

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Google LLC,

Plaintiff,

-against-

Zubair Saeed; Raheel Arshad; Mohammad
Rasheed Siddiqui; and Does 1–15,

Defendants.

Case No.

FILED UNDER SEAL

**COMPLAINT FOR DAMAGES AND
INJUNCTIVE RELIEF**

Plaintiff Google LLC (“Google”) for its Complaint against the Defendants listed below alleges as follows:

INTRODUCTION

1. Malicious software, or “malware,” finds its way onto unsuspecting victims’ computers through a number of different distribution methods. One of the primary means of distributing malware is through using illegally “cracked” software,¹ which purports to be innocuous third party software, that can be modified to surreptitiously install malware on a user’s device, such as a computer. Users download such cracked software and install on their computers, thus infecting their computer with malware.

2. CryptBot is a kind of malware that is commonly spread through the distribution of cracked software, as described above. The Defendants are engaged in the distribution of CryptBot malware designed to steal sensitive information from victims’ computers, through

¹ “Cracked software” refers to software that has been modified without authorization from its owner, typically to undermine technical protection measures designed to prevent copying. The term “cracked software” in this Complaint refers to all maliciously modified software, including freely available software that is distributed by its developer without technical protection measures.

websites that distribute “cracked” software (“Malware Distribution Enterprise”). Defendants’ criminal scheme is perpetrated via a pay-per-install (“PPI”) network known as “360installer,” which fosters the creation of websites that offer illegally modified software (“Cracked Software Sites”).² These websites offer software infected with CryptBot malware, such as maliciously modified versions of Google Chrome and Google Earth Pro, and also cracked third party software. The Malware Distribution Enterprise operated by Defendants in this case is one of the primary means of spreading the CryptBot malware to new victims.

3. CryptBot is malware often referred to as an “infostealer” because it is designed to steal user information from victims’ computers such as social media account logins, website logins, browser cookies, credit cards, and cryptocurrency wallets. Such information is uploaded to the CryptBot botnet command-and-control (“C2”) server, and then sold for use in malicious computer hacking campaigns with serious consequences for victims.³

4. CryptBot is designed to target the users of certain Internet browsers including Google Chrome. Once executed, the CryptBot malware checks the infected computer for an installation of Google Chrome, and then attempts to locate, collect, and extract user credentials saved to Google Chrome.

5. Google brings this action under the Racketeer Influenced and Corrupt Organizations Act (“RICO”), Computer Fraud and Abuse Act (“CFAA”), Lanham Act, and New York state common law against Defendants’ criminal enterprise to disrupt the Malware Distribution Enterprise and the CryptBot botnet, to prevent it from causing further harm to users, and to recover damages for the harm Google has already endured.

² Appendix A lists the domains associated with the Cracked Software Sites.



³ Appendix B lists the domains associated with the CryptBot botnet’s command-and-control infrastructure.

PARTIES

Plaintiff

6. Plaintiff Google LLC (“Google”) is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway in Mountain View, California.

7. Google is a leading technology company that offers a wide variety of services to organize the world’s information and make it universally accessible and useful. Google strives to provide its users worldwide with safe and secure platforms.

8. Google operates numerous products, platforms, and services, three of which are relevant here: (1) Google Chrome is Google’s free-to-use internet browsing application; (2) Chrome Extensions are applications that can embed certain functionality into the Google Chrome browser; and (3) Google Earth Pro is a free-to-use tool that renders a three-dimensional representation of Earth based on satellite imagery. Google owns and uses multiple trademarks in interstate commerce in connection with Google Earth Pro and Google Chrome, including GOOGLE, GOOGLE EARTH PRO, the Google Earth Design () , GOOGLE CHROME, CHROME and the Chrome Design () (collectively the “Google Marks”), among others.

9. Google owns the following U.S. trademark registrations (among many others) for the Google Marks for use in connection with computer services and operating and browsing software, all of which are valid and subsisting on the Principal Register of the U.S. Patent and Trademark Office:

Mark	Reg. No.	Reg Date	First Use in U.S. Commerce
GOOGLE	2,806,075	Jan. 20, 2004	Sept. 1, 1997 (Classes 38, 42)
	4,035,756	Oct. 4, 2011	Sept. 1, 2008 (Classes 9, 42)
	5,380,809	Jan. 16, 2018	Mar. 29, 2011 (Class 9)
GOOGLE CHROME	5,448,706	Apr. 17, 2018	Sept. 2, 2008 (Classes 9, 42)
CHROME	5,355,294	Dec. 12, 2017	Sept. 2, 2008 (Classes 9, 42) Dec. 7, 2010 (Class 35)
	5,536,709	Aug. 7, 2018	Apr. 18, 2017 (Classes 9, 39, 42)

10. Pursuant to Section 7(b) of the Lanham Act, 15 U.S.C. § 1057(b), Google's registrations for the Google Marks constitute prima facie evidence of their validity and of Google's exclusive right to use the marks in connection with the identified goods and services.

11. Google has expended substantial time, money, and other resources in developing, advertising, and promoting the Google Marks. The Google Marks have been the subject of substantial and continuous marketing and promotion by Google since as early as 1997.

12. The Google Marks are distinctive and identify goods and services as originating from, endorsed by, or otherwise affiliated with Google.

Defendants

13. The defendants listed in paragraphs 14 through 17 are individuals who have conspired to engage in a pattern of racketeering activity. They each have participated in the operation or management of the Malware Distribution Enterprise and have engaged in criminal acts causing harm to Google and countless others.

