iALERT White Paper

Ukrainian-Russian Hackers the Stealth Group and Its Leader, LovinGOD

By Jim Melnick, Director of Threat Intelligence
iDEFENSE Intelligence Operations
di@idefense.com

Aug. 13, 2002

iDEFENSE Inc.
14151 Newbrook Drive
Suite 100
Chantilly, VA 20151
Main: 703-961-1070
Fax: 703-961-1071
http://www.idefense.com

Copyright © 2002, iDEFENSE Inc.
"The Power of Intelligence" is trademarked by iDEFENSE Inc.
iDEFENSE and iALERT are Service Marks of iDEFENSE Inc.

TABLE OF CONTENTS

Copyright © 2002, iDEFENSE Inc.

EXECUTIVE SUMMARY

The Stealth Group has been described as "the most powerful group of virus-writers operating on the territory of the ex-USSR."[1] That claim has not been independently confirmed, but the group has created destructive viruses since 1994. Recently, the group has undergone an internal struggle, which is the subject of an extensive exposé published online in June 2002.

The head of the group, LovinGOD or LG, has reportedly expressed his great admiration for the Sept. 11 terrorist attacks against the US. This implied support of al Qaeda is very worrisome, given the possibility that Stealth could attempt to make its destructive viruses — and information on how best to launch them — available to al Qaeda supporters. Nothing suggests that such an action has occurred. Nevertheless, if the head of reportedly the "most powerful group of virus-writers" in the former Soviet Union chose to pursue an alliance with al Qaeda, this development should deeply concern governments and law enforcement personnel worldwide.

The online exposé, written by a former member of the Stealth Group known as TS, suggests that LG might be an informant of the Russian Federal Security Service.[2] But even if that is the case (and it is by no means confirmed), various layers of deception could be at work. Regardless of his ultimate motives, LG and any group he leads constitute a continuing threat as long as they are creating and distributing viruses.

[1] *Zanimatel'naya virusologiya, Chast' 3*. ("Interesting Virusology Part 3"). Accessed on Aug. 1, 2002, at http://drmad.chat.ru/virus3.htm.

[2] TS, the author of the exposé, said, "The history that LG told later provides indirect confirmations of my conjecture about LG's ties with the FSB" (Russian Federal Security Service).

Copyright © 2002, iDEFENSE Inc.

LovinGOD, Leader of the Stealth Group

A virus author called LovinGOD, aka LG, founded the Stealth Group of virus-writers. His real name is not known, but his choice of handle is suggestive of his anti-Christian opinions, according to his own explanation. One Russian assessment said that "practically nothing is known" about his personal background, what he is really called, or even how he looks.[3]

Personal Background

A search of materials reveals a number of details about LovinGOD. The following are details derived from those sources.

AGE

27 years old[4]

WORK BACKGROUND

LG worked as an "applied programmer" in 1999; his present employment, if any, is unknown. He claimed to live alone in 1999.

HOBBIES AND INTERESTS

LG likes to read the works of Steven King and Jack London. He is deeply interested in *chernukha* (Russian term for art or literature devoted to the negative or darker side of life). LG's favorite musical groups include Slayer, Sepultura and Kreator.

FORMER NAMES

According to his own account, LG's other former names include Slayer, LodeRunner, Russian Bear, One and Digital Karlos.[5]

PHILOSOPHIES

LG is very anarchistic and anti-social, described in one place as a "professional sadomasochist and fascist." He operates in tight hacker circles, claims to support terrorism and reportedly identifies with al Qaeda as "terrorist-colleagues."[6] LG said he is "absolutely indifferent to national interests." Despite his strong anti-societal attitudes, the recent exposé ponders whether LG might be an informant to the Russian Federal Security Service (FSB).[7] This interesting supposition remains unproven.

---

[3] *Zanimatel'naya virusologiya*, op. cit.
[4] In an interview in March 1999, LovinGOD said he was 24 years old, making him at least 27 in August 2002.
[5] These handles no longer appear to be used.
[6] iDEFENSE Intelligence Reports ID# 109814, June 12, 2002, and ID# 109900, June 17, 2002.
[7] TS exposé, op. cit.

Copyright © 2002, iDEFENSE Inc.

COMPUTER BACKGROUND

LG started out by learning Basic and Pascal programming languages. LG also knows C and Assembler languages, FoxPro and Visual Basic.

VIRUS AUTHORSHIP

LG claims authorship of the Tchechen family of viruses. He knows OneHalf and CIH viruses well. LG admires the Anarchy and MME.SSR viruses. The first virus of the Stealth organization was a destructive Maverick virus launched on Kiev-area bulletin board services in 1994.

