IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *v.* HAMZA BENDELLADJ (A.K.A. "BX1")	Criminal Action No. 1:11-CR-557-AT-2

Sentencing Memorandum

The United States of America, by John A. Horn, United States Attorney, and Kamal Ghali and Steven D. Grimberg, Assistant United States Attorneys for the Northern District of Georgia, files this Sentencing Memorandum.

1. Procedural History.

This is an international computer hacking case. On June 2, 2013, a grand jury in the Northern District of Georgia charged Russian-national Aleksandr Andreevich Panin (a.k.a. "Gribodemon") and Algerian-national Hamza Bendelladj (a.k.a. "Bx1")[1] in a 23-count Superseding Indictment alleging bank and wire fraud conspiracy, wire fraud, conspiracy to commit computer fraud and abuse, and multiple acts of computer fraud and abuse. Doc. 35.

On June 26, 2015, Bendelladj pled guilty to all 23 felony counts without the benefit of a negotiated plea agreement. Doc. 136. The Court set Bendelldaj's

[1] *See* PSR, at ¶ 40 ("Bendelladj used multiple aliases and email accounts as part of his computer hacking activities including: Bx1, bx1@hotmail.com, airlord1988@gmail.com, bx1@jabber.org, rozz.scglobal@gmail.com, danieldelcore@gmail.com, Daniel DelCore, Hamza Minetti, Danny Hamza, bx1@xmpp.org, alertz1@swissjabber.ch, and dejavu@thesecure.biz.").

sentencing for March 7, 2016. Doc. 149. The Presentence Investigation Report ("PSR") holds Bendelladj responsible for $100 million in financial losses. PSR, at ¶¶ 38 and 76. Indeed, on the date of Bendelladj's arrest in Thailand in January 2013, agents seized his laptops and multi-media, which housed a treasure trove of incriminating evidence: chat messages with other notorious cyber-criminals; malicious software ("malware") for well-known botnets such as SpyEye and Zeus; stolen credit card information belonging to 200,000 people located around the world (including 80,000 people in the U.S., as well as citizens of the Northern District of Georgia); and the source code for www.vcc.sc, or "Virtual Credit Card," Bendelladj's web-based business that sold stolen financial information to other cyber-criminals and thieves.

In short, Bendelladj is a prolific computer hacker, botnet master, and thief. As part of his international campaign to steal financial information using botnets, he stole 200,000 credit cards, cashed out millions of dollars stolen from bank accounts across the world, and inflicted millions in damage on personal computers by infecting them with malicious software. His sentence should reflect the enormous destructive impact that he has inflicted through cyber means around the world.

2. Bx1's prolific infection of personal computers around the world.

Bendelladj perpetrated his international theft campaign by running massive "robot networks" of personal computers—tens of thousands of computers at a time—referred to as "botnets." In order to bring a personal computer under his control, he needed to infect it with malware. Once infected, Bendelladj could

control a victim's personal computer.[2] And using different tools, including malware such as SpyEye,[3] Bendelladj stole personal and financial information.

His methods of infecting computers varied: he used spam email messages; he infected popular websites; and he used a custom-built "Spreader" designed to push out malicious software, such as SpyEye and Zeus, onto hundreds of thousands of personal computers.

Once he infected a personal computer, with whatever malicious software ("malware") he happened to be running, whether it was Zeus, SpyEye, or a custom built private bot, he proceeded to steal personal information from the computers and to use that information to steal from bank or credit accounts.

When interviewed by agents in Thailand, Bendelladj admitted to having up to 50,000 computers under his control at one time. PSR, at ¶ 61. But a review of Bx1's chat messages, which were saved on his laptop, reveals that from 2011 to 2012 alone, he likely infected hundreds of thousands of personal computers around the world for the purpose of creating massive botnets to steal personal information. *Cf.* PSR, at ¶ 64 (noting that Bendelladj's electronic media contained "online instant chat logs between Bendelladj and others . . . in which they discussed assorted nefarious cyber activities, including the development and operation of SpyEye").

---

[2] *See* PSR, ¶ 30 ("Cybercriminals electronically distribute and installed SpyEye files onto victim computers through one or more of numerous infection methods.").

[3] *See* PSR, ¶ 32 ("SpyEye is a sophisticated malicious computer code designed to automate the theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information.").

A. Bendelladj infected at least 200,000 computers, or bots, with malware using spam email messages.

For starters, Bendelladj admitted to spreading "his malicious binaries via spam campaign services he purchased." PSR, at ¶ 61. This admission is corroborated by multiple chats that show the numbers of bots under his control waxed and waned over a 2-year period. On January 28, 2011, he told a compatriot that he sent "over 1 million" spam messages in the "U.S" that were "fresh"; that spamming campaign yielded 200,000 bots.[4] In September 2011, he casually noted that he was "spamming to get bots."[5] During that month, he tried a method of spamming that spawned 2,500 bots in a single day.[6]

During the month of October 2011, he controlled 20,000 bots in the U.S. alone.[7] On October 16, 2011, on www.darkode.com,[8] Bx1 advertised a spam method under

---

[4] *See* January 28, 2011 chat between xlt@voicore.ru and bx1@jabber.org ("i spammed all and i recieved 200 000 bots").

[5] *See* September 25, 2011 chat between bx1@jabber.org and parabola@xmpp.jp ("[9/25/2011 12:15:56 AM] parabola: sup [9/25/2011 6:44:28 AM] bx1: nothig much [9/25/2011 6:44:36 AM] bx1: am spamming to get bots").

[6] September 28, 2011 chat between bx1@jabber.org and greatbeast2000@jabber.org "I found a method of SPAM Just Tried i it 1 day 2500 bot and no virus or detection").

[7] October 4, 2011 chat between bx1@jabber.org and nibo@xmpp.jp ("bx1: i got over 20k US frech Bots").