14. Defendant Zubair Saeed is an individual who resides in Pakistan.

15. Defendant Raheel Arshad is an individual who resides in Pakistan.

16. Defendant Mohammad Rasheed Siddiqui is an individual who resides in Pakistan (Defendants Zubair Saeed, Raheel Arshad, and Mohammad Rasheed Siddiqui, collectively, referred to as the "Malware Distribution Defendants").

17. Plaintiff does not know the true names and capacities of the operators of the CryptBot botnet (the "CryptBot Defendants"), and therefore sues these defendants by the fictitious names Does 1 through 15. Each of the Doe Defendants is responsible in some manner for the conduct alleged, having agreed to become part of the Malware Distribution Enterprise in an effort to distribute CryptBot malware that forms the larger botnet.

JURISDICTION AND VENUE

18. This Court has federal question jurisdiction over Google's claims under RICO, the CFAA, and the Lanham Act. This Court has supplemental jurisdiction over the state law claim under 28 U.S.C. § 1367. The state law claims asserted herein are intimately related to the RICO, CFAA, and Lanham Act claims, are built on the same factual predicates, and are part of the same controversy.

19. Defendants are subject to personal jurisdiction in this district, and the exercise of jurisdiction over Defendants is proper pursuant to 18 U.S.C. § 1964 and N.Y. C.P.L.R. 301 and 302 (McKinney 2022). Defendants have transacted business and engaged in tortious conduct in the United States and in New York that gives rise in part to Google's claims. Defendants have also engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants knew and intended would be felt in the United States and New York. Defendants have intentionally distributed maliciously modified software, leveraging infrastructure hosted in New York, caused malware to be installed on victims' machines in this district, in New York, and throughout the United States; have intentionally directed victims' machines in this district, in New York, and throughout the United States to participate in intentional, wrongful, illegal, and/or tortious acts. Defendants were aware of the effects in the United States and New York of those acts; the activities of their co-conspirators and agents were to the benefit of Defendants; and their co-conspirators and agents were working at the direction, under the control, at the request, and/or on behalf of Defendants in committing those acts.

20. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial

district, because part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Defendants avail themselves of the privilege of conducting business in New York, and utilize instrumentalities located in this judicial district to carry out acts alleged herein.

21. Defendants have affirmatively directed actions at New York and the Southern District of New York by targeting their activities, including theft of funds and information, at individual computer users located in the Southern District of New York. Defendants have distributed maliciously modified software to and directed harmful computer code at the computers of individual users located in New York and the Southern District of New York.

FACTUAL ALLEGATIONS
Pay-Per-Install Networks

22. "Pay-Per-Install" or "PPI" refers to a service designed to generate and direct Internet traffic so that users download and then install a particular file. PPI services offer the ability to attract users to download a particular file or link provided by a customer. That customer is usually a developer seeking to find users to download and install a particular file. The developer pays the PPI service for each user installation. A PPI service will often have a network of different domain names and websites to generate and maintain a user base to whom they target download links. Accordingly, a single PPI service may be associated with hundreds of seemingly unrelated websites.

23. The ultimate value of a PPI service relies upon the developer's ability to convert installations into revenue, since the developer has to pay the PPI service. When a developer wants to use a PPI service to promote the distribution of its software, the goal is to generate a profit. In other words, a developer hires a PPI because it has devised a way to make money off

the cracked software installation. In some cases, the value of paying a fee to the PPI is tied the developer's ability to convert users from the free, demonstration ("demo") version of the software to the paid version. This is not the case when it comes to cracked software (since the entire point of cracked software is that it is "free"), which has a different revenue model. For "cracked" software distributed with PPIs, a developer's revenue model is typically stealing information from the users that click the promoted installation files.

24. For PPIs that advertise the free distribution of cracked software, the websites that are created to host the installation links typically advertise that they are cracked versions of otherwise legitimate software. These websites are created by the PPI's affiliates. PPI affiliates create or manage the websites the PPIs use to promote a developer's installation links. On information and belief, malicious hackers use cracked software as a vehicle to distribute malware because users downloading such software are less likely to make a formal complaint or to exercise good cyber hygiene.

25. Cracked software PPIs, which already operate outside of the law by distributing cracked software in violation of intellectual property laws, are aware that their sites are associated with the distribution of malware and often use a wide collection of seemingly unrelated domain names and website addresses in order to obfuscate their illicit conduct.

Distribution of "Cracked" Software as a Means for Spreading Malware

26. Cracked software is typically downloaded by users looking for free versions of paid products, but malware is also often distributed in maliciously modified versions of software programs that developers, including Google, make freely available to users. In some instances, the cracked software retains all or most of the legitimate software's functionality.

27. PPI networks that focus on the distribution of malware are aware that their paying developer customers pay them from the proceeds of malicious computer hacking.⁴ PPI networks distribute their customers' installation links through "affiliate" webpage developers. PPI networks pay their affiliates a fee for every installation their webpage generates.⁵ PPIs pay this fee from their customers' payment of the PPI service for the installations. PPIs have a network of different affiliate websites they can use to promote their developers' customer software.

28. When a user downloads software, whether legitimate or maliciously modified, they typically have to run an executable file that will either install the software from the downloaded file itself or run an installer application that pulls in relevant install files from the Internet. Because users expect to run an executable file to install software, users typically do not realize that the installer is installing malware, in addition to the desired software. And a user's subsequent attempt to uninstall the maliciously modified software would not remove any malware deployed from the initial installation.

