

[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](#)

16

Jul 18

'LuminosityLink RAT' Author Pleads Guilty

A 21-year-old Kentucky man has pleaded guilty to authoring and distributing a popular hacking tool called “**LuminosityLink**,” a malware strain that security experts say was used by thousands of customers to gain unauthorized access to tens of thousands of computers across 78 countries worldwide.


[Home](#)
[Features](#)
[Pictures](#)
[Help](#)
[Buy Now](#)

Introducing LuminosityLink

Feature Packed and Incredibly Stable, Luminosity Brings new innovations to the table!



Surveillance

Luminosity allows you to control your clients via Remote Desktop, Remote Webcam, and a professional Client Manager.



File Manager & Searcher

View, download, and delete files on your clients computer. You may also search for specific files, and have them uploaded automatically.



RDP Manager

Login and control your systems on a new user session via Microsoft Remote Desktop Protocol (RDP)



Malware Remover

Remove Malicious Items on your clients computer. In addition, you may block specific processes, and stop the installation of specified software.



Reverse Proxy

Use your clients IP Address as a SOCKS 5 Proxy in any application. Very stable and fast!



Password Recovery

Recovers Lost Passwords from all Major Web Browsers, all Email Clients, FileZilla, and Windows Serial Key.

[View Pictures](#)[Purchase Now](#)

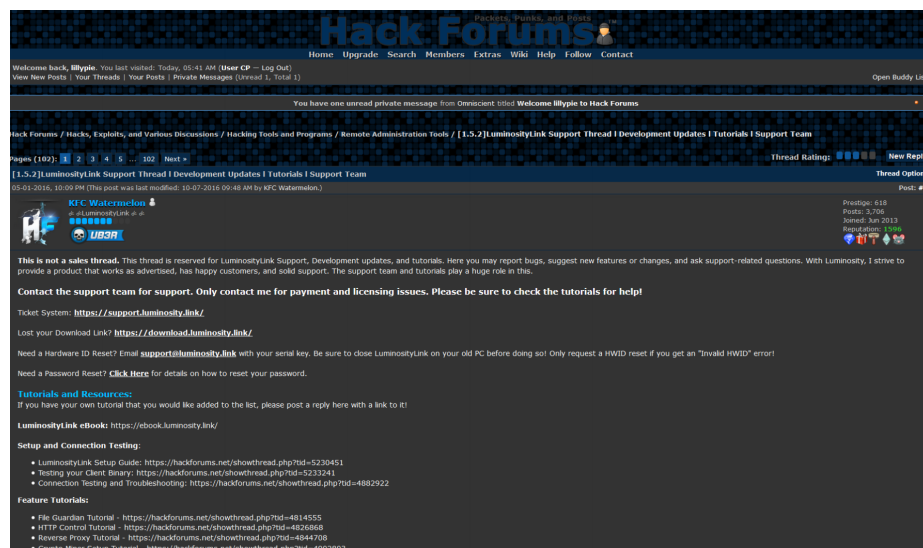
The LuminosityLink Remote Access Tool (RAT) was sold for \$40 to thousands of customers, who used the tool to gain unauthorized access to tens of thousands of computers worldwide.

Federal prosecutors say **Colton Ray Grubbs** of Stanford, Ky. conspired with others to market and distribute the LuminosityLink RAT, a \$40 Remote Access Tool that made it simple for buyers to hack into computers to surreptitiously view documents, photographs and other files on

victim PCs. The RAT also let users view what victims were typing on their keyboards, disable security software, and secretly activate the webcam on the target's computer.

Grubbs, who went by the pseudonym “**KFC Watermelon**,” began selling the tool in May 2015. By mid-2017 he'd sold LuminosityLink to more than 8,600 customers, according to [Europol](#), the European Union's law enforcement agency.

Speculation that Grubbs had been arrested began [surfacing last year](#) after KFC Watermelon stopped responding to customer support queries on [Hackforums\[dot\]net](#), the Web site where he primarily sold his product.



Grubbs, using the hacker nickname “KFC Watermelon,” advertised and sold his RAT via Hackforums.net.

