13 virus máy tính nguy hiểm nhất

Đã 20 năm trôi qua kể từ ngày virus máy tính đầu tiên xuất hiện, đã có nhiều virus mới ra đời nhưng điển hình trong số này chỉ có 13 loại virus nguy hiểm nhất và gây ra thiệt hại ở mức cao nhất.

Những vius máy tính "phá hoại" nhất trong lịch sử

1. CIH (1998)

Thiệt hại ước tính: 20-80 triệu USD trên toàn thế giới (không tính dữ liệu PC bị phá huỷ).

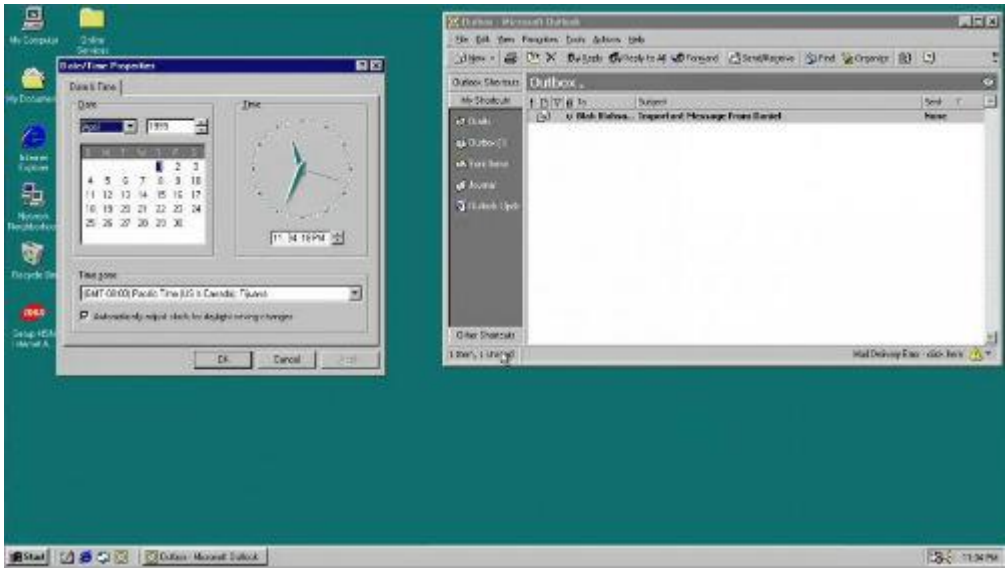
Có nguồn gốc từ **Đài Loan** (6/1998), CIH được nhận dạng là một trong những virus nguy hiểm và có sức tàn phá lớn nhất thời đại. Virus này tấn công vào các file thực thi của hệ điều hành Windows 95,98 và ME; có khả năng cư trú trên bộ nhớ máy tính để lây nhiễm và các file thực thi khác.

CIH nguy hiểm ở chỗ chỉ sau một thời gian ngắn hoạt động, nó có thể ghi đè dữ liệu trên ổ cứng máy tính, biến dữ liệu thành một mớ vô dụng. CIH cũng có khả năng **ghi đè thông tin BIOS**, ngăn không cho máy tính khởi động. Bởi khả năng lây nhiễm vào các file thực thi nên CIH có thể được phát tán rộng rãi.
CIH còn được biết đến với một cái tên khác là **virus Chernobyl** do thời điểm kích hoạt trùng với ngày xảy ra vụ nổ nhà máy nguyên tử Chernobyl.

Ngày nay, virus CIH đã không còn nguy hiểm do các nền tảng hệ điều hành mới như Windows 2000, XP và NT đã được cải tiến.

