Tội phạm công nghệ cao năm 2011 và định hướng phòng chống tấn công mạng của doanh nghiệp

Đại tá TS. Trần Văn Hòa
Phó cục trưởng
Cục cảnh sát phòng chống tội phạm sử dụng công nghệ cao

Hanoi – 2012

Nội dung chính:

1- Tình hình tội phạm công nghệ cao trong năm 2012

2- Xu hướng và dự báo tình hình tội phạm CNC trong thời gian tới

3- Giải pháp hướng dẫn doanh nghiệp phòng chống

Tình hình tội phạm công nghệ cao trong năm 2012

Một số hoạt động tấn công mạng nguy hiểm mới:

1- Tấn công bằng phần mềm gián điệp – trojan có chức năng:

+ Điều khiển từ xa;
+ Ghi thông tin gõ bàn phím;
+ Duyệt các file dữ liệu, lấy cắp thông tin;
+ Ghi log gửi qua email hoặc FTP;
+ Điều khiển bật webcam, chụp ảnh, chụp màn hình;
+ Mã hóa dữ liệu khi gửi đi;
+ Tự động cập nhật lệnh mới từ trung tâm điều khiển;
+ Quét các tập tin;
+ Chủ yếu lấy thông tin tài khoản ngân hàng.

Tình hình tội phạm công nghệ cao trong năm 2012

Một số trojan rất nguy hiểm, đang lây lan hiện nay là:

- Trojan “Sinh Tử Lệnh” lây qua phần mềm Unikey, tạo ra Botnet
- Zeus (phát tán rộng từ tháng 3 năm 2009)
- Spyeye (xuất hiện từ tháng 12 năm 2009)
- Trojan-Banker (xuất hiện từ tháng 9 năm 2009)
- Ainslot.L (xuất hiện từ tháng 9 năm 2011)

Tình hình tội phạm công nghệ cao trong năm 2012

- Một biến thể của ZeuS có tên là ZitMo: lây nhiễm vào điện thoại di động, để lấy cắp mã mTans, do ngân hàng gửi qua tin nhắn SMS tới điện thoại, để rút tiền từ tài khoản.

- Các Trojan này ở trạng thái “chờ” đến khi một dịch vụ ngân hàng trực tuyến được thực hiện, để lấy cắp thông tin thẻ tín dụng

Tình hình tội phạm công nghệ cao trong năm 2012

Tình hình tội phạm công nghệ cao trong năm 2012

- Mua bán lỗ hổng rất sôi động trên mạng
- Mua bán virus, trojan như Zues, Spyeye, thậm chí cả những mạng botnet để tấn công từ chối dịch vụ hoặc phát tán thư rác.
- Dữ liệu bị lấy cắp, kể cả thông tin thẻ ngân hàng, thông tin cá nhân, doanh nghiệp… cũng được rao bán công khai trên mạng

Ví dụ: thông tin chia sẻ trên FaceBook có thể bị hacker sử dụng vào mục đích tội phạm.

80% số người chia sẻ thông tin cá nhân của mình, để lộ thông tin bảo mật cho “bạn bè” trên FaceBook,

2- TẤN CÔNG CƠ SỞ DỮ LiỆU, WEBSITE

-Tấn công xâm nhập để lấy cắp, phá hoại dữ liệu xảy ra thường xuyên:
- Vụ tấn công website forum.bkav.com.vn ngày14/02/2012, cài đặt backdoor lên máy chủ, sao chép toàn bộ cơ sở dữ liệu của website vào 02 tập tin dump.sql và dump.zip và chia sẻ trên chính trang chủ website http://forum.bkav.com.vn/includes/dump.sql cho tải về tự do

2- TẤN CÔNG CƠ SỞ DỮ LiỆU, WEBSITE

Bốn phương pháp truy cập bất hợp pháp thường gặp:

1. Tấn công lỗ hổng bảo mật web SQL Injection, chủ yếu là tấn công deface, truy cập vào và sửa đổi dữ liệu của trang web.

2. Cài đặt sniffer trong mạng LAN, cài keylogger, spyware, bằng cách gửi email kèm theo attached file, quảng cáo kèm đường dẫn, sử dụng USB, sử dụng proxy..., lấy username, password của Admin,

3. Tấn công thông qua mạng nội bộ LAN, VPN,

4. Tấn công thông qua lỗ hổng bảo mật của các website sử dụng chung server hoặc chung hệ thống máy chủ của nhà cung cấp dịch vụ ISP, làm cầu nối tấn công đích.

2- TẤN CÔNG CƠ SỞ DỮ LiỆU, WEBSITE

Thể hiện cụ thể:

Năm 2011, trên 200 trang web của Việt Nam bị hacker nước ngoài tấn công:

-Phần lớn là những trang web của các đơn vị nhỏ, thuê host dùng chung, chạy trên hệ thống cũ,

- ISP không được cập nhật những bản vá cần thiết, có nhiều lỗi thông thường, dễ bị tấn công bằng các phương pháp và công cụ phổ biến.