The sale and marketing of remote access tools, also known as remote administration tools, is not illegal in the United States, and indeed there are plenty of such tools sold by legitimate companies to help computer experts remotely administer computers.

However, these tools tend to be viewed by prosecutors instead as “**Remote Access Trojans**” when their proprietors advertise the programs as hacking devices and provide customer support aimed at helping buyers deploy the RATs stealthily and evade detection by anti-malware programs.

According to the indictment against him, Grubbs “recruited and encouraged co-conspirators to answer questions on Skype, an internet messaging service, from potential and actual purchasers of LuminosityLink seeking to use the software to get unauthorized and undetected access to victim computers and steal information.”

Linking Grubbs to LuminosityLink was likely not a tall hurdle for prosecutors. A [public filing](#) at the **Kentucky Secretary of State** office lists Grubbs as the owner of **Luminosity Security Solutions LLC**.

However, there are indications that Luminosity was not Grubbs' first foray into making and selling malware tools. According to [a February 2018 blog post](#) by **Palo Alto Networks**, the Skype account connected to KFC Watermelon's identity on Hackforums is tied to the email address “codyjohnson1337@live.com; that email account was used in 2013 to register “plasmarat.pw,” a similar RAT sold and marketed on Hackforums.



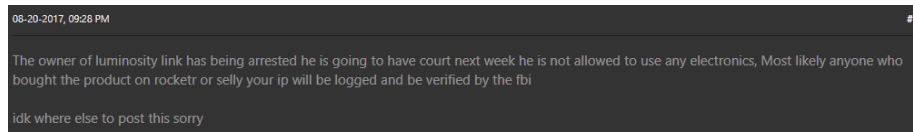
KFC Watermelon's Skype profile (the "HF" in his Skype name is a likely reference to HackForums, where both Luminosity RAT and Plasma RAT were primarily sold and marketed).

The street address listed by the Kentucky Secretary of State's office for Luminosity Security Solutions (127 Circle Dr., Stanford, KY) shows up in the original registration records for dozens of domains, including at least a half-dozen that early on listed the email address coltongrubbs@gmail.com. That same email address appears in the early registration records for [barracudasec\[dot\]com](http://barracudasec[dot]com), a domain that as far back as 2012 was identified as a popular "command and control" server that many denizens of Hackforums used to remotely administer large numbers of remotely commandeered computers or "bots."

Around the time that KFC Watermelon stopped responding to support requests on Hackforums, federal prosecutors were [securing a guilty plea](#) against **Taylor Huddleston**, a then 27-year-old programmer from Arkansas who sold the "NanoCore RAT." Like Grubbs, Huddleston initially pleaded not guilty to computer intrusion charges, arguing that [he wasn't responsible for how customers used his products](#). That is, until prosecutors presented Skype logs showing that Huddleston routinely helped buyers work out how to use the tools to secretly compromise remote computers.

Grubbs' guilty plea could well lead to further arrests and prosecutions of customers who purchased and used LuminosityLink. Case in point: The author of the **Blackshades Trojan** — once a wildly popular RAT sold principally on Hackforums — was arrested along along with dozens of his customers in [a global law enforcement sweep](#) in 2014.

Indeed, many former customers of LuminosityLink have posted to Hackforums that they are expecting similar treatment:



Hackforums users speculate that Grubbs' arrest could lead to the arrest and prosecution of his customers. Image: Palo Alto Networks.

Grubbs initially pleaded not guilty, and his trial was slated to begin in August. But in a plea agreement released today, Grubbs admitted to conspiring to make and sell LuminosityLink, and to knowingly assisting customers in using his software to break into computers.

The plea agreement notes that on July 10, 2017, when Grubbs found out the FBI was about to raid his apartment, he hid the phone and debit card tied to his Bitcoin account, and also removed the hard drives from his computer and apartment prior to the search. "Three days later, Defendant transferred over 114 bitcoin from his LuminosityLink bitcoin address into six new bitcoin addresses," the agreement states.

The charges to which Grubbs has pleaded guilty carry punishments of up to 25 years in prison and as much as \$750,000 in fines, although any sentence the judge hands down in this case may be significantly tempered by U.S. Sentencing Guidelines.

A copy of the plea agreement is available [here](#) (PDF).


