Krebs on Security

In-depth security news and investigation

28
Jul 14

Hackers Plundered Israeli Defense Firms that Built ‘Iron Dome’ Missile Defense System

Three Israeli defense contractors responsible for building the “Iron Dome” missile shield currently protecting Israel from a barrage of rocket attacks were compromised by hackers and robbed of huge quantities of sensitive documents pertaining to the shield technology, KrebsOnSecurity has learned.

The never-before publicized intrusions, which occurred between 2011 and 2012, illustrate the continued challenges that defense contractors and other companies face in deterring organized cyber adversaries and preventing the theft of proprietary information.

READ PREVIOUS POST:
Service Drains Competitors’ Online Ad Budget

The longer one lurks in the Internet underground, the more difficult it becomes to ignore the harsh reality that for...

A component of the ‘Iron Dome’ anti-missile system in operation, 2011.

According to Columbia, Md.-based threat intelligence firm **Cyber Engineering Services Inc.** (CyberESI), between Oct. 10, 2011 and August 13, 2012, attackers thought to be operating out of China hacked into the corporate networks of three top Israeli defense technology companies, including **Elisra Group**, **Israel Aerospace Industries,** and **Rafael Advanced Defense Systems**.

By tapping into the secret communications infrastructure set up by the hackers, CyberESI determined that the attackers exfiltrated large amounts of data from the three companies. Most of the information was intellectual property pertaining to Arrow III missiles, Unmanned Aerial Vehicles (UAVs), ballistic rockets, and other technical documents in the same fields of study.

Joseph Drissel, CyberESI's founder and chief executive, said the nature of the exfiltrated data and the industry that these companies are involved in suggests that the Chinese hackers were looking for information related to Israel's all-weather air defense system called Iron Dome.

The Israeli government has credited Iron Dome with intercepting approximately one-fifth of the more than 2,000 rockets that Palestinian militants have fired at Israel during the current conflict. The U.S. Congress is currently wrangling over legislation that would send more than $350 million to Israel to further development and deployment of the missile shield technology. If approved, that funding boost would make nearly $1 billion from the United States over five years for Iron Dome production, according to The Washington Post.

Neither Elisra nor Rafael responded to requests for comment about the apparent security breaches. A spokesperson for Israel Aerospace Industries brushed off CyberESI's finding, calling it "old news." When pressed to provide links to any media coverage of such a breach, IAI was unable to locate or point to specific stories. The company declined to say whether it had alerted any of its U.S. industry partners about the breach, and it refused to answer any direct questions regarding the incident.


Arrow 3 launch in January 2014.

"At the time, the issue was treated as required by the applicable rules and procedures," IAI Spokeswoman **Eliana Fishler** wrote in an email to KrebsOnSecurity. "The information was reported to the appropriate authorities. IAI undertook corrective actions in order to prevent such incidents in the future."

Drissel said many of the documents that were stolen from the defense contractors are designated with markings indicating that their access and sharing is restricted by International Traffic in Arms Regulations (ITAR) — **U.S. State Department** controls that regulate the defense industry. For example, Drissel said, among the data that hackers stole from IAI is a 900-page document that provides detailed schematics and specifications for the Arrow 3 missile.

"Most of the technology in the Arrow 3 wasn't designed by Israel, but by **Boeing** and other U.S. defense contractors," Drissel said. "We transferred this technology to them, and they coughed it all up. In the process, they essentially gave up a bunch of stuff that's probably being used in our systems as well."

WHAT WAS STOLEN, AND BY WHOM?

According to CyberESI, IAI was initially breached on April 16, 2012 by a series of specially crafted email phishing attacks. Drissel said the attacks bore all of the hallmarks of the "Comment Crew," a prolific and state-sponsored hacking group associated with the Chinese People's Liberation Army (PLA) and credited with stealing terabytes of data from defense contractors and U.S. corporations.

Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.

From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges.

Image: FBI

The Comment Crew is the same hacking outfit profiled in a February 2013 report by Alexandria, Va. based incident response firm **Mandiant**, which referred to the group simply by it's official designation — "P.L.A. Unit 61398." In May

2014, the **U.S. Justice Department** charged five prominent military members of the Comment Crew with a raft of criminal hacking and espionage offenses against U.S. firms.

