

Method and system for detecting a POS terminal network compromise

FIELD

[0001] The present technique relates to computer networking and, more particularly, to a system and method for detecting a POS terminal network compromise.

BACKGROUND

[0002] A Point-Of-Sale (POS) terminal is a hardware system for processing contactless payments. This system can accept payment cards with a chip or with a magnetic stripe, contactless cards, as well as other devices equipped with contactless interfaces, such as smartphones. For simplicity of presentation, such devices designed for contactless interfacing with a POS terminal will be hereinafter collectively referred to as bankcards regardless of specific design.

[0003] A POS terminal is also sometimes referred to as a hardware/software module installed at the paymaster's workplace and generally consisting of a computing device and the POS terminal module per se.

[0004] This computing device can be somehow compromised by fraudsters. If a POS terminal was successfully compromised, fraudsters get the opportunity to steal (copy) bankcard data that were used to make payments at this terminal. As a result, the bankcard also became compromised, and the stolen data, as a rule, are collected by the fraudsters and subsequently are posted up for sale in special web resources of so-called darknet (an Internet segment especially designed for anonymous communications).

[0005] A POS terminal network shall be understood to mean a system of POS terminals located in points of sale belonging to the same company. It is obvious that generally there are many different, usually independent, POS terminal networks in each city or region. For example, one such network can belong to a refueling stations company, another one to a flower shops chain, the third one to branches of a hotel complex, the fourth one to a restaurants chain, etc.

[0006] A method for transaction legitimacy automated verification using a postal code specified by the bankcard owner during the bankcard issuing is known from the prior art. This check is called "Address Verification System" or AVS. The verification is based on the fact that the cardholder knows the postal code that he or she indicated when issuing the card. When trying to make a payment or transfer, the cardholder is asked for information about this postal code. If the postal code specified by the cardholder matches the postal code specified during the bankcard issuing, then the transaction is considered legitimate.

[0007] Based on the Address Verification System's postal code check, a transaction legitimacy automated verification system was developed, which, upon receipt of transaction data,

compares the post address of ongoing transaction against a limited list of post addresses pre-established as allowed for this transaction. The list of allowed addresses is built in advance based on principle of proximity to the home address of the bankcard holder. The home address and postal code should be disclosed by the bankcard holder during issuing the bankcard. It is assumed that the bankcard holder will make most of the purchases in a relative proximity to home. It is not assumed that the bankcard holder will make purchases from remote locations, for example, from different parts of the world. Consequently, if fraudsters had stolen card data and try to use these data by making a transaction from a location far from the bankcard holder's home, such transaction will be automatically blocked by the bank. At present, such automatic verification system is implemented and intensively used by many banks. However, when the principle of AVS operation became known to fraudsters, they had found ways to bypass it as well.

[0008] As was mentioned above, fraudsters sell databases containing information about compromised bankcards in specialized online stores of darknet. Generally, databases of two types are offered for sale, CC and DUMP. CC type databases contain text data comprising card number, expiration date, CVV code, owner's name, etc. As a rule, these data were collected by fraudsters when a user disclosed them during shopping in a web store. DUMP type databases contain information copied from magnetic stripe or chip on a plastic card. Just these databases fraudsters form as a result of POS terminals compromise. Anybody skilled in the art can write such information onto a blank medium and fabricate a physical copy of a compromised card. The physical copy of bankcard can be thereafter used by intruders to pay in conventional offline stores that accept payments from bank cards. Hereinafter, DUMP type databases containing information copied from plastic cards are referred to as "bankcard dump databases" or simply "dump databases".

[0009] Besides the information copied from a plastic card, a bankcard dump database indicates, as a rule, compromise location for this card, more particularly, postal code of the area where the compromised POS terminal through which the intruder copied the card information was located. It is necessary to provide a potential buyer with possibility to bypass AVS systems when using the acquired bankcard data. In other words, a buyer usually should purchase the bankcard dump database with postal codes corresponding to the region where he or she intends to use the fabricated copies of bank cards for offline purchasing. In this manner, intruders succeed in bypassing AVS systems since transactions each time take place in stores that are located physically close to the place where the original but compromised bankcard was issued.

[0010] In particular, it is known that the leak of bankcard data that occurred in 2014 from Sally Beauty company's points of sale was exactly the result of the POS terminal network

compromise. Articles on investigations into this case (in English) as of application filing date are available at the following URLs:

<https://krebsonsecurity.com/2014/03/sally-beauty-hit-by-credit-card-breach/> и
<https://krebsonsecurity.com/2014/03/zip-codes-show-extent-of-sally-beauty-breach/comment-page-1/>.

[0011] These publications disclose the fact that the source of data leak was possible to establish by comparing list of postal codes from the bank cards dump posted up in the darknet with the list of postal codes within the area where Sally Beauty chain's points of sale were located, full coincidence of these lists being used as a criterion for making a decision on POS terminal network compromise.

[0012] However, said articles do not disclose any methods for detecting a compromised POS terminals network, if lists of postal codes from the bank card dump and a company's points of sale does not fully coincide. Besides, said articles do not disclose any methods of automated data analysis that would allow to identify a company's compromised POS terminals network among a variety of other companies having points of sale within areas that corresponds to the list of postal codes from the bank card dump.

[0013] Technical solutions are also known from the prior art that enable to detect the fact of leakage of bank card data. In particular, U.S. patent US 11062317 B2 (Akli Adjaoute, DATA BREACH DETECTION, publ. 07/13/2021, Int. Cl. G06Q 20/40, G06Q 30/02) is known disclosing a method for detecting data leakage by analyzing transaction records in real time. Suspicious transactions are compared with routine transactions typical for the same client over days, weeks, or months. All bank cards from which suspicious transactions were made are registered in an integrated database. This database is used to investigate suspicious transactions in any company. An identifier is formed for each company in order for subsequent tracking and collecting information on the transactions conducted by this company. Based on this information on transactions, a probability of fraud is calculated. If the calculated probability becomes greater than the specified threshold value, a warning is generated about a possible data leak and the suspected compromise location.

[0014] However, it is obvious that this method can only be implemented when a detailed information about transactions history is available, access to transaction database of the card issuing bank being obligatory for its implementation.

[0015] The present technique is aimed at elimination of at least some disadvantages inherent to solutions known from the prior art. In particular, the described method does not require access to a bank transaction history or other similar information to identify a compromised POS terminals network.

SUMMARY

[0016] Within the context of this description, unless expressly stated in the field, the special terms listed below are used to mean the following:

[0017] Compromised POS terminals network is a network in which a malicious hardware or software has been installed on at least one POS terminal to copy bank card data.

[0018] Area identifiers can be postal codes, ZIP codes, geocodes, street names, block names, district names, city names, county names, municipality names, county names, state names, province names, region names, country names, etc.

[0019] Compromised areas are areas whose identifiers are listed in a bankcard dump database posted up for sale.

[0020] Compromised area identifiers are identifiers of areas specified in a bankcard dump database.