Tags: [Blackshades trojan](#), codyjohnson1337@live.com, [Colton Grubbs](#), [Colton Ray Grubbs](#), [Hackforums](#), [KFC Watermelon](#), [Luminosity Security Solutions LLC](#), [LuminosityLink](#), [NanoCore RAT](#), [Palo Alto Networks](#), [plasma rat](#), [RAT](#), [remote access tool](#), [Taylor Huddleston](#)

This entry was posted on Monday, July 16th, 2018 at 3:09 pm and is filed under [Ne'er-Do-Well News](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. Both comments and pings are currently closed.

38 comments


1.  [The Sunshine State](#)
[July 16, 2018 at 3:22 pm](#)

Good read !

2.  [JCitizen](#)
[July 16, 2018 at 4:00 pm](#)

The ignorant news media pop stories once and a while about RAT Trojans, with absolutely no explanation as to what they do, and in fact they act like it was a specific name for a specific Trojan variation. Good thing the public can come to KOS to get the straight poop on just what it is, and what is going on!

We can't thank you enough, or donate enough to show our true appreciation Brian!

3.  [vb](#)
[July 16, 2018 at 4:38 pm](#)

Mr Grubbs should learn a lesson from Martha Stewart – the obstruction charges matter. Martha was cleared of the fraud charges, but went to prison for obstruction.

This is what gets you prison time:

“...he hid the phone and debit card tied to his Bitcoin account, and also removed the hard drives from his computer and apartment prior to the search. “Three days later, Defendant transferred over 114 bitcoin from his LuminosityLink bitcoin address into six new bitcoin addresses,”



o *Lars*

[July 16, 2018 at 9:01 pm](#)

But how do they prove he was trying to hide the money and not just pushing his funds around coincidentally?... and spring cleaning his hard drive..



▪ *Quid*

[July 16, 2018 at 9:52 pm](#)

@Lars#1

https://www.law.cornell.edu/wex/mens_rea

It's a judgement call, like all criminal and civil cases.

Circumstantial evidence (timing (routine or one-off), methodology, etc.) coupled with the defendant's explanation (purpose of actions) and attitude, the prosecutor's and defense counsel's arguments and actual evidence, the judge and jury's perception determines guilt(y) or not guilty. Legal guilt may or may not be the same as "truth".



▪ *treFunny*

[July 17, 2018 at 9:06 am](#)

Yeah that didn't make it look good....

kind of like writing 0 and 1s to a server that might have incriminating emails on it (hint hint hint HRC)... nothing to see there though!



▪ *Anon404*

[July 18, 2018 at 1:20 pm](#)

According to the FBI and years worth of investigations, no there wasn't. 32 indictments and 4 guilty pleas after 1 year and Mr Trump is starting to look awfully guilty though.



▪ *Anon E. Moose*

[July 17, 2018 at 11:17 am](#)

We could put our heads in the sand and ignore the circumstantial evidence. Or figure he got wind of the raid, and decided that his approx. \$750000 was better served in several baskets instead of one big one.

Questions should be asked like:

How was it distributed? In what amounts, to whom?

Could it be payment for accomplices?

Could this guy be a high end mule?

Is it just coincidence that the distribution occurred at that time?

Investigations into criminal activity need to poke and prod at many different angles to unearth the buried truth.



4. *Lee*

[July 16, 2018 at 5:20 pm](#)

Brian,

Thank You for your education that you provide to us on how these asswipes work to steal our information. We are wondering if you know of any tools that can find and identify these "RAT"s on our systems that anti-virus programs like NOD32 or Microsoft Security Essentials may miss or get deactivated?

Also how do you scan e-mails and their attachments that are stored on e-mail servers (web based e-mails) like msn.com, outlook.live.com, hotmail.com and gmail.com that may harbor malicious spyware, Trojans and rat's in the pictures in attachments and embedded in the e-mails body's waiting to be opened allowing the crap-ware to open and embed on our local systems?

At least in the old days we could download and store the e-mails and attachments to our computer first and scan the entire batch before opening the e-mails and if there was rat's or malware present we could quarantine and delete before any trouble could be caused.

So do you have a detector program to find "RAT's" like the "Luminosity Link" and others?

