Subscribe to RSS
Follow me on Twitter
Join me on Facebook

# Krebs on Security

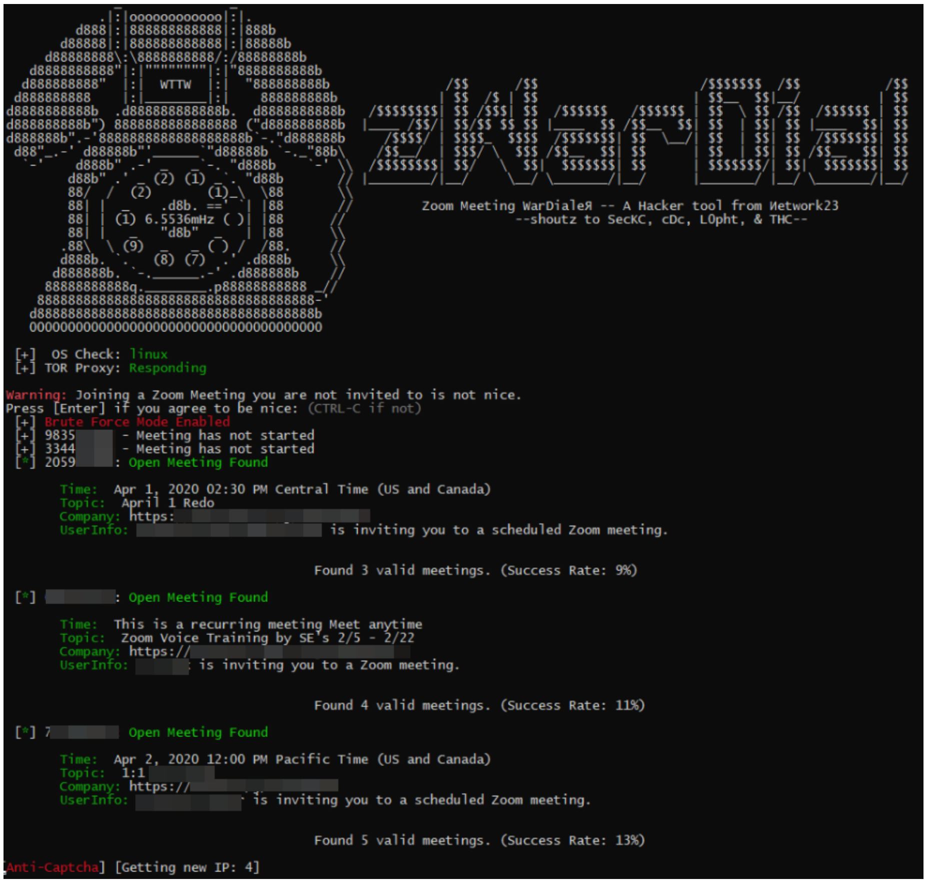
## In-depth security news and investigation