2- TẤN CÔNG CƠ SỞ DỮ LiỆU, WEBSITE

Đối tượng trong nước và nước ngoài cấu kết tấn công, sử dụng công nghệ mới để tránh bị phát hiện như:

- Tấn công qua trung gian-Proxy;
- Tấn công lỗ hổng bảo mật web,
- Lợi dụng lỗ hổng bảo mật từ nội bộ, truy cập không dây, internet công cộng, di động với Ipv6,

Ví dụ:

Vụ hacker tấn công vào hệ thống server của Công ty bảo hiểm AAA tháng 4 năm 2011, xóa toàn bộ cơ sở dữ liệu, kể cả hệ thống backup (chỉ backup online 1 lần trong 1 tuần)

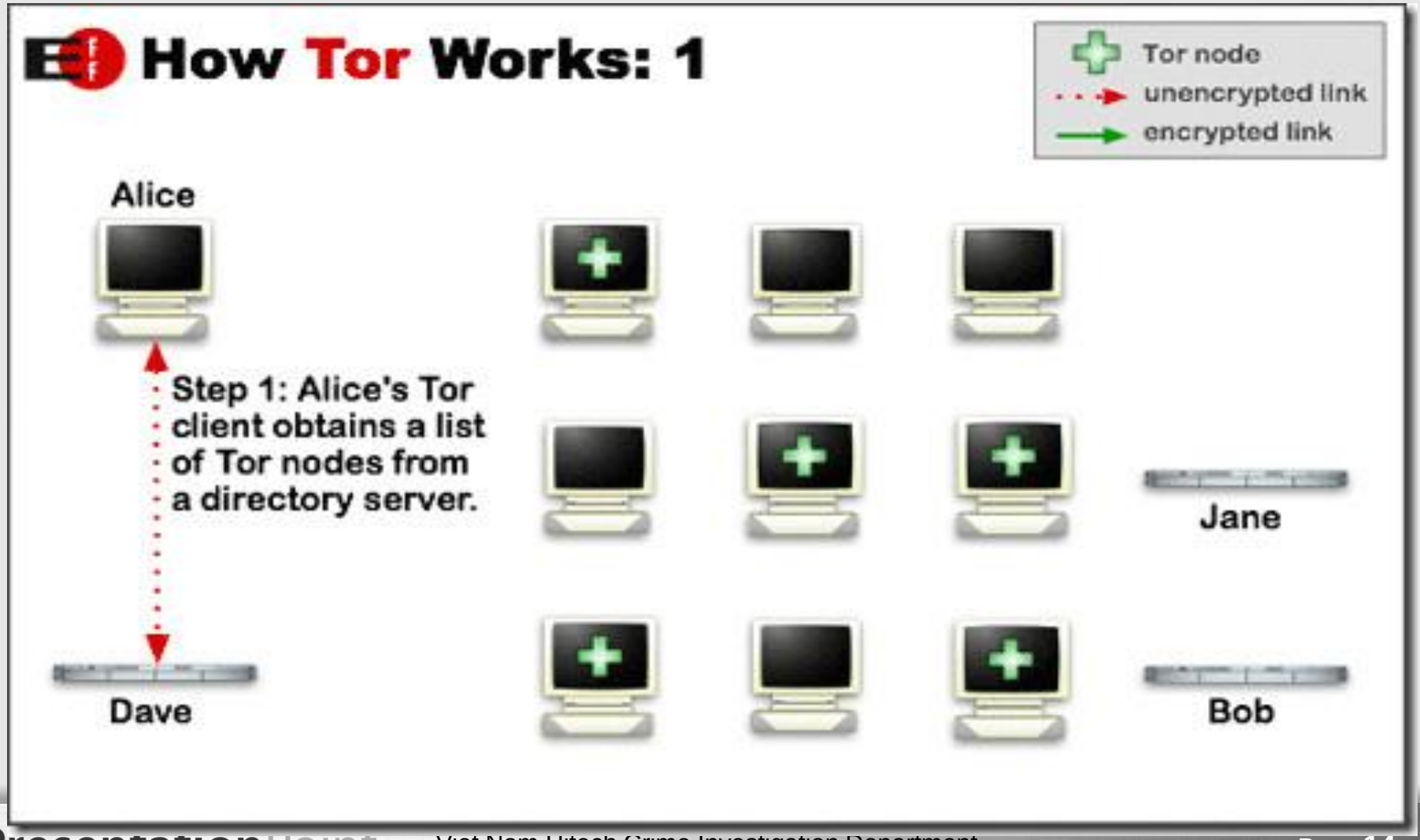
2- SỬ DỤNG PROXY TẤN CÔNG CƠ SỞ DỮ LiỆU, WEBSITE

