مرکز تخصصی
آپا
دانشگاه صنعتی اصفهان
(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

Phishing

(بخش اول)

زمستان ۱۳۸۹

www.nsec.ir

۱. مقدمه

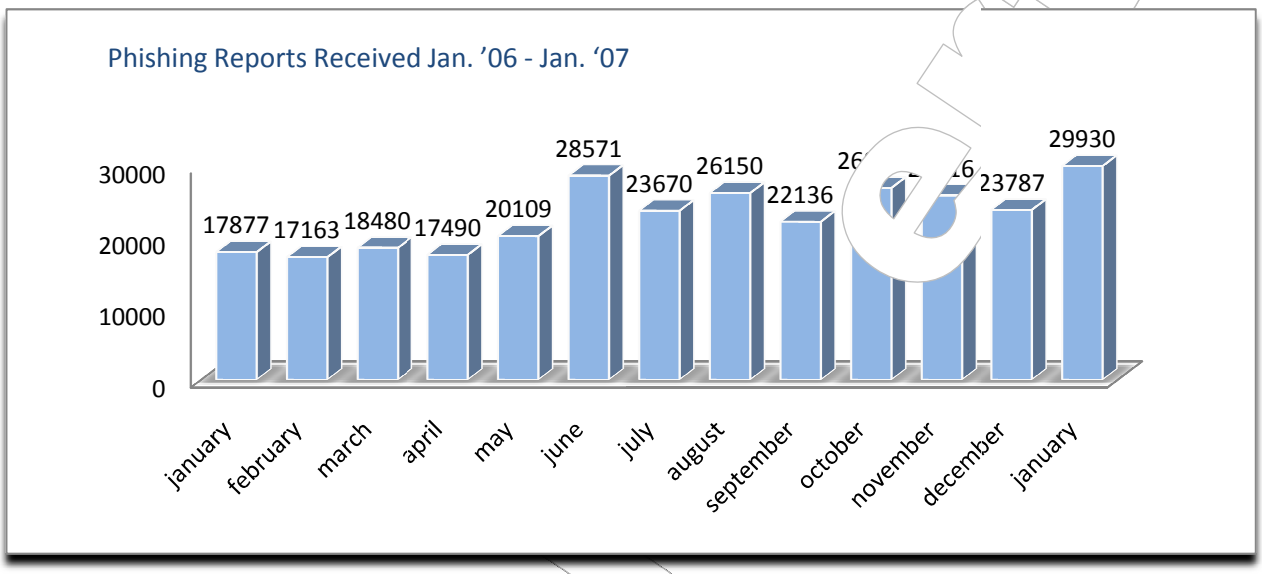
در سال ۲۰۰۴ حساب‌های کاربری نزدیک به دو میلیون نفر از شهروندان آمریکا مورد هجوم مجرمان اینترنتی[1] قرار گرفت. بر طبق گزارشات رسیده در این واقعه نزدیک به ۲ بیلیون دلار خسارت وارد شد. بر طبق آمارها انتشار phishing e-mail که در آن سعی می‌شود با ارسال نامه‌های جعلی از طرف موسسات قانونی، نام کاربری و کلمه‌ی عبور کاربران دزدیده شود، در شش ماه گذشته به بیش از ۴۰۰۰ درصد رشد یافته است. واژه‌ی phishing از این حقیقت ناشی می‌شود که مجرمان اینترنتی سعی دارند با استفاده از تکنیک‌هایی، اطلاعات به‌دست آورند یا به اصطلاح صید[2] کنند. تعویض حرف f با ph به علت تکنیک‌هایی است که نفوذگران به کار می‌برند تا به این ترتیب تمایزی بین این فعالیت‌ها و fishing ساده باشد.

در طول چند سال اخیر، بانکداری اینترنتی که شامل پرداخت صورت‌حساب‌ها به طور آنلاین نیز می باشد، بسیار رواج پیدا کرده است و بیشتر موسسات مالی، این سرویس‌های آنلاین را به مشتریان خود ارائه می‌کنند. با رشد تهدیدات آنلاین و جعل هویت افراد، تخلفات مالی از حملات مستقیم به حملات غیر مستقیم تغییر یافته است. به عبارت دیگر به جای بانک و حمله و دزدی از آن، هدف مجرمان مشتریان بانک‌ها می‌باشد. این حمله‌ی غیر مستقیم نیز نهایتاً بر موسسه مالی اثر خواهد گذاشت زیرا عدم توانایی آن‌ها در حفاظت از سرمایه‌ی مشتریان، اعتبار و قابلیت اعتماد آن‌ها را زیر سوال خواهد برد.