- About the Author
- Advertising/Speaking

02
Apr 20

## 'War Dialing' Tool Exposes Zoom's Password Problems

As the Coronavirus pandemic continues to force people to work from home, countless companies are now holding daily meetings using videoconferencing services from **Zoom**. But without the protection of a password, there's a decent chance your next Zoom meeting could be "Zoom bombed" — attended or disrupted by someone who doesn't belong. And according to data gathered by a new automated Zoom meeting discovery tool dubbed "**zWarDial**," a crazy number of meetings at major corporations are not being protected by a password.



```
                         Zoom Meeting WarDialeЯ -- A Hacker tool from Иetwork23
                                --shoutz to SecKC, cDc, L0pht, & THC--

 [+]  OS Check: linux
 [+] TOR Proxy: Responding

Warning: Joining a Zoom Meeting you are not invited to is not nice.
Press [Enter] if you agree to be nice: (CTRL-C if not)
 [+] Brute Force Mode Enabled
 [+] 9835[redacted] - Meeting has not started
 [+] 3344[redacted] - Meeting has not started
 [*] 2059[redacted]: Open Meeting Found

       Time:  Apr 1, 2020 02:30 PM Central Time (US and Canada)
       Topic:  April 1 Redo
       Company: https:[redacted]
       UserInfo: [redacted] is inviting you to a scheduled Zoom meeting.


                                        Found 3 valid meetings. (Success Rate: 9%)

 [*] [redacted]: Open Meeting Found

       Time:  This is a recurring meeting Meet anytime
       Topic:  Zoom Voice Training by SE's 2/5 - 2/22
       Company: https://[redacted]
       UserInfo: [redacted] is inviting you to a Zoom meeting.


                                        Found 4 valid meetings. (Success Rate: 11%)

 [*] 7[redacted] Open Meeting Found

       Time:  Apr 2, 2020 12:00 PM Pacific Time (US and Canada)
       Topic:  1:1 [redacted]
       Company: https://[redacted]
       UserInfo: [redacted] is inviting you to a scheduled Zoom meeting.


                                        Found 5 valid meetings. (Success Rate: 13%)

[Anti-Captcha] [Getting new IP: 4]
```

zWarDial, an automated tool for finding non-password protected Zoom meetings. According to its makers, zWarDial can find on average 110 meetings per hour, and has a success rate of around 14 percent.

Each Zoom conference call is assigned a Meeting ID that consists of 9 to 11 digits. Naturally, hackers have figured out they can simply guess or automate the guessing of random IDs within that space of digits.

Security experts at **Check Point Research** did exactly that last summer, and found they were able to predict approximately four percent of randomly generated Meeting IDs. The Check Point researchers said enabling passwords on each meeting was the only thing that prevented them from randomly finding a meeting.

Zoom responded by saying it was enabling passwords by default in all future scheduled meetings. Zoom also said it would block repeated attempts to scan for meeting IDs, and that it would no longer automatically indicate if a meeting ID was valid or invalid.

Nevertheless, the incidence of Zoombombing has skyrocketed over the past few weeks, even prompting an alert by the FBI on how to secure meetings against eavesdroppers and mischief-makers. This suggests that many Zoom users have disabled passwords by default and/or that Zoom’s new security feature simply isn’t working as intended for all users.

New data and acknowledgments by Zoom itself suggest the latter may be more likely.

Earlier this week, KrebsOnSecurity heard from Trent Lo, a security professional and co-founder of SecKC, Kansas City’s longest-running monthly security meetup. Lo and fellow SecKC members recently created **zWarDial**, which borrows part of its name from the old phone-based war dialing programs that called random or sequential numbers in a given telephone number prefix to search for computer modems.

Lo said zWarDial evades Zoom’s attempts to block automated meeting scans by routing the searches through multiple proxies in Tor, a free and open-source software that lets users browse the Web anonymously.

“Zoom recently said they fixed this but I’m using a totally different URL and passing a cookie along with that URL,” Lo said, describing part of how the tool works on the back end. “This gives me the [Zoom meeting] room information without having to log in.”

Lo said a single instance of zWarDial can find approximately 100 meetings per hour, but that multiple instances of the tool running in parallel could probably discover most of the open Zoom meetings on any given day. Each instance, he said, has a success rate of approximately 14 percent, meaning for each random meeting number it tries, the program has a 14 percent chance of finding an open meeting.

Only meetings that are protected by a password are undetectable by zWarDial, Lo said.