Once inside the IAI's network, Comment Crew members spent the next four months in 2012 using their access to install various tools and trojan horse programs on systems throughout company's network and expanding their access to sensitive files, CyberESI said. The actors compromised privileged credentials, dumped password hashes, and gathered system, file, and network information for several systems. The actors also successfully used tools to dump Active Directory data from domain controllers on at least two different domains on the IAI's network.

All told, CyberESI was able to identify and acquire more than 700 files — totaling 762 MB total size — that were exfiltrated from IAI's network during the compromise. The security firm said most of the data acquired was intellectual property and likely represented only a small portion of the entire data loss by IAI.

"The intellectual property was in the form of Word documents, PowerPoint presentations, spread sheets, email messages, files in portable document format (PDF), scripts, and binary executable files," CyberESI wrote in a lengthy report produced about the breaches.

"Once the actors established a foothold in the victim's network, they are usually able to compromise local and domain privileged accounts, which then allow them to move laterally on the network and infect additional systems," the report continues. "The actors acquire the credentials of the local administrator accounts by using hash dumping tools. They can also use common local administrator account credentials to infect other systems with Trojans. They may also run hash dumping tools on Domain Controllers, which compromises most if not all of the password hashes being used in the network. The actors can also deploy keystroke loggers on user systems, which captured passwords to other non-Windows devices on the network."

The attackers followed a similar modus operandi in targeting Elisra, a breach which CyberESI says began in October 2011 and persisted intermittently until July 2012. The security firm said the attackers infiltrated and copied the emails for many of Elisra's top executives, including the CEO, the chief technology officer (CTO) and multiple vice presidents within the company.

The attackers infiltrated and copied the emails for many of Elisra's top executives, including the CEO, the chief technology officer (CTO) and multiple vice presidents within the company.

CyberESI notes it is likely that the attackers were going after persons of interest with access to sensitive information within Elisra, and/or were gathering would be targets for future spear-phishing campaigns.

Drissel said like many other such intellectual property breaches the company has detected over the years, neither the victim firms nor the U.S. government provided any response after CyberESI alerted them about the breaches at the time.

"The reason that nobody wants to talk about this is people don't want to re-victimze the victim," Drissel said. "But the real victims here are the people on the other end who are put in harm's way because of poor posture on security and the lack of urgency coming from a lot of folks on how to fix this problem. So many companies have become accustomed to low-budget IT costs. But the reality is that if you have certain sensitive information, you've got to spend a certain amount of money to secure it."

ANALYSIS

While some of the world's largest defense contractors have spent hundreds of millions of dollars and several years learning how to quickly detect and respond to such sophisticated cyber attacks, it's debatable whether this approach can or should scale for smaller firms.

Michael Assante, project lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security at the **SANS Institute**, said although there is a great deal of discussion in the security industry about increased information sharing as the answer to detecting these types of intrusions more quickly, this is only a small part of the overall solution.

Maybe a $100 million security program can do all these things well or make progress against these types of attacks, but that 80-person defense contractor? Not so much.

"We collectively talk about all of the things that we should be doing better — that we need to have better security policies, better information sharing, better detection, and we're laying down the tome and saying 'Do all of these things'," Assante said. "And maybe a $100 million security program can do all these things well or make progress against these types of attacks, but that 80-person defense contractor? Not so much."

Assante said most companies in the intelligence and defense industries *have* gotten better at sharing information and at the so-called "cyber counter-intelligence" aspect of these attacks: Namely, in identifying the threat actors, tactics and techniques of the various state-sponsored organizations responsible. But he noted that most organizations still struggle with the front end of problem: Identifying the original intrusion and preventing the initial compromise from blossoming into a much bigger problem.

"I don't think we've improved much in that regard, where the core challenges are customized malware, persistent activity, and a lot of noise," Assante said. "Better and broader notification [by companies like CyberESI] would be great, but the problem is that typically these notifications come after sensitive data has already been exfiltrated from the victim organization. Based on the nature of advanced persistent threats, you can't beat that time cycle. Well, you might be able to, but the amount of investment needed to

change that is tremendous."

