

Advertisement

-  [Subscribe to RSS](#)
-  [Follow me on Twitter](#)
-  [Join me on Facebook](#)

**Say YES to  
Cloud Security**



Get your eBook –  
Definitive Guide to Cloud  
Access Security Brokers

## Krebs on Security

In-depth security news and investigation



- [About the Author](#)
- [Blog Advertising](#)

30  
Jan 16

### Sources: Security Firm Norse Corp. Imploding



Norse Corp., a Foster City, Calif. based cybersecurity firm that has attracted [much attention from the news media](#) and investors alike this past year, fired its chief executive officer this week amid a major shakeup that could spell the end of the company. The move comes just weeks after the company laid off almost 30 percent of its staff.

Sources close to the matter say Norse CEO Sam Glines was asked to step down by the company's [board of directors](#), with board member Howard Bain stepping in as interim CEO. Those sources say the company's investors have told employees that they can show up for work on Monday but that there is no guarantee they will get paid if they do.



A snapshot of Norse's semi-live attack map.

Glines agreed earlier this month to an interview with KrebsOnSecurity but later canceled that engagement without explanation. Bain could not be immediately reached for comment.

Two sources at Norse said the company's assets will be merged with Irvine, Ca. based networking firm [SolarFlare](#), which has some of the same investors and investment capital as Norse. Neither Norse nor SolarFlare would comment for this story.

The pink slips that Norse issued just after New Year's Day may have come as a shock to many employees, but perhaps the layoffs shouldn't have been much of a surprise: A careful review of previous ventures launched by the company's

founders reveals a pattern of failed businesses, reverse mergers, shell companies and product promises that missed the mark by miles.

## EYE CANDY

In the tech-heavy, geek-speak world of cybersecurity, infographics and other eye candy are king because they promise to make complicated and boring subjects accessible and sexy. And Norse's [much-vaunted interactive attack map](#) is indeed some serious eye candy: It purports to track the source and destination of countless Internet attacks in near real-time, and shows what appear to be multicolored fireballs continuously arcing across the globe.

Norse says the data that feeds its online attack map come from a network of more than eight million online "sensors" — [honeypot](#) systems that the company has strategically installed at Internet properties in 47 countries around the globe to attract and record malicious and suspicious Internet traffic.

According to the company's marketing literature, Norse's sensors are designed to mimic a broad range of computer systems. For example, they might pretend to be a Web server when an automated attack or bot scans the system looking for Web server vulnerabilities. In other cases, those sensors might watch for Internet attack traffic that would typically only be seen by very specific machines, such as devices that manage complex manufacturing systems, power plants or other industrial control systems.

Several departing and senior Norse employees said the company's attack data was certainly voluminous enough to build a business upon — if not especially sophisticated or uncommon. But most of those interviewed said Norse's top leadership didn't appear to be interested in or capable of building a strong product behind the data. More worryingly, those same people said there are serious questions about the validity of the data that informs the company's core product.

## UP IN SMOKE(S)

Norse Corp. and its fundamental technology arose from the ashes of several companies that appear to have been launched and then acquired by shell companies owned by Norse's top executives — principally the company's founder and chief technology officer [Tommy Stiansen](#). Stiansen did not respond to multiple requests for comment.

This acquisition process, known as a "reverse merger" or "reverse takeover," involves the acquisition of a public company by a private company so that the private company can bypass the lengthy and complex process of going public.

Reverse mergers are completely legal, but they can be abused to hide the investors in a company and to conceal certain liabilities of the acquired company, such as pending lawsuits or debt. In 2011, the U.S. Securities and Exchange Commission (SEC) issued a bulletin cautioning investors about plunking down investments in reverse mergers, warning that they may be prone to fraud and other abuses.

The founders of Norse Corp. got their start in 1998 with a company called Cyco.net (pronounced "psycho"). According to a press release issued at the time, "Cyco.net was a New Mexico based firm established to develop a network of cyber companies."

"This site is a lighthearted destination that will be like the 'People Magazine' of the Internet," said Richard Urrea, Cyco's CEO, in a [bizarre explanation](#) of the company's intentions. "This format has proven itself by providing Time Warner with over a billion dollars of ad revenue annually. That, combined with the CYCO.NET's e-commerce and various affiliations, such as Amazon.com, could amount to three times that figure. Not a portal like Yahoo, the CYCO.NET will serve as the launch pad to rocket the Internet surfer into the deepest reaches of cyberspace."

