



Mô hình ứng dụng Hội chẩn Mã độc Trực tuyến trong tiếp cận Máy học Anti-virus



SECURITY BOOTCAMP 2013

Đơn vị tổ chức:



Đơn vị tài trợ:



Safety from thinking



Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

Nội dung





Giới thiệu

- Thời gian gần đây, tình hình tấn công an ninh mạng (ANM) gây nhiều tổn thất cho các hệ thống CNTT và cộng đồng người sử dụng
- Tìm hiểu các cơ chế tấn công ANM phổ biến, ngăn chặn các hình thức thâm nhập hệ thống mạng, bảo vệ an toàn an ninh thông tin là việc làm cấp bách hiện nay



Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

Tình hình an ninh mạng

- Tình hình an ninh mạng trong nước
- Tình hình an ninh mạng quốc tế
- Mã độc trong tấn công an ninh mạng
- Minh họa trojan và tấn công DDoS



Tình hình an ninh mạng trong nước

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- Năm 2012: Việt Nam bị xếp thứ 15 về phát tán mã độc, thứ 10 về tin rác, thứ 15 về zombie
 - Hơn 2200 website bị tấn công tắc nghẽn
 - 78/100 trang web chính phủ được khảo sát có thể bị tấn công
 - Xuất hiện nhiều virus ăn cắp tài khoản ngân hàng trực tuyến
 - Bộc phát lượng mã độc chuyên đánh cắp thông tin
- Năm 2013: mỗi tháng có khoảng 300 website bị tấn công làm thay đổi giao diện, đăng các thông tin sai lệch, phá hoại hoạt động của website
 - Tháng 7-2013: các báo điện tử Vietnamnet, Dân trí và Tuổi trẻ bị tấn công tắc nghẽn gần 3 tuần
 - Tháng 8-2013: 437 website của các cơ quan, doanh nghiệp tại Việt Nam bị hacker xâm nhập



Tình hình an ninh mạng quốc tế

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- 20/3/2013: máy chủ 3 đài truyền hình lớn và 2 ngân hàng quan trọng Hàn Quốc bị nhóm tin tặc “Đội Whois” (được cho là của Triều Tiên) tấn công làm tê liệt
- 27/3/2013, Cục Cảnh sát Phòng chống Tội phạm Sử dụng Công nghệ cao (Bộ Công an) cảnh báo hacker TQ có kế hoạch đánh cắp dữ liệu Việt Nam
- 6/2013: Mỹ cáo buộc hacker TQ tấn công đánh cắp nhiều tài liệu mật trước thời điểm cuộc gặp cấp cao nguyên thủ hai nước



Tình hình an ninh mạng quốc tế...

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- 6/2013: cựu nhân viên Cục Tình báo Trung ương Mỹ (CIA) Edward Snowden tiết lộ chương trình bí mật do thám điện thoại và chương trình Tempora theo dõi Internet của Cơ quan An ninh quốc gia Mỹ (NSA)
- 8/2013: hacker Dr@cul@ tấn công 6000 website Ấn Độ
- 9/2013: hacker Syria tấn công website Thủy quân lục chiến Mỹ
- 10/2013: báo Pháp *Le Monde* đăng tải chi tiết về Genie, một chương trình theo dõi được cho là của NSA, trong đó các phần mềm gián điệp được cài vào các máy tính bên ngoài nước Mỹ, kể cả các đại sứ quán nước ngoài



Tình hình an ninh mạng quốc tế...

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- 6/10: kênh truyền hình Globo (Brazil) tiết lộ Canada bí mật theo dõi các hệ thống thông tin của Bộ Năng lượng và hầm mỏ Brazil
- 13/10: tổng thống Braxin yêu cầu Cơ quan Xử lý Dữ liệu Liên bang triển khai hệ thống email an toàn ở các cơ quan chính phủ Brazil
- 10/10: máy chủ web của chính phủ Thổ Nhĩ Kỳ bị thâm nhập dùng làm nơi phát tán mã độc...
- 24/10: Đức yêu cầu Mỹ làm rõ nghi vấn cài phần mềm nghe lén thiết bị di động của Thủ tướng Angela Merkel