29. When PPI networks are identified as sharing maliciously modified software, they are often the subject of complaints by the legitimate software developers who demand removal of the offending material. PPI networks that ignore these demands (and continue to advertise their services) have a reputation as providers who are willing to distribute digital contraband including malicious software. In such instances, and upon information and belief, the PPI networks and their customers are aware that the software they distribute is not provided or sanctioned by its legitimate owners, and that the customer responsible for that maliciously

⁴ This Complaint recognizes that "hacking" is a term that can describe both malicious and non-malicious conduct and specifies that it is referring to malicious "hacking" that represents the unauthorized access of a computer system for purposes of fraud or other malicious conduct.

⁵ For example, the 360installer website discussed below advertises that it pays \$2 per installation.

modified product must monetize installations in order to pay the PPI network's per-installation fees.

The CryptBot Botnet

30. A “bot” (short for “robot”) is a computer or device that is infected by malware and that can be tasked to conduct specific activities. A “botnet” is a network of internet-connected devices (bots), each of which are infected by malware. The botnet is controlled by “command-and-control” (“C2”) servers, which can instruct the devices comprising the botnet to perform any number of disruptive or even criminal tasks. The C2 servers typically are controlled remotely by individual operators, referred to as “bot controllers.” While a botnet may operate through various pieces and iterations of malware used to access and control computers without authorization, the term itself describes the resulting network of computers that can be controlled by a malicious actor or actors for one or more malicious purposes.

31. A botnet can leverage its infected computers in many different ways, and different botnets may have different foci. The CryptBot botnet specifically focuses on the theft of user information related to authentication, such as credentials, certain computer and browser identifying information, cryptocurrency account information, and other personal information about a computer's user.

32. CryptBot was initially identified in 2019, but made a resurgence in early 2022. While CryptBot has been known to be distributed through the use of phishing emails, the most recent open source intelligence from various security analysts notes that one of CryptBot's primary distribution methods is through websites—such as the Cracked Software Sites—that offer links to cracked software.⁶

⁶ <https://www.bleepingcomputer.com/news/security/revamped-cryptbot-malware-spread-by-pirated-software-sites/>

33. CryptBot is coded, operated, and managed by the CryptBot Defendants. CryptBot leverages multiple distribution methods, but focuses heavily on distribution through cracked software sites generally.

34. CryptBot is designed to automatically identify and steal sensitive information from the computers it infects and then send the stolen data to C2 servers to be harvested and eventually transferred or sold to hackers to use in connection with data breach campaigns. Malicious hackers who target large computer networks will usually incorporate the use of stolen account credentials throughout the course of their hacking campaign. These can be used to gain an initial foothold into an organization's network, or to help a threat actor move laterally within a breached network once they are inside.

35. CryptBot is designed to target the users of a number of specific Internet browsers, including Google Chrome. Once executed, the CryptBot malware checks the infected machine for installation of Google Chrome, and then attempts to locate, collect, and extract user credentials saved to Google Chrome. Additionally, CryptBot is coded to take screenshots and steal data stored by users in Chrome Extensions. The CryptBot Defendants recently released an update to the CryptBot malware specifically designed to overcome certain limitations in its ability to steal information associated with the latest version of Chrome, showing that the botnet's creators have and continue to specifically adapt the malware to target Google Chrome and its users.

36. Today's malicious hacker has online access to a myriad of tools and services to support their nefarious conduct. Typically, a malicious threat actor hacking an organization's network may use a large number of stolen credentials that are purchased from an online illicit marketplace ("Stolen Credential Vendors").

37. Upon information and belief, credentials stolen by the CryptBot malware are primarily monetized through the trafficking of such stolen credentials and other sensitive information (such as social security numbers and credit card information) through Stolen Credential Vendors.

The Cracked Software Sites

38. The Malware Distribution Enterprise leverages the “360installer” PPI service that maintains approximately 161 active domains, each of which is associated with the Cracked Software Sites as part of its distribution network.

39. The Malware Distribution Defendants work together to maintain and support the Cracked Software Sites, which distribute cracked software in order to attract users to their customers’ (the CryptBot Defendants’) download links in return for payment from the CryptBot Defendants as set forth below.

40. Specifically, the Malware Distribution Defendants operate the PPI business known as 360installer as well as its associated bulletproof hosting service, “Offshoric.” As a part of their service model, the Malware Distribution Defendants incentivize the creation of cracked software sites by paying their affiliates a fee for every installation that results from a download from that affiliate’s site. See Declaration of David J. Youssef (“FTI Decl.”) ¶¶ 6-12, 16-24. According to the Malware Distribution Defendants’ 360installer.com website, affiliates are paid \$2 per installation. *Id.* ¶ 17.

41. In order to pay this fee and also turn a profit, the Malware Distribution Defendants work with the CryptBot Defendants, who monetize the installations through the theft and eventual sale of sensitive, stolen information. This criminal activity funds 1) the sustaining operation of the Malware Distribution Defendants’ PPI service and its Cracked Software Sites; 2) the promotion of the PPI service’s affiliates; and 3) creation of additional websites for

maliciously modified software, creating more opportunities for the CryptBot Defendants to spread CryptBot. *Id.* ¶¶ 57-59.

42. The Malware Distribution Defendants and the CryptBot Defendants share and jointly pursue the same goal: profit from the distribution of CryptBot malware through cracked software installation files seeded with malware. The Malware Distribution Defendants maintain the Cracked Software Sites, which use the allure of free and popular software, to sustain an infrastructure that directs Internet traffic to download CryptBot, infecting more computers.

