IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KEEPER SECURITY, INC., Plaintiff, v. DAN GOODIN and ADVANCE MAGAZINE PUBLISHERS INC. d/b/a CONDÉ NAST and ARS TECHNICA, Defendants.	Civil Action No. 17-cv-9117 **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff Keeper Security, Inc. ("Keeper"), for its complaint against Defendants Dan Goodin ("Goodin") and Advance Magazine Publishers Inc. d/b/a Condé Nast and Ars Technica ("Ars Technica") (collectively the "Defendants"), alleges the following:

Summary Of The Claims

1. On December 15, 2017, the ARS Technica website made false and misleading statements about the Keeper software application suggesting that it had a 16-month old bug that allowed sites to steal user passwords. The article contained numerous false and misleading statements. Ars Technica has revised the article twice, but to date has failed to remove the false statements. Keeper now asserts claims for defamation, violation of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS 510/2, and commercial disparagement under Illinois law.

The Parties

2. Keeper Security, Inc. is an Illinois corporation having its principal place of business at 850 West Jackson Boulevard, Suite 500, Chicago, Illinois 60607.

3. Keeper is in the business of software security. Keeper creates one of the world's most downloaded password management and digital vault software for mobile devices and computers.

4. Keeper sells and manages a software product called "Keeper® Password Manager & Digital Vault" for managing user passwords and other private information. It may be preinstalled on a device (such as a smartphone, tablet or computer) or it can be downloaded from an Internet site or App store. Keeper protects its users against hackers through its secure and convenient password manager. The passwords, logins, credit card numbers, bank accounts and other personal information are saved in a private digital vault that is encrypted and highly protected. The Keeper software operates as a native software application on Smartphones, Tablets and Computers, with separate components (which must be separately installed and logged into by the user) such as the Keeper Browser Extension.

5. Keeper also offers a Browser Extension, which requires discretionary, manual installation by a user. The Browser Extension allows users to auto-fill login credentials (namely a user name and password) into websites for access.

6. A user can log into the preinstalled Keeper application, which directs users to download and install a separate application, namely the Keeper Browser Extension.

7. Keeper is an innovator and leader of password management software in the United States with several million registered users and thousands of business customers. Keeper software is published in 21 languages and is sold in over 100 countries.

8. The Keeper product is available over the Internet and in various "App" stores including Apple's App store, Google Play store and Microsoft App Store. The Keeper product has received thousands of five-star reviews on the App stores.

9. Keeper has contracts with its users whereby a user pays an annual subscription fee for use of the Keeper Password Manager & Digital Vault software. Keeper fully expects that it will retain the users for several years. The users of Keeper's product rely on the integrity of the Keeper product, as well as, the reputation of Keeper in deciding to enter and renew annual subscriptions with Keeper.

10. Ars Technica is the name of an online magazine that provides technology news, analysis and other information, through the website arstechnica.com.

11. Defendant Dan Goodin is an individual who resides permanently in the San Francisco area of California, and is a citizen of California. Goodin is the Security Editor at Ars Technica, where he oversees coverage of malware, computer espionage and hardware hacking.

12. "Ars Technica" and "Condé Nast" are assumed names of Defendant Advance Magazine Publishers Inc., which owns and operates the Ars Technica website and online magazine, and numerous other publications under the Condé Nast umbrella.

13. Defendant Advance Magazine Publishers Inc. is a corporation formed in the State of New York with its principal place of business at One World Trade Center, New York, New York, 10007. It also is registered to do business in the State of Illinois and has a registered agent located at 801 Adlai Stevenson Drive, Springfield, Illinois 62703.

14. Ars Technica has offices in Chicago, Illinois.

15. Goodin and Ars Technica are responsible for publishing the Article at issue in this action.

Jurisdiction and Venue

16. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332. Keeper is a citizen of the State of Illinois. Goodin is a citizen of the State of California. Ars Technica is a citizen of the State of New York. Keeper claims damages in this action that exceed $75,000.