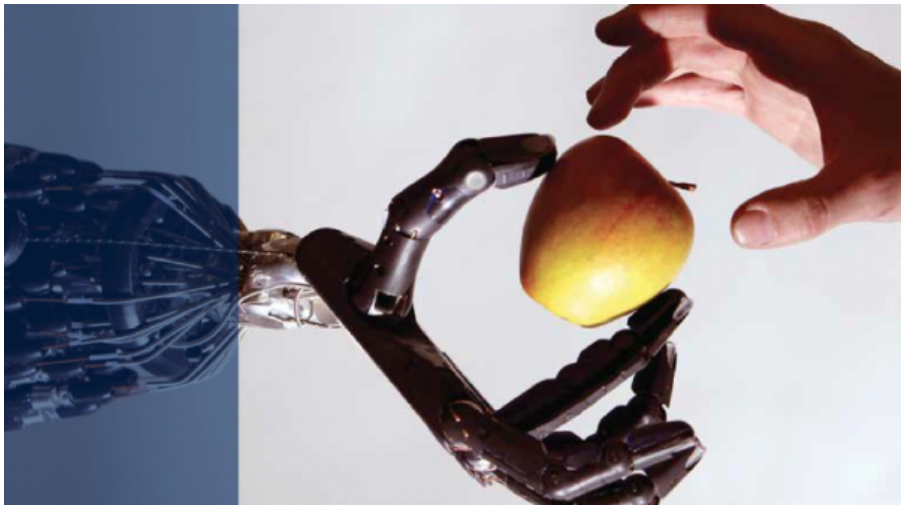
Ultimately, securing sensitive systems from advanced, nation-state level attacks may require a completely different approach. After all, as Einstein said, "We cannot solve our problems with the same thinking we used when we created them."

Indeed, that appears to be the major thrust of a report released this month by **Richard J. Danzig**, a board member of the **Center for New American Security**. In "Surviving on a Diet of Poison Fruit," (PDF) Danzig notes that defensive efforts in major mature systems have grown more sophisticated and effective.

"However, competition is continuous between attackers and defender," he wrote. "Moreover, as new information technologies develop we are not making concomitant investments in their protection. As a result, cyber insecurities are generally growing, and are likely to continue to grow, faster than security measures."

In his conclusion, Danzig offers a range of broad (and challenging) suggestions, including this gem, which emphasizes placing a premium on security over ease-of-use and convenience in mission-critical government systems:

"For critical U.S. government systems, presume cyber vulnerability and design organizations, operations and acquisitions to compensate for this vulnerability. Do this by a four-part strategy of abnegation, use of out-of-band architectures, diversification and graceful degradation. Pursue the first path by stripping the 'nice to have' away from the essential, limiting cyber capabilities in order to minimize cyber vulnerabilities. For the second, create non-cyber interventions in cyber systems. For the third, encourage different cyber dependencies in different systems so single vulnerabilities are less likely to result in widespread failure or compromise. And for the fourth, invest in discovery and recovery capabilities. To implement these approaches, train key personnel in both operations and security so as to facilitate self-conscious and well- informed tradeoffs between the security gains and the operational and economic costs from pursuing these strategies."



Source: Center for New American Security

Tags: Arrow III, Center for New American Security, Comment Crew, Cyber Engineering Services Inc., CyberESI, Eliana Fishler, Elisra Group, Iron Dome, Israel Aerospace Industries, Joseph Drissel, Rafael Advanced Defense Systems, Richard J. Danzig

137 comments

1. *joni*
   July 30, 2014 at 12:57 pm

   god jobs brother china, u r the best, PRAY FOR GAZA….

   Reply

2. *Mr_bloke*
   July 30, 2014 at 2:04 pm

   "Three Israeli defense contractors responsible for building the "Iron Dome" missile shield currently ~~protecting Israel from a barrage of rocket attacks~~"

   I think you meant "murdering innocent civilians".

   Reply

-  *JCitizen*
  July 30, 2014 at 2:37 pm

  Collateral damage has been greatly reducing as time goes on, and accuracy improves, but I'm with anyone who wants to put pressure on any military to eliminate killing "innocent civilians" – whatever that term means.

  Reply
- *Tommy*
  July 30, 2014 at 2:58 pm

  The Iron Dome is 100% defensive, built to protect the citizens of Israel from the terrorists next door who openly profess their goal of killing every Israeli and Jew. Maybe if Hamas had invested in similar defensive measures, or any defensive measures at all, they would not be suffering the casualties they are.

