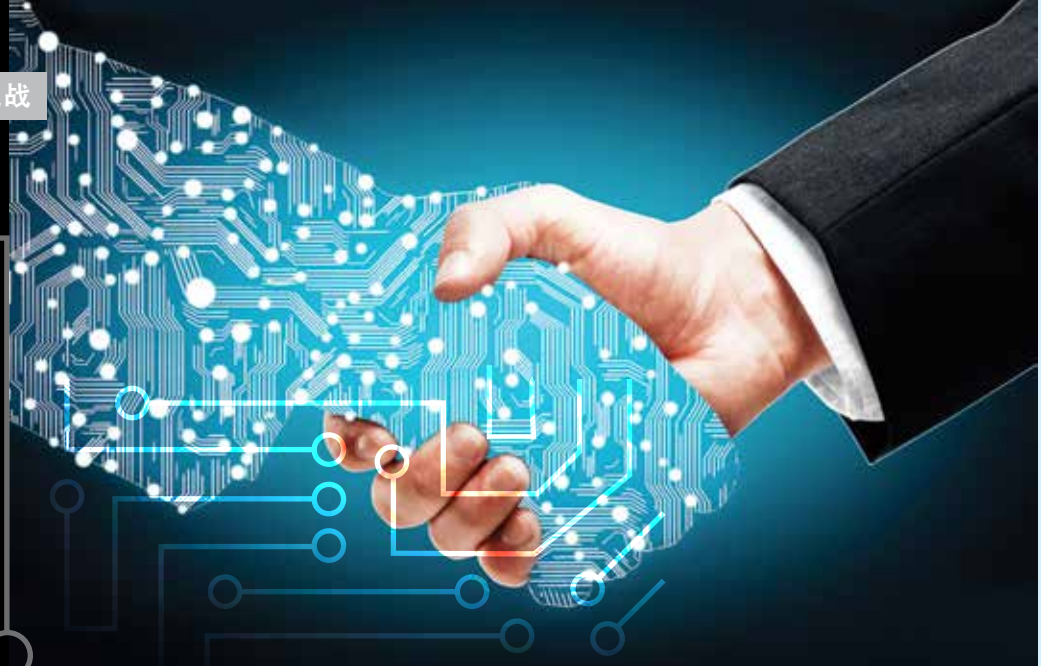

网络安全：IP 地址、其他网络标识和威胁标志（IOC）

美国财政部金融犯罪执法局 (FinCEN) 最近就网络事件和网络犯罪问题向金融机构发布了公告[1]及常见问题解答。[2]

金融犯罪执法局的公告鼓励相关方编写证实重大电子活动和行为的“可疑活动报告”(SAR)，以便及时审查与三个数据点有关的网络风险：互联网协议 (IP) 地址（电脑或服务器的唯一网络连接标识）、其他网络标识和威胁标志 (IOC)。

IP 地址

网络用户可通过众多公共网站查询自己或其他用户的 IP 地址，无论是动态（可变）还是静态（固定）的。[3]

由于手持设备和其他设备的社交媒体和物联网连接剧增，IP 地址的需求量不断飙升。为满足这一需求，采用了地址更长、更加复杂的 IP 地址，在可疑活动报告中必须更加仔细和精确。公众熟悉的 IPv4 32 位数字 IP 地址方案由地址更长的 IPv6 128 位字母数字 IP 地址方案所取代。[4]

IPv4 地址方案支持 4,294,967,296 个唯一地址，使用 nnn.nnn.nnn.nnn（n 代表数字）格式，用英文句号间隔。相比而言，新的 IPv6 方案支持 340,282,366,920,938,463,463,374,607,431,768,211,456 个唯一地址，格式为 cccc:cccc:cccc:cccc:cccc:cccc:cccc:cccc（c 代表字符），用英文冒号间隔，包含字母数字。据悉，金融犯罪执法局可疑活动报告表第 44 项中，最多可输入任一格式的 99 个 IP 地址。[5]

最近一起联邦诉讼涉及到了 IP 地址地理位置追踪的准确性。原告称，约 6 亿个 IP 地址被错误地归属到美国地理中心堪萨斯州的一个农场。原告称，由于该失误，他们受到了有关儿童离家出走、自杀未遂、儿童色情、电脑欺诈和垃圾邮件的不公平调查。[6] 联邦法官拒绝了被告撤销指控的请求。[7]

