Phishing Attacks Digital Trace Analysis for Security Awareness

Vyacheslav Zolotarev [1], Elena Zolotareva [1] *and* Vladimir Mawla [2]

[1] *Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarskii rabochii prospekt, Krasnoyarsk, 660037, Russia*
[2] *North-Caucasus Federal University, Prospect Kulakova, 2, 355000, Stavropol, Russia*

Abstract

The presented work contains recommendations for collecting a digital trail of phishing attacks. Some examples of algorithms for collecting a digital trace, studied indicators, and collected data are considered. The features of working with a digital trace are given. The authors also provide a set of functions that an attacked system must have in order to successfully collect evidence of a phishing attack. There are also specific recommendations for working in the area of increasing user awareness in this area.

The aim of the work is both to simplify the collection of evidence of such attacks, and to study the possibility of increasing the security of interaction between participants in network educational projects that are the object of social engineering attacks now. For this purpose, the examples given are tied to the properties of the object under study and are considered based on practical recommendations.

Keywords

Digital trace, phishing, education, attack, digital evidence

1. Introduction

Working with digital traces of attacks is one of the most important components of assessing their consequences and managing incidents as a whole process and forensic applications [1, 2], including from the legal side (for example, [3]). At the same time, different types of attacks generate different typical digital traces. It is advisable to single out both typical for certain attacks and for certain objects of the tactics of collecting a digital trace.

Considering the various phishing attacks [4-5], one can draw attention to the different types of data collected:

- technical data (device and process identifiers, packet and letter headers, etc.);
- organizational data (attacked positions and positions, departments and structural units);
- social data (parameters of social connections).

At the level of interaction with the attacked, parameters such as the response time to an attack (incident) associated with phishing, as well as the amount of damage from an attack (incident), expressed in various dimensions (time of elimination of consequences, damage economics, etc.) can also be used.

The sequence of data collection is negotiated separately. It is generally easier to collect technical parameters, which can also be collected automatically. For a phishing attack, a useful property in terms of collecting digital traces can be a common entry point to the system - a mail server or a general forum, file storage, which allows you to implement a single point of data collection.

Social and organizational parameters should be determined either on the basis of a comparison of technical data and, for example, an organizational structure (say, IP addresses and a network map

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: amida.2@yandex.ru (Vyacheslav Zolotarev); umka.82@mail.ru (Elena Zolotareva); vladimirmawla.vm@gmail.com (Vladimir Mawla)
ORCID: 0000-0002-8054-8564 (Vyacheslav Zolotarev); https://orcid.org/0000-0003-2495-344X (Elena Zolotareva); 0000-0002-5433-8934 (Vladimir Mawla)

associated with the organization's business processes), or on the basis of expert assessments and user surveys. It is also allowed to use forecasting of such parameters using statistics of attacks (incidents).

2. Indicators of Compromise

Therefore, for phishing attacks on various types of objects, one can distinguish both methods of identifying their consequences (indicators of compromise) and detecting an attack in the course of its implementation.

If we talk about indicators of compromise, then first of all they will show not the progress of the phishing attack itself, but the signs of its implementation. This means that such traces should be collected mainly in technical parameters - mail server logs, letter headers, anomalous operations. For example, logging in to a particular account or, say, launching certain software can be signs of this type of attack.

The main ways to collect indicators of compromise can be:

- Retrospective analysis of collected records. The goal will be to identify sequences of actions that begin with abnormal use of entry points or abnormal user feedback to requests.
- Iterative analysis of signs of compromise in various sources of collected data. The goal is both to find deviations and to poll users to confirm or deny the malicious intent of these deviations.
- Assessment of interactions. Users can be exposed to various types of phishing attacks at any given time. Therefore, it is necessary to evaluate changes in the interaction of users with external and internal data sources.
- Automation of work with heterogeneous sources of records. Collected records of different formats should be analyzed in a consistent manner to reduce response times.

In general, the problem of working with indicators of compromise for a phishing attack is the difficulty of predicting its development. In fact, working with traces of an attack, one can allow significant damage and encounter certain opposition, including the destruction of traces of an attack (intentional or unintentional) on the part of the attacker.