ATTITUDE TOWARD ANTI-VIRUS SERVICES

LG is adamantly opposed to any anti-virus services or software. Any friendship with persons involved with anti-virus companies is grounds for expulsion from LG's hacker organization, the Stealth Group. In an article in one of his publications, *Infected Voice*, LG wrote about his attempts to overcome Anti-Virus Pro, the anti-virus application of the Russian anti-virus company Kaspersky Labs.[8] LG said he sometimes uses anti-virus applications to see how he can deceive them and also to search "for undesirable viruses" on his own PC. "Of course," he said, "I never pay for these commercial programs."

EDITOR OF E-ZINES

LG edits *Infected Voice/Kiev* and *Infected Moscow.* He claims authorship "of the first Russian electronic journal on viruses." LG said in 1999 that his programming employment left him with a great deal of time for pursuing his passion: writing destructive viruses. When asked what was his greatest achievement, he said that his "greatest achievement as a virus-maker would occur" in the future. He felt he had somewhat achieved his "goal of creating bands of cyberwarriors."

Authorship/View of Viruses and Other Malicious Code

The adulatory press copy on the Russian Civil Hackers' School describes LovinGOD as "the most famous specialist on computer viruses." While hardly the case, LG is very well known among hackers and would-be hackers in the former Soviet Union.

LG believes viruses are "similar to art forms." When asked which viruses of those he had authored was he most proud, LG replied, "The best known was the family of Tchechen viruses. I cannot say that I am proud of them. Certainly, I have more interesting projects, which need to be finished, but viruses from this family have been well distributed and contained good technologies and were original."

LG said that the names developed for his viruses are "accidental." "I don't like to think about such things as names…prior to when the virus is finished, since this…diverts attention from the algorithm. And I never sign viruses with my own name."

[8] *Infected Voice* #7.

Copyright © 2002, iDEFENSE Inc.

LG was also asked what groups and persons he most respected among malicious code authors. LG said, "From the time of the Morris worm, there has been nothing that I recall positively. As far as groups are concerned, the most professional one now is 29A."[9]

Based on his discussions with students at the Russian Civil Hackers' School, LG appears to have a strong technical knowledge of the OneHalf and CIH viruses. LG said he believes that virus creation will gradually move toward greater use of artificial intelligence (AI).

In a 1998 article, LG described virus-making: "It is a science on creating and using computer weaponry and combat machines in cyberspace, a creative process."

According to the 2002 exposé by insider TS, LG has wanted to "monopolize the entire virus-making scene with brute force!" LG was also reportedly the main force behind a Russian Convention of Association of Virus-Makers planned event. However, what this convention consisted of, and whether it has been held yet in 2002 or not, is still unclear.

Support for Terrorism

LovinGOD has openly stated his support for terrorism. In 1999 he stated: "I support terrorism and … make destructive things [viruses] in order to express my feelings toward a sick society." LG's support for terrorism has a strong anarchistic streak.[10]

LG has reportedly expressed very positive feelings toward Osama bin Laden and what he called his "terrorist-colleagues" who blew up the World Trade Center towers in New York and attacked the Pentagon on Sept. 11, 2001. LG said the al Qaeda terrorists are "working beautifully!"[11] No direct connection between Stealth and al Qaeda is known, but the threat Stealth Group and LG could pose if they put their virus-making skills at the service of al Qaeda is troubling.

[9] Several iDEFENSE Intelligence Reports on virus-authoring group 29A are available in at iALERT Web, https://ialert.idefense.com. Search on 29A.
[10] iDEFENSE Intelligence Report ID# 109814, June 12, 2002.
[11] iDEFENSE Intelligence Report ID# 109900, June 17, 2002.

Copyright © 2002, iDEFENSE Inc.

THE STEALTH GROUP

LovinGOD launched Stealth Group in September 1994 in Kiev, Ukraine, with a friend using the hacker name Crazy. The organization's "birthday" is Sept. 30. The exposé written by former insider TS claims the group has turned into a religious sect for LG's private benefit.[12]

Admission and Membership

- A prospective member of Stealth Group must be able to create a "viable, undetected virus, used on Windows 9x operating systems, with destructive capability and distributed by the author." Remaining candidates "can receive help but are not members" of the organization.
- Every prospective member must fill out an application form and will be rejected if he is not "an inhabitant of the cyberspace underground who stands out." He can also be rejected if he manifests any "pro-societal and/or anti-destructive views."
- Members must be anti-pacifist, anti-family values and anti-societal in their attitudes.

LG said in 1999 that the "virus scene" should not be large: "I see no more than 30 to 50 virus-makers in the entire world."[13] He did say he thinks the "virus scene" should be "more organized, like a mafia clan and better hidden from outside eyes." This is important, LG believes, in order to enhance the strike impact of viruses: "Now we see nothing like this — it is like a kindergarten — a disorganized crowd."

Structure

The group reportedly has members in Russia, Ukraine, Colombia and the US with ages ranging from 16 to 27. The largest number of members in Stealth resides in the Moscow area, according to a 1998 article.

