

Số: /BC-CATTT

Hà Nội, ngày tháng năm 2020

## BÁO CÁO KỸ THUẬT

### Tình hình an toàn thông tin tháng 09/2020 và thống kê kết nối chia sẻ của các Tỉnh/Thành

#### 1. Tin tức nổi bật về an toàn thông tin

**Cảnh báo: Cấu hình mặc định của thiết bị FortiGate VPN cho phép đối tượng tấn công chặn bắt dữ liệu MitM.**

Các nhà nghiên cứu cho biết cấu hình mặc định SSL-VPN có vấn đề về chứng chỉ. Theo dõi, hơn 230.000 thiết bị FortiGate dễ bị tấn công bằng chức năng VPN. Trong số đó, 88% hoặc hơn 200.000 doanh nghiệp, đang sử dụng cấu hình mặc định và có thể dễ dàng tấn công MitM.



**Cảnh báo: Hơn 25 lỗi có ảnh hưởng lớn trong hệ điều hành, phần mềm IOS và IOS XE của Cisco.**

Hãng đã đưa ra cảnh báo và đề nghị cập nhật cho hàng chục lỗ hổng bảo mật mức độ nghiêm trọng cao, cho phép đối tượng tấn công từ xa có thể xác thực và sử dụng giao diện người dùng web trên thiết bị.

**Cảnh báo: Microsoft đã phát hiện các cuộc tấn công đang hoạt động tận dụng lỗ hổng Zerologon.**

Zerologon là lỗi nguy hiểm được tiết lộ trong năm nay. Trung tâm NCSC đã cảnh báo về lỗ hổng bảo mật này tại công văn số 797/CATTT-NCSC ngày 15/09/2020.



### ZeroLogon

Detection & Prevention  
CVE-2020-1472

**Hạ viện Hoa Kỳ đã thông qua 4 dự luật nhằm đảm bảo lưới điện và cơ sở hạ tầng năng lượng chống lại các cuộc tấn công mạng.**

Tất cả bốn dự luật hiện chuyển đến Thượng viện để xem xét. Các biện pháp đã được phê duyệt đều nhằm đến mục tiêu bảo vệ mạng của lưới điện an toàn.



**Google xóa 17 ứng dụng Android bị phát hiện tham gia gian lận thanh toán khỏi của hàng GG Play.**

17 ứng dụng được phát hiện bởi các nhà nghiên cứu bảo mật từ Zscaler đã bị nhiễm phần mềm độc hại Joker (hay còn gọi là Bread) đã xuất hiện từ năm 2017.

**Tổng thống Putin đề xuất ký kết Hiệp ước không can thiệp bầu cử với Hoa Kỳ.**

Trước đó, nhiều lần Nga đã bác bỏ mọi cáo buộc can thiệp vào bầu cử, thay vào đó cáo buộc các nhà lãnh đạo phương Tây tiến hành một cuộc chiến tranh thông tin sai lệch chống lại Nga.



### **Trong tháng 09:**

- Trong tháng 09/2020 có **02 tỉnh (Yên Bái, Cao Bằng)** đã cập nhật, bổ sung danh sách địa chỉ IP tĩnh cần theo dõi giám sát từ xa về Trung tâm Giám sát an toàn không gian mạng quốc gia.

- Trong tháng có **04 tỉnh (Trà Vinh, Hà Giang, Khánh Hòa, Hà Nam)** đã thực hiện kết nối chia sẻ thông tin về mã độc. Đến hết tháng 9/2020 đã có **51/63** các đơn vị ở tỉnh/thành thực hiện kết nối chia sẻ thông tin về mã độc với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin theo Chỉ thị 14/CT-TTg ngày 25/5/2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại.

Ngoài ra có **05 tỉnh (Kiên Giang, Hà Nam, Hà Giang, Khánh Hòa, Trà Vinh)** tiếp tục cung cấp chia sẻ, mở rộng kết nối với Trung tâm Giám sát an toàn không gian mạng quốc gia.

- Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia theo dõi vẫn còn nhiều máy tính vẫn tồn tại nhiều lỗ hổng bảo mật đã có hướng dẫn khắc phục (Danh sách tại Phụ lục 2). Đề nghị Sở TTTT các tỉnh đơn đốc và hỗ trợ các đơn vị trên địa bàn mình quản lý thực hiện vá lỗ hổng để ngăn chặn sớm các nguy cơ tấn công mạng thông qua các lỗ hổng này, đặc biệt là các lỗ hổng đã và đang được các nhóm tấn công lợi dụng để thực hiện tấn công APT nguy hiểm.

## **2. Tình hình lây nhiễm mã độc tại một số địa phương**

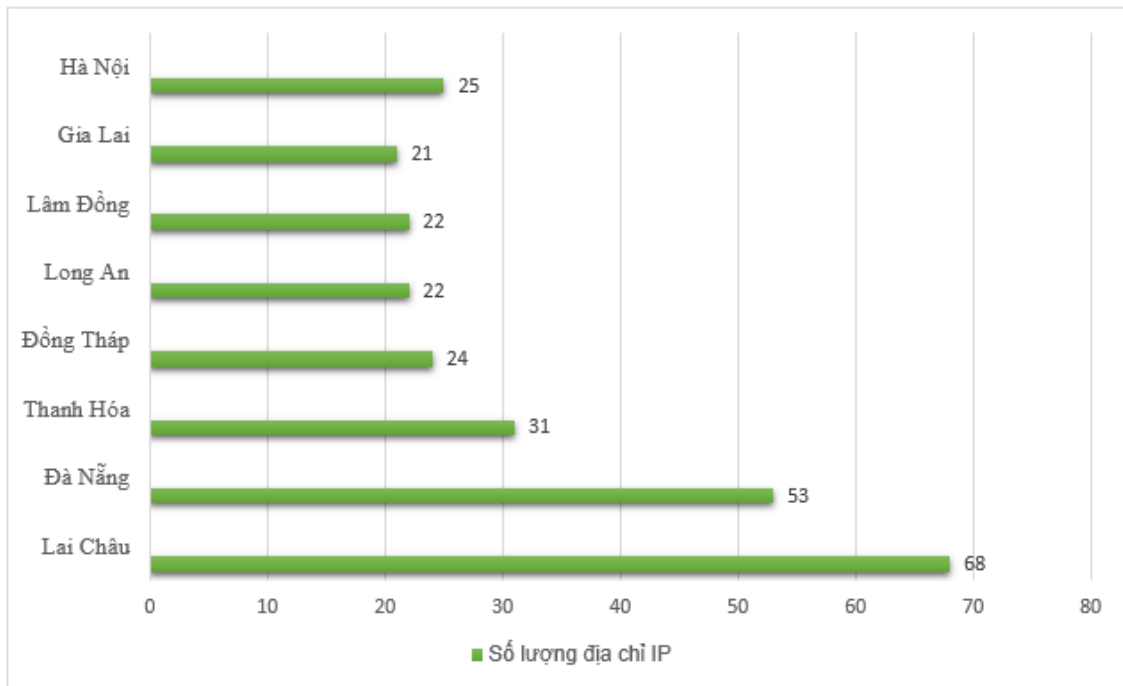
Để hỗ trợ Đơn vị chuyên trách về ATTT, Sở TT&TT tại các địa phương trên cả nước sớm nắm bắt được tình hình lây nhiễm mã độc, hoạt động của các mạng máy tính ma (botnet) một cách độc lập, không phụ thuộc vào giải pháp kỹ thuật đã triển khai, Cục An toàn thông tin (ATTT) đã triển khai Hệ thống giám sát từ xa tại Trung tâm Giám sát an toàn không gian mạng quốc gia. Thông tin giám sát từ Hệ thống có thể tham khảo, sử dụng để đánh giá hiệu quả giải pháp giám sát, phòng chống mã độc tập trung đang triển khai tại địa phương. Hiện nay, tài khoản truy cập hệ thống đã được Cục ATTT cấp cho Lãnh đạo các đơn vị chuyên trách.

Việc giám sát mã độc được Hệ thống giám sát từ xa thực hiện dựa trên danh sách địa chỉ IP tĩnh, public do Sở TT&TT tại địa phương cung cấp. Việc giám sát không tương tác với hệ thống mạng nội bộ do đó không làm ảnh hưởng tới hiệu năng và lưu lượng mạng và hoạt động của hệ thống thông tin. Ngoài ra,

hoạt động giám sát từ xa còn hỗ trợ phát hiện các nguy cơ, rủi ro, điểm yếu của hệ thống trên các Dải địa chỉ IP/Tên miền của cơ quan; và tài khoản lộ lọt thông tin và nhiều nguy cơ khác.