17. Goodin and Ars Technica are subject to personal jurisdiction under the Illinois long-arm statute, 735 ILCS 5/2-209, for the reasons alleged herein including the commission of a tortious act within Illinois.

18. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) for the reasons alleged herein, including that a substantial part of the events giving rise to the claim occurred in this judicial district.

Background Facts

19. Ars Technica owns and operates an online publication on the Internet website www.arstechnica.com ("the "Ars Technica website").

20. The Ars Technica website publishes articles in technology, computer science, software and computer hardware.

21. The Ars Technica website operates under the Condé Nast umbrella of public websites. Ars Technica has an extensive readership (millions of unique visitors per month) within the technology industry throughout the United States and in Illinois.

22. The Ars Technica website provides public access to articles about software and computer applications. The Ars Technica website is directed to residents throughout the United States, including residents of Illinois. The Ars Technica website is widely followed by residents of Illinois.

23. Condé Nast touts itself as "attracting more than 120 million consumers across its industry-leading print, digital and video brands, the company portfolio includes some of the most iconic media: …Ars Technica…."

24. Goodin and Ars Technica published the Article at issue in this action knowing and intending that that it would be read by residents of Illinois, and knowing and intending that the Article would cause injury to Keeper, an Illinois company.

25. On December 15, 2017, the Ars Technica website published an article by Goodin titled: "Microsoft is forcing users to install a critically flawed password manager: Win 10 version of Keeper has a 16-month old bug allowing sites to steal passwords" (the "Article"). A copy of the Article in its original form is attached as Exhibit 1.

26. The Article was originally published at the following URL: *https://arstechnica.com/information-technology/2017/12/microsoft-is-forcing-users-to-install-a-critically-flawed-password-manager/.*

27. According to the byline associated with the Article, Goodwin wrote, edited and assisted in publishing the Article: "Dan Goodin: Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News and other Publications."

28. The readership of the Ars Technica website (and the intended audience of the Article) includes vendors, investors, customers and partner companies of Keeper, a fact known by Goodin and Ars Technica at the time of the publication.

29. The Ars Technica website claims that "Ars has been building a real on-line community since its founding in 1998." It further touts that it is "one of the Internet's true treasure troves, and one of the largest, documented community databases of tips, technical help, and camaraderie on the planet."

30. The Article published by Goodin and Ars Technica makes several knowingly false and misleading statements about Keeper, its employees and its product(s). The following quotations are examples of the false and misleading statements made in the Article:

1) "Microsoft is forcing users to install a critically flawed password manager."

2) "Win 10 Version of Keeper has 16-month-old bug allowing sites to steal passwords";

3) "Microsoft is quietly forcing some Windows 10 computers to install a password manager that contains a critical vulnerability almost identical to one disclosed 16 months ago that allows websites to steal passwords…";

4) "…quietly forced…";

5) "…unwanted app…";

6) "…allowing any website to steal any password…";

7) "Fortunately, Windows 10 users aren't vulnerable unless they open Keeper and begin trusting it with their passwords."

8) "Still, the incident raises questions about the security vetting Microsoft gives to apps it bundles with Windows."

9) "If an outsider can find a 16-month-old vulnerability so quickly and easily, it stands to reason people inside the software company should have found it long ago."

10) "It's possible Microsoft has a process in place for ensuring the security of third-party apps that get installed on Windows 10 machines and that somehow the Keeper vulnerability slipped through anyway."

11) "It's also possible third-party apps don't come with the same security assurances of other Microsoft software."

31. Goodin knew these statements were false. Goodin failed to speak with Keeper, and failed to verify his facts with Keeper or Microsoft, before publishing the Article.

32. Furthermore, the Article omitted several important facts about the subject of the Article. Among other things, the Article misled users of any computer running Microsoft Windows 10, who were led to believe that they were infected simply by having the Keeper software application installed on their device(s).

33. There has been no reported or actual security breach or loss of customer information in connection with the subject of the Article.