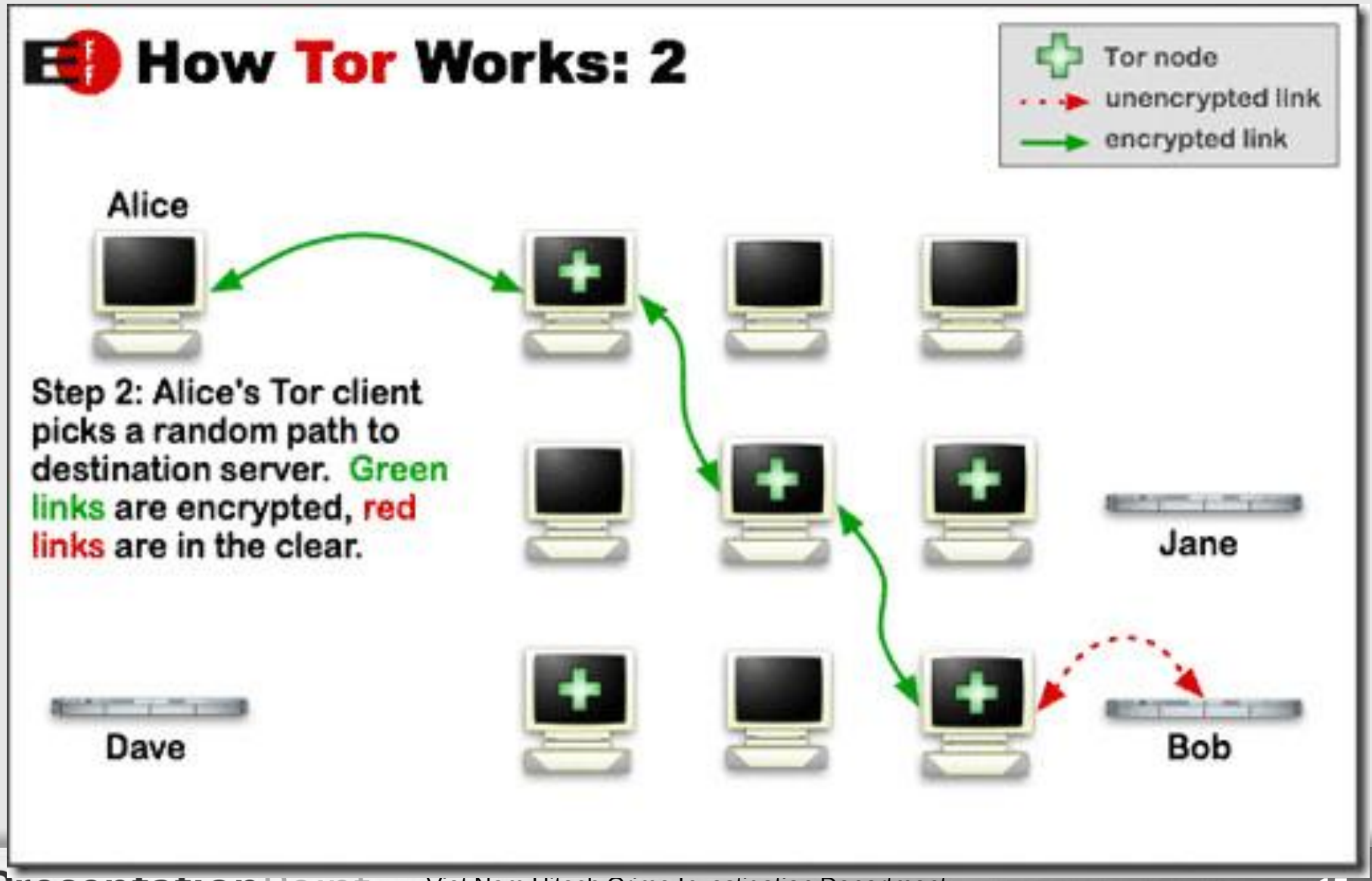
- Sử dụng công cụ TOR để tấn công: là proxy che dấu địa chỉ IP thật bằng cách liên tục thay đổi việc sử dụng các máy chủ proxy khác nhau.