Thank You in advance and may God's blessings be upon you for your great service that you provide for us!



Quid

[July 16, 2018 at 8:59 pm](#)

@Lee,

Web-based email can still be downloaded locally using an email client bundled with your OS (Windows or MacOS) or a 3rd party free email client such as Thunderbird or pay for MS Outlook.

<https://www.tenforums.com/tutorials/64683-turn-off-email-account-windows-10-mail-app.html>

<https://www.thunderbird.net/en-US/>

BUT, do you really want to download potential malware to your local computer versus letting the email provider scan it first? Because thinking that whatever antimalware/antivirus software you have on your local computer will always be superior to Outlook.com, Gmail.com, or other major providers, is likely incorrect.

<https://support.google.com/mail/answer/25760?hl=en>

<https://www.mail.com/mail/antivirus/503882-virus-scan.html#.473882-stage-link1-6>

You can safely preview MS Office (.docx, .xlsx, .pptx, etc.) attachments via the browser, without downloading when using Outlook.com and likely other providers. They are just an image of the real file and any macros would be disabled.

Executable (.exe, .bat, .com, etc.) file attachments would be scanned also, but could still escape detection the first day or week, if malware. But who would be sending you an .exe file unannounced? I just tried sending myself a batch (.bat) file via Outlook.com and it won't let me access the file.

You can forward suspect emails with their attachments to VirusTotal and get 50+ different antimalware programs to scan your attachments. Even then there is no guarantee that a zero-day malware won't slip past all of them, there is strength in numbers.

<https://www.virustotal.com/en/documentation/email-submissions/>

You wouldn't want to forward sensitive personal email to VT, just the suspicious ones that you still believe you should open.

Spearphishing type emails, Adobe Flash, and malvertising are the most likely paths to infection. Don't click on email links or attachments without thinking, disable Flash, install uBlock Origin ad blocker as well as keeping your antivirus/antimalware up to date.

Quid



Lee

[July 17, 2018 at 1:40 am](#)

Quid,

Thank you for the informative reply. We are trying to help a friend that we are quite sure a keylogger or rat was installed upon her computer. She is legally blind and although we can wipe and reinstall her o/s, the person we suspect may have installed thru a .jpeg pictures that he likes to send about his winnings in Vegas, pictures of jackpots. I think it is called "stenography" or something like that.

Similar with malware embedded text messages, therefore we have a flip phone with no text ability.


We have our suspicions ever since the last time we found a Trojan rat on her system and she tells me that she does not click on links, but the pictures come as attachments in the body of the message.

We just need to be able to prove the extent of his tainted e-mails so she will let us block him, however these kinds of asswipes have a way of sweet talking and getting their fangs into vulnerable people and make us out to be the bad guys for wanting to keep our family members safe.

We are very familiar with safe computing and blocking large numbers of domains from our e-mail. However even Microsoft and gmail e-mail systems let bad payloads through. Also even if we are expecting an attachment we still call the person just to verify the name and size of the attachment.

I do keep one computer that is airgapped from our system just for experimenting with suspicious files and hard drives, flash drives and SD cards. Amusing what we find, that is why we need a rat detector to help detect this guy and his game.

Thank You in advance,
Lee

o  *Hav0c*
[July 17, 2018 at 10:04 am](#)

@Lee –

attack vectors for computers are

- 1) email
- 2) web
- 3) removable drives
- 4) physical access (directly tamper with system, tamper with your network gear, jackbox, change DNS, ...)

Best way to prevent persistence assuming computer only is to surf from a bootable drive running Linux/Ubuntu. (CD, non writeable USB (Kanguru)). Your session can be taken over, you can leak data, but attacker cannot persist.

Plan B is to surf from an OS running within a VM and have it revert to native state on power-off.


If privacy is not a concern, you can get a security suite that proxies your traffic through a cloud firewall This will give you some indications of malicious behaviour, but a lot of good malware will evade detection initially, though social engineering is harder to pickup since there is no malware and may be targeted specifically.

Email is the easiest way to reach someone or have them come back to you. Largest attack vector against layer 8. I only open ~ 5 – 10 percent of emails that I know I went looking for and expected. If at a company Proofpoint, Mimecast, MS Advanced threat Protection. If personal on MS sign up for Pro/Plus account and get Exchange Online Protection (EOP) equiv (pretty weak).