[0021] Higher level administrative and territorial unit (HLATU) is a unit of administrative and territorial division in a particular country that is one level higher than the given area. HLATU for an area corresponding to a specific postal code or ZIP code is, for example, district in Russia or county in the USA. In turn, HLATU for district in Russia is region while HLATU for county in the USA is state. It is obvious that the region or state is also a HLATU for an area corresponding to a post code or ZIP code.

[0022] List of potentially compromised companies is a list of companies that own points of sale located in a compromised areas.

[0023] Bankcard dump database is a database containing information copied from the magnetic stripe or chip of original bank cards. Also referred to as the dump database here for brevity.

[0024] The technical problem to be solved by the claimed technical solution is creation of the computer implementable method and system for detecting compromise of a POS terminals network owned by a certain company. The method and system for detecting a POS terminal network compromise are disclosed in independent claims. Additional embodiments of the present technical solution are presented in dependent claims.

[0025] The technical result consists in providing automated detecting a POS terminal network compromise.

[0026] The claimed technical solution is a computer implementable method for detecting a POS terminal network compromise. This method comprises steps of obtaining identifiers of compromised areas; creating a database of potentially compromised POS terminals networks; determining parameters of compromise for at least one POS terminals network; determining

probability of compromise for at least one POS terminals network; creating a compromise probability ranked list of POS terminals networks, and identifying at least one POS terminals network from the ranked list as compromised one.

[0027] One possible embodiment of the disclosed method comprises preliminary creating a geographic database and a database of commercial companies.

[0028] Another possible embodiment of the disclosed method comprises after obtaining a set of compromised areas identifiers, determining the country to which said compromised areas identifiers belong using queries to a preliminarily prepared geographic database.

[0029] Yet another possible embodiment of the disclosed method comprises determining parameters of compromise using queries to a preliminarily prepared database of commercial companies.

[0030] Yet another possible embodiment of the disclosed method, wherein the database of potentially compromised POS terminals networks comprises at least: compromised areas identifiers; names of companies owning the POS terminals networks located in compromised areas; post addresses of points of sale owned by companies owning the POS terminals networks located in compromised areas, and higher level administrative and territorial units (HLATU) corresponding to the compromised areas.

[0031] Yet another possible embodiment of the disclosed method, wherein parameters of compromise for a chosen POS terminals network include: quantity of identifiers of compromised areas containing at least one point of sale owned by a chosen company; total quantity of compromised area identifiers; quantity of points of sale owned by the chosen company and located within the compromised areas, and total quantity of points of sale owned by the chosen company and located within all HLATUs corresponding to the compromised areas.

[0032] Yet another possible embodiment of the disclosed method comprises determining probability of compromise for at least one POS terminals network as the multiplication of a POS terminals networks frequency within the compromised areas for the chosen company by a probability of occurring POS terminals networks owned by this company within the compromised areas.

[0033] Yet another possible embodiment of the disclosed method comprises determining the POS terminals networks frequency within the compromised areas for a chosen company as the ratio of quantity of identifiers of compromised areas containing at least one point of sale owned by a chosen company to the total quantity of compromised area identifiers.

[0034] Yet another possible embodiment of the disclosed method comprises determining probability of occurring POS terminals networks owned by a chosen company within the compromised areas as ratio of quantity of points of sale owned by the chosen company and located

within the compromised areas to the total quantity of point of sale owned by the chosen company and located within all HLAUs corresponding to the compromised areas.

[0035] Yet another possible embodiment of the disclosed method comprises defining the compromised POS terminals network as the POS terminals network that has the highest value of compromise probability.

[0036] Yet another possible embodiment of the disclosed method comprises defining compromised POS terminals networks as all POS terminals networks that have calculated values of compromise probability exceeding a preset threshold value.

[0037] The claimed method is implemented in a system for detecting compromise of a POS terminals network comprising at least a processor and a long-term memory containing at least one database and machine-readable instructions, which, if being executed by the processor, implement the described method.

DESCRIPTION OF THE DRAWINGS

[0038] Implementation of the technique will be further described in accordance with the attached drawings, which are presented to clarify the technique chief matter and by no means limit the field of the technique. The following drawings are attached to the application:

[0039] Fig. 1A illustrates a method of detecting a POS terminal network compromise.

[0040] Fig. 1B illustrates step of determining parameters of POS terminals network compromise being a part of the POS network compromise detecting method.

[0041] Fig. 2 exemplifies a schematic diagram of the computing device.

DETAILED DESCRIPTION

[0042] Numerous implementation details intended to ensure clear understanding of this technique are listed in the detailed description of the technique implementation below. However, it is obvious to a person skilled in the art how to use this technique as with the given implementation details as without them. In other cases, the well-known methods, procedures and components have not been described in details so as not to obscure the present technique.

[0043] Besides, it will be clear from the given explanation that the technique is not limited to the given implementation. Numerous possible modifications, changes, variations and replacements retaining the chief matter and form of this technique will be obvious to persons skilled in the art.

[0044] The present technique is aimed at creation of the computer implementable method and system for detecting a POS terminals network compromise. POS terminals can be compromised by intruders by installing malicious software or hardware such as a so-called

skimmers onto these terminals. Every time someone uses a bank card to pay through a compromised POS terminal, details of the bank card used for this purpose are copied by fraudsters. Fraudsters aggregate collected data into dump databases and post them up for sale in specialized web resources, namely, in so-called darknet.

[0045] In addition to data copied from magnetic stripes or chips of bank cards, dump databases frequently contain also identifiers of areas where these data were copied using compromised POS terminals. Compromised areas identifiers can comprise, for example, postal codes or ZIP codes. Besides these identifiers, dump databases may additionally contain information about city and/or country corresponding to said identifiers.

[0046] For example, each entry in the dump base can be supplemented with a following line:

73301, USA,

where 73301 is an American postal code (ZIP code) while USA indicates the country related with this code.

[0047] Thus, the entry concerning any bank card in the dump base is always associated with a compromised area identifier, which indicates a specific area where the compromised POS terminal was located, and where presented bank card data were collected.

[0048] However, just these compromised area identifiers contained in a dump database can be used to identify compromised POS terminal networks.

[0049] As shown in Fig. 1A, claimed method of detecting a POS terminal network (100) compromise can be implemented as follows.

[0050] One possible embodiment of the disclosed method comprises the preliminary step of forming a geographic database containing information about all existing area identifiers (for example, postal codes) and related countries. Such database can be formed in any well-known way using open Internet sources.

[0051] To build a geographic database, a preliminary written script that implements functions of a crawler (search robot) and a parser can be used, for example. At first, the script is used to form and send search queries to any public search engine such as Google or Yandex based on preliminarily prepared list of countries and regions of the world. These search queries may, for example, in the case of postal codes have the following form:

"list of codes of [country_name]" or

"list of postal codes of [country_name]",

where field [country_name] in each query is substituted with specific name of the next country or region from the preliminarily prepared list of countries and regions of the world. Similar search queries can be generated for street names, city names, or other area identifiers.