In 2003, Cyco.net [acquired Orion Security Services](#), a company founded by Stiansen, Norse's current CTO and founder and the one Norse executive who is actually [from Norway](#). Orion was billed as a firm that provides secure computer network management solutions, as well as video surveillance systems via satellite communications.

The Orion acquisition reportedly came with \$20 million in financing from a private equity firm called Cornell Capital Partners LP, which listed itself as a Cayman Islands exempt limited partnership whose business address was in Jersey City, NJ.

Cornell later changed its name to Yorkville Advisors, an entity that became the subject of an investigation by the U.S. Securities and Exchange Commission (SEC) and a subsequent lawsuit in which the company was accused of reporting "false and inflated values."

Despite claims that Cyco.net was poised to "rocket into the deepest riches of cyberspace," it somehow fell short of that destination and ended up selling cigarettes online instead. Perhaps inevitably, the company soon found itself the target of a lawsuit by several states led by the Washington state attorney general that accused the company of selling tobacco products to minors, failing to report cigarette sales and taxes, and for falsely advertising cigarettes as tax-free.

## COPYRIGHT COPS

In 2005, Cyco.net changed its name to Nexicon, but only after acquiring by stock swap another creation by Stiansen — Pluto Communications — a company formed in 2002 and whose stated mission was to provide "operational billing solutions for telecom networks." Again, Urrea would issue a press release charting a course for the company that would have almost no bearing on what it actually ended up doing.

"We are very excited that the transition from our old name and identity is now complete, and we can start to formally reposition our Company under the new brand name of Nexicon," Urrea [said](#). "After the divestiture of our former B2C company in 2003, we have

---

*Despite claims that Cyco.net was poised to "rocket into the deepest riches of cyberspace," it somehow fell short of that destination and ended up selling cigarettes online instead.*

laid the foundation for our new business model, offering all-in-one or issue-specific B2B management solutions for the billing, network control, and security industries.”

In June 2008, [Sam Glines](#) — who would one day become CEO of Norse Corp. — joined Nexicon and was later promoted to chief operating officer. By that time, Nexicon had [morphed itself into an online copyright cop](#), marketing a technology they claimed could help detect and stop illegal file-sharing. The company’s “GetAmnesty” technology sent users [a pop-up notice](#) explaining that it was expensive to sue the user and even more expensive for the user to get sued. Recipients of these notices were advised to just click the button displayed and pay for the song and all would be forgiven.

In November 2008, Nexicon was acquired by Priviam, another shell company operated by Stiansen and Nexicon’s principals. Nexicon went on to sign Youtube.com and several entertainment studios as customers. But soon enough, reports began rolling in of [rampant false-positives](#) — Internet users receiving threatening legal notices from Nexicon that they were illegally sharing files when they actually weren’t. Nexicon/Priviam’s business began drying up, and it’s stock price plummeted.

In September 2011, the Securities and Exchange Commission [revoked](#) the company’s ability to trade its penny stock (then NXCO on the pink sheets), noting that the company had failed to file any periodic reports with the SEC since its inception. In June 2012, the SEC also revoked Priviam’s ability to trade its stock, citing the same compliance failings that led to the de-listing of Nexicon.

By the time the SEC revoked Nexicon’s trading ability, the company’s founders were already working to reinvent themselves yet again. In August 2011, they raised \$50,000 in seed money from Capital Innovators to jump-start Norse Corp. A year later, Norse received \$3.5 million in debt refinancing, and in December 2013 got its first big infusion of cash — \$10 million from Oak Investment Partners. In September 2015, KPMG [invested \\$11.4 million](#) in the company.

Several former employees say Stiansen’s penchant for creating shell corporations served him well in building out Norse’s global sensor network. Some of the sensors are in countries where U.S. assets are heavily monitored, such as China. Those same insiders said Norse’s network of shell corporations also helped the company gain visibility into attack traffic in countries where it is forbidden for U.S. firms to do business, such as Iran and Syria.

### THE MAN BEHIND THE CURTAIN

By 2014, Norse was throwing lavish parties at top Internet security conferences and luring dozens of smart security experts away from other firms. Among them was [Mary Landesman](#), formerly a senior security researcher at Cisco Systems. Landesman said Norse had recently hired many of her friends in the cybersecurity business and had developed such a buzz in the industry that she recruited her son to come work alongside her at the company.