34. The goal, and result, of the Article was to injure Keeper and its employees, and disparage Keeper's products.

35. Keeper contacted Goodin on December 15, 2017 to inform him that the Article contained false and misleading statements and omissions regarding Keeper and its software. Keeper further informed Goodin that the Article placed Keeper's "relationships with vendors and customers" at risk.

36. Keeper provided a written list of the false and misleading statements and omissions in the Article and described how the Defendants "twisted facts, mischaracterized several issues and sensationalized the Article with a defamatory headline (and sub-headline) to destroy [Keeper]."

37. Goodin and Ars Technica revised and republished the Article, but failed to correct the false and misleading statements and omissions made in the Article.

38. The revised Article contained false and misleading statements, including those quoted below:

1) "Microsoft forced users to install a password manager with a critical flaw";

2) "Win 10 version of Keeper had bug allowing sites to steal passwords."

3) "For almost two weeks, Microsoft quietly forced some Windows 10 computer systems to install a password manager with a browser plugin that contained a critical vulnerability almost identical to one disclosed 16 months ago that allows websites to steal passwords…"

4) "…the non-bundled version of the Keeper browser plugin 16 months ago that posed the same threat."

5) "It's possible Microsoft has a process in place for ensuring the security of third-party apps that get installed on Windows 10 machines and that somehow the Keeper vulnerability slipped through anyway."

6) "It's also possible third-party apps don't come with the same security assurances of other Microsoft software."

7) "If an outsider can find a bug similar to the 16-month-old vulnerability so quickly and easily, it stands to reason people inside the software company should have found it long ago."; and

8) "Fortunately, Windows 10 users wouldn't have been vulnerable unless they opened Keeper, registered an account (or logged in if he or she had an existing account), installed the browser plugin and visited a malicious website."

A copy of the first revised version of the Article is attached as Exhibit 2.

39. Later, the Article was further revised without addressing the false and misleading statements, for example those quoted below:

1) "For 8 days Windows bundled a password manager with a critical plugin flaw."

2) "plugin for Win 10 Version of Keeper had bug allowing sites to steal passwords."

3) "For about eight days, some versions of Windows 10 quietly bundled a password manager that contained a critical vulnerability in its browser plug in, a researcher said Friday."

4) "If an outsider can find a bug similar to the 16-month-old vulnerability so quickly and easily, it stands to reason people inside the software company should have found it first."

5) "It's also possible third-party apps don't come with the same security assurances of other Microsoft software."

A copy of the third and most recent version of the Article is attached as Exhibit 3.

40. All versions of the Article also omitted material facts about the purported "vulnerability" that was its subject. Before any such "vulnerability" could have any chance to impact a user, the user would have to be subject to specific conditions and take the following steps: (1) the user would have to separately install the Keeper Browser Extension; then (2) sign into the Keeper Browser Extension (which requires the user to first have a registered Keeper account); then (3) create and store (or have existing and previously created) website login credentials inside their Keeper Vault; then (4) visit a malicious website set up to steal a user's website login credentials; then (5) the malicious website would have to inject a specific type of malware into the Keeper Browser Extension. This omission from all versions of the Article was

material because without this relevant information, readers were misled to believe that their computers were infected simply by having Keeper software installed on their devices.

41. The purported "bug" referred to in all versions of the Article was specifically related to Keeper's Browser Extension which is not "bundled" or "preloaded"; it is a separate application that must be separately installed and registered by a user.

42. Goodin and Ars Technica knew that the Keeper Browser Extension is not bundled or preloaded, yet continued to publish the knowingly false and misleading information. Goodin and Ars Technica also knew of the other falsehoods and omissions contained in the Article, but refused to change or retract the Article.

43. Goodin and Ars Technica wrote, published and disseminated all versions of the Article knowing that statements contained therein were false, and acted in reckless disregard for the truth or falsity of the statements.

44. The Article was intended to and did cause harm to Keeper.

45. The false and misleading statements in the Article have since been republished by third parties on other websites, further injuring Keeper.

Claims for Relief

Count I
(Defamation)

46. Keeper repeats and realleges the allegations in Paragraphs 1 through 45 above.

47. Defendants published an Article titled "Microsoft Is Forcing Users To Install A Critically Flawed Password Manager" on December 15, 2017.

