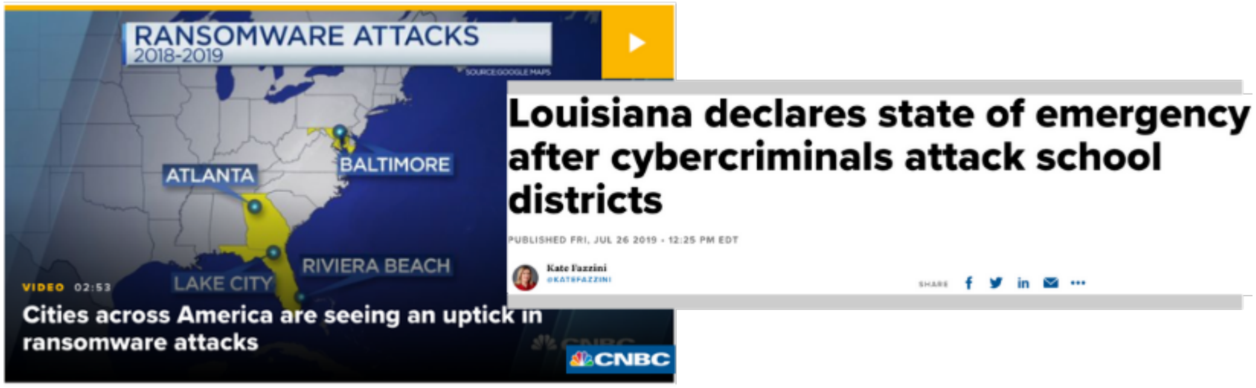
In July, the Governor of Louisiana declared a state of emergency in response to a rash of cyberattacks against its schools. The declaration is the second one of its type since Colorado did the same last year.



Cities across America are seeing an uptick in ransomware attacks

Louisiana declares state of emergency after cybercriminals attack school districts

PUBLISHED FRI, JUL 26 2019 · 12:25 PM EDT

Kate Fazzini
@KATEFAZZINI

SHARE

On Tuesday last week, La. Gov. John Bel Edwards, still reeling from the aftermath of the attacks, said:

"While it's school systems today, it could be any public or private entity tomorrow. This is really serious." La. Gov. Edwards. Read more.

Now, the National Governors Association advises all states to:

"... develop response plans that put cyberattacks on the same level of severity as natural disasters or acts of physical terrorism." National Governors Association, more.

This, after Naples was the fourth city in Florida to report a breach and loss costing $700,000. According to the FBI, victims in Florida lost $83 million in 2018 to the same scam Naples suffered last week

✓ In each case, from Baltimore to Florida, to Louisiana, the hacks and financial losses were avoidable with basic employee training and elementary cybersecurity solutions.

Why is this happening?

Sophisticated cyber-attacks against smaller, unprotected targets is a booming business.

Big companies and organizations, like the headline breaches of years past, are generally harder targets now. After years of attacks and regulatory pressures they require more resources and patience to attack successfully.

- Today, when large organizations are attacked, it's not so much for intellectual property or trade secrets anymore as it is for the vast pools of personal information they hold - to be used against smaller, less prepared targets in the future.

The public sector? They're slower to adapt and thus, easier to hack. As we heard last month from one of the three Florida cities that paid big-dollar ransoms:

"Every day I'm learning how this even operates because it just sounds so far fetched to me." A Florida city council chair, more.

Lack of awareness and preparedness make bloody waters for cyber-predators using NSA-grade hacking tools today.

✓ Unfortunately, we will continue to see spikes in public sector activity that will prompt more emergency measures across the country.

The public sector is expected to be transparent with issues affecting tax-payer money and public policy. When schools, municipalities, police departments, and others are hacked, it makes the news - at least on a local basis.

Attacks on small, private entities are rarely reported to the press, and it happens far more than most understand.