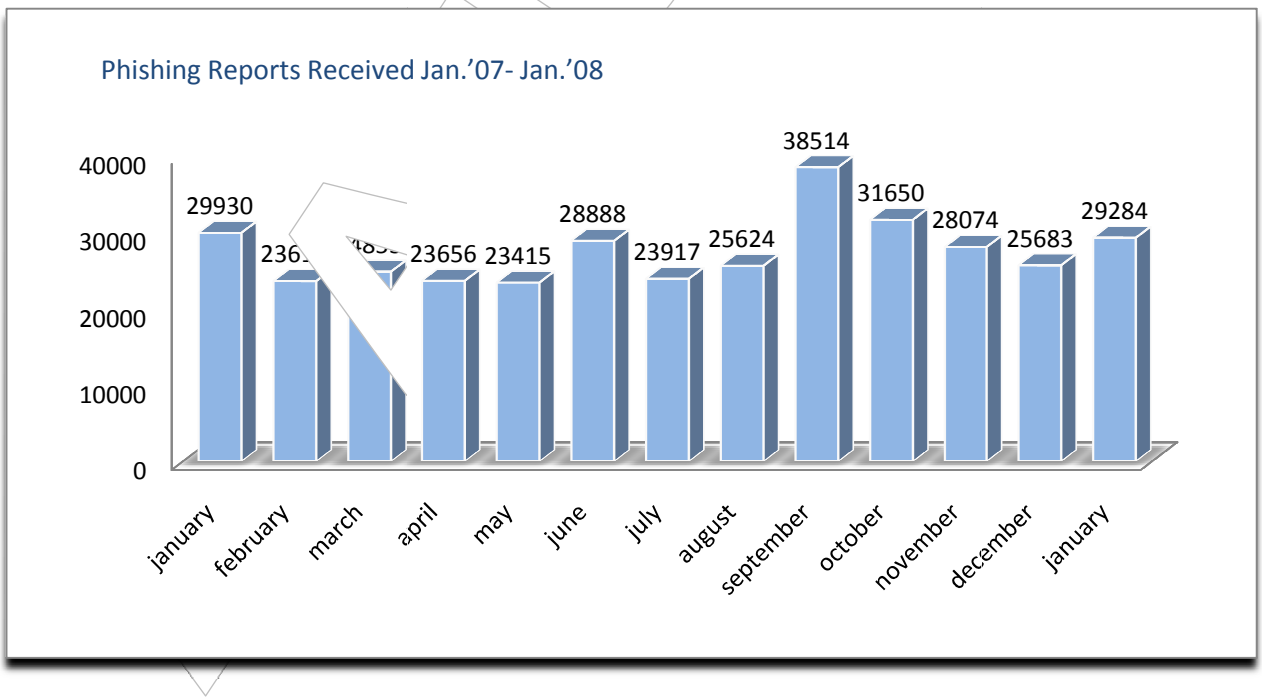
در حقیقت phishing email نوع دیگری از هرزنامه[3] می‌باشد که carding نیز نامیده میشود. بر طبق گزارشات، ۶۳ درصد از ۲/۹۳ بیلیون ایمیل در سال ۲۰۰۵ توسط نرم افزار آنتی اسپم شرکت Brightmail فیلتر شده است. در جولای سال ۲۰۰۴ فیلترهای آنتی‌اسپم Brightmail، ۹ میلیون تلاش برای phishing را در هفته بلاک نمودند. این رقم در دسامبر سال ۲۰۰۴ به ۳۳ میلیون پیغام بلاک شده در هفته رسید.

[1] cyber criminals
[2] fishing
[3] spam

تعداد ایمیل‌های Phishing گزارش شده و ثبت شده در APWG در ماه ژانویه در سال ۲۰۰۸ برابر با ۲۹۲۸۴ گزارش بوده است که نسبت به ماه قبل از آن ۳۶۰۰ گزارش افزایش داشته است. در نمودارهای زیر این آمار در طی سال‌های ۲۰۰۶ و ۲۰۰۷ به تصویر کشیده شده است. لازم به ذکر است که این ارقام تنها گزارش‌های دریافتی APWG[4] می‌باشد.



