(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 6 月 22 日 (22.06.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/101874 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2016/110469

(22) 国际申请日: 2016 年 12 月 16 日 (16.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510959102.0 2015 年 12 月 18 日 (18.12.2015) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **北京奇安信科技有限公司 (BEIJING QIANXIN TECHNOLOGY CO., LTD.)** [CN/CN]; 中国北京市朝阳区酒仙桥路甲 10 号 3 号楼 15 层 17 层 1701-26, Beijing 100015 (CN)。

(72) 发明人: **江爱军 (JIANG, Aijun)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **张聪 (ZHANG, Cong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京智汇东方知识产权代理事务所（普通合伙） (WISEAST INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区花园路 13 号 5 幢 320 房间, Beijing 100088 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: DETECTION METHOD FOR APT ATTACK, TERMINAL DEVICE, SERVER AND SYSTEM

(54) **发明名称** : APT 攻击的检测方法、终端设备、服务器及系统

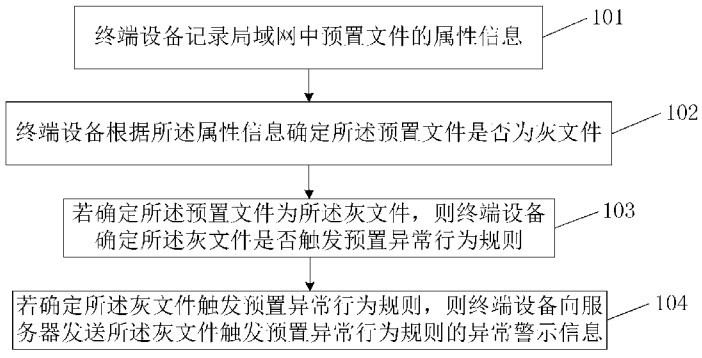


图 1

101 A TERMINAL DEVICE RECORDING ATTRIBUTE INFORMATION ABOUT A PRE-SET FILE IN A LOCAL AREA NETWORK

102 THE TERMINAL DEVICE DETERMINING WHETHER THE PRE-SET FILE IS A GREY FILE ACCORDING TO THE ATTRIBUTE INFORMATION

103 IF IT IS DETERMINED THAT THE PRE-SET FILE IS A GREY FILE, THEN THE TERMINAL DEVICE DETERMINING WHETHER THE GREY FILE HAS TRIGGERED A PRE-SET ABNORMAL BEHAVIOUR RULE

104 IF IT IS DETERMINED THAT THE GREY FILE HAS TRIGGERED A PRE-SET ABNORMAL BEHAVIOUR RULE, THEN THE TERMINAL DEVICE SENDING TO A SERVER ABNORMALITY ALARM INFORMATION ABOUT THE GREY FILE HAVING TRIGGERED THE PRE-SET ABNORMAL BEHAVIOUR RULE

(57) **Abstract**: Disclosed are a detection method for an APT attack, a terminal device, a server and a system, which relate to the technical field of information security and are primarily used for realizing rapid and precise detection of APT attacks. The primary technical solution of the present invention comprises: a terminal device recording attribute information about a pre-set file in a local area network, wherein the attribute information about the pre-set file comprises identification information, time information, source information, and transfer target information; determining whether the pre-set file is a grey file according to the attribute information, wherein the grey file neither exists in a white list of the pre-set file nor a black list in the pre-set file; if it is determined that the pre-set file is a grey file, then determining whether the grey file has triggered a pre-set abnormal behaviour rule; and if it is determined that the grey file has triggered the pre-set abnormal behaviour rule, sending to a server abnormality alarm information about the grey file having triggered the pre-set abnormal behaviour rule, wherein the abnormality alarm information contains identification information about the terminal device. The present invention is primarily applied in the process of detecting an APT attack.

(57) **摘要**:

[见续页]

WO 2017/101874 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种 APT 攻击的检测方法、终端设备、服务器及系统，涉及信息安全技术领域，主要目的在于实现快速、精确的对 APT 攻击进行检测。本发明的主要技术方案包括：终端设备记录局域网中预置文件的属性信息；其中，预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；根据属性信息确定预置文件是否为灰文件；灰文件既不存在于预置文件的白名单内，也不存在预置文件的黑名单内；若确定预置文件为灰文件，则确定灰文件是否触发预置异常行为规则；若确定灰文件触发预置异常行为规则，则向服务器发送灰文件触发预置异常行为规则的异常警示信息；其中，异常警示信息包含终端设备的标识信息。本发明主要应用于 APT 攻击的检测过程中。

APT 攻击的检测方法、终端设备、服务器及系统

技术领域

本发明涉及信息安全技术领域，特别是涉及一种 APT 攻击的检测方法、终端设备、服务器及系统。

背景技术

随着计算机技术的不断发展，人类社会的信息化程度越来越高，整个社会对计算机信息的依赖程度也越来越高。与此同时，计算机文件中的安全存在的威胁也在不断的增长,而高级持续性威胁 (Advanced Persistent Threat，APT) 成为信息安全领域最严重的威胁之一，是一种持续性网络攻击。

APT 攻击的原理相对于其他攻击形式更为高级和先进,其高级性主要体现在 APT 在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集。在此收集的过程中，此攻击会主动挖掘被攻击对象信任的系统和应用程序的漏洞，利用这些漏洞组建攻击者所需的网络，并利用 0day 漏洞进行攻击。APT 攻击的手段，在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据，这种发生在数字空间的偷窃资料、搜集情报的行为，就是一种"网络间谍"的行为。

为了能够将隐藏的 APT 攻击检测出来，以便及时的进行修复，人们想出各种各样的方案。目前常用的技术方案为：依靠人的经验进行判断，该种判断方法不能快速、精确地检测出 APT 攻击，可能会错过潜伏的 APT 攻击，因此，可能会严重威胁计算机数据信息的安全。

发明内容

有鉴于此，本发明提供的一种 APT 攻击的检测方法、终端设备、服务器及系统，主要目的在于解决人工检测 APT 攻击时，不能快速、精确地检测出 APT 攻击，可能会错过潜伏的 APT 攻击，因此，可能会严重威胁计算机数据信息的安全的问题。

依据本发明的一个方面，本发明提供了一种 APT 攻击的检测方法，包括：

终端设备记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

根据所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；

若确定所述预置文件为所述灰文件，则确定所述灰文件是否触发预置异常行为规则；

若确定所述灰文件触发所述预置异常行为规则，则向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息。

依据本发明的另一个方面，本发明提供了一种 APT 攻击的检测方法，包括：

服务器接收局域网中各终端设备上报的灰文件的属性信息；其中，所述灰文件的属性信息包括标识信息、来源信息及流转目标信息、时间信息；

当接收到所述局域网中终端设备发送的异常警示信息时，根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件；所述异常警示信息根据所述灰文件触发预置异常行为规则产生；

根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息；

根据所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径；其中，所述流转路径是将所述灰文件的来源信息及流转目标信息按照时间先后顺序串联形成的。