Mã độc trong tấn công ANM

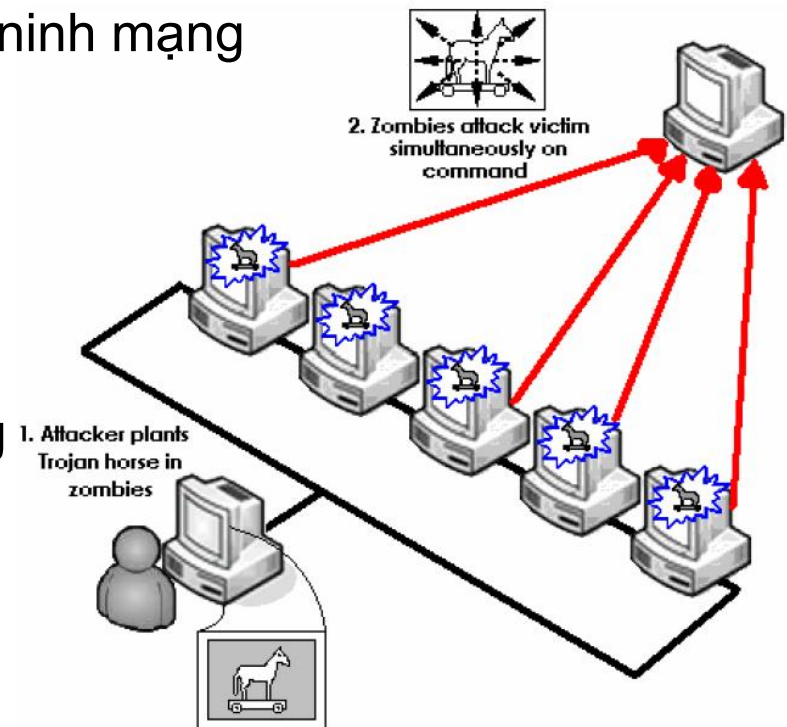
- Mã độc (malicious code, malware): loại chương trình (program) chèn bí mật vào hệ thống nhằm làm tổn hại tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống
- Các loại mã độc: computer virus, trojan horse, Internet worm, rootkit, backdoor, spyware...
- Kịch bản tấn công ANM của hacker:
 1. Hacker thiết kế mã độc
 2. Hacker phát tán mã độc trên mạng
 3. Mã độc đánh cắp dữ liệu, gửi về cho hacker
 4. Hacker phát lệnh cho mã độc tấn công hệ thống



Minh họa trojan và tấn công DDoS

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- Từ chối dịch vụ (DoS - Denial of Service): hình thức tấn công làm suy giảm năng lực phục vụ mạng
- Distributed DoS: tấn công từ chối dịch vụ trên diện rộng
- Giai đoạn 1, chuẩn bị lực lượng:
 - Bí mật cài nội ứng (trojan, worm...) vào các trạm (zombie)
 - Liên lạc zombie, nắm tình hình an ninh mạng
- Giai đoạn 2, tấn công:
 - Khi số zombie đủ lớn, phát lệnh tấn công vào các host thứ cấp
 - Khi các host tiền phương bị tê liệt, tập trung tấn công host trung ương





Các phần mềm Anti-virus

- Anti-virus (AV): các hệ chương trình bảo vệ máy tính khỏi mã độc xâm nhập
- Chức năng: canh phòng, kiểm tra, phát hiện mã độc xâm nhập, bảo vệ an toàn dữ liệu, an ninh hệ thống
- Nguyên tắc: nhận dạng mã độc dựa vào tập đặc trưng
- Vai trò: tăng cường tính năng tường lửa (Firewall) và lọc web (Internet Security)
- Sản phẩm Việt Nam: BKAV, CMC, D2...
- Sản phẩm nước ngoài: Avira, Kaspersky, NOD32, Panda, Symantec...



Các tiếp cận Anti-virus

- Tiếp cận chuỗi mã (signature matching):
 - Đối chiếu thông tin đối tượng với thông tin mã độc được tổ chức, cập nhật trong CSDL
 - Nhận dạng chính xác mã độc đã biết
 - Không phát hiện mã độc chưa có trong CSDL mẫu
- Tiếp cận hành vi (behavior checking):
 - Thi hành heuristic mã lệnh nghi ngờ trong môi trường mô phỏng
 - Phát hiện tốt các loại mã độc biến thể, đa hình
 - Có thể nhận dạng nhầm mã tương tự



