Analysis of DNS Graph of Phishing Websites Using Digital Certificates

Yuki Ishida*, Masaki Hanada†, Atsushi Waseda†, Moo Wan Kim‡
* Graduate School of Informatics, Tokyo University of Information Sciences, Japan
† Department of Informatics, Tokyo University of Information Sciences, Japan
‡ TA Tech., Japan
Email: h22001iy@edu.tuis.ac.jp, mhanada@rsch.tuis.ac.jp

***Abstract*— The prevalence of phishing threats has grown substantially over the past several years. Because phishing domains generally have a very short lifetime to avoid detection, they must be identified as soon as possible to prevent damage. In general, phishers frequently reassign resources, such as domain names and IP addresses, to avoid detection. Consequently, multiple domains may be hosted by the same IP address, or vice versa. Furthermore, phishing websites often employ certificates and HTTPS encryption to appear more trustworthy. In this study, we focused on HTTPS-enabled phishing websites to construct and analyze DNS graphs of domain names and IP addresses of phishing websites using Certificate Transparency (CT) logs. From the analysis results, we examined the differences between benign and phishing websites in terms of the number of nodes per component and average node degree.**

***Keywords*— Phishing, DNS, DNS Graph, Security**

Yuki Ishida received the B.E. degree and M.S. degrees in Informatics from Tokyo University of Information Sciences, Japan, in 2014 and 2016, respectively. He worked at Digital Arts, Inc in 2016, and had been engaged in developing security products. In 2019 he joined SecureBrain Corporation in Japan, and has been engaged in research and development for cyber security. At the same time, he has been enrolled at the doctoral program of Graduate School of Informatics, Tokyo University of Information Sciences in Japan since 2022. His research interests include cyber security and network quality control. He is a member of the IEEE, IEICE and IPSJ.

Masaki Hanada received the B.E. degree in resources engineering from Waseda University in 1996, the M.S. degree in information science from Japan Advanced Institute of Science and Technology (JAIST) in 1999, and the M.S. and D.S. degrees in global information and telecommunication studies from Waseda University in 2003 and 2007, respectively. He worked at Waseda University and Tokyo University of Science. After joining Tokyo University of Information Sciences as an Assistant Professor in 2011, he has been a Professor in the Department of Information Systems, Tokyo University of Information Sciences, since 2019. His research interests include network QoS control, network resource control and management, and network security. He is a member of the IEEE, IEICE and IPSJ.

Atsushi Waseda received the B.E. degree in communication engineering from the University of Electro-Communications in 2000. He received his M.S. and Ph.D. in information science from Japan Advanced Institute of Science and Technology (JAIST) in 2002, and 2007, respectively. He worked at the National Institute of Information and Communications Technology and KDDI research inc. After joining Tokyo University of Information Sciences as an Assistant Professor in 2019. His research interests include information security, quantum security and privacy protection. He is a member of the IEICE and IPSJ.

Moo Wan Kim received B.E., M.E. and Ph.D degree in electronic engineering from Osaka University, Osaka, Japan in 1974, 1977 and 1980, respectively. He joined Fujitsu Lab. in 1980 and had been engaged in research and development on multimedia communication systems, Intelligent Network, ATM switching system and operating system. In 1998 he joined Motorola Japan and had been engaged in research and development on CDMA2000 system. In 2000 he joined Lucent Japan and had been engaged in research and development on W-CDMA system, IMS and Parlay. In 2005 he joined Tokyo University of Information Sciences and had been engaged in research on Ubiquitous Network. In 2022 he joined TA Tech. as a lecture.