  Reply
  - *MrDin*
    August 1, 2014 at 12:41 pm

    US should STOP supplying Israel, weapon and ammo

    Reply
  - *John*
    August 3, 2014 at 12:31 pm

    I'm pretty sure that stopping the illegal occupation of Palestinian land by Israel would be the best solution.

    Reply
- *David Shields*
  July 30, 2014 at 3:14 pm

  Iron Dome is a purely defensive weapon, designed and manufactured by the U.S. The system is currently being used in Israel to protect Israeli Jews, Muslims, Christians, and Druze, from rockets being fired from Gaza. The success of Iron Dome augers well for the possibility of sales of the system to other nations.

  Reply
  - *paul*
    August 2, 2014 at 8:14 pm

    it's developed by Rafael Advanced Defense Systems from Israel.
    yeah read more. it's free on the internet.

    Reply
- *SeymourB*
  July 30, 2014 at 8:13 pm

  Someone needs to work with Hamas to patent these ethnic-seeking missiles its created, which solely injure Jewish citizens of Israel and nobody else.

  Or you can admit that Hamas just fires rockets indiscriminately and don't care who they kill, similar to their tunnel-based raids into surrounding territories.

  Reply
- *Common Sense*
  July 31, 2014 at 1:22 am

  Mr. Bloke,

  The innocent civilians are in Israel. Check your history and facts before you spew more propaganda. Clearly you represent the ignorant group who believe Israel wants to kill innocents. Sadly, the terrorists use schools and mosques as bases of operations to launch their attacks. They also do not allow innocents to leave and were captured by German media beating and killing their own kind who were innocently trying to leave the oppressive thumb of Hamas. Perhaps you should go there yourself and be educated first hand as clearly reading real reports is a challenge for people like you. When you get there, try escorting innocents out of Gaza in front of Hamas forces. I suspect you will only then truly understand your ignorance of this terrible situation. Israel is forced to fight to protect itself. They have exercised far more restraint than they should. Sadly, your ignorance is incapable of such restraint, so Shalom Mother Fucker to you and others who think like you.

Reply

- *MrDin*
  August 1, 2014 at 12:58 pm

  1. The educated adult do not call names on someone and using a profanity words.
  2. You hear the news, same others hear same news what you hear. Just depend on what side are you. NOTHING propaganda.
  3. Correct me if I'm wrong, Israel said "TO DEFENSE THEMSELVES". if a man punch you on your face, so you defense yourself, by shooting him, and his family, and destroy his home.
  Israel shoot more than 1300 civilians including hundreds of children in Gaza, and destroy most building, and electric power. Is that you call "defense themselves"?

  Reply

  - *paul*
    August 2, 2014 at 8:24 pm

    so you think Hamas using Tunnels to enter Israel and killing civilians is okay? Don't tell me you don't watch that kind of random YouTube videos.
    Nobody can justfy the innocents killed in any war. But only because they died more in number doesn't make thier side better. Also you can read everywhere on the internet on different websites etc or even talk to people if you don't believe one source that they betrayed Israel many times and it's not possible to make peace with people who just want to kill you and your family.

    I'm not Israeli and I'm not jewish, I'm not Muslim either but somebody starts a fight with our country then we'll be the one to end it.

    Free Palastine from HAMAS.

    Reply

    - *DigiDude*
      August 3, 2014 at 7:14 am

      Paul, If IDF Puts Down It's Weapons Tomorrow There'll Be Peace n If Palestine Puts Down It's Weapons Tomorrow There'll Be No Palestine!

      Reply

    - *Adam*
      August 10, 2014 at 8:49 pm

      English please?

      Reply

- *Bruce*
  July 31, 2014 at 1:41 pm

  Mr_bloke you are quite misled by radical progressive propaganda. Israel is totally moral and acting responsibly to protect its innocent citizens from the constant immoral attacks from those who have fled other Moslem countries and are not accepted back where they came from.
  Perhaps you should do yourself a favor and check out the real history instead of pumping out nonsense.
  http://www.science.co.il/History-Palestine.php

  Reply

  - *Margaret*
    August 3, 2014 at 4:44 pm

    The website you referenced is an Israeli science site. How about giving an unbiased website?