نمودار شماره ۱



نمودار شماره ۲

[4] Anti-Phishing Work Group

از مقایسه دو نمودار می‌توان نتیجه گرفت که در طی این دوسال متوالی بر تعداد ایمیل‌های phishing افزوده شده است.

۲. دسته بندی اسپم‌ها

با استفاده از تکنیک‌های دسته بندی، می‌توان دسته‌های مختلف اسپم‌ها را مشخص نمود. در این دسته بندی، در بعضی مواقع یک گروه می‌تواند شامل یک مورد خاص و در موارد دیگر، مجموعه‌ای از ایمیل‌ها می‌توانند عضو گروه مشابه و غیر قابل انتظاری باشند.

با وجود اینکه تکنیک‌های دسته‌بندی توضیح داده‌شده به عنوان روش‌های کلی برای بررسی اسپم‌ها شناخته شده‌اند، اما به هر حال این روش‌ها توانایی استثنایی در مشخص نمودن زیرمجموعه‌ای از اسپم‌ها شامل phishing دارند و به همین علت مورد توجه قرار گرفته‌اند.

۳. سازماندهی spam ها

دو آیتم کلیدی در شناخت spammer ها و گروهای spam خاص وجود دارد:

- ابزار bulk mailing
- روش‌های کاربردی spammer ها

افرادی که اسپم ارسال می‌کنند، معمولاً میلیون‌ها ایمیل را در یک زمان ارسال می‌کنند. آن‌ها برای تولید چنین حجم بزرگی، از ابزار bulk-emailing استفاده می‌کنند. این ابزار ایمیل‌هایی با سرآیند و ویژگی‌های یکسان تولید می‌کند که می‌توان از آن‌ها برای تشخیص ایمیل‌های تولید شده توسط ابزار مختلف استفاده نمود. اگرچه بعضی از ابزارهای bulk-mailing ایمیل‌هایی با سرآیندهای تصادفی تولید می‌کنند، اما با این وجود مجموعه‌ی آیتم‌هایی که می‌توانند تصادفی تولید شوند و همچنین مجموعه‌ی مقدار تصادفی به زیرمجموعه‌ی داده‌ای مشخصی محدود هستند.

نکته‌ی مهمتر از ابزارهای ارسال کننده‌ی ایمیل، این است که ارسال کنندگان اسپم‌ها انسان هستند و ویژگی آن‌ها این است که تا زمانی که نیاز به تغییر نداشته باشند، یکسان و بدون تغییر عمل می‌کنند. آن‌ها از ابزارهای مشابه، سیستم‌ها و زیرمجموعه‌ای از ویژگی‌های مشابه استفاده می‌کنند.