3. Digital trace of the attack

A digital trace will be a set of interrelated records, including those containing indicators of compromise, including for targeted attacks [6, 7]. The key features of using the collected digital trace will be response time and the success of detecting an attack (incident).

The following possibilities of collecting a digital trace can be distinguished:

- The collection of a digital trace is planned at certain "key points", which will be selected based on the model of interaction between the user and the system (depending on data flows, access control, an attacker's algorithm of actions, as well as predictive models of attack development, if such were foreseen and implemented in system).
- Formation of a digital trace should take into account the peculiarities of data exchange for a specific research object.
- Analysis of the digital trace should be possible at various stages of interaction - from the current values at the time of collecting the digital trace to the level that allows us to talk about the effectiveness of the actions of one or another participant in the field of secure data exchange and work with them.

4. Collecting information - basic steps

The key to successfully collecting digital trace data is working with the steps involved in generating attack data. An approximate sequence of steps for collecting data could be as follows:

- A unified data collection methodology should be formed. It should be accompanied by clear instructions for each type of phishing attack and each type of target; if appropriate (you cannot apply a generic methodology).

- Responsible for collecting information should be appointed. In fact, you will also need to work with the authority of those in charge to eliminate obstruction of collection by other employees.
- Digital trace collection tools such as SIEM or log collection systems are defined.
- Databases (knowledge bases) are formed containing various types of indicators of compromise for phishing attacks specific to a particular object.
- Methods of notification about fixed indicators of compromise are being formed. Methods of communication should also be provided for exchanging information about possibly detected attacks.
- Thus, the coverage by research algorithms of the total array of records collected in the field of the studied processes will be formed.

5. Evaluating the effectiveness of an attacker's actions

The overall effectiveness of the attacker's actions can be a consequence of the success of individual elements of the attack and should be assessed in accordance with certain logic.

The sequence of steps in the assessment should look like this:

- Assessment of possible targets of the attack - assets or resources.
- Assessment of possible problems, the solution of which may reduce the effectiveness of the attack. For specific issues (for example, low user awareness of information security tasks), an iterative assessment procedure should be provided.
- Assessment of the possible tasks of the attacker.
- Analysis of solutions applicable for a phishing attack aimed at a specific object.

As a result, metrics should be formed for the situation of a phishing attack, as well as countermeasures that reduce its effectiveness. Feedback (calculating or predicting response times) should also be evaluated and tested.

Applying this course of action should generate the following results:

- the risks of actions for the target of the attack (a specific employee, department) are assessed based on the tasks solved and the resources spent, the key of which is the risk of failure to achieve the goal, thus, the formation of a digital trace at this stage can be focused on calls to resources or assets and requests for specific tasks;
- a decrease in the number and lifetime of incidents that interrupt the process under study, depending on the organizational structure of such an incident and the reasons that cause it, which, when forming a digital trace, requires taking into account errors and failures in the execution of the attacker's task, including in small groups or as part of a network collaboration ;
- increasing the document ability (collection of records and evidence) of the process, which in turn improves quality management;
- collection of supporting and fixing documents and records;
- collection of input data for various business processes of the attack object.

6. Implementing indicators of compromise as components of the digital trace

Let us consider further examples of implementation of indicators of compromise as components of a digital trace. As an example, we will consider attacks on a mass mailing system for an educational resource (1); attack through the exchange of mail messages (2); attack on the educational forum (3). The goal of forming a set of indicators, as mentioned earlier, will be to increase user awareness and, through it, increase the security of data exchange within the framework of using the educational resource.

For educational resources such as forums, education management systems, and mass mailings, when viewed as the target of a phishing attack, there are many opportunities to collect digital traces. The positive properties of such an object are a single entry point for the attacker and the ability to control content; negative – the impossibility of blocking (prohibition) of some actions preventively.