2. Melissa (1999)

Thiệt hại ước tính: 300-600 triệu USD

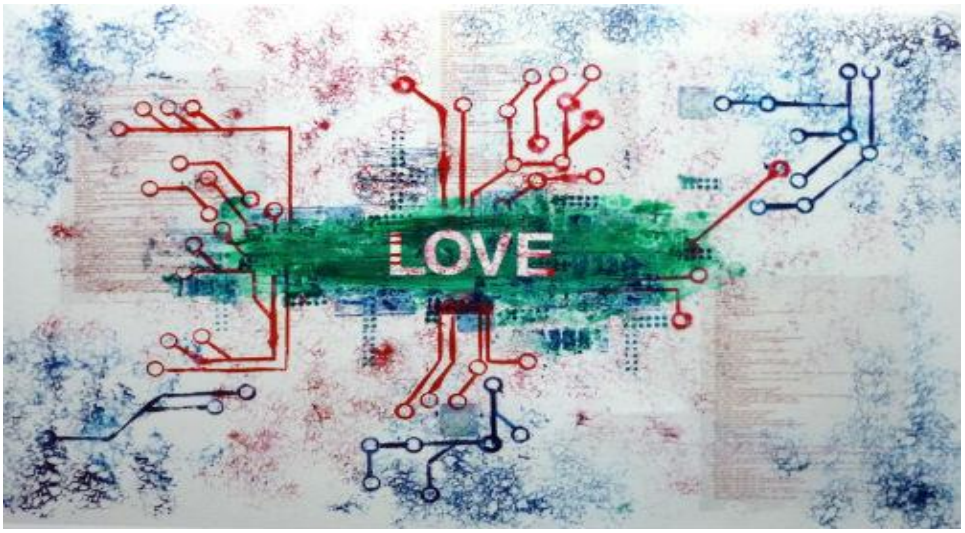


Ngày thứ sáu, 26/3/1999, virus **W97M/Melissa** đã lây nhiễm ở mức độ toàn cầu. Các thông kê cho thấy loại virus dạng kịch bản macro trong Word này đã lây nhiễm vào 15/20 chiếc máy tính doanh nghiệp trên toàn cầu. Melissa phát tán nhanh đến nỗi Intel, Microsoft và một số hãng phần mềm khác sử dụng **Outlook**đã buộc phải đóng toàn bộ hệ thống e-mail để hạn chế thiệt hại.

Melissa sử dụng **Microsoft Outlook** để gửi mail đính kèm (trong file Word) phiên bản virus tới 50 địa chỉ e-mail trong danh sách liên lạc người dùng. Thông điệp của e-mail có câu: "*"Here is that document you asked for...don't show anyone else. ;-)"*". Khi nhấn vào file .DOC đính kèm, virus sẽ bắt đầu lây nhiễm vào máy tính và lặp lại chu trình phát tán như trên.

3. ILOVEYOU (2000)

Thiệt hại ước tính: 10-15 triệu USD



Còn được biết đến với cái tên **Loveletter** và **The Love Bug**, loại virus này là một dạng kịch bản **Visual Basic** với một cái tên rất mỹ miều: **lời hứa tình yêu.**
Ngày 3/5/2000, sâu ILOVEYOU lần đầu tiên được phát hiện tại Hong Kong, sau đó nhanh chóng phát tán qua e-mail với dòng tiêu đề *"ILOVEYOU*" cùng file đính kèm: Love-Letter-For-You.TXT.vbs. Cũng giống Melisa, virus ILOVEYOU tự động gửi thư tới các địa chỉ liên lạc trong **Microsoft Outlook.**

Virus ILOVEYOU ghi đè các tệp tin nhạc, ảnh và một số định dạng khác với bản copy của chính nó. Nguy hiểm hơn, virus còn tìm kiếm tên và mật khẩu người dùng và gửi chúng tới e-mail tác giả.

Tác giả của virus đã không bị kết án do Philippines không có đạo luật chống tội phạm máy tính với thời điểm đó.