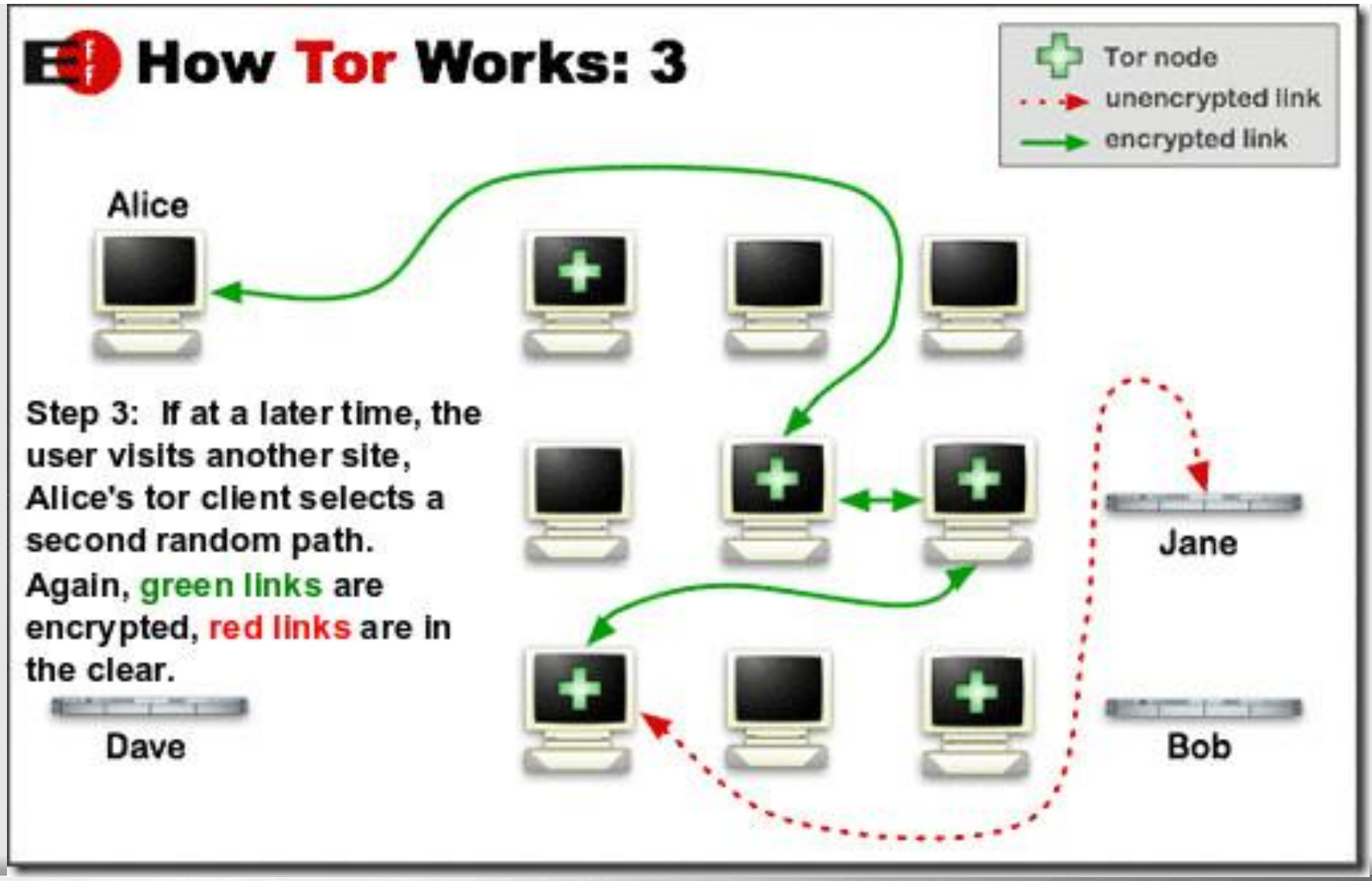
- Vụ hacker sử dụng công cụ Tor, để xâm nhập vào cơ sở dữ liệu của máy chủ web. Một đối tượng tấn công, nhưng khoảng 10 phút, IP lại thay đổi sang các quốc gia khác nhau, với logfile như sau:

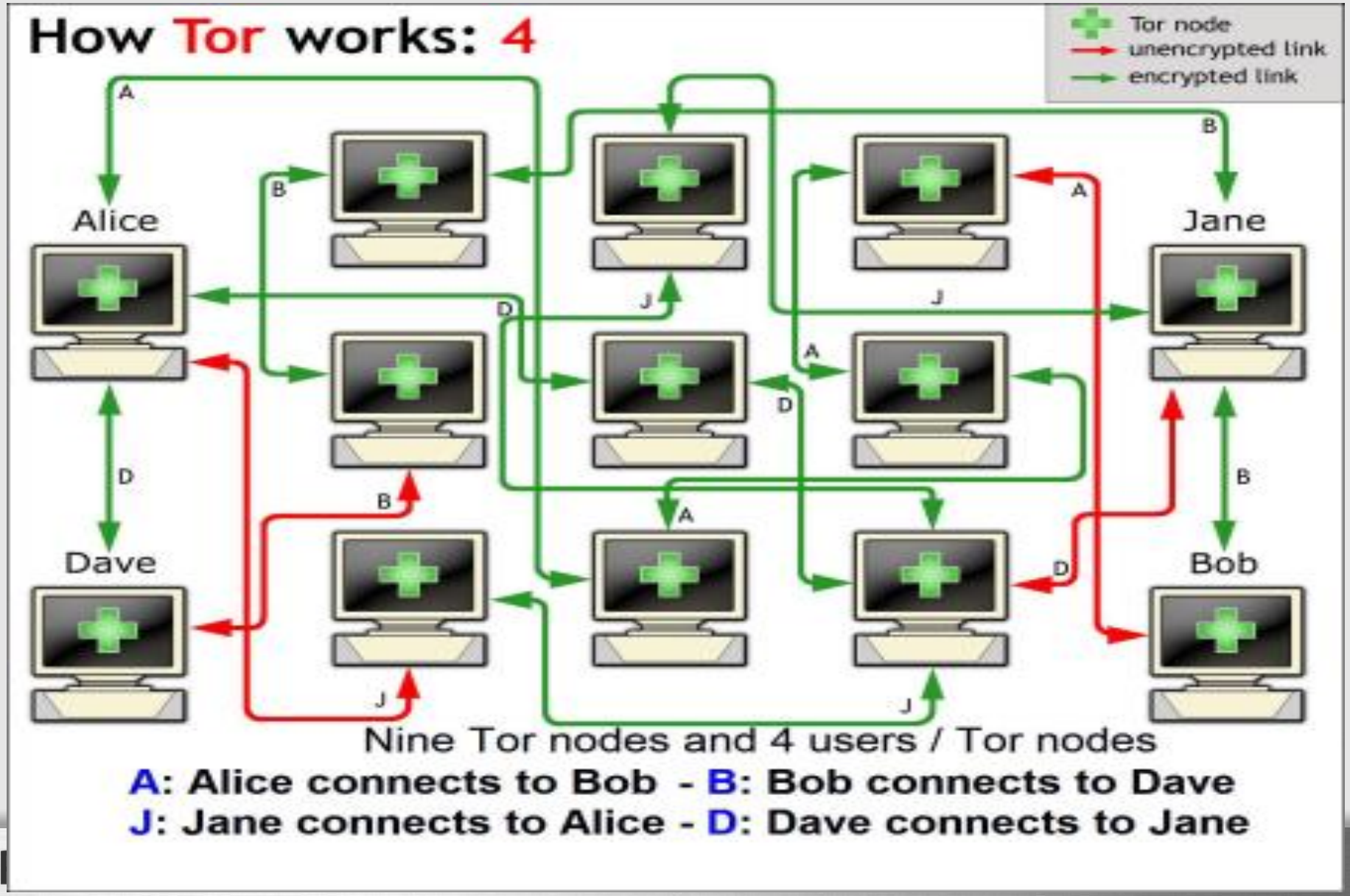
2- SỬ DỤNG PROXY TẤN CÔNG CƠ SỞ DỮ LiỆU, WEBSITE

