FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 01/02/2014

On December 5, 2013, THOMAS KENNEDY MCCORMICK, date of birth [redacted], , social security account number student residential address University of Massachusetts – Amherst, Dorm Room 231 Baker Hall, 160 Clark Hill Road, Amherst, MA, was interviewed pursuant to a federal search warrant being executed at his Dorm Room. After MCCORMICK was advised that this was a search warrant, he was not under arrest, he was free to leave at any time, and speaking to Agents was voluntary, MCCORMICK was invited to talk with the interviewing Agents in a vehicle parked in the front of Baker Hall citing purposes of privacy and discretion for MCCORMICK. MCCORMICK indicated that he understood that he was not under arrest and that he was interested in cooperating and talking with the interviewing Agents. While in his dorm room, he requested water which he took with him to the vehicle. MCCORMICK was offered to use and used the restroom when walking to the vehicle. After being advised of the identities of the interviewing Agents, MCCORMICK voluntarily provided the following information:

MCCORMICK (hereinafter TM) advised Special Agent David Hitchcock of his academic background and employment history while in the dorm room prior to walking to the vehicle. TM was currently in his Junior year at the University of Massachusetts (UMASS) – Amherst and majoring in Computer Science. He attended the Cambridge Rindge and Latin School and took a "gap year" following high school, where he took one year off, during some of which he traveled in Europe.

TM had interned at Microsoft for several summers and Cisco for one summer. He was seeking full-time employment with Microsoft.

The foregoing information was provided to both interviewing Agents in the vehicle. TM thought that the search warrant was possibly related to malware. He had skills in malware analysis and this was a main interest since he was young. He also had skills in reverse engineering. TM indicated he had not done anything with malware in a long time which he later defined as years.

TM provided that he had stopped talking to people online and had not been involved in any online forums for a while.

Investigation on 12/05/2013 at Amherst, Massachusetts, United States (In Person)

File # 288A-WF-240934-S11 Date drafted 12/05/2013

by David L. Hitchcock, HOOL KEVIN J

TM then asked for the situation to be explained in further detail and asked what he was involved in. The interviewing Agents explained that the search warrant being executed was related to computer crimes. TM was advised again that this was a search warrant of his dorm room, that there was no warrant for his arrest, and that he was free to stop talking with the Agents at any time and free to leave at any time. He was further instructed that his cooperation, and answering any of the Agents questions, was completely voluntary. TM indicated that he understood that his cooperation was voluntary and that he was interested in answering any questions asked of him.

TM was then asked about the Darkode hacking forum (hereinafter DK) and TM indicated he had multiple accounts on DK. He no longer had access to his FUBAR account which was his old, big account that had the largest number of posts.

TM indicated that he wanted to be cooperative but he did not want to "screw" himself.

TM said that he had provided the true identity of the Spy Eye author to Brian Krebs.

TM said he talked to the Zeus author four years ago and did not know him very well.

TM then asked how the morning would end for him and said that he would like to establish a cooperative relationship, but was concerned about what would happen to him. The interviewing Agents explained again that there was no arrest warrant for TM and that he would not be arrested at any point during the day. He asked if he should get an attorney and he was instructed that it was his decision. TM was again advised of the voluntariness of the interview and his cooperation, and that he was free to leave the interview at any point in time. He again indicated he understood and that he wanted to continue answering any questions that were asked of him.

Darkode was started by . was an admin of DK and a security expert who lived in Argentina and was named (Last Name Unkown). , aka , aka lived in Europe and took over DK when Iserdo was arrested. TM was "pretty sure" CRIM authored CRIMEPACK and indicated that he did not chat with often and did not remember ever knowing his true name. He then said that he discussed Darkode administrative items with .

TM also had access to the Sorcerer or Wizard account on DK. TM first joined DK in 2006, 2007, or 2008.

TM had email accounts including but not limited to

. He forwarded mail for many of the accounts to root@botnet.biz. TM used the account to register domain names. He used tempomail.fr accounts for DNSexit.com to manage DNS records for domain names. TM indicated that he setup accounts at DNS providers for people who did not know how to use tempomail.fr. TM also used tempomail accounts at FreeDNS.