As a senior data scientist at Norse, Landesman’s job was to discover useful and interesting patterns in the real-time attack data that drove the company’s “cyber threat intelligence” offerings (including its [eye candy online attack map](#) referenced at the beginning of this story). By this time, former employees say Norse’s systems were collecting a whopping 140 terabytes of Internet attack and traffic data per day. To put that in perspective [a single terabyte](#) can hold approximately 1,000 copies of the Encyclopedia Britannica. The entire printed collection of the U.S. Library of Congress would take up about ten terabytes.

Landesman said she wasn’t actually given access to all that data until the fall of 2015 — *seven months after being hired as Norse’s chief data scientist* — and that when she got the chance to dig into it, she was disappointed: The information appeared to be little more than what one might glean from a Web server log — albeit millions of them around the world.

“The data isn’t great, and it’s pretty much the same thing as if you looked at Web server logs that had automated crawlers and scanning tools hitting it constantly,” Landesman said in an interview with KrebsOnSecurity. “But if you know how to look at it and bring in a bunch of third-party data and tools, the data is not without its merits, if not just based on the sheer size of it.”

Landesman and other current and former Norse employees said very few people at the company were permitted to see how Norse collected its sensor data, and that Norse founder Stiansen jealously guarded access to the back-end systems that gathered the information.

“With this latest round of layoffs, if Tommy got hit by a bus tomorrow I don’t think there would be a single person in the company left who understands how the whole thing works,” said one former employee at Norse who spoke on condition of anonymity.

### SHOW ME THE DATA

[Stuart McClure](#), president and founder of the cybersecurity firm [Cylance](#), said he found out just how reluctant Stiansen could be to share Norse data when he visited Stiansen and the company’s offices in Northern California in late 2014. McClure said he went there to discuss collaborating with Norse on two upcoming reports: One examining Iran’s cyber warfare capabilities, and another about exactly who was responsible for the massive [Nov. 2014 cyber attack on Sony Pictures Entertainment](#).

The FBI had already attributed the attack to North Korean hackers. But McClure was intrigued after Stiansen confidentially shared that Norse had reached a vastly different conclusion than the FBI: Norse had data suggesting the attack on Sony was the work of disgruntled former employees.

McClure said he recalls listening to Stiansen ramble on for hours about Norse’s suspicions and simultaneously dodging direct questions about how it had reached the conclusion that the Sony attack was an inside job.

“I just kept going back to them and said, ‘Tommy, show me the data.’ We wanted to work with them, but when they couldn’t or wouldn’t produce any data or facts to substantiate their work, we couldn’t proceed.”

After that experience, McClure said he decided not to work with Norse on either the Sony report or the Iran investigation. Cylance ended up releasing its own report on Iran's cyber capabilities; that analysis — dubbed "[Operation Cleaver](#)" (PDF) — was later tacitly acknowledged in a confidential report by the FBI.

Conversely, [Norse's take on Iran's cyber prowess](#) (PDF) was trounced by critics as a deeply biased, headline-grabbing report. It came near the height of international negotiations over lifting nuclear sanctions against Iran, and Norse had teamed up with the [American Enterprise Institute](#), a conservative think tank that has traditionally taken a hard line against threats or potential threats to the United States.

In its report, Norse said it saw a half-million attacks on industrial control systems by Iran in the previous 24 months — a 115 percent increase in attacks. But in a scathing analysis of Norse's findings, critical infrastructure security expert [Robert M. Lee](#) said Norse's claim of industrial control systems being attacked and implying it was definitively the Iranian government was disingenuous at best. Lee said he obtained an advanced copy of an earlier version of the report that was shared with unclassified government and private industry channels, and that the data in the report simply did not support its conclusions.

"The systems in question are fake systems...and the data obtained cannot be accurately used for attribution," Lee [wrote](#) of Norse's sensor network. "In essence, Norse identified scans from Iranian Internet locations against fake systems and announced them as attacks on industrial control systems by a foreign government. The Norse report's claims of attacks on industrial control systems is wrong. The data is misleading. The attention it gained is damaging. And even though a real threat is identified it is done in a way that only damages national cybersecurity."

#### FROM SMOKES TO SMOKE & MIRRORS?

KrebsOnSecurity interviewed almost a dozen current and former employees at Norse, as well as several outside investors who said they considered buying the firm. None but Landesman would speak on the record. Most said Norse's data — the core of its offering — was solid, if prematurely marketed as a way to help banks and others detect and deflect cyber attacks.