[0052] Then search results for each sent query are analyzed using the same script, and at least one web resource containing the searched list is selected. Finally, the same script is used to go to selected web resource, parse the list and save the list in the database, adding respective name of country and adopted in this country designation of this identifier to each list element in the database. For example, adopted identifier can be ZIP code or postal code in USA or post index in Russian Federation, etc.

[0053] Alternatively, a geographic database can be built based on commonly known open web resources such as www.worldpostalcode.org, города-россия.рф, etc. containing area identifier lists categorized by country.

[0054] Thereafter lists formed for different countries are merged. If the same code is encountered in several countries, all these countries are indicated in a special consolidated list for this code. In such manner, a database is formed consisting of entries, each of which looks, for example, like this:

'90630' – Estonia, Finland, USA.

[0055] Additionally, geographic database for each country is provided with sets of keywords in the state languages of this country to designate institutions where POS terminals can be installed. As a non-limiting example, the following sets of keywords for Russia, United States and Finland can be provided:

Russia: аптека, банк, столовая, магазин, торговый центр, казино...

USA: drugstore, bank, foods, shop, mall, casino...

Finland: apteekki, pankki, ruokala, kauppa, supermarket, kasino ...

[0056] Another possible embodiment of the disclosed method comprises forming at a preliminary stage a database of commercial companies for each country. A database of commercial companies is formed on the basis of a country-specific list of area identifiers (for example, list of postal codes existing in the given country).

[0057] Then the list of points of sale (offices, shops, restaurants, bank branches, etc.) covered by each identifier (for example, located within area corresponding to a definite ZIP code in USA) is formed and saved in the database of commercial companies.

[0058] This can be done by generating queries to open sources such as Google maps, GIS2, Mapsme, Yandex maps, or Yellow pages with syntaxes specific for these sources from the computing device using a preliminarily prepared script. If, for example, Google maps are used as the source and the database of commercial companies is built for Russia, then search queries generated for the area identifier (post index) 123098 may be following appearance:

Россия индекс 123098 аптека (Russia index 123098 pharmacy),

Россия индекс 123098 банк (Russia index 123098 bank),

Россия индекс 123098 кафе (Russia index 123098 cafe),
 Россия индекс 123098 магазин (Russia index 123098 shop),
 Россия индекс 123098 торговый центр (Russia index 123098 supermarket),
 and so on. Obviously, a set of names and post addresses of corresponding points of sale located in the area corresponding to this index will be sent by search engine in response to such query. Proper keywords such as bank, pharmacy, canteen, etc. are chosen specific for the country, for which the database is being built.

[0059] A set of points of sale obtained for each area identifier is ordered by names of companies in any commonly known way and saved in the database of commercial companies as a supplement to said identifier.

[0060] In addition, each of so found companies in database of commercial companies can be associated with the identifier of area where the company is located as well as all relevant HLATU. For example, the company

Pharmacy "Floria", Moscow, 123098, Bochvara street, 10A

in the database can be associated in any commonly known way with post index 123098 and the following HLATUs: Northwestern Administrative District of Moscow, Moscow, Central Federal District of Russian Federation.

[0061] Alternatively, database of commercial companies for each country can be formed manually by operator.

[0062] All above listed actions are non-specific, are well known to those skilled in the art, and can be performed in any commonly known manner.

[0063] Results of the preliminary step are the geographic database, in which each area identifier is associated with name of at least one country where the area denoted by this identifier is located, and the database of commercial companies, in which each commercial company is associated with the area identifier, for example, postal code or post index, and at least one HLATU.

Step 110. Obtaining identifiers of compromised areas

[0064] The claimed method 100 begins from step 110 where the computing device obtains a set of compromised areas identifiers. As mentioned earlier, such identifiers can comprise, without limitation, postal codes, ZIP codes, post indexes, names and/or numbers of individual buildings, as well as names of streets, blocks, districts, cities, okrugs, counties, communes, voivodeships, provinces and other administrative and territorial units. Below, principle of claimed method operation will be demonstrated using US postal codes (ZIP codes) as an example; however, any other identifiers, without limitation, can be used instead in a similar way. Hereinafter postal codes may be referred to as simply codes or ZIP codes.

[0065] At step 110, compromised area identifiers and related information (for example, name of the country), if any, are extracted from the dump database and transferred to the computing device. This can be done in any commonly known way, for example, using a script that implements parser functions in order for automatic reading all text lines from the dump database posted up for sale and save them on the computing device.

[0066] One possible embodiment of the method disclosed comprises obtaining by computing device only a previously extracted from a dump database set of compromised area identifiers without any accompanying information about countries related with said identifiers.

[0067] Another possible embodiment of the method disclosed comprises obtaining by computing device both set of compromised area identifiers associated with bank cards and accompanying information about countries related with said identifiers.

[0068] In all possible embodiments, step 110 comprises deduplicating the obtained list of compromised area identifiers by the computing device, that is, removing duplicate identifiers are from the list. As a result, a modified list of unique compromised area identifiers is obtained and saved in the database.

[0069] One example of a set of compromised area identifiers containing 951 identifiers is presented below.