[8] PSR, at ¶ 41 ("Darkode was an online, password-protected forum in which hackers and other cyber-criminals convened to buy, sell, trade and share information, ideas, and tools to facilitate unlawful intrusions on others' computers and electronic devices. Before becoming a member of Darkode, prospective members were vetted through a process in which an existing member invited a prospective member to the forum for the purpose of presenting the skills or products that he or she could bring to the group. Darkode members used each other's skills and products to infect computers and electronic devices of victims around the world with malware and, thereby gain access to, and control over, those devices. Both Panin and **Bendelladj** were members of Darkode. ").

the heading: "Spam Millions to Inbox." Despite his own spamming capabilities, he supplemented his efforts by purchasing services from other cyber-criminals. In December 2011, Bendelladj relied on notorious cyber-criminal Rescator for additional spamming services.[9]

By June of 2012, he generated 10,000 bots from the U.S. in a single day, because, in his words, he spammed "24x7."[10] During that month, he infected 12,416 computers as part of his ICEIX botnet.[11] In the month leading up to his arrest, he

---

[9] *See* December 27, 2011 chat between bx1@swissjabber.ch and rescator@lampeduza.org (bx1 requesting "250k" messages and Rescator indicating that it would be "no problem").

[10] June 20, 2012 chat between bx1@jabber.org and g0dlike@jabber.org:

bx1:	what country u need
g0dlike:	usa
bx1:	i can get fresh good bots
bx1:	i can get u
bx1:	more then 10k a day
g0dlike:	how many a week?
bx1:	easy for me
g0dlike:	u 100% sure?
bx1:	yes bro
bx1:	i spam
bx1:	24x7
bx1:	i got my method
. . .	
bx1:	and got over 100000 fresh base

[11] June 20, 2012 chat between bx1@jabber.org and g0dlike@jabber.org ("[6/20/2012 2:07:29 PM] bx1: Total bots: 12 416 [6/20/2012 2:07:35 PM] bx1: on ICE XI").

targeted the US for his spamming activities.[12] And he noted how easy it was to find bots by spamming.[13]

B. Bendelladj infected numerous computers using and selling the "Spreader" tool.

Bendelladj distributed and sold a tool designed to rapidly proliferate the spread of malware and computer infections: the "Spreader." True to its name, the "Spreader" helped to "spread" SpyEye, Zeus, and other types of malware designed to steal personal information.[14] In May 2011, on www.darkode.com, Bx1 started a thread entitled "Selling Spreader BINS (Facebook, USB, IM . . . .)."[15] *See also* Exhibit A attached hereto.

He wrote, "I'm selling Spreader that **help you get more bots with fast spread**. Spreading method are:

- Facebook (IM, Comment, MSG)
- Twitter (MSG, Status)
- Tagged (MSG)
- eBuddy
- USB (Ink, autorun.inf)

---

[12] *See* December 4, 2012 chat between teardrop@xmpp.jp and dejavu@thesecure.biz ("(1:07:22 PM) dejavu@thesecure.biz: i preparing to spam USA").

[13] *See* December 4, 2012 chat between teardrop@xmpp.jp and dejavu@thesecure.biz (teardrop@xmpp.jp: "i wouldnt even know where to find bots" dejavu@thesecure.biz: "easy to find just spam bro").

[14] PSR, at ¶ 46 ("In a May 2011 post, Bendelladj offered to sell a SpyEye plugin called 'Spreader,' which was a method for delivering malicious software.").

[15] *Id*.

- Gmail (MSN, IM)
- Hi5 (Comment, MSG)

and many other methods and adding more in future (OFC by request)."*Id*. He further noted that "it works with SpyEYE because its Plugin for it." *Id*. His post guaranteed "from 20K BOTS YOU CAN JUMP TO 200K WITHIN FEW WEEKS." *Id*. In other words, each sale of the Spreader would translate into 200,000 infected computers with "a few weeks." On June 15, 2011, he posted about the Spreader again "just to let everyone know it works with SpyEYE" and that the Spreader also included a "Fixed Facebook Spreading" feature whereby "Infected User cannot see the message that spreader sent." *See* Exhibit A, at 3.

Chats reveal that Bendelladj sold the Spreader tool to multiple different cyber-criminals. In April of 2011, he was actively working on a "spreader" capable of amassing 10,000 bots in a single day.[16] On May 29, 2011, he confirmed that a SpyEye user named "solotech" had "purchased my spreader for 6k."[17] He told another compatriot that he had sold at least 2 batches of Spreader and had 3 more left.[18] He agreed to provide it to a cyber-criminal named g0dlike[19] And he tried to

---

[16] April 28, 2011 chat between snas@jabber.ru and bx1@jabber.org:
bx1: cos i'm working
bx1: on Spreader
snas@jabber.ru: this your zeus ?
bx1: a spreader that able to get over 10k bots a day
See also April 3, 2011 chat between bx1@jabber.org and mafioso@xmpp.jp: ("bx1: i writting bx1: a spreader").

[17] May 29, 2011 chat between snas@jabber.ru and bx1@jabber.org: ("he use spyeye solotech purchased my spreader for 6k").

[18] *See* March 29, 2011 chat between bx1@jabber.org and parabola@thesecure:

sell it to at least one of Panin's existing SpyEye customers.[20] In May of 2011, his SpyEye spreader yielded him 36,000 botnets (*i.e.*, infected personal computers) in France alone.[21] And he explained that his SpyEye module had the capacity to grow to 150,000 bots in one month.[22]

---

bx1:	hey do u use spyeye?
parabola:	yes
bx1:	u saw my spreader
bx1:	i sold 2 copy's already and only 3 copy left
bx1: i	can sell u

[19] May 27, 2011 chat between bx1@jabber.org and g0dlike@jabber.org:

g0dlike:	can u give it to me THE SPREADer when i setup spyeye
bx1:	dll ?
bx1:	or i setup for u ?
g0dlike:	whatever way you want
bx1:	ok np
g0dlike:	thanks bro

[20] *See also* May 29, 2011 chat between snas@jabber.ru and bx1@jabber.org: ("bx1: anyway if u're intressted on spreader i can sell u dll under license of ur spyeye for 3k").