48. Defendants subsequently published other versions of the Article.

49. All versions of the Article contained knowingly false and misleading statements about Keeper, its software and its employees.

50. All versions of the Article were published to third parties.

51. Publication of the Article and the revisions has caused damage to Keeper.

52. The Article and all revisions were published with false and defamatory statements, with knowledge of the falsity, and with reckless disregard of whether the statements were true or false.

53. As a result of the false and defamatory statements in all versions of the Article published by Defendants, Keeper has suffered damages to its business, its stakeholder relationships and other damages which will be proven at trial, in an amount that exceeds $75,000.

Count II
(Uniform Deceptive Trade Practices Act)

54. Keeper repeats and realleges the allegations in Paragraphs 1 through 53 above.

55. Under 815 ILCS 510/2(a)(8): "A person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation, the person . . . disparages the goods, services, or business of another by false or misleading representation of fact."

56. Defendants wrote, published and disseminated all versions of the Article in the course of their business. The statements made in all versions of the Article are false and misleading representations of fact that disparage the products, services and business of Keeper.

Count III
(Commercial Disparagement)

57. Keeper repeats and realleges the allegations in Paragraphs 1 through 56 above.

58. Defendants made statements in all versions of the Article impugning the quality of the Keeper software product and other aspects of the Keeper services.

59. Defendants made false and demeaning statements regarding the quality of Keeper's products and services in all versions of the Article.

60. All versions of the Article falsely criticized the quality of Keeper's products and services.

61. Keeper suffered damages as a direct result of Defendants' actions.

Request for Relief

WHEREFORE, Keeper requests that this Court:

A. Enter a judgment in favor of Keeper against Goodin and Ars Technica on Counts I through III;

B. Award damages in favor of Keeper against Goodin and Ars Technica on Counts I and III;

C. Grant attorney's fees and costs as provided by law, including 815 ILCS 510/3;

D. Enter an Order permanently enjoining Goodin and Ars Technica, including removal and full retraction of the Article; and

E. Grant such other and further relief as the Court may deem just and proper.

Jury Demand

Keeper requests a jury trial on all issues.

Dated: December 19, 2017

Respectfully submitted,

/s/Dean D. Niro

Dean D. Niro (dniro@vvnlaw.com)
Patrick F. Solon (solon@vvnlaw.com
VITALE, VICKREY, NIRO & GASEY LLP
311 S. Wacker Drive, Suite 2470
Chicago, Illinois 60606
Tel.: (312) 236-0733
Fax: (312) 236-3137

Attorneys for Keeper Security, Inc.