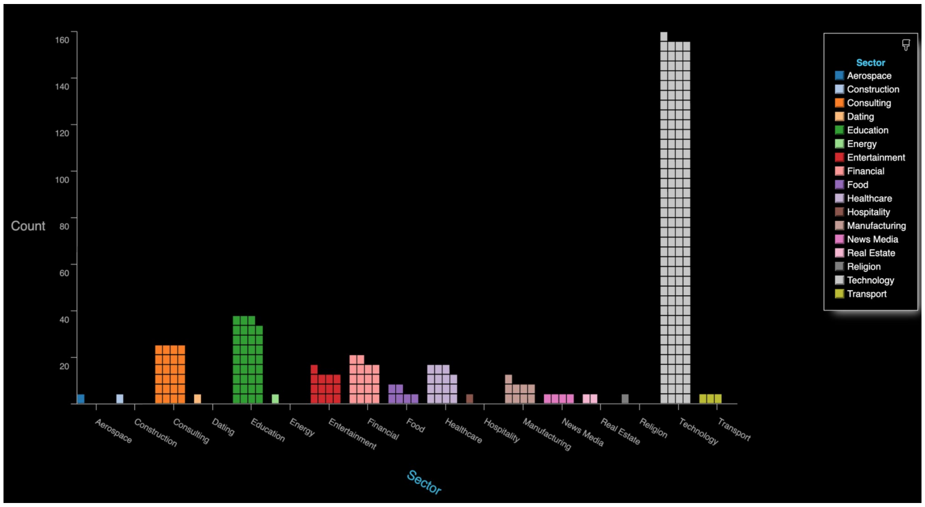
“Having a password enabled on the meeting is the only thing that defeats it,” he said.

Lo shared the output of one day’s worth of zWarDial scanning, which revealed information about nearly 2,400 upcoming or recurring Zoom meetings. That information included the link needed to join each meeting; the date and time of the meeting; the name of the meeting organizer; and any information supplied by the meeting organizer about the topic of the meeting.

The results were staggering, and revealed details about Zoom meetings scheduled by some of the world’s largest companies, including major banks, international consulting firms, ride-hailing services, government contractors, and investment ratings firms.

KrebsOnSecurity is not naming the companies involved, but was able to verify dozens of them by matching the name of the meeting organizer with corporate profiles on LinkedIn.

By far the largest group of companies exposing their Zoom meetings are in the technology sector, and include a number of security and cloud technology vendors. These include at least one tech company that’s taken to social media warning people about the need to password protect Zoom meetings!



The distribution of Zoom meetings found by zWarDial, indexed by industry. As depicted above, zWarDial found roughly 2,400 exposed meetings in less than 24 hours. Image: SecKC.

## A GREMLIN IN THE DEFAULTS?

Given the preponderance of Zoom meetings exposed by security and technology companies that ostensibly should know better, KrebsOnSecurity asked Zoom whether its approach of adding passwords by default to all new meetings was actually working as intended.

In reply, Zoom said it was investigating the possibility that its password-by-default approach may fail under certain circumstances.

“Zoom strongly encourages users to implement passwords for all of their meetings to ensure uninvited users are not able to join,” the company said in a written statement shared with this author.

“Passwords for new meetings have been enabled by default since late last year, unless account owners or admins opted out,” the statement continues. “We are looking into unique edge cases to determine whether, under certain circumstances, users unaffiliated with an account owner or administrator may not have had passwords switched on by default at the time that change was made.”

*Under certain circumstances, users unaffiliated with an account owner or administrator may not have had passwords switched on by default at the time that change was made.*

The acknowledgment comes amid a series of security and privacy stumbles for Zoom, which has seen its user base grow exponentially in recent weeks. Zoom founder and chief executive **Eric Yuan** said in a recent blog post that the maximum number of daily meeting participants — both paid and free — has grown from around 10 million in December to 200 million in March.

That rapid growth has also brought additional scrutiny from security and privacy experts, who’ve found plenty of real and potential problems with the service of late. TechCrunch’s **Zack Whittaker** has a fairly comprehensive breakdown of them here; not included in that list is a story he broke earlier this week on a pair of zero-day vulnerabilities in Zoom that were publicly detailed by a former NSA expert.

Zoom CEO Yuan acknowledged that his company has struggled to keep up with steeply growing demand for its service and with the additional scrutiny that comes with it, saying in a blog post that for the next 90 days all new feature development was being frozen so the company’s engineers could focus on security issues.

**Dave Kennedy**, a security expert and founder of the security consultancy TrustedSec, penned a lengthy thread on Twitter saying while Zoom certainly has had its share of security and privacy goofs, some in the security community are unnecessarily exacerbating an already tough situation for Zoom and the tens of millions of users who rely on it for day-to-day meetings.