电子前哨基金会 (EFF) 在对相关方依赖 IP 地址鉴别犯罪地点和个人身份的做法提出质疑时，就以堪萨斯州农场案件为例。电子前哨基金会向执法部门和法院提出建议，鼓励对 IP 地址数据进行恰当评估并尽早证实。[8]

[1] “FIN-2016-A005 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime”（就网络事件和网络犯罪问题对金融机构发布的 FIN-2016-A005 公告），*美国财政部金融犯罪执法局*，2016 年 10 月 25 日，https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

[2] “Frequently Asked Questions (FAQs)”（常见问题解答），美国财政部金融犯罪执法局，2016 年 10 月 25 日，https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF

[3] *WhatIsMyIPAddress.com（我的 IP 地址查询网）*，http://whatismyipaddress.com

[4] John D. Schanz，“How IPv6 lays the foundation for a smarter network”（IPv6 如何为智能网络奠定基础），*Network World*，2016 年 6 月 27 日，http://www.networkworld.com/article/3088322/internet/how-ipv6-lays-the-foundation-for-a-smarter-network.html

[5] “FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions”（金融犯罪执法局可疑活动报告电子表单编写说明），第 1.2 版，*金融犯罪执法局*，2012 年 10 月，https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf

[6] 原告：James 和 Theresa Arnold；被告：MaxMind 公司，*美国堪萨斯州区地区法院*，2016 年 8 月 5 日，https://consumermediallc.files.wordpress.com/2016/08/gov-uscourts-ksd-null-null-0.pdf

[7] 备忘录及法令，原告：James 和 Theresa Arnold；被告：MaxMind 公司，第 16-1309-JTM 号，美国堪萨斯州区地区法院，2016 年 10 月 20 日，https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2016cv1309-16

[8] Aaron Mackey、Seth Schoen、Cindy Cohn，“Unreliable Informants:IP Addresses, Digital Tips and Police Raids”（不可靠的信息提供者：IP 地址、数字提示和警察搜捕），电子前哨基金会，2016 年 9 月，https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf

通过欺诈性 IP 地址，名为 Methbot 的僵尸网络造成了超过 1.8 亿美元的资金损失。Methbot 使用美国和荷兰托管的服务器来运行 850,000 多个虚假 IP 地址的自动程序，网络犯罪分子借此进行了迄今为止发现的最大广告欺诈活动。据报道，这一诈骗活动通过海外网络注册以欺骗方式获取 IP 地址，然后在美国互联网服务提供商上虚假注册，每天获得欺诈性广告收入 300-500 万美元。这些 IP 地址看起来就像是美国国内的真实用户注册的，从而避开了欺诈检测。[9]

IP 地址通常与某一电脑或服务器相关，但是与具体用户却可能相关也可能不相关，这就会引发数据隐私问题。美国联邦贸易委员会 (FTC) 工作人员将 IP 地址视为个人身份信息，在该地址或其他永久性标识与个人、电脑或设备相连时，应受到适当的保护。[10]

联邦贸易委员会工作人员已警告获取永久性标识的网站运营商不得作出未收集个人信息或匿名收集数据的一般性声明。对收集的所有数据必须有恰当的数据保护措施和风险评估，而不仅是对个人姓名或邮件地址这类数据。[11]

欧盟法院 [12] 最近规定，动态 IP 地址在与个人用户可识别数据结合时可归类为个人数据。[13] 这与欧盟《通用数据保护条例》(GDPR) 一致。该《条例》将在 2018 年 5 月 25 日正式生效。

《通用数据保护条例》第 30 条规定，自然人可与网络标识（例如 IP 地址）关联。这类网络标识可能会留下痕迹，与唯一标识和服务器收到的其他信息结合时可用于形成自然人个人资料并识别他们。[14]

通过本地或云服务器 [15] 收集欧盟个人数据的网站运营商和应用软件提供商应熟知《通用数据保护条例》对 IP 地址收集的规定。其中包括更严格的授权、保留和跨境数据传输义务，可有例外。[16]

