netwire_technical_analysis_report.pdf

Sida 3 av 17

2

INTRODUCTION

NetWire is a RAT that has been used by criminal organizations and other malicious groups since 2012. NetWire is distributed through various campaigns, and we usually see it sent through malicious spam (malspam).

Computers infected with this malware;

- To remote control
- Records keyboard strokes and mouse behavior
- to take screenshots
- To check system information
- To create fake HTTP proxies
- Allows access to data on the clipboard
- It allows access to data on various browsers.

Unlike many RATs, this one can target every major operating system, including Windows, Linux and MacOS.

PREVIEW

The NetWire malware in the examined version was combined with an Excel file and continued to spread with phishing methods. The malicious file was originally named “shipment.xlsm”. As the name suggests, it has targeted cargo companies and companies using it. First of all, it comes to us as an Excel document in order not to arouse suspicion. As a result of the analysis, it has been determined that this file acts as a loader to realize Stage 1.

File Name: shipment.xlsm

MD5 8fa508038223405c14000d0a2d909aa6

SHA1 4bbcb5766ec862e7a674ca9a420443bc18aa4855

SHA256 4426f68adbceaa14bd026618a134a3c84f83b546777f2f63bec6506d9fce9157