43. Websites such as the Cracked Software Sites are subject to being taken down by legal authorities or private parties pursuant to law enforcement activity, legal process, or cease and desist letters related to violations of intellectual property rights. Accordingly, many such websites are hosted by what are known in the hacking community as “bulletproof” hosters. “Bulletproof” hosters are web hosting services that turn a blind eye to illegal content and will ignore or evade legitimate complaints or legal process to remove or take down the offending content.

44. The Cracked Software Sites are hosted by a number of different web hosting providers, but a majority of these sites are hosted by OffShoric, a “bulletproof” web hosting service owned and operated by the Malware Distribution Enterprise. *Id.* ¶¶ 11, 16, 54.

45. The “About Us” page on OffShoric’s website lists Defendants Saeed and Siddiqui as “Founders” of OffShoric, and has links under the “Trusted Clients” section to a number of Cracked Software Sites that blatantly advertise cracked software.

The Malware Distribution Enterprise Distributes Cracked Google Software and CryptBot

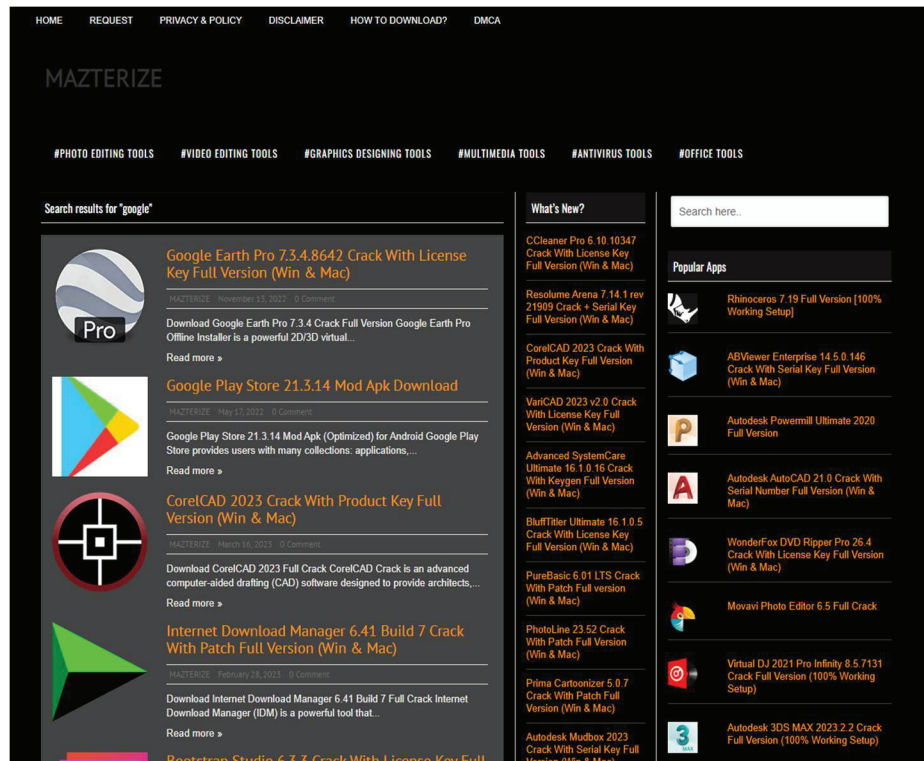
46. The Malware Distribution Enterprise offers maliciously modified versions of Google software to its users.

47. In a number of instances, the Malware Distribution Enterprise follows their usual model of soliciting affiliates to create webpages advertising cracked versions of software that otherwise requires a licensing fee but ultimately delivers malware. In other instances, and in particular with Google products that are otherwise free to users such as Google Earth Pro and Google Chrome, the Malware Distribution Enterprise uses installer packages bearing Google trademarks to deliver malware. Analysis of these software packages reveals that they redirect users to a series of hacker-related infrastructure that assess certain aspects of the computer (e.g., its operating system and browser versions) to identify whether affiliate malware would be effective on the relevant machine. If so, malware is installed on the machine.

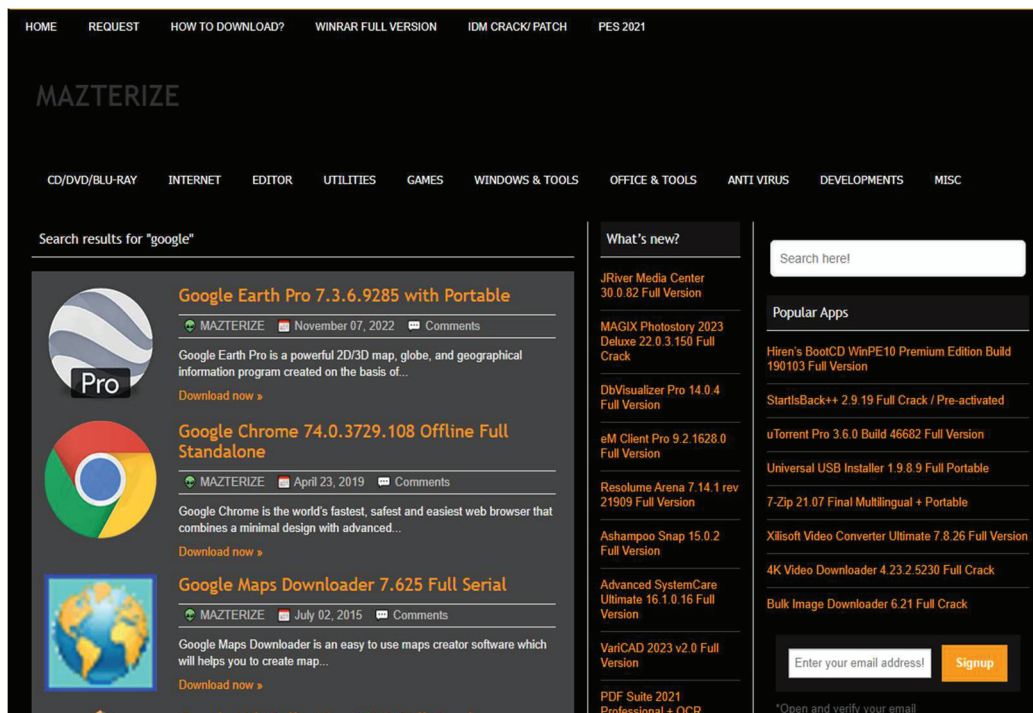
48. Paragraphs 49 through 51 provide some examples of the Cracked Software Sites used by the Malware Distribution Enterprise to distribute CryptBot.