Tiếp cận máy học Anti-virus

- MAV - Machine Learning Approach to Anti-virus System: ‘dạy’ máy tính học cách xử lý mã độc dựa vào cơ sở tri thức của chuyên gia
- Hoạt động theo mô hình hệ chuyên gia:
 - Giai đoạn học: chuyên gia xây dựng cơ sở tri thức (CSDL+ luật nhận dạng) và động cơ suy diễn
 - Giai đoạn xử lý: máy chạy động cơ suy diễn, vận dụng CSTT nhận dạng mã độc trên máy đích
- Đặc điểm:
 - Tái hiện hoạt động phân tích, nhận dạng mã độc của chuyên gia trong thế giới thực
 - Học tương tự, dự báo mã độc lạ, tự tăng trưởng CSTT
 - Khả năng dự báo phụ thuộc vào mô hình, chất lượng CSTT



Các vấn đề của Anti-virus

- Xu hướng của các Anti-virus:
 - Giai đoạn tiền xử lý: áp dụng tiếp cận chuỗi mã
 - Giai đoạn dự báo: áp dụng các tiếp cận tiên tiến
- Mã độc bộc phát, các anti-virus cần:
 - Tăng cường thu thập mẫu, đẩy nhanh tiến độ phân tích mã độc, gia tăng tần suất cập nhật CSDL
 - Mở rộng quy mô công ty, bổ sung chuyên gia phân tích, tuyển mộ cộng tác viên, chăm sóc khách hàng...
- Các vấn đề của Anti-virus:
 - Tập mẫu gia tăng, tiêu tốn tài nguyên, chạy chậm
 - Tối thiểu CSDL, nhận dạng tối đa, giảm nhu cầu tài nguyên, tăng tốc truy vấn...



