تـــاریخ: ۱۲ اسفند ۱۴۰۲
پیوست: ۸ صفحه

بسمه تعالی

از: محمدصالح سوزنچی

به : رئیس پلیس فتا همدان

موضـوع: اعلام و معرفی منبع اصـلی انتشـار نامه ارسـالی، از نیروی انتظامی جمهوری اسـلامی ایران، به دادسـتان محترم کل کشـور- حجت الاسـلام والمسـلمین حاج آقا منتظری، با موضـوع دسـترسـی به افزونه فیلترینگ، به تاریخ ۱۳۹۶/۰۹/۲۹ و شـماره ۱۴/۱۱۷/۶/۱۲/۶/۱۲۵، که توسـط ضـابطین محترم پلیس فتا در تفتیش و بازرسی از کیس کامپیوتر تحت بازداشت اینجانب کشف شده بود، بدین شرح می‌باشد:

با عرض سلام؛

احتراما همانگونه که مستحضرید، اینجانب محمدصالح سوزنچی، خوانده در پروندۀ کلاسه ۱۴۰۲۲۸۹۲۰۰۰۰۲۲۱۶۵۰۴ با شماره بایگانی ۰۲۰۱۶۴۱، در بازجویی سوم خود که در تاریخ ۹ اسفند ۱۴۰۲ و پیرامون موضوع همین پرونده صورت گرفته بود، در برگه اظهارات مطلع که آنرا امضا و اثر انگشت زده‌ام، متعهد شده بودم که تا تاریخ یکشنبه ۱۳ اسفند ۱۴۰۲ منبع اصلی انتشار نامه زیر را کشف و علت و نحوه دانلود شدن آنرا توضیح داده و در نهایت نتیجه را به سرهنگ زارعی، رئیس محترم پلیس فتا همدان گزارش بکنم.

بسم الله الرحمن الرحیم

نیروی انتظامی جمهوری اسلامی ایران

طبقه بندی :
شماره : ۱۴/۱۱۷/۶/۱۲/۶/۱۲۵
تاریخ : ۱۳۹۶/۰۹/۲۹
پیوست : ندارد

فرماندهی

از: نیروی انتظامی جمهوری اسلامی ایران

به: دادستان محترم کل کشور- حجت الاسلام والمسلمین حاج آقا منتظری

موضوع: دسترسی به افزونه فیلترینگ

سلام علیکم

با صلوات بر محمد(ص) وآل محمد (ص) وعرض احترام به استحضار می رساند:

مهم ترین راهکار برای ایجاد محدودیت در فضای مجازی، بهره گیری از فیلترینگ است که امروزه در اغلب کشورها بر پایه خط مشی های گوناگون و با درجاتی از شدت و ضعف رایج می باشد. در این راستا پلیس اطلاعات و امنیت عمومی مسئولیت اشراف بر حوزه های **"ضد امنیتی، ساماندهی کسب و کارهای اینترنتی و موضوع های علیه عفت و اخلاق عمومی در فضای مجازی"** با رویکرد پیشگیرانه را برعهده دارد که برای تحقق اهداف سازمانی، بهره گیری از ظرفیت فیلترینگ و مسدودسازی به عنوان خاکریز بنیادی و یکی از شاخص های اثرگذار برای پاک سازی و ایجاد امنیت در فضای مجازی، اجتناب ناپذیر می باشد؛ از این رو با عنایت به هماهنگی انجام شده، به منظور تطابق مأموریت های تخصصی در این حوزه با محورهای متعدد تعریف شده درافزونه کارگروه تعیین مصادیق مجرمانه؛ خواهشمند است دستور فرمایید امکان دسترسی مستقیم پلیس اطلاعات و امنیت عمومی به افزونه فیلترینگ در شش حوزه تخصصی زیر با قابلیت گزارش گیری مستقل ومجزا(سلسله مراتبی) را فراهم نموده و نتیجه را به این نیرو اعلام نمایند.