Đến tháng 09/2020, Trung tâm Giám sát an toàn không gian mạng quốc gia đã phối hợp với Sở TT&TT các tỉnh thành, thực hiện theo dõi, giám sát mã độc từ xa cho **63/63** tỉnh thành và phát hiện có nhiều địa chỉ IP sử dụng trong cơ quan nhà nước ở các tỉnh thành nằm trong các mạng botnet.

### *Tình hình lây nhiễm mã độc tại một số địa phương tháng 09/2020<sup>1</sup>*



### **DANH SÁCH MÃ ĐỘC TẠI MỘT SỐ ĐỊA PHƯƠNG**

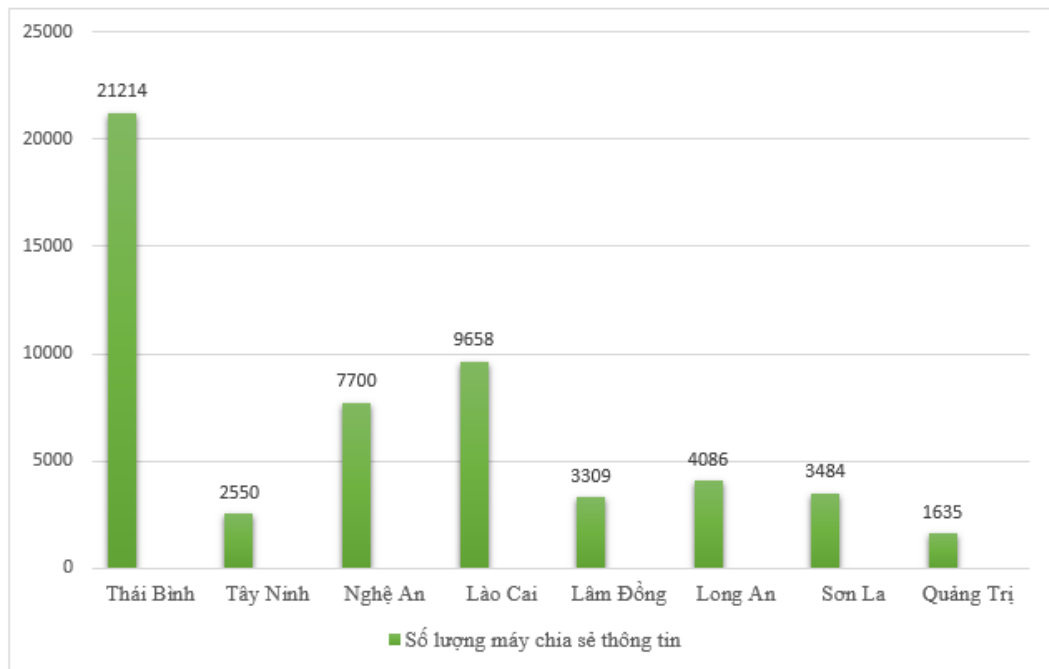
Địa phương	Tên mã độc
<b>Lai Châu</b>	Avalanche, Conficker, Stealrat, Sality
<b>Thanh Hóa</b>	Conficker, Lokibot, Shauth, Gamut, Minerpanel
<b>Lạng Sơn</b>	Iotbotnet, Stealrat, Necurs, Sality, Wannacry
<b>Lâm Đồng</b>	Smokerloader, Avalanche
<b>Hà Nam</b>	Avalanche, Conficker, Sality

### 3. Tình hình chia sẻ dữ liệu theo Chỉ thị 14/CT-Ttg 2018

Bên cạnh Hệ thống giám sát từ xa dựa trên dải địa chỉ IP tĩnh do các địa phương cung cấp, Cục ATTT hiện đã triển khai kết nối chia sẻ thông tin theo chỉ đạo tại Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 25/5/2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại. Để được hỗ trợ kỹ thuật, các địa phương cần chia sẻ thông tin về Trung tâm Giám sát an toàn không gian mạng quốc gia. Hướng dẫn kết nối chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật tại văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.