49. “Mazterize.net” is a Cracked Software Site.

a. Below is a screen capture from Mazterize.net:

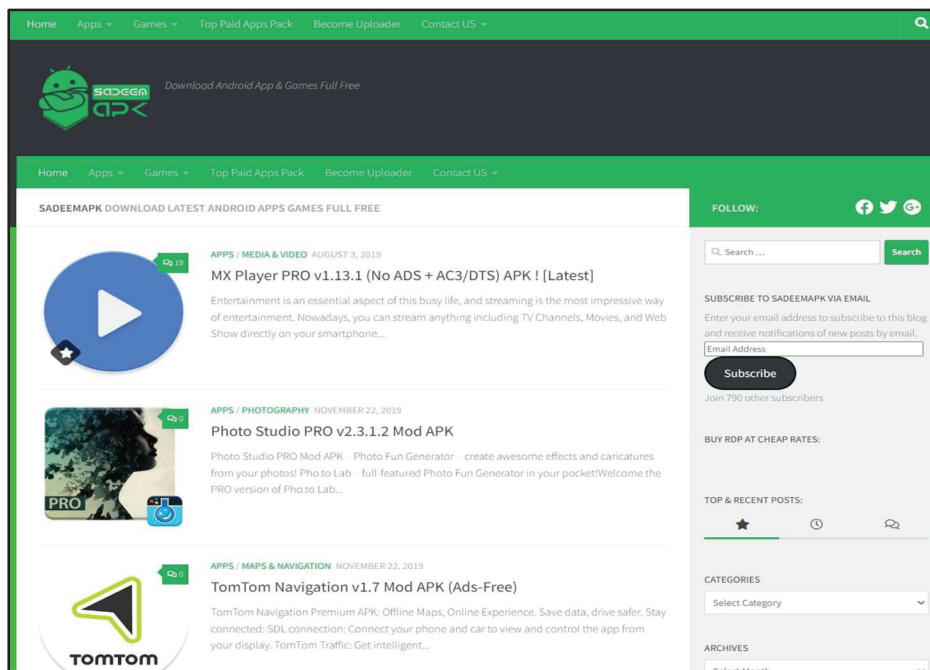


b. “Mazterize.com” is a related site, using the “.com” top-level domain. Below is a screen capture from “Mazterize.com”:



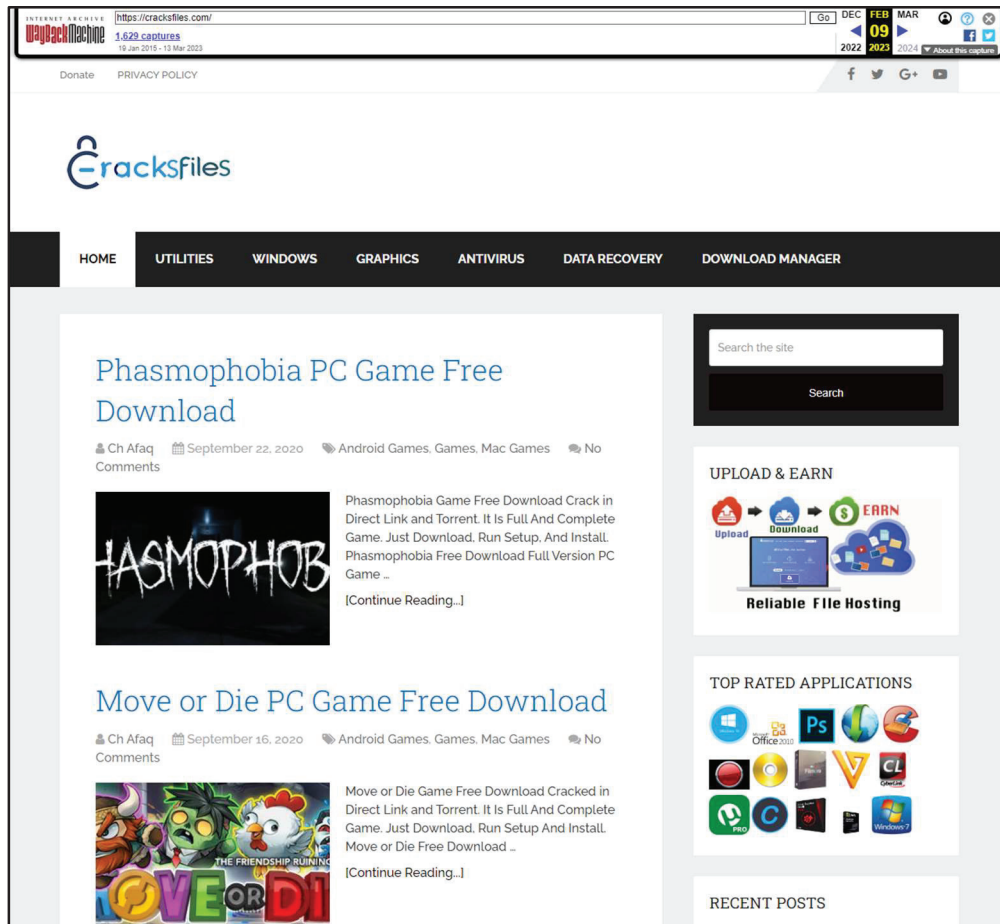
50. “SadeemAPK” is a Cracked Software Site with the domain name sadeemapk.com.