“What we have here is a company that is relatively easy to use for the masses (comes with its challenges on personal meeting IDs) and is relatively secure,” Kennedy wrote. “Yet the industry is making it out to be ‘this is malware’ and you can’t use this. This is extreme. We need to look at the risk specific applications pose and help voice a message of how people can leverage technology and be safe. Dropping zero-days to the media hurts our credibility, sensationalizes fear, and hurts others.”

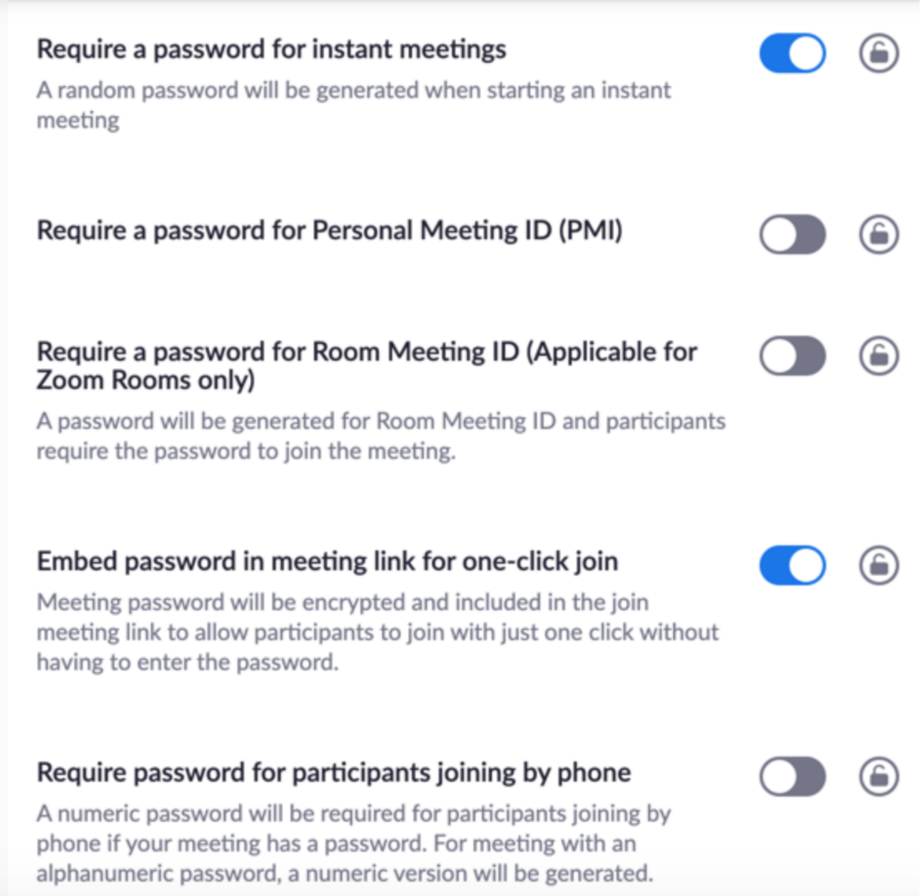
“If there are ways for a company to improve, we should notify them and if they don’t fix their issues, we should call them out,” he continued. “We should not be putting fear into everyone, and leveraging the media as a method to create that fear.”

Zoom’s advice on securing meetings is here. SecKC’s Lo said organizations using Zoom should avoid posting the Zoom meeting links on social media, and always require a meeting password when possible.

“This should be enabled by default as a new customer or a trial user,” he said. “Legacy organizations will need to check their administration settings to make sure this is enabled. You can also enable ‘Embed password in meeting link for one-click join.’ This prevents an actor from accessing your meeting without losing the usability of sharing a link to join.”

In addition, Zoom users can disable “Allow participants to join the meeting before the host arrives.”