Trong tháng 09/2020, đã có **51/63** địa phương kết nối với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Tổng số máy tính chia sẻ thông tin về mã độc là **98.151** máy.

#### TOP ĐỊA PHƯƠNG CHIA SẺ DỮ LIỆU MÃ ĐỘC



Trung tâm Giám sát an toàn không gian mạng quốc gia sẽ thường xuyên giám sát, cảnh báo nguy cơ, đánh giá và hỗ trợ và các điểm yếu lỗ hổng đối với những địa phương đã kết nối dữ liệu tới Hệ thống Chia sẻ thông tin mã độc (MIS – Malware Information Sharing) tại địa chỉ: <https://mis.ais.gov.vn>.

Trong tháng 09/2020, Hệ thống MIS của Trung tâm Giám sát an toàn không gian mạng quốc gia đã ghi nhận có **2.278** điểm yếu, lỗ hổng an toàn thông tin

tại các hệ thống thông tin của cơ quan nhà nước. Lỗ hổng gây mất an toàn thông tin tồn tại trên nhiều máy tính đã kết nối, chia sẻ thông tin.

Số lượng điểm yếu, lỗ hổng nêu trên là rất lớn, do đó Cục ATTT đã chỉ đạo Trung tâm Giám sát an toàn không gian mạng quốc gia triển khai đánh giá, xác định các lỗ hổng nguy hiểm, có ảnh hưởng trên diện rộng và hướng dẫn các cơ quan, tổ chức khắc phục. Đặc biệt có một số lỗ hổng đã và đang được các nhóm tấn công lợi dụng để thực hiện tấn công APT. Danh sách lỗ hổng đã có hướng dẫn trang phụ lục kèm theo. Dưới đây là 03 lỗ hổng vẫn còn tồn tại trên nhiều máy tính, chưa được xử lý và khắc phục.

Tên lỗ hổng	Số máy có lỗ hổng tháng 8	Số máy có lỗ hổng tháng 9	Mô tả tóm tắt	Ghi chú
CVE-2019-0708	6.396	3921	Lỗ hổng trong dịch vụ Remote Desktop của hệ điều hành Windows	Tham khảo Báo cáo tháng 8/2019
CVE-2013-3900 (MS13-098)	5.270	3.206	Lỗ hổng trong hệ điều hành Windows	Tham khảo Báo cáo tháng 8/2019
CVE-2015-0009 (MS15-014)	4.961	3.043	Lỗ hổng trong Group Policy của Microsoft Windows cho phép đối tượng tấn công truy cập trái phép.	Tham khảo Báo cáo tháng 9/2019

Nhằm đảm bảo an toàn hệ thống, đề nghị các Cán bộ chuyên trách ATTT thực hiện rà soát, đánh giá các thiết bị tại cơ quan, tổ chức của mình để xác định lỗ hổng và tiến hành “Vá” lỗ hổng theo hướng dẫn.

Để có thông tin về điểm yếu, lỗ hổng tồn tại trong hệ thống của các cơ quan, tổ chức trực thuộc địa phương, Sở TT&TT có thể liên hệ với Trung tâm Giám sát an toàn không gian mạng quốc gia để được chia sẻ./.

***Nơi nhận:***

- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

**KT. CỤC TRƯỞNG  
PHÓ CỤC TRƯỞNG**

**Nguyễn Khắc Lịch**

**Phụ lục 1**  
**Danh sách các đơn vị chưa triển khai giải pháp phòng chống**  
**mã độc đáp ứng yêu cầu của Chỉ thị số 14/CT-TTg năm 2018**  
 (Chưa kết nối chia sẻ dữ liệu về Cục ATTTT)

STT	Tỉnh/Thành	STT	Tỉnh/Thành
1	Bắc Kạn	7	Phú Thọ
2	Bình Dương	8	Yên Bái
3	Đồng Tháp	9	Nam Định
4	Hà Tĩnh	10	Ninh Thuận
5	Hòa Bình	11	Quảng Bình
6	Quảng Nam	12	Thái Nguyên

**Ghi chú:** Thông tin về các bộ ngành, địa phương chưa thực hiện kết nối chia sẻ thông tin về mã độc sẽ được Cục ATTTT tổng hợp, báo cáo hàng tháng nhằm đôn đốc việc thực hiện chỉ tiêu mà Chính phủ đưa ra tại Nghị quyết 01/NQ-CP ngày 01/01/2020 của Chính phủ.