Raising awareness through the collection of a digital trace and its study, including in a playful way, is one of the basic technological processes of the awareness raising process, often analyzed in scientific publications [8]. The work on gamification in the field of security education at the university correlates with similar work done by specialists who train employees in countering certain types of attacks [9]. The specifics of a particular type of activity can also be taken into account to assess the features of the digital trace, for example, a given type of technical support [10]. Game options for educational purposes can also be considered [11-13]. At the same time, it is possible to take into account the features of detecting a phishing attack, for example, by methods based on machine learning, the most significant examples of phishing attacks are identified and their parameters are used in the future as components of the digital trace [14, 15].

If we turn to the types of objects (1) - (3), then we can distinguish the following components of the digital trace that are characteristic of them:

Object type (1):

- archives of letters for retrospective analysis;
- Source and destination IP addresses;
- electronic signatures and certificates, as well as statistics of their use;
- facts of loading and changing content;
- facts of creation, removal and modification of links;
- facts of masking links and pre-texting;
- reverse request facts and analysis of such requests;
- spam filters triggering;
- statistics of transitions and calls to specific resources.

As can be seen from the list, for an object of type (1), it is possible to single out the focus of the attacker's work, focused on injection into public resources. At the same time, he seeks to verify the data uploaded to the mass mailing and mask the signature of the phishing attack.

Object type (2):

- the purpose of the appeals;
- email headers;
- archive of letters for retrospective analysis;
- signatures of attacking actions in emails and configurations;
- configuration of the mail server (servers);
- archive of network traffic;
- triggering an attack detection system;
- firewall triggering;
- statistics of clicks on links;
- Attachment download statistics.

The type of object under consideration (2) is a classic object for studying in phishing attacks. Here, indicators of compromise should be used primarily to identify attacked mail server accounts and assess the actions associated with them, including as part of a retrospective analysis of records of various system logs.

Object type (3):

- archives of forum posts and trends for retrospective analysis;
- IP addresses of sources and recipients, as well as identification data of user profiles and their accounts;
- electronic signatures and certificates, as well as statistics of their use;
- facts of loading and changing content;
- facts of creation, removal and modification of links;
- facts of masking links and pre-texting;
- reverse request facts and analysis of such requests;
- statistics of blocking accounts and requests for blocking, as well as the timing and consequences of blocking (using account cloning, etc.);
- statistics of transitions and calls to specific resources.

For an object of type (3), the fact of decentralization of control is often essential for an attacker. Global moderators can detect the fact of an attack after its implementation, while local moderators of forum threads may not pay attention to the triggering of automatic warnings (if any). At the same

time, it is advisable to work both with archived data (including recording the ignoring of system warnings by local moderators) and assessing the response time (separately for a local moderator; for a global moderator; for the system as a whole; for automatic response tools).

An example of collecting a digital trace, taking into account forecasting, can be the use of the following indicators and types of data (for an example of interaction through communication channels in a network educational project):

In database format:

- number of tracked users;
- number of tracked data types;
- coverage of user actions by controlling means;
- number of indicators of compromise;
- the state of the object before the attack;
- the state of an object after an attack (or on a specific control point).

In digital attack trail format:

- identifier or other designation of the attack;
- statistics of detected attack attempts;
- attacked accounts;
- successfully attacked accounts;
- successfully blocked accounts;
- statistics of reflected attacking actions;
- the state of the object before the attack;
- the state of the object after the attack.

As a result of the consideration, it can be noted that the formation of a digital trace even for such a standard object as an educational resource, and even for such a well-studied attack with fixed attack vectors such as phishing, can present significant complexity. It is associated both with the shortcomings of tools for detecting digital traces of an attack, and with a lack of user awareness and a high threshold for reaction to attacking actions.

7. Conclusions

The analysis of data on the possibilities of collecting a digital trail of phishing attacks, suitable for educational resources, has been carried out. Various variants of data are selected, which may be components of the digital trace, applicable in this task, their description and recommendations for use are given.

A brief overview of the implementation of collecting a digital trail of phishing attacks for individual attack targets has been completed. The possibilities and points of collection of the digital trace are presented.

The analysis of the possibilities of collecting a digital trace is carried out, taking into account the peculiarities of its application as data to increase user awareness.

The usefulness of the data presented lies in the methodological and algorithmic support for collecting a digital trace, and specifically indicators of phishing attacks, for the purpose of response and awareness raising.