依据本发明的再一个方面，本发明提供了一种终端设备，包括：

第一记录单元，用于记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

第一确定单元，用于根据所述第一记录单元记录的所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；

第二确定单元，用于当所述第一确定单元确定所述预置文件为所述灰文件时，确定所述灰文件是否触发预置异常行为规则；

第一发送单元，用于当所述第二确定单元确定所述灰文件触发所述预置异常行为规则时，向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息。

依据本发明的又一个方面，本发明提供了一种服务器，包括：

第一接收单元，用于接收局域网中各终端设备上报的灰文件的属性信息；其中，所述灰文件的属性信息包括标识信息、来源信息及流转目标信息、时间信息；

第一获取单元，用于当接收到所述局域网中终端设备发送的异常警示信息时，根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件；所述异常警示信息根据所述灰文件触发预置异常行为规则产生；

第二获取单元，用于根据所述第一接收单元接收的所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息；

第三获取单元，用于根据所述第二获取单元获取的所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径；其中，所述流转路径是将所述灰文件的来源信息及流转目标信息按照时间先后顺序串联形成的。

依据本发明的又一个方面，本发明提供了一种 APT 攻击的检测系统，所述系统包括：如上所述的终端设备及如上所述的服务器。

依据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当上述计算机可读代码在计算设备上运行时，导致计算设备执行上述的 APT 攻击的检测方法。

依据本发明的又一个方面，提供了一种计算机可读介质，其中存储了上述的计

算机程序。

借由上述技术方案，本发明提供的APT攻击的检测方法、终端设备、服务器及系统，在检测 APT 攻击时，终端设备记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；根据所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；若确定所述预置文件为所述灰文件，则确定所述灰文件是否触发预置异常行为规则；若确定所述灰文件触发预置异常行为规则，则向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息；与现有技术中，通过人工检测 APT 攻击的方式相比，本发明中当灰文件的异常行为触发预置异常行为规则时，终端向服务器发送异常警示信息，服务器会根据局域网内各个终端上报的灰文件的标识信息，获取灰文件的流转路径，根据流转路径获取灰文件进行该局域网的时间信息、来源信息等，能够快速、精确的对APT攻击进行检测。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了本发明实施例提供的一种APT攻击的检测方法的流程图；

图 2 示出了本发明实施例提供的另一种APT攻击的检测方法的流程图；

图 3 示出了本发明实施例提供的一种终端设备的组成框图；

图 4 示出了本发明实施例提供的另一种终端设备的组成框图；

图 5 示出了本发明实施例提供的一种服务器的组成框图；

图 6 示出了本发明实施例提供的另一种服务器的组成框图；

图 7 示出了本发明实施例提供一种APT攻击的检测系统的组成框图；

图 8 示意性地示出了用于执行根据本发明的APT攻击的检测方法的计算设备的框图；以及

图 9 示意性地示出了用于保持或者携带实现根据本发明的APT攻击的检测方法的程序代码的存储单元。

具体实施方式

下面结合附图和具体的实施方式对本发明作进一步的描述。

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能

够将本公开的范围完整的传达给本领域的技术人员。

本发明实施例提供一种 APT 攻击的检测方法，该方法应用于终端设备侧，如图 1 所示，该方法包括：

101、终端设备记录局域网中预置文件的属性信息。

在局域网环境中，包含多个终端设备，每个终端设备均会记录预置文件的属性信息，其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；需要说明的是，所述预置文件是指从网络下载或者从 U 盘、硬盘、智能手机有线或无线传输所获取的文件；网络下载包含但不局限于以下内容，例如：网站下载、邮件下载、网络共享等等。本发明实施例对预置文件的来源及预置文件的具体类型不进行限定。

为了确保终端设备记录预置文件属性信息的准确性，在终端设备第一次接收到预置文件时，对预置文件的属性信息进行记录，在终端设备记录预置文件的属性信息时，仅记录一次；在记录预置文件的属性信息之前，不能确定该预置文件的安全等级，因此，需要将终端设备中所有的预置文件的属性信息都进行记录；其中，所述预置文件的安全等级包括：白名单文件、黑名单文件、灰文件，所述灰文件为既不属于白名单，也不属于黑名单的文件；本发明实施例对终端设备记录局域网中预置文件的属性信息的具体时机以及预置文件的安全等级不进行限定。

为了更清晰的对记录预置文件的属性信息，以下将以示例的形式进行详细说明。示例性的，当终端设备 A 中含有预置文件 I，该预置文件 I 是于 2015 年 3 月 4 日，通过用户使用 U 盘传递给终端设备 A 的，终端设备 A 于 2015 年 5 月 28 日，将预置文件 I 又通过邮件的方法发送给终端设备 B 及终端设备 C。针对同一个预置文件 I，终端设备 A 记录预置文件的属性信息包括：预置文件标识信息为 WJ-001，时间信息为 2015 年 3 月 4 日，来源信息为 U 盘，流转目标信息为终端设备 B 及终端设备 C；终端设备 B 记录预置文件的属性信息包括：预置文件标识信息为 WJ-001，时间信息为 2015 年 5 月 28 日，来源信息为终端设备 A，流转目标信息为无；终端设备 C 记录预置文件的属性信息包括：预置文件标识信息为 WJ-001，时间信息为 2015 年 5 月 28 日，来源信息为终端设备 A，流转目标信息为无。以上仅为示例性的举例，本发明实施例对终端设备记录预置文件的属性信息的具体内容不进行限定。

102、终端设备根据所述属性信息确定所述预置文件是否为灰文件。

本步骤中基于步骤 101 中记录预置文件的属性信息，确定预置文件的安全等级，若预置文件为白名单文件，则说明预置文件是安全的，该预置文件内不可能存在 APT 攻击；若预置文件为黑名单文件，则说明该预置文件是危险文件，将该预置文件进行过滤或者删除；若预置文件为灰文件，则说明该预置文件的危险系数为未知。因此，需要对灰文件进行跟踪。

103、若确定所述预置文件为所述灰文件，则终端设备确定所述灰文件是否触发预置异常行为规则。

在确定预置文件为灰文件之后，若该灰文件在局域网内的终端设备之间流转过程中，没有任何的异常行为，则说明该灰文件中不存在 APT 攻击；若该文件在局域

网内的终端设备之间流转过程中，出现异常行为，则说明该灰文件中可能存在 APT 攻击。由于 APT 攻击具备高度的隐蔽性，且其发起 APT 攻击的时间具有不确定性，因此，在本发明实施例中，终端设备通过对灰文件进行监控，确定灰文件是否触发预置异常行为规则。

所述预置异常行为规则为是经验值，在设置异常行为规则时，所述异常行为规则可以包含但不局限于以下的内容，例如：灰文件的访问权限、灰文件的执行时间等等。

在具体实施时，不同的终端设备用户均会设置有不同的访问权限，如财务部门会有其相应的访问权限，研发部门会有其相应的访问权限；若研发部分的终端设备中的灰文件去访问财务部门，则该灰文件触发了预置异常行为规则。或者，终端设备会有固定的工作时间，假设，终端设备的工作时间为 09:00-17:30，若终端设备中的灰文件在 22:00 自动执行，则该灰文件触发了预置异常行为规则。本发明实施例对预置异常行为规则的具体设置内容不进行具体限定。