“If you have to have this feature enabled at least enable “notify host when participants join the meeting before them,” Lo advised. “This will notify you that someone might be using your meeting without your knowledge. If you must keep your meeting unprotected you should enable ‘Mask phone number in the participant list.’ Using the waiting list feature will prevent unwanted participants from accessing your meeting but it will still expose your meeting details if used without a password.”



**Require a password for instant meetings**
A random password will be generated when starting an instant meeting

**Require a password for Personal Meeting ID (PMI)**

**Require a password for Room Meeting ID (Applicable for Zoom Rooms only)**
A password will be generated for Room Meeting ID and participants require the password to join the meeting.

**Embed password in meeting link for one-click join**
Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

**Require password for participants joining by phone**
A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.

Some of the security settings available to Zoom users. These and others can be found at https://www.zoom.us/profile/settings/

Tags: Dave Kennedy, Eric Yuan, SecKC, Techcrunch, Trent Lo, TrustedSec, Zack Whittaker, Zoom, zWarDial

This entry was posted on Thursday, April 2nd, 2020 at 10:43 am and is filed under A Little Sunshine, The Coming Storm, Time to Patch. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

## 77 comments

1. *Ikijibiki*
   April 4, 2020 at 2:02 pm

   It gets worse.

   “An app with easily-identifiable limitations in cryptography, security issues, and offshore servers located in China which handle meeting keys presents a clear target to reasonably well-resourced nation state attackers, including the People’s Republic of China,” the report says.

   https://www.theregister.co.uk/2020/04/03/dont_use_zoom_if_privacy

2. *iqbaal*
   April 5, 2020 at 10:52 pm

   they write news titles to get viewers too open the links.
   You might add a related video or a picture or twwo to get people sattadon0001

3. *Absalom*
   April 6, 2020 at 11:49 am

   Hello. Mr Bryan Krebs do you think that weight internet traffic resist in this times of coronavirus

   - *Indian Spammer Detector*
     April 28, 2020 at 2:20 pm

Spam!

4. *Vino*
   [April 7, 2020 at 11:47 am](#)

   Hey brian thanksb for running the story. I had this concern back in july 2019. Sent you dm at twitter. We could have avoided catastrophy if you were ran the story before .now nevertheless its not too late

5. *Raymond Luk*
   [April 7, 2020 at 3:05 pm](#)

   Honestly, I have yet seen a zoom meeting from work that requires a password. I also tried to check my own setting, and 1) you can’t setup password setting from the app/client, you have to go to login to the web and look for setting there (srsly who does that?) and 2) my password setting were all disabled and I don’t know when they were ever set

   So my opinion is it seems to be the password settings are disabled by default, and it is not easy to find where to change that setting 🙁

   - *Bob*
     [April 9, 2020 at 3:48 am](#)

     Your company zoom admin can set defaults – you should contact them and ask them to require all meetings have passwords by default

   - *Mo*
     [April 9, 2020 at 8:16 pm](#)

     GoToMeeting does the same, this is not unique to zoom

     - *[kam](#)*
       [April 21, 2020 at 8:57 pm](#)

       can you give me a code

6. *Bruce Lowenthal*
   [April 8, 2020 at 4:55 pm](#)

   What is the recommended minimum size of the password and how is this minimum derived?

7. *[Hector Lopez](#)*
   [April 8, 2020 at 8:48 pm](#)

   Where I can download the code—-¿¿¿?? pls

   - *heckforums*
     [April 15, 2020 at 1:52 am](#)

     heckforums bru

8. *Peter*
   [April 9, 2020 at 3:38 am](#)

   test

   - *[Bikini](#)*
     [April 9, 2020 at 6:42 pm](#)

     Test what u mean test bru

9. *[Hal de Becker](#)*
   [April 9, 2020 at 1:48 pm](#)

It’s striking how much we trust technology and then how easily uninformed users can be taken advantage of. If Zoom corrects their default settings that will help a lot. I also read that they didn’t have solid end-to-end encryption.

10. *George Q Tyrebyter*
April 9, 2020 at 8:55 pm

If someone zoombombs your meeting, so what? What is the harm here?