با ساده شدن فرآیند شناخت، بیشتر spammer ها ساده و معمول به نظر می‌رسند. اگرچه ابزارهای bulk-mailing تجاری وجود دارند، ولی بسیار گران قیمت هستند. ممکن است spammer ها ترجیح دهند ابزاری برای خود تولید کنند و یا با پرداخت هزینه‌ی کم به شخص دیگری ابزار ارزان‌تری به‌دست آورند. ابزارهای معمول، توزیع محدودی دارند اما افراد مختلف از ابزارهای مختلفی استفاده می‌کنند. برای مثال، شرکت Secure science Corporation (SSC) یک ابزار تحقیقاتی منحصر به فردی ارائه کرده است. این ابزار یک سرآیند واحد تولید می‌کند که به روش یکسانی مورد استفاده قرار گرفته و در بیشتر موارد عمل مرتب کردن و مشخص کردن ایمیل را ساده می‌سازد. شکل ۱.۱ مجموعه‌ای از اسپم‌های دریافتی توسط SSC را نشان می‌دهد.

```
750 Aug 30 * kjjhhgt@yahoo.com  (42)   Affordable Healthcare for families                ZR
751 Aug 30 * Breanna6762v88@hot (67)   Now's your chance
752 Aug 29 * lloihhg@yahoo.com  (49)   Russian Girls Looking for men              HHBV
753 Aug 29 * Lorene2284f64@mult (104)  You missed this investment last time, didn't you? 0054qbVf1-834EQrE-16
754 Aug 29 * latestnews7205g83@ (51)   We Have a FREE Euro For You!
755 Aug 29 * bdrake16user@aol.c (57)   Huge Profit on eBay                        16104
756 Aug 29 * bballjac@hotmail.c (174)  Attn: SYSTEMWORKS CLEARANCE SALE_ONLY $29.99            ZENRT
757 Aug 29 * Mason              (49)   Spend More Time With Your Kids! Work at Home & Make Great Money!                19249
758 Aug 29 * cezazuser@aol.com  (58)   Make a fortune on eBay - FREE Info                      19530
759 Aug 29 * Jeremiah           (51)   Spend More Time With Your Kids! Work at Home & Make Great Money!                  20884
760 Aug 29 * loras@atncorp.com  (300)  NIGHT VISION NZT-1 Just $99!
761 Aug 28 * ccxcfdxz@yahoo.com (93)   300 percent boost for cellphone             QDQLIB
762 Aug 28 * ccxcfdxz@yahoo.com (35)   Want a Home Improvement Loan               P
763 Aug 29 * Halina7638y28@iris (53)   You won't believe this! 1368Ugie3-287Rw-14
764 Aug 29 * kickboxthequeen    (1931) Welcome to my hometown
765 Aug 29 * Akilah2006w31@yaho (66)   The decision is yours 6526EeCu8-485ktQ-15
766 Aug 28 * Christopher_ChaseU (92)   Money Manager Site                c3N33-gHt-jma
767 Aug 27 * lurchpa@hotmail.co (174)  PROTECT YOUR INFORMATION AND YOUR COMPUTER!              8777
768 Aug 27 * mnetwork@bubfet.co (149)  Adv: Reduce your term on your mortgage.
769 Aug 27 * a56772176y45@lycos (46)   ** Your -approval-. **
770 Aug 27 * jbroder@netzero.ne (197)  Extended Auto Warranties Here
771 Aug 27 * zeroday@idir.net   (188)  Baby Boomers, Get Your Youth Back Now
772 Aug 26 * a10in983118x05@lyc (42)   * * Your -approval-! * *
773 Aug 26 * bbssw2@yahoo.com   (132)  Need a good lawyer cheap                MTCNDU
774 Aug 27 * mnytzen@bubfet.com (86)   Adv: Reach Million of Opt-In Customers Now!
775 Aug 27 * momentous@bubfet.c (93)   Adv: Generate Wealth on Wall Street
```

شکل ۱.۱

این مثال نشان می‌دهد که انواع مختلف اسپم وجود دارد. تشخیص یک اسپم مشخص یا یک گروه از این مجموعه کار بسیار دشواری است. اما می‌توان این اسپم‌ها را بر اساس ویژگی‌هایی فیلتر نمود. برای مثال، در تعداد قابل توجهی از این اسپم‌ها، در انتهای قسمت موضوع مجموعه‌ی درهم از حروف بزرگ قرار دارد. بنابراین می‌توان اسپم‌ها را بر اساس اسپم‌هایی که شامل این مجموعه‌ی حروف بزرگ درهم[5] هستند، مرتب نمود (شکل ۱.۲).