Web surfing – I would use bootable OS (CD/USB – non-writeable) or OS in VM reverting to native state. VPN with security features (web firewall) may help. A lot of the good malware will score 0 hits out of ~ 60 on virustotal, so caveat emptor.

USB/local drives – dont plug anything into your system that you dont have pretty good comfort level came from a reliable source that practices good hygiene.

Physical – dont let anyone have access to your systems.

■  *vb*
[July 17, 2018 at 12:20 pm](#)

Just use a Chromebook for email and browsing.

Unchangeable OS, unchangeable hardware, minimally changeable browser. The only known malware are browser extensions installed by trickery. That malware takes about 10 seconds to uninstall. If in doubt, you can “powerwash” the Chromebook in a couple minutes.

■  *SeymourB*
[July 19, 2018 at 5:21 pm](#)

Where there's a will there's a way. Chromebooks can be infected but the infections are generally only persistent until the next update is released. Or, sometimes, until the system is rebooted.

The problem I have is that the Chromebooks I'm responsible for are in the hands of individuals who get pop-up notifications about updates that need to be installed which they promptly ignore because zomg social media is more important. I set the policy that forces a reboot once a month but half the time that policy doesn't work because people bring in Chromebooks that haven't been updated in 6+ months for help because they're not working properly.

5.  *Andrew*
[July 16, 2018 at 7:57 pm](#)

It is just pure arrogance that these people use easily identifiable accounts to register domains that are linked to Dark Web Activities?

I'm always amazed at the raw/pure talent of these people to create such a tool but then the sheer stupidity of the online breadcrumb trail.

o  *MattyJ*
[July 16, 2018 at 8:27 pm](#)


I think the second word in the article (“21-year-old”) explains a lot. The kids these days have no idea how this Internet thing works. You don't usually see 40-year-old fraudsters making mistakes like this.

■  *BrianKrebs*


[July 16, 2018 at 8:29 pm](#)

Actually, you do. It's just that usually those people are not from the United States.

The truth is that most cybercriminals — including many career cybercrooks — positively suck at operational security. And thank goodness.

■  [Alexander](#)
[July 17, 2018 at 2:52 am](#)

NSA hackers don't make mistakes .
Unit 8200, NSO Group, etc.

■  [Russell](#)
[July 17, 2018 at 8:52 am](#)

Except when the NSA itself gets hacked (Snowden, Hal Martin, Shadow Brokers, etc.) So even the NSA makes security mistakes.

“A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools.”

— Douglas Adams

■  [treFunny](#)
[July 17, 2018 at 9:10 am](#)


Saying the NSA was hacked is a bit of a stretch....

All of these folks copied not hacked: Snowden, Hal Martin, Shadow Brokers.


BUT hey it makes great headlines

■  [Betty Torrey](#)
[July 17, 2018 at 8:59 am](#)

OPSEC is hard.

6.  [Lars](#)
[July 16, 2018 at 9:13 pm](#)

Kid wouldve benefited from brushing up on the law, it seems. Too bad he turned to the dark side, did he actually develop luminositylink himself? It seems pretty impressive, the only difference between this and a legit RSAT is that this kid coached users on how to evade AV detection, right? I never understood why these youngsters would waste their talent by using their knowledge to perpetrate fraud. Such a shame.

○  [Hav0c](#)
[July 17, 2018 at 10:50 am](#)


It may be a pathing issue.
Assuming this is all his code, he clearly has some talent in that area.

It is unclear his level of education – but if his parents were not in IT/coders it is likely he fell in the wrong crowd and obtained recognition for his talents from the hacker community.

At 21 – what is easier? Develop and publish an app \$40 * 8.600 = \$344,000. or try and navigate the process of finding coding work with no resume/experience, where you have to get through resume parsers, HR people that can't ferret out talent, and bureaucracy?

Clearly 1 is a potentially lucrative long-term path that will probably NOT land you in jail, but at 21, with little guidance and the allure of fame and a nice chunk of money, it is not hard to see the first path.