الف) محتوای علیه عفت و اخلاق عمومی
ب) محتوای علیه مقدسات اسلامی
ج) محتوای علیه امنیت و آسایش عمومی
د) محتوای علیه مقامات و نهادهای دولتی و عمومی
ح) محتوای مجرمانه مرتبط با انتخابات مجلس شورای اسلامی
ط) محتوای مجرمانه مرتبط با انتخابات ریاست جمهوری

فرمانده نیروی انتظامی جمهوری اسلامی ایران

سرتیپ پاسدار حسین اشتری

رئیس محترم پلیس فتا همدان، جناب سـرهنگ زارعی همانطور که در مسـتندات بعدی بخوبی مشـهود اسـت، منبع اصلی نشت و انتشار نامه فوق‌الذکر که ظاهرا مورد توجه خاص سردار مجید[احتمالا]نیز قرار گرفته است، بطوریکه ایشان در راستای پیگیری این موضوع، دوتن از متخصصان فتای تهران را ماموریت کرده بودند که به همدان آمده و در بازجویی از بنده متوجه بشوند که این نامه چرا و چگونه بدست اینجانب رسیده است.

Subject: دسترسی به افزونه فیلترینگ
From: پلیس امنیت <pava@internet.ir>
Date: 2/8/2018, 9:52 AM
To: اداره نظارت <nezarat@internet.ir>
CC: پلیس امنیت <pava@internet.ir>

با سلام
با عنایت به هماهنگی های صورت گرفته با جناب آقای امیری تصویر مکاتبه درخواستی در خصوص دسترسی به افزونه فیلترینگ برای پاوا، ارسال می گردد
با تشکر

Attachments:

IMG_20180207_0003.rar 401 kB

شوربختانه مشخص شد که منبع اصلی این نامه نیز مثل اکثر نامه‌ها و دیتاهای حاکیمتی و دولتی که به بر روی سیستم من به فراوانی یافت می‌شود، همگی رسما یک منبع مشترک دارند. یعنی منبع اصلی آنها همان بکاپ ایمیل‌های ایمیل سرور هک شده دادستانی کل کشور(INTERNET.IR) است که در تاریخ ۱۳ آبان ۱۴۰۱ توسط هکرهای ناشناس هک شدند و بکاپ‌هایش را بصورت عمومی در فضای مجازی منتشر ساختند.

مهندس امیری-معاون مدیرکل نظارت و پیگیری امور فضای مجازی دادستانی کل کشور و بازپرس ویژه رسیدگی به پرونده‌های قمارخانه‌های اینترنتی

اینجانب نیز همانند سایر افراد دیگر با اطلاع از این موضوع آنها را دانلود کردم و پس از بررسی مختصری متوجه یکسری مسائل مهمی شدم، که هریک در آینده نزدیک پتانسیل تبدیل شدن به یک تهدید ملی را داشتند. براین اساس بر خودم لازم دیدم که بر روی آنها کمی تحقیق کنم. برای همین منظور با مطالعه هر یک از این ایمیل‌ها، آندسته از محتواهایی که بنظرم مهم می‌رسیدند را استخراج کرده و دستبندی می‌کردم تا بتوانم از هر یک از آنها و بسته به نوع نیازهایم مثل ارسال گزارش به نهادهای امنیتی از آنها استفاده نمایم.

دسترسی به افزونه فیلترینگ

Subject: دسترسی به افزونه فیلترینگ
From: پلیس امنیت <pava@internet.ir>
Date: 2/8/2018, 9:52 AM
To: اداره نظارت <nezarat@internet.ir>
CC: پلیس امنیت <pava@internet.ir>
X-Mozilla-Status: 0001
X-Mozilla-Status2: 10000000
Return-Path: pava@internet.ir
Received: from internet.ir (LHLO internet.ir) (94.232.175.83) by internet.ir with LMTP; Thu, 8 Feb 2018 09:53:10 +0330 (IRST)
Received: from localhost (localhost [127.0.0.1]) by internet.ir (Postfix) with ESMTP id 55B45209C74; Thu, 8 Feb 2018 09:53:10 +0330 (IRST)
X-Spam-Flag: NO
X-Spam-Score: 1.061
X-Spam-Level: *
X-Spam-Status: No, score=1.061 tagged_above=-10 required=6.6 tests=[ALL_TRUSTED=-1, BAYES_00=-1.9, DNS_FROM_AHBL_RHSBL=2.699, RCVD_IN_BRBL_LASTEXT=1.449, RDNS_NONE=0.793, RP_MATCHES_RCVD=-1, T_HELO_NO_DOMAIN=0.01, T_KHOP_THREADED=-0.01, T_LONG_HEADER_LINE_80=0.01, T_NOT_A_PERSON=-0.01, T_PUBLISHED_DNSBLS_BRBL=0.01, T_THREAD_INDEX_BAD=0.01] autolearn=no
Received: from internet.ir ([127.0.0.1]) by localhost (internet.ir [127.0.0.1]) (amavisd-new, port 10032) with ESMTP id MER_zOB3ZFVZ; Thu, 8 Feb 2018 09:53:05 +0330 (IRST)
Received: from localhost (localhost [127.0.0.1]) by internet.ir (Postfix) with ESMTP id 2D71C209C7E; Thu, 8 Feb 2018 09:53:05 +0330 (IRST)
X-Virus-Scanned: amavisd-new at internet.ir
Received: from internet.ir ([127.0.0.1]) by localhost (internet.ir [127.0.0.1]) (amavisd-new, port 10026) with ESMTP id V7viV6Dd4BrF; Thu, 8 Feb 2018 09:52:51 +0330 (IRST)
Received: from internet.ir (internet.ir [94.232.175.83]) by internet.ir (Postfix) with ESMTP id 93077209C8B; Thu, 8 Feb 2018 09:52:51 +0330 (IRST)
Message-ID: <1455997291.517335.1518070971062.JavaMail.root@internet.ir>
In-Reply-To: <1518213591.517319.1518070820193.JavaMail.root@internet.ir>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_Part_517333_410215790.1518070971044"
X-Originating-IP: [92.61.185.5]
X-Mailer: Zimbra 8.0.3_GA_5664 (ZimbraWebClient - FF49 (Win)/8.0.3_GA_5664)
Thread-Topic: دسترسی به افزونه فیلترینگ
Thread-Index: yGBJUAmZmans1P3jzrwJLw1BTM+LpQ==