"I think they just went to market with this a couple of years too soon," said one former Norse employee who left on his own a few months prior to the January 2016 layoffs, in part because of concerns about the validity of the data that the company was using to justify some of its public threat reports. "It wasn't all there, and I worried that they were finding what they wanted to find in the data. If you think about the network they built, that's a lot of power."

On Jan. 4, 2016, Landesman learned she and roughly two dozen other colleagues at Norse were being let go. The data scientist said she vetted Norse's founders prior to joining the firm, but that it wasn't until she was fired at the beginning of 2016 that she started doing deeper research into the company's founders.

"I realized that, oh crap, I think this is a scam," Landesman said. "They're trying to draw this out and tap into whatever the buzzwords du jour there are, and have a product that's going to meet that and suck in new investors."

Calls to Norse investor KPMG International went unreturned. An outside PR firm for KPMG listed on the press release about the original \$11.4 million funding for Norse referred my inquiry to a woman running an outside PR firm for Norse, who declined to talk on the record because she said she wasn't sure whether her firm was still representing the tech company.

"These shell companies formed by [the company's founders] bilked investors," Landesman said. "Had anyone gone and investigated any of these partnerships they were espousing as being the next big thing, they would have realized this was all smoke and mirrors."



Tags: [American Enterprise Institute](#), [Cisco Systems](#), [Cornell Capital Partners](#), [Cyco](#), [Cyco.net](#), [Cylance](#), [fbi](#), [Howard Bain](#), [KPMG](#), [Mary Landesman](#), [Nexicon](#), [Norse Corp.](#), [Oak Investment Partners](#), [Operation Cleaver](#), [Orion Security Services](#), [Pluto Communications](#), [Priviam](#), [Richard Urrea](#), [Robert M. Lee](#), [Sam Glines](#), [SolarFlare](#), [Sony Pictures Entertainment](#), [Stuart McClure](#), [Tommy Stiansen](#), [Yorkville Advisors](#)

This entry was posted on Saturday, January 30th, 2016 at 8:51 am and is filed under [A Little Sunshine](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. You can skip to the end and leave a comment. Pinging is currently not allowed.

#### 44 comments

1.  [Patrick](#)  
[January 30, 2016 at 9:52 am](#)

The semi live eye candy map is not operational at the moment:  
<http://map.norsecorp.com/>

[Reply](#)

- o  [brian krebs](#)  
[January 30, 2016 at 9:58 am](#)

wow. that was fast. it was working just a few minutes before this article was published.

[Reply](#)

■ *The Norse PewPew Map*  
[January 30, 2016 at 10:08 am](#)

Brian,

Bad news – I just got my pink slip...are there any other infosec industry charlatans hiring?

Sincerely,

The Norse PewPew Map

[Reply](#)

■ *Rebecca Kline*  
[January 30, 2016 at 12:25 pm](#)

Malwarebytes. We are in Santa Clara.

[Reply](#)

■ *Edward W.*  
[January 30, 2016 at 2:53 pm](#)

The Norse PewPew Map was being sarcastic unless you truly believe Malwarebytes are charlatans.

[Reply](#)

■ *Steve Cain*  
[January 30, 2016 at 10:17 am](#)

Still working for me as of 10:17am EST.

[Reply](#)

■ *Michael kern*  
[January 30, 2016 at 12:24 pm](#)

Brian

Great reporting as always. I observed the eye candy site is down too.

[Reply](#)

■ *Tank*  
[January 30, 2016 at 3:34 pm](#)

Looks like the main map is down, but the IPViking map is still online:

<http://map.norsecorp.com/> – dead jim

<http://map.norsecorp.com/v1/> – still kicking it

[Reply](#)

2. *Eaglewerks*  
[January 30, 2016 at 10:10 am](#)

Good Reporting Brian!

It seems some in the firm were reminiscent of men like Charles Ponzi or Bernard “Bernie” Madoff.

[Reply](#)

3. *Joe*  
[January 30, 2016 at 10:15 am](#)

Excellent story, Brian. I love all the digging into old facts. Maybe a blog entry on Steven Avery? 😊

[Reply](#)

4. *Kurt Stammberger*  
[January 30, 2016 at 10:17 am](#)

Brian:

Thanks for your investigative work on this article. My hat’ s off to my colleague Mary Landesman who had the



courage to blow the whistle, and I stand by her analysis. My time at Norse was the most surreal and frustrating 18 months in my 25 year career in security and intelligence, but I'll say one thing: I've certainly learned some hard lessons from it.


