

(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
2020 年 7 月 2 日 (02.07.2020)



(10) 国际公布号
WO 2020/133986 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/093331

(22) 国际申请日: 2019 年 6 月 27 日 (27.06.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811584694.2 2018 年 12 月 24 日 (24.12.2018) CN

(71) 申请人: 深信服科技股份有限公司 (SANGFOR TECHNOLOGIES INC.) [CN/CN]; 中国广东省深圳市南山区学苑大道 1001 号南山智园 A1 栋一层, Guangdong 518055 (CN)。

(72) 发明人: 闫凡(YAN, Fan); 中国广东省深圳市南山区学苑大道 1001 号南山智园 A1 栋一层, Guangdong 518055 (CN)。 赵振洋(ZHAO, Zhenyang); 中国广东省深圳市南山区学苑大道 1001 号南山智园 A1 栋一层, Guangdong 518055 (CN)。 古亮(GU,

Liang); 中国广东省深圳市南山区学苑大道 1001 号南山智园 A1 栋一层, Guangdong 518055 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦 B 座 18C2、18D、18E、18E2, Guangdong 518001 (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, JO, 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。

(54) Title: BOTNET DOMAIN NAME FAMILY DETECTING METHOD, APPARATUS, DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 僵尸网络域名家族的检测方法、装置、设备及存储介质

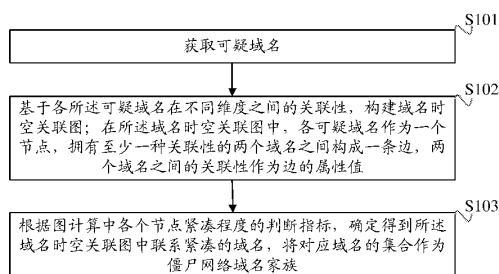


图 1

S101 Acquire suspicious domain names

S102 Construct a domain name spatiotemporal association graph on the basis of associations between various suspicious domain names in different dimensions; take each suspicious domain name as a node in the domain name spatiotemporal association graph, two domain names having at least one association forming an edge therebetween, and the association between the two domain names serving as an attribute value of the edge

S103 According to determination indexes of a compactness degree between various nodes in graph calculation, determine closely associated domain names in the domain name spatiotemporal association graph, and take a set of the corresponding domain names as a botnet domain name family

(57) Abstract: A botnet domain name family detecting method, an apparatus, a device, and a computer-readable storage medium. Said method comprises: acquiring suspicious domain names; constructing a domain name spatiotemporal association graph on the basis of associations between various suspicious domain names in different dimensions; taking each suspicious domain name as a node in the domain name spatiotemporal association graph, two domain names having at least one association forming an edge therebetween, and the association between the two domain names serving as an attribute value of the edge; and according to determination indexes of a compactness degree between various nodes in graph calculation, determining closely associated domain names in the domain name spatiotemporal association graph, and taking a set of the corresponding domain names as a botnet domain name family. The present application shows the associations between domain names in various different dimensions uniformly in the form of an association graph, and has a stronger detection capability. Moreover, the invention is able to detect a botnet domain name family quickly, and is widely applicable.

[见续页]

(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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种僵尸网络域名家族的检测方法、装置、设备以及计算机可读存储介质, 通过获取可疑域名; 基于各可疑域名在不同维度之间的关联性, 构建域名时空关联图; 在域名时空关联图中, 各可疑域名作为一个节点, 拥有至少一种关联性的两个域名之间构成一条边, 两个域名之间的关联性作为边的属性值; 根据图计算中各个节点紧凑程度的判断指标, 确定得到域名时空关联图中联系紧凑的域名, 将对应域名的集合作为僵尸网络域名家族。本申请将域名之间各个不同维度之间的关联性统一用关联图的形式表示出来, 具备更强的检测能力。同时, 能够更快速检测出僵尸域名家族, 具备更广泛的适用性。