[21] May 6, 2011 chat between bx1@jabber.org and mafioso@xmpp.jp:

bx1:	just busy with my family and building botnets
bx1: :	D
mafioso@xmpp.jp:	hehe
bx1:	my net is growing up
bx1: :	D
mafioso@xmpp.jp:	how big
bx1:	36K
bx1:	FR Only
bx1:	because i denied other bots
bx1:	i need good packs
mafioso@xmpp.jp:	hehe nice
mafioso@xmpp.jp:	how u get this many FR
bx1:	Spreader
bx1:	Pluguin for SpyEye

By June of 2011, he was actively selling the Spreader.[23] And in that month, he was generating 5,000 to 1,000 bots a day from a spreader for his own botnet:[24] His campaign continued well into March 2012, where he told others that he was developing a Spreader that would work with Zeus and "any bot."[25]

---

[22] May 20, 2011 chat between snas@jabber.ru and bx1@jabber.org:

bx1:	on mine is built in
bx1:	this
bx1:	with SPYEYE
bx1:	Module
snas@jabber.ru:	very nice :)
bx1:	:)
bx1:	u can get
bx1:	if u 10k bots
bx1:	garanted
bx1:	1 month u'll be with
bx1:	150k bots

[23] June 24, 2011 chat between inkubus@jabber.org and bx1@jabber.org: ("bx1: all i do now is selling Spreader").

[24] June 15, 2011 chat between bx1@jabber.org and ling0@jabber.org:

ling0:	How many bots you getting daily now?
ling0:	From spreader
bx1:	depend
bx1:	sometimes
bx1:	5k
bx1:	sometimes
bx1:	4
bx1:	sometimes 1

[25] *See* March 15, 2012 chat between bx1@swissjabber.ch and s3x@neko.im ("bx1: i make a auto FB Spreader that work with Zeus and any bot without hooking Auto Spreader").

3. Bendelladj's use of SpyEye and related-botnets.

During the investigation, the FBI obtained samples of SpyEye malware in the "wild," *i.e.*, samples of the malware found on infected personal computers and computers of internet security research companies. Those samples proved that certain SpyEye binaries were directly linked to Bendelladj. PSR, at ¶ 58.

Bendelladj admits that he obtained copies of SpyEye from his co-defendant, Panin (a.k.a. "Gribodemon"). *See* Bendellad's PSR Objections, at ¶ 81 (describing himself as Panin's "client"). And he does not dispute that "Panin embedded the nickname and other particular information about his customers into every version of SpyEye that he sold." PSR, at ¶ 36. In other words, Bendelladj's strains of SpyEye had his name on it. To that end, an analysis of the source code of at least 4 versions of SpyEye malware detected by other anti-virus companies shows that Bendelladj's nickname ("bx1") and the server domain ("100myr.com") were both embedded in the malware binaries. PSR, at ¶ 58.[26]

The source code's reference to www.100myr.com also confirms Bendelladj's active involvement in running SpyEye botnets and the location of some of his Command and Control servers. *Cf.* PSR, at ¶¶ 27, 53-56. Indeed, in a sworn affidavit filed with this Court, Bendelladj admitted that he was the "registered owner and manager" of www.100myr.com. *See* Bendelladj's Objections to Report & Recommendation, at 118, at 2 ("Bendelladj asserts that he is owner of …

[26] Likewise, the FBI analyzed the source code from 59 other strains of SpyEye malware detected by a Norwegian-based internet security research organization and found that they shared the word "Bx1" in the binary and that the configuration files showed that the malware was designed to steal from at least 253 different financial institutions located in the U.S. and around the world. *Cf.* PSR, at ¶ 56.

100myr.com") (citing to affidavit executed by Hamza Bendelladj).[27] A search of Bendelladj's laptop and multi-media on the date of his arrest revealed multiple references to www.100myr.com and SpyEye source code. PSR, at ¶ 64.

But www.100myr.com is the domain name of a server that Bendelladj used to control his botnet. An analysis of the SpyEye source code shows that the malware instructed infected computers to send data (including bank and credit card login information) to the Internet Protocol address associated with www.100.myr.com. PSR, at ¶¶ 56-58. That domain, www.100myr.com, had different IP addresses at different times. Indeed, from February 2, 2011 through April 10, 2011, Bendelladj changed the Internet Protocol address of his Command and Control server at least 3 times in an effort to keep it hidden from law enforcement. *See,e.g.*, Exh B and C (showing the location of the server switched from Lansing, Michigan; to Atlanta, Georgia; to San Jose, California; to Luxembourg and corresponding IP addresses). From February 13, 2011 through March 7, 2011, www.100myr.com resolved to IP address 75.127.109.16, an Atlanta, Georgia-based IP address. *Id*.

A review of the data on the Atlanta-server (75.127.109.16) showed that 217 personal computers located around the world—and infected with SpyEye—were sending "GET requests" (or "calling home") to the Atlanta-server. PSR, at ¶¶ 53-58. An analysis of the data coming into that server showed that the incoming data had the same digital fingerprint, or MD5 hash values, as other SpyEye binaries with the

[27] Notably, "Myr" is an abbreviation for Malaysia's currency, the Malaysian Ringgit. Moreover, Bendelladj lived in Malaysia during the course of his criminal conduct and was travelling from Malaysia through Thailand on the date of his arrest. *See* PSR, at ¶ 59.

word "bx1" embedded in the code. PSR, at ¶ 56.[28] In other words, those 217 computers were infected with Bendelladj's SpyEye malware and calling home to the Command and Control server.

Bendelladj's penchant for quickly changing Command and Control servers to stay ahead of law enforcement is corroborated by a September 1, 2011 post on www.darkode.com, where under the heading "Santrex Police Bitches," he complained that an internet hosting company "gave my server to Cops." *See* Exh. D. He noted that "on all ways I changed everything and no trace☺ and root pass was changed . . . so they can't get shit." *Id*. On that same date, he posted that "there is nothing important on server only SpyEYE collector without DB." *Id*.