4. Code Red (2001)

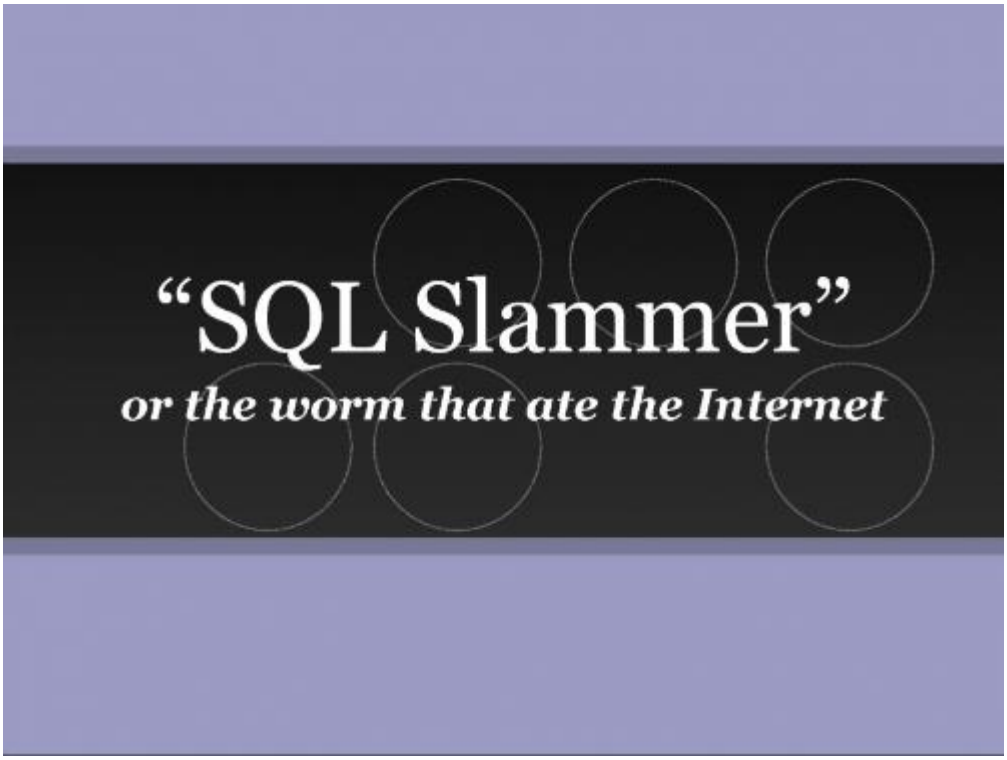
Thiệt hại ước tính: 2,6 triệu USD

Code Red là một dạng **sâu máy tính** lây nhiễm trên hệ thống máy chủ mạng, bắt đầu từ ngày 13/7/2001. Đây là loại virus cực kỳ độc hại bởi đích ngắm của chúng là các máy tính chạy phần mềm máy chủ Web Internet Information Server (IIS).
Sâu Code Red có khả năng khai thác một lỗ hổng trong **IIS**. Điều khôi hài là Microsoft đã ban hành miếng vá lỗ hổng này từ giữa tháng 6 trước đó.
Code Red còn có tên là Bady, được thiết kế với mục đích phá huỷ ở mức lớn nhất có thể. Khi đã lây nhiễm vào máy tính, website lưu trữ trên máy

chủ bị ảnh hưởng sẽ hiển thị thông điệp: ""*HELLO! Welcome to http://www.worm.com! Hacked By Chinese!"*. Sau đó, virus sẽ tìm kiếm các máy chủ bị lỗi và tiếp tục lây nhiễm. 20 ngày tiếp theo đó, virus sẽ kích hoạt các cuộc tấn công từ chối dịch vụ (DoS) vào những địa chỉ IP nhất định, bao gồm cả máy chủ của **Nhà Trắng**. Chỉ chưa đến một tuần, virus đã lây nhiễm vào khoảng 400.000 máy chủ trên toàn thế giới. Ước tính có tới 1 triệu máy tính bị virus này tấn công.

5. SQL Slammer (2003)

Thiệt hại ước tính: Bởi SQL Slammer được kích hoạt vào thứ bảy (ngày nghỉ) nên thiệt hại ước tính (về tiền) không cao. Tuy nhiên, virus cũng đã "*hạ gục"*500.000 máy chủ trên toàn thế giới, và là nhân tố gây nên *"cơn bão"* dữ liệu ồ ạt, khiến toàn bộ mạng Internet của Hàn Quốc bị sập trong 12 tiếng.



SQL Slammer còn được biết đến với cái tên **Sapphire**, được kích hoạt vào ngày 25/1/2003. SQL Slammer có tác động rất xấu tới toàn bộ giao vận Internet toàn thế giới. Điều thú vị là loại virus này không tìm kiếm các máy PC đầu cuối mà chỉ hướng tới **máy chủ.** SQL Slammer là một gói dữ liệu đơn lẻ và tự gửi tới các**địa chỉ IP**. Nếu địa chỉ IP là một máy tính chạy bản SQL Server Desktop Engine (Microsoft) chưa được vá lỗi, thì chiếc máy chủ đó sẽ ngay lập tức bị nhiễm virus và trở thành công cụ tấn công các địa chỉ IP khác.