    Reply

    - *jc*
      August 12, 2014 at 10:59 am

      Simply because you dont go to a pally or arab site to get Israeli pov.
      Hamas deserves what they are getting.By extension the civilians who voted for voted to exterminate jews.

      Nuff said.

Nevermind that most of you all are off topic.

Reply

- *Tim*
  August 1, 2014 at 5:53 am

  How ignorant can someone get…it's an anti-missile system targeting rockets in the sky in Israel not towards Gaza.

  Some people develop rockets to kill people and some people develop rockets to protect people but I guess logic is not the best expertise of the Ignorant

  Reply

3. *Ziad K Abdelnour*
   July 31, 2014 at 3:16 am

   We believe the industry's fate largely depends on Pentagon's decisions on how it will modernize U.S. forces to confront future threats. In its Cold War heyday, the Pentagon was the leading developer of cutting-edge technology and still commands the world's most advanced military force. But at the same time, it has created self-defeating mechanisms that quash innovation and fail to capitalize on available opportunities. The United States is still way ahead of competitors in areas such as fighter aircraft and submarines. But there are segments of the weapons market such as ballistic missiles and cruise missiles where other people are doing quite well compared to us.

   Reply

4. *Mario*
   July 31, 2014 at 11:31 am

   Common Sense, the innocent civilians are in Israel. True. Innocent civilians live in Gaza, too. Somehow 1200 of them who got killed in the last ten days used to live in former mentioned area, not Israel. And how many wounded on top? What kind of state is defending itself by obliterating and murdering civilian population? If "Iron Dome" is so effective, Israel doesn't have to fear of few home made projectiles. Or, perhaps Chinese hackers infiltrated the rockets systems and are shooting Gaza on their own accord?

   Reply

   - *MrDin*
     August 1, 2014 at 1:18 pm

     Mario, don't you know that " the innocent civilians" are ONLY live in Israel? LOL. The civilian and children in Gaza were NOT the innocent civilian and not innocent children. That's why Israel kill all not innocent children and not innocent civilians in Gaza.

     Israel has New High Tech of War, they sent text message to ALL not innocent civilians/children in Gaza, to hide in school, so Israel can shoot missile on civilian and children and kill all of them at once.

     Reply

   - *DigiDude*
     August 2, 2014 at 3:22 pm

     Mario I Totally Agree With You… Some Jews Infact Zionists Are Hit With Myopia So It's Actually Hard For Them To Swallow The Truth Or Even Hear It… I Don't Remember If I Heard Of Any Of Hamas's Rocket Killing a Israeli Citizen But At The Same Time I've Never Heard Of An Israeli Rocket/Shell Fire Missing Any Of It's Innocent Civilian Targets… I've Friends In Gaza n When Is Ask Them Nicely "Hey, What's Up? :)"
     They Reply "Bombs Are Up! :'("

     Look Brothers n Sisters(Doesn't Matter If You Are Black Or Blue Or Even ET Or a Zion)… You Just Need To Be a Human To Care For Them… They(Innocent Palestinians) At Their Most Desire Your Care Before They Are Bombed n Left Dead Right At Their Bed In Their Own Home Where Their Parents Tell Them It's Safe Here .. Goto Sleep Now.. I"ll Kick Off Every Incoming Bomb, By The IDF!

     Genocide Has Hit It's Climax In #Gaza n #Rafah .. We Need To Make a New Word For It … Cause It Is Simply Not Genocide Its Not a War Crime .. We Need a Word Like "Holocaust" Here .. But Guess What?! Holocaust Lasted No More Than 4 Years But This Ruthless n Merciless Killing Of Millions Of Innocent Palestinians Has Been Continuing Since 1948(That Makes About 66 Years Of Killings In Total Which Is More Than 16 Times Of The Deadly Holocaust) Here's a Concise If Not Brief History Of The Past Muslim Holocaust
     http://www.rense.com/general21/pastzionist.htm
     n It Is a Collected By an American n I Don't Think He's Even Muslim But He's Indeed Proof He Is a Good, Caring n Just Human..