104、若确定所述灰文件触发预置异常行为规则，则终端设备向服务器发送所述灰文件触发预置异常行为规则的异常警示信息。

当确定灰文件触发预置异常行为规则时，终端设备确定该灰文件中可能存在 APT 攻击，因此，终端设备针对该异常行为向服务器发送异常警示信息；其中，所述异常警示信息包含终端设备的标识信息。

本发明实施例提供的 APT 攻击的检测方法，在检测 APT 攻击时，终端设备记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；根据所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；若确定所述预置文件为所述灰文件，则确定所述灰文件是否触发预置异常行为规则；若确定所述灰文件触发预置异常行为规则，则向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息；与现有技术中，通过人工检测 APT 攻击的方式相比，本发明实施例中当灰文件的异常行为触发预置异常行为规则时，终端向服务器发送异常警示信息，服务器会根据局域网内各个终端上报的灰文件的标识信息，获取灰文件的流转路径，根据流转路径获取灰文件进行该局域网的时间信息、来源信息等，能够快速、精确的对 APT 攻击进行检测。

进一步的，作为对图 1 所示方法的细化和扩展，在步骤 101 终端设备记录局域网中预置文件的属性信息，可以采用但不局限于以下的方式实现：

方式一：基于预置驱动程序记录局域网中预置文件的属性信息。

当终端设备作为流转目标信息，且接收预置文件时，预置驱动程序会自动识别该预置文件，并记录该预置文件的属性信息；在具体操作时，该预置驱动程序可以包含但不限于是 U 盘监控驱动，本发明实施例对预置驱动程序的具体类型不进行限定。

方式二：基于预置网关设备记录局域网中预置文件的属性信息。

当终端设备利用互联网进行预置文件下载时，预置网关设备会自动识别该预置文件，并记录该预祝文件的属性信息。

需要说明的是，在通过方式一记录局域网中预置文件的属性信息时，若该预置文件为灰文件，且灰文件触发预置异常行为规则，则由终端设备向服务器上报灰文件触发预置异常行为规则的异常警示信息；在通过方式二记录局域网中预置文件的属性信息时，若该预置文件为灰文件，且灰文件触发预置异常行为规则，则由预置网关设备向服务器上报灰文件触发预置异常行为规则的异常警示信息。

进一步的，为了让服务器能够在终端设备上报异常警示信息时，及时对终端设备内的灰文件进行追溯，因此，在终端设备向服务器发送所述灰文件触发预置异常行为规则的异常警示信息之前，终端设备根据灰文件的标识信息，记录灰文件的时间信息、来源信息及流转目标信息，终端设备将记录的灰文件的时间信息、来源信息及流转目标信息发送至服务器。需要说明的是，同一终端设备中可能存在多个灰文件，终端设备需要根据各个灰文件的不同标识信息，分别记录灰文件的时间信息、来源信息及流转目标信息。局域网内的各个终端设备均向服务器上报灰文件的时间信息、来源信息及流转目标信息，确保服务器在后续追溯灰文件的流转路径时，其流转路径的完整性和准确性。

进一步的，在终端设备根据属性信息确定预置文件是否为灰文件时，其具体过程如下：终端设备记录预置文件的属性信息之后，将该属性信息发送至云查杀服务器，云查杀服务器中记录有预置文件的黑名单和白名单，云查杀服务器在接收到预置文件的属性信息之后，获取属性信息中的标识信息，基于标识信息遍历黑名单以及白名单，若该标识信息存在于黑名单中，则直接将该标识信息对应的预置文件进行过滤；若该标识信息存在于白名单中，确定该标识信息对应的预置文件为安全文件；若该标识信息既不存在于白名单中，也不存在于黑名单中，则确定该标识信息对应的预置文件为灰文件，此时，云查杀服务器会向终端设备返回灰文件的标识信息，以便终端设备对该灰文件的属性信息进行记录，并上报至服务器。

进一步的，在终端设备确定所述灰文件是否触发预置异常行为规则之前，生成预置异常行为规则，所述预置异常行文规则用于确定所述灰文件是否存在异常行为。

进一步的，在生成预置异常行为规则之后，终端设备确定所述灰文件是否触发预置异常行为规则具体包括：获取预置异常行为规则，确定灰文件是否存在异常行为，判断异常行为是否触发预置异常行为规则。示例性的，假设，预置异常行为规则中包含：以一天为标准，灰文件的异常执行时间超过一次时，确定该灰文件触发预置异常行为规则，异常执行时间为 22:00-次日 05：00；若灰文件在 23:00 时执行一次，则终端设备确定灰文件的执行为异常行为，并查看在一天时间内，该灰文件异常执行的次数是否超过一次；若灰文件的异常执行为一次，则不会向服务器上报异常警示信息；若灰文件的异常执行为两次，则向服务器上报异常警示信息。

本发明实施例还提供另一种攻击的检测方法，该方法应用于服务器侧，如图 2 所示，该方法包括：

201、服务器接收局域网中各终端设备上报的灰文件的属性信息。

其中，所述灰文件的属性信息包括标识信息、来源信息及流转目标信息、时间信息；有关灰文件的详细说明，请参考步骤 101 中的详细描述，本发明实施例在此不再进行赘述。

202、服务器当接收到所述局域网中终端设备发送的异常警示信息时，根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件。

当终端设备上报异常警示信息时，说明该终端设备中的灰文件中可能存在 APT 攻击，所述异常警示信息根据所述灰文件触发预置异常行为规则产生；由于终端设备中可能包含多个灰文件，在不能确定该异常警示信息是哪个灰文件触发的前提下，服务器接收到终端设备发送的异常警示信息时，根据异常警示信息中包含的终端设备的标识信息，获取终端设备在预置时间段内的所有灰文件，并获取所有灰文件对应的标识信息。

所述预置时间段为局域网运维人员人工设置的，在设置预置时间段时，可以设置预置时间段为一周；或者，也可以设置预置时间段为一个月，具体的本发明实施例对预置时间段的设置不进行限定。

203、服务器根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息。

由于灰文件在局域网内的流转是随机性的，且终端设备在向服务器上报灰文件的时间信息、来源信息及流转目标信息是各个终端设备单独发送的，服务器在接收到终端设备发送的时间信息、来源信息及流转目标信息时，仅将接收到的信息进行保存，而不会根据灰文件的标识信息将灰文件在局域网内的流转路径进行串联。只有当终端设备发送异常警示信息时，服务器才会将灰文件在局域网内的时间信息、来源信息及流转目标信息时进行串联。

204、服务器根据所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径。

在步骤 203 获取所述局域网中各终端设备上报的所述灰文件的属性信息之后，服务器按照时间的先后顺序根据灰文件的标识信息将灰文件的来源信息及流转目标信息进行串联；服务器获取灰文件的流转路径，并将流转路径进行输出，以便局域网的运维人员查找 APT 攻击的源头。

作为本发明实施例的一种实现方式，在输出显示流转路径时，以图表的形式进行显示，图表中包含灰文件在局域网内流转的时间信息；或者，以时间轴的方式将灰文件的流转路径进行显示。本发明实施例对输出显示流转路径的方式不进行限定。