- Sử dụng công cụ TOR

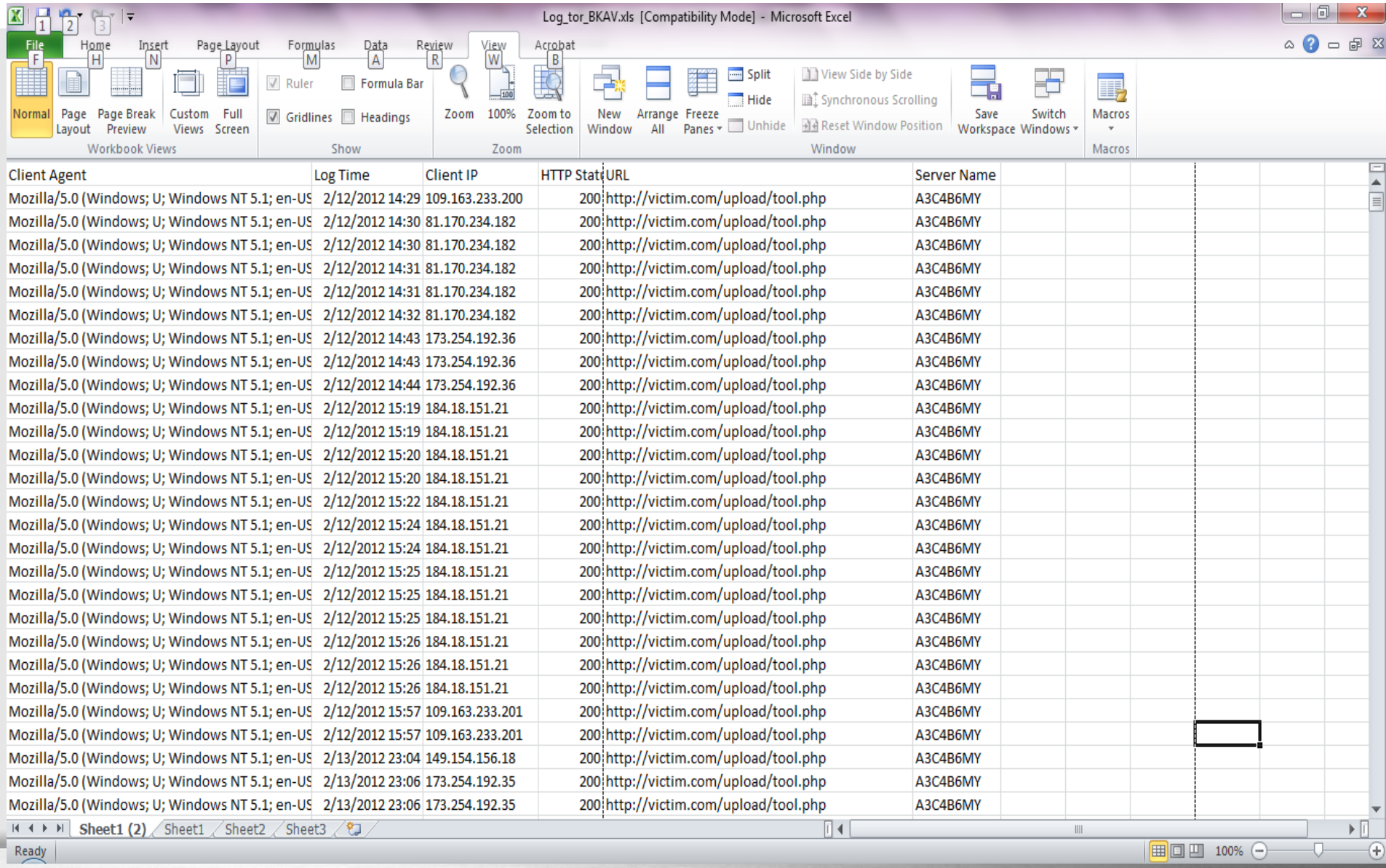



How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.
Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob


How Tor works: 4
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob
A
B
D
J
Nine Tor nodes and 4 users / Tor nodes
A: Alice connects to Bob - B: Bob connects to Dave
J: Jane connects to Alice - D: Dave connects to Jane

-Tấn công đã sử dụng phần mềm TOR



Client Agent	Log Time	Client IP	HTTP Stat	URL	Server Name
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:29	109.163.233.200	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:30	81.170.234.182	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:30	81.170.234.182	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:31	81.170.234.182	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:31	81.170.234.182	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:32	81.170.234.182	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:43	173.254.192.36	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:43	173.254.192.36	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 14:44	173.254.192.36	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:19	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:19	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:20	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:20	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:22	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:24	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:24	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:25	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:25	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:25	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:26	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:26	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:26	184.18.151.21	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:57	109.163.233.201	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/12/2012 15:57	109.163.233.201	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/13/2012 23:04	149.154.156.18	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/13/2012 23:06	173.254.192.35	200	http://victim.com/upload/tool.php	A3C4B6MY
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US	2/13/2012 23:06	173.254.192.35	200	http://victim.com/upload/tool.php	A3C4B6MY

Một số vụ tấn công với virus Sinh Tử Lệnh

Thủ đoạn nhúng virus vào phần mềm phổ biến ở Việt Nam do nhóm hacker với biệt danh “Sinh Tử Lệnh” sử dụng để tấn công nhiều vụ trong năm 2011:

- Sáng ngày 1/3/2012 ,website http://unikey.org/ đã bị tin tặc trỏ các link tải phần mềm Unikey về một website giả SourceForge.net.
- Các file của Unikey ở website chứa virus “Sinh Tử Lệnh”, tạo thành mạng Botnet, điều khiển bởi virus hosting tại nước ngoài.
- Có các chức năng điều khiển từ xa, backdoor, keylogger, lấy cắp thông tin, tấn công DDOS
- Hacker đã sử dụng virus Sinh Tử Lệnh nhiều lần tấn công bkav.com.vn, vietnamnet.vn

Tổng hợp thông tin về tập lệnh của Sinh Tử Lệnh

Mã lệnh	Mô tả	Tham số
101	Load 1 dll	In: Dll ID
105	Enum windows title	Out: "%Temp% \ ypt*.tmp"
106	Post WM_CLOSE message	In: Process ID
107	Liệt kê các process đang chạy	Out: %Temp%
108	Terminate process theo Pid	In: Process ID
109	Terminate process theo Name	In: Process name
110	Upload file lên FTP server	In: Đường dẫn đến file cần lấy (FTP server, username, password chưa debug ra)
111	Giải mã và chạy 1 file exe	In: Đường dẫn đến file bị mã hóa
112	Chụp hình qua webcam, ghi ra file	In: Đường dẫn
113	Kiểm tra sự tồn tại webcam driver	Out: có/không
114	Quay video bằng webcam, ghi ra file	In: Đường dẫn
115	Tạo file (nội dung trắng)	In: Đường dẫn
125	Write dữ liệu ra pipe (\\.\pipe\NannedPipe)	In: Dữ liệu cần write
126	Gửi danh sách các phần mềm cài đặt trên máy về server	
127	Reboot system	
128	Shutdown system	
131	Liệt kê danh sách các ổ đĩa	In: Đường dẫn tới file log
132	Lấy clipboard	
133	Create pipe (\\.\pipe\NannedPipe)	
136	Suspend 1 thread theo ThreadID	In: ThreadID
139	Giải mã dll và đăng ký service dll	In: %Dll Path%
151	Hook bàn phím (kelogger)	
140	Update	In: Link update
401	Xóa 1 file theo Dll ID	Tham chiếu bảng Dll ID