Below is a screen capture from SadeemAPK.



51. “CracksFiles” is a Cracked Software Site with the domain name cracksfiles.com.

Below is a screen capture of CracksFiles from February 2023. As recently as March 1, 2023, the links on the CracksFiles page have been removed.



52. The Malware Distribution Enterprise is a major distribution arm for CryptBot. Of the 161 domains associated with the Cracked Software Sites that were active on March 3, 2023 (the “Active Domains”), approximately 90 are associated with the delivery of malware, and approximately 29 are confirmed to be associated with CryptBot. Additionally, the Cracked Software Sites include an additional 14 inactive domains that have historically been used by the

Malware Distribution Enterprise to distribute CryptBot. All of the Cracked Software Sites listed in paragraphs 49 through 51 have been associated with the distribution of CryptBot malware.

53. While a significant portion of the Active Domains were associated with CryptBot at the time of testing,⁷ the domains associated with both the Cracked Software Sites and CryptBot C2 infrastructure change dynamically. CryptBot is known to be generally distributed through “phishing emails and cracked software,”⁸ and has been described as “one of the most actively-changing malware with distribution pages constantly being distributed.”⁹ Accordingly, at any given point in time, only a portion of the Cracked Software Sites are likely to include installation files that lead to the distribution of CryptBot. This allows both the Malware Distribution Defendants and the CryptBot Defendants to more effectively keep their distribution pages online. As set forth above, CryptBot targets Google users’ information and Google products once it is installed on a machine, and CryptBot has been updated specifically in order to make it more effective against later versions of Google software.

Harm to Google, its Users, and the Public

54. The Malware Distribution Enterprise harms Google, its users, and the public in two distinct, but related ways.

55. First, the Malware Distribution Enterprise relies on attracting users that are willing to click on links that the Cracked Software Sites promote. In doing so the Malware Distribution Enterprise harms the legitimate owners of such software, including Google (in the case of Google Chrome and Google Earth Pro).

⁷ See FTI Decl. ¶ 39.

⁸ <https://any.run/cybersecurity-blog/cryptbot-infostealer-malware-analysis/>

⁹ <https://asec.ahnlab.com/en/31802/>

56. Monetization of the Cracked Software Sites by the Malware Distribution Enterprise ultimately relies on the malicious theft (and sale) of sensitive information, including user credentials, to monetize both the operation of the CryptBot botnet as well as the Cracked Software Sites. As alleged in paragraph 34, although CryptBot is designed to steal information associated with many different browsers and applications, it also specifically targets Google Chrome users. Accordingly, the distribution of CryptBot harms not only Google Chrome users, but tarnishes the product's reputation as a secure browsing platform.

57. The owners of infected devices are harmed in numerous ways, including through the unauthorized access and criminal misuse of their device or information stolen from the same.

58. Beyond Google and Google users, the continued proliferation of malware via the Cracked Software Sites harms the Internet as a whole. Based on an assessment of web traffic associated with the Cracked Software Sites connected to the distribution of CryptBot, these sites alone have led to approximately 672,220 CryptBot infections a year. FTI Decl. ¶ 63. Each infection can lead to the theft of user information that is leveraged in malicious hacking.

CLAIMS FOR RELIEF

CLAIM 1

Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)–(d) as to all Defendants

59. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

60. At all relevant times, Google is a person within the meaning of 18 U.S.C. § 1961(3).

61. At all relevant times, Google is a “person injured in his or her business or property by reason of a violation of” RICO within the meaning of 18 U.S.C. § 1964(c).

62. At all relevant times, each Defendant is a person within the meaning of 18 U.S.C. §§ 1961(3) and 1964(c).

The RICO Enterprise

63. The Defendants are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs of this Complaint; namely, the Malware Distribution Enterprise, which distributes malware through the distribution of illegally cracked software via the Cracked Software Sites.

Pattern of Racketeering Activity and Predicate Acts

64. At all relevant times, the Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the Malware Distribution Enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c), with such conduct and activities affecting interstate and foreign commerce.

65. Defendants have directly or indirectly engaged in an unlawful pattern of racketeering activity involving thousands of RICO predicate offenses, including violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B); wire fraud (18 U.S.C. § 1343); identity fraud (18 U.S.C. § 1028); and access device fraud (18 U.S.C. § 1029).

66. Google was injured in its business and property by reason of the Defendants' violations of 18 U.S.C. § 1962(c), as described herein. These injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Google will continue to be harmed.

67. Under 18 U.S.C. § 1964(c), Google is entitled to recover treble damages plus costs and attorneys' fees from the Defendants.

The Computer Fraud and Abuse Act Predicate Offenses as to all Defendants

68. RICO provides, in 18 U.S.C. § 1961(1)(G), that any act indictable under 18 U.S.C. § 2332b(g)(5)(B) constitutes a RICO predicate act. Among the acts that are indictable under 18 U.S.C. § 2332b(g)(5)(B) are violations of 18 U.S.C. § 1030(a)(5)(A)—a provision of the CFAA—if such violation results in damage as defined in §1030(c)(4)(A)(i)(VI).