[5] Hash

```
125 Sep 06 * vvcxzza@yahoo.com  (71)   FREE HGH -Look Ten Years Younger in 3 Weeks            LZKHF
126 Sep 06 * bbarber612@hotmail (167)  PROTECT YOUR INFORMATION AND YOUR COMPUTER!EZBCYT
127 Sep 06 * zzsaw@yahoo.com    (34)   Mortgage Rates are going lower                 LYLSJE
128 Sep 05 * alice149@hotmail.c (157)  Re: BE healthy with this BREAKTHROUGH product!          XMUJL
129 Sep 04 * bconst3442@hotmail (91)   actually work?"NRWR
130 Sep 03 * zzxdw@festie.com   (91)   Get crystal reception on your cell phone              IZKQLO
131 Sep 03 * ljhuyt@chilly-bin. (71)   Discount Viagra                    G
132 Sep 03 * asdw2@well-in.com  (41)   Affordable Healthcare                      FSX
133 Sep 02 * ccxcfdxz@yahoo.com (34)   Save thousands rates are low             ESLGW
134 Sep 02 * lloihhg@yahoo.com  (77)   Magical Laser Keychain                    NNJODQ
135 Sep 02 * connie_1_1@hotmail (170)  Fw: PROTECT YOUR COMPUTER AGAINST HARMFUL VIRUSES!              GMKTPIW
136 Sep 01 * binder39@hotmail.c (168)  Fw: NORTON SYSTEMWORKS CLEARANCE SALE_ONLY $29.99!            HTHIPNE
137 Aug 31 * bbssw2@yahoo.com   (70)   FREE HGH -Look Ten Years Younger in 3 Weeks                  CGU
138 Aug 31 * lloihhg@yahoo.com  (41)   Dont pay to much for cigs              UKMPC
139 Aug 30 * breaks26@hotmail.c (167)  Fw: DON'T LET A COMPUTER VIRUS RUIN YOUR DAY!                CEUDG
140 Aug 30 * kjjhhgt@yahoo.com  (41)   Affordable Healthcare for families              ZR
141 Aug 29 * lloihhg@yahoo.com  (48)   Russian Girls Looking for men              HHBV
142 Aug 29 * bballjac@hotmail.c (173)  Attn: SYSTEMWORKS CLEARANCE SALE_ONLY $29.99          ZENRT
143 Aug 28 * ccxcfdxz@yahoo.com (92)   300 percent boost for cellphone             QDQLIB
144 Aug 28 * ccxcfdxz@yahoo.com (34)   Want a Home Improvement Loan               P
145 Aug 26 * bbssw2@yahoo.com   (131)  Need a good lawyer cheap                MTCNDU
146 Aug 26 * lloihhg@yahoo.com  (42)   Healthcare you can afford                YCZHEBRCXTJN
147 Aug 25 * bbkke861@hotmail.c (160)  Fw: PROTECT YOUR COMPUTER,YOU NEED SYSTEMWORKS!              WDKCJW
148 Aug 23 * ttteersw@yahoo.com (65)   FREE HGH -Look Ten Years Younger in 3 Weeks           LUPWMSIMDR
149 Aug 22 * ttteersw@yahoo.com (91)   Get crystal reception on your cell phone                   LGAT
```

شکل ۱.۲

با مرتب کردن اسپم‌ها بر اساس ویژگی خاص، می‌توان بررسی‌های دقیق‌تری بر روی مجموعه‌ی آن‌ها انجام داد و ویژگی‌های معمول دیگری را جست و جو نمود. برای مثال، در شکل ۱.۳ تعداد قابل توجهی از اسپم‌ها، تاریخی با منطقه‌ی زمانی ۱۷۰۰- دارند در حالی که چنین منطقه‌ی زمانی وجود ندارد. بنابراین می‌توان از این موضوع به عنوان ویژگی واحدی برای سازماندهی اسپم‌ها استفاده نمود.

```
Dec 07 * ttyrew21@yahoo.com (101)  Get better reception on your cell phoneSBCZFIHRN
Dec 07 * kkjhg65@yahoo.com  (101)  Boost your cell phone receptionKP
Dec 07 * minir221@yahoo.com (83)   Need to be revitalizedVC
Dec 07 * ggdsa2@yahoo.com   (83)   Want to look youngerIAT
Dec 06 * vdsd221@yahoo.com  (108)  FW: HOT New Toy for Christmas 2002!KEDMIXBV
Dec 06 * ccvds21@yahoo.com  (108)  FW: HOT New Toy for Christmas 2002!HQZGA
Dec 06 * rrewe21@yahoo.com  (132)  Protect your pc from hackersJQZI
Dec 06 * ppiou66@yahoo.com  (133)  Keep the hackers off your computerJDLIKTMS
Dec 05 * llkjy56@yahoo.com  (41)   Automated Life Insurance quotes.JOBQ
Dec 05 * zxxas21@yahoo.com  (42)   We can save you thousands on life insuranceAMKG
Dec 04 * erww221@yahoo.com  (107)  HOT New Toy for Christmas 2002!              J
Dec 04 * qqwss3@yahoo.com   (108)  FW: Remote Controlled Mini Matchbox Cars                  CI
Dec 04 * yytr453@yahoo.com  (46)   Mortgage Rates are going lower
Dec 04 * mmjh543@yahoo.com  (46)   Mortgage Rates are going lowerUHW
Dec 03 * opioi78@yahoo.com  (101)  Tired of Dropped Cell CallsMS
Dec 03 * ccxsd2@yahoo.com   (100)  Get crystal reception on your cell phoneFBPNO
Dec 02 * bcvbcv32@yahoo.com (107)  RE: Remote Controlled Mini Matchbox CarsQNM
Dec 02 * vvds2122@yahoo.com (107)  FW: MINI RADIO_CONTROLLED CARS ARE SOLD OUT  IN STORESH
Dec 02 * cxzxca12@yahoo.com (78)   Look and feel 30 years youngerXRDRJBAOSVW
Dec 02 * cxzxca12@yahoo.com (78)   Look and feel 30 years youngerABCT
Dec 01 * vbcx21@yahoo.com   (58)   Enlarge your packageGTGIL
Dec 01 * vvdsd21@yahoo.com  (59)   Feeling SmallLPMVEDV
Nov 30 * bcvbcv32@yahoo.com (53)   Refinance today and save thousandsJAL
```