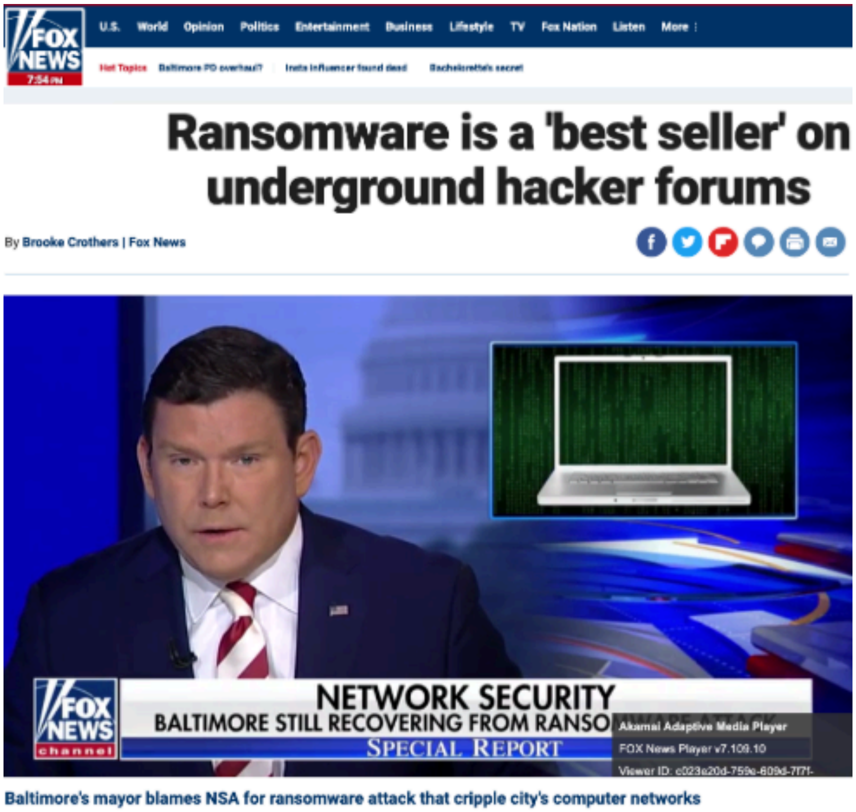
✓ Small targets are suffering from sophisticated attacks because the profit motive is so great, and so few are prepared to defend

Cybercrime-as-a-Service

Cyber-syndicates are building "as-a-service" platforms to scale their growth and pump massive illegal profits.

The operators provide subscribers, or "affiliates" the tools they need for cyber-attacks and split the spoils 60/40 with the syndicate. No resume' or experience required, and no technical expertise or capital outlay needed.

Anyone with a computer browser can subscribe.



Ransomware is a 'best seller' on underground hacker forums

By Brooke Crothers | Fox News

Baltimore's mayor blames NSA for ransomware attack that cripple city's computer networks

How's the payday?

The planet's #1 cyber-sleuth is Brian Krebs. Nobody disputes that. Many cyber-actors from around the world wish he wasn't around at all.

This month, Krebs shared some deep looks into cyber activity in the U.S. and how the criminal infrastructure is being built to scale for criminal profits around the world.

First up, the state of ransomware:

"The cybercriminals behind the ransomware-as-a-service offering recently announced they were closing up shop and retiring after having allegedly earned more than $2 billion in extortion payments from victims.

Retiring on $2 billion? Tax-free? Not a bad gig.

Oh, wait. It turns out the cybercrime biz is too good to quit, so now it seems:

"... the criminal team have instead (of retiring) quietly regrouped behind a more exclusive and advanced ransomware programs ..." Krebs

In another report, from Wired magazine on August 1st, three Ukrainians were shut down after earning upwards of $1 billion. More; "The Inner Workings of a Billion-Dollar Hacking Group."

Yes, it's a pattern. Cybercriminals are more ambitious and thinking bigger than ever. Suddenly, uber-wealth status is in reach for anyone with an internet connection and some imagination.

✓ It's the promises of great riches that are fueling hyper-growth in cybercrime.

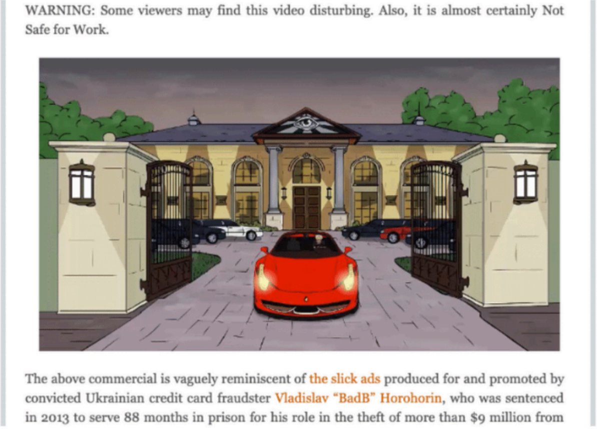
According to Krebs' intelligence, cybercrime-as-service is so profitable that operators are now advertising on the Dark Web for affiliates to partner in their growth and fortune. For more about *"Party Like a Russian"* see below.