We need to do a better job (as a society/and the IT industry) of recognising talent and getting the right path. Somebody knew what this guy could do back in school, he should have been identified and funneled for success.

-  *McLaughlin*
[July 17, 2018 at 11:18 am](#)

It really is too bad.

We need to find a way to simultaneously serve justice and rehabilitate this kid. It seems like he just needed better guidance and support from the start.

Such a waste of talent...


- 7.  *Reader*
[July 18, 2018 at 4:19 am](#)

He should've taken it to trial. This is begging for jury nullification.

Inventors, artists, engineers, authors, and coders shouldn't have to be responsible for what bad people do with their creations. If you write a book on being a ninja, it's the ninja who's responsible for its use, not you.

A jury would have also realized that it's perfectly natural to hide stuff when you think someone, like the government or a jackbooted thug, wants to take your stuff.

All he appears to be guilty of is good marketing skills and helping people use his product. Big deal.


-  *Bobby Jr*
[July 18, 2018 at 8:56 am](#)

"According to the indictment against him, Grubbs "recruited and encouraged co-conspirators to answer questions on Skype, an internet messaging service, from potential and actual purchasers of LuminosityLink seeking to use the software to get unauthorized and undetected access to victim computers and steal information.""

He helped them commit crimes (allegedly). That means he does, in fact, bear some responsibility for what his customers did since, you know, he actually helped them do it. And it also means he was well aware of the illegal acts his product was being used for and that he, effectively, encouraged them.

Brian explained it pretty well in the article (and, IIRC, in other articles as well). You'd be 100% right if he didn't choose to market the tool places where known black hats play and then help said black hats use the tool to do black hat stuff. Thing is, he did – hence the case against him.

All that said, I'm in full agreement with your sentiment. You can't hold someone responsible for what someone else does with their product. The only difference here is that he helped people do the illegal stuff.

-  *Reader*
[July 19, 2018 at 5:25 am](#)

Brian reported and provided analysis of the government activities and his research on the subject. He did not (and, as a journalist of high ethics, should not) attempt to justify how the law is applied.


I'm not a journalist, so I've got no qualms in commenting on the idiocy of the charge of conspiracy. 😊

What separates conspiracy from ordinary criminal behavior? THOUGHTS AND SPEECH. That's why conspiracy is such an idiotic charge; it asks juries to punish someone for a basic natural right.

Any juror in his or her right mind should nullify a charge of conspiracy.

Providing customer service and advertising in a hacking forum is not conspiracy. It's free speech. There's no harm in it. There's no criminal act.


/rant

-  *Bobby Jr*
[July 19, 2018 at 8:04 am](#)


Again, when you tell a criminal how to use your tool to commit criminal acts you are aiding said criminal which is, last I heard, a criminal act.

Advertising? Not criminal. Tech support? Not criminal. Advertising to criminals and then helping them commit criminal acts? Criminal.

Speech is a protected right but it's also one with limits. Sad but true.

-  *Reader*
[July 20, 2018 at 1:55 am](#)

Reply read and appreciated.

8.  *Max*
[July 18, 2018 at 8:46 am](#)


I find it interesting how the man who made the RAT is getting in all of this trouble...

Cool, he made a RAT; I wish companies were being held more responsible for this sort of thing.

Who's the one at fault; the seller of the gun or the shooter?


-  *Jason*
[July 18, 2018 at 1:48 pm](#)

He's just the first domino. Expect more to come as they work their way through his client list, especially any that they have records of him helping with the illicit side of the software.


-  *somguy*
[July 18, 2018 at 1:52 pm](#)

Sellers of guns don't answer a phone call for tech support and tell them how to dispose of the body. (i.e. the tech support this guy gave for using it in hacking)

At least they'd better not be. Because if gun makers/sellers are answering tech questions on hiding bodies, pretty sure they could be liable for things.

-  *Reader*
[July 19, 2018 at 5:29 am](#)


Somguy,
I like the analogy you provided. Clever.

-  *Reader*
[July 19, 2018 at 6:18 am](#)

It's not the shopkeeper's fault if you combine cleaning products you bought to make a bomb or a cloud of chlorine gas.