[0070] ['72076', '92867', '90630', '94565', '33612', '77379', '89123', '33809', '90712', '75056', '04106', '80016', '89052', '33169', '34741', '33467', '34119', '78045', '17404', '75070', '92083', '65804', '33511', '70663', '07457', '85204', '72032', '28117', '85296', '37919', '71292', '76011', '72212', '85032', '76177', '33896', '30519', '81601', '78154', '23602', '30014', '80601', '33027', '75034', '78660', '29607', '75126', '78155', '80110', '76201', '67206', '23456', '78738', '32703', '74135', '92555', '27713', '48101', '14580', '33012', '84003', '72401', '07936', '30720', '01810', '78501', '34481', '73132', '78410', '85374', '78235', '30062', '37129', '28078', '32534', '78664', '30052', '34769', '85635', '48228', '34711', '76182', '32312', '85365', '32757', '28303', '68137', '75052', '35235', '27105', '92591', '33556', '33309', '28602', '77511', '28704', '08753', '30144', '10941', '91763', '95670', '77505', '73110', '35601', '90242', '01803', '33186', '33781', '44115', '85209', '90303', '11385', '72015', '30097', '01453', '32225', '32960', '95678', '33433', '80134', '94066', '04401', '85206', '28546', '36303', '75023', '75965', '33021', '71270', '02762', '78613', '33919', '92336', '76039', '81008', '92562', '33913', '75110', '91387', '90660', '17601', '79414', '33180', '77833', '33566', '39110', '02865', '32159', '47129', '76028', '37064', '32832', '70507', '37221', '74501', '77357', '76711', '92545', '07094', '34222', '32218', '95380', '33859', '77303', '28216', '32608', '32765', '76048', '86429', '34639', '75013', '85746', '86314', '71913', '33461', '34787', '10954', '77037', '95242', '73134', '79102', '10505', '32792', '32940', '86001', '33823', '85035', '03060', '21014', '27030', '78245', '33618', '33426', '92374', '37076', '76108', '78028', '75771', '74008', '75211', '28805', '28470', '33324', '93907', '95630', '24740', '30106', '33126', '39206', '79606', '32746', '87110', '73505', '75119', '93534', '06492', '77840', '91910', '77338', '77573', '78109', '80124', '85086', '34613', '33062', '95928', '33132', '33909', '80011', '95122', '95037', '17111', '74401', '32701', '34668', '11735', '71457', '93230', '06010', '78572', '06484', '75062', '75237', '91765', '28262', '93312', '76063', '72450', '92408', '37115', '78541', '03784', '78596', '30542', '07424', '37027', '75901', '33030', '28217', '48104', '70791', '27203', '78753', '34689', '37415', '78205', '37604', '93277', '32503', '80123', '78610', '78745', '91784', '76021', '33323', '65616', '27502', '87123', '75156', '45440', '01501', '33410', '92223', '77581', '32818', '77085', '07073', '87124', '28056', '78752', '77396', '31322', '48375', '76132', '33543', '70068', '15122', '37203', '37214', '78526', '80234', '28043', '30078', '71603', '32003', '37701', '76401', '78634', '24012', '71446', '07310', '30101', '30161', '11590', '90620', '85737', '02150', '14564', '84065', '70301', '29621', '77027', '77346', '85051', '64081', '30121', '39503', '77571', '93551', '75503', '30043', '92108', '92508', '78259', '89118', '88201', '90605', '95051', '26501', '74012', '06702', '32405', '33763', '48150', '30013', '06095', '72956', '32826', '70816', '95758', '77007', '77515', '33778', '33414', '83706', '92311', '30189', '70726',

'75040', '34266', '37772', '77598', '91320', '23322', '78332', '80023', '48917', '37067', '80246', '30534', '15904', '27529', '48083', '92025', '95993', '77079', '78748', '06416', '81505', '71105', '15238', '93313', '95687', '91324', '75063', '33409', '11731', '27545', '70560', '79072', '79936', '84014', '21093', '74133', '77354', '84720', '92886', '34293', '85743', '34986', '92392', '93274', '81101', '64057', '91730', '68505', '05201', '38138', '27262', '21236', '11714', '78602', '91709', '29730', '91307', '48092', '70460', '30606', '73703', '88310', '78102', '25801', '77388', '75218', '75662', '95356', '72756', '77070', '76502', '89503', '80922', '88240', '34997', '37934', '27587', '93036', '32174', '38017', '34957', '30096', '88220', '85027', '32258', '94531', '27103', '33071', '72802', '93117', '70808', '32571', '74464', '46142', '95118', '33156', '13214', '16148', '85201', '27403', '72143', '92606', '38501', '78852', '21222', '90503', '31406', '76801', '34714', '41042', '87106', '32114', '93635', '02904', '48307', '32086', '76148', '77656', '74075', '75098', '77040', '95035', '28025', '94520', '48316', '93065', '80538', '94588', '08816', '01851', '30269', '28607', '60450', '75022', '91915', '80501', '78654', '71301', '74601', '33625', '94587', '75149', '94538', '17050', '91381', '91748', '33331', '30141', '94550', '37066', '80634', '06040', '75801', '13021', '34606', '64801', '80525', '25504', '73401', '32177', '28277', '30324', '78064', '07724', '07733', '14845', '30338', '30022', '06070', '87532', '14221', '03079', '70471', '28403', '33541', '39402', '48195', '89117', '23666', '02184', '30501', '79924', '06382', '12077', '77449', '85226', '77630', '07446', '23510', '32809', '94928', '12205', '28227', '80108', '75090', '75670', '02917', '76087', '92532', '74019', '05495', '37402', '75605', '34429', '02032', '06351', '95834', '10950', '30329', '75044', '76067', '06489', '17013', '33948', '06111', '85281', '12601', '93955', '10994', '93720', '91750', '84790', '91316', '41076', '86403', '78749', '15237', '77550', '13090', '78570', '79925', '34677', '77459', '45805', '29418', '31909', '75087', '32256', '70526', '20166', '38606', '11706', '43302', '77565', '77380', '95010', '76710', '84070', '92881', '13850', '45044', '14226', '71111', '30047', '07836', '89109', '77494', '06320', '21784', '92054', '30253', '77478', '80026', '79423', '01035', '77429', '77414', '84102', '27896', '02379', '33596', '06810', '48066', '15601', '27540', '01867', '85305', '72205', '77521', '06033', '33477', '90802', '73099', '80132', '27617', '38655', '28625', '07728', '69101', '74361', '30260', '91016', '14304', '08902', '32097', '87402', '78539', '75150', '76262', '78666', '80021', '75028', '87507', '78582', '41017', '93446', '02842', '84084', '28387', '02767', '77065', '78520', '27804', '70809', '78130', '28273', '37160', '68510', '78503', '28226', '02360', '14850', '37090', '79109', '33024', '43219', '38671', '87031', '64506', '80012', '27534', '10314', '77057', '95020', '77034', '78412', '85541', '11720', '43240', '01128', '88101', '87004', '87120', '32536', '06512', '60435', '08822', '76033', '37167', '45251', '78230', '75007', '84404', '11742', '76904', '78750', '16602', '34233', '45424', '76548', '39465', '90266', '45069', '76309', '46368', '78006', '78756', '40353', '90631', '75104', '75460', '77377', '40601', '79705', '76240', '32413', '35806', '70058', '75165', '38133', '43056', '40511', '73118', '72903', '01923', '23185', '44446', '76543', '78209', '01886', '33615', '38305', '85042', '03276', '76308', '78250', '85210', '85382', '43623', '46804', '43512', '45013', '92656', '45373', '77584', '91791', '92024', '75230', '34231', '02019', '45504', '38117', '44906', '70737', '40324', '47374', '75248', '70601', '45420', '70401', '46805', '45245', '75402', '68521', '92691', '77640', '60123', '66604', '77029', '38804', '40503', '72653', '30041', '45040', '66801', '79121', '64055', '45459', '73013', '34208', '36535', '74055', '84119', '45385', '75081', '30286', '68516', '43202', '23321', '80033', '82009', '45014', '78758', '64468', '60440', '43068', '70510', '68601', '77471', '85339', '85711', '92110', '12065', '80918', '45011', '76051', '43026', '40422', '15401', '40475', '46410', '43130', '66502', '46383', '46825', '75701', '85205', '45255', '46530', '30004', '40356', '45840', '03874', '45449', '70360', '46580', '78573', '45066', '07652', '78550', '85284', '61354', '74820', '85008', '41056', '85302', '46703', '78504', '46526', '74701', '46706', '43123', '45365', '44512', '46375', '46750', '43040', '71291', '43537', '85012', '85282', '43617', '60805', '82070', '68847', '08820', '46818', '45231', '85395', '32550', '45238', '78374', '46321', '60115', '60050', '86301', '82636', '60099', '40391', '85705', '46563', '60525', '43420', '45601', '43536', '82716', '60409', '46514', '46755', '85741', '60915', '73533', '46628', '46614', '82901', '68467', '79106', '39564', '68803', '60652', '78521', '60478', '73521', '69162', '68901', '60707', '84041', '33559', '77024', '75088', '32223', '43228', '85122', '74006', '76137', '30331', '32801', '53201', '89044', '19019', '30301', '33601', '60007', '60090', '60148', '60290', '66217', '67114', '73101', '80002', '80010', '80020', '80126', '80301', '80521', '81433', '81615', '89002', '89028', '91355', '92071', '92647', '94301'].