Điều tra vụ tấn công vietnamnet.vn

Vụ tấn công DDOS vietnamnet.vn, sử dụng virus *oxdex.com/logo.jpg:*

- hacker cấy virus *oxdex.com/logo.jpg* vào file unikey40RC2-1101-win32.zip và đã tải lên trang http://***.com.vn/
- virus nhận lệnh điều khiển từ một server tại Anh tại địa chỉ http://oxdex.com/logo.jpg, địa chỉ IP 178.162.225.254 của nhà cung cấp dịch vụ Internet Santrex.
- C50 đã đề nghị Cảnh sát Anh hỗ trợ xác minh thông tin liên quan đến máy chủ có địa chỉ IP 178.162.225.254 tại Anh,

Đây chính là virus “Sinh Tử Lệnh”

Tội phạm gian lận thẻ ngân hàng

Lấy cắp, mua bán thông tin thẻ ngân hàng:

1- Tấn công truy cập vào các website mua bán hàng trực tuyến để lấy cắp thông tin thẻ ngân hàng

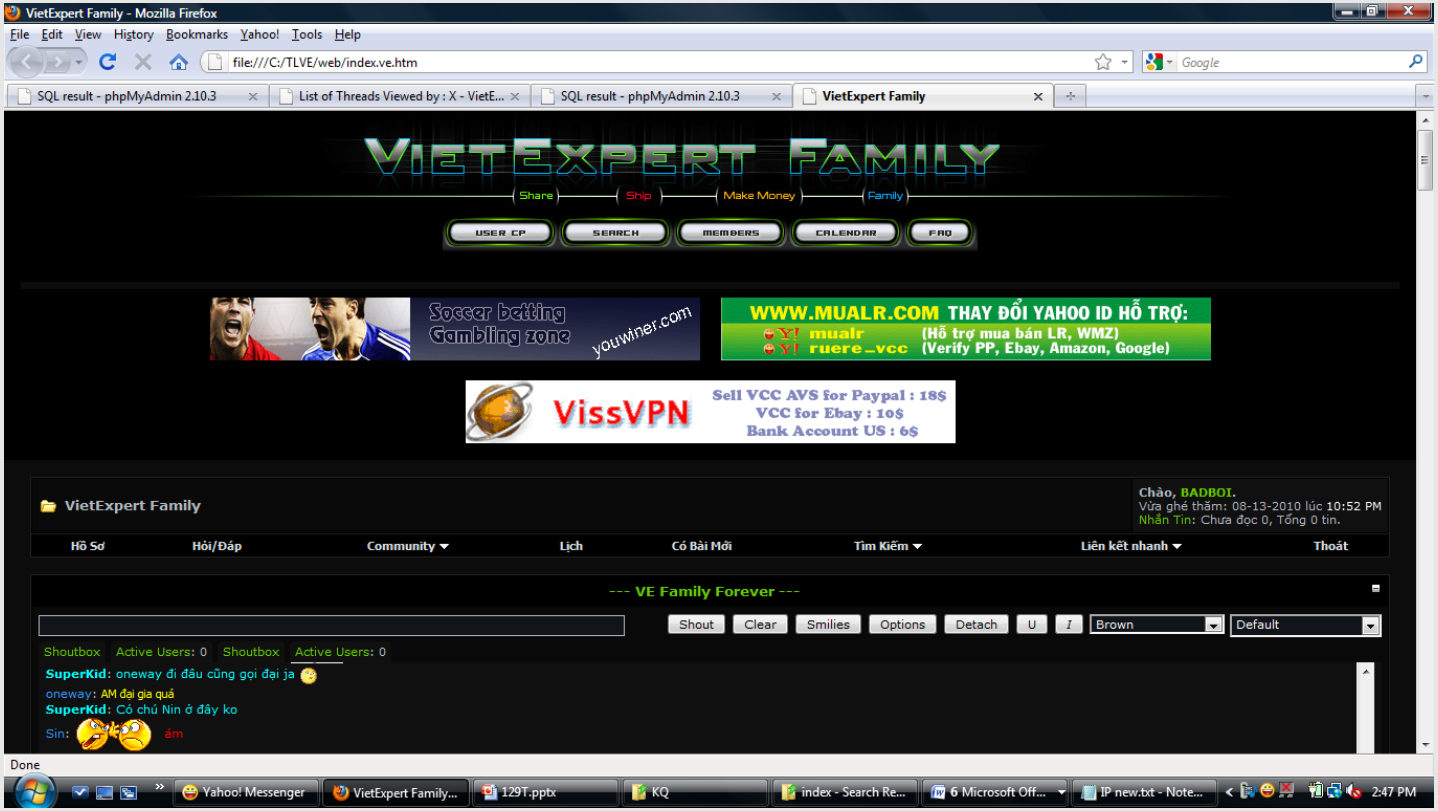
2- Phishing,

3- Mua bán thông tin thẻ ngân hàng trên mạng (website UG)

