Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

Compliance and Enforcement Decision CRTC 2022-132

PDF version

Ottawa, 19 May 2022

File numbers: 9094-201500417-001 and 9094-201500417-002

1882914 Ontario Inc., operating as Datablocks Inc. and 2348149 Ontario Inc., operating as Sunlight Media Networks Inc. – Alleged violations of Canada's Anti-Spam Legislation

The Commission finds that the evidence on the record of this proceeding is not sufficient to conclude that 1882914 Ontario Inc., operating as Datablocks Inc. and 2348149 Ontario Inc., operating as Sunlight Media Networks Inc. aided in seven installations of a computer program on another person's computer system without the express consent of its owner or authorized user. Accordingly, pursuant to section 25 of Canada's Anti-Spam Legislation (CASL), the Commission determines that no violation of section 9 of CASL has been committed and therefore the administrative monetary penalties set out in the notices of violation will not be imposed.

Introduction

1. In 2015, Commission enforcement staff identified five Canadian Internet Protocol (IP) addresses linked to 1882914 Ontario Inc., operating as Datablocks Inc. (Datablocks) and 2348149 Ontario Inc., operating as Sunlight Media Networks Inc. (Sunlight Media) [together, the Companies] that appeared to be redirecting users to webpages hosting exploit kits.[1]

2. Sunlight Media[2] operated an online ad network and served as a broker between advertisers and publishers of such ads. Sunlight Media used Datablocks' software and network routing infrastructure that enable the delivery of online ads through a fully automated digital auction process known as a Real-Time Bidding system.

3. In the course of Commission enforcement staff's extensive investigation, a notice to produce documents (NTP) was issued in June 2016 to Shared Services Canada (SSC) to obtain information and data regarding traffic directed to or from Government of Canada (GC) IP addresses and the five IP addresses of interest. The purpose of the

[1] The Canadian Centre for Cyber Security defines exploits as "malicious code that takes advantage of an unpatched vulnerability. An "exploit kit" is a collection of multiple exploits that affect unsecure software applications. Each exploit kit is customized to search for specific vulnerabilities and execute the corresponding exploit for the vulnerability it finds."

[2] Sunlight Media completed its voluntary dissolution on 16 November 2018.

NTP was also to obtain all network packet capture files (pcap files)[3] and malware samples (pcap samples) related to the five IP addresses of concern.

4. On 9 July 2018, the Chief Compliance and Enforcement Officer (the designated person[4]) issued one notice of violation (NOV) each to Sunlight Media and Datablocks, pursuant to section 22 of the *Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act* (the Act or Canada's Anti-Spam Legislation [CASL]). NOVs may be reviewed independently by the Commission.

5. In the NOVs, the designated person informed the Companies that there were reasonable grounds to believe that between 8 February 2016 and 30 May 2016, the Companies each committed a violation of section 9 of the Act, by aiding, through their acts and omissions, in seven contraventions of subsection 8(1) of the Act, namely the installation, by an unknown person, of a computer program on another person's computer system without express consent.

6. More specifically, the designated person indicated that in seven instances, Sunlight Media's domain provided direct instructions to a GC computer system to connect to a server, which in turn installed a malicious computer program on the GC computer system without express consent.

7. The designated person also concluded that Datablocks provided the software and infrastructure to Sunlight Media that enabled Sunlight Media's clients to participate in the Real-Time Bidding process.

8. The NOVs, which were each accompanied by the designated person's investigation report and the evidence gathered during the investigation, set out an administrative monetary penalty (the penalty) of $150,000 for Sunlight Media and $100,000 for Datablocks.

9. In their joint representations dated 24 September 2018, the Companies argued, among other things, that the investigation report and the evidence provided to support the designated person's findings did not demonstrate that the Companies had committed any violation of the Act. The Companies also submitted an expert report they commissioned. Based on that report, the Companies argued that the technical analysis and digital evidence on the record did not prove the alleged installations, by an unknown person, of malicious computer programs.