     I Cannot Say Anymore… Or I'll Crook My Laptop's KeyBoard With My Tears…

Reply

- *Mario(another one)*
  August 3, 2014 at 1:00 pm

  sorry dude but your comment is really unreadable, with so many capital letters.
  If you are not aware, please have a look to https://www.ietf.org/rfc/rfc1855.txt (Netiquette)

  Reply

- *Margaret*
  August 3, 2014 at 5:05 pm

  Thank you for the website. I looked up the 1948 Palestine exodus and the massacre at Dier Yassin in a search engine. What terrible tragedies. Many people want to make one side the 'bad guy', but they don't want to quit pointing fingers and dropping bombs long enough to work for Peace. Peace is possible – but it is so much easier to take sides and hate each other!!!

  Reply

5. *Sean*
   July 31, 2014 at 5:58 pm

   If only those pesky hackers had convinced a rich sugar daddy to build the children of Gazza a rocket defence system. I hear the NSA are looking for new PR people, is this part of the interview process Brian?

   Reply

6. *kimsunam*
   August 1, 2014 at 4:26 am

   It seems that Countries always like to spy on each other, looks like they need more security. Actually, there is no real security for today's people all use the internet to do whatever they want. But some software can be legal or also illegal to use, like Micro Keylogger, when you use it on your own PC, legal.

   Reply

7. *nebular*
   August 1, 2014 at 8:55 am

   "When Israel, in the occupied territories now, claim that they have to defend themselves, they are defending themselves in the sense that any military occupier has to defend itself against the population that they're crushing." – Noam Chomsky

   Reply

   - *Varera*
     August 1, 2014 at 9:24 am

     Right. Take an outdated citation of a self-hating Jew leftist activist like it means anything. For your information, Israel has withdrawn its troops and settlers from Gaza in 2005.

     Is it time for you to get back in touch with the reality?

     Reply

     - *Mario*
       August 1, 2014 at 9:40 am

       Even older quote:

       "Palestine belongs to the Arabs in the same sense that England belongs to the English or France to the French. It is wrong and inhuman to impose the Jews on the Arabs… Surely it would be a crime against humanity to reduce the proud Arabs so that Palestine can be restored to the Jews partly or wholly as their national home"
       — Mahatma Gandhi

       Reply

       - *Mr Din*
         August 1, 2014 at 1:24 pm

         and America belong to Africa – B Hussein Obama LOL

Reply

8. *Mario*
August 3, 2014 at 12:50 pm

———————
Cit. John (August 3, 2014 at 12:31 pm)

I'm pretty sure that stopping the illegal occupation of Palestinian land by Israel would be the best solution.
———————

Sorry John, I have to do it, your comment is brilliant!

Reply

- *Mario*
August 3, 2014 at 12:52 pm

oh my god, it was supposed to be a replay to "Common Sense" without sense and common.
sorry for that.

Reply

- *Mario*
August 3, 2014 at 12:53 pm

oh, sorry. This was supposed to be a replay to "Common Sense" without commmon sense. Sorry for that

Reply

9. *Bawlfungus*
August 6, 2014 at 11:21 am

"Wang Dong" Tell me i'm not the only one that's entertained by that guy's name.

Reply

← Older Comments

Leave a comment

Name (required) NAME_FULL

Email (required) EMAIL_ADDRESS

Website UNKNOWN_TYPE

Comment UNKNOWN_TYPE

Submit Comment

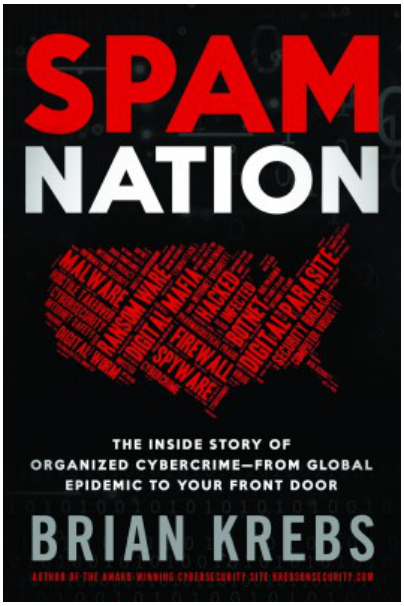
Notify me of followup comments via e-mail

-

Recent Posts

- Tenn. Firm Sues Bank Over $327K Cyberheist
- Adobe, Microsoft Push Critical Security Fixes
- Personalize Your Copy of Spam Nation
- New Site Recovers Files Locked by Cryptolocker Ransomware
- Q&A on the Reported Theft of 1.2B Email Accounts

Pre-order "Spam Nation"



Due out Nov. 18, 2014

- Buy at Amazon
- BARNES & NOBLE BOOKSELLERS BUY NOW
-

Subscribe by email

Your email:

Enter email address...