Anyone considering taking a job these days should run paid background checks on senior leadership, shame on me for not doing so.

[Reply](#)

5.  *J Taylor*  
[January 30, 2016 at 10:40 am](#)

Thanks, Brian. Quite a tangled web!! Funny though, when I read the story lead on my email, it reminded me of the last episode of Season 1 of Mr. Robot!!

[Reply](#)

6.  *Slander*  
[January 30, 2016 at 10:40 am](#)

I think you should reword some of this article as you are lumping things/people together that seem unrelated. Kind of grasping for straws to put pieces together to make a good sounding story. Seems like a bunch of disgruntled ex-employees making statements. I would be careful of slander and defamation of character lawsuits.

[Reply](#)

- o  *brian krebs*  
[January 30, 2016 at 10:55 am](#)

I think you should reacquaint yourself with the definition of slander. In the United States, it's a legal term that means uttering falsities against another intended to defame them. What you're actually getting at is called "libel" — which is the form of slander that happens in writing.

In either case, for there to be slander or libel, there must be malice — i.e., the intention to harm the person or entity's reputation. Listing facts that are embarrassing or inconvenient for the subject, however, is hardly libelous.

[Reply](#)

-  *Alan Jenkins*  
[January 31, 2016 at 1:12 am](#)

Please continue to do so, Brian. Lifting the veil on such scams is vital to safeguard the reputation of our fledgling industry, particularly the startups where so much of our innovation comes from. As well as the likes of my employer, IBM's Security Division!

[Reply](#)

- o  *Failing Upwards*  
[January 30, 2016 at 10:59 am](#)


Can you buy character?

[Reply](#)

-  *ed*  
[January 30, 2016 at 2:00 pm](#)


No, but on TV you can sometimes buy vowels.

[Reply](#)

- o  *TY*  
[January 30, 2016 at 2:37 pm](#)

How about those dealings with Saudi Arabia? Remember the female analyst who had to be escorted by her brother into the space?

[Reply](#)

7.  *patti*  
[January 30, 2016 at 11:30 am](#)

I've been quite concerned about how long it would take organized cybercrime to enter the mainstream by appearing as a valid company — is this a potential MO for such an operation? They could do a lot of damage.

[Reply](#)*Chris*[January 30, 2016 at 12:35 pm](#)

Maybe they have :^)

[Reply](#)8. *Teksquisite*[January 30, 2016 at 12:06 pm](#)

Finally – I have some closure on this Norse deal – thank you Brian for great investigative reporting. I had the honor of working with Mary Landesman at Norse- she is highly respected in her field—always honest and forthcoming—also has a highly analytical mind, while at the same time would never adopt a “disgruntled employee” stance. Mary stands steadfast against injustices and does not fear speaking the truth.

Whistleblowers generally get a very bad deal when the truth is finally revealed. My hat’s off to Mary—since our demise on January 4, 2016 when 25+ of us were called into a “Q4 Quarterly Review” meeting, when three minutes into the meeting— we all learned that we had pink slips. Mary was the only one who spoke up and questioned company mismanagement.

Another top hat goes to Kurt Stammberger—for a succinct and honest analysis + his show of support for a great colleague.

[Reply](#)9. *Gary Hayslip*[January 30, 2016 at 12:10 pm](#)

As always, excellent article Brian. Enjoyed the backstory, I actually attended some of their parties at Blackhat.

[Reply](#)10. *BGC*[January 30, 2016 at 12:43 pm](#)

Webroot is making big noise about being the latest, greatest cloud-based security system utilizing . Lots of top end blather.

[Reply](#)*Mike Malloy*[January 30, 2016 at 10:58 pm](#)

Webroot threat data is genuine and utilized by more than 30 security industry vendors. It has been heavily tested for accuracy and efficacy by the most critical evaluators in the business: their competitors.

[Reply](#)11. *B Brodie*[January 30, 2016 at 12:55 pm](#)

KPMG funded them? I dealt with KPMG in the past and my personal experience was they have few business ethics.