Nor is it the fault of the manufacturer if you deliberately misuse their At-home Nuclear Reactor Kit for Exceptional Children.


End users are responsible for what they do with products that aren't defective or mislabeled.

-  *Doug*
[July 19, 2018 at 8:32 am](#)

Reader how stupid are you. It would be the shopkeepers fault, if said shopkeeper told his customers how to make such a bomb. That's the kind of 'support' this kid gave this customers.

"How do I hack into a computer?" – at that point the kid should of said figure it out on your own. Instead, he actively gave help on how to get around security and illegally get into systems.

Thus, he's at least partially responsible, and cannot claim to be ignorant of how his customers used his product, as he was the one helping them!

-  *Reader*
[July 20, 2018 at 2:02 am](#)

Doug,

You *should have* paid more attention to grammar in your comment.


◦  *Michael*
[July 19, 2018 at 8:35 pm](#)

If the seller provides aid and support to the shooter for the purpose of a crime, the seller is also criminally liable.

9.  *Chris M*
[July 19, 2018 at 12:54 pm](#)

So a white guy from Kentucky whose handle is KFC Watermelon is going to prison eh?

I'm sure he will have no problems explaining his reasoning behind the selection of that kind of name.

• 

• Mailing List

[Subscribe here](#)

•

**SIMPLE
APPLICATION
SECURITY
FOR FREE**

TRY AKAMAI NOW



WEB APPLICATION FIREWALL

FTEs needed to manage a WAF
3 or more according to 60% of respondents
(FTE = Full Time Equivalent Employee)

• Recent Posts

- [Leader of DDoS-for-Hire Gang Pleads Guilty to Bomb Threats](#)
- [Browser Extensions: Are They Worth the Risk?](#)
- [For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records](#)
- [Alleged 'Satori' IoT Botnet Operator Sought Media Spotlight, Got Indicted](#)
- [Instagram's New Security Tools are a Welcome Step, But Not Enough](#)

•

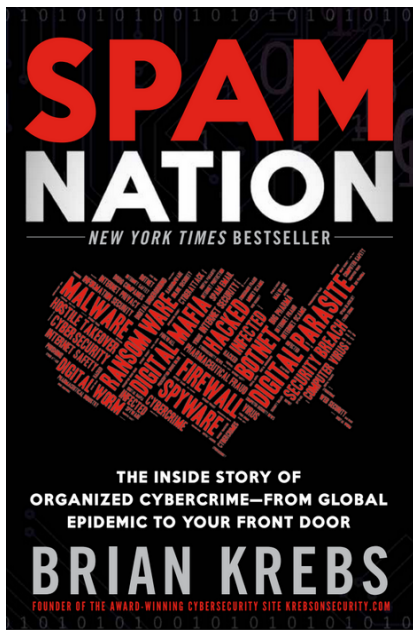
• All About Skimmers



Click image for my skimmer series.



- **Spam Nation**



A New York Times Bestseller!



- ## • The Value of a Hacked PC



Badguy uses for your PC

- ## • Tools for a Safer PC



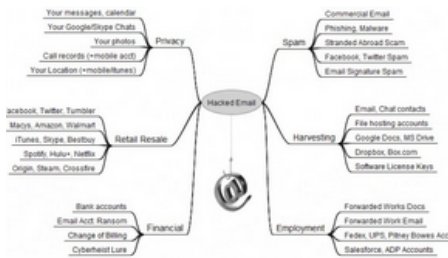
Tools for a Safer PC

• 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



ID Protection Services Examined

• Is Antivirus Dead?



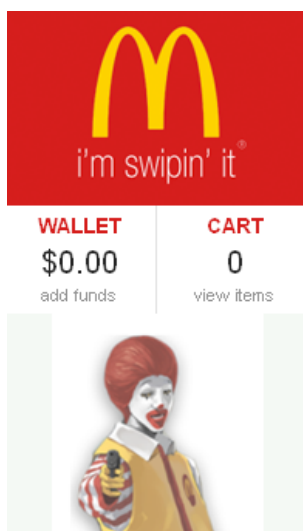
The reasons for its decline

• 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



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.

© 2018 Krebs on Security. Powered by [WordPress](#). [Privacy Policy](#).