Nonetheless, he quickly rebounded after changing servers. By May 2011, Bendelladj was running SpyEye off of six Command and Control servers that controlled around 50,000 bots.[29] A week later, he appeared to have amassed an

---

[28] While Bendelladj notes in a "supplemental objection" letter that this Atlanta-based server was "not his" and belonged to his friend "mimou," this objection contradicts his sworn affidavit (whereby Bendelladj claimed to be the manager and owner of www.100myr.com) and contradicts the factual basis for pleading guilty to counts 14 through 23. Because he has pled guilty, he cannot dispute that, for example, in February 2011, he "intentionally access[ed] a computer without authorization . . . to obtain information . . . for the purpose of private financial gain," that he did so from a server located in the Northern District of Georgia, and that his conduct impacted, at a minimum, the computers identified in Counts 14 through 23 of the Superseding Indictment. Doc. 35 (referring to 18 §§ U.S.C. 1030(a)(2)(C) and 1030(c)(2)(B)(i)). Such frivolous objections, if pursued at the sentencing hearing, jeopardize Bendelladj's eligibility for acceptance credit.

[29] May 11, 2011 chat between inkubus@jabber.org and bx1@jabber.org

bx1:	no i dont need bots
bx1:	i got around
bx1:	50k
bx1:	ady
bx1:	:D

additional 50,000 bots.[30] And he admitted to using a Luxembourg-based internet hosting provider to run SpyEye.[31]

---

bx1: thx u
inkubu: wow :D
bx1: i've bots bro thx u
bx1: i've 6 servers running
bx1: and hidden SpyEye
bx1: impossible to be detected

[30] May 17, 2011 chat between bx1@jabber.org and mafioso@xmpp.jp:
bx1: new spyeye
bx1: is good
bx1: he change alot
. . .
bx1: i wanna good bot
bx1: at least to save my bots
mafioso@xmpp.jp: yeah it's hard
mafioso@xmpp.jp: better use them while u can
bx1: yes
bx1: problem now with SPYEYE
bx1: is
bx1: the one
bx1: when u click get
bx1: EXTRACTED
bx1: that one detected
bx1: i didnt test it on other bots
. . .
mafioso@xmpp.jp: u still have over 100k bots so dont complain hehe

[31] May 30, 2011 chat between bx1@jabber.org and g0dlike@jabber.org:
bx1: Luxmuburg
bx1: very fast
bx1: and good
bx1: i using it
bx1: to host my net
bx1: 2 month
bx1: np
bx1: at all
g0dlike: ya but spyeye is ok for that ?

By June of 2011, he was setting up SpyEye for other cyber-criminals.[32] Meanwhile, he used a "crypter" to make his own SpyEye botnet "fud" or fully undetectable.[33] He continued using SpyEye through October 2011 including via Remote Desktop.[34] During that month, October 2011, he purchased the ICE-IX

---

bx1: i use spyeye

[32] June 29, 2011 chat between bx1@jabber.org and ling0@jabber.org:

bx1:	give me server info
bx1:	i setup for u
bx1:	now
bx1:	broski
bx1:	and sorry for late
ling0:	spy.ixloader.com
	User - **REDACTED**
	Password – **REDACTED**

[33] June 30, 2011 chat between snas@jabber.ru and bx1@jabber.org:

bx1:	i make personel crypter
bx1:	for
bx1:	SpyEYE
bx1:	even Dropped EXE and BIN
bx1:	will be fud
. . .	
bx1:	with my crypter cannot detected

[34] October 19, 2011 chat between snas@jabber.ru and bx1@jabber.org:

bx1:	i like to use
bx1:	RDP
bx1:	on SpyEYE
. . .	
snas@jabber.ru:	what u use?
bx1:	SpyEYE
snas@jabber.ru:	spyeye?
bx1:	Yup

botnet from an individual using chat handle zebra7753@secure-jabber.biz and the nickname ICE9.[35]

By July 2012, Bendelladj was still actively involved in trying to get credential stealing malware; in that month, he solicited "hapyfrieends@jabbim.cz" in an effort to get his hands on another "botnet like Zeus or SpyEYE . . . [that] works on Chrome."[36] Even in the weeks leading up to his arrest, he bought another notorious malware tool kit designed to steal from banks, Carberp.[37] And he noted that Carberp was "working ggr8."[38]

4. Bendelladj's sale of the Automatic Transfer System

In September 2011, posting as Bx1, Bendelladj advertised the sale of an "Automated Transfer System" module for botnets such as SpyEye. PSR, at ¶ 47; *see also* Exhibit E attached. In January 2012, Bx1posted to www.darkode.com and

---

[35] Ice9: godlike sad that we can make a deal
Ice9: i can offer you ice9 bonten
Ice9: and he sad you have ats
bx1: Yea

[36] *See* July 20, 2012 chat between bx1@jabber.org and hapyfrieends@jabbim.cz ("Inject must be same as Zeus format").

[37] *See* dejavu@thesecure.biz chat with batman@xabber.de on Dec. 24, 2012 ("hello i would like to buy Carberp . . . how much for Carberp pack . . . am ready to buy now full 15k and later I add 25k for bootkit"); *id*. on January 1, 2013 (identifying purchase and test) ("I setup already . . . works perfect"); June 6, 2011 chat between bx1@jabber.org and g0dlike@jabber.org: ("[6/6/2011 10:21:16 AM] bx1: can u send me [6/6/2011 10:21:25 AM] bx1: Carberp"); *see* December 4, 2012 chat between teardrop@xmpp.jp and dejavu@thesecure.biz: ("(1:26:30 PM) dejavu@thesecure.biz/20253775191356662473691544: i purchased carberp"); http://krebsonsecurity.com/2013/06/carberp-code-leak-stokes-copycat-fears/ ("The source code for "Carberp" — a botnet creation kit coded by a team of at least two dozen hackers who used it to relieve banks of an estimated $250 million.").

