WikiLeaks – Following the Cybertrail

2011 VT InfraGard WikiLeaks Synposium

Dr. Peter Stephenson, CISSP, CISM, FICAF
Director, NUCAC-DF and CISO
Norwich University

NORWICH UNIVERSITY

A Tail of Digital Forensics and Anti-Forensics

- The players
  - PFC Bradley Manning
  - Julian Assange
  - Adrian Lamo
  - Kevin Poulsen
  - Glen Greenwald
  - Chet Uber
  - Mark Rasch
  - Kim Zetter
  - Tyler Watkins
  - David Finkel
  - John Cook
  - Ellen Nakashima
  - Numerous other writers and journalists

NORWICH UNIVERSITY

The Timeline in Brief*

2008:
U.S. Army Counterintelligence Center prepares a classified report placing WikiLeaks on "the list of the enemies threatening the security of the United States." That Report discussed ways to destroy WikiLeaks' reputation and efficacy, and emphasized creating the impression that leaking to it is unsafe.
October:
Manning enters the Army as a private

2009:
November 24:
Per chat logs, Manning said he first started working with Wikileaks after release of 9/11 pager messages, which was first announced on November 24, 2009
November 19:
Earliest possible day Manning downloaded "Collateral Murder" video & all charges except accessing the Rejkjavik 13 cables, per Charge Sheet (Spec. 2 & 4)
November 1:
Earliest date for which government subpoenas Wikileaks related twitter accounts
October:
Manning arrives in Iraq.

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

2010:
January 21:
Manning leaves for US
February 11:
Manning returns to Baghdad from US
February:
Manning gives Wikileaks the video of the 2007 Army helicoper attack on Iraqi insurgents, according to Adrian Lamo in the Washington Post
February 18
Wilikeaks publishes Rejkjavik cable dated January 13, 2010. According to the Manning/Lamo chat transcripts, after the leak Manning tracked the Northern Europe Diplomatic Security Team tailing Assange in Sweden.
March 15
Wikileaks publishes March 18, 2008 NGIC document analyzing the threat Wikileaks posed to the Army.
March 18
Two people carrying diplomatic passports follow Assange from Iceland to Norway.
March 22
Wikileaks volunteer detained and questioned about Assange.

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

May 20
Lamo tweets that people should donate to Wikileaks
Bradley Manning contacts Adrian Lamo on AIM "out of the blue," Lamo tells Yahoo News. He tells Glenn Greenwald Manning first contacted him via encrypted email.
May 21
First chats begin between Lamo and Manning, according to Wired.
Lamo tells Greenwald he lost the PGP key and never decripted emails from Manning, but sent him an invitation to chat over AIM anyway and the two began their alleged exchanges
May 23
Lamo begins "cooperating with federal agents," he tells AOL, after he "passed on what he knew to his ex, who happened to work for Army counterintelligence."
May 23 or 24
"Security pro" Chet Uber gets a phone call from Lamo, who says he has "**received classified documents from a U.S. Army intelligence analyst named Bradley Manning** and wanted advice about what to do."
Uber puts him in touch with the former DOJ head of computer crimes, Mark Rasch. Uber suggests Lamo told him him about having received emails–but when Uber refers Lamo to Rasch, he describes ongoing AIM chats.

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

May 24
Poulsen claims Lamo tells him for the first time of his chats with Manning, after Lamo had already scheduled his first meeting with the FBI the next day
May 26
Manning is arrested in Iraq**, per Lamo and Wired.**
Lamo later tells CNET, "I and the FBI wanted to continue feeding him disinformation," but the criminal investigation unit of the Army had other plans.
May 27
Poulsen meets with Lamo in Sacramento for several hours. Alleges Lamo tells him for the first time the details of his chats with Manning, and he learns Manning's name.
Poulsen says he leaves Lamo at 3pm with the chats on a thumbnail drive
At 4pm, Lamo says he met with FBI for the second time and FBI told him Manning was arrested the previous day in Iraq
Manning's Charge Sheet, however, say Manning's alleged activities continued until "on or about 27 May 2010"
Latest possible date for "introducing" classified information onto his personal computer and obtaining "more then 150,000 diplomatic cables."
Manning's pre-trial confinement begins, and presumably ties to the date when they first assessed what they had on Manning's seized computer

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

How Did Manning Get the Leaked Info Out of Iraq?