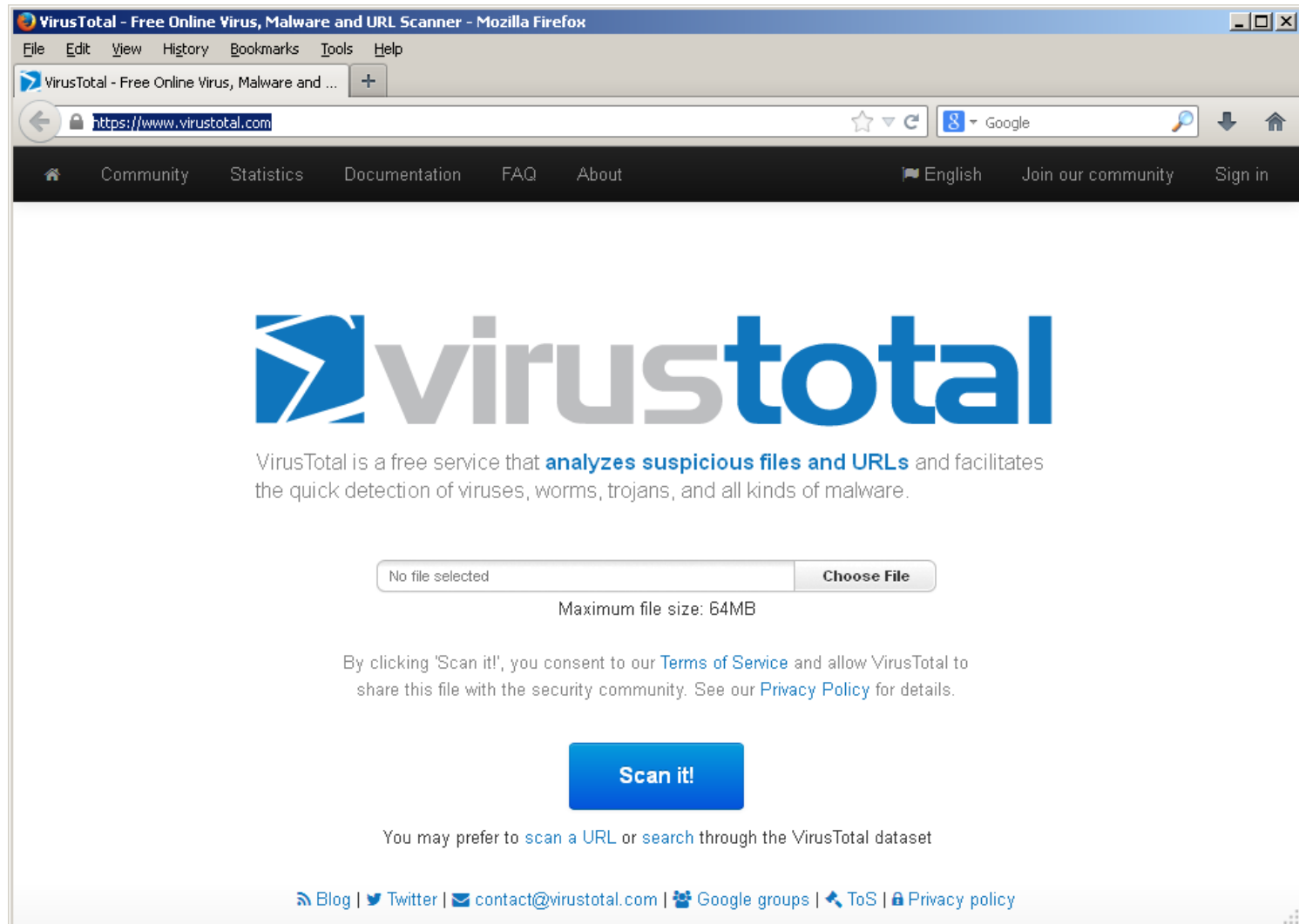
Kiểm tra mã độc trực tuyến

- Dịch vụ kiểm tra, tư vấn mã độc trực tuyến, tạm gọi MOC - Malicious Online Consultation
- Cơ chế hoạt động:
 - User upload file nghi ngờ mã độc lên MOC server
 - Các anti-virus của MOC kiểm tra file
 - MOC tổng hợp kết quả, gửi báo cáo cho user
- Các MOC phổ biến:
 - VirusTotal: www.virustotal.com
 - Jotti: www.virusscan.jotti.org/en



Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

VirusTotal





Kết quả kiểm tra mã độc bằng VirusTotal

Cty TNHH Công nghệ Phần mềm D2

D2 Software Technology Co., Ltd

Antivirus scan for ca7dae4109c5bd58e011ecf651edb00a at 2013-03-18 08:11:20 UTC - VirusTotal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Antivirus scan for ca7dae4109c5bd58e0... Google Dịch

https://www.virustotal.com/en/file/fdb7d3d15cf1949c6eec568c4ec13b7aeb5ab432afb04180c156753a4779869e/analysis/

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: fdb7d3d15cf1949c6eec568c4ec13b7aeb5ab432afb04180c156753a4779869e

File name: test.txt

Detection ratio: 40 / 45

Analysis date: 2013-03-18 08:11:20 UTC (7 months, 1 week ago)

More details

Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
Agnitum	I-Worm.Luder!KYjdh9G6UGM	20130317
AhnLab-V3	Win32/Luder.worm.27136	20130317
AntiVir	TR/Spy.Gen	20130317
Antiy-AVL	Worm/Win32.Luder.gen	20130317
Avast	Win32:Luder	20130318
AVG	unknown virus Win32/DH{A2cJD01kXSAklg}	20130318
BitDefender	Win32.Luder.B@mm	20130318





Kết quả kiểm tra mã độc bằng Jotti

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

Luder.exe - Jotti's malware scan - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Luder.exe - Jotti's malware scan x Google Dịch

virusscan.jotti.org/en/scanresult/925d6b26e68d78d0d760335f9fcbdd0482461cca8

Jotti

Jotti's malware scan

Filename: Luder.exe
Status: Scan finished. 21 out of 23 scanners reported malware.
Scan taken on: Thu 24 Oct 2013 17:16:19 (CET)
[Permalink](#)
[Next file](#)

Download 100,000+ Apps
[www.Mobogenie.com](#)
All-in-One Android Phone Manager.
Free Download Now! (Windows Only)

Additional info

File size: 27136 bytes
Filetype: PE32 executable (GUI) Intel 80386, for MS Windows, PECompact2 compressed
MD5: ca7dae4109c5bd58e011ecf651edb00a
SHA1: 8eb30c08087e97cb9de3947ac42711afa80a65fa
Packer (Avast): PECompact