本发明实施例提供的 APT 攻击的检测方法，在检测 APT 攻击时，终端设备记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；根据所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；若确定所述预置文件为所述灰文件，则确定所述灰文件是否触发预置异常行为规则；若确定所述灰文件触发预置异常行为规则，则向服务器发送所

述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息；与现有技术中，通过人工检测 APT 攻击的方式相比，本发明实施例中当灰文件的异常行为触发预置异常行为规则时，终端向服务器发送异常警示信息，服务器会根据局域网内各个终端上报的灰文件的标识信息，获取灰文件的流转路径，根据流转路径获取灰文件进行该局域网的时间信息、来源信息等，能够快速、精确的对 APT 攻击进行检测。

进一步的，作为对图 2 所示方法的细化和扩展，在步骤 203 根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息之后，根据灰文件的标识信息对灰文件的属性信息进行解析，确定灰文件的时间信息、来源信息及流转目标信息，根据时间信息的先后顺序将灰文件的来源信息及流转目标信息进行串联。

示例性的，假设，若灰文件的标识信息为 HWJ-008，根据该标识信息 HWJ-008，服务器查找各个终端设备上报的属性信息，其中，上报属性信息中包含 HWJ-008 的终端设备有终端设备 1、终端设备 8、终端设备 45、终端设备 12，其中，终端设备 1 中记录时间信息为 2015 年 3 月 9 日、来源信息为终端设备 8、流转目标信息 12；终端设备 8 中记录时间信息为 2015 年 2 月 20 日、来源信息为 XXX 网站、流转目标信息 1；终端设备 12 中记录时间信息为 2015 年 3 月 15 日、来源信息为终端设备 1、流转目标信息为终端设备 45；终端设备 45 中记录时间信息为 2015 年 4 月 6 日、来源信息为终端设备 12、流转目标信息为无。服务器根据时间信息，形成标识信息为 HWJ-008 的灰文件的流转路径为：终端设备 8（2015 年 2 月 20 日）→终端设备 1（2015 年 3 月 9 日）→终端设备 12（2015 年 3 月 15 日）→终端设备 45（2015 年 4 月 6 日）。以上仅为示例性的举例，本发明实施例对标识信息、灰文件在局域网内终端设备流转的来源信息及流转目标信息等内容不进行限定。

进一步的，在服务器接收局域网中各终端设备上报的灰文件的属性信息之前，接收终端设备发送的预置文件，同时，接收云查杀服务器发送的数据库表格，该数据库表格为云查杀数据库根据预置文件的白名单及黑名单生成，服务器根据数据库表格确定接收到的预置文件是否为灰文件，当确定预置文件为灰文件之后，接收终端设备上报的灰文件的属性信息。其中，服务器确定预置文件为灰文件的目的在于，仅接收灰文件的属性信息，而不接收云查杀服务器确定的白名单或者黑名单中的预置文件对应的属性信息，能够节省部分服务器的处理资源；同时，白名单中的预置文件不会存在 APT 攻击，因此，无需对该类预置文件进行跟踪。

作为本发明实施例的一种实现方式，云查杀服务器实时对终端设备记录的预置文件进行查杀，确定该预置文件的安全性，即确定该预置文件是否是白名单文件、黑名单文件或者灰文件；确定出预置文件的类型之后，存储于数据库表格中，并按照预置周期将数据库表格发送至服务器；或者，在确定预置文件的类型之后，实时将数据库表格发送至服务器，本发明实施例对云查杀向服务器发送数据库表格的时机不进行限定。

进一步的，作为对上述图 1 所示方法的实现，本发明另一实施例还提供了一种

终端设备。该装置实施例与前述方法实施例对应，为便于阅读，本装置实施例不再对前述方法实施例中的细节内容进行逐一赘述，但应当明确，本实施例中的装置能够对应实现前述方法实施例中的全部内容。

本发明实施例提供的一种终端设备，如图 3 所示，包括：

第一记录单元 31，用于记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

第一确定单元 32，用于根据所述第一记录单元 31 记录的所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；

第二确定单元 33，用于当所述第一确定单元 32 确定所述预置文件为所述灰文件时，确定所述灰文件是否触发预置异常行为规则；

第一发送单元 34，用于当所述第二确定单元 33 确定所述灰文件触发所述预置异常行为规则时，向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息。

进一步的，如图 4 所示，所述第一记录单元 31 包括：

第一记录模块 311，用于基于预置驱动程序记录局域网中预置文件的属性信息；

第二记录模块 312，用于基于预置网关设备记录局域网中预置文件的属性信息。

进一步的，如图 4 所示，所述终端设备还包括：

第二记录单元 35，用于在所述第一发送单元 34 向服务器发送所述灰文件触发预置异常行为规则的异常警示信息之前，根据所述灰文件的标识信息，记录所述灰文件的时间信息、来源信息及流转目标信息；

第二发送单元 36，用于将所述第二记录单元 35 记录的所述时间信息、来源信息及所述流转目标信息发送至所述服务器。

进一步的，如图 4 所示，所述第一确定单元 32 包括：

发送模块 321，用于将所述属性信息发送至云查杀服务器，以便所述云查杀服务器根据所述属性信息判断所述预置文件是否为所述灰文件，当所述云查杀服务器返回所述灰文件的标识信息时，确定所述预置文件为灰文件；

确定模块 322，用于在所述发送模块 321 将所述属性信息发送至所述云查杀服务器之后，根据所述云查杀服务器是否发送所述标识信息，确定所述预置文件是否为灰文件。

进一步的，如图 4 所示，所述终端设备还包括：

生成单元 37，用于在所述第二确定单元 33 确定所述灰文件是否触发预置异常行为规则之前，生成预置异常行为规则。

进一步的，如图 4 所示，所述第二确定单元 33 包括：

获取模块 331，用于获取所述预置异常行为规则；

确定模块 332，用于确定所述灰文件是否存在异常行为；

判断模块 333，用于判断所述确定模块 332 确定的所述异常行为是否触发所述获取模块 331 获取的所述预置异常行为规则。

进一步的，作为对上述图 2 所示方法的实现，本发明另一实施例还提供了一种服务器。该装置实施例与前述方法实施例对应，为便于阅读，本装置实施例不再对前述方法实施例中的细节内容进行逐一赘述，但应当明确，本实施例中的装置能够对应实现前述方法实施例中的全部内容。

本发明实施例提供一种服务器，如图 5 所示，包括：

第一接收单元 51，用于接收局域网中各终端设备上报的灰文件的属性信息；其中，所述灰文件的属性信息包括标识信息、来源信息及流转目标信息、时间信息；

第一获取单元 52，用于当接收到所述局域网中终端设备发送的异常警示信息时，根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件；所述异常警示信息根据所述灰文件触发预置异常行为规则产生；

第二获取单元 53，用于根据所述第一接收单元 51 接收的所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息；

第三获取单元 54，用于根据所述第二获取单元 53 获取的所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径；其中，所述流转路径是将所述灰文件的来源信息及流转目标信息按照时间先后顺序串联形成的。