69. The Defendants have violated and continue to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), resulting in damage as defined in Section 1030(c)(4)(A)(i)(VI), by knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer.¹⁰

70. As noted above in paragraph 58, the Cracked Software Sites connected to the distribution of CryptBot have led to approximately 672,220 CryptBot infections a year. Each installation of a malicious installer package leading to the installation of CryptBot amounts to multiple transmissions of code intended to cause damage without authorization to a protected computer.

Wire Fraud Predicate Offenses as to all Defendants

71. The Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, commit wire fraud in violation of 18 U.S.C. § 1343 by transmitting or causing to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, and signals for the purpose of executing fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute.

72. The Malware Distribution Enterprise commits wire fraud, in violation of 18 U.S.C. § 1343, each time that it tricks the owner of a device into unknowingly downloading

¹⁰ A “protected computer” includes any computer “used in or affecting interstate or foreign commerce or communication.” 18 U.S.C § 1030 (e)(2).

and installing CryptBot malware on the owner's device through fraud, misrepresentation, and deception, as alleged in paragraphs 38-45.

73. As described in paragraphs 47 and 49, the Malware Distribution Enterprise leverages installer packages for Google Earth Pro and Google Chrome to install malware on unsuspecting users' machines.

74. Google has suffered injury to its business or property as a result of these fraudulent schemes.

Identity Fraud Predicate Offenses as to all Defendants

75. The Defendants, in furtherance of the Malware Distribution Enterprise, commit identity fraud in violation of 18 U.S.C. § 1028(a)(7) by knowingly transferring, possessing, and using, without lawful authority, means of identification of their victims with the intent to commit, or to aid or abet, or in connection with, unlawful activity in violation of state and federal law and affecting interstate commerce.

76. Specifically, as alleged in paragraphs 34-37, the CryptBot Defendants target and steal, among other things, users credentials, in order to traffic in such credentials for profit. Additionally, as alleged in paragraphs 32-42, the CryptBot Defendants' theft of such credentials is aided and abetted by the Malware Distribution Defendants, who help distribute the CryptBot malware used to exfiltrate such sensitive information from victim users.

77. Google has suffered injury to its business or property as a result of these actions.

Access Device Fraud Predicate Offenses as to all Defendants

78. The Defendants, knowingly and with intent to defraud, and in furtherance of the Malware Distribution Enterprise, committed and continue to commit access device fraud in violation of 18 U.S.C. §§ 2 and 1029(a)(2)-(3), by trafficking in or using unauthorized access devices in the form of stolen passwords, credentials, and other account information in order to

obtain anything of value aggregating \$1,000 or more during a one-year period, and/or possessing fifteen or more unauthorized access devices, and affecting interstate or foreign commerce. As previously mentioned, FTI estimates that the Malware Distribution Enterprise is associated with approximately 672,220 infections annually, and each infection is likely to lead to the theft of sensitive information.¹¹ 360installer pays \$2 per installation, so with over hundreds of thousands of infections, the affiliate payments alone are believed to be well in excess of \$1,000 annually. Those affiliate payments are only a portion of the value of the stolen information. Accordingly, and upon information and belief, the stolen information at issue here exceeds \$1,000 per year.

79. Specifically, as alleged in paragraph 34-37, the CryptBot Defendants target and steal “access devices” in the form of stolen credentials from Google Chrome users to traffic these credentials for profit. Additionally, the CryptBot Defendants’ theft of such credentials is aided and abetted by the Malware Distribution Defendants, who help distribute the CryptBot malware used to exfiltrate such sensitive information from victim users.

80. Google has suffered injury to its business or property as a result of these actions, which the Malware Distribution Enterprise uses to carry out its schemes.

Conspiracy to Violate RICO as to all Defendants

81. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

82. Defendants have not undertaken the practices described herein in isolation, but rather as part of a common scheme. In violation of 18 U.S.C. § 1962(d), each Defendant unlawfully, knowingly, and willfully agreed and conspired together with others to violate 18 U.S.C. § 1962(c) as described above, in violation of 18 U.S.C. § 1962(d).

¹¹ This is extrapolated from a three-month period beginning December 1, 2022 to February 28, 2023, in which 168,055 computers were infected.

83. The Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses, and they knew that the predicate offenses were part of such racketeering activity, and their participation and agreement was necessary to allow the commission of this pattern of racketeering activity. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

84. The Malware Distribution Defendants and CryptBot Defendants agreed to participate in, directly or indirectly, the conduct, management, or operation of the Malware Distribution Enterprise's affairs through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). Each Defendant knew about and agreed to facilitate the Malware Distribution Enterprise's schemes. The purpose of the conspiracy was to commit a pattern of racketeering activity in the conduct of the affairs of the Malware Distribution Enterprise, including the acts of racketeering set forth above, specifically, violation of the CFAA, wire fraud, identity fraud, and access device fraud.

85. Google has been and continues to be directly injured by Defendants' conduct. Defendants' conduct undermined the security and reputation of Google's products and services.

86. Google seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

87. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which there is not adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

CLAIM 2

Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 as to all Defendants

88. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

89. As alleged in paragraphs 34-37, Defendants knowingly and with intent to defraud, trafficked and continue to continue to traffic in passwords and/or similar information through which computers may be accessed without authorization. *See* 18 U.S.C. § 1030(a)(6)(A).