Noted for churning customer billings and ‘thickening’ reports ( “The client is paying millions for this report: Make it thicker!” – verbatim quote from KPMG regional manager)

[Reply](#)*Spud Hosnick*[January 30, 2016 at 6:44 pm](#)

If there were a high school yearbook of accounting firms, KPMG would be most likely to be voted “most likely to aid and abet fraud” while billing handsomely. I once worked with a KPMG CPA on a small project. He was incredibly knowledgeable and quite competent, even when he was obviously drunk.

[Reply](#)*Common Sense*[January 30, 2016 at 8:40 pm](#)

Anybody writing for paid consumption is automatically under pressure to “tell a good story” . The take away is that with startups key personalities can make or break it. There a lot of bitter haters out there, if someone handed you a large check you would do the same!

[Reply](#)

P Finkelstein

[January 30, 2016 at 9:21 pm](#)

While I can't vouch for all of KPMG, many of us especially in the cyber security team actually want our clients to succeed and be secure and try to give the best advice we can often going above and beyond the fees we charge.

I can't speak for the the accounting part. But KPMG has a large advisory team too, it's very unfair for you to say that all of us have no ethics. As for the part about us aiding and abetting fraud, I don't know how. The amount of risk procedures that you have to go through to begin working with a client is immense. In fact so much so that often we can't move fast enough for certain sectors and industries.

I have no insight into the Norse thing. KPMG Capital invests in what it likes away from the main teams and country. This is as disappointing to the actual people in KPMG doing cyber as it probably is to you all reading it.

[Reply](#)

CiphersSon

12. [January 30, 2016 at 12:58 pm](#)

Roll your own attack map with blinky lights and zingy sounds... <https://github.com/hrbrmstr/pewpew>

[Reply](#)

Nikhil Seetharaman

13. [January 30, 2016 at 12:58 pm](#)

Excellent article and illuminates some of the charlatany happening in the security space.

[Reply](#)

Ken

14. [January 30, 2016 at 1:16 pm](#)

Norse had hired some pretty solid people from the industry. They will all find new jobs quickly, I'm sure. Dear Norse staff: if you need help getting to , give me a call.

[Reply](#)

TY

o [January 30, 2016 at 2:40 pm](#)

Here come the ambulance chasers...

[Reply](#)

Mark D

15. [January 30, 2016 at 2:40 pm](#)

I have the Norse's map on my desktop. I am willing to give it out for free if the map goes away with Norse.

Thank you, Brian, for the informative article. I actually knew nothing about the company. I certainly enjoyed the eye candy map.

[Reply](#)

S. Frisco

16. [January 30, 2016 at 2:54 pm](#)

Same story, again and again.

I look forward to your breakdown of the lack of research and lost money thrown at the similarly-shady TrustPipe executive team when they, shockingly, implode.

[Reply](#)

paul vixie

17. [January 30, 2016 at 2:55 pm](#)

brian, thanks for an excellent expose here. see also the related article published last year by frode hommedal and myself in CircleID:

[http://www.circleid.com/posts/20150420\\_internet\\_security\\_marketing\\_buyer\\_beware/](http://www.circleid.com/posts/20150420_internet_security_marketing_buyer_beware/)



[Reply](#)

18.  *OOooMoment*  
[January 30, 2016 at 6:23 pm](#)


Good article... Do one about how many cyber startups failed in 2015 and how many new startup ramped up in 2015. Maybe You could in list some now available graphical guru expertise to fashion a display of those comings and goings, the millions made and list and the jobs lost and obtained...

[Reply](#)

- o  *Shakespear*  
[January 30, 2016 at 8:43 pm](#)

Me thinks there will be a lot more startup failures in the next year...the tide is going out!

[Reply](#)

19.  *Ken*  
[January 30, 2016 at 7:30 pm](#)

Wasn' t Jason Clark on the advisory board? What does he say?

[Reply](#)

20.  *Kristen*  
[January 30, 2016 at 9:29 pm](#)

Pretty shady stuff, given their past track record ... hope the truth will come out soon.

[Reply](#)

21.  *Brice*  
[January 30, 2016 at 10:25 pm](#)

Nice article Brian, and great job hunting down the information. These seem like some shady characters, with some shoddy business practices. Further, a sales professional I know that pretty pictures can help make sale, but the stuffs gotta work in order to get the renewal the next year. I feel bad for the legit Norse employees that lost their jobs, but don' t fret. Solid security professionals are in high demand.