进一步的，如图 6 所示，所述服务器还包括：

解析单元 55，用于在所述第二获取单元 53 根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息之后，根据所述灰文件的标识信息对所述灰文件的属性信息进行解析；

第一确定单元 56，用于在所述解析单元 55 根据所述灰文件的标识信息对所述灰文件的属性信息进行解析之后，确定所述灰文件的时间信息、来源信息及流转目标信息；

串联单元 57，用于根据所述第一确定单元 56 确定的所述时间信息的先后顺序将所述灰文件的所述来源信息及所述流转目标信息进行串联；

形成单元 58，用于形成所述灰文件的所述流转路径。

进一步的，如图 6 所示，所述服务器还包括：

第二接收单元 59，用于在所述第一接收单元 51 接收局域网中各终端设备上报的灰文件的属性信息之前，接收所述终端设备发送的预置文件；

第三接收单元 510，用于接收云查杀服务器发送的数据库表格，所述数据库表格为所述云查杀服务器根据所述预置文件的白名单及黑名单生成；

第二确定单元 511，用于根据所述第三接收单元 510 接收的所述数据库表格确定所述预置文件是否为所述灰文件；

所述第一接收单元 51，还用于当所述第二确定单元 511 根据所述数据库表格确定所述预置文件为所述灰文件时，接收局域网中各终端设备上报的灰文件的属性信息。

进一步的，本发明实施例还提供一种 APT 攻击的检测系统，如图 7 所示，所述系统包括：如图 3 或图 4 任一幅图所示的终端设备 71 及如图 5 或图 6 任一幅图所示

的服务器 72。

本发明实施例提供的终端设备、服务器及 APT 攻击的检测系统，在检测 APT 攻击时，终端设备记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；根据所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；若确定所述预置文件为所述灰文件，则确定所述灰文件是否触发预置异常行为规则；若确定所述灰文件触发预置异常行为规则，则向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息；与现有技术中，通过人工检测 APT 攻击的方式相比，本发明实施例中当灰文件的异常行为触发预置异常行为规则时，终端向服务器发送异常警示信息，服务器会根据局域网内各个终端上报的灰文件的标识信息，获取灰文件的流转路径，根据流转路径获取灰文件进行该局域网的时间信息、来源信息等，能够快速、精确的对 APT 攻击进行检测。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运

行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的地图搜索结果的显示装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 8 示出了可以实现根据本发明的 APT 攻击的检测方法的计算设备。该计算设备传统上包括处理器 810 和以存储器 820 形式的计算机程序产品或者计算机可读介质。存储器 820 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 820 具有用于执行上述方法中的任何方法步骤的程序代码 831 的存储空间 830。例如，用于程序代码的存储空间 830 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 831。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 9 所述的便携式或者固定存储单元。该存储单元可以具有与图 8 的计算设备中的存储器 820 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 831’，即可以由例如诸如 810 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种 APT 攻击的检测方法，其特征在于，包括：

终端设备记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

根据所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；

若确定所述预置文件为所述灰文件，则确定所述灰文件是否触发预置异常行为规则；

若确定所述灰文件触发所述预置异常行为规则，则向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息。

2、根据权利要求 1 所述的方法，其特征在于，终端设备记录局域网中预置文件的属性信息包括：

基于预置驱动程序记录局域网中预置文件的属性信息；

或者，基于预置网关设备记录局域网中预置文件的属性信息。

3、根据权利要求 2 所述的方法，其特征在于，在向服务器发送所述灰文件触发预置异常行为规则的异常警示信息之前，所述方法还包括：

根据所述灰文件的标识信息，记录所述灰文件的时间信息、来源信息及流转目标信息；

将所述时间信息、来源信息及所述流转目标信息发送至所述服务器。

4、根据权利要求 3 所述的方法，其特征在于，根据所述属性信息确定所述预置文件是否为灰文件包括：

将所述属性信息发送至云查杀服务器，以便所述云查杀服务器根据所述属性信息判断所述预置文件是否为所述灰文件，当所述云查杀服务器返回所述灰文件的标识信息时，确定所述预置文件为灰文件；

根据所述云查杀服务器是否发送所述标识信息，确定所述预置文件是否为灰文件。

5、根据权利要求 1-4 中任一项所述的方法，其特征在于，在确定所述灰文件是否触发预置异常行为规则之前，所述方法还包括：

生成预置异常行为规则。

6、根据权利要求 5 所述的方法，其特征在于，确定所述灰文件是否触发预置异常行为规则包括：

获取所述预置异常行为规则；

确定所述灰文件是否存在异常行为；

判断所述异常行为是否触发所述预置异常行为规则。

7、一种 APT 攻击的检测方法，其特征在于，包括：

服务器接收局域网中各终端设备上报的灰文件的属性信息；其中，所述灰文件

的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

当接收到所述局域网中终端设备发送的异常警示信息时，根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件；所述异常警示信息根据所述灰文件触发预置异常行为规则产生；

根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息；

根据所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径；其中，所述流转路径是将所述灰文件的来源信息及流转目标信息按照时间先后顺序串联形成的。

8、根据权利要求 7 所述的方法，其特征在于，在根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息之后，所述方法还包括：

根据所述灰文件的标识信息对所述灰文件的属性信息进行解析；

确定所述灰文件的时间信息、来源信息及流转目标信息；

根据所述时间信息的先后顺序将所述灰文件的所述来源信息及所述流转目标信息进行串联；

形成所述灰文件的所述流转路径。

9、根据权利要求 7 或 8 所述的方法，其特征在于，在服务器接收局域网中各终端设备上报的灰文件的属性信息之前，所述方法还包括：

接收所述终端设备发送的预置文件；

接收云查杀服务器发送的数据库表格，所述数据库表格为所述云查杀服务器根据所述预置文件的白名单及黑名单生成；

根据所述数据库表格确定所述预置文件是否为所述灰文件；

所述服务器接收局域网中各终端设备上报的灰文件的属性信息包括：

若根据所述数据库表格确定所述预置文件为所述灰文件，则接收局域网中各终端设备上报的灰文件的属性信息。

10、一种终端设备，其特征在于，包括：

第一记录单元，用于记录局域网中预置文件的属性信息；其中，所述预置文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

第一确定单元，用于根据所述第一记录单元记录的所述属性信息确定所述预置文件是否为灰文件；其中，所述灰文件既不存在于所述预置文件的白名单内，也不存在所述预置文件的黑名单内；

第二确定单元，用于当所述第一确定单元确定所述预置文件为所述灰文件时，确定所述灰文件是否触发预置异常行为规则；

第一发送单元，用于当所述第二确定单元确定所述灰文件触发所述预置异常行为规则时，向服务器发送所述灰文件触发预置异常行为规则的异常警示信息；其中，所述异常警示信息包含终端设备的标识信息。

11、根据权利要求 10 所述的终端设备，其特征在于，所述第一记录单元包括：

第一记录模块，用于基于预置驱动程序记录局域网中预置文件的属性信息；

第二记录模块，用于基于预置网关设备记录局域网中预置文件的属性信息。

12、根据权利要求 11 所述的终端设备，其特征在于，所述终端设备还包括：

第二记录单元，用于在所述第一发送单元向服务器发送所述灰文件触发预置异常行为规则的异常警示信息之前，根据所述灰文件的标识信息，记录所述灰文件的时间信息、来源信息及流转目标信息；

