

DL
SC

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 NICHOLAS PAUL KNIGHT,)
 a/k/a "Inertia",)
 a/k/a "Logic",)
 a/k/a "nickmc01",)
 a/k/a "Solo",)
 a/k/a "INER7IA",)
 a/k/a "| Logic |",)
 DANIEL TRENTON KRUEGER,)
 a/k/a "Thor",)
 a/k/a "Orunu",)
 a/k/a "Gambit",)
 a/k/a "Chronus",)
 a/k/a "7hor",)
 a/k/a "G4mbi7",)
)
 Defendants.)

Case No. **14 CR 074 JHP**
INFORMATION
[18 U.S.C. § 371: Conspiracy]

FILED
MAY 5 2014
Phil Lombardi, Clerk
U.S. DISTRICT COURT

THE UNITED STATES ATTORNEY CHARGES:

At all times relevant:

INTRODUCTORY ALLEGATIONS

1. All dates are on or about the dates listed.
2. "Protected computer" means a computer within the definition of Title 18, United States Code, Section 1030(e)(2).
3. Database "schema" is the technical structure of a database. This schema is kept private, in part, because disclosure of it makes databases more vulnerable to being hacked.

4. "Hack" means to access a protected computer without authorization.
5. Passwords can be stored in "cleartext" and "encrypted" forms. A "cleartext" password is stored in the same format in which a user enters it. An encrypted password is stored following the application of a security-related algorithm and, as used below, includes both "hashed" passwords, which are one-way encrypted passwords, and two-way encrypted passwords.
6. Postings to Twitter ("Tweets"), identified below, were made to the Twitter account of Team Digi7al.
7. The United States Navy ("Navy"), an agency of the United States government, was the naval warfare service branch of the United States Armed Forces.
8. The Naval Criminal Investigative Service ("NCIS"), an agency of the United States government, was the primary investigative law enforcement agency of the Navy. In June 2012, NCIS began investigating a breach of the United States Navy's Smart Web Move website and database ("Navy-SWM").
9. Team Digi7al (pronounced digital), a renamed continuation of Team Hav0k (pronounced havoc), was a criminal association organized to hack protected computers, steal sensitive and private information, make unauthorized public disclosures of that stolen sensitive and private information, and commit various other crimes related to its hacking activities, including to obstruct justice by destroying records. Members of Team Digi7al Tweeted boasts of their hacks and publicly disclosed stolen sensitive and private information obtained from their hacks of protected computers.

10. **NICHOLAS PAUL KNIGHT** (“**KNIGHT**”), the self-professed leader of Team Digi7al, was the primary publicist and Twitter poster. **KNIGHT**, a hacker since age 16, completed some of the technical work behind the hacks and used various aliases online, including the following: “Inertia”, “Logic”, “nickmc01”, “Solo”, “INER7IA” (pronounced inertia), and “| Logic |”. **KNIGHT** resided in the Eastern District of Virginia, first in Virginia Beach and later in Chantilly, and was an active duty enlisted member of the Navy stationed in Norfolk, Virginia, and assigned to duties aboard nuclear aircraft carrier USS Harry S. Truman as a systems administrator in the nuclear reactor department. While aboard the USS Harry S. Truman, **KNIGHT** conducted unlawful Team Digi7al activities on the Navy’s computer network and was discharged by the Navy after he was caught trying to hack into a Navy database while at sea.
11. **DANIEL TRENTON KRUEGER** (“**KRUEGER**”), who performed much of the technical hacking work for Team Digi7al, posted Tweets of sensitive and private information obtained during his hacks and sent other such information to **KNIGHT** for Tweets on behalf of Team Digi7al. **KRUEGER** resided in Salem, Illinois in the Southern District of Illinois and used various aliases online, including the following: “Thor”, “Orunu”, “Gambit”, “Chronus”, “7hor” (pronounced Thor), and “G4mbi7” (pronounced gambit). **KRUEGER** was a student at an Illinois community college where he studied network administration.