KEY MEMBERS OR PERSONS ASSOCIATED WITH STEALTH GROUP[14]

- LovinGOD ("LG"), founder and leader
- Vovchik
- Gart (GurtHower)
- TS, author of June 2002 exposé on the group. "TS" stands for "Tovarishch Sadist" ("Comrade Sadist").
- Dirty Nazi
- SSR
- Reminder
- Zhengxi

[12] iDEFENSE Intelligence Report ID# 109785, June 10, 2002.
[13] Whether LG was speaking ideally or whether he believes there are actually only 30-50 competent virus authors in the world is unclear.
[14] This list is not all-inclusive but lists persons involved with LG or Stealth Group over the last couple of years based on the TS exposé of June 2002.

Copyright © 2002, iDEFENSE Inc.

- Radar
- Ryzhik (female), opposed to LG. She became involved in a long psychological struggle with him over what he was doing to members of Stealth Group. Her opposition appears to have eventually led to the partial break-up of the group sometime during 2001.

The Russian Civil Hackers' School

LG has served as an instructor at the Russian Civil Hackers' School.[15] LG seems to have been treated like a rock star by many would-be Russian hackers who adulated him.[16] One article said that when the young people saw LG, they "were in ecstasy" to see a "living author of [a series] of viruses…" LG played up the part as much as possible, showing up with a black hood with only slits for his eyes.

It is not known how long LG taught at the Russian Civil Hackers' School or what his current relationship is to leading hacker groups in Moscow. Although LG participated in the Civil Hackers' School, he apparently had issues with its name due to the word "civil" in its title. According to TS, LG uses the word "civil" ("tsivil") with utmost contempt. Someone who is a "tsivil" is "a square" or a conformist — just the opposite of the type of hacker lifestyle that LG and others associated with his worldview are trying to develop. The same is true of the Russian adjective "grazhdanskaya" ("civil") used in the name of the school itself. It indicates something that is part of "civil society," which is the very antithesis of the anti-social values taught by LG and his band of hackers. As such, why the school bore the name Russian Civil Hackers' School is open to debate. Perhaps it was just one more means for hackers to snub their noses at society.

Other participants at the school are more supportive of establishment yet want to have a foot in the hacker world. Appearing after LG at the 1999 presentation of candidates in Moscow for the Civil Hacker School was Andrei Mikhailovich Chepovskiy, who leads the Bauman University department on information security. In addressing the candidates, Chepovskiy did not dispute LG's characterization of virus-creation as an art form, but "suggested another variant — the secretive language of REFAL."[17] Using REFAL would provide an alternative means of pursuing a sort of art form, as opposed to creating viruses, Chepovskiy said.

The current status of the Civil Hackers' School is unknown. As far as can be determined, there have not been recent Internet postings about the school.

---

[15] One website of the school is at http://hscool.netclub.ru/exams/99/EE99.html.

[16] iDEFENSE Intelligence Report ID# 109790, June 10, 2002.

[17] REFAL, which stands for **RE**cursive **F**unctions **A**lgorithmic **L**anguage, is a computer language developed by Professor Valentin Turchin (Professor Emeritus of Computer Sciences, CUNY, and editorial board member of *Principia Cybernetica*). Turchin emigrated to the US from Russia in 1977. REFAL is described as a "language for processing XML documents." It is a *metalanguage* that is "a purely functional language based on pattern matching." It appears to be more or less concentrated among some computer science researchers in the former Soviet Union. More information on REFAL is available at http://www.refal.net/english/xmlref_1.htm.

Copyright © 2002, iDEFENSE Inc.

Photos of entrance exam from 1998 of Moscow Civil Hackers' School, where LG had great influence.

Infected Voice and Infected Moscow E-zines

Infected Voice and *Infected Moscow* are two virus-related e-zines founded by LG and the Stealth Group. The VX Heavens virus archive[18] described them as follows: "E-zines consisting of, among other things, virus-oriented assembly programming techniques, virus source codes, and a group application form."

[18] Located at http://vx.netlux.org.

Copyright © 2002, iDEFENSE Inc.

Old Website of Stealth Group (English version)[19]

[19] http://web.redline.ru/~one (the website has not been recently updated).

Copyright © 2002, iDEFENSE Inc.

HACKER SECT, CULT BEHAVIOR

Establishment of the LG Hacker Sect/Cult

LG created what amounts to the first hacker sect in the former Soviet Union, perhaps the first ever in the world, according to an article dated June 6, 2002, on the Xakep.ru Russian hacker website.[20] The article said that LG had turned his hackers into "zombies," used them as his slaves, and had them create viruses "to raise the authority of the group." The sect members also had to "work in the kitchen and clean toilets" and some sold or used money from apartments to raise money for the group. The Xakep.ru website contained a warning to readers: "Hacker, be careful of the [kind of] people you associate with; otherwise, you risk finding yourself in a sect!"

Various reactions