Subscribe Unsubscribe

Made possible by Prolocation

Prolocation: For all your hosting needs. Fast. Reliable. Powerful.

Support KrebsOnSecurity!

Donate

Support KrebsOnSecurity!

Donate Bitcoins

SANS Network Security

Use “SANS_Krebs150” for $150 off any class

Categories

- A Little Sunshine
- All About Skimmers
- Breadcrumbs
- Data Breaches
- How to Break Into Security
- Latest Warnings

- Ne'er-Do-Well News
- Other
- Pharma Wars
- Security Tools
- Target: Small Businesses
- The Coming Storm
- Time to Patch
- Web Fraud 2.0

All About ATM Skimmers

Click image for my skimmer series.

Archives

- August 2014
- July 2014
- June 2014
- May 2014
- April 2014
- March 2014
- February 2014
- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013
- July 2013
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011

- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009

The Value of a Hacked PC

Badguy uses for your PC

Tags

0day adobe adobe flash player adobe reader apple atm skimmer chrome chronopay cyberheist f-secure Facebook fbi firefox Glavmed gmail google Google Chrome Igor Gusev internet explorer java Liberty Reserve Mac mastercard mcafee microsoft money mules opera Oracle pavel vrublevsky Pharma Wars RSA Rx-Promotion safari sans internet storm center Spamit spyeye Symantec twitter U.S. Secret Service Visa webmoney windows zero day zeus ZeuS Trojan

Tools for a Safer PC

Tools for a Safer PC

Blogroll

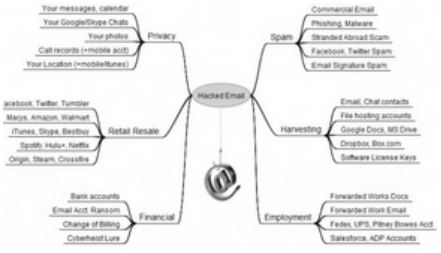
- Arbor Networks Blog
- Bleeping Computer
- CERIAS / Spaf
- Contagio Malware Dump
- Cyber Crime & Doing Time
- Cyveillance Blog
- DHS Daily Report
- DSL Reports
- ESET Threat Blog
- F-Secure Blog
- FireEye Malware Intel Lab

- Fortinet Blog
- Fox-IT International
- Google Online Security Blog
- 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

The Pharma Wars

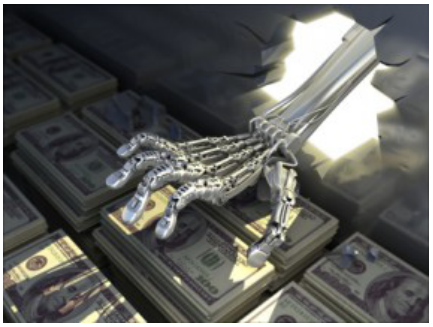
Spammers Duke it Out

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

  - Sources: Target Investigating Data Breach (620)
  - Cards Stolen in Target Breach Flood Underground Markets (445)
  - Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
  - True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
  - Following the Money, ePassporte Edition (353)
  - U.S. Government Seizes LibertyReserve.com (315)
  - Sony Pictures Plans Movie About Yours Truly (273)
  - Who's Selling Credit Cards from Target? (269)
  - Target Hackers Broke in Via HVAC Company (268)
  - Email Attack on Vendor Set Up Breach at Target (265)

- ## Category: Web Fraud 2.0

Innovations from the Underground

- 

ID Protection Services Examined

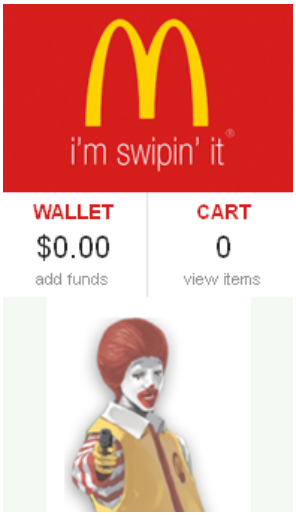
- ## Is Antivirus Dead?

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

Sign up, or Be Signed Up!