[0071] In above example, only area identifiers were extracted from a dump database, and there is no any indications to a country related to these identifiers. In similar situations, queries are sent to the previously prepared geographic database from the computing device, and the country related with these identifiers is determined. This problem can be solved in any commonly known way by choosing the country related with the largest number of identifiers.

[0072] If, for example, queries to a geographic database for the sample of three identifiers: '72076', '92867', and '90630' yielded the following result:

'72076' – Germany, USA,
 '92867' – USA,
 '90630' – Estonia, Finland, USA,

then the country to be chosen as related with all these identifiers is United States.

[0073] In another embodiment, when both compromised area identifiers and information about related countries was obtained from the dump database, queries to the geographic database are not required.

[0074] At that, step 110 is completed, and the method proceeds to step 120.

Step 120. Creating a database of potentially compromised POS terminal networks

[0075] Further, the computing device that implements the claimed method proceeds to step 120, which is aimed to forming database of potentially compromised POS terminal networks. This database consists of the set of compromised area identifiers obtained at the previous step, each identifier being associated with a list of companies that own points of sale located in respective compromised area, and each point of sale being provided with its post address.

[0076] It is understood that a first embodiment is possible, when many points of sale technically belong to one POS terminal network and are owned by the same company, but have different post addresses. At the same time, the second embodiment is also possible, when each point of sale of the same company has its own, technically separate, network of POS terminals. However, dump database hardly contains information that would allow to reliably distinguish between said first and second embodiments of those POS terminals network that originated appearance of the specific compromised area identifier in the dump database. For this reason, the set of all points of sale owned by a particular company and located in a compromised territory was adopted as a POS terminals network within the scope of the claimed method.

[0077] In addition, each identifier at this step is associated with HLATU (Higher Level Administrative and Territorial Unit) in a corresponding country. In particular, in the example under consideration, where US ZIP codes are the compromised area identifiers, the role of HLATU can play, for example, the state related to a given ZIP code.

[0078] To form the database, queries to open sources such as Google maps, GIS2, Mapsme, Yandex maps, or Yellow pages with syntaxes specific for these sources may be generated by the computing device using a preliminarily prepared script. If, for example, Google maps are used as the source, then search queries generated for the area identifier 90630 may have the following appearance:

usa postal code 90630 drugstore (in response, the search engine will return a list of names and addresses of pharmacies located in the area corresponding to ZIP code 90630),

usa postal code 90630 bank (a list of banks will be returned),

usa postal code 90630 foods (a list of public catering establishments will be returned),

usa postal code 90630 shop (a list of shops will be returned),

usa postal code 90630 mall (a list of supermarkets will be returned),

usa postal code 90630 casino (a list of gambling establishments will be returned),

and so on.

[0079] The keywords such as bank, shop, foods, as well as the name of country and particular area identifier for the queries (in above examples, it was 'postal code' while in queries in Russian it would be 'post index', etc.) are selected by the script from the geographic database in accordance with rules of the country related with compromised area identifiers.

[0080] The lists of POS terminal networks (or points of sale) obtained for each area identifier are ordered by names of companies and saved in a database of potentially compromised POS terminal networks in association with those identifier for which each list was built. For example, a fragment of such list for ID 90630 might look like this:

Marshalls, 9801 Walker St, Cypress, CA 90630.

...

McDonald's, 10011 Valley View St, Cypress, CA 90630,

McDonald's, 4125 Ball Rd, Cypress, CA 90630,

[0081] An alternative embodiment of the claimed method is possible, when queries are made to a preliminary formed database of commercial companies rather than open sources such as Google maps. In such case, queries are built in any commonly known way to a selected database of commercial companies corresponding to the country related with obtained compromised area identifiers, each query containing the next compromised area identifier taken from the list of identifiers obtained at step 110.

[0082] In response to each such request, a list of all selling venues (or POS terminal networks) related to indicated identifier will be obtained from the database of commercial companies.

[0083] Additionally, names of companies that own the POS terminal network data are extracted from the list of POS terminal networks built for each identifier in any of above described ways and both lists of POS terminal networks and company names are saved in the database of potentially compromised POS terminal networks.

[0084] The following list of companies owning selling venues with addresses related to the identifier 90630 that was formed using the claimed method is presented below for example:

Marshalls,
 Nothing Bundt Cakes,
 Five Guys,
 AT&T,
 Verizon Wireless,
 McDonald's.

[0085] In addition, at least one HLATU is assigned to each compromised area identifier. To do this, the query to a search engine is generated by a script, which for the aforementioned ZIP code 90630, for example, may look like the following:

usa postal code 90630

In response to such query, the search engine will return information about HLATU corresponding to queried ZIP code, which can appear in the example under consideration as follows:

Orange County, CA, USA.

[0086] Either county, or state, or both can be indicated as HLATU in accordance with the claimed method. A state as a HLATU will be shown hereinafter as a non-limiting example.

[0087] Yet another possible embodiment of the method disclosed comprises sending the query to a preliminary formed database of commercial companies, a compromised area identifier being used as the keyword in the query. In response, a list of points of sale located within indicated area will be received from the database of commercial companies with HLATUs assigned to each selling venue (obviously, identical for all found companies). HLATUs required are extracted from the obtained list in any commonly known way.

[0088] HLATUs obtained for each compromised area identifier are saved in the database of potentially compromised POS terminal networks using any of above mentioned approaches.

[0089] For example, the following list of higher level US territorial divisions (states) was obtained and saved in the database as a result of this step: ['AL', 'PA', 'OK', 'VA', 'OH', 'MI', 'NM', 'MA', 'AZ', 'CA', 'LA', 'IL', 'NE', 'NV', 'TN', 'ID', 'NH', 'TX', 'CT', 'MS', 'ME', 'CO', 'NY', 'WV', 'FL', 'NJ', 'MD', 'KS', 'VT', 'KY', 'MO', 'NC', 'UT', 'IN', 'RI', 'GA', 'WY', 'AR', 'SC']. This list of HLATU includes all states that have at least one ZIP code from the original set of compromised area identifiers.