Party Like a Russian, Retire Like a King

Krebs discovered a video clip on the Dark Web advertising a ransomware-as-a-service platform. The ad, produced by a criminal syndicate operating a cybercrime-as-a-service business, is marketing to would-be hacker millionaire wannabes.

The video ad promises to equip "affiliates" with all they need to begin mouse-clicking their way toward living their best dreams today and retiring rich tomorrow.

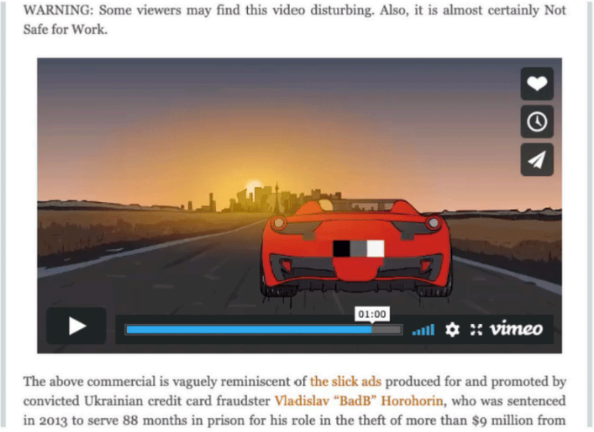
Party Like a Russian



WARNING: Some viewers may find this video disturbing. Also, it is almost certainly Not Safe for Work.

The above commercial is vaguely reminiscent of the slick ads produced for and promoted by convicted Ukrainian credit card fraudster Vladislav "BadB" Horohorin, who was sentenced in 2013 to serve 88 months in prison for his role in the theft of more than $9 million from

Retire Like a King



WARNING: Some viewers may find this video disturbing. Also, it is almost certainly Not Safe for Work.

The above commercial is vaguely reminiscent of the slick ads produced for and promoted by convicted Ukrainian credit card fraudster Vladislav "BadB" Horohorin, who was sentenced in 2013 to serve 88 months in prison for his role in the theft of more than $9 million from

I'm not linking the video here because it's disgusting. But it's on Krebs' site (it's his job to post this stuff.)

The point is this - these guys going big in cybercrime know their market. The aim of their advertising video is to target prospective new affiliates that:

" ... that mostly views America's financial system as one giant ATM that never seems to run out of cash." Krebs

The ad for criminal affiliates hits all the notes for one that feels they are due a better life and sees the U.S. as a boundless ATM for retribution.

✓ Cybercrime is becoming known as the fastest, easiest path to great riches by those that feel marginalized, excluded, and disadvantaged by society.

Why are so few caught?

The nature of digital crime is free from many of the obstacles and limitations held by traditional crime. Professional perpetrators know how to exploit the strength of their digital (virtual) operation against weaknesses in tax and law enforcement authorities built around conventional (physical) systems.

✓ Criminal syndicates in cyber-space use "bulletproof" systems - named for their ability to deflect law enforcement and legal jurisdiction.

"Bulletproof hosting administrators operating from within Russia probably are not going to get taken down or arrested, provided they remain within that country (or perhaps within the confines of the former republics of the Soviet Union)." Krebs

In the "bulletproof" domain, subpoenas and complaints don't matter.

The passport for Alexander Volosovyk a.k.a. "AbdAllah," a major operator of bulletproof hosting services.
https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/

Servers allegedly tied to AbdAllah's bulletproof hosting network. Image: Gp.gov.ua.
https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/

Alexander Volosovyk, a major operator of bulletproof hosting services.

✓ Perpetrators succeed by leveraging the lack of awareness, defenses, and retribution from small, unprepared targets. Particularly in foreign jurisdictions.

What's next?

Cybercrime, for more and more around the world, is the fastest, easiest path to great riches and a better life.

- cybercrime is easy - you can make a fortune from your couch as an "affiliate"
- hacking tools work - the NSA developed many of them
- the loot is anonymous, portable, and liquid - no laundering, fencing, etc.

And for the growing ranks of aspiring black-hats everywhere, the U.S. is target #1.

- it's where the money is
- as a nation, we are among the least aware of digital risk
- we think the internet is free
- and we do not value our personal information or privacy near the level of other developed countries

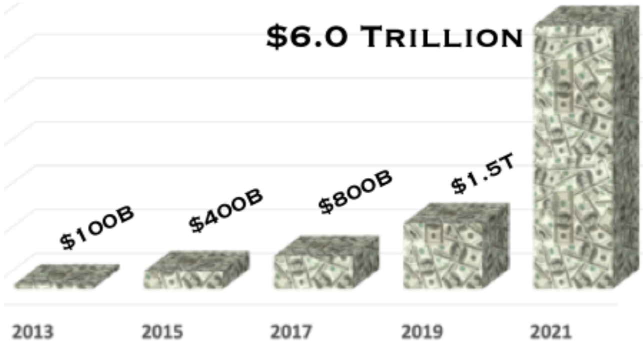
The bad guys are looking for the most unaware and unprepared targets - and today, that's people, their technology and information, their email, banking, and investment accounts.