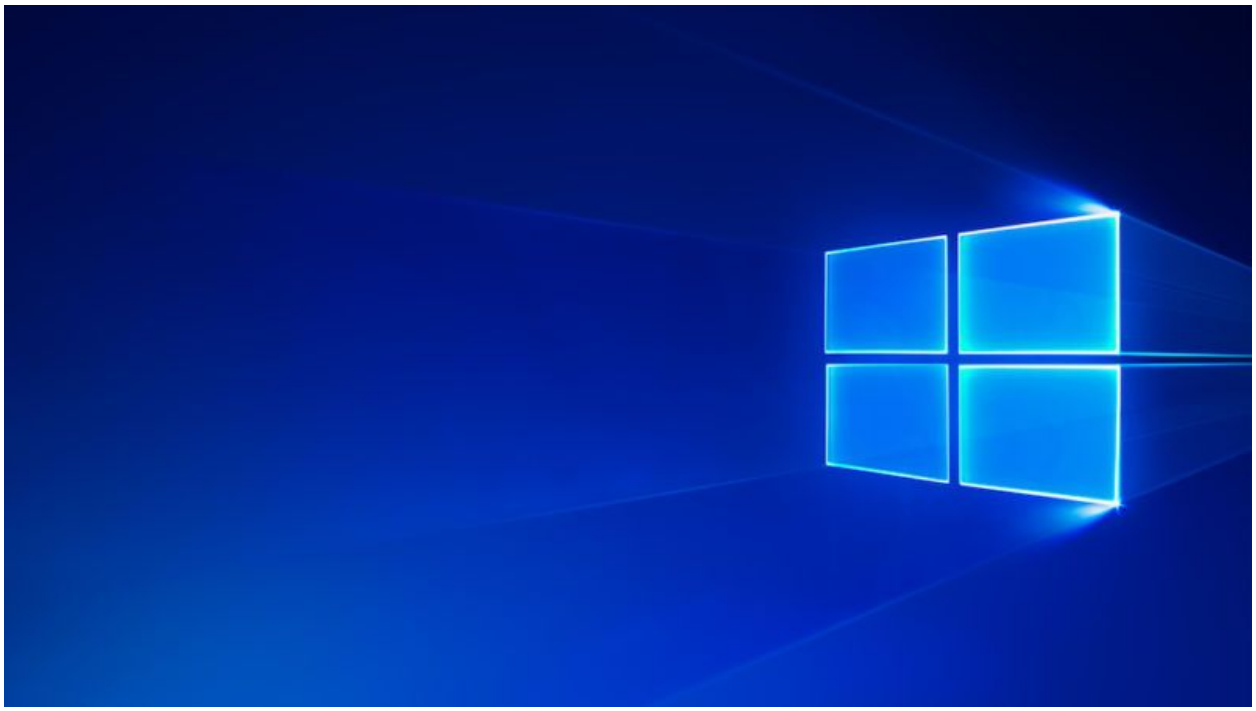
EXHIBIT 1 TO COMPLAINT

https://web.archive.org/web/20171215201301/https://arstechnica.com/information-technology/2017/12/microsoft-is-forcing-users-to-install-a-critically-flawed-password-manager/

Microsoft is forcing users to install a critically flawed password manager

Win 10 version of Keeper has 16-month-old bug allowing sites to steal passwords.

DAN GOODIN - 12/15/2017, 11:58 AM



Microsoft is quietly forcing some Windows 10 computers to install a password manager that contains a critical vulnerability disclosed 16 months ago that allows websites to steal passwords, a researcher said Friday.

Google Project Zero researcher Tavis Ormandy said in a blog post that the Keeper Password Manager came pre-installed on a newly built Windows 10

system derived directly from the Microsoft Developer Network. When he tested the unwanted app, he soon found it contained a critical flaw he had found in August 2016 in the non-bundled version of Keeper. The bug, he said, represents "a complete compromise of Keeper security, allowing any website to steal any password."

With only basic changes to "selectors," the old proof-of-concept exploit worked on the version installed without notice or permission on his Windows 10 system. Ormandy's post linked to this publicly available proof-of-concept exploit, which steals an end user's Twitter password if it's stored in the Keeper app. Ormandy said Keeper developers have released a fixed version. Keeper representatives didn't immediately respond to questions for this post.

Fortunately, Windows 10 users aren't vulnerable unless they open Keeper and begin trusting it with their passwords. Still, the incident raises questions about the security vetting Microsoft gives to apps it bundles with Windows. If an outsider can find a 16-month-old vulnerability so quickly and easily, it stands to reason people inside the software company should have found it long ago. Microsoft officials have yet to respond to questions about what testing it gives to third-party apps before they're pre-installed, and by some accounts these apps are repeatedly reinstalled against users' wishes on end users' computers.

It's possible Microsoft has a process in place for ensuring the security of third-party apps that get installed on Windows 10 machines and that somehow the Keeper vulnerability slipped through anyway. It's also possible third-party apps don't come with the same security assurances of other Microsoft software. Microsoft should provide an explanation how this happened.

