@unavarra.es` (Mikel Izal)