第二发送单元，用于将所述第二记录单元记录的所述时间信息、来源信息及所述流转目标信息发送至所述服务器。

13、根据权利要求 12 所述的终端设备，其特征在于，所述第一确定单元包括：

发送模块，用于将所述属性信息发送至云查杀服务器，以便所述云查杀服务器根据所述属性信息判断所述预置文件是否为所述灰文件，当所述云查杀服务器返回所述灰文件的标识信息时，确定所述预置文件为灰文件；

确定模块，用于在所述发送模块将所述属性信息发送至所述云查杀服务器之后，根据所述云查杀服务器是否发送所述标识信息，确定所述预置文件是否为灰文件。

14、根据权利要求 10-13 中任一项所述的终端设备，其特征在于，所述终端设备还包括：

生成单元，用于在所述第二确定单元确定所述灰文件是否触发预置异常行为规则之前，生成预置异常行为规则。

15、根据权利要求 14 所述的终端设备，其特征在于，所述第二确定单元包括：

获取模块，用于获取所述预置异常行为规则；

确定模块，用于确定所述灰文件是否存在异常行为；

判断模块，用于判断所述确定模块确定的所述异常行为是否触发所述获取模块获取的所述预置异常行为规则。

16、一种服务器，其特征在于，包括：

第一接收单元，用于接收局域网中各终端设备上报的灰文件的属性信息；其中，所述灰文件的属性信息包括标识信息、时间信息、来源信息及流转目标信息；

第一获取单元，用于当接收到所述局域网中终端设备发送的异常警示信息时，根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件；所述异常警示信息根据所述灰文件触发预置异常行为规则产生；

第二获取单元，用于根据所述第一接收单元接收的所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息；

第三获取单元，用于根据所述第二获取单元获取的所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径；其中，所述流转路径是将所述灰文件的来源信息及流转目标信息按照时间先后顺序串联形成的。

17、根据权利要求 16 所述的服务器，其特征在于，所述服务器还包括：

解析单元，用于在所述第二获取单元根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息之后，根据所述灰文件的标识信息对所述灰文件的属性信息进行解析；

第一确定单元，用于在所述解析单元根据所述灰文件的标识信息对所述灰文件的属性信息进行解析之后，确定所述灰文件的时间信息、来源信息及流转目标信息；

串联单元，用于根据所述第一确定单元确定的所述时间信息的先后顺序将所述灰文件的所述来源信息及所述流转目标信息进行串联；

形成单元，用于形成所述灰文件的所述流转路径。

18、根据权利要求 16 或 17 所述的服务器，其特征在于，所述服务器还包括：

第二接收单元，用于在所述第一接收单元接收局域网中各终端设备上报的灰文件的属性信息之前，接收所述终端设备发送的预置文件；

第三接收单元，用于接收云查杀服务器发送的数据库表格，所述数据库表格为所述云查杀服务器根据所述预置文件的白名单及黑名单生成；

第二确定单元，用于根据所述第三接收单元接收的所述数据库表格确定所述预置文件是否为所述灰文件；

所述第一接收单元，还用于当所述第二确定单元根据所述数据库表格确定所述预置文件为所述灰文件时，接收局域网中各终端设备上报的灰文件的属性信息。

19、一种 APT 攻击的检测系统，其特征在于，所述系统包括：如权利要求 10-15 中任一项所述的终端设备及如权利要求 16-18 中任一项所述的服务器。

20、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-9 中的任一项所述的 APT 攻击的检测方法。

21、一种计算机可读介质，其中存储了如权利要求 20 所述的计算机程序。

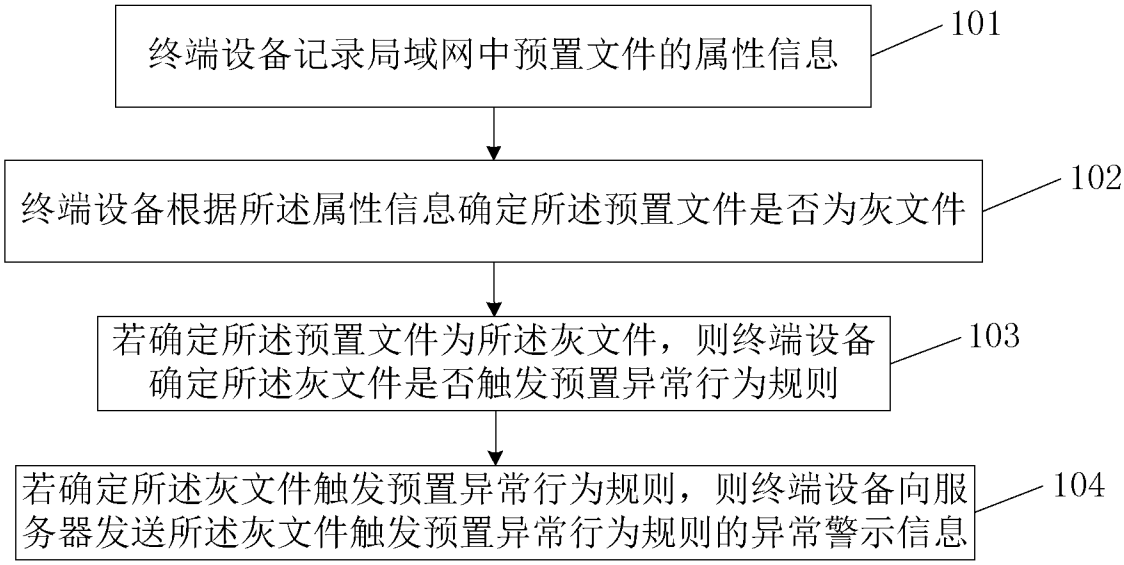

终端设备记录局域网中预置文件的属性信息
101
终端设备根据所述属性信息确定所述预置文件是否为灰文件
102
若确定所述预置文件为所述灰文件，则终端设备确定所述灰文件是否触发预置异常行为规则
103
若确定所述灰文件触发预置异常行为规则，则终端设备向服务器发送所述灰文件触发预置异常行为规则的异常警示信息
104