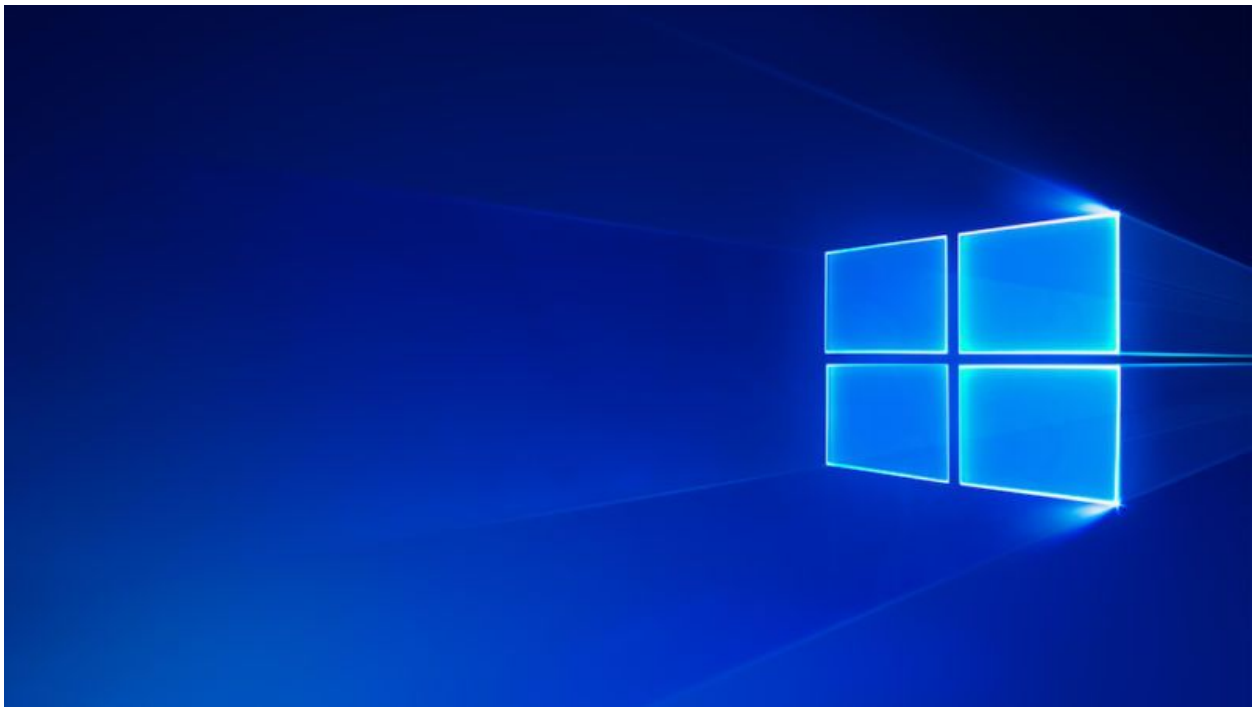
EXHIBIT 2 TO COMPLAINT

https://web.archive.org/web/20171215220038/https://arstechnica.com/information-technology/2017/12/microsoft-is-forcing-users-to-install-a-critically-flawed-password-manager/

Microsoft forced users to install a password manager with a critical flaw

Win 10 version of Keeper had bug allowing sites to steal passwords.

DAN GOODIN - 12/15/2017, 11:58 AM



For almost two weeks, Microsoft quietly forced some Windows 10 computers to install a password manager with a browser plugin that contained a critical vulnerability almost identical to one disclosed 16 months ago that allows websites to steal passwords, a researcher said Friday. Google Project Zero researcher Tavis Ormandy said in a blog post that the Keeper Password Manager came pre-installed on a newly built Windows 10 system derived directly from the Microsoft Developer Network. When he tested the unwanted app, he soon found it contained a bug that represents "a complete compromise of Keeper security, allowing any website to steal any password." He said he uncovered a flaw in the non-bundled version of the Keeper browser plugin 16 months ago that posed the same threat.

With only basic changes to "selectors," the old proof-of-concept exploit worked on the version installed without notice or permission on his Windows 10 system. Ormandy's post linked to this publicly available proof-of-concept exploit, which steals an end user's Twitter password if it's stored in the Keeper app. After this post went live, a Keeper spokesman said the bug was different than the one Ormandy reported 16 months ago. He said it affected only version 11 of the app, which was released on December 6, and then only when a user had the accompanying browser plugin installed. The developer has fixed the flaw in the just-released version 11.4 by removing the vulnerable "add to existing" functionality.