- SPECIFICATION 4: In that Private First Class Bradley E. Manning, U.S. Army, did, between on or about 19 November 2009 and **on or about 3 April 2010**, at or near Contingency Operating Station Hammer, Iraq, violate a lawful general regulation, to wit: Paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007, **by wrongfully adding unauthorized software to a Secret Internet Protocol Router network computer**.
  - Adrian Lamo, the California computer hacker who turned in Pte Manning to military authorities in May, claimed in a telephone interview he had firsthand knowledge that someone helped the soldier set up encryption software to send classified information to Wikileaks.
  - Mr Lamo, who is cooperating with investigators, wouldn't name the person but said the man was among a group of people in the Boston area who work with Wikileaks. He said the man told him "he actually helped Private Manning set up the encryption software he used".
  - Mr Lamo said the software enabled Pte Manning to send classified data in small bits so that it would seem innocuous.
  - "It wouldn't look too much different from your average guy doing his banking on line," Mr Lamo said.

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

The Forensics and Anti-Forensics

- Manning's computer
- The cybertrail
  - Manning-Lamo chat logs
  - Twitter
  - Email
- Anti-forensics
  - Encryption

NORWICH UNIVERSITY

Operation Payback

- Anonymous
  - Forensics
    - The Low Orbit Ion Cannon (LOIC)
      - DoS tool derived from a load testing tool
      - Logs the source IP of the attack
    - Computers – both victim and attackers
    - Cybertrail
  - Anti-forensics
    - None for the LOIC
    - Skilled hackers in Anonymous
      - Depend mostly on address spoofing to obfuscate attacks
    - Secure wipe incriminating disks/drives
    - Full disk encryption

NORWICH UNIVERSITY

References

Source Info
Information allegedly accessed by Manning, per his charging document:
The video of the July 12, 2007 Apache killing of Reuters journalists
The Rejkjavik State Department cable leaked by WikiLeaks
50 State Department cables (loaded onto his unsecured computer, transmitted to someone unauthorized to receive them)
150,000 State Department cables (obtained information from them via unauthorized access)
A classified Microsoft Powerpoint presentation

Chat Logs
Wired – 6/10/10
Washington Post – 6/10/10
Boing-Boing – 6/19/10
Merged Manning-Lamo Chat Logs

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

References

Resources

Manning charge sheet
Marcy Wheeler on the glaring inconsistencies in Adrian Lamo's stories
Marcy Wheeler: more inconsistencies in Lamo's stories
Judge's order unsealing Twitter subpoena (PDF)
Justice Department's subpoena of Twitter (PDF)
AdrianLamoLogs Timeline
Cryptome Timeline
Adrian Lamo Interview Transcript Page
Key Articles in the Wikileaks – Manning investigation

Related Links

David E. Coombs, Attorney for Bradley Manning
Bradley Manning Support Network
Courage to Resist
Xeni Jardin on BoingBoing
Threat Level on Wired

http://firedoglake.com/bradley-manning-wikileaks-timeline/

NORWICH UNIVERSITY

Other Sources

- http://www.anti-forensics.com/hunting-anonymous
- http://catastrophist.wordpress.com/2010/07/29/wikileaks-internal-dissent/
- http://www.foxbusiness.com/markets/2011/01/28/fbi-executes-search-warrants-wikileaks-probe/
- http://praetorianprefect.com/archives/2010/12/anonymous-turns-operation-payback-toward-the-jester/
- http://arstechnica.com/tech-policy/news/2011/02/the-ridiculous-plan-to-attack-wikileaks.ars
- http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars
- http://www.securitynewsdaily.com/censoring-wikileaks-virtually-impossible-0336/
- http://www.securitynewsdaily.com/wikileaks-hacktivists-not-so-anonymous-after-all-0383/
- http://www.dailyrosetta.com/computer-forensic-to-examine-wikileaks-founder%E2%80%99s-internal-emails/4215.html

NORWICH UNIVERSITY