Scanners

Ad-Aware	2013-10-24 Win32.Luder.B@mm	FARTINET	2013-10-24 W32/Luder.C@mm
agnitum	2013-10-24 I-Worm.Luder!KYjdh9G6UGM	F-PROT	2013-10-24 W32/Luder.A
ArcaVir	2013-10-24 Found nothing	F-Secure	2013-10-24 Win32.Luder.B@mm
avast!	2013-10-23 Win32:Luder	G DATA	2013-10-24 Win32.Luder.B@mm
AVG	2013-10-24 I-Worm/Luder.A.dropper	IKARUS	2013-10-24 Email-Worm.Win32.Luder.b
AntiVir	2013-10-24 TR/Spy.Gen	KASPERSKY	2013-10-24 Email-Worm.Win32.Luder.b
bitdefender	2013-10-24 Win32.Luder.B@mm	PANDA	2013-10-24 Found nothing
ClamAV	2013-10-24 Worm.Luder	Quick Heal	2013-10-23 I-Worm.Luder.b
CP Secure	2013-10-24 W32.Email.W.Luder.B	SOPHOS	2013-10-24 Mal/Luder-A
Dr.Web	2013-10-24 Win32.HLLM.Duel	TREND MICRO	2013-10-23 PE_LUDER.GEN
eScan	2013-10-24 Win32.Luder.B@mm	VBA32	2013-10-24 Email-Worm.Win32.Luder.b
eset	2013-10-24 Win32/Luder.B worm		



Đánh giá MOC

- Ưu điểm:
 - Kiểm tra miễn phí, hỗ trợ nhiều định dạng mẫu
 - Tham vấn nhiều ‘chuyên gia’ anti-virus, độ tin cậy cao
- Nhược điểm:
 - Kiểm tra từng file, tốc độ chậm
 - Chỉ báo cáo kết quả, không xử lý mẫu
 - Không bảo vệ máy tính trong thời gian thực
- Câu hỏi nghiên cứu:
 - Có thể khai thác kinh nghiệm của các “chuyên gia” anti-virus, đẩy nhanh tiến độ phân tích mẫu?
 - Cơ chế tích hợp kiến thức chuyên gia vào CSTT?



Quy trình ứng dụng “MOC-MAV”