阿根廷、[17] 加拿大、[18] 中国香港、[19] 日本 [20] 和瑞士 [21] 等国家和地区在 IP 地址与可识别数据结合时将其归类为个人数据。

巴西对 IP 地址采取了一项显著措施。为了方便鉴别涉嫌违法行为或侵犯个人数据的用户，巴西要求在连接日志（跟踪用户的网络连接）和应用使用日志（跟踪用户的互联网软件使用）上保留用户的 IP 地址。连接日志必须在安全环境下保留一年；应用使用日志保留六个月。警察或行政人员可要求延长日志保留时间。用户必须知晓数据保护和日志保留措施。[22]

[9] “The Methbot Operation”（Methbot 操作），White Ops, 2016 年 12 月 20 日，http://go.whiteops.com/rs/179-SQE-823/images/WO_Methbot_Operation_WP.pdf

[10] “Protecting Consumer Privacy in the Digital Age:Reaffirming the Role of Consumer Control, Keynote Address of FTC Chairwoman Edith Ramirez Technology Policy Institute Aspen Forum”（数字时代客户隐私保护：重申客户控制作用，联邦贸易委员会主席 Edith Ramirez 在技术政策研究院阿斯彭论坛上的主旨演讲），联邦贸易委员会，2016 年 8 月 22 日，https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf

[11] Jessica Rich，“Keeping Up with the Online Advertising Industry”（跟上网络广告业的步伐），联邦贸易委员会，2016 年 4 月 21 日，https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry

[12] 奥地利、比利时、保加利亚、克罗地亚、塞浦路斯、捷克、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典和英国。

[13] “Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland”（C-582/14 号案件，原告：Patrick Breyer；被告：德意志联邦共和国），法院判决（德国联邦参议院），2016 年 10 月 19 日，http://curia.europa.eu/juris/document/document_print.jsf;jsession...qMbN4PahaLe0?doclang=EN&text=&pageIndex=0&docid=184668&cid=90876

[14] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016”（2016 年 4 月 27 日欧洲议会和欧洲委员会第 2016/679 号规定），《欧盟官方杂志》，2016 年 4 月 5 日，http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[15] “Managing the Challenges of the Cloud Under the New EU General Data Protection Regulation”（新《欧盟通用数据保护条例》下的云管理挑战），Netskope，2016 年，http://cloudfseurope.com/wp-content/uploads/sites/3/2016/05/Netskope-EU-GDPR-Managing-the-Challenges-of-Cloud-White-Paper.pdf

[16] Alex van der Wolk，Hanno Timner，“European Court of Justice:IP Addresses Are Personal Information”（欧洲法院：IP 地址为个人信息），Westlaw Journal Computer & Internet，2016 年 11 月 4 日，https://media2.mofo.com/documents/161104-wlj-european-court-of-justice.pdf

[17] Maximiliano D'Auro、Florencia Rosati、Manuela Adrogué、Ambrosio Nougués，“Data protection in Argentina:Overview”（阿根廷数据保护概况），Practical Law，2016 年 9 月 1 日，http://us.practicallaw.com/3-586-5566

[18] “What an IP Address Can Reveal About You”（IP 地址可能透露你的什么信息），加拿大隐私专员办公室，2013 年 5 月，https://www.priv.gc.ca/media/1767/ip_201305_e.pdf

[19] “Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's perspective (2nd Edition)”（从隐私专员视角看数据保护原则（隐私）条例）（第 2 版），香港个人资料隐私专员公署，2010 年，https://www.pcpd.org.hk/english/resources_centre/publications/books/files/Perspective_2nd.pdf

[20] Mangyo Kinoshita、Shino Asayama、Eric Kosinski，“Data protection in Japan: overview”（日本数据保护概况），Practical Law，2014 年 11 月 1 日，http://uk.practicallaw.com/5-520-1289

[21] Tom Espiner，“Swiss fileshare software broke DP law, says court”（法院称瑞士文件共享软件违反数据保护法），ZDNet，2010 年 9 月 10 日，http://www.zdnet.com/article/swiss-fileshare-software-broke-dp-law-says-court/

[22] Raphael de Cunto、Julia Arruda，“A civil rights framework for the internet in Brazil”（巴西互联网民权框架），*Financier Worldwide*，2014 年 7 月，https://www.financierworldwide.com/a-civil-rights-framework-for-the-internet-in-brazil/#.WFiuJ7GZMmo