图 1

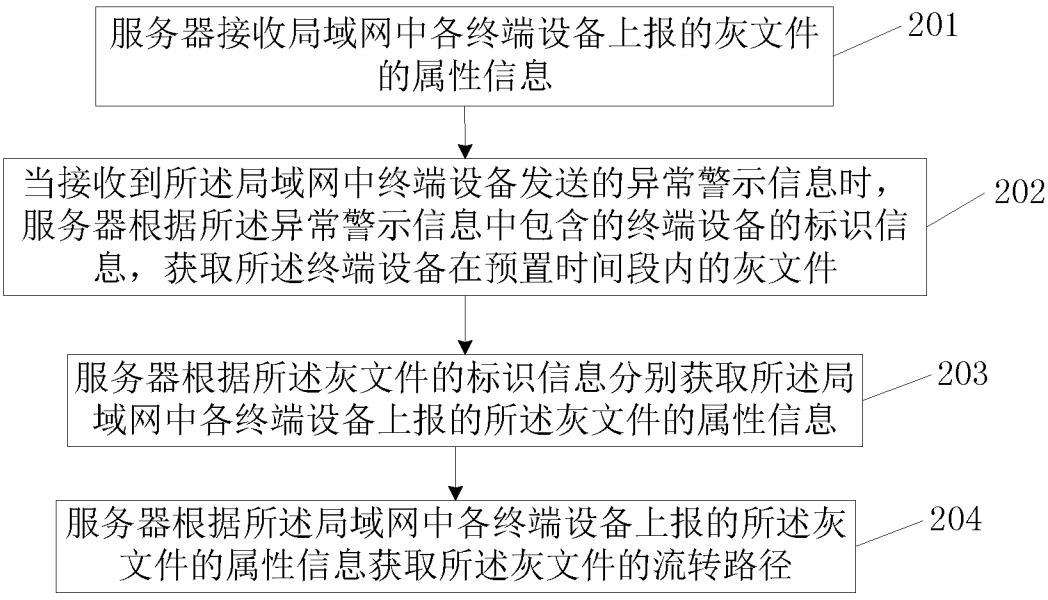

服务器接收局域网中各终端设备上报的灰文件的属性信息
201
当接收到所述局域网中终端设备发送的异常警示信息时，服务器根据所述异常警示信息中包含的终端设备的标识信息，获取所述终端设备在预置时间段内的灰文件
202
服务器根据所述灰文件的标识信息分别获取所述局域网中各终端设备上报的所述灰文件的属性信息
203
服务器根据所述局域网中各终端设备上报的所述灰文件的属性信息获取所述灰文件的流转路径
204

图 2

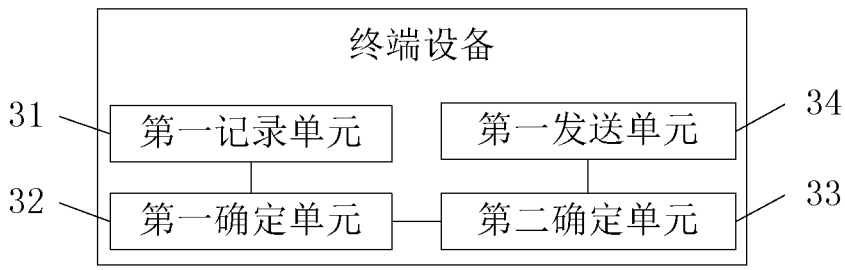

终端设备
31
第一记录单元
34
第一发送单元
32
第一确定单元
第二确定单元
33

图 3

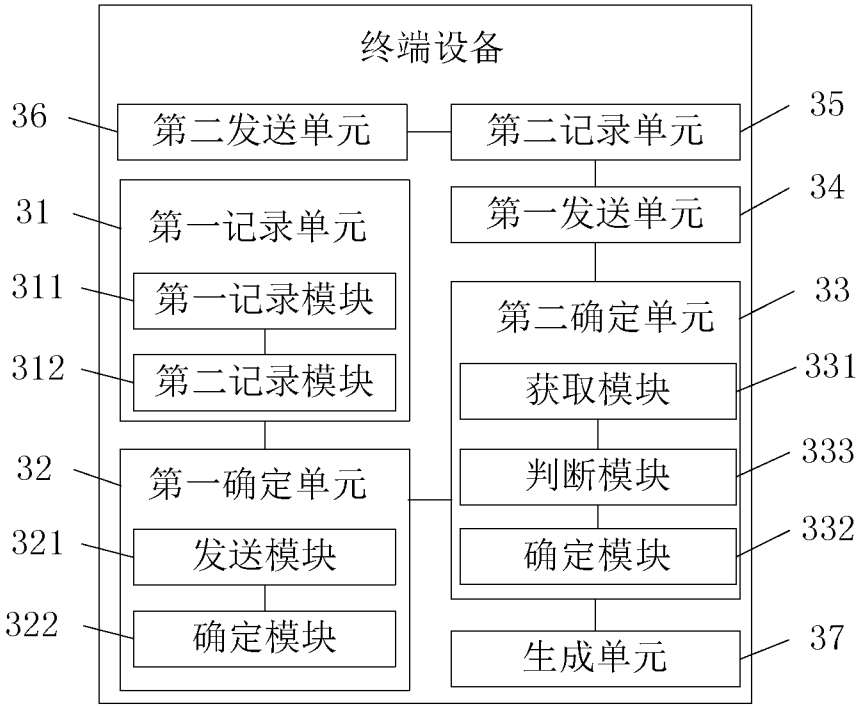

终端设备
36
第二发送单元
第二记录单元
35
31
第一记录单元
第一发送单元
34
311
第一记录模块
第二确定单元
33
312
第二记录模块
获取模块
331
32
第一确定单元
判断模块
333
321
发送模块
确定模块
332
322
确定模块
生成单元
37

图 4

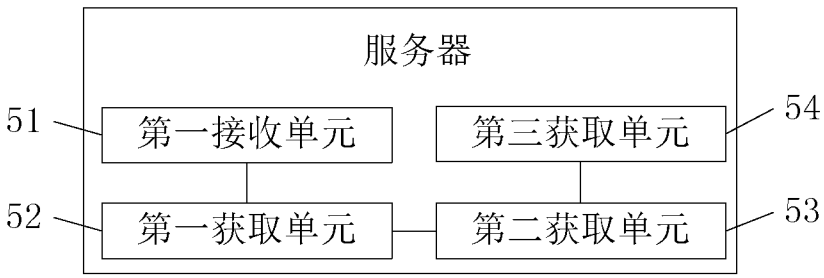

服务器
51
第一接收单元
第三获取单元
54
52
第一获取单元
第二获取单元
53

图 5

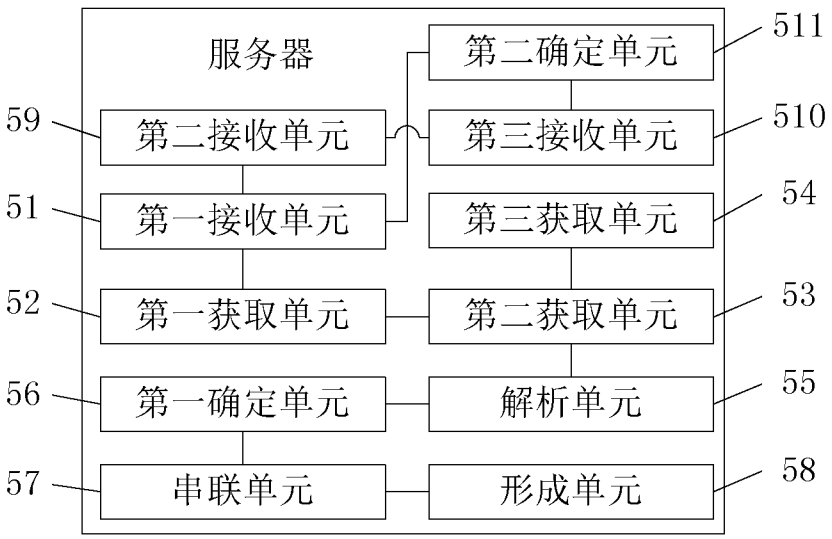

服务器
第二确定单元
511
59
第二接收单元
第三接收单元
510
51
第一接收单元
第三获取单元
54
52
第一获取单元
第二获取单元
53
56
第一确定单元
解析单元
55
57
串联单元
形成单元
58