   - *Victim*
   April 9, 2020 at 11:39 pm

   Organization running a family event for their customers and kids. ZoomBombing happens, random unauthorized individual starts presenting pornographic, violent, torture, death, killing, videos… racial slurs, death threats…

   You get the idea.

11. *Alex*
April 10, 2020 at 8:32 am

Hey, Brian. Can you advise how to report guys buying stolen goods of the money mules?

Any email to report that kind of fraud? Any phone or anything?

12. *Anonymous Group*
April 12, 2020 at 11:07 am

We also have seen some issues in zoom account. Sometimes we had seen that when we run zoom on our smartphone, it works like someone taking screenshot of our every single activity.

https://krebsonsecurity.com/

13. *A College Teacher*
April 19, 2020 at 2:36 pm

Heck, I’m just happy if I can get 1/2 my students to log in even on an open meeting…

Getting bombed might provide enough extra entertainment to make it worthwhile!

(this is sarcasm, but I suspect how some of my fellow faculty think…)

14. *James P*
April 30, 2020 at 6:47 am

Perhaps Zoom should take a note from cloudflare’s book.

Make access via known open proxies and Tor exit nodes disabled by default.

← Older Comments

-

- ## Mailing List

  Subscribe here

- ## Recent Posts

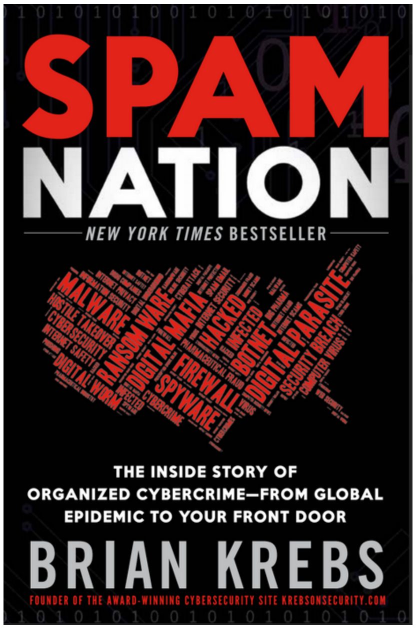
  - QAnon/8Chan Sites Briefly Knocked Offline
  - Breach at Dickey’s BBQ Smokes 3M Cards
  - Microsoft Patch Tuesday, October 2020 Edition
  - Microsoft Uses Trademark Law to Disrupt Trickbot Botnet
  - Report: U.S. Cyber Command Behind Trickbot Tricks

- ## All About Skimmers

Click image for my skimmer series.

Donate with PayPal

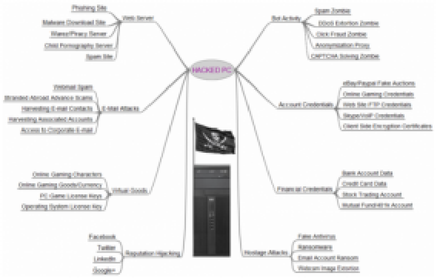
- ## Spam Nation

  
  SPAM
NATION
NEW YORK TIMES BESTSELLER
MALWARE
RANSOM WARE
DIGITAL MAFIA
HACKED
BOTNET
DIGITAL PARASITE
FIREWALL
SPYWARE
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
FOUNDER OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

  A New York Times Bestseller!