[0090] Then, a numerical value corresponding to total number of selling venues (offices, shops, restaurants, bank branches, etc.) owned by each potentially compromised company and located in one of above HLATUs where at least one compromised area identifier was found, is calculated and saved in the database for said company. To do this, a query to a search engine, for

example, Google, is generated by a respective script. In particular, for the State of California (CA) and the McDonald's company, the query can be following:

usa california mcdonald's

[0091] In response to such query, the search engine will return a list of selling venues (in this case, restaurants) owned by the specified company and located within territory of the specified state. The length of this list, that is, the number of restaurants included in it, is adopted as the desired numerical value.

[0092] Yet another possible embodiment of the disclosed method comprises sending the query to a preliminary formed database of commercial companies in desired country, HLATU identifier and the company name being used as the keywords in the query. In response, a list of selling venues owned by the specified company and located within indicated HLATU will be received, and the length (number of lines) of this list, which is interpreted as the desired number, is calculated in any commonly known way.

[0093] This numerical value is saved in the database in association with the state and the company in any well-known way, for example, as a text string:

McDonald's, CA, 1221.

[0094] In the same way, numerical values are calculated and saved for all other potentially compromised companies and for all other HLATUs (in this case, US states).

[0095] In such way, a database of potentially compromised POS terminal networks is formed. The database itself can be organized in any commonly known way.

[0096] It should be noted that it will be obvious to those skilled in the art that above listed methods of extracting information from open web sources to form a database of potentially compromised POS terminal networks are not exhaustive and serve only as an example.

[0097] At that, step 120 is completed, and the method proceeds to step 130.

Step 130. Determining parameters of POS terminals network compromise

[0098] At step 130, parameters of compromise are determined for each POS terminal network from the database of potentially compromised POS terminal networks. Details of step 130 are illustrated in Fig. 1B.

[0099] In accordance with the claimed method, to determine the compromise probability of at least one POS terminal network owned by a particular company, the following parameters must be calculated:

- zip_kf: Frequency of POS terminal networks in compromised areas for a given company; it is defined as the ratio of number of compromised areas containing at least one POS terminals network owned by a chosen company (Z_1) to the total quantity of compromised areas (Z);

- cmp_kf : Probability of occurring POS terminals networks (or points of sale) owned by a chosen company in all compromised areas; it is defined as ratio of quantity of POS terminals networks (or selling venues) owned by the chosen company and located within the compromised areas (B_Z) to the total number of POS-terminal networks owned by the chosen company and located within all HLAUs corresponding to the compromised areas (B_S).

[0100] In accordance with above, step 130, as shown in Fig. 1B, begins from the substep 131.

Substep 131. Determining the quantity of compromised areas containing at least one selling venue owned by a chosen company as well as total number of selling venues owned by the same company and located in all compromised areas

[0101] At the first substep 131 of step 130, the number of identifiers of compromised areas where a particular company is represented (Z_1) is determined. To do this, a search query with the keyword denoting a desired company to the database of potentially compromised POS terminal networks is generated for each of companies from the list of companies compiled in step 120. In response to this query, all lines containing name of this company will be received. As described above in relation to step 120, each selling venue owned by this company will be provided with an identifier of the compromised area (in example under consideration, it is ZIP code) where this selling venue is located.

[0102] Thereafter this dataset is used to calculate, in any commonly known way, the number of revealed unique (that is, counted only once) compromised area identifiers and then number of identifiers of compromised areas where a particular company is represented (Z_1).

[0103] Then the length (number of lines) of this list of selling venues owned by the specified company is used to calculate parameter B_Z , that is, number of POS terminals (or selling venues) owned by the chosen company and located in all compromised areas.

[0104] For example, a database query might look like:

McDonald's

[0105] A list of all McDonald's restaurants found in step 120 will be returned in response to this query. Next, a number of different compromised area identifiers (ZIP codes) in list of restaurants obtained is counted. In the example under consideration, such count yielded the number of different identifiers equals to 311. Actions described above can be performed in any commonly known way.

[0106] Next, the total length (number of lines) of obtained list of McDonald's restaurants is determined, and the B_Z value, that is, total number of these restaurant in all compromised areas is calculated; in the considered example, it turned out to be 408.

[0107] Said parameters are calculated in a similar way for all other companies. Results are saved in the database in the form of, for example, the following dataset (in entry format 'company name', Z_1, B_Z):

Marshalls, 61, 79
 Nothing Bundt Cakes, 61, 61
 Five Guys, 119, 124
 AT&T, 121, 131
 Verizon Wireless, 129, 146
 McDonald's, 311, 408

[0108] In addition, total number of compromised areas (Z) is determined at substep 131. Since this number is numerically equal to the number of different compromised area identifiers obtained at step 110, it is determined by counting unique compromised area identifiers contained in the database of potentially compromised POS terminal networks in any commonly known way. The resulting value is saved, for example, in a separate field Z of said database. In the example under consideration Z=951.

[0109] By this substep (131) is completed, and the method proceeds to substep (132).

Substep 132. Determining a total quantity of selling venues owned by the chosen company and located within all HLATUs corresponding to the compromised areas

[0110] At the step 132, the total quantity of selling venues owned by the chosen company and located within all HLATUs corresponding to the compromised areas is determined. A list of all HLATUs corresponding to compromised areas was obtained in step 120 and saved in the database. Also at step 120, information about quantities of selling venues located within all HLATUs was obtained and saved in the database of potentially compromised POS terminals networks.

[0111] To determine quantity of selling venues owned by a chosen company and located within all HLATUs associated with compromised areas, the query can be sent to the database of potentially compromised POS terminals. The query may comprise HLATU and name of company.

The query may look, for example, as follows:

MacDonald's, CA

The response to such query will contain the quantity of selling venues owned by the indicated company and located within indicated HLATU.

[0112] In the example under consideration, the numerical value 1221 found at step 120 and corresponding to the number of Macdonald's selling venues in California was received in response to such query.

[0113] Similar queries are made for all HLATUs determined in step 120 and the results are consolidated. In similar manner, value B_S representing the total quantity of selling venues owned by the chosen company and located within all compromised HLATUs is obtained, which in considered example was equal to 3129. Obtained results are saved in the database.

[0114] In an alternative embodiment of the method, if information about quantities of selling venues located within each HLATU was not saved at step 120, the quantity of selling venues owned by each chosen company and located within all compromised HLATUs can be determined at this step in real time. This is done in exactly the same way as described above with respect to step 120.

[0115] The following provides result of substep 132 of step 130 in entry format 'company name', Z_1, B_Z, B_S:

Marshalls, 61, 79, 202

Nothing Bundt Cakes, 61, 61, 311

Five Guys, 119, 124, 573

AT&T, 121, 131, 2982

Verizon Wireless, 129, 146, 933

McDonald's, 311, 408, 3129

[0116] At that, substep 132 of step 130 is completed, step 130 is completed as well, and the method, referring to Fig. 1A, proceeds to step 140.