✓ So, what's next is waves of financial loss, blackmail, extortion, fraud, and scams perpetrated on individuals over their everyday technology.

When will it end?

How long will it take before the risk/reward equation for cybercrime finds its clearing point? And how much will it cost before we are resilient enough to level the field?

Reports say it will be years and trillions in dollars, and it represents the greatest transfer of wealth ever.



It is likely a cybercriminal will rank in the Forbes wealthiest list by 2023. It won't be by hacking Home Depot or Target. It will be on the backs of hordes of slow-to-adapt individuals and small entities everywhere.

But, mostly from the U.S.

✓ We have several years at least before cybercrime activity climaxes, peaks, and levels. Digital security and information protection will eventually be a part of everyday mainstream activities.

What to do?

Criminal actors from around the world are increasingly focusing on low-hanging fruit. They're attacks are "opportunistic" - aiming for small targets, unaware, unprepared - and potentially lucrative when faced against military-grade hacking tools.

- For cybercriminals, target size will decrease, and attack volume and success rates will increase.
- For the rest of us, it means don't be low-hanging fruit and avoid "opportunistic" attacks

The risk is manageable. But certain changes are invariably required sooner or later. We call them *"The Four Fundamentals of Cybersecurity for Life."*

The Four Fundamentals approach essentially builds an eco-system for considerably more privacy and much less cyber-risk for all you do.

✓ Don't be low-hanging-fruit.

The #1 best way to start is by privatizing your personal email.

Privatize Personal Email

Every loss we mentioned in the first section of this letter started with an email. Almost 90% of all successful cyber-attacks start with an email.

In July a grand jury in California said it's not so much "fake news" and disinformation that is risking our elections - it's our damn email accounts!

Krebs wrote about the grand jury's report and called email "unsexy." I know exactly what he means - people could care less about their email accounts.

Fact is though that nothing works better to reduce risk and increase digital autonomy. And, importantly, to begin the process of owning more of your personal information (vs Big Tech and your email provider.)

Private email is a game-changer. And it's affordable, simple, and very secure.

✓ Talk to Diane, she's an email pro: diane@totaldigitalsecurity.com

Thanks for reading,

Brad

Brad Deflin

Read online - https://www.totaldigitalsecurity.com/support-resources/newsletter

18th Annual

TOTAL WEALTH SYMPOSIUM

September 12th – 14th, 2019

Omni Amelia Island Resort
Amelia Island, FL

ABOUT THE EVENT

The **Total Wealth Symposium 2019** is Banyan Hill Publishing's premier event of the year. From **September 12-14, 2019**, we are assembling the best minds in finance in Amelia Island, Florida.

Paul Mampilly, Matt Badiali, Mike Carr, Ted Bauman, Ian King, Chad Shoop and nearly a dozen other investment and asset protection professionals will be there, and we're pulling out all the stops for this year's event.

Here's what you can expect:

- Three days of exclusive presentations from the top financial minds in the industry

Total Wealth Symposium

Brad Deflin returns for the 5th consecutive year to speak on "Cybersecurity fro Life" with Sovereign Society members and investors at the Total Wealth Symposium in Amelia Island this September.

Read More

YPO - Gold Chapter

It will be Milwaukee in December for ***"Cybersecurity for Life - how to protect in a new age of risk."*** with the Wisconsin YPO Gold Chapter.

Read More

Top VPNs Secretly Owned by Chinese

"Nearly a third of top VPNs are secretly owned by Chinese companies, while other owners are based in countries with weak or no privacy laws, potentially putting users at risk, security researchers warn."

Read More

DHS - General Aviation at Risk to Flight Data Manipulation

DHS Warns Small Airplanes Vulnerable to Flight Data Manipulation Attacks via @TheHackersNews

Read More

Stormy Summer for Scams

Last couple of months show trends including **"The Strong-arm Hack."** As usual, email is the source, so here's an email checker tool too.

Read More

The best way to start protecting?

Go private! Over 80% of cybercrime originates with an email.

- Own your email - not Big Tech
- Professionals, families - for privacy, security, and physical safety

https://www.totaldigitalsecurity.com/products/private-email/purchase-private-email-form