自 2012 年 10 月以来，美国联邦调查局、国土安全局和其他联邦政府机构通过非机密联合指标公报 (JIB) 披露了与网络威胁有关的 IP 地址。联合指标公报揭露了与恶意网络活动有关的 IP 地址和域名，以此减轻僵尸网络和分布式拒绝服务 (DDoS) 攻击的网络威胁。公报已通过安全渠道向美国金融机构和海外合作伙伴发布。[23]

网络罪犯和恐怖主义者可能会通过洋葱路由器 (Tor)、虚拟专用网络 (VPN) 或代理工具来隐藏 IP 地址位置或身份以便匿名上网，[24] 尤其是在有报道披露某些罪犯因未使用该类匿名网络浏览工具而被捕的案件后，犯罪分子会更倾向于使用该类工具。[25]TORWallet 可使 IP 地址每 30 秒钟就清除一次，让比特币钱包活动能够匿名进行。[26]

美国联邦刑事诉讼程序规则第 41 条规则的最新规定于 2016 年 12 月 1 日起生效。电子前哨基金会称，根据第 41 条规则的新规定，只要某台计算机使用 Tor、VPN 或代理工具之类的匿名保护软件，执法部门获取搜查令的程序将比以前更加简单，因此，应为这条新规定增设保证条款。[27]

在线博彩网站（例如 10Bet）可能会直接在条款和细则及有关隐私、cookies、反欺诈、反洗钱、通报执法机关的政策中对匿名浏览网页做出规定，[28] 部分原因在于网站用户可以使用这些工具避开身份验证和地理限制。[29]

金融犯罪侦查员可以利用 Tor 项目数据库 ExoneraTor，该数据库让公众可以检查某个 IP 地址在某一天是否成了 Tor 网络中继。[30]

尽管媒体公司（如 Netflix 和 Hulu）一直限制用户使用 VPN 或代理工具避开地域限制，但是检测使用 VPN 或代理工具的 IP 地址并非易事。[31] 而且，据《*财富*》报道，由于美国国会投票废除了互联网服务提供商可收集和出售客户数据的限制，近期 VPN 的需求猛增。[32]

金融犯罪执法局的公告提供了义务和自愿提交可疑活动报告的案例，鼓励对相互关联的网络犯罪和事件提交单个可疑活动报告，例如旨在隐藏网络犯罪、符合义务提交条件的 DDoS 网络事件。例如，应通过描述欺骗攻击的基本细节 [33] 来说明犯罪分子如何使用 IP 地址和其他网络标识来假冒用户或设备进行复杂的 DDoS 网络事件，以及金融犯罪侦查员如何在可疑活动报告中简洁地描述该类复杂网络事件。

其他网络标识

与 IP 地址类似，由设备、应用、工具和协议提供的网络标识在与可识别数据结合时可视为个人数据。根据《一般数据保护条例》第 30 条规定，该类网络标识包括 cookie 标识和射频识别标识。[34]

网络标识还可包括：地理位置数据、设备标识（如 MAC 地址）、操作系统和浏览器属性、应用数据、网站活动和应用使用数据。如 DocuSign 的隐私政策所示，数字签名的身份验证要求特别关注设备和其他网络标识。[35]

[23] “Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015”（2015 年网络安全信息共享法案下联邦政府网络威胁指标和防范措施），*美国国家情报总监办公室*、*国土安全部*、*国防部*、*司法部*，2016 年 2 月 16 日，https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf

[24] Mark Wilson，“The best free tools for anonymous browsing 2016”（2016 年匿名浏览网页的最佳免费工具），*Techradar*，2016 年 10 月 11 日，http://www.techradar.com/news/software/best-free-tools-for-anonymous-browsing-1321833

[25] Catalin Cimpanu，“Crook Who Used His Home IP Address for Banking Fraud Gets 5 Years in Prison”（诈骗犯用家庭 IP 地址进行银行诈骗，获刑 5 年），*Bleeping Computer*，2016 年 12 月 21 日，https://www.bleepingcomputer.com/news/security/crook-who-used-his-home-ip-address-for-banking-fraud-gets-5-years-in-prison/