[38] *See* December 4, 2012 chat between teardrop@xmpp.jp and dejavu@thesecure.biz.

noted that his ATS module worked with "Zeus/SpyEye/Ice9." *See* Exh. F attached hereto. The ATS module permits a cyber-criminal to steal money from a victim's bank account via an automated setting that quickly wires money from the victim account to a "drop" account, *i.e.*, an account set up by the cyber-criminal for the purpose of obtaining fraudulent proceeds, usually under the name of an alias. But the ATS program generates a fake screen on the victim's computer that conceals the amount of money in the bank holder's account. In other words, a quick check of one's bank account online might reveal that one has $1,000; but in reality, an ATS victim might have no money left at all because the cyber-criminal has stolen it.[39]

Multiple chats reveal that Bendelladj was using and selling his ATS software and targeting banks around the world in 2011. In February 2011, he targeted Malaysian banks.[40] In March 2011, he admitted to having an ATS that targeted HSBC in Australia and New Zealand.[41] That month, he purported to have

---

[39] *See,e.g.*, Automating Online Banking Fraud, Automatic Transfer System: The Latest Cybercrime Toolkit Feature, at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf.

[40] February 24, 2011 chat between bx1@jabber.org and mafioso@xmpp.jp:

bx1:	working on ATS
bx1:	Malaysian Banks
bx1:	:D
bx1:	Time to make
bx1:	$$$$

[41] March 23, 2011 chat between snas@jabber.ru and bx1@jabber.org:

snas@jabber.ru:	your ATS
snas@jabber.ru:	what bank you have?
bx1:	HSBC
bx1:	ING
bx1:	ANZ

"millions of drops," or bank accounts that collected stolen money.[42] In May 2011, he conspired with another cyber-criminal to use bots and "drops" based in Italy to obtain the funds.[43] In a subsequent chat, he referred to his "drops" as "bitches" suggesting that he had subordinates located abroad who would cash out the stolen funds from Italian banks.[44] He acknowledged that ATS was working and copied

---

[42] March 16, 2011 chat between bx1@jabber.org and g0dlike@jabber.org:

bx1:	i just
bx1:	got ATS
bx1:	HSBC
bx1:	i wanna make
bx1:	some $$$
. . .	
bx1:	i got millions
bx1:	of drops

[43] May 12, 2011 chat between bx1@jabber.org and g0dlike@jabber.org:

g0dlike:	if u get ats tell me i will go 5050 with u
g0dlike:	this guy can make it in 2-3 days
bx1:	i waiting
bx1:	he said he can make
bx1:	for Unicreditbanca
bx1:	Italy
bx1:	and i got many drops
bx1:	and bots from IT

[44] May 13, 2011 chat between bx1@jabber.org and g0dlike@jabber.org:

g0dlike:	lets get europe ats's for sepa wires
g0dlike:	well go 5050 ?
bx1:	am here
bx1:	yes
bx1:	we can go 50/50
bx1:	for
bx1:	Unicredit
bx1:	u know
bx1:	its most used bank in italy
. . .	
g0dlike:	i dont know if i can get drops there i will chk first

and pasted records of his ATS thefts to a cyber-criminal named g0dlike.[45] In September 2011, he admitted to using his botnet for ATS fraud.[46]

In October 2011, he admitted to having lots of "drops" or places where he was wiring the ATS-stolen funds.[47] His sales continued through January 2012, and he claimed to sell ATS modules "very cheap."[48]

---

g0dlike:	and tell u
g0dlike:	by tomorrow
bx1:	hahaha
bx1:	nah
bx1:	i can get
bx1:	last 2 months
g0dlike:	oh
bx1:	i was in italy
g0dlike:	i transfer to urs ?
bx1:	did u remembers
bx1:	i got
bx1:	Bitches there

[45] March 2, 2011 chat between bx1@jabber.org and g0dlike@jabber.org:

bx1:	ATS
bx1:	working
bx1:	:d
bx1:	HSBC UK
bx1:	**[ACCOUNT DATA REDACTED]**

[46] September 26, 2011 chat between bx1@jabber.org and greatbeast2000@jabber.org:

bx1:	i sit home
bx1:	working on
bx1:	to get alot of bots
bx1:	for ATS

[47] October 7, 2011 chat between bx1@jabber.org and meboss@jabber.org:

bx1:	i want to make ATS
bx1:	for ANZ
bx1:	i want to work on local banks
bx1:	here i got alot of drops

In November 2012, He bragged about to yummba@limun.org about his ATS thefts. Using the handle "dejavu," Bendelladj wrote:

dejavu@thesecure.biz:	i have made my own ats
dejavu@thesecure.biz:	LOL
dejavu@thesecure.biz:	everytime
dejavu@thesecure.biz:	user login
dejavu@thesecure.biz:	it fuck his money hahaha
dejavu@thesecure.biz:	from 1 account
dejavu@thesecure.biz:	20 transfer
dejavu@thesecure.biz:	to same account
dejavu@thesecure.biz:	LOL

See November 29, 2012 chat between yummba@limun.org and dejavu@thesecure.biz. In December 2012, he admitted to cashing out $12,000,000 € that he stole from Bank of America. In a December 4, 2012 chat with teardrop@xmpp.jp, Bendelladj, using the handle dejavu@thesecure.biz, said "I have made my day cashouted 12 million euro . . . I preparing my luggage going to australia." He further notes:

dejavu@thesecure.biz:	i took
dejavu@thesecure.biz:	**12 million**
dejavu@thesecure.biz:	from cashproonline.bankofamerica.com.

---

[48] January 5, 2012 chat between snas@jabber.ru and bx1@jabber.org:

bx1:	if u need any bank ATS
bx1:	i sell very cheap

To that end, in the November 27, 2012 chat with yummba@limun.org, Bendelladj explains his cash-out method: "people here don't know what I do and I drive miles to collect cash and some other guys collect for me."

5. Bendelladj's theft of 200,000 credit cards.

In January 2013, FBI agents obtained a search warrant to search Bendelladj's laptop computers and hard drives. A forensic review of the equipment revealed a file named "Grabber.zip" that housed two additional files named 1.txt and 2.txt. PSR, at ¶ 65. Those files, which Bendelladj's hard drive directory showed to have been last modified on December 7, 2011, contained full credit card information including name, address, credit card number, card CVV, and other data belonging to 200,000 people around the world. PSR, at ¶¶ 64-66, 69. Records from American Express, Capitol One, JP Morgan Chase, Discover, USAA, TelComm, and Visa revealed that there was $3.25 million dollars' worth of attempted fraud on those accounts and $878,000 in sustained losses by credit card companies. PSR, at ¶ 65.