شکل ۱.۳

بر اساس این نتایج می‌توان ویژگی‌های مشخصی از این spammer را تعیین نمود:

- همیشه عبارت درهمی در کنار موضوع ایمیل وجود دارد.
- موضوع معمولاً با نقطه گذاری ختم نمی‌شود. اگر نقطه گذاری نیز رعایت شده باشد، معمولا یک علامت تعجب خواهد بود.
- حجم فایل تقریبا مقدار مشخصی است (بین ۵۰ تا ۱۴۰ خط).
- به نظر می‌رسد که تمام آدرس‌های ایمیل جعل شده از yahoo.com دریافت شده‌اند.
- به نظر می‌رسد که نام تمامی حساب‌های جعل شده، حروف تکراری هستند که با یک عدد دنبال شده‌اند. این حروف عموماً از حروف سمت چپ صفحه کلید می‌باشند. این ابزار bulk-mailing خاص نیاز دارد که کاربر نام حساب‌های کاربری جعل شده را تعیین کند. این کار می‌تواند به دو روش زیر انجام شود. کاربر می‌تواند پایگاه‌داده‌ای از اسامی را وارد کند یا آن‌ها تایپ کند. در این مورد به نظر می‌رسد کاربر با دست چپ به طور تصادفی اسامی را وارد کرده و با دست راست خود بر روی کلید Enter توسط موشواره کلیک کرده است. از آن‌جا که کاربر با دست راست خود با موشواره کار کرده است، می‌توان نتیجه گرفت که او دست راست است.

از آن‌جا که این spammer ایمیل‌ها را روزانه ارسال می‌کند، در بعضی از روزهای خاص، از قبیل روز شکرگذاری، شب سال نو، چند روز پس از کریسمس ارسال قطع می‌شود.

گزینه‌های اصلی که به این شناسایی کمک می‌کنند عبارتند از:

- شناسایی ابزار bulk-mailing: این گزینه به معنی مشخص نمودن ابزار خاص مورد استفاده نیست. بلکه منظور تعیین ویژگی‌های منحصر به فرد موجود در سرآیند ایمیل می‌باشد.
- آیتم‌های زیر مجموعه‌ی خصوصیات از قبیل hash buster (فرمت و محل)، ویژگی‌های متن (خطاهای املایی و گرامر) و مجموعه‌ی ویژگی‌های یکتای حاصل از ابزار bulk mailing.
- متدهای ارسال: آیا اسپمر از open relay ها استفاده می‌کند؟ آیا برای ارسال، زمان یا روز مشخصی را ترجیح می‌دهد؟

۴. تکنیک‌های دسته‌بندی

بعد از تعیین کردن گروه‌های اسپم، می‌توان اهداف آن‌ها را بررسی نمود. تا کنون اسپم‌ها را به هشت گروه عمده تقسیم نموده‌اند که در ادامه چهار نوع آن‌ها معرفی شده‌اند.