[26] “Anonymous Bitcoin Wallet”（匿名比特币钱包），*TORWallet*，https://torwallet.com

[27] Jamie Williams，“Expanded Government Hacking Powers Need Accompanying Safeguards”（需为扩大的政府黑客入侵权力制定保证条款），*电子前哨基金会*，2016 年 12 月 14 日，https://www.eff.org/deeplinks/2016/12/expanded-government-hacking-powers-need-accompanying-safeguards

[28] “Terms and Conditions”（条款），10Bet，2016 年 12 月 15 日，https://www.10bet.com/help/terms-and-conditions/

[29] “The prevention of money laundering and combating the financing of terrorism - Guidance for remote and non-remote casinos”（反洗钱和反恐融资——远程与非远程赌场指南），*博彩委员会*，2016 年 7 月，http://www.gamblingcommission.gov.uk/PDF/AML/Prevention-of-money-laundering-and-combating-the-financing-of-terrorism.pdf

[30] *ExoneraTor*，https://exonerator.torproject.org

[31] Chris Hoffman，“How to Watch Netflix, Hulu, and More Through a VPN Without Being Blocked”（如何收看 Netflix 和 Hulu 并使用 VPN 无门槛看节目），*How-To Geek*，2016 年 1 月 20 日，http://www.howtogeek.com/239616/how-to-watch-netflix-hulu-and-more-through-a-vpn-without-being-blocked/

[32] “Congress Voted to Roll Back Internet Privacy Rules.Now People Are Looking to VPNs”（国会投票废除互联网隐私规则，VPN 广受青睐），*《财富》*，2017 年 3 月 28 日，http://fortune.com/2017/03/28/congress-internet-privacy-rules-vpns/

[33] Neil DuPaul，“Spoofing Attack:IP, DNS & ARP”（欺骗攻击：IP，DNS & ARP），*Veracode*，https://www.veracode.com/security/spoofing-attack

[34] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016”（2016 年 4 月 27 日欧洲议会和欧洲委员会第 2016/679 号规定），*《欧盟官方杂志》*，2016 年 4 月 5 日，http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[35] “Privacy Policy”（隐私政策），DocuSign，2016 年 12 月 15 日，https://www.docusign.com/company/privacy-policy

[36] “Mobile Fraud Gone in a (Device) Flash”（重写清除移动欺诈），*DataVisor*，2016 年 7 月 5 日，https://www.datavisor.com/threat-blogs/mobile-fraudsters-gone-in-a-device-flash/

随着金融服务网络和移动设备访问能力越来越强，网络罪犯试图通过网络标识来规避欺诈检测。[36]

资金转账公司（如 PayPal）直接在其欧盟网站的条款和细则中对设备和其他网络标识做出来规定。还制定了有关隐私、cookies、反欺诈、反洗钱和通报执法机关的政策。[37]

威胁标志

10 多年来，威胁标志 (IOC) 一直被电脑安全公司（如 IBM）用作指示网络攻击的数字证据。该类数字证据可报告异常情况，例如网络攻击者链接到被攻击网络的 IP 地址、域、文件和数字线索，使用终端管理工具检测安全事件、补救网络环境。[39]

IOC 可根据与某一地理位置有关的 IP 地址捕获到意想不到的网络访问细节。网络安全公司（如 Kaspersky Lab）会公开 IOC，以便让各公司组织能够鉴别金融网络攻击集团（如 Metel、GCMAN 和 Carbanak 2.0）的访问痕迹。

相比而言，在过去几年，攻击术语 Indicators of Attack (IoA)（攻击标志）被电脑安全公司（如 IBM、英特尔 和 CrowdStrike）用来指明代表网络攻击正在发生或未来可能发生的数字证据，并同时使用终端管理工具检测安全事件，补救网络环境。

Crowdstrike 使用 IOC 指代恶意软件、签名、漏洞利用程序、漏洞和 IP 地址。IoA 指代密码执行、持续性、秘密行动、控制和横向移动。

Crowdstrike 对 IoA 的说明与 Cyber Kill Chain® 框架 一致。Cyber Kill Chain® 是由美国最大的防护商 Lockheed Martin 研发的框架，旨在通过 7 个步骤鉴别和预防网络攻击：踩点、组装、投送、攻击、植入、控制、横向移动。