TM did not keep chat logs and turned the logging feature off for chat services. His old chat logs might be on his old Macbook Pro laptop. He was currently using the Microsoft Surface Tablet.

TM talked on ICQ with the creator of Zeus years ago. TM never sold Zeus and only knew one person, with the online moniker D[something followed by numbers], who purchased Zeus. When asked if it was Dethan, TM agreed that it was Dethan who purchased Zeus. Dethan got the Zeus builder either from TM or the creator, and later TM indicated that TM "might have given it to" Dethan. Dethan paid the author for Zeus, and three days later, Dethan was told what to do. TM said that he talked big online to build his credibility and that the Zeus author stopped talking to him after one month.

TM used the Jabber ID until his Jabber server got attacked.

ngrBot was coded by in England, a Dutch guy named and that TM had contributed to it. TM said that he never saw the source code and only sent code snippets to contribute. TM said that he had probably posted an ad for ngrBot on Darkode. got arrested and then stole money from TM. All ngrBot sales had to go through . TM made the ngrBot Jabber account. and others had access to the ngrBot Jabber account. All proceeds from the sale of ngrBot went to via Liberty Reserve, Webmoney, and Western Union. Western Union was used to exchange funds from Liberty Reserve. TM never accepted any wire transfers.

TM offered to help identify individuals who purchased ngrBot. Logs of the sales would be on TM's Macbook Pro. A list of customer information was on the Macbook and/or USB drive. His new Surface Tablet was a clean break from the illegal activity. The Macbook was encrypted with TrueCrypt and TM said he did not remember the password and that he had not used the Macbook

in three months. The ngrBot customer list might be on the Tablet or on an unencrypted SD card inside the Tablet.

TM stated that he never cashed out the proceeds from his criminal activity online. TM also said that he never exchanged virtual currencies onto a credit/debit card. He then said that one time he purchased a prepaid debit card from CVS and loaded proceeds from his criminal activity onto the prepaid card. No one else ever loaded TM's money onto cards on TM's behalf. TM converted sales to Liberty Reserve and sent the money to others. TM used the proceeds to purchase servers and infrastructure for botnets and to further his criminal activity, but never cashed out money that he made online. TM purchased the Macbook with money he earned during his Microsoft internship. TM stated that he never benefited from selling malware.

TM provided input on how to code a Skype spreader to an individual using the online moniker because asked for help with developing the spreader. TM said that he hated giving out source code and that he made a binary to generate strings and gave it to . had an account on DK. , aka , asked for a DK account and TM gave access to the account. TM also setup a Jabber account, chrysus@thesecure.biz, for . was named had a last name that started with an L, and attended a state college in Florida. worked with a Macedonian named that was "sketchy and dumb." and used ngrBot and the Skype spreader to run a botnet, and they might have sold the Skype spreader. TM also said that he fixed source code for the Skype spreader and sent it back to . TM had known for a long time and had originally met him on a hacking forum like Unkn0wn.

TM created the domain hustling4life.biz. He also setup DNS for the hustling4life.biz domain for an individual using the online moniker , aka , on DK. TM said he never managed the botnet on the domain. TM said that he originally had a partnership with . would give directions and TM would follow them. TM said that he never got paid or wanted to get paid by . often complained about getting screwed over by partners. asked TM to register DNS, setup a server, and code a cookie cleaner. TM did these things for . used Zeus, Spyeye, Ice IX, and Citadel for bank fraud. The cookie cleaner that TM created for was used to clean the cookies from a victim's computer which would force the victim to log back into their bank account and a bank trojan would then be used to harvest personally identifiable information (PII) such as the victim's username, password, PIN numbers, and answers to security questions. Specifically, the cookie cleaner would clear the victim's web browser's

session, or connection, with the bank's web site and force a new login. TM then recanted and said that paid him on a few occasions for the work that TM did for .

TM gave access to the hustling4life.biz domain after was no longer using the domain. TM said that and had monetized a botnet with fake antivirus, participating in pay-per-install affiliate programs, and selling installs to other individuals. was not involved with banking malware but might have worked with Ransomware.

TM had found the email address of the Spyeye author in an old fake antivirus affiliate program database and that TM was able to find the true name of the Spyeye author from searching online for an individual that used the email address. TM passed this information onto Brian Krebs.