- ایمیل‌های تجاری ناخواسته[6]: این نوع توسط شرکت‌های حقیقی تولید می‌شود که سعی می‌کنند با مشتری‌های موجود و مستعد ارتباط برقرار کنند. اسپم‌های UCE بسیار نادر هستند (در حدود یک دهم درصد تمامی اسپم‌های موجود).
- ایمیل‌های تجاری بدون پاسخ[7]: NCE ها توسط کمپانی‌های حقیقی برای ادامه‌ی ارتباط با مشتری برخلاف میل او ارسال می‌شوند. تفاوت اصلی بین UCE و NCE این است که در ابتدا کاربر آغازگر ارتباط می‌باشد و سپس تمایلی به ارتباط بیشتر ندارد اما ارسال کننده‌ی NCE به ارسال ادامه می‌دهد. NCE مشکلی است برای افرادی که از سرویس‌های زیادی استفاده می‌کنند مثلاً خرید آنلاین انجام می‌دهند یا ارتباطی را با یک شرکت NCE آغاز می‌کنند.
- لیست سازها: این گروه‌ها، گروه‌های اسپمی هستند که با به‌دست آوردن لیستی ازآدرس‌های ایمیل و فروش آن‌ها به spammer های دیگر و یا عامل[8]های بازاریابی کسب درآمد می‌نمایند.
- Scams: این گروه اکثریت اسپم‌ها را تشکیل می‌دهند. هدف scam این است که با جعل واقعیت، اطلاعات با ارزش به‌دست آورد. Malware و phishing زیرمجموعه‌ای از scam ها می‌باشند.

۵. Phishing

Phishing زیرمجموعه‌ای از گروه scam می‌باشد. Phisher ها خود را به عنوان کمپانی‌های مجاز معرفی می‌کنند تا بدین وسیله بتوانند حساب‌های کاربری مشتریان و اطلاعات و امتیازات دسترسی آن‌ها را به‌دست آورند. با استفاده از تکنیک‌های دسته‌بندی که توضیح داده شد، می‌توان گروهای phishing خاص را مشخص نمود. آیتم‌های کلیدی برای این تشخیص شامل موارد زیر هستند:

- شناخت ابزارهای bulk-mailing و ویژگی‌ها
- عادات و روش‌ها و الگوهای ارسال اسپم

[6] Unsolicited commercial e-mail(UCE)
[7] Nonresponsive commercial e-mail (NCE)
[8] agent

- نوع سیستم‌های استفاده شده برای ارسال اسپم
- نوع سیستم‌های استفاده شده برای میزبانی سرور phishing
- طرح سرور phishing شامل استفاده از HTML ، JS ، PHP و اسکریپت‌های دیگر

مطابق با گزارشات SSC، به طور تقریبی حدود چهار دوجین گروه phishing در سرتاسر جهان وجود دارد. در ادامه تکنیک‌هایی را مورد بحث قرار می‌دهیم که به درک بهتر و پی‌گیری phisher ها کمک می‌کند.

۶. Phishing چیست؟

Phishing که با نام‌های carding یا brand spoofing نیز شناخته شده است، تعاریف مختلفی دارد. اگر بخواهیم در تعریف این کلمه نهایت دقت را به خرج دهیم، بایستی به جای ارائه‌ی یک تعریف استاتیک، نگاهی به متدهای اولیه‌ی phishing و سیر تکاملی فعالیت‌ها و آینده‌ی پیش‌رو اندازیم. از این‌رو در ابتدا دیدگاه اولیه را به صورت زیر تعریف می‌کنیم: عمل ارسال ایمیل جعلی (با استفاده از bulk mailer) به یک گیرنده و جعل یک موسسه‌ی قانونی برای فریب گیرنده در فاش‌سازی اطلاعات محرمانه مانند شماره‌ی کارت اعتباری و یا کلمه‌ی عبور حساب بانکی. این ایمیل در بیشتر مواقع از کاربر می‌خواهد که از یک وب‌سایت دیدن کند و اطلاعات خود را در آن وارد کند. برای ایجاد اعتماد بیشتر، وب سایت شبیه به وب‌سایت موسسه‌ای است که scammer سعی دارد آن را جعل کند. البته در حقیقت این وب‌سایت، سایت موسسه‌ی مورد نظر نیست و تنها اطلاعات محرمانه را برای مقاصد مالی سرقت خواهد نمود. بنابراین کلمه‌ی phishing تغییر مشهودی در کلمه‌ی fishing است به این علت که scammerها به امید به دست آوردن اطلاعات از قربانیان، با جعل‌سازی برای کاربران "قلاب" می‌اندازند.