[Reply](#)

22.  *JC*  
[January 30, 2016 at 10:47 pm](#)

What really is disappointing is what this does for our industry. All the investors (including the angels that funding their early rounds, not cool to burn good people looking to help a team build a company.

[Reply](#)

23.  *Mark St. Amour*  
[January 30, 2016 at 11:09 pm](#)

Brian,

I recall at the time that Norse thought the Sony attack was disgruntled employees. It was attention grabbing certainly but I think this research is more so. As always, extensive and in-depth review and research in your article here. You certainly know how to get information.

I suspect the dust has settled for those who were at Norse, but if there are any looking; Bit9 + Carbon Black is hiring all over. The leadership, products and people here are pretty awesome. Certainly I welcome anyone to do their own research. I can be reached anytime for those interested, @mstamour

[Reply](#)

24.  *bruce*  
[January 31, 2016 at 1:27 am](#)

Wonderful research and comments. Couldn' t help but note less than exciting comments about Malwarebytes. Any reason to be concerned with them ?

[Reply](#)

25.  *G*  
[January 31, 2016 at 2:07 am](#)

(To the tune of the Marshmallow Fluff “FlufferNutter” ad jingle)

Oh you need fluff! fluff! fluff! to make a Netter-Fluffer  
Internet Fluff! with lots of graphic clutter!

First you spread! spread! spread! some jargon as a buffer  
Add Internet Fluff!, and that’ s a Netter-Fluffer!

So enjoy! -joy! joy! until the times get tougher  
Then sell your founders’ stock, and go out and start another!

[Reply](#)

## Leave a comment

Name (required)

Email (required)

Website

Comment

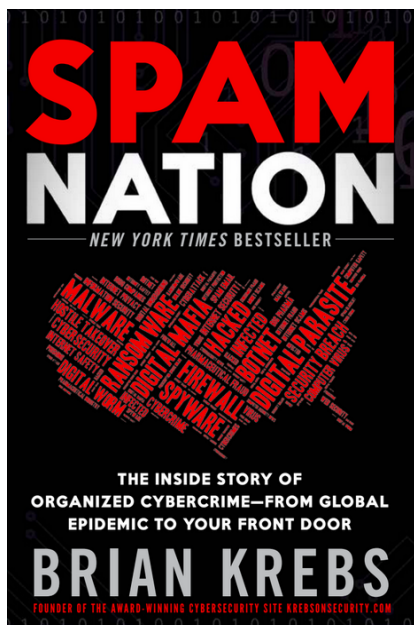
Reply notification?

## Advertisement



The advertisement features a blue and white geometric background. On the left, there is a logo for 'msgsafe.io' consisting of a blue envelope icon and the text 'msgsafe.io'. To the right of the logo is a circular icon containing a silhouette of a person's head. Below these elements, the text 'Use MsgSafe to minimize or eliminate ways governments intercept your communications.' is displayed in a sans-serif font. At the bottom of the ad, there is a prominent blue rectangular button with the white text 'LEARN MORE'.

- 
- My New Book!



A New York Times Bestseller!

Buy at Amazon

## Recent Posts

- [Sources: Security Firm Norse Corp. Imploding](#)
- [FTC: Tax Fraud Behind 47% Spike in ID Theft](#)
- [Wendy's Probes Reports of Credit Card Breach](#)
- [Oracle Pushes Java Fix: Patch It or Pitch It](#)
- [Skype Now Hides Your Internet Address](#)

## Subscribe by email

Please use your primary mailbox address, not a forwarded address.

Your email:

Subscribe

Unsubscribe

## All About Skimmers



Click image for my skimmer series.

## Thanks for your Support!

Donate



- o [A Little Sunshine](#)
- o [All About Skimmers](#)
- o [Breadcrumbs](#)
- o [Data Breaches](#)
- o [DDoS-for-Hire](#)
- o [How to Break Into Security](#)
- o [Latest Warnings](#)
- o [Ne'er-Do-Well News](#)
- o [Other](#)
- o [Pharma Wars](#)
- o [Security Tools](#)
- o [Spam Nation](#)
- o [Target: Small Businesses](#)
- o [Tax Refund Fraud](#)
- o [The Coming Storm](#)
- o [Time to Patch](#)
- o [Web Fraud 2.0](#)