---

[3] Pcap files refer to the interception of data packets as they are moving over a computer network over a given period of time.

[4] Under section 14 of the *Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, the Commission can designate persons to exercise powers related to the purposes of sections 15 to 46, which includes the issuance of notices of violation.

10. In 2019, the Commission contracted with an external computer forensics expert (the external specialist) to help the Commission better understand the technical arguments and digital evidence included on the record of this proceeding (the external forensics report), independently of the evidence submitted by the designated person and the Companies.

11. In a letter dated 18 August 2020, the Commission added the external forensics report to the record of the review proceeding and provided an opportunity to the designated person to comment on matters noted in the external forensics report, while also providing the Companies with an opportunity to comment on the designated person's comments and on the external forensics report.

12. In a subsequent letter dated 22 December 2020, the Commission clarified that comments were to be limited to the methodology and tools used by the external specialist to assess the digital evidence, as well as the technical findings and conclusions based on that evidence.[5]

13. In addition to the procedural letters mentioned above, the record of this proceeding includes the following:

    - the NOVs issued to the Companies on 9 July 2018;
    - an investigation report setting out the designated person's evidence, analysis, and findings in support of the NOVs;
    - the joint representations made by the Companies on 24 September 2018 in response to the NOVs that included an expert report;
    - the external forensics report contracted by the Commission; and
    - the designated person's comments on the external forensics report and the Companies' comments on both the report and the designated person's comments.

14. The record closed on 16 February 2021.

15. Pursuant to section 25 of the Act, if a person makes representations in accordance with a NOV, the Commission must decide, on a balance of probabilities, whether the person committed the violation, and if so, whether to impose, reduce, waive, or suspend the penalty, subject to any conditions it considers necessary to ensure compliance.

[5] The Commission took into consideration those limitations when it reviewed the submissions from the Companies and the designated person in response to that letter and in its analysis and conclusions in this decision.

Issue

16. The Commission has identified the following issue to be addressed:

    - Does the record support the findings in the NOVs that the Companies aided, in contravention of section 9 of the Act, with the commission of acts contrary to subsection 8(1) of the Act, namely the installation of a computer program?

17. In order for the Commission to come to a conclusion on any section 9 contravention, it must first determine whether any of the seven installations of a computer program occurred contrary to subsection 8(1) of the Act. Should the Commission fail to find, on a balance of probabilities, that a computer program was installed, it would not be possible to find that the Companies violated section 9 of the Act.

18. Furthermore, prior to determining whether a computer program was installed, the Commission must establish whether Shockwave Flash Files constitute "computer programs" within the meaning of subsection 1(1) of the Act. The meaning of "installation" in the context of the phrase "installation of a computer program" set out in subsection 8(1) of the Act must also be determined in the specific circumstances of this review proceeding, since the Act does not provide a definition for "install" or "installation."

Alleged computer programs listed in the NOVs

19. The Commission notes that the term "computer program" is defined at subsection 1(1) of the Act as having the same meaning as in subsection 342.1(2) of the *Criminal Code*, which defines it as

    > computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

20. Furthermore, the terms "data" and "computer system" found in that definition of computer program are also defined in subsection 1(1) of the Act. More specifically, data is defined as

    > signs, signals, symbols or concepts that are being prepared or have been prepared in a form suitable for use in a computer system.

21. As for "computer system," the Act indicates that it has the same meaning as in subsection 342.1(2) of the *Criminal Code*, which defines it as

    > a device that, or a group of interconnected or related devices one or more of which, contains computer programs or other computer data, and by means of computer programs, (i) performs logic and control, and (ii) may perform any other function.

22. As for the computer programs at the heart of this proceeding, the designated person claims that the Companies aided in installing Shockwave Flash Files embedded with Flash exploit programs.