90. Defendants' conduct involved and affected, and continue to involve and affect, interstate and/or foreign communications and commerce, including involving protected computers located inside the United States as well as protected computers located outside the United States that are used in a manner that affects interstate or foreign commerce or communication of the United States.

91. Defendants' conduct has caused damage to Google, including by impairing the integrity of products being offered to its users.

92. Defendants' conduct has caused a loss to Google during a one-year period aggregating at least \$5,000.

93. Google seeks injunctive relief and compensatory damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

94. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

CLAIM 3

Trademark Infringement and Counterfeiting in Violation of the Lanham Act, 15 U.S.C. § 1114 as to all Defendants

95. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

96. Defendants use reproductions, counterfeits, copies, or colorable imitations of the Google Marks in interstate commerce in connection with the Malware Distribution Enterprise.

97. Google has not licensed or authorized Defendants to use the Google Marks.

98. Defendants' unauthorized use of the Google Marks is likely to cause confusion and mistake among consumers as to the source, origin, or sponsorship of the maliciously modified Google software made available through the Malware Distribution Enterprise.

99. Defendants' unauthorized use of the Google Marks is also likely to cause confusion and mistake among consumers as to the source, origin, or sponsorship of CryptBot itself, if and when affected users are alerted to the malware on their computers.

100. Defendants unauthorized use or imitation of the Google Marks is a knowing, willful, and intentional violation of Google's rights.

101. Defendants' activities constitute willful trademark infringement and counterfeiting in violation of Sections 32 and 35 of the Lanham Act, 15 U.S.C. §§ 1114 and 1117.

102. Defendants' infringement diminishes the value of the Google Marks and damages Google's goodwill and business reputation.

103. The injuries sustained by Google have been the direct and proximate result of Defendants' wrongful reproduction, counterfeiting, and use of the Google Marks.

104. By reason of the foregoing, Google is entitled to recover actual damages or Defendants' profits, including treble damages pursuant to 15 U.S.C. § 1117(b), statutory damages pursuant to 15 U.S.C. § 1117(c), as well as costs, attorneys' fees under the Lanham Act.

105. As a direct result of Defendants' actions, Google has also suffered irreparable harm for which no adequate remedy at law exists, which will continue unless Defendants' activities are not restrained.

CLAIM 4

False Designation of Origin in Violation of the Lanham Act, 15 U.S.C. § 1125(a), as to all Defendants

106. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

107. Google owns and uses the Google Marks in connection with its offering of software, among other things.

108. Defendants use reproductions, counterfeits, copies, or colorable imitations of the Google Marks in interstate commerce in connection with the Malware Distribution Enterprise.

109. Google has not licensed or authorized Defendants to use the Google Marks.

110. Defendants' unauthorized use of the Google Marks is likely to cause confusion and mistake, as well as to deceive consumers, as to the origin, sponsorship, or affiliation of the cracked software and CryptBot.

111. Defendants unauthorized use or imitation of the Google Marks is a knowing, willful, and intentional violation of Google's rights.

112. Defendant's use of the Google Marks constitutes false designation of origin in violation of Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a).

113. Defendants' infringement diminishes the value of the Google Marks and damages Google's goodwill and business reputation.

114. The injuries sustained by Google have been the direct and proximate result of Defendants' use of the Google Marks, including counterfeits of the same, in order to falsely represent the origin and sponsorship of the maliciously modified software and CryptBot.

115. Google is entitled to recover actual damages or Defendants' profits, including treble damages pursuant to 15 U.S.C. § 1117(b), as well as costs, attorneys' fees, and other statutory damages under the Lanham Act.

116. As a direct result of Defendants' actions, Google has also suffered irreparable harm for which no adequate remedy at law exists, which will continue unless Defendants' activities are not restrained.

CLAIM 5
Tortious Interference with Business Relationship as to all Defendants

117. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

118. Defendants knew or should have known that Google had an actual and continuing business relationship with numerous users who interact with Google's systems and use its products.

119. In violation of the common law of New York, Defendants intentionally and maliciously interfered with Google's business relationships with its users by distributing maliciously modified versions of Google software and targeting Google Chrome and Google Earth Pro users for the installation of malicious software. Defendants' actions were dishonest, unfair, and improper.

120. Defendants' improper actions were the proximate cause of harm to Google and resulted in injury to Google's relationship with its users.

121. Google seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

122. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as set forth below:

- A. Judgment in favor of Google and against Defendants;
- B. A declaration that Defendants have engaged in acts or practices that violate the Racketeer Influenced and Corrupt Organizations Act, Computer Fraud and Abuse Act, and Lanham Act, and they have engaged in tortious interference with business relationships;
- C. A declaration that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression;
- D. A temporary restraining order and preliminary and permanent injunctions enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;
- E. Award of appropriate equitable relief available under applicable statutes and law, including injunctive relief and an accounting of profits;
- F. Judgment awarding Google actual and/or statutory damages from Defendants adequate to compensate Google for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;
- G. Judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial;

- H. Judgment awarding attorneys' fees and costs; and
- I. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Google respectfully requests a trial by jury on all triable issues in accordance with Fed.

R. Civ. P. 38.

Dated: April 20, 2023

Respectfully submitted,

GOOGLE LLC

By: 

PERKINS COIE LLP

Andrew Sun Pak
APak@perkinscoie.com
1155 Avenue of the Americas, 22nd Floor
New York, New York 10036-2711
Tel: +1.212.262.6900
Fax: +1.212.977.1649

Margot Adams (*pro hac vice forthcoming*)
MargotAdams@perkinscoie.com
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Tel: +1.206.359.8000
Fax: +1.206.359.9000

Counsel for Plaintiff Google LLC