Step 140. Determining compromise probability for the next POS terminals network

[0117] At this step, compromise probability for the next POS terminals network owned by a specified company is determined. This value, sort_kf, is calculated as the product

$$\text{sort_kf} = \text{zip_kf} * \text{cmp_kf},$$

where zip_kf is frequency of POS terminals networks within compromised areas for a specified company and cmp_kf is probability of occurring POS terminals networks (or selling venues) owned by the specified company in all compromised areas.

[0118] As disclosed earlier, parameter zip_kf, is calculated as a ratio of a number of compromised areas containing at least one POS terminals network owned by the specified company (Z_1) to the total quantity of compromised areas (Z):

$$\text{zip_kf} = Z_1 / Z,$$

while parameter cmp_kf is calculated as a ratio of quantity of POS terminals networks (or points of sale) owned by a specified company and located within the compromised areas (B_Z) to the total number of POS-terminal networks owned by the specified company and located within all HLATUs corresponding to the compromised areas (B_S):

$$\text{cmp_kf} = B_Z_1 / B_S.$$

[0119] Another possible embodiment of the disclosed method comprises calculating the desired parameter sort_kf as:

$$\text{sort_kf} = \text{zip_kf} * \text{cmp_kf}^2$$

[0120] Yet another possible embodiment of the disclosed method comprises calculating the desired parameter sort_kf as:

$$\text{sort_kf} = \text{zip_kf}^3 * \text{cmp_kf},$$

where parameters zip_kf and cmp_kf are calculated in the same way as described above.

[0121] The parameters Z_1 , Z , B_S , and B_Z were previously determined at steps 120 and 130 and saved in a database of potentially compromised POS terminal networks. Further at this step, name of the next company in a previously obtained list of companies is selected in any commonly known way, and a query is made to the said database with this name, thereafter obtaining values Z_1 , B_S and B_Z for this company.

[0122] Based on these values, parameter sort_kf for this company is calculated using above presented formulas in any commonly known way, and resulted value is saved in the database of potentially compromised POS terminal networks.

[0123] In particular, in above example under consideration, in response to the query with the company name 'McDonald's', values $Z_1=311$, $B_Z=408$ and $B_S=3129$ are obtained from the database. The value of parameter Z representing the total quantity of compromised area identifiers, are identical for all companies and in this example is $Z=951$.

[0124] In the example provided the compromise probability subject is saved in the database for McDonald's POS network is $\text{sort_kf} = 0.0426417$.

[0125] That is the end of step 140.

[0126] It should be noted that steps 130 and 140 are performed each time for a single specific network of POS terminals. Besides, steps 130 and 140 are iterative and are repeated until they are completed for all companies listed at step 120 and contained in the database of potentially compromised POS terminal networks.

[0127] Yet another possible embodiment of the method disclosed comprises performing steps 130 and 140 in parallel, in multi-threading mode, simultaneously for many companies from the list of companies.

[0128] In any case, upon completion of the last iteration of step 140, the method proceeds to verification carried out at step 150.

Step 150. Is there at least one POS terminals network omitted at determining compromise probability?

[0129] Step 150 is devoted to verification of whether there are remain companies in the list, and the method claimed, depending on a result of verification, either returns to step 130, or proceeds to step 160. The method returns to step 130, if there are remain POS terminal networks in the list of POS terminal networks omitted at calculating the compromise probability. The method proceeds to step 160, if the probability of compromise value has been calculated for the entire list of POS terminal networks.

Step 160. Creating a list of POS terminals networks ranked according to compromise probability

[0130] At step 160, a compromise probability ranked list of POS terminals networks is formed. To do this, POS networks are ranked in any commonly known way in descending order by the compromise probability value sort_kf calculated in step 140. This operation can be executed using a previously prepared script.

[0131] As a result of the script execution, a ranked list of potentially compromised POS terminal networks is obtained, in which the networks are located in descending order of the compromise probability parameter sort_kf. The ranked list is saved in the database.

[0132] For the example above, such ranked list of probabilities can be following:

[0133] McDonald's, 0,042641696,

[0134] Five Guys, 0,027079055,

[0135] Marshalls, 0,025085632,

[0136] Verizon Wireless, 0,021226599,

[0137] Nothing Bundt Cakes, 0,012581104,

[0138] AT&T, 0,005589443.

[0139] At that, step 160 is completed, and the method proceeds to step 170.

Step 170. Considering compromised at least one POS terminal network with the highest compromise probability value

[0140] At step 170, the POS terminal network with the highest compromise probability value in the ranked list is selected in any commonly known way. Exactly this POS terminals network is admitted as compromised one.

[0141] In one alternative embodiment of the method claimed, two or more POS terminal networks from a probability ranked list are admitted as compromised rather than one network. In particular, all POS terminal networks that have probability values exceeding a pre-established relative threshold value may be admitted as compromised ones. The relative threshold may be adopted equal to 0.97 of the highest compromise probability value reached, for instance. If such threshold was established, all POS terminal networks with compromise probability values exceeding 0.97 of the highest compromise probability value reached will be marked as compromised ones.

[0142] Results are saved.

[0143] In addition, at step 170, a message can be generated informing about at least one detected compromised POS terminals network. This message can be sent via e-mail or any other known means of data transmission, or displayed on a screen through the graphical interface of the computing device. In the considered example, the McDonald's company's POS terminals network will be identified as compromised one.

[0144] At this point, step 170 and the method claimed 100 are completed.

[0145] Fig. 2 below illustrates a schematic diagram of the computer device (200) processing the data required for embodiment of the claimed solution.

[0146] In general, the device (200) comprises components such as one or more processors (201), at least one core memory (202), data storage means (203), input/output interfaces (204), input/output means (205), and networking means (206).

[0147] The processor (201) of the computing device executes main computing operations required for functioning the device (200) or functionality of one or more of its components. The processor (201) runs the required machine-readable commands, contained in core memory (202).

[0148] The core memory (202) is typically the random-access memory (RAM) and contains the necessary program logic ensuring the required functional.

[0149] The data storage means (203) could be HDD, SSD, RAID, network storage, flash memory, optical drives (CD, DVD, MD, Blue-Ray disks), etc. The means (203) enable to save different information, for example, above-mentioned files with source code, intermediate datasets, lists, databases, etc. for a long time.

[0150] Interfaces (204) are standard means for connection and operation, for example, USB, RS232, RJ45, LPT, COM, HDMI, PS/2, Lightning, FireWire, etc.

[0151] Specific set of interfaces (204) depends on configuration of computing device (200), which can be a personal computer, mainframe, server, server cluster, thin client, smartphone, laptop, etc.

[0152] The data input/output means (205) can primarily consist of a keyboard. In addition to the keyboard, the input/output means can also include: a joystick, a display (or touch-screen display), a projector, a touch pad, a mouse, a trackball, a light pen, loudspeakers, a microphone, etc.