12. Team Digi7al members known to the United States Attorney and not charged in this Information include the following individuals:

- a. Team Digi7al Member A (“TD Member A”), a minor and a resident of Montgomery, Alabama in the Middle District of Alabama, performed much of the technical hacking work for Team Digi7al.
- b. Team Digi7al Member B (“TD Member B”), a minor when he joined Team Digi7al and the conspiracy and a resident of Pitkin, Louisiana in the Western District of Louisiana, performed technical hacking work for Team Digi7al.
- c. Team Digi7al Member C (“TD Member C”), a minor when he joined Team Digi7al and the conspiracy and a resident of Decatur and Covington, Georgia, both in the Northern District of Georgia, performed technical hacking work for Team Digi7al and disclosed sensitive and private information stolen during hacks.

13. In furtherance of the conspiracy, Team Digi7al’s members hacked the following websites:

- a. Navy-SWM:
 - i. The United States Navy managed the logistics of duty station transfers for active duty members of the United States Navy, Army, Air Force, Marines, and Coast Guard, and their families (“Service Members”). To do so effectively, the Navy maintained the Navy-SWM website and database.

- ii. To initiate a move, Service Members input a variety of personal private information on Navy-SWM, which was stored on at least one protected computer located in Tulsa County, Oklahoma in the Northern District of Oklahoma, including Social Security numbers, full names, dates of birth, encrypted passwords, and password reminders (which regularly contained information like mothers' maiden names, children's names, and additional personal account passwords) ("Personal Information").
 - iii. Navy-SWM stored this Personal Information for approximately 220,000 Service Members, with information dating back to 2001, on at least one protected computer located in Tulsa County, Oklahoma in the Northern District of Oklahoma.
- b. United States National Geospatial-Intelligence Agency ("NGA") was a United States governmental agency with the mission of providing combat support to the United States Department of Defense by collecting, analyzing, and distributing geospatial intelligence in support of national security.
- c. United States Department of Homeland Security Transportation Worker Identification ("DHS-TWIC"): under the Maritime Transportation Security Act, transportation workers who require unescorted access to secure areas of maritime facilities and vessels are issued DHS-TWIC credentials, which contain biometric and other sensitive personal information.

- d. Los Alamos National Laboratory (“LANL”) was a United States government-run laboratory with the mission of developing and applying science and technology to ensure the safety, security, and reliability of the United States nuclear deterrent, to reduce global threats, and to solve other emerging national security and energy challenges.
- e. Toronto Police Service, Canada (“TPSC”) was the investigative law enforcement agency in Toronto, Canada.
- f. AT&T Uverse: AT&T hosted a website that contained information related to its Uverse telecommunications customers.
- g. Rashod Holmes was a musician who promoted and sold items through a Zipbox Media account, hosted at www.rashodholmes.com.

COUNT ONE
[18 U.S.C. § 371]

- 14. Paragraphs 1-13 of the Introductory Allegations are realleged and incorporated here.
- 15. From not later than in or about April 2012 to in or about June 2013, in the Northern District of Oklahoma and elsewhere, the Defendants, **KNIGHT** and **KRUEGER**, did knowingly, intentionally, and willfully combine, conspire, confederate, and agree with each other and with others known and unknown to the United States Attorney, including TD Member A, TD Member B, and TD Member C, to defraud the United States by impeding, impairing, and defeating the lawful

functions of the United States government and to commit offenses against the United States, as follows:

- a. To access protected computers without authorization and thereby obtain information from protected computers in furtherance of criminal and tortious acts in violation of the laws of Oklahoma, specifically, violations of Title 21, Oklahoma Statutes, Section 1953(A)(1) (willfully and without authorization gain access to and disclose the contents of a computer), and invasion of privacy, in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii);
- b. To access protected computers without authorization and, as a result of such conduct, recklessly cause damage to persons during a one-year period resulting from the Defendants' related course of conduct that affected protected computers in the aggregate of at least \$5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(B) and 1030(a)(5)(c)(4)(A)(i)(I);
- c. To commit identity theft in and affecting interstate and foreign commerce in connection with a felony under the laws of Oklahoma, specifically, a violation of Title 21, Oklahoma Statutes, Section 1953(A)(1) (willfully and without authorization gain access to and disclose the contents of a computer), in violation of Title 18, United States Code, Sections 1028(a)(7) and 1028(c)(3)(A); and

- d. To alter, destroy, mutilate, conceal, and cover up records and documents with the intent to impede, obstruct, and influence an investigation and proper administration of a matter within the jurisdiction of a department and agency of the United States, in violation of Title 18, United States Code, Section 1519.