4- Sử dụng Keylogger, spyware… để lấy cắp thông tin thẻ ngân hàng

5- Skimming

Diễn đàn tội phạm mạng ww.Vefamily.com
Giao diện forum



GiẢI PHÁP PHÒNG CHỐNG CỦA DOANH NGHIỆP

-Nhận thức đe dọa bảo mật trong các DN vừa và nhỏ năm 2011 cho thấy, phần lớn DN chưa quan tâm đến bảo mật.
- Thiếu các biện pháp phòng ngừa để bảo vệ dữ liệu.

GiẢI PHÁP PHÒNG CHỐNG CỦA DOANH NGHIỆP

Một số giải pháp an ninh mạng:

- Cập nhật các bản vá trên hệ điều hành: *Hầu hết máy chủ của các ISP cho thuê đều sử dụng chung một bản hệ điều hành và thường không hỗ trợ cập nhật các bản vá định kỳ, là nguyên nhân chính làm cho các website thuê dịch vụ bị tấn công hàng loạt.*
- Bị lỗi SQL injection, do lập trình không chú trọng đến bảo mật, hầu hết đều có lỗi SQL injection.
- Áp dụng ngay một hệ thống firewall: phần lớn website hosting tại một vài ISP lớn như VDC, Hostvn.net, MatBao, PA Việt Nam và nếu dùng chung webserver, sẽ dễ bị tấn công.
- Server thường không được cofig để chống lại DOS. Khi bị tấn công DDOS và sử dụng chung SQL server, thì không thể chống đỡ khi bị tấn công DDOS.

Một số giải pháp phòng ngừa của Doanh nghiệp

Doanh nghiệp có mạng máy tính riêng phải tập trung giải quyết đồng bộ 3 vấn đề:

1- Xây dựng cơ sở hạ tầng công nghệ: Hệ thống thiết bị, phần mềm an toàn thông tin:

- hệ thống firewall,
- thiết bị phát hiện và ngăn chặn xâm nhập, công cụ dò quét lỗ hổng bảo mật, thiết bị giám sát an ninh mạng, phần mềm chống mã độc...,
- Đánh giá mức an toàn của hệ thống theo định kỳ, Cập nhật bản vá,
- Bảo mật dữ liệu lưu trữ và dữ liệu trên đường truyền,

Một số giải pháp phòng ngừa của Doanh nghiệp

2- Xây dựng các Quy trình:
- Quy trình đánh giá các thiết bị,
- Quy trình kiểm tra các lỗ hổng an ninh,
- Quy trình phản ứng, xử lý các sự cố, nguy cơ về an toàn TT,
- Quy trình giám sát và kiểm soát truy cập,
- Quy trình sao lưu dữ liệu,
- Quy trình kiểm tra và đảm bảo hoạt động liên tục của hệ thống,
- Quy trình gửi nhận thông tin trên mạng chuyên dùng,
- Quy trình nâng cấp hệ thống mạng;
- Quy trình quản lý người sử dụng;
- Xây dựng hệ thống: Quản trị an ninh tổ chức (Enterprise security management - ESM) và Quản trị rủi ro tổ chức (Enterprise risk management - ERM).

Một số giải pháp phòng ngừa của Doanh nghiệp

3- Quản lý con người:
- Đội ngũ chuyên trách,
- Đào tạo nâng cao nghiệp vụ,

4- Ứng dụng công nghệ phòng ngừa cho hệ thống máy chủ:
- Luôn có hệ thống tường lửa (Firewalls);
- Sử dụng mật mã (Cryptography);
- Sử dụng mật khẩu sử dụng 1 lần
- Có công cụ phân tích khả năng bị tấn công.

Một số giải pháp phòng ngừa của Doanh nghiệp

Những đơn vị lớn, cần đầu tư:
- Hệ thống phát hiện xâm nhập IDS (Intrusion detection system)
- Hệ thống ngăn ngừa xâm nhập IPS (Intrusion prevention system)
- Công nghệ phát hiện (Detection Technology): để ghi lại các dấu vết bị tấn công, chống xâm nhập bất hợp pháp, chống các loại virus, phần mềm gián điệp (như keylogger, trojan horse, điều khiển từ xa, backdoor), hệ thống lọc IP chống DDOS.

Vietnam Hightech Crime Police Department

Thank you

http://www.hitechcrime.vn

hoatv@hitechcrime.vn