[0153] Networking means (206) are selected among devices providing receiving and transferring network data, for example, Ethernet-card, WLAN/Wi-Fi module, Bluetooth module, BLE module, NFC module, IrDa, RFID module, GSM modem, etc. Means (206) provide data exchange through wire or wireless data communication channels, for example, WAN, PAN, LAN, Intranet, Internet, WLAN, WMAN or GSM.

[0154] The components of the computing device (200) are interconnected by the common data bus (210).

[0155] Although only preferred embodiments of the technical solution claimed were disclosed in materials of this application, they should not be considered as limiting other particular embodiments, which fall within claimed scope of protection and are obvious to those skilled in the art.

CLAIMS

1. A computer-implementable method of identifying a compromised Point-of-Sale (POS) terminal network, the method comprising:
generating a database, including, for a given geographical area of a plurality of geographical areas: (i) a respective identifier of the given geographical area; and (ii) commercial entities present in the given geographical area;

receiving one or more card dump databases, a given one of which includes: (i) card dumps; and (ii) respective identifiers of geographical areas where the card dumps were obtained;

identifying, using the one or more card dump databases and the database, identifiers of a plurality of compromised geographical areas;

identifying in a given compromised geographical area of the plurality of compromised geographical areas, at least one respective POS terminal network of a plurality of POS terminal networks,
 the at least one respective POS terminal network including a plurality of POS terminals in the given compromised geographical area associated with a respective commercial entity;

using the database, identifying, for a given commercial entity present in the given compromised geographical area, based on the respective identifier thereof, POS terminal networks associated with the given commercial entity, thereby generating a potentially compromised POS terminal networks database including: (i) the plurality of POS terminal networks; and (ii) respective entities associated therewith;

determining, for the at least one respective POS terminal network, a plurality of compromise parameters, the plurality of compromise parameters including at least one of:
 a frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas; and

a probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

determining, based on the plurality of compromise parameters, a respective compromise probability value for each POS terminal network of the plurality of POS terminal networks, the determining comprising determining according to at least one equation selected from a group of equations consisting of:

$$\text{sort_kf} = \text{zip_kf} * \text{cmp_kf}^2,$$

$$\text{sort_kf} = \text{zip_kf}^3 * \text{cmp_kf},$$

where sort_kf is the respective compromise probability value,

zip_kf is the frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas, and

cmp_kf is the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

ranking the plurality of POS terminal networks according to respective compromise probability values determined therefor, thereby generating a ranked list of POS terminal networks;

determining a top-ranked POS terminal network in the ranked list of POS terminal networks as being the compromised POS terminal network; and

storing, in the potentially compromised POS terminal networks database, data indicative of the top-ranked POS terminal network being compromised.

2. The method of claim 1, wherein;
prior to the generating the database, the method comprises generating a first database including for the given geographical area the respective identifier of the given geographical area;

the generating the database is executed using the first database; and

after the identifying the identifiers of the plurality of compromised geographical areas, the method further comprises determining, by submitting a respective query to the first database, a respective territorial unit of a plurality of territorial units, with which the plurality of compromised geographical areas is associated.
3. The method of claim 1, wherein the determining the plurality of compromise parameters comprises querying the database.
4. The method of claim 1, wherein the potentially compromised POS terminal networks database is configured to store at least one selected from a group consisted of:
the identifiers of the plurality of compromised geographical areas;

names of commercial entities, whose POS terminal networks are located in respective ones of the plurality of compromised geographical areas;

addresses of the commercial entities, whose POS terminal networks are located in the respective ones of the plurality of compromised geographical areas, and

territorial units corresponding to each one of the plurality of the compromised geographical areas.
5. The method of claim 1, wherein the determining the plurality of compromise parameters of the at least one respective POS terminal network comprises determining:
a number of compromised geographical areas having at least one POS terminal network associated with the respective commercial entity;

a total number of compromised geographical areas in the plurality of compromised geographical areas;

a number of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas, and

a total number of POS terminal networks associated with the respective commercial entity, located in each one of a plurality of territorial units,

a respective one of the plurality of territorial units including the plurality of compromised geographical areas.

6. The method of claim 5, wherein the frequency of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas is determined as a ratio between the number of compromised geographical areas having at least one POS terminal network associated with the respective commercial entity and the total number of compromised geographical areas in the plurality of compromised geographical areas.
7. The method of claim 5, wherein the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas is determined as a ratio between the number of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas and the total number of the POS terminal networks associated with the respective commercial entity, located in each one of the plurality of territorial units.
8. The method of claim 1, wherein the determining the respective compromise probability value for the at least one respective POS terminal network comprises multiplying between the frequency and the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas.

9. The method of claim 1, wherein the determining the top-ranked POS terminal network comprises determining a sub-set of top-ranked POS terminal networks in the ranked list of POS terminal networks whose respective compromise probability values do not exceed a predetermined compromise probability threshold value.

10. A system for identifying a compromised Point-of-Sale (POS) terminal network, the system comprising at least one processor and a non-transitory computer-readable memory storing instructions, which, when executed by the at least one processor, cause the system to:
 - generate a database, including, for a given geographical area of a plurality of geographical areas: (i) a respective identifier of the given geographical area; and (ii) commercial entities present in the given geographical area;

 - receive one or more card dump databases, a given one of which includes: (i) card dumps; and (ii) respective identifiers of geographical areas where the card dumps were obtained;

 - identify, using the one or more card dump databases and the database, identifiers of a plurality of compromised geographical areas;

 - identify, in a given compromised geographical area of the plurality of compromised geographical areas, at least one respective POS terminal network of a plurality of POS terminal networks,
 - the at least one respective POS terminal network including a plurality of POS terminals in the given compromised geographical area associated with a respective commercial entity;

 - use the database to identify, for a given commercial entity present in the given compromised geographical area, based on the respective identifier thereof, POS terminal networks associated with the given commercial entity, thereby generating a potentially compromised POS terminal networks database including: (i) the plurality of POS terminal networks; and (ii) respective entities associated therewith;

determine, for the at least one respective POS terminal network, a plurality of compromise parameters, the plurality of compromise parameters including at least one of:

a frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas; and

a probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

determine, based on the plurality of compromise parameters, a respective compromise probability value for each POS terminal network of the plurality of POS terminal networks by determining the respective compromise probability value at least one equation selected from a group of equations consisting of:

$$\text{sort_kf} = \text{zip_kf} * \text{cmp_kf}^2,$$

$$\text{sort_kf} = \text{zip_kf}^3 * \text{cmp_kf},$$

where sort_kf is the respective compromise probability value,

zip_kf is the frequency of occurrence of POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas, and

cmp_kf is the probability of occurrence of the POS terminal networks associated with the respective commercial entity in the plurality of compromised geographical areas;

rank the plurality of POS terminal networks according to respective compromise probability values determined therefor, thereby generating a ranked list of POS terminal networks;

determine a top-ranked POS terminal network in the ranked list of POS terminal networks as being the compromised POS terminal network; and

store, in the potentially compromised POS terminal networks database, data indicative of the top-ranked POS terminal network being compromised.