Bendelladj's private chats and posts on ww.darkode.com reveal that he stole the data from a printer ink cartridge company using his botnet. On December 3, 2011, Bendelladj advertised "AMEX + VISA + MASTER + DISCOVER" cards from "US/CANADA/UK/SOUTH AFRICA/EUROPE." PSR, at ¶ 48; *see also* Exhibit G.[49] On that same date, someone using the chat handle mrvalaci@jabber.ru sent

[49] Bendelladj's December 2011 post is similar to a May 4, 2011 post on www.darkode.com where he posted that "VCC Service is back online." *See* Exhibit H attached. The May 4, 2011 post noted that he "just want[ed] to notify all that the service is back online☺ and now I'm able to provide virtual cards." A user named "King" posts that Bendelladj (a.k.a. Bx1) provides "very good service" and "fast delivery."

Bendelladj (at bx1@jabber.org) a message that said "so basically you wanna sell the whole thing or partner up and make more $$?" Bendelladj acknowledged that "around 30k" or the cards were "expired."[50] But Bendelladj and mrvalaci proceeded to test various cards to determine whether the batch of stolen credit card data was usable. After performing the tests, mrvalaci noted that "ur base is good." After Bendelladj admitted that he stole the data from one company, he clarified that "i didn't hack it with SQL injection." Rather, Bendelladj wrote that he "hacked it with my Bot."

Bendelladj's June 20, 2012 chat with "g0dlike" confirms that he stole 200,000 "ccs" (credit cards) using his bot, that he sold the data to mrvalaci, that there was $3 million dollars in attempted losses, and that he "pwned" USA credit cards:

bx1:	Listen
bx1:	we start job
bx1:	i spam get u bots
bx1:	cashout
g0dlike:	but lets do partnership bro
bx1:	i make money

[50] Under the Guidelines, Bendelladj is responsible for even possessing "expired" access devices, whether they were used or not. *See* U.S.S.G. 2B1.1 Application Note 3(F)(i) ("In a case involving any unauthorized access device, loss . . . shall be not less than $500 per access device."). The Guidelines incorporate the definition of "unauthorized access device" used in Title 18, U.S.C. Section 1029(e). *See* § 1029(e)(3) (the term 'unauthorized access device' means any access device that is lost, stolen, **expired**, revoked, canceled, **or obtained with intent to defraud**[.]") (emphasis added) *cf. United States v. Gilmore*, 431 F. App'x 428, 430 (6th Cir. 2011) ("The plain language sets a floor for calculating the loss attributable to each device, namely $500; it does not limit loss calculations to devices actually used."); *United States v. Dodson*, 357 F. App'x 324, 325 (2d Cir. 2009) ("Such loss 'shall not be less than $500 per access device,' even in the absence of an actual loss.").

bx1:	:D
g0dlike:	on usa
bx1:	yae right
g0dlike:	we get one good server
g0dlike:	2 panels
g0dlike:	u know ?
bx1:	i told u
bx1:	last time u saw me
bx1:	hw much i pwned USA ccs
g0dlike:	usa ccs
g0dlike:	are shit
g0dlike:	lol
bx1:	nah
bx1:	200k
bx1:	ccs
g0dlike:	i can cash us token wires
g0dlike:	big money
bx1:	is not shit
bx1:	Mr Valaci
bx1:	made
bx1:	over 3 million
bx1:	from them
bx1:	and i sold them
bx1:	cheap to him

6. Bendelladj's theft of 200,000 credit cards constitutes "relevant conduct.

Under the U.S. Sentencing Guidelines, Bendelladj is responsible for "all acts and omissions . . . that occurred during the commission of the offense of conviction, in preparation for that offense, or in the course of attempting to avoid detection or responsibility for that offenses . . . **[and]** all acts and omissions . . . that were part of

the same course of conduct or common scheme or plan as the offense of conviction." U.S.S.G. § 1B1.3(a)(1) and (a)(2) (emphasis added).[51]

Bendelladj pled guilty to 23 different "offense[s] of conviction":

Count 1:	Conspiracy to commit wire and bank fraud, in violation of Title 18, United States Code, Section 1349;
Counts 2-11:	Wire fraud, in violation of Title 18, United States Code, Section 1343;
Count 12:	Conspiracy to commit three different types of computer fraud, in violation of Title 18, United States Code, Section 371;
Count 13:	Computer fraud in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 2; and
Count 14-23:	Computer fraud in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), and 2.

Doc. 35. Those offenses encompass conduct such as running botnets, infecting computers with malware, infecting computers for the purpose of stealing money, and conspiring with others to steal money through the use of botnets.

Bendelladj's PSR Objections suggest that he should only be responsible for "actual financial loss directly linked to the SpyEye intrusion into personal

[51] Here, Bendelladj engaged in "relevant conduct" that inflicted (and was intended to inflict) economic loss properly calculated under U.S.S.G. § 2B1.1. Therefore, U.S.S.G. § 1B1.3(a)(2) applies as such crimes "would require grouping." *See* U.S.S.G. 1B1.3(a)(2) ("(2) solely with respect to offenses of a character for which § 3D1.2(d) would require grouping of multiple counts, all acts and omissions described in subdivisions (1)(A) and (1)(B) above that were part of the same course of conduct or common scheme or plan as the offense of conviction"). For example, his possession of at least fifteen unauthorized access devices violates 18 U.S.C. § 1029(h) and groups with the wire fraud, bank fraud, and computer fraud charges. Bendelladj is also responsible for jointly undertaken activity that he embarked upon with Panin and others. *See* U.S.S.G. 1B1.3(a)(1)(B).

computers." *See* Bendelladj's PSR Objection, at ¶ 76.[52] Such a position is palpably inconsistent with the broad view of relevant conduct under the Guidelines.