TM had operated numerous botnets over the years including but not limited to IM Bot, rx Bot, Zeus, Ice IX, and ngrBot. and TM did not ever use or purchase Citadel. TM did not ever use bank trojans. He had operated a Zeus version 1.x botnet with 4,000 to 5,000 peak online. TM used Nuclear pack, Fiesta, and Crimepack exploit kits. He used Nuclear for a couple of months and he used Fiesta when he was in high school.

TM tested ngrBot extensively and the largest botnet he had with ngrBot was 15,000 to 20,000 peak online, as that was the maximum connections that his server could handle. He used 10 to 20 domains for ngrBot. TM used the following domains to operate botnets:

- Hsbc-bank.co.uk (IM Bot)
- Kaspersky<something>.ru (ngrBot)
- Kaspersky<something>.su (ngrBot)
- Photobeat.su (Zeus, Ice IX)
- Saturn.losa.pl (ngrBot and used with [redacted] and [redacted])

TM did not use the bigbucks.cc domain for botnets, but did use the domain for Gmail, MSN Messenger, and other chat services.

ngrBot was cracked between April 2011 and July 2011. TM started UMass in the Fall of 2011.

TM setup Ice IX or an old version of Zeus for [redacted].

To keep TM's binaries fully undetectable to antivirus (FUD), TM used crypting services. He "bummed" Father Crypter crypting service from [redacted]. Father Crypter chose this name after his father died. TM also used Robo Crypter.

TM last logged into DK in the summer of 2013. He got bored with DK and wanted to "close that chapter" of his life. He thought that had changed the password to his fubar account.

TM used the botnet.biz server as a socks proxy and Jabber server. Botnet.biz was hosted on a Santrex VPS that TM leased annually. TM confirmed that the IP started with 46.166.143. He would use the proxy to login to DK and his various accounts used for malware-related activities. TM switched to proxy through Tor in the end of 2012 or early 2013. He may have also used other paid VPN or VPS hosts and free proxies for anonymity, as well. TM shared the Santrex VPS with . TM said that he would share his Santrex proxy with anyone who asked. When TM was prompted for names of individuals he shared the proxy with, he recanted and said that he did not recall giving access to anyone other than .

TM likely last talked to in the last month and definitely talked to him online during the Fall 2013 semester.

TM currently only talked to three individuals on Jabber: at the University of Massachusetts using Jabber ID's and , [redacted], and [redacted].

TM had two to three WMZ accounts and last accessed Webmoney in early 2013. He preferred Liberty Reserve (LR) and had three LR accounts. One LR account was registered with joshuamilestone@gmail.com. and had access to this LR account and stole $5,000 from TM. was from Macedonia, lived in Switzerland, and could also be located in Albania. At one time, TM had true name from a Facebook link that someone sent TM. The most that TM had in the shared LR account was $5,000. TM used the LR funds to buy servers, software, or to donate the money to people he met on the criminal hacking forums who were poverty-stricken living in villages in Peru and other countries.

TM used proceeds to get a Vanilla Visa card from a guy in a forum like Verified. He paid $50 to $100 to get the prepaid Visa card mailed to him. The Vanilla Visa did not work for him. TM then obtained a prepaid debit card from CVS. He used an exchanger to move approximately $200 from LR to the prepaid card from CVS. He then used the prepaid card to buy items at CVS and groceries.

TM installed Ransomware for a pay-per-install affiliate program with a .de domain. He received money from the affiliate program in LR or in prepaid vouchers. He never made money and the Ransomware killed his botnet. On a

separate occasion, a "sketchy Russian" gave TM prepaid vouchers.

TM provided the password for the Microsoft Surface Tablet was . He also provided part of the TrueCrypt password for the Macbook Pro, <and random characters that were non-alpha-numeric>. The password to the iPhone was .

TM was offered food and restroom breaks throughout the interview, and had water on his person throughout the entire interview. TM was also provided the time of day throughout the interview because he indicated he had an afternoon exam that same day.

TM stopped the interview at approximately 10:10 AM in order to prepare for his afternoon exam. The interviewing Agents provided their contact information and instructed TM to call the interviewing Agents after his exam in order to discuss what data TM would need a copy of for academic purposes.