Cụ thể: "90% các bộ, ngành, địa phương kết nối với Trung tâm Giám sát an toàn không gian mạng quốc gia".

## Phụ lục 2

## Danh sách điểm yếu lỗ hổng phổ biến đã có hướng dẫn kỹ thuật

STT	Mã điểm yếu/ lỗ hổng	Ghi chú
1	CVE-2019-0708	Tham khảo Báo cáo tháng 8/2019
2	CVE-2013-3900 (MS13-098)	Tham khảo Báo cáo tháng 8/2019
3	CVE-2014-4114 (MS14-060)	Tham khảo Báo cáo tháng 8/2019 <b>Sandworm APT</b>
4	CVE-2015-0009 (MS15-014)	Tham khảo Báo cáo tháng 9/2019
5	CVE-2015-1635 (MS15-034)	Tham khảo Báo cáo tháng 9/2019
6	CVE-2015-0084 (MS15-028)	Tham khảo Báo cáo tháng 9/2019
7	CVE-2014-0315 (MS14-019)	Tham khảo Báo cáo tháng 10/2019
8	CVE-2017-0144 (MS17-010)	Tham khảo Báo cáo tháng 10/2019
9	CVE-2013-3129 (MS13-053)	Tham khảo Báo cáo tháng 11/2019
10	CVE-2015-0073 (MS15-025)	Tham khảo Báo cáo tháng 11/2019
11	CVE-2015-0080 (MS15-024)	Tham khảo Báo cáo tháng 11/2019
12	CVE-2015-0076 (MS15-029)	Tham khảo Báo cáo tháng 12/2019
13	CVE-2013-3940 (MS13-089)	Tham khảo Báo cáo tháng 12/2019
14	CVE-2015-0012 (MS15-017)	Tham khảo Báo cáo tháng 12/2019
15	CVE-2014-0260 (MS14-001)	Tham khảo Báo cáo tháng 01/2020
16	CVE-2014-1818 (MS14-036)	Tham khảo Báo cáo tháng 01/2020
17	CVE-2014-6352 (MS14-064)	Tham khảo Báo cáo tháng 01/2020 <b>Moonsoon APT</b>
18	CVE -2014-0263 (MS14-007)	Tham khảo Báo cáo tháng 02/2020
19	CVE-2014-4148 (MS14-058)	Tham khảo Báo cáo tháng 02/2020 <b>APT 31</b>



20	CVE-2015-0078 (MS15-023)	Tham khảo Báo cáo tháng 02/2020
21	CVE-2008-4250 (MS08-067)	Tham khảo Báo cáo Tháng 03/2020 <b>Silence APT</b>
22	CVE-2014-2778 (MS14-034)	Tham khảo Báo cáo Tháng 03/2020
23	CVE-2013-3891 (MS13-086)	Tham khảo Báo cáo Tháng 03/2020