Phishing در حدود ۱۴ سال قبل با America Online (AOL) در سال ۱۹۹۵ آغاز شد. در آن زمان برنامه‌هایی شبیه به AOHell وجود داشتند که فرآیند phishing برای حساب‌های کاربری و کارت های اعتباری را اتوماتیک می‌ساختند. در گذشته phishing در مقایسه با ایمیل‌ها بیشتر از Internet Relay Chat (IRC) یا سیستم‌های messaging alert استفاده می‌کرد. Phisherها خود را به عنوان یک مدیر AOL معرفی می‌کردند و به قربانیان اعلام می‌کردند که برای رفع برخی مشکلات به وجود آمده، باید اطلاعات ورودی و کارت اعتباری خود را تجدید کنند. به علت این‌که در آن زمان استفاده از کامپیوترهای شخصی در خانه‌ها و استفاده از اینترنت به عنوان یک تجربه‌ی تازه بود، این متد برخلاف امروز روش موثری بود.

حمله‌ی ناگهانی phishing به موسسات مالی برای اولین بار در جولای ۲۰۰۳ گزارش شد. بنا بر گزارش Great Spam Archive، اهداف اولیه E-loan ، E-gold ، Wells Fargo و Citibank بودند. نکته‌ی قابل توجه در ارتباط با پدیده‌ی phishing این است که phishing گروه جدیدی از فاکتورهای حمله را که تا آن زمان در بودجه‌ی امنیتی سازمان‌های مالی در نظر گرفته نشده بود، معرفی کرد: عامل انسانی. تمام دیواره‌های آتش گران قیمت، گواهی‌نامه‌های SSL، قوانین IPS و مدیریت وصله‌ها هیچ یک نمی‌توانند سوءاستفاده از اعتماد آنلاین را متوقف کنند. این اعتماد نه تنها اطلاعات محرمانه‌ی کاربر را زیر سوال می‌برد، بلکه بر اعتماد مشتری در ارتباطات موسسه و کلاینت‌های آن نیز تاثیر می‌گذارد.

پروتکل SMTP در سال ۱۹۸۲ طراحی شد و تنها افراد محدود و قابل اعتماد از آن استفاده می‌کردند. در سال ۲۰۰۱ که بیش از ۶ سال بود که RFC 2821 و SMPT توسط عموم استفاده می‌شدند، ضعف‌های امنیتی موجود به طور کامل مستند شد.

روش جعل‌سازی توضیح داده شده در RFC 2821، چیزی است که Phisherها و Spammer ها برای ارسال ایمیل به قربانیان به کار گرفته‌اند. ذکر این نکته مهم است که این مسئله به معنی افزایش مهارت Phisher ها نمی‌باشد. علت بالا بودن آمار phishing در تمامی زمان‌ها، مجموعه ابزار در دسترس می‌باشد نه مهارت Phisher ها. برای اثبات این موضوع، متخصصین حوزه‌ی امنیت از سال ۱۹۸۲ به همراه جریان SMTP شناخته شدند. اولین حمله بر ایمیل‌ها به عنوان e-mail bombing شناخته شد. اما این موضوع به علت وجود ابزارهای متعددی از قبیل Avalanche ، Kaboom و Ghost Mail بود که در دسترس عموم قرار داشت. این ابزار کل فرایند را با یک کلیک ماوس اتوماتیک می‌کردند و حساب‌های ایمیل بدون استفاده را ارائه می‌کردند و کارایی mail server مربوط به حساب‌های ایمیل را زیر سوال می‌بردند. در این حمله با ارسال ایمیل‌های بیش از حد و با سرعت بالا، سرریز حساب‌های کاربری رخ خواهد داد و به‌طور خاص، یک حمله‌ی denial-of-service علیه حساب‌های ایمیل و ارائه دهندگان سرویس‌های آنان به شمار می‌آید. تا زمانی که ابزارها در دسترس هستند، حملات phishing نیز وجود خواهند داشت. می‌توان این موضوع را با آزادی خرید اسلحه و جنایات مسلحانه مقایسه نمود.