Title: Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware

Author: Yasuyuki Tanaka Mitsuaki Akiyama Atsuhiro Goto

PII: S1877-7503(17)30629-4
DOI: http://dx.doi.org/doi:10.1016/j.jocs.2017.05.027
Reference: JOCS 696

To appear in:

Received date: 14-9-2016
Revised date: 24-5-2017
Accepted date: 28-5-2017

Please cite this article as: Yasuyuki Tanaka, Mitsuaki Akiyama, Atsuhiro Goto, Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware, <*![CDATA[Journal of Computational Science]]*> (2017), http://dx.doi.org/10.1016/j.jocs.2017.05.027

Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware

Yasuyuki TANAKA[a,c], Mitsuaki AKIYAMA[d], Atsuhiro GOTO[b]

[a] *Institute of Information Security (IISEC)*
2-14-1 Tsuruyacho, Kanagawa-ku,
Yokohama, Kanagawa, 211-0835, Japan
Email: dgs155102@iisec.ac.jp
[b] *Institute of Information Security (IISEC)*
[c] *NTT Communications Corporation*
[d] *NTT Secure Platform Laboratories*

Abstract

As the use of Internet increases, malicious activity has become increasingly problematic. In particular, drive-by download attacks have become a serious problem. As part of an *exploit-as-a-service* ecosystem for drive-by download attacks, malware download sites play a particularly important role. In this study, we analyzed approximately 43,000 malware download URLs to investigate malware distribution and the behavior of malware download sites over an extended period, i.e., over 1.5 years. We found that some sites survive for a very long time and are revived frequently, a finding not revealed in previous research. By focusing on the malware variation, we have identified three categories of malware download sites, i.e., *unchanged*, *every time changed*, *changed occasionally*. We found that 10% of *unchanged* sites survived for more than 500 days, and 10% of *changed occasionally* sites were revived more than 15 times in the entire observation period. We also analyzed sites in terms of IP address changes, anti-virus application results, URL features, and VirusTotal results. We found that each category had different attacker operational and resource characteristics. Finally, based on our findings, we discuss effective countermeasures for each category.

Keywords: measurement, analysis, modeling, malware, malware download site