**Phụ lục 3**  
**Thông tin về các loại mã độc/botnet**

Tên gọi	Một số IP – Tên miền	Mô tả
<b>Avalanche</b> <b>(Win32/Gamarue)</b>	somicrososoft.ru morphed.ru a.deltaheavy.ru hzmksreiuojoy.in devicesta.ru designthefuture.ru andall.andddddzandddd2.com ochengorit.ru and32.microscobisoftng5.com letstryitnowx.online cp.4jhlti79.ru cp.oa505txz.ru cp.qc0zt6eo.ru cp.4nbizac8.ru b.deltaheavy.ru c.deltaheavy.ru cp.x1yuqjh9.ru and19.themarket12345sushi3.com cp.ekic4bf5.ru	<ul style="list-style-type: none"> <li>- Thời gian xuất hiện: Năm 2011.</li> <li>- Mục tiêu tấn công: Doanh nghiệp sử dụng thẻ thanh toán.</li> <li>- Các chức năng chính như: Keylogging; Rootkit; Truy cập từ xa ẩn; Thu thập thông tin đăng nhập từ trình duyệt.</li> <li>- Mục đích chính là phát tán các dòng mã độc khác nhằm phục vụ các cuộc tấn công phần mềm độc hại toàn cầu. Mạng botnet Andromeda bao gồm và có liên quan đến ít nhất 80 họ phần mềm độc hại, trong đó chủ yếu là họ mã độc Point of Sale (POS), ví dụ như GamaPOS.</li> </ul>
<b>SmokeLoader</b>	173.231.184.57 173.231.184.5 206.189.61.126 ukcompany.me ukcompany.pw ukcompany.top	<ul style="list-style-type: none"> <li>- Thời gian xuất hiện: Năm 2011 và đã từng tham gia trong các chiến dịch email giả mạo, với tần suất không thường xuyên nhưng vẫn tiếp tục được phát triển. Xuất hiện từ đầu tháng 01/2018, Meltdown và Specter là hai phương pháp tấn</li> </ul>

		<p>công qua kênh mới nhắm vào bộ vi xử lý hiện đại và được cho là ảnh hưởng đến hàng tỷ thiết bị. Đây là các lỗ hổng ở cấp CPU, cho phép các ứng dụng độc hại truy cập vào dữ liệu khi đang được xử lý, bao gồm mật khẩu, ảnh, tài liệu, email và những thứ tương tự. Mã độc Smoke Loader đặc biệt hoạt động mạnh trong suốt năm 2018 với nhiều chiến dịch phát tán Smoke Loader qua các bản vá lỗi giả mạo dành cho lỗ hổng Meltdown và Spectre.</p>
<p><b>Conficker</b></p>	<p>149.93.100.83  149.93.123.143  149.93.131.229  149.93.132.110  149.93.138.146  149.93.149.250  149.93.154.218  149.93.155.237  149.93.16.132  149.93.16.142  149.93.170.119  149.93.173.38  149.93.179.14  149.93.179.249  149.93.180.45  149.93.184.113  149.93.196.247  149.93.2.46  149.93.20.179  149.93.203.187</p>	<ul style="list-style-type: none"> <li>- Thời gian phát hiện: từ tháng 10/2008.</li> <li>- Lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật.</li> <li>- Mục tiêu: Nhắm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống</li> </ul>

		khác.
<b>Sality (KuKu)</b>	<p>4b998.bmakemegood24.com  axr.lukki6nd2kdnc.info  bdd.f5ds1jkkk4d.info  blog.inform1ongung.info  businecessity.com  dddrbcash.net  dyfa.lukki6nd2kdnc.info  gyi.f5ds1jkkk4d.info  jcnqg.lukki6nd2kdnc.info  jlw.lukki6nd2kdnc.info  jwyo.f5ds1jkkk4d.info  kukustrustnet666.info  mdagk.f5ds1jkkk4d.info  mim.lukki6nd2kdnc.info  opxp.f5ds1jkkk4d.info  qdxk.lukki6nd2kdnc.info  rqkh.f5ds1jkkk4d.info  rvj.lukki6nd2kdnc.info  trfqi.f5ds1jkkk4d.info  vawp.lukki6nd2kdnc.info</p>	<p>- Thời gian phát hiện: lần đầu tiên bị phát hiện vào 04/6/2003.</p> <p>- Tấn công vào các máy tính sử dụng hệ điều hành Windows,</p> <p>- Thời điểm Sality là một mã độc lây nhiễm vào hệ thống qua các đoạn mã chèn vào đầu tập tin host để mở cửa hậu và lấy trộm thông tin bàn phím. Đến năm 2010 xuất hiện biến thể Sality nguy hiểm hơn và trở thành một trong những dòng mã độc phức tạp và nguy hiểm nhất đối với an toàn của hệ thống. Máy tính bị nhiễm mã độc sẽ trở thành một điểm trong mạng ngang hàng để tiếp tục phát tán mã độc sang các máy tính khác. Sality chủ yếu để phát tán thư rác, tạo ra các proxy, ăn cắp thông tin cá nhân, lây nhiễm vào các máy chủ web để biến các máy chủ này thành máy chủ điều khiển của mạng botnet để tiếp tục mở rộng mạng botnet.</p>