- Buy at Amazon

- ## The Value of a Hacked PC

  Badguy uses for your PC

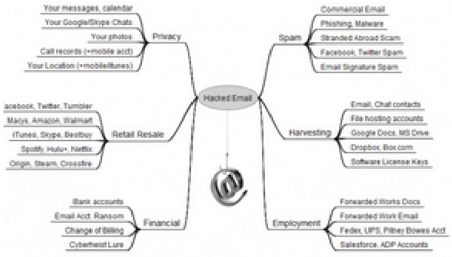
- ## Tools for a Safer PC

  Tools for a Safer PC

- ## The Pharma Wars

Spammers Duke it Out

## Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

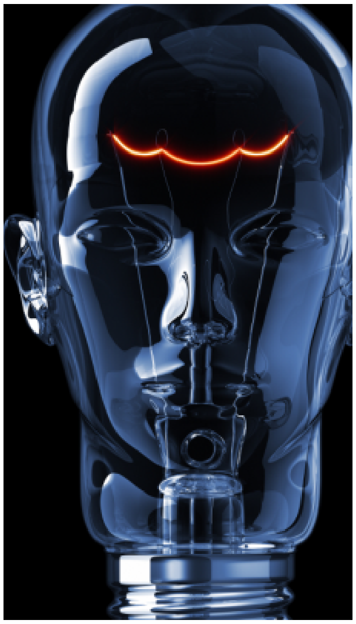
## eBanking Best Practices

eBanking Best Practices for Businesses

## Most Popular Posts

- Sextortion Scam Uses Recipient's Hacked Passwords (1076)
- Online Cheating Site AshleyMadison Hacked (798)
- Sources: Target Investigating Data Breach (620)
- Cards Stolen in Target Breach Flood Underground Markets (445)
- Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
- Was the Ashley Madison Database Leaked? (376)
- True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
- Who Hacked Ashley Madison? (361)
- Following the Money, ePassporte Edition (353)
- U.S. Government Seizes LibertyReserve.com (315)

## Category: Web Fraud 2.0

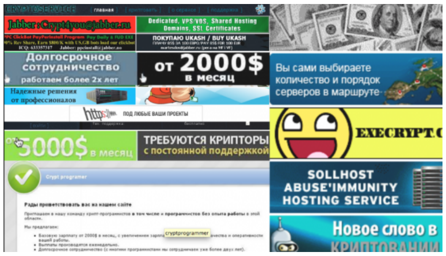


Innovations from the Underground

-
Is credit monitoring really worth it?*
*Not if you can read the fine print

  ID Protection Services Examined

- ## Is Antivirus Dead?

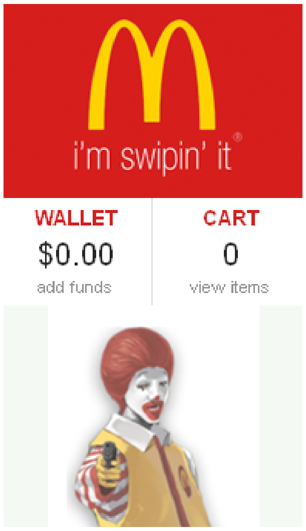
  
Dedicated, VPS/VDS, Shared Hosting Domains, SSL Certificates
ПОКУПАЮ UKASH / BUY UKASH
Долгосрочное сотрудничество работаем более 2х лет
от 2000$ в месяц
Вы сами выбираете количество и порядок серверов в маршруте
Надежные решения от профессионалов
от 3000$ в месяц
ТРЕБУЮТСЯ КРИПТОРЫ с постоянной поддержкой
EXECRYPT
SOLLHOST ABUSE'IMMUNITY HOSTING SERVICE
Новое слово в криптовании

  The reasons for its decline

- ## The Growing Tax Fraud Menace

File 'em Before the Bad Guys Can

- ### Inside a Carding Shop



A crash course in carding.

- ### Beware Social Security Fraud

*my* Social Security– Sign In Or Create An Account

*my* Social Security

Sign in

Create an Account

At each stage of your life, *my* Social Security is for you. Your personal online *my* Social Security account is a valuable source of information beginning in your working years and continuing throughout the time you receive Social Security benefits.

**If you receive benefits or have Medicare, you can:**

Use a *my* Social Security online account to:

- Get your benefit verification letter;
- Check your benefit and payment information and your earnings record;
- Change your address and phone number; and
- Start or change direct deposit of your benefit payment.

Sign up, or Be Signed Up!

- ### How Was Your Card Stolen?

Finding out is not so easy.

- **Krebs's 3 Rules…**

...For Online Safety.

© 2020 Krebs on Security. Powered by WordPress. Privacy Policy