MEANS AND METHODS

16. The members of Team Digi7al organized to steal and disclose sensitive and personal private information, such as database schema and peoples' website usernames, full names, addresses, telephone numbers and mobile carriers, email addresses, encrypted and cleartext passwords, password questions and reminders, bank account information containing access devices, and private email content.
17. The members of Team Digi7al conspired to defraud the United States by impeding, impairing, obstructing and defeating the lawful functions of the Navy to effectively and efficiently manage the logistics of Service Members' transfers to new duty stations and to move Service Members' household goods.
18. To attempt and to accomplish the goals of their conspiracy, Team Digi7al members frequently used the following process:
 - a. First, a member scanned Internet websites for security vulnerabilities on protected computers, taking a particular interest in hacking government websites, including military, educational, intelligence, homeland security, and critical infrastructure websites.

- b. Second, a member exploited the vulnerability, frequently using a structured query language injection (“SQLi”) method. This exploitation involved gaining access to a website database’s schema and, when possible, the sensitive private data contained in that database.
- c. Third, a member then saved the sensitive private information to his or her own personal computer’s hard drives or other physical storage medium.
- d. Fourth, the member uploaded the sensitive private information to a variety of cloud storage websites, making the sensitive private information accessible to the public.
- e. Fifth, a member used Team Digi7al’s Twitter account to announce the successful hack, embarrass the victim of the hack, and post a link to the web storage site, making the sensitive private information easy for the public to access and download, thereby victimizing the individuals whose sensitive private information was stolen.
- f. When rival hacking groups like Digital Corruption claimed credit for one of Team Digi7al’s hacks by reposting the sensitive private information, it was common for Team Digi7al’s members to post more information about their successful hack as evidence to the hacking world of their unlawful exploits.
- g. By publicizing the private information and technical schema of the databases of victim organizations, Team Digi7al’s members damaged the websites they attacked by making the databases more vulnerable to subsequent attacks and causing the websites to shut down in order to

identify and mitigate the damage and to strengthen their security to avoid future attacks. Team Digi7al's members knew that this damage and loss would occur and were at least reckless regarding the result of their hacks.

19. Team Digi7al's members had varied reasons for conducting unlawful hacking and disclosure activities, but all agreed to conduct those activities to violate the laws of the United States.

- a. **KNIGHT** called himself a "nuclear black hat" who fought for the people of the United States, not the government. **KNIGHT** used this description to explain why Team Digi7al targeted government-related websites. A black hat hacker is someone who actively performs hacking activities with the intent to damage computer systems and compromise sensitive data.
- b. **KRUEGER** explained that he hacked Navy-SWM "out of boredom."
- c. According to another Team Digi7al member, the group hacked into protected computers and publicly disclosed the sensitive private information they obtained because they were "somewhat politically inclined to release the things [they had]" but also because it was "fun, and we can . . . [w]hich if you get right down to it, that's what everyone does."

OVERT ACTS

20. To effect the objects of the conspiracy and to accomplish its purposes and objectives, the conspirators committed the following overt acts, among others, in the Northern District of Oklahoma and elsewhere:

LANL Hack

21. On April 19, 2012, an unknown member of Team Digi7al hacked into at least one LANL protected computer but was caught by an LANL systems administrator during the hack and managed to steal only a small amount of information from LANL.