با سلام
با عنایت به هماهنگی های صورت گرفته با جناب آقای امیری تصویر مکاتبه درخواستی در خصوص دسترسی به افزونه فیلترینگ برای پاوا، ارسال می گردد
با تشکر

Attachments:

IMG_20180207_0003.rar	401 kB

تاریخ: ۱۲ اسفند ۱۴۰۲
پیوست: ۸ صفحه

طبقه بندی :
شماره : ۱۴/۱۱۷/۶/۱۲/۹۶/۱۲۵
تاریخ : ۱۳۹۶/۰۹/۲۹
پیوست : ندارد

فرماندهی

از: نیروی انتظامی جمهوری اسلامی ایران

به: دادستان محترم کل کشور- حجت الاسلام والمسلمین حاج آقا منتظری

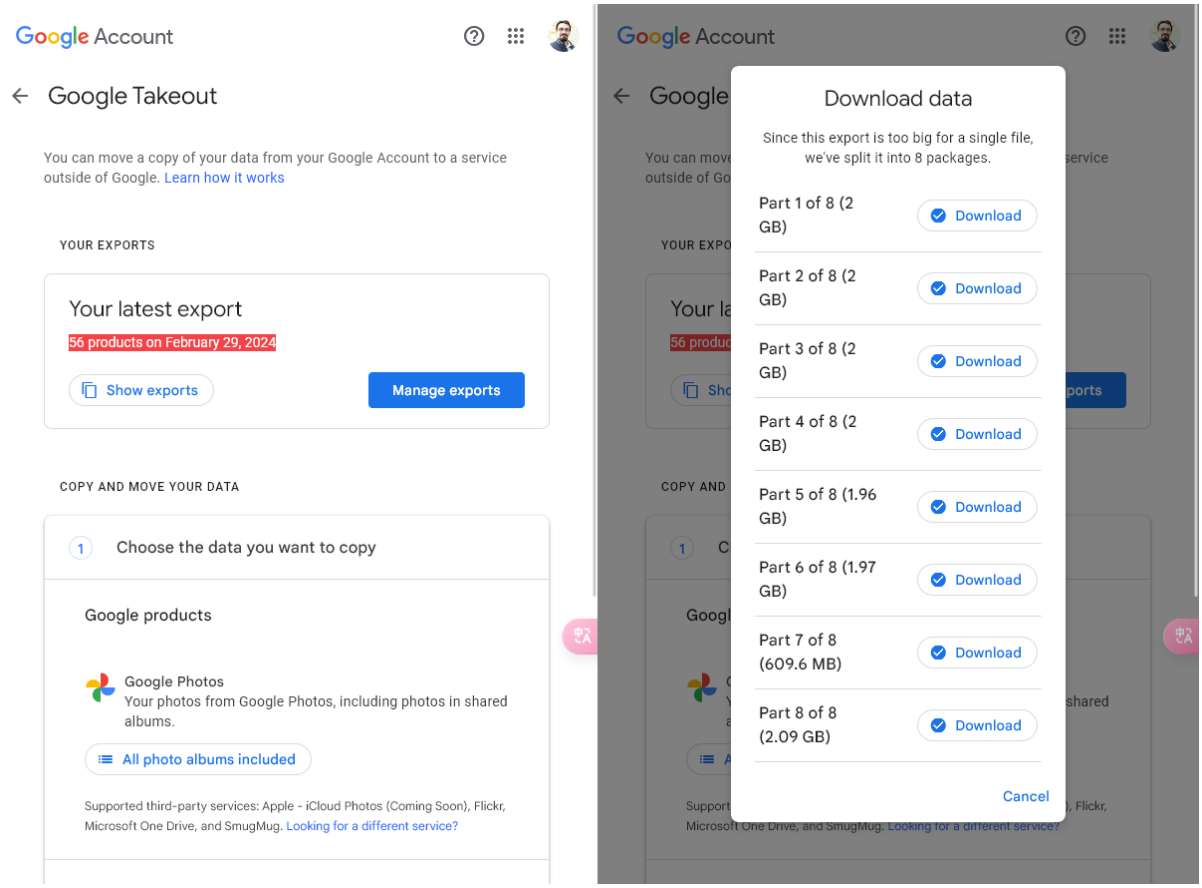
موضوع: دسترسی به افزونه فیلترینگ

سلام علیکم

با صلوات بر محمد(ص) وآل محمد (ص) وعرض احترام به استحضار می رساند؛

مهم ترین راهکار برای ایجاد محدودیت در فضای مجازی، بهره گیری از فیلترینگ است که امروزه در اغلب کشورها بر پایه خط مشی های گوناگون و با درجاتی از شدت و ضعف رایج می باشد. در این راستا پلیس اطلاعات و امنیت عمومی مسئولیت اشراف بر حوزه های **"ضد امنیتی، ساماندهی کسب و کارهای اینترنتی و موضوع های علیه عفت و اخلاق عمومی در فضای مجازی"** با رویکرد پیشگیرانه را برعهده دارد که برای تحقق اهداف سازمانی، بهره گیری از ظرفیت فیلترینگ و مسدودسازی به عنوان خاکریز بنیادی و یکی از شاخص های اثرگذار برای پاک سازی و ایجاد امنیت در فضای مجازی، اجتناب ناپذیر می باشد؛ از این رو با عنایت به هماهنگی انجام شده، به منظور تطابق مأموریت های تخصصی در این حوزه با محورهای متعدد تعریف شده درافزونه کارگروه تعیین