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

1

Đệ trình tập mẫu

2

Nhận kết quả kiểm tra

3

Đặc tả tri thức chuyên gia

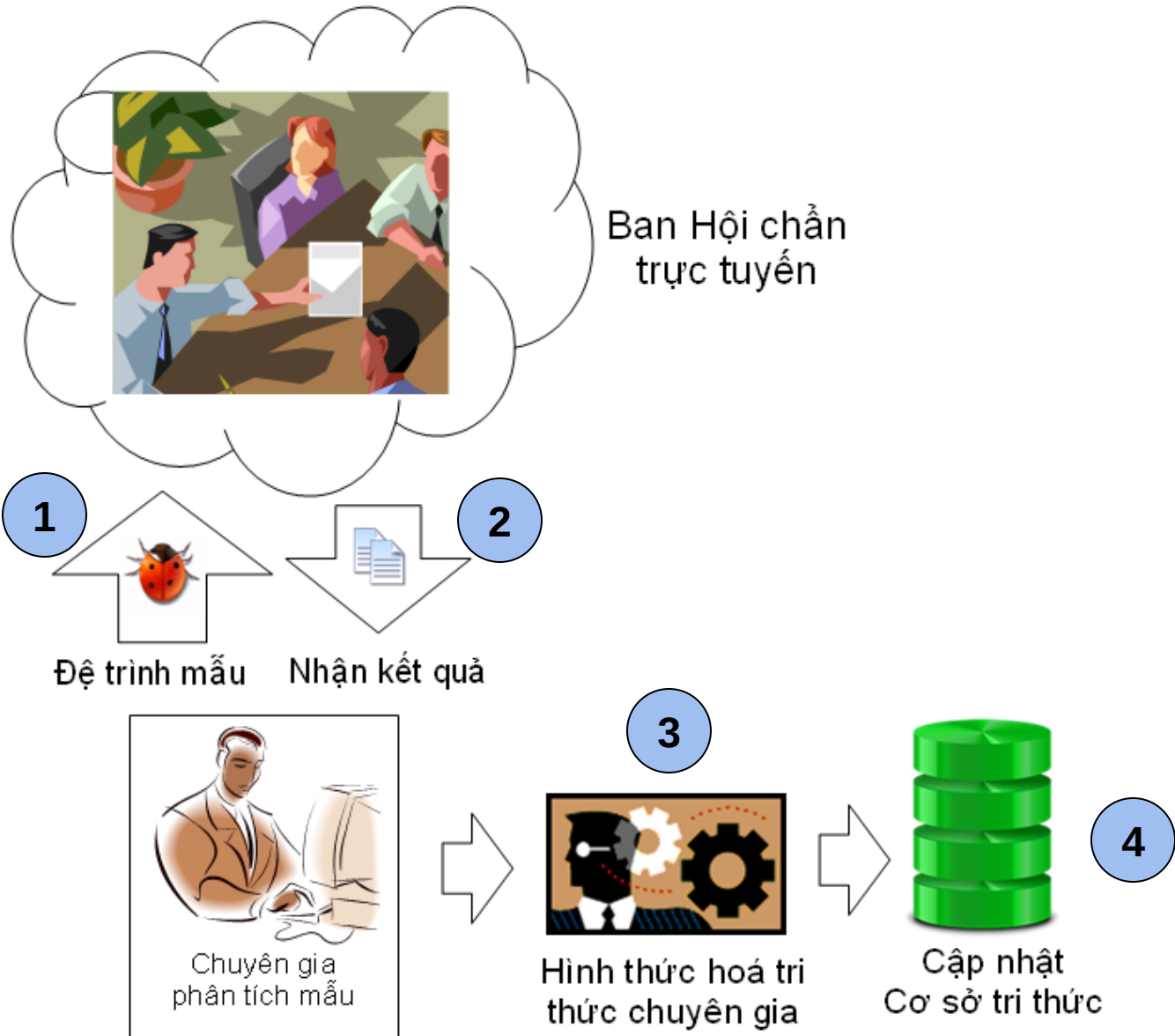
4

Cập nhật, tăng trưởng CSTT



Mô hình ứng dụng “MOC-MAV”

Cty TNHH Công nghệ Phần mềm
D2 Software Technology Co., Ltd





Vấn đề thiết kế mô hình “MOC-MAV”

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- Các vấn đề của MOC:
 - Cải tiến đầu vào: upload 1 mẫu => upload nhiều mẫu
 - Cải tiến đầu ra: nhận 1 kết quả => nhận nhiều kết quả
- Các vấn đề của MAV:
 - Phân tích kết quả kiểm tra của MOC
 - Phân loại, tinh chế, đặc tả tri thức kiểm tra
 - Ứng dụng hệ chuyên gia hỗ trợ quyết định
 - Tích hợp, cập nhật tri thức chuyên gia



Giới thiệu D2 Anti-virus* 2013

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- D2 Anti-virus* - Diagnose and Destroy Computer Viruses: anti-virus hướng tiếp cận máy học
- Hệ phần mềm D2 gồm 2 gói:
 - Gói Chuyên gia (D2 Expert Utilities): upload tập mẫu lớn, thu nhận, phân tích kết quả MOC, ra quyết định đặt tên mã độc, trích chọn đặc trưng, xây dựng CSDL, phân hoạch tập mẫu, rút luật nhận dạng, mã hóa băm chỉ mục, sắp xếp, lưu trữ, xuất bản CSTT...
 - Gói Người dùng (D2 Anti-virus* 2013): xử lý mã độc, bảo vệ thời gian thực; dự báo heuristic; ước lượng mã tương đồng; phát hiện hành vi lây nhiễm trên thiết bị lưu trữ cá nhân...



Giới thiệu D2 Anti-virus* 2013...

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd

- Các tính năng cơ bản:
 - Tốc độ quét nhanh, ít tiêu thụ bộ nhớ (~40MB)
 - Ngôn ngữ Việt-Anh, giao diện đa điểm
 - Tự động cập nhật CSDL từ Internet
- Các tính năng đặc biệt:
 - Nhận dạng thông minh, phát hiện mã độc lạ
 - Chủ động ngăn chặn nguy cơ từ đĩa USB, mã độc phát tán qua mạng và qua các trang web
 - Tích hợp nhiều tiện ích: phục hồi tập tin ẩn trên USB, quản trị tiến trình linh hoạt
 - Hỗ trợ gửi mẫu, định nghĩa tập tin nguy hiểm...