AT&T Uverse Hack

22. On May 25, 2012, **KRUEGER** hacked at least one AT&T Uverse protected computer and downloaded the following sensitive and private information: database schema; over 7,500 individuals' mobile phone numbers; users' records containing email addresses, full names, mobile phone numbers with carrier names and phone models, and full physical addresses; users' records containing email addresses and mobile numbers with carrier names; users' records containing email addresses, full names, city information, and mobile phone numbers; and users' usernames and cleartext passwords.

TPSC Hack

23. Between May 23, 2012, and June 1, 2012, TD Member B hacked at least one TPSC protected computer and downloaded a large file containing over 100 tables with the following sensitive and private information: more than 3,500 email

addresses; over 2,500 usernames and cleartext passwords, including administrator usernames and cleartext passwords; names, addresses, phone numbers, and email addresses of citizens who gave police tips through TPSC's online tip system; names, addresses, phone numbers, and email addresses of greater than 500 police informants; suspect descriptions; and press releases, police reports, and Tweets.

24. On June 1, 2012, a Team Digi7al member posted a Tweet containing this sensitive and private information.

DHS-TWIC Hack

25. On June 3, 2012, **KRUEGER** and **KNIGHT** hacked at least one DHS-TWIC protected computer and downloaded its database schema.
26. Between June 3, 2012, and June 5, 2012, **KNIGHT** used Team Digi7al's Twitter account to make unlawful public disclosure of database schema, damaging DHS-TWIC's website by making it more vulnerable to future attacks.

Navy-SWM Hack

27. On June 7, 2012, on behalf of Team Digi7al and without authorization, **KRUEGER** intentionally accessed at least one protected computer by using SQLi to hack into Navy-SWM. After hacking into Navy-SWM, he downloaded the contents of the Navy-SWM database, obtaining thousands of Service Members' Personal Records, the precise number of which is unknown to the United States Attorney. **KRUEGER** obtained this information for the purpose of later making unlawful public disclosure of it. As a result of Team Digi7al's actions, Navy-SWM was shut down and never resumed operation. Although some Service

Members could access Move.mil for the same purpose they had used Navy-SWM, as a result of Navy-SWM's premature shutdown, over 700 deployed overseas Service Members could not access logistical support for transfers for more than 10 weeks. Team Digi7al's Navy-SWM hack foreseeably caused loss to the Navy of approximately \$514,000, which included the cost to respond to the attack, assess the damage, pay contractors and employees for their time devoted to the damage assessment and mitigation response, provide Service Members with identity theft and credit monitoring services, and fund a call center devoted to helping Service Members potentially impacted by the hack.

28. Between June 7, 2012, and June 17, 2012, **KRUEGER** transmitted the Service Members' Personal Records to **KNIGHT**.
29. On June 17, 2012, **KNIGHT** used Team Digi7al's Twitter account to make unlawful public disclosure of the Personal Information stolen from Navy-SWM for 20 Service Members. When **KNIGHT** disclosed this Personal Information obtained from the Navy-SWM hack, he obscured the Social Security numbers and disclosed encrypted passwords. **KNIGHT** also posted Navy-SWM's database schema, which damaged SWM by making it more vulnerable to future attacks. Through Twitter postings and links to online storage sites, **KNIGHT** and **KRUEGER** boasted about the Navy-SWM hack, stating that Navy.mil had been "owned", the team had hacked "MY OWN BOAT", and the database should be "FIRE[D]."

30. Between June 17, 2012, and June 23, 2012, TD Member C found Team Digi7al's Twitter posting disclosing the stolen Personal Information from the Navy-SWM hack.
31. On June 23, 2012, TD Member C reposted 20 Service Members' Personal Information, again publicly disclosing this sensitive information.