图 6

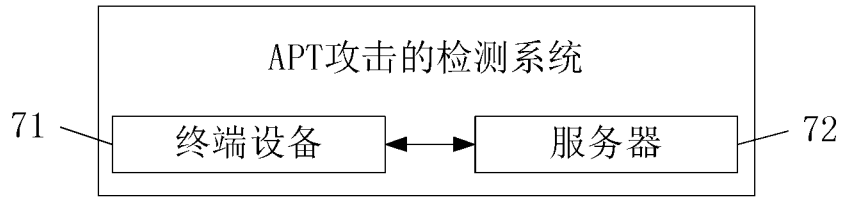

APT攻击的检测系统
71
终端设备
服务器
72

图 7

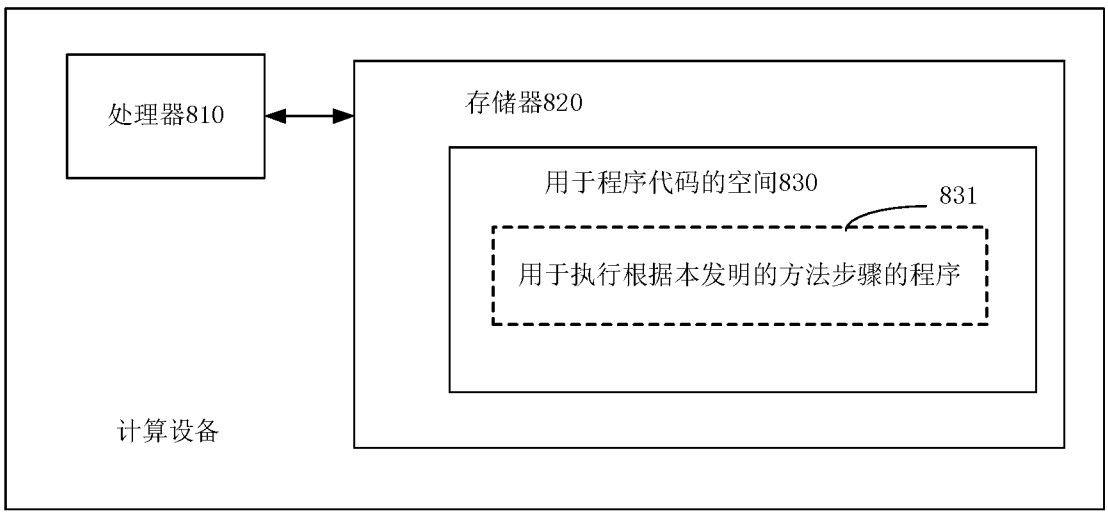

处理器810
存储器820
用于程序代码的空间830
831
用于执行根据本发明的方法步骤的程序
计算设备

图 8

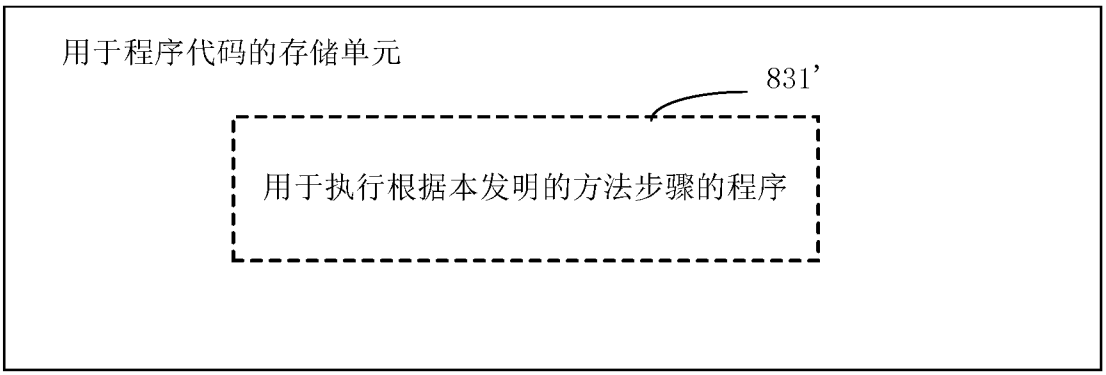

用于程序代码的存储单元
831'
用于执行根据本发明的方法步骤的程序

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/110469

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC; CNKI: circulation, behaviour, gray file, gray list, server, black list, white list, alert, report, APT, terminal, sever, black, white, gray, list, file, document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105430001 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 23 March 2016 (23.03.2016), claims 1-10, and description, paragraph [0198]	1-21
Y	CN 105138901 A (INSPUR ELECTRONIC INFORMATION INDUSTRY CO., LTD.), 09 December 2015 (09.12.2015), description, paragraphs [0005]-[0007]	1-21
Y	CN 104461826 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 25 March 2015 (25.03.2015), claims 1-3 and 10	1-21
A	CN 103902894 A (ZHUHAI JUNTIAN ELECTRONIC TECHNOLOGY CO., LTD. et al.), 02 July 2014 (02.07.2014), the whole document	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 February 2017 (16.02.2017)	**01 March 2017 (01.03.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XU, Hongyan** Telephone No.: (86-10) **62413251**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/110469

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105430001 A	23 March 2016	None	
CN 105138901 A	09 December 2015	None	
CN 104461826 A	25 March 2015	None	
CN 103902894 A	02 July 2014	None	

国际检索报告

国际申请号
PCT/CN2016/110469

A. 主题的分类

G06F 21/56(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT;WPI;EPODOC;CNKI:流转，行为，灰文件，灰名单，终端，服务器，黑名单，白名单，报警，告警，警示，上报，APT，terminal，sever，black，white，gray，list，file，document

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 105430001 A (北京奇虎科技有限公司等) 2016年 3月 23日 (2016-03-23) 权利要求1-10，说明书第[0198]段	1-21
Y	CN 105138901 A (浪潮电子信息产业股份有限公司) 2015年 12月 9日 (2015-12-09) 说明书第[0005]-[0007]段	1-21
Y	CN 104461826 A (北京奇虎科技有限公司等) 2015年 3月 25日 (2015-03-25) 权利要求1-3、10	1-21
A	CN 103902894 A (珠海市君天电子科技有限公司等) 2014年 7月 2日 (2014-07-02) 全文	1-21

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 2月 16日	2017年 3月 1日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 许洪岩 电话号码 (86-10)62413251

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/110469

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 105430001 A	2016年 3月 23日	无	
CN 105138901 A	2015年 12月 9日	无	
CN 104461826 A	2015年 3月 25日	无	
CN 103902894 A	2014年 7月 2日	无	