Với phương thức lây nhiễm trên, Slammer có thể tấn công 75.000 máy tính chỉ trong... 10 phút, làm tắc nghẽn toàn bộ mạng Internet, khiến các router phải ngừng hoạt động.

6. Blaster (2003)

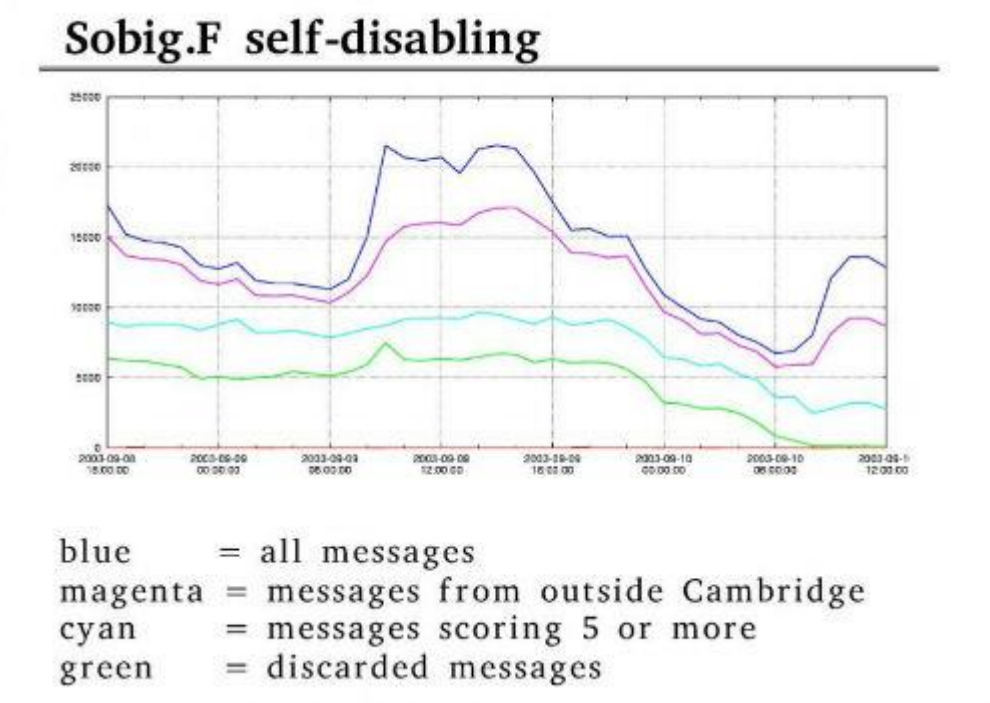
Thiệt hại ước tính: 2-10 tỷ USD, hàng trăm nghìn máy tính bị lây nhiễm.

Mùa hè năm 2003 là thời gian khó khăn đối với mạng máy tính doanh nghiệp do sự xuất hiện gần như nối tiếp nhau trong thời gian khá ngắn của sâu Blaster và Sobig. Blaster còn được biết đến với cái tên **Lovsan** hay **MSBlast**, là quả "*bom tấn"* nổ ra trước. Virus này được phát hiện vào ngày 11/8 và đã nhanh chóng lây nhiễm trên quy mô toàn cầu chỉ trong ... 2 ngày.
Được phát tán qua mạng và giao vận Internet, Blaster khai thác một lỗ hổng trong**Windows 2000 và Windows XP;** và khi được kích hoạt, sâu sẽ cho hiển thị một hộp thông báo *"chết người*" rằng máy tính sẽ bị tắt sau ít phút. Được che giấu trong mã nguồn tệp tin **MSBLAST.EXE** là dòng thông điệp tác giả: *"Bill Gates, tại sao ông lại khiến cho điều này xảy ra. Hãy ngừng kiếm tiền và sửa chữa phần mềm của ông đi".*

Blaster còn chứa đoạn mã kích hoạt tấn công DoS vào website windowsupdate.com của Microsoft vào ngày 15/4.

7. Sobig.F (2003)

Thiệt hại ước tính: 5-10 tỷ USD; hơn 1 triệu máy tính bị lây nhiễm.