در پایان نیز می‌بایســت به این نکته اشــاره کنم، باتوجه به اینکه تا همین لحظه که فقط به ایمیلم توانســتم مجددا دســترســی پیدا کنم. متوجه شــدم که نمایندگان پلیس فتا تهران همراه خودشــان ۶۰ گیگ از اطلاعات هارددیســک کامپیوترم و ۱۴٫۶ گیگ اطلاعات از ایمیل(saleh.souzanchi@gmail.com) اصــلی بنده را برای ســردار عزیز به تهران منتقل کرده‌اند تا ایشــان بتوانند از نزدیک به همه اطلاعات اینجانب دســترســی و اشــراف کامل داشته باشند.



بر این اســاس بود که دیدم جهت محکم کاری بد نیســت برای راهنمایی ســردار عزیز، یک ویدیویی آموزشــی مختصر هم تهیه کنم تا به ایشان نحوه آسان بررسی و صحت‌سنجی این مستندات را آموزش بدم. که انشالله به محض آنکه مجدد به گوشی دومم که در همان روز بازجویی بصورت موقت بازداشت شده بود، دسترسی پیدا کنم، آن را نیز در کانال زیر منتشر می‌سازم که دیگر جایی برای شک و شبهه باقی نمانده باشد:

https://t.me/ToofanReports

همچنین می‌بایست این موضوع را نیز به لطف ایت گزارش به اطلاع ایشان برسانم که با هزار سختی و مکافاتی که بخاطر عدم دسترسی به تجهیزاتم که اکنون نزد شما توقیف است ایجاد شده بود، بالاخره با موفقیت نسبی توانستم یکی از گزارش‌های تحقیقاتی‌ام را که ۱۰۰% مورد توجه ایشان قرار خواهد گرفت را به اتمام برسانم.