8. Acknowledgement

This work was supported by the Russian Foundation for Basic Research project No19-013-00711 a.

9. References

[1] F. Servida, E. Casey. "IoT forensic challenges and opportunities for digital traces", Digital Investigation. 2019, vol. 28. pp 22-29. doi: 10.1016/j.diin.2019.01.012

[2] O. Omelian. "Concept and signs of digital traces that form during cybercrimes". Criminalistics and Forensics. 2020. pp. 457-466. doi: 10.33994/kndise.2020.65.45
[3] A. Galimkhanov, A. Khaliullina. "Procedure for detecting, seizing and recording digital traces of crime". The rule-of-law state: theory and practice. 2020, vol. 16. pp. 40-44. doi: 10.33184/pravgos-2020.4.22
[4] L. Kang, K. Chek, L. Choon. "A survey of phishing attacks: Their types, vectors and technical approaches". Expert Systems with Applications, 2018, vol. 106. pp. 1-20. doi: 10.1016/j.eswa.2018.03.050
[5] J.A. Chaudhry, S.A. Chaudhry, R.G. Rittenhouse. "Phishing Attacks and Defenses". International Journal of Security and Its Applications. 2016, vol. 10, no. 1, pp.247-256. doi: 10.14257/ijsia.2016.10.1.23
[6] Kaspersky Anti Targeted Attack Platform, Using indicators of compromise (IOC) and attack (IOA) for Threat Hunting. URL: https://support.kaspersky.com/KATA/3.7/en-US/194907.htm.
[7] E. Hutchins, M.J. Cloppert, R. M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation, 2010. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
[8] A. Yasin, L. Liu, T. Li, R. Fatima, W. Jianmin. "Improving Software Security Awareness Using A Serious Game". IET Software. 2019, vol. 13, no. 2, pp. 159-169. doi: 10.1049/iet-sen.2018.5095
[9] S. Hart, A. Margheri, F. Paci, V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education". Computers & Security, 2020, vol. 95, no. 101827. doi: 10.1016/j.cose.2020.101827
[10] M. Lapina, K. Lokhacheva, D. Parfenov, Designing of Information System for Semantic Analysis and Classification of Issues in Service Desk System // YRID-2020 Proceedings of the International Workshop on Data Mining and Knowledge Engineering Stavropol, Russia, October 15-16, 2020. CEUR Workshop Proceedings, 2021, 2842, Pp. 70-76, http://ceur-ws.org/Vol-2842/paper_8.pdf
[11] Strategies of social engineering attacks on information resources of gamified online education projects / V. V. Zolotarev, A. B. Arkhipova, N. Y. Parotkin, A. P. Lvova. – Text: electronic // CEUR Workshop Proceedings. – 2021. – Vol. 2861: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET–2020), Stavropol, 12–13 Nov. 2020. – P. 386–391. – URL: http://ceur-ws.org/Vol-2861/. – Publication date: 13.05.2021.
[12] Menelaos N. Katsantonis, Panayotis Fouliras, and Ioannis Mavridis. 2017. Conceptualization of Game Based Approaches for Learning and Training on Cyber Security. In Proceedings of the 21st Pan-Hellenic Conference on Informatics (PCI 2017). Association for Computing Machinery, New York, NY, USA, Article 36, 1–2. DOI: https://doi.org/10.1145/3139367.3139415
[13] Pirocca S., Allodi L., Zannone N. (2020) A Toolkit for Security Awareness Training Against Targeted Phishing. In: Kanhere S., Patil V.T., Sural S., Gaur M.S. (eds) Information Systems Security. ICISS 2020. Lecture Notes in Computer Science, vol 12553. Springer, Cham. https://doi.org/10.1007/978-3-030-65610-2_9
[14] F. Salahdine, Z. El Mrabet and N. Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 0250-0255, doi: 10.1109/UEMCON53757.2021.9666627.
[15] Tang L, Mahmoud QH. A Survey of Machine Learning-Based Solutions for Phishing Website Detection. *Machine Learning and Knowledge Extraction*. 2021; 3(3):672-694. https://doi.org/10.3390/make3030034