最近有一项研究对“把 IoA 作为检测和补救网络攻击的更优报告工具的缺点”进行了评估，突出了 IOC 对电脑安全行业的重要性。商业和非营利组织可能会更多地使用 IoA，因为他们更注重使用 Cyber Kill Chain® 框架 来预防网络攻击，包括某些国家发起的攻击。

总之，这份有关 IP 地址、其他网络标识和 IOC 的及时评估，通过提出如 IPv6 是否准备就绪、IP 数据的恰当评估和确认、IP 地址和网络标识作为个人数据的处理方式等相关操作问题，有助于可疑活动报告的编制。

网站隐私通知和条款应及时更新，并实行类似于欧盟《一般数据保护条例》的更严格的个人数据保护要求。

应加强关于网络罪犯如何利用 IP 地址和其他网络标识避开检测、如何利用 Tor、VPN 和代理工具规避身份验证和地理限制的教育。除 IOC 数据外，IoA 数据也有助于依照金融犯罪执法局的公告来编制可疑活动报告。

Miguel Alcántar，CAMS-FCI，合规顾问，美国加利福尼亚州奥克兰，alcantar@aya.yale.edu

[37] “Privacy Policy for PayPal Services”（PayPal 服务隐私政策），*PayPal*，2017 年 1 月 27 日，https://www.paypal.com/uk/webapps/mpp/ua/privacy-full

[38] “Indicators of compromise”（威胁标志），*IBM*，2015，https://pcatt.org/techblog/wp-content/uploads/2015/10/IndicatorsOfCompromise.pdf

[39] “How BigFix Helps Investigate a Threat in Forensic Activities”（司法活动中 BigFix 如何协助侦察威胁），*IBM*，https://www.ibm.com/developerworks/community/wikis/form/anonymous/api/wiki/90553c0b-42eb-4df0-9556-d3c2e0ac4c52/page/2a87e237-39ca-4489-81c5-c81124f91a48/attachment/446c7dd5-8737-4342-9acb-3712b0c57556/media/Investigating_threats_with_Bigfix.pdf

[40] Jason Andress，“Working with Indicators of Compromise”（处理威胁标志），*ISSA Journal*，2015 年 5 月，https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0515.pdf

[41] “APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks”（Metel、GCMAN 和 Carbanak 2.0 攻击导致 APT 式银行抢劫增多），*Kaspersky Lab*，2016 年 2 月 8 日，https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/

[42] IBM BigFix Detect，*IBM*，https://www.ibm.com/us-en/marketplace/bigfix-detect#product-header-top

[43] “Indicators of Attack (IoA)”（攻击标志），*英特尔*，http://www.mcafee.com/us/resources/solution-briefs/sb-indicators-of-attack.pdf

[44] Jessica DeCianno，“Indicators of Attack versus Indicators of Compromise”（攻击标志 (IOA) 与威胁标志 (IOC) 的区别），*CrowdStrike*，2016 年 12 月 9 日，https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/

[45] Cyber Kill Chain®，*Lockheed Martin*，http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

[46] Lysa Myer，“Cyber Kill Chain is a Great Idea, But is It Something Your Company Can Implement?”（Cyber Kill Chain 创意虽好，但适合你的公司么？），*Infosec Institute*，2013 年 5 月 31 日，http://resources.infosecinstitute.com/cyber-kill-chain-is-a-great-idea-but-is-it-something-your-company-can-implement/#gref

[47] Dave Dittrich、Katherine Carpenter，“Misunderstanding Indicators of Compromise”（误解威胁标志 (IOC)），*Threatpost Op-Ed*，2016 年 4 月 21 日，https://threatpost.com/misunderstanding-indicators-of-compromise/117560/

[48] Lysa Myers，“The practicality of the Cyber Kill Chain approach to security”（Cyber Kill Chain 对网络安全的实用性），*CSO*，2016 年 10 月 4 日，http://www.csoonline.com/article/2134037/strategic-planning-erm/the-practicality-of-the-cyber-kill-chain-approach-to-security.html

[49] Dave Dittrich、Katherine Carpenter，“Misuse of Language: ‘Cyber’; When War is Not a War, and a Weapon is Not a Weapon”（语言误用：“网络”；当花非花雾非雾），*Threatpost Op-Ed*，2016 年 8 月 9 日，https://threatpost.com/misuse-of-language-cyber-when-war-is-not-a-war-and-a-weapon-is-not-a-weapon/119740/