لذا تصمیم گرفتم بدینوسیله از سردار مجید و سایر همکاران محترم‌شان دعوت بعما بیاورم تا عضو کانال بنده بشــوند تا بتوانند و از طریق در اســرع وقت در جریان انتشــار کلیات و جزییات این گزارش نیز قرار بگیرند. البته اگر این افتخار را به بنده حقیر متهم به کلاهبرداری بدهند.

محمد صالح سوزنچی

قوه قضائیه
دادستانی کل کشور
معاونت پیگیری امور فضای مجازی

بسمه تعالی

تاریخ : .....
شماره : .....
پیوست : .....

استفاده از رمزهای ایستا در این فرآیندها است که موجب شده مجرمین با بدست آوردن رمز دوم و اطلاعات کارت قربانی، به‌راحتی بتوانند از حساب بانکی بزه‌دیده برداشت نموده و یا از فروشگاه‌های اینترنتی خرید نمایند.

اطلاع رسانی صداوسیما و سایر مراجع ذیصلاح در خصوص اجرایی شدن بکارگیری رمزهای پویا باعث گردید، اطلاعات کارتهای بانکی مردم که در طول سالیان گذشته از طریق درگاه‌های پرداخت جعلی و فیشینگ در اختیار مجرمین قرار گرفته بود، با نزدیک شدن به موعد اجرای رمزهای پویا (۹۸/۳/۱) در ابعاد بسیار گسترده و فراگیر توسط مجرمین سایبری مورد سوء استفاده قرار گیرد.

این آمار فزآینده بیانگر وضعیت بحرانی رشد این جرایم در کشور است به نحوی که فقط در تهران بطور روزانه حدود ۲۰۰ فقره پرونده جدید ثبت می‌شود و صرفاً در خردادماه سال جاری بیش از ۲۴۰ میلیارد ریال خسارت مالی وارده به بزه‌دیدگان این جرایم بوده است.(این آمار صرفاً مربوط به آمار یک ماه برداشت غیرمجاز از حساب با مبالغ بالای ۵۰۰ هزارتومان و براساس پرونده‌های ارجاع شده به پلیس فتا بوده است و با احتساب تخمین مشابه از سایر ماه‌های سال و لحاظ جرایم زیر ۵۰۰هزار تومان و باتوجه به اینکه بسیاری از جرایم خرد بدلیل طولانی بودن فرآیندهای قضایی اساساً مورد شکایت قرار نمی‌گیرد و برخی دیگر از این شکایات در پلیس آگاهی به ثبت می‌رسد، آمار واقعی این جرایم و خسارات وارده ده‌ها برابر بیشتر از آمار اعلامی خواهد بود.)

ضمناً براساس تخمین پلیس فتا اگر این وضعیت ادامه پیدا کند در پایان سال جاری حدود **۱۸۰ هزار تا ۶۰۰ هزار نفر** از مشتریان بانکی، متأثر از این جرایم شده و علاوه بر اینکه هزینه‌های هنگفت مادی و معنوی به بزه دیدگان، دستگاه قضایی و ضابطان دادگستری تحمیل خواهد کرد، ممکن است موجب ایجاد تبعات اجتماعی و امنیتی و نارضایتی گسترده در جامعه شود.

علاوه بر موارد فوق عواید مالی ناشی از برخی دیگر از جرایم نظیر سایر کلاهبرداری‌های رایانه‌ای و قماربازی‌های اینترنتی نیز از طریق کارت‌های بانکی که اطلاعات ایستای آن‌ها از طریق فیشینگ در اختیار مجرمین قرار گرفته است تبادل می‌شود و چنانچه بخشنامه بانک مرکزی مبنی بر استفاده از رمزهای پویا اجرایی نشود ، سوء استفاده از کارت‌های بانکی اشخاص در دیگر جرایم فضای مجازی نیز رشد چشمگیری خواهد داشت. براساس گزارش پلیس فتا ، گردش مالی قمارخانه‌های آنلاین در سال گذشته به رقم ۲۲۰۰ میلیارد تومان بالغ شده است و پیش‌بینی می‌شود بیش از یک میلیون و دویست هزار نفر در کشور به این جرایم آلوده شده باشند.

یکی از مهمترین دلایل من برای جمع‌آوری آن همه اطلاعات هویتی نشت پیدا کرده از هک‌های اخیر ، برسی ابعاد مختلف و نشان دادن تهدیدات احتمالی یک فاجعه بود. فاجعه‌ای که بدون این دیتاها کسی حاضر به پذیرش آن به این راحتی‌ها نبود و با دیتا نیز که خودتان از نزدیک شاهدش بودید و تجربه‌اش کردید ☹