Obstruction of Justice

32. Between June 22, 2012, and September 26, 2012, **KNIGHT** and **KRUEGER** learned that their hack had received publicity when various news outlets and online blogs reported that Navy-SWM had been hacked and that the personal records of over 200,000 military service members may have been stolen.
33. On October 24, 2012, **KNIGHT** and **KRUEGER** communicated on Facebook using private messaging regarding the Navy-SWM hack. **KNIGHT** ended the conversation with **KRUEGER** by stating, "if anything happens . . . send me a message saying goodbye so we know one of us is caught."
34. On December 14, 2012, TD Member A communicated in an online chat that he was still a member of Team Digi7al and that the group was still communicating, but, because "Navy got pissed" and "started investigating [the Team Digi7al hack]", Team Digi7al had changed its team name and online aliases and that they were "la[ying] low" because he did not "like the sound of prison."
35. Between October 2012 and January 2013, **KRUEGER**, knowing the Navy-SWM hack was within the jurisdiction of NCIS and the Federal Bureau of Investigation, two agencies of the United States, and knowing that the agencies would

investigate the hack, destroyed records with the intent to impede that investigation. Specifically, **KRUEGER** deleted all record of the Navy-SWM hack from his computer's hard drive using a technique known as a "three-pass wipe," which makes recovery of deleted data nearly impossible. This deletion contrasted with his other hacking exploits for which he maintained files on his personal computer, along with a list of hundreds of vulnerable websites for future hacks.

36. On February 6, 2013, pursuant to a federal search warrant in the Eastern District of Virginia, NCIS searched **KNIGHT**'s Virginia residence. NCIS told **KNIGHT** that the agency was investigating the Navy-SWM hack and interviewed **KNIGHT**, who admitted to many of his Team Digi7al activities. **KNIGHT** agreed to cooperate with NCIS in the investigation.
37. Between May and June 2013, knowing that NCIS, an agency of the United States, was investigating the Navy-SWM hack, and having agreed to cooperate in the investigation, **KNIGHT** acted with intent to impede that investigation by encouraging TD Member A to delete all records relating to hacking activities from TD Member A's personal computer hard drive. **KNIGHT** told TD Member A about a specific computer program TD Member A could use to delete all evidence from TD Member A's hard drive. As a result of **KNIGHT**'s instructions, TD Member A deleted those records, intending to impede the investigation.

NGA Hack

38. On July 4, 2012, **KRUEGER** hacked into at least one NGA protected computer and downloaded the database schema for more than 10 databases. **KRUEGER** tried but failed to download from the NGA's computer the sensitive agency information he sought.
39. To execute this hack, **KRUEGER** used SQLi and connected to the NGA server using virtual private network in an attempt to mask his hacking activities.
40. On July 4, 2012, **KRUEGER** unlawfully disclosed the stolen NGA database schema, damaging the NGA's website by making it more vulnerable to future attacks.

RashodHolmes.com Hack

41. On August 3, 2012, TD Member A hacked into at least one Rashod Holmes protected computer and downloaded its database schema, sensitive private information regarding over 1,000 customers (including names, emails, usernames, cleartext passwords, and phone numbers with area codes) and more than 70 individuals' private bank account information (including bank routing numbers, account numbers, and account holders' names).
42. The Rashod Holmes Zipbox Media account that Team Digi7al hacked no longer sells items to the public.

Other Hacks

43. As specified in the table below, from April 7, 2012, to November 17, 2012, Team Digi7al's members hacked into victims' websites and downloaded sensitive information:

	Date	Primary Hacker	Victim	Stolen Information
a.	07-Apr-12	KNIGHT	Leavenworth, WA	1 administrator and 6 users' usernames and cleartext passwords
b.	08-Apr-12	KNIGHT	Spinea Ltd.	2 administrators' usernames, email addresses, and encrypted passwords; claimed to log in to 1 administrator's email account
c.	08-Apr-12	KNIGHT	www.zoolyshop.com	50+ usernames and encrypted passwords
d.	09-Apr-12	KRUEGER	Library of Congress, Civil Rights History Project	Database schema, 8 usernames, encrypted passwords, and email addresses, 4 cracked passwords
e.	11-Apr-12	TD Member B	Email account for Ambassador of Peru in Bolivia	Entire contents of ambassador's email account
f.	13-Apr-12	KRUEGER	Harvard University, Engineering and Applied Sciences, Mooney Lab, Laboratory for Cell and Tissue Engineering	75+ usernames, encrypted passwords, full names, email addresses, and titles
g.	29-Apr-12	TD Member A	Rogsmodels	Database schema, 20+ email addresses
h.	01-May-12	TD Member A	Goon Skate	Database schema, 1,500+ email addresses
i.	01-May-12	TD Member A	Tachograph Analysis Consultants	Database schema, 4 encrypted passwords