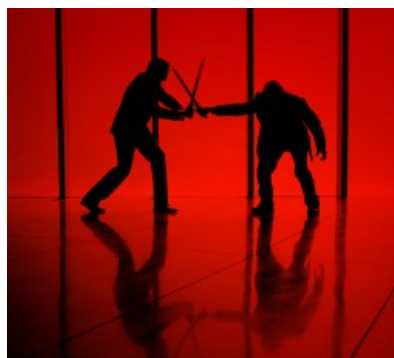
The mind map illustrates various security risks centered around 'SECURITY RISKS'. The branches include:

- Physical Security:** Data Center, Server, Storage, Backup, Disaster Recovery, etc.
- Network Security:** Firewall, Intrusion Detection, Denial of Service, etc.
- Application Security:** Software Bugs, Vulnerabilities, Malware, etc.
- Human Resources:** Social Engineering, Phishing, Insider Threats, etc.
- Legal and Compliance:** Data Privacy Laws, Industry Standards, etc.
- Environmental:** Natural Disasters, Power Outages, etc.

- Tools for a Safer PC

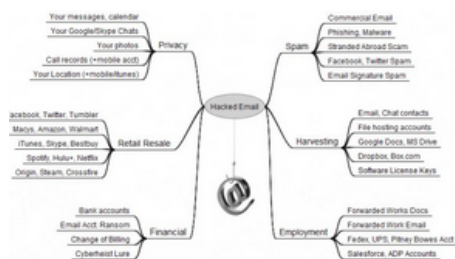


- The Pharma Wars



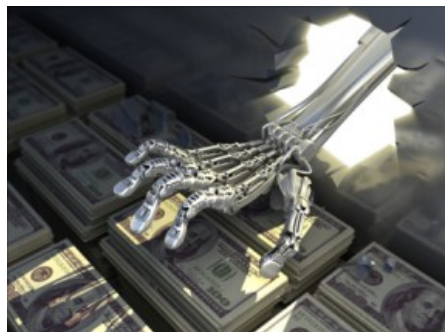
12/16

## • 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

- [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?](#) (377)
- [True Goodbye: 'Using TrueCrypt Is Not Secure'](#) (363)
- [Who Hacked Ashley Madison?](#) (360)
- [Following the Money, ePassporte Edition](#) (353)
- [U.S. Government Seizes LibertyReserve.com](#) (315)
- [Extortionists Target Ashley Madison Users](#) (310)

## • Category: Web Fraud 2.0





## Innovations from the Underground

Is credit monitoring  
really worth it?\*



ID Protection Services Examined

- Is Antivirus Dead?



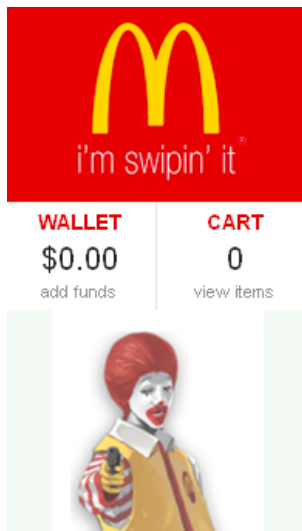
The reasons for its decline

- 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.

•

## • Blogroll

- [Arbor Networks Blog](#)
- [Bleeping Computer](#)
- [CERIAS / Spaf](#)
- [Contagio Malware Dump](#)
- [Cyber Crime & Doing Time](#)
- [Cyveillance Blog](#)
- [DHS Daily Report](#)
- [DSL Reports](#)
- [ESET Threat Blog](#)
- [F-Secure Blog](#)
- [FireEye Malware Intel Lab](#)
- [Fortinet Blog](#)
- [Fox-IT International](#)
- [Google Online Security Blog](#)
- [HP Security Research](#)
- [Imperva Blog](#)
- [Malcovery Security](#)
- [Malware Domain List Forum](#)
- [Malware Don't Need Coffee](#)
- [Microsoft Malware Protection Center](#)
- [Naked Security \(Sophos\)](#)
- [SANS Internet Storm Center](#)
- [Schneier on Security](#)
- [SecureWorks](#)
- [Securing the Human](#)
- [Securosis](#)
- [Spamtitan Blog](#)
- [Steve Gibson/Security Now](#)
- [StopBadware](#)
- [Symantec Response Blog](#)
- [TaoSecurity](#)
- [TrendMicro Blog](#)
- [Unmask Parasites Blog](#)
- [US CERT](#)
- [Websense](#)
- [Wilders Security Forums](#)
- [Wired.com's Threat Level](#)
- [Xylitol](#)