Giao diện chính D2 Anti-Virus* 2013

Cty TNHH Công nghệ Phần mềm D2
D2 Software Technology Co., Ltd



Cập nhật CSDL, quét USB

Cập nhật Cơ sở Dữ liệu Virus



Cơ sở dữ liệu phần mềm D32 trên máy bạn đã cũ.
Số mẫu virus mới máy bạn cần cập nhật: **1676 (141 KB)**
Bạn có muốn cập nhập dữ liệu virus mới không?

Cập nhật Cơ sở Dữ liệu Virus



Đang tích hợp cơ sở dữ liệu virus.
Xin vui lòng chờ giây lát...

D2 Anti-Virus* Enterprise - Kiểm tra thiết bị cắm thêm

Đang kiểm tra virus...

E:_new_virus\20101014\Da hình

Số tập tin: 934 Số tập tin lạ: 8 Số virus: 845

Số tập tin ẩn được phục hồi:

D2 Anti-Virus* Enterprise - Phát hiện tập tin lạ

Tập tin	Kích th...	Thời gian	Địa chỉ	Kết quả
Copy of Shortcut to (1)...	718	3/18/2012...	E:\	Đã cách ly
Copy of Shortcut to (2)...	630	3/18/2012...	E:\	Đã cách ly
Copy of Shortcut to (3)...	830	3/18/2012...	E:\	Đã cách ly
Copy of Shortcut to (4)...	917	3/18/2012...	E:\	Đã cách ly
oBbNdeoC.cpl	3584	3/18/2012...	E:\RECYCLER\5-2-0-28-0226724526...	Đã cách ly
HjsxPAQd.cpl	3584	3/18/2012...	E:\RECYCLER\5-2-0-28-0226724526...	Đã cách ly
RCdWKnxj.cpl	3584	3/18/2012...	E:\RECYCLER\5-2-0-28-0226724526...	Đã cách ly
hzr5qGFF.cpl	3584	3/18/2012...	E:\RECYCLER\5-2-0-28-0226724526...	Đã cách ly

Tổng số tập tin đã xử lý thành công: 8/8

Đổi tên Xóa bỏ Thoát



Kết quả ứng dụng MOC-MAV

- Giao tiếp MOC:
 - Gửi hàng ngàn mẫu đến MOC server bằng 1 thao tác click chuột
 - Nhận hàng ngàn phiếu kết quả kiểm tra từ MOC server
- Giao tiếp MAV:
 - Phân tích nhanh hàng ngàn phiếu đánh giá của MOC
 - Tách ngoại lệ, phân tích mẫu tự động bằng sandbox (Automated Malware Analysis), loại bỏ các phiếu mơ hồ, không tin cậy
 - Áp dụng hệ chuyên gia hỗ trợ ra quyết định
 - Hình thức hoá kết luận MOC, tương thích đặc tả tri thức MAV
 - Tối ưu tri thức, tích hợp, tăng trưởng CSTT
- Kết quả nghiên cứu: cập nhật 2000 - 3000 mẫu/ngày



Bàn luận về MOC-MAV

- Nhận xét về MOC:
 - Về mặt tổ chức, MOC là một ‘hội đồng tư vấn’ không có người điều hành, các thành viên hội đồng không có sự giao tiếp, thảo luận trong quá trình làm việc
 - Kết quả phiên làm việc của MOC là một checklist các ý kiến đánh giá độc lập, không có kết luận cuối cùng về tình trạng mẫu thử
- Vai trò của MAV:
 - Tổng hợp các ý kiến đánh giá từ MOC, kết hợp hệ chuyên gia hỗ trợ quyết định, MAV đóng vai trò chairman ra phán quyết cuối cùng của phiên họp
 - MOC-MAV thống nhất các ý kiến chuyên gia, nâng cao chất lượng MOC



Kết luận

- Mô hình ứng dụng MOC-MAV khai thác kinh nghiệm của các chuyên gia anti-virus, giúp đẩy nhanh tiến độ phân tích mẫu, góp phần giải quyết tình trạng mã độc lan tràn
- Trong vai trò chairman tổng hợp kiến thức chuyên gia, MAV đã hiện thực hoá mô hình Hội chẩn Mã độc Trực tuyến, làm tiền đề xây dựng “Trung tâm Tư vấn Chẩn đoán Mã độc” cho các Anti-virus ngày nay



Xin cảm ơn!

TS. Trương Minh Nhật Quang - 2013