j.	09-May-12	TD Member A	Department of Family Practice, University of British Columbia	Database schema, 25+ usernames, full names, email addresses, and encrypted passwords
k.	18-May-12	KRUEGER	Richardson Patel Law Firm	3 administrators' and 10+ users' usernames and cleartext passwords; 60+ client usernames, cleartext passwords, and full names
l.	25-May-12	KRUEGER	World Health Organization - Regional Office for the Eastern Mediterranean	Database schema
m.	03-Jun-12	TD Member A	University of Alabama, University Libraries	Database schema, 40+ usernames and encrypted passwords
n.	11-Jun-12	TD Member A	City of Montgomery and Alabama Police Department	Database schema, stolen records including 7 email addresses and full names (3 of whom were administrators) from IT staff database, Montgomery Police Department's most wanted list with height, weight, hair color, and eye color
o.	18-Jun-12	TD Member A	Alabama Cylinder Head	Database schema, 1 administrator's username, encrypted password, and email address; 4 customers' usernames, cleartext passwords, and email addresses
p.	25-Jun-12	KNIGHT	San Jose State University, Associated Students	Database schema, at least 2 administrators' usernames and cleartext passwords, 60+ additional usernames and cleartext passwords

q.	25-Jun-12	TD Member A	University of Nebraska-Lincoln	100+ email addresses and encrypted passwords, 15+ full names, and 5 cracked passwords
r.	14-Jul-12	KRUEGER	MeTV Network	1,000+ usernames, email addresses, cleartext passwords, and titles
s.	26-Jul-12	KRUEGER	Kawasaki	Database schema
t.	09-Aug-12	KRUEGER	Ultimate Car Page	3,500+ usernames, emails, encrypted passwords, and titles
u.	18-Sep-12	TD Member A	Johns Hopkins University, Peabody Institute	Database schema
v.	30-Sep-12	TD Member A	Exploratorium Museum	Database schema, Twitter username and password
w.	22-Oct-12	TD Member A	Louisville University	Database schema, 20+ staff member records, including full names, email addresses, job titles, and campus telephone numbers
x.	22-Oct-12	TD Member A	Stanford University, School of Earth Sciences	Database schema, 4 users' email addresses and encrypted passwords, research data regarding numerous topics involving the San Andreas Fault Observatory at Depth, 300+ vendor full names, accounting codes and daily costs

y.	09-Nov-12	TD Member A	Montgomery, AL Public Schools	Database schema from the Baldwin Arts and Academics Magnet School
z.	17-Nov-12	TD Member A	Autotrader.com	Database schema, 200+ partial credit card numbers, 4,000+ users' usernames, cleartext passwords, email addresses, names, and telephone numbers

44. In addition to Team Digi7al's verified hacks, its members claimed to have hacked the websites of more than 20 other victim organizations, including governmental civilian and intelligence agencies, universities, and foreign websites.

45. As specified in the table below, from May 15, 2012, to August 11, 2012, Team Digi7al's members Tweeted the following messages to the Team Digi7al Twitter account:

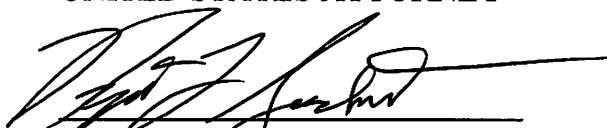
	Date	Team Digi7al Tweet
a.	07-Apr-12	"Here's some .edu emails, users and passes i've had laying around for a while"
b.	11-Apr-12	"In case u didn't no we are TeamHav0k just reformed"
c.	11-Apr-12	"We have something really nice coming your way!"
d.	11-Apr-12	"Just got done dumping the Bolivian Ambassadors inbox, not going to translate it but am uploading"
e.	19-Apr-12	"Newest leak from TeamDigi7al... target http://lanl.gov"
f.	22-May-12	"I would just like to say that in the next few days, me and my team will be releasing our rampage across Canada ;) love ya."
g.	23-May-12	"Didn't I say you were gonna be #owned? Here's day one of our #lulz crusade across #canada"
h.	23-May-12	"theres a statement inside the dump folder, download it and take a look ;) also Toronto PD's DB is coming soon (cont)"
i.	23-May-12	"its a huge [expletive] DB but we're gonna get the job done ;) with what we have so far, we have so much personal info lulz."
j.	23-May-12	"Well heres day 1 of our lulz crusade across canada"

k.	28-May-12	"We've got two big #dumps coming :) the #Toronto #PD and one yet to be disclosed :)"
l.	29-May-12	"#Hacked #Wolrd #Health #Organization #WHO DB"
m.	02-Jun-12	"Hope you all are enjoying the rampage as much as we are! More to come soon!!"
n.	02-Jun-12	"MAJOR @TeamDigi7al hack coming up, stay tuned ;D"
o.	03-Jun-12	"@UofAlabama Your site has been #hacked"
p.	03-Jun-12	"@Torontopolice why is there nothing on your site about us hacking you? :(Don't tell us your trying to sweep it under the rug into the dark."
q.	03-Jun-12	"We have one hell of a #hack coming up in the next few hours ;) stay tuned #HolyLulzCrusade"
r.	03-Jun-12	"HERE IT IS! #DHS"
s.	04-Jun-12	"Pastebin got taken down heres a download for the #DHS"
t.	05-Jun-12	"Looks like good ole' DHS shutdown their vuln link. Makes me sad. Especially since we started dumping the tables ;)"
u.	06-Jun-12	"Its ok, we have another one coming out soon :)"
v.	07-Jun-12	"I've got a major #hack coming up sometime in the next month 23% done with it working 2 days straight.. T.T its a killer i tell you!! [Thor]"
w.	07-Jun-12	"AT&T #hacked, had this sitting around for a month or so"
x.	08-Jun-12	"The people saying #TPD was fake can stfu now, it was an old DB apparently but still we DID #hack them"
y.	08-Jun-12	"@TorontoPolice you are trying to figure out who hacked you? it was us as we said numerous times."
z.	17-Jun-12	"So heres that #Dump i was talking about. #US #Navy was our target >:}"
aa.	23-Jun-12	"Big release from use soon. More to come :)"
bb.	23-Jun-12	Responding to TD Member C taking credit for Team Digi7al hacks after joining Digital Corruption, "which btw you couldnt have bc the DHS and Navy vulns were both patched the day after we released them."
cc.	23-Jun-12	"did i once mention anything about those...nope. But att, dhs,and navy all done by us."
dd.	23-Jun-12	Continuing to respond to TD Member C taking credit for Team Digi7al hacks after joining Digital Corruption,"really? your own work. give me a few seconds to upload some screenshots and i'll prove you guys stole my hacks (7hor)"
ee.	23-Jun-12	To TD Member C, "oh, its being sent to your local pd, turns out hacking dhs is bad lol I mean since you really did it and all"
ff.	25-Jun-12	"Oh hai there. #UniversityofNebraska-Lincoln hacked."

gg.	26-Jun-12	"Hacker c0mrade arrested and charged with 10 counts of malicious attacks against websites"
hh.	04-Jul-12	"National Geospatial-Intelligence Agency #SQL #vulnerable"
ii.	11-Aug-12	"For the information of everyone, we will not be using twitter any longer to post our hacks...good day sirs and ma'ams"
jj.	30-Dec-12	"So we decided to start posting our hacks again :) More to come soon!"

All in violation of Title 18, United States Code, Section 371.

DANNY C. WILLIAMS, SR.
UNITED STATES ATTORNEY



RYAN L. SOUDERS
Assistant United States Attorney