23. The Commission notes that Shockwave Flash Files are comprised of signs, symbols, and concepts that are being prepared in a form suitable for use in a computer system to bring animated graphics, video, sound, and user interactions to the Web. More specifically, they are created from computer code, which are signs and symbols that represent instructions or statements that, when interpreted by a web browser plugin or other compatible software such as Adobe Flash Player will display the content of the Shockwave Flash Files.

24. The Commission further notes that both the designated person and the Companies acknowledged that Shockwave Flash Files are made of computer data/code meant to be operated or read by a web browser plugin or other compatible software, all of which, the Commission considers, aligns with the definition of "computer program" referred to under the Act.

25. Accordingly, both Shockwave Flash Files and Flash exploit programs (embedded in Shockwave Flash Files) constitute, in the context of this review proceeding, computer programs.

Definition of "installation" for the purpose of this proceeding

26. As noted earlier, the Act does not define "installation," which resulted in the designated person and the Companies each providing their own definition.

27. The Commission notes that the Companies indicated that there is no conclusive definition of the terms "install" or "software installation" in the software industry, but that it generally means to make software ready for execution. The Companies also submitted that installation can be as complex as running an installation program for a software suite or as simple as copying a file either in the memory or on the hard drive of a computer system.

28. The Commission also notes that multiple definitions of "installation" can be found in the investigation report. In Appendix 1 of the report, it is defined as

> the act of making a computer program ready for execution by a computer system processing unit. The installation process may vary but at a minimum, installation involves providing the computer program instructions to the computer system. These instructions are typically in the form of machine code being copied or generated. Installation of a computer program does not necessarily require an actual file stored in a persistent manner on a computer hard-drive.

29. In Appendix 9 of the investigation report, it is stated that

> the installation may be performed by silently placing machine code on a computer's hard-drive or Random Access Memory (RAM) without the user's consent or notice. From there, a program is subsequently executed, for example, by the user's web browser.

30. The Commission further notes that common elements were submitted in each definition and both the designated person and the Companies acknowledged that

    - installation requires that the computer program be made ready for execution; and
    - installation of a computer program may be performed silently by copying or placing files or codes on a computer's RAM (i.e., temporary memory) or hard-drive (i.e., permanent memory).

31. In the absence of a definition of "installation" under the Act, the Commission considers that the term should be interpreted in its grammatical and ordinary sense, consistent with the objectives of the Act.

32. In light of the representations and arguments submitted by both the Companies and the designated person, and when considering the record and the facts specific to the review at hand, the following definition of "installation" is to be used to determine, for the purpose of this proceeding, whether the record demonstrates, on the balance of probabilities, that a computer program was installed

    > to make a computer program ready for execution by copying or placing computer codes on a computer system's RAM or hard-drive.

33. The Commission notes that the terms "computer system" and "computer program" in this definition have the same meaning as under the Act.[6]

34. The designated person's proposed definition specifically used the term "machine codes" rather than "computer data" or "computer codes" without providing additional justification. The Commission notes that the term "machine codes" has a limited scope as it only applies to binary files, such as executable (.exe) files for Windows, that are ready to be sent to the computer's processor, or hardware, by the operating system. The Commission considers that the use of the term "computer codes" in the definition above is broader since it encompasses programming languages that are read by software, such as a web browser or a plug-in. This better reflects the broad wording and purpose of the Act and does not restrain the definition to one specific scenario, as would be the case if the Commission was to use the term "machine codes."

Were computer programs installed, without express consent, on GC computer systems?

35. The Commission notes that following the analysis of the pcap samples acquired from SSC in response to the NTP, the designated person concluded that seven computer programs were installed on GC computer systems between 8 February and 30 May 2016. The designated person did not claim that the Companies installed the computer programs themselves, but rather aided unknown person(s) in installing the seven computer programs without the computer program's owner or its authorized user's express consent.

---

[6] The definition of computer system under subsection 342.1(2) of the *Criminal Code* is broad and does not only include individual devices, but also a group of interconnected or related devices.