Fortunately, Windows 10 users wouldn't have been vulnerable unless they opened Keeper, trusted it with their passwords, and used the browser plugin. If an outsider can find a bug similar to the 16-month-old vulnerability so quickly and easily, it stands to reason people inside the software company should have found it long ago. Microsoft officials declined to say what testing it gives to third-party apps before they're pre-installed, and by some accounts these apps are repeatedly reinstalled against users' wishes on end users' computers. The representatives also declined to say what conditions caused Windows 10 computers to install the app.
In a statement, the representatives wrote: "We are aware of the report about this third-party app, and the developer is providing updates to protect customers."

While Ormandy reported Keeper was installed on a virtual machine created from a version of Windows intended for developers, people participating in the Reddit discussion reported Keeper was also installed on laptops, in one case right after it was taken out of the box and in another after it had been wiped clean and had Windows reinstalled. A third person reported Keeper being installed on a virtual machine created with Windows 10 Pro.

It's possible Microsoft has a process in place for ensuring the security of third-party apps that get installed on Windows 10 machines and that somehow the Keeper vulnerability slipped through anyway. It's also possible third-party apps don't come with the same security assurances of other Microsoft software. Microsoft should provide an explanation how this happened and explain the precise conditions under which Keeper and other apps do and don't get installed.

This post, including the headline, was updated to add comment from Keeper and Microsoft and to reflect details about the vulnerability and the Windows 10 versions reported to receive automatic installs.