In fact, Bendelladj is responsible for "all acts and omissions . . . that were part of the same course of conduct or common scheme or plan as the offense of conviction." U.S.S.G. § 1B1.3(a)(1) and (a)(2) (emphasis added). Such conduct includes other computer hacking activities designed to steal financial information such as a credit card data, whether Bendelladj used SpyEye, Zeus, Carberp, or any other malware. Part and parcel of that conduct is his efforts to monetize those thefts (*i.e.*, selling stolen credit card data, stealing from banks, and cashing the money out). Under the Guidelines, "[f]or two or more offenses to constitute part of a common scheme or plan, they must be substantially connected to each other by at least one common factor, such as common victims, common accomplices, common purpose, or similar modus operandi." U.S.S.G. § 1B1.3 cmt. 5(B)(i).[53] *See United States v. Siegelman*, 786 F.3d 1322, 1334 (11th Cir. 2015) (no clear error so long as offenses are "substantially connected" by one of the following: "common victims, common accomplices, common purpose, or similar *modus operandi*").

---

[52] Bendelladj appears to admit that he is responsible for the full scope of his conduct as it relates to promoting and spreading SpyEye, working with Panin to facilitate SpyEye's use amongst cyber-criminals, infecting computer users around the world with SpyEye, using SpyEye to steal personal and financial information, administering SpyEye botnets, and agreeing to use "spyware" to steal information. *See* Bendelladj's PSR Objection, at ¶ 76 ("The offense conduct centers on the insertion of a malware program called 'SpyEye'"); *See* Guilty Plea Hr'g Tr., at 21 (Mr. Strongwater: "Bendelladj would agree in principal that there was an agreement to install spyware in order to obtain information that he was not authorized to receive.").

[53] See U.S.S.G. § 1B1.3 cmt. 5(B)(i) provides (describing a "common scheme or plan" as encompassing a fraud scheme perpetrated by "computer manipulations").

Here, Bendelladj attacked common victims (financial institutions and their customers), his acts had a common purpose (to steal money from financial institutions and their customers), and a similar modus operandi (using infected computers as part of a botnet to obtain customer financial information).

Even if Bendelladj's theft of 200,000 credit cards were not part of a "common scheme or plan," such a theft would still be part of the "same course of conduct." *See* U.S.S.G. § 1B1.3 cmt. (B)(ii). Under the Guidelines:

> Offenses that do not qualify as part of a common scheme or plan may nonetheless qualify as part of the same course of conduct if they are sufficiently connected or related to each other as to warrant the conclusion that they are part of a single episode, spree, or ongoing series of offenses. Factors that are appropriate to the determination of whether offenses are sufficiently connected or related to each other to be considered as part of the same course of conduct include the degree of similarity of the offenses, the regularity (repetitions) of the offenses, and the time interval between the offenses.

U.S.S.G. § 1B1.3 cmt. (B)(ii).

Bendelladj does not dispute that one of SpyEye's core functions was to steal credit card information and banking login information from victims.[54] Moreover, because he has pled guilty, he cannot dispute that, for example, in February 2011, he "intentionally access[ed] a computer without authorization . . . to obtain information . . . for the purpose of private financial gain," and that his conduct

[54] *See* PSR, ¶ 32 ("SpyEye is a sophisticated malicious computer code designed to automate the theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information.").

impacted the computers identified in Counts 14 through 23 of the Superseding Indictment. Doc. 35 (referring to 18 §§ U.S.C. 1030(a)(2)(C) and 1030(c)(2)(B)(i)). He is therefore responsible for other ongoing series of offenses that he committed as late as 2012. At root, Bendelladj used botnets to steal banking and credit card data, and under the Guidelines he is responsible for all such conduct, including the theft of 200,000 credit cards. *See* U.S.S.G. 2B1.1 Application Note 3(F)(i) ("In a case involving any unauthorized access device, loss . . . shall be not less than $500 per access device.").

Just as a defendant convicted of being a felon-in-possession of a revolver on one date can be held responsible for the possession of a rifle on another date as "relevant conduct", *cf. United States v. Jones*, 367 F. App'x 109, 111-12 (11th Cir. 2010) ("Though the firearms were different types of weapons and were originally charged as separate offenses, we do not find the district court clearly erred.") (unpublished); *United States v. Barbour*, 191 F. App'x 471, 474 (7th Cir. 2006) ("As for the actual ten-month period at issue here, there is no support for his suggestion that it was clear error for the district court to count firearms possessed within that time frame.") (unpublished), Bendelladj is responsible for using a botnet to hack a business for the purpose of stealing 200,000 credit cards in December 2011, even though he was convicted of using a botnet in February 2011 to steal financial information from other computers.

This Circuit takes an "expansive view" of what constitutes relevant conduct. *United States v. Ignancio Munio*, 909 F.2d 436, 438 (11th Cir. 1990); id. at 439 ("conduct not contained in the indictment may be considered at sentencing"); *United States v. Behr*, 93 F.3d 764, 765 (11th Cir. 1996) ("This Court broadly

interprets the provisions of the relevant conduct guideline."). This Court can consider uncharged criminal conduct as a "relevant conduct." *See United States v. Scroggins*, 880 F.2d 1204, 1212 (11th Cir. 1989) (finding "relevant conduct" encompassed theft offenses to which the defendant did not plead guilty); *United States v. Alston*, 895 F.2d 1362, 1372 (11th Cir. 1990) ("The idea that a sentencing court may consider conduct not covered by the counts of conviction is neither new nor radical."). And it can also "consider criminal conduct that occurred outside of the statute of limitations period as relevant conduct for sentencing purposes." *Behr*, 93 F.3d at 766; *United States v. Hunter*, 323 F.3d 1314, 1319 (11th Cir. 2003) ("The limits of sentencing accountability are not coextensive with the scope of criminal liability.") (citing U.S.S.G. § 1B1.3).