36. According to the designated person, the digital evidence confirmed that the GC computer systems visited landing pages hosting Angler exploit kits, a specific type of exploit kit, which sent back Flash exploit programs to take advantage of a vulnerability found in the computer systems' version of Adobe Flash Player.

37. Based on the analysis of the digital evidence on the record, the designated person determined that Flash exploit programs were successfully installed, resulting in the GC computer systems subsequently downloading second programs. According to the designated person, these second programs are the exploit kits' "payload,"[7] which targeted the computer systems' Adobe Flash Player.

38. Additionally, for each pcap sample where the GC computer system downloaded a second program, the designated person submitted that it was impossible to tell what the secondary payload was or to see any post-infection indicators, because the pcap session capturing the network traffic ended following the downloading of the second program.

39. The designated person further submitted that the physical GC computer systems were not available for examination of post-infection indicators because compromised computers are usually reimaged (i.e., cleaned by being restored to a previous state) fewer than three days following infection. It was therefore impossible for the designated person to identify the precise nature of the payload.

40. The Companies argued that the investigation report failed to demonstrate that any programs were installed on the GC computer systems without express consent. They argued that the evidence on the record relates to the loading of the Shockwave Flash Files onto the GC computer systems, not the installation.

41. The Companies argued that it is not possible to determine, based on the digital evidence on the record, whether the Shockwave Flash Files were executed or whether they caused other programs to be loaded on the GC computer systems, because Commission enforcement staff failed to collect the digital forensics evidence required to make that determination.

42. The Angler exploit kit consists of a series of stages, and the Companies submitted that there is insufficient evidence to conclude that any stage beyond the first one was successful. The Companies argued that a successful compromise of the GC computer systems, as claimed in the investigation report, would entail successful installation and execution of the subsequent stages.

[7] The designated person indicated that the term "payload" refers to malware for the purpose of the investigation. However, the term "payload" more generally refers to the data being transported by packets over a network, and that data is not necessarily malicious.

43. The Companies submitted that the evidence on the record does not prove that the Shockwave Flash Files listed in the NOV were executed, which would have caused secondary files to be installed. Rather, the Companies argued that the evidence simply shows that those secondary files were requested for download.

44. The Companies submitted that since the type of data in some of the samples could not be confirmed, it is incorrect to label that data as being a “program” or a “payload.”

45. The Companies submitted that the conclusion that the compromise was successful on some GC computer systems, in the investigation report, is not valid since the evidence necessary to determine whether subsequent stages of the exploit kit were installed or executed would reside on the GC computer systems and those computer systems were not collected during the investigation.

46. The Companies also submitted that Commission enforcement staff should have collected a copy of the memory of the GC computer systems while they were believed to have been infected, and complete forensic copies of the hard drives of infected computers. This would have allowed Commission enforcement staff to obtain key data, such as the configuration settings of the computer systems that may have been changed by the malware and saved to the hard drive, a history of programs that were executed, a history of websites connected to by the browser, and the programs that sent and/or received network data.

47. The Companies argued that Commission enforcement staff should have collected complete pcap files showing all network traffic to and from the infected computers before, during, and after the time of infection.

48. The Companies also argued that the NTP addressed to SSC did not request all the relevant networking traffic. Instead, it only requested information and/or data, pcap files, and malware samples related to the five IP addresses belonging to the Companies.

49. The external specialist submitted, with regard to the installation of computer programs on GC computer systems, that it was not possible to conclude whether these computer programs were installed (i.e., made ready to execute), or whether any vulnerabilities were exploited or caused other malicious code to be fetched, installed, and executed, because the required digital forensics evidence from the computer systems under discussion were not available for examination, study, and analysis to draw that conclusion.

50. The designated person disputed some of the external specialist’s findings, while also recognizing that the best source of evidence would have been the compromised computers. However, the designated person submitted that access to such computers is not necessary as the pcap samples demonstrated that the Flash exploit programs were made ready for execution by the mere fact that they were fetched and transmitted to the computer systems.

51. In their comments on the external forensics report, the Companies agreed with the majority of the observations and findings from the external assessment. The Companies submitted that the external forensics report confirms that the digital evidence was both flawed and incomplete and that the investigation report provides insufficient evidence to prove that any programs were installed. The Companies also added that, at best, the technical evidence in the investigation report shows that an unknown party may have attempted to install malware.

Commission's analysis and determinations

52. Subsection 8(1) of the Act states that

> a person must not, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system […] unless (a) the person has obtained the express consent of the owner or an authorized user of the computer system and complies with subsection 11(5) or (b) the person is acting in accordance with a court order.

53. The Commission notes that subsection 8(1) of the Act refers to the installation of a computer program, not an attempt to install one. If the intent of Parliament in writing the Act had been to cover attempts to install, it likely would have included that language in subsection 8(1) of the Act. Furthermore, contrary to certain arguments made on the record, the issue is not necessarily about the infection, or compromise, of a computer system, since those actions or consequences are not referred to in the Act. The question is whether there is sufficient evidence on the record of the proceeding to conclude, on a balance of probabilities, that the Shockwave Flash Files listed in the NOVs were installed.

54. In the Commission's view, getting access to a forensic copy of the memory of the GC computer systems at the time they were believed to have been infected would have been helpful in demonstrating that the Shockwave Flash Files were copied or placed on the computer's RAM or hard-drive. In its comments on the external forensics report, the designated person recognized that the physical computers would have provided the best source of evidence. The Companies' expert and the external specialist also came to a similar conclusion as the designated person.

55. While there is no indication on the record that a request was made to SSC during the investigation to access the computer system that might have been compromised, the Commission appreciates that gaining physical access to computers systems days, if not weeks, after they might have potentially been compromised is not always feasible or practical. That is especially true when computers may be reimaged after a certain amount of time. The Commission is not suggesting that without access to such evidence, proving violations of subsection 8(1) of the Act would not be possible.

56. However, as a result of not having access to the computers, the central element of the investigation report's conclusions about the installation of the Shockwave Flash Files was mostly the result of the technical analysis of pcap samples provided by SSC,

which, in this case, only demonstrate what happened over a given period of time on a specific part of the GC network traffic. Accordingly, the conclusions that can be drawn from the analysis of these pcap samples are indirect, and do not by themselves specify if, or where, the computer programs were installed.

57. Since pcap samples are a snapshot of travelling data packets over a given period of time, they allow for the observation and analysis of data travelling on a network between hosts. However, a pcap sample does not demonstrate what happens at the endpoint. The Commission notes that this observation was supported by the Companies' expert, as well as the external specialist, both of whom indicated that the digital evidence provided in support of the NOVs is insufficient to prove whether installation actually occurred.

58. While the pcap samples examined by the Commission's enforcement staff do confirm that packets containing Shockwave Flash Files traveled over the GC network at some point, they do not confirm that the Shockwave Flash Files present in the packets were ultimately installed (i.e., copied or placed on the GC computer systems' RAM or hard-drives).

59. The Commission considers that while it is likely possible for a pcap sample to contain sufficient information to demonstrate the exchange and receipt of data between computers, the specific pcap samples on the record of the proceeding did not provide that level of detailed information. More specifically, it appears that the filtering[8] of these pcap samples limited the amount of information provided, including the information needed to demonstrate whether all steps to have a program retrieved, and consequently installed, were indeed completed.

60. The Commission notes that the designated person's comments on the external forensics report address the issue of the limited conclusions that can be drawn through the analysis of the pcap samples. The designated person submitted that the status code "200 OK" in the pcap samples was sufficient proof that the Flash exploit programs were installed when they were downloaded and received, even if they were not yet executed.

61. However, the Commission notes that the "200 OK" response from the server indicates that the browser's request has been successfully received, and that a response is being transmitted back. It does not indicate that the data and/or computer program itself was successfully received (i.e., installed but not yet executed) by the browser.

62. The Hypertext Transfer Protocol (HTTP) response from the client computer that would have indicated that the computer program was indeed received would have come in the form of an acknowledgement (ACK) response to the server, as opposed to the "200 OK" response from the server. However, the investigation report and the designated person's comments on the external forensics report are silent as to whether the client computer acknowledged, via an ACK response, receipt of the computer

[8] Different filters can be used when capturing data packets on computer networks, such as IP filters.

program. In the absence of such an ACK response, it appears to the Commission that installation of the Flash exploit program was inferred by the designated person and not necessarily supported by clear evidence on the record.

63. The Commission notes that the investigation report attempts to further demonstrate the installation of the Shockwave Flash Files by claiming, based on the analysis of the pcap samples, that they were executed on GC computer systems.

64. According to the investigation report, the proof that these Shockwave Flash Files were not just merely made ready for execution but were actually executed (and therefore clearly installed) resides in the fact that a second program was allegedly retrieved, which the designated person referred to as the payload or malware in the investigation report.

65. The Commission considers there are several issues with that conclusion, including the fact that two of the seven pcap samples do not demonstrate that a second program was downloaded. More specifically, in one instance, a download of a second program was attempted but was unsuccessful, while another pcap sample demonstrates that there was no attempt to download a second program.

66. The Commission also notes that part of the designated person's rationale is that Shockwave Flash Files must have been installed since those Shockwave Flash Files retrieved what the designated person referred to as a payload. However, there is no in-depth malware analysis on the record demonstrating that the Shockwave Flash Files contained malicious codes (i.e., instructions), or that those instructions were executed in order to fetch a second program.

67. The Commission further considers that it is more likely that it was the browser, rather than the Shockwave Flash Files, that caused the second program to be fetched. The Commission notes that the common practice is for browsers to fetch data for any resource a webpage lists as being necessary for proper display of the page (such as images, code, etc.). These types of requests do not automatically originate from the Shockwave Flash Files. Finally, while those second programs were identified as malware in the investigation report, this claim was not supported by any malware analysis of the second programs.

68. The Commission would have been more inclined to consider the analysis of the pcap samples on the record to infer installation, as the designated person did, if the inference had been supported by other evidence. For example, a security incident report could have been submitted to demonstrate that the GC's information technology (IT) security posture did not stop the computer programs before they were installed, or an affidavit from SSC employees could have been submitted confirming that the Shockwave Flash Files had been found on the hard-drives, and therefore the hard-drives had to be reimaged.

69. The absence of such supporting evidence allows for other plausible and conceivable explanations as to what happened to the computer programs. For example, the computer programs could have been detected by GC's IT security posture. Considering that the record indicates that the GC computer systems have a hardened IT security posture, the Commission notes that it is plausible that the Shockwave Flash Files would have been blocked before they reached the GC computer systems' RAM or hard-drives and had an opportunity to be installed on these.

Conclusion

70. The Commission appreciates the level of complexity of the investigation that resulted in the issuance of NOVs to the Companies. The Commission also does not question the decision by Commission enforcement staff to initiate an investigation into IP addresses linked to the Companies. The Commission also does not suggest that the designated person's views on the possible installation of Shockwave Flash Files on the GC's computer systems are without any merit.

71. However, the Commission finds that the evidence on the record is not sufficient to conclude on a balance of probabilities, that the seven Shockwave Flash Files were installed, meaning copied or placed on the GC computer systems' RAM or hard-drive. Such installations would have been in contravention of subsection 8(1) of the Act.

72. Given these findings, there is no need to consider whether the record demonstrates that the Companies committed violations of section 9 of the Act.

73. Therefore, the Commission determines that the Companies did not commit violations of section 9 of the Act by aiding in the commission of an act contrary to subsection 8(1) of the Act, namely the installation of a computer program. Accordingly, the administrative monetary penalties set out in the NOVs will not be imposed.

Secretary General