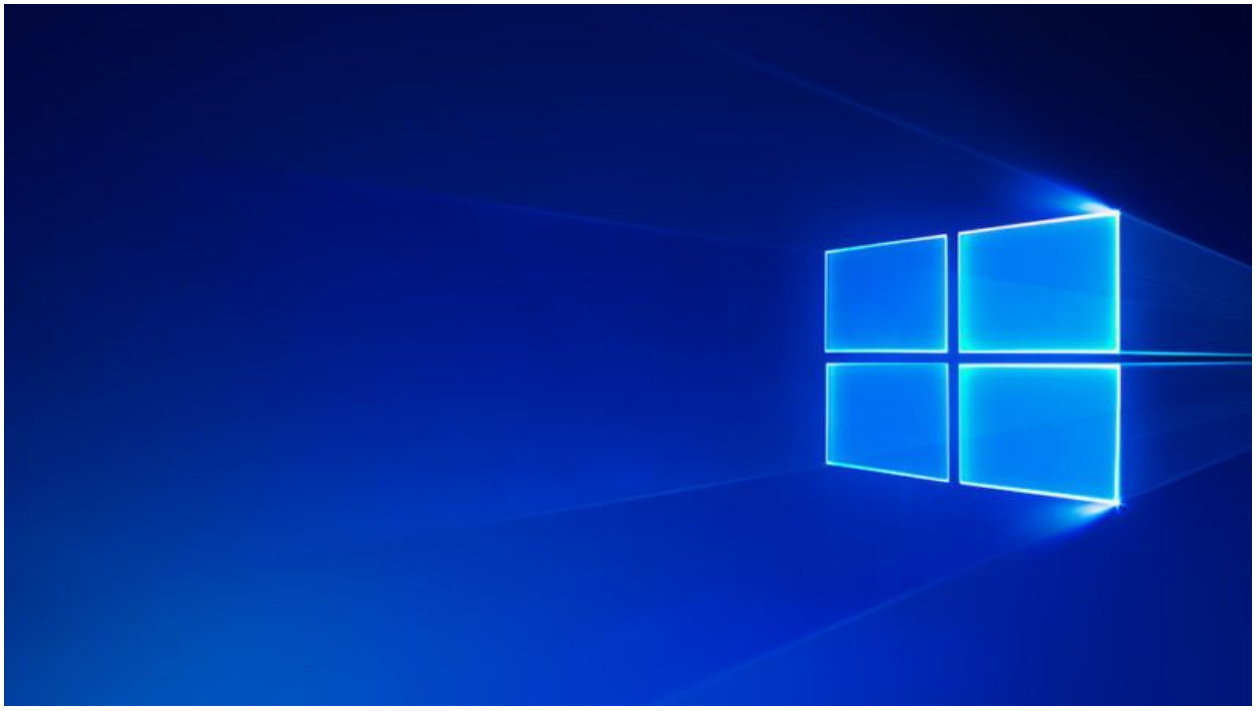
EXHIBIT 3 TO COMPLAINT

https://web.archive.org/web/20171217002153/https://arstechnica.com/information-technology/2017/12/microsoft-is-forcing-users-to-install-a-critically-flawed-password-manager/

For 8 days Windows bundled a password manager with a critical plugin flaw

Plugin for Win 10 version of Keeper had bug allowing sites to steal passwords.

DAN GOODIN - 12/15/2017, 11:58 AM



For about eight days, some versions of Windows 10 quietly bundled a password manager that contained a critical vulnerability in its browser plug in, a researcher said Friday. The flaw was almost identical to one the same researcher disclosed in the same manager plugin 16 months ago that allowed websites to steal passwords.

Google Project Zero researcher Tavis Ormandy said in a blog post that the Keeper Password Manager came pre-installed on a newly built Windows 10 system derived directly from the Microsoft Developer Network. When he tested the unwanted app, he soon found the browser plugin the app prompted him to enable contained a bug that represents "a complete

compromise of Keeper security, allowing any website to steal any password." He said he uncovered a flaw 16 months ago in the non-bundled version of the Keeper browser plugin that posed the same threat.

With only basic changes to "selectors," Ormandy's old proof-of-concept exploit worked on the new Keeper plugin. Ormandy's post linked to this publicly available proof-of-concept exploit, which steals an end user's Twitter password if it's stored in the Keeper app and the plugin is enabled. After this post went live, a Keeper spokesman said the bug was different than the one Ormandy reported 16 months ago. He said it affected only version 11 of the app, which was released on December 6, and then only when a user followed Keeper prompts to install the browser plugin. The developer on Friday fixed the flaw in the just-released version 11.4 by removing the vulnerable "add to existing" functionality. The fix came 24 hours after Ormandy privately reported the flaw to Keeper.

Fortunately, Windows 10 users wouldn't have been vulnerable unless they opened Keeper, trusted it with their passwords, and followed prompts to install the browser plugin. If an outsider can find a bug similar to the 16-month-old vulnerability so quickly and easily, it stands to reason people inside the software company should have found it first. Microsoft officials declined to say what testing it gives to third-party apps before they're pre-installed, and by some accounts these apps are repeatedly reinstalled against users' wishes even after being uninstalled. Microsoft representatives also declined to say what conditions caused Windows 10 computers to install the app.

In a statement, the representatives wrote: "We are aware of the report about this third-party app, and the developer is providing updates to protect customers."

While Ormandy reported Keeper was installed on a virtual machine created from a version of Windows intended for developers, people participating in the above-linked Reddit discussion reported Keeper was also installed on laptops, in one case right after it was taken out of the box and in another after it had been wiped clean and had Windows reinstalled. A third person reported Keeper being installed on a virtual machine created with Windows 10 Pro.
It's possible Microsoft has a process in place for ensuring the security of third-party apps that get installed on Windows 10 machines and that somehow the Keeper vulnerability slipped through anyway. It's also possible third-party apps don't come with the same security assurances of other Microsoft software. Microsoft should provide an explanation how this happened and explain the precise conditions under which Keeper and other apps do and don't get installed.

This post, including the headline, was updated to add comment from Keeper and Microsoft and to reflect details about the vulnerability and the Windows 10 versions reported to receive automatic installs. It was later edited to remove characterization the Keeper was forced on some Windows 10 users and to clarify the amount of time the prebundled version was vulnerable and the role of the browser plugin.