In short, Bendelladj is responsible for a loss amount of at least $100,000,000 dollars (200,000 cards x $500). *See* U.S.S.G. 2B1.1 Application Note 3(F)(i) ("In a case involving any unauthorized access device, loss . . . shall be not less than $500 per access device.").[55]

7. Bendelladj's history and characteristics.

Bendelladj's chat messages reveal a rabid and frenetic drive to use botnets to

---

[55] Bendelladj is also responsible for the damage inflicted on victim computers all over the world. According to the Financial Services-Information Sharing and Analysis Center ("FS-"ISAC"), which counts thousands of banks as member institutions, the damage done to each personal computer infected with malware ranges from $75 (in human hours to remediate the computer) to $300 (for an individual consumer without an IT department that has to contact say, the Geek Squad). *See* Doc. 156, FS-ISAC Victim Impact Letter, at Attachment 1.

steal money from people all over the world. In one chat, he declares that he is "horny . . . to work" and that his job is "getting bots daily."[56] Other chats reveal a penchant for violence.[57] At various points, he has expressed contempt for Brian Krebs, the author of the "Krebs on Security," and claims that he has credit cards ("ccs") of Mr. Krebs's family and that Bendelladj will be "after him until he die."[58] He even suggests inflicting a Distributed Denial of Service[59] attack against Mr. Krebs.[60]

Moreover, the chats reveal that despite the fact that he worked with Panin to fuel the rise of SpyEye by vouching for him on forums such as "darkode," the two had an antagonistic relationship. Indeed, after Bendelladj "cracked" SpyEye and made it available to others without having to purchase it from Panin, the two had a falling out. In a January 21, 2011 chat between bx1@jabber.org and Jam3s@jabber.org, Bendelladj says:

---

[56] *See* December 21, 2012 chat between flowglike@jabber.ru and dejavu@thesecure.biz

[57] November 3, 2012 chat between illusionist@jabber.se and bx1@xmpp.jp ("I was arrested I was abt to kill some dude"); *id*. ("I shoot some asshole . . . they attacked me I had nada to do just to shoot"); March 25, 2012 chat between deja-vu@jabber.org and gramsey@verdammung.org ("when you catch him [Gribodemon] let me know so I hire a killer to kick his ass"); *see also* July 1, 2012 chat between illusionist@jabber.se and bx1@xmpp.jp ("man if he mess with me . . . he gonna be dead . . . even on his Russian city and in his own house am mad"); November 12, 2012 chat between meboss@jabber.org and bx1@xmpp.jp ("he ripped me already if I see him face t face I would kill him").

[58] *See also* December 23, 2011 chat between bx1@jabber.org and mafioso@xmpp.jp.

[59] "Distributed Denial of Service (DDoS) attacks" are attacks characterized by an explicit attempt by a malicious actor to shut down or "crash" a website (or other online service) by flooding the website with unwanted packets of information.

[60] *See* December 23, 2011 chat between bx1@jabber.org and mafioso@xmpp.jp ("bx1: wanna ddos bx1: krebs bx1: :D").

bx1: me an gonna fuck grib
bx1: :)
james: what
bx1: i gonna fuck gribo
bx1: lol
bx1: i will rape him

In a November 27, 2012 chat with yummba@limun.org, Bendelladj, using the handle dejavu@thesecure.biz, admitted to bribing local police officials to avoid detection.[61] He admits to hiding his assets from law enforcement,[62] and appeared to be able to wire fraudulent proceeds all over the world.[63]

Lastly, at various times, Bendelladj has suggested that he was merely a malware analyzer who worked for a security company, not a hacker. His private messages

---

[61] (dejavu@thesecure.biz: i got link dejavu@thesecure.biz: in local police dejavu@thesecure.biz: anything comes about me [. . .] dejavu@thesecure.biz: they tell me everything dejavu@thesecure.biz: and made for him dejavu@thesecure.biz: salary dejavu@thesecure.biz: 2k $).

[62] January 21, 2011 chat between bx1@jabber.org and Jam3s@jabber.org:
bx1: and i took all importrant stuff
bx1: to other apartment under my brother name and hide it
bx1: lol
bx1: i even transfeered founds to my mom and wife

[63] March 15, 2012 chat between westthug@jabber.org and bx1@swissjabber.org:
westthug@jabber.org: anywayZ bro, my main question is, can u wire 2k to poland bank accounts ?
bx1: i can wire anywhere in the world
bx1: even to INDIA
westthug@jabber.org: ok, and u charge 60% ?
bx1: DK member 50%

put the lie to this assertion.[64] In November 2012, he bluntly said: "if they pay me the whole money of the world . . . I wont work for security."[65]

Conclusion

Bendelladj is a prolific computer hacker who, over the course of just three years, systematically used sophisticated hacking techniques to infect hundreds of thousands of computers around the world with malware and to steal millions from unsuspecting victims. His sentence should reflect the magnitude of his conduct.

---

[64] November 29, 2012 chat between yummba@limun.org and dejavu@thesecure.biz.

[65] *Id.*; *see also* March 25, 2012 chat between bx1@jabber.org and g0dlike@jabber.org (in reference to Microsoft's accusation that bx1 is a SpyEye and Zeus user):

bx1:	they accuse me
bx1:	as user
bx1:	:D
g0dlike:	lol
g0dlike:	wow
bx1:	and i said i'm a malware analyzer
bx1:	i like to analyze things
bx1:	and i never used
g0dlike:	lol
g0dlike:	ok smart
bx1:	or purchased i get public
g0dlike:	and they left?
g0dlike:	how did they find u
bx1:	MSN
bx1:	because its Microsoft

See also March 25, 2012 chat between deja-vu@jabber.org and gramsey@verdammung.org ("i confirm that I've used SpyEye for Debug and Analyze Propose . . . i'm a malware analyzer and debugger and if you come to accuse me with certain things you will be responsible for your future").

Respectfully submitted,

JOHN A. HORN
United States Attorney

/s/KAMAL GHALI
Assistant United States Attorney
Georgia Bar No. 805055
kamal.ghali@usdoj.gov

/s/STEVEN D. GRIMBERG
Assistant United States Attorney
Georgia Bar No. 312144
steven.grimberg@usdoj.gov

600 U.S. Courthouse
75 Ted Turner Drive S.W.
Atlanta, GA 30303
(404) 581-6000 fax (404) 581-6181

Certificate of Service

I served this document today by filing it using the Court's CM/ECF system, which automatically notifies the parties and counsel of record.

Jay Strongwater

March 2, 2016

/s/ KAMAL GHALI
KAMAL GHALI
Assistant United States Attorney