Sobig xuất hiện ngay sau *"cơn bão" Blaster*", biến tháng 8/2003 trở thành tháng "*tồi tệ*" nhất cho người dùng máy tính doanh nghiệp và gia đình. Phiên bản nguy hiểm nhất của virus này là Sobig.F, phát tán rộng rãi vào ngày

19/8 và đã lập kỷ lục mới (sau đó bị MyDoom qua mặt) là tạo ra hơn 1 triệu bản copy của sâu chỉ trong 24 giờ đầu tiên.
Virus lây nhiễm vào máy tính thông qua tệp tin đính kèm **e-mail,** chẳng hạn như: application.pif, thank_you.pif... Khi được kích hoạt, sâu này sẽ tự gửi vào các địa chỉ e-mail lưu trữ trên máy tính nạn nhân.
Ngày 10/9/2003, Sobig đã tự "*phân huỷ*" và không còn là mối đe doạ nữa. Microsoft đã treo giải thưởng 250.000USD cho những ai cung cấp thông tin dẫn tới việc bắt giữ tác giả sâu Sobig, thế nhưng cho tới nay, vẫn chưa có ai làm được điều này.

8. Bagle (2004)

Thiệt hại ước tính: Hàng chục triệu USD.

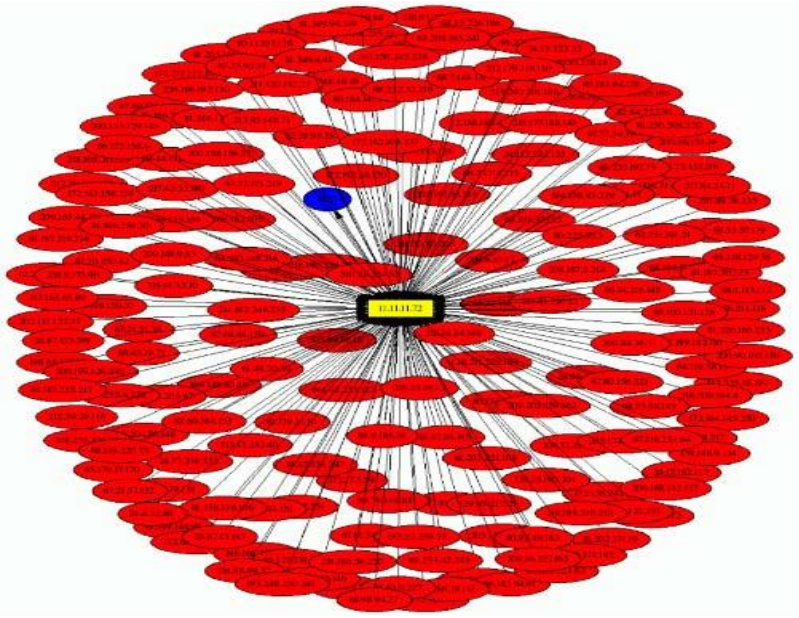
Bagle là một điển hình cho loại sâu máy tính có cơ chế hoạt động tinh vi, xuất hiện vào ngày 18/1/2004. **Mã độc hại** của sâu lây nhiễm vào hệ thống thông qua e-mail, và sau đó sẽ tìm kiếm địa chỉ e-mail trên ổ cứng máy tính để phát tán.

Sự nguy hiểm của Balge (và 60-100 biến thể sâu) là ở chỗ khi lây nhiễm vào máy tính, sâu sẽ mở một cổng sau (backdoor) tại cổng TCP để tin tặc điều khiển từ xa (truy cập, đánh cắp dữ liệu...).

Phiên bản Bagle.B được thiết kế để ngừng toàn bộ sự hoạt động của Bagle sau ngày 28/1/2004; tuy nhiên cho tới tận nay, các biến thể rời rạc của virus này vẫn còn phát tán trên mạng.

9. MyDoom (2004)

Thiệt hại ước tính: Làm cho mạng Internet toàn cầu chậm mất 10%; tăng thời gian tải xuống (load) trang web lên 50%.



Chỉ mất vài giờ (26/1/2004), *"làn sóng"* MyDoom đã có mặt trên toàn thế giới bằng phương thức phát tán truyền thống: **qua e-mail.**
MyDoom còn có tên là **Norvarg**, có khả năng tự lây nhiễm theo một phương thức đặc biệt: tự gửi bản sao của sâu trong một e-mail có tên "*Mail Transaction Failed*" (một dạng thông báo phản hồi thông thường của máy chủ Mail khi phát sinh lỗi trong quá trình chuyển mail). Khi nhấn vào file đính kèm, sâu sẽ phát tán vào các địa chỉ mail tìm thấy trên máy tính nạn nhân. MyDoom cũng lây nhiễm qua thư mục chia sẻ của các tài khoản mạng ngang hàng Kazaa.
Khả năng nhân bản của MyDoom hiệu quả đến nỗi các hãng bảo mật thống kê rằng cứ mỗi 10 e-mail được gửi đi có một e-mail *"dính"* sâu. MyDoom được lập trình ngừng hoạt động vào ngày 12/2/204.

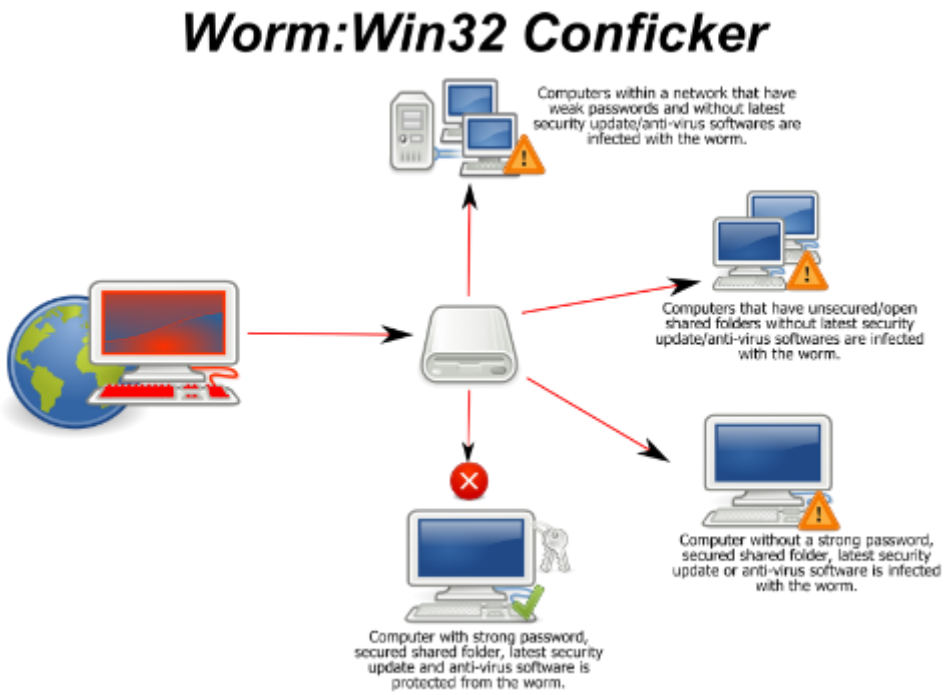
10. Sasser (2004)

Thiệt hại ước tính: Hàng triệu USD.

Sasser bắt đầu lây nhiễm vào ngày 30/4/2004, và đủ mạnh để đánh sập liên lạc qua vệ tinh của một số hãng thông tấn Pháp. Sasser cũng chính là nguyên nhân kiến cho vài chuyến bay của hãng hàng không Delta phải hoãn lại vì máy tính bị trục trặc.

Không giống các loại sâu trước đó, Sasser không phát tán qua e-mail và không cần sự tương tác của người dùng để lây nhiễm. Thay vào đó, sâu khai thác một **lỗ hổng bảo mật trong bản Windows 2000 và Windows XP c**hưa được nâng cấp để tấn công vào hệ thống. Khi đã nhân bản thành công, sâu sẽ tiến hành quét các hệ thống máy tính khác và tự gửi bản sao tới. Các hệ thống nhiễm Sasser liên tục gặp trục trặc và mất ổn định.

11. Conficker

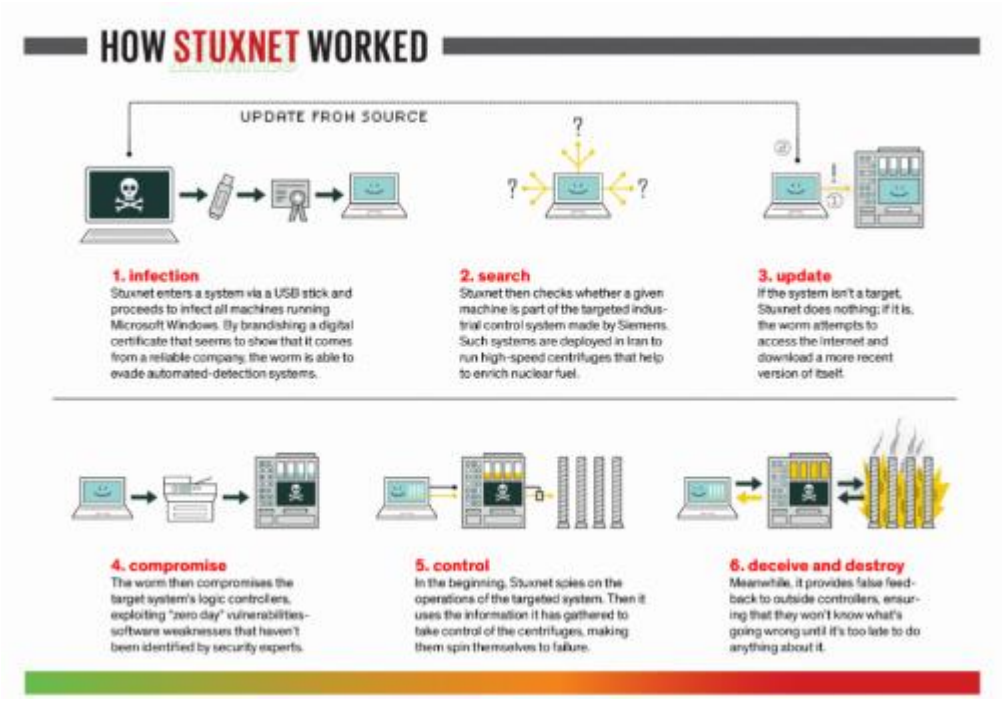


Đây là một loại sâu máy tính được lập trình để tấn công các hệ điều hành**Microsoft** vào năm 2008. Conficker rất khó bị phát hiện và nó có thể lây nhiễm qua thư điện tử, USB, ổ cứng ngoài hay thậm chí điện thoại thông minh. Sau khi lây nhiễm, sâu sẽ kết nối máy tính với một botnet được kiểm soát bởi người tạo ra sâu. Botnet này sau đó có thể được sử dụng để thực hiện tấn công từ chối dịch vụ (DoS) hay thu thập các thông tin tài chính quan trọng.

12. Storm Worm

Storm Worm là một loại virus có chức năng như sâu Conficker, lây nhiễm vào các máy tính và ép chúng tham gia vào một **botnet**. Nó bắt đầu phát tán vào năm 2006 qua một bức thư điện tử có tiêu đề "*230 người chết khi một cơn bão quét qua châu Âu"* và sau đó được thay bằng nhiều tiêu đề gác như '*Tin xấu'* hay**Chiến tranh Thế giới thứ ba đã bắt đầu**. Virus này đã lây nhiễm rất nhanh với khoảng 10 triệu máy tính trở thành nạn nhân của nó.

13. Stuxnet



Đây không phải là sâu máy tính được tạo ra để đánh cắp thông tin thẻ tín dụng, mật khẩu hay những thứ thông thường khác. Nó là một **vũ khí mạng** được Mỹ và Israel hợp tác phát triển để phá hủy **nhà máy hạt nhân** của Iran cũng như làm chậm hay phá hủy chương trình phát triển vũ khí hạt nhân của Tehran.

Iran đã phát hiện thấy sâu Stuxnet trong hệ thống kiểm soát nhà máy hạt nhân của nước này vào năm 2010, nhưng họ tin rằng nó đã xuất hiện trước đó 1 năm. Nó phá hoại bằng cách làm tăng tốc độ của các **máy li tâm hạt nhân** và dần dần phá hủy chúng, trong khi phản hồi thông tin về trung tâm tâm kiểm soát rằng mọi việc vẫn hoạt động bình thường. Stuxnet đã phá hủy 1/5 máy ly tâm tại **nhà máy hạt nhân Natanz của Iran.**

Sau khi tấn công nhà máy hạt nhân Natanz, Stuxnet đã nhanh chóng phát tán trên mạng internet và lây nhiễm các máy tính trên toàn thế giới. **Mã nguồn** của nó có thể được tải xuống và chỉnh sửa bởi bất kỳ ai có kiến thức về lập trình. Nó được sử dụng để tấn công các hệ thống điều khiển các công trình lớn như hồ trữ nước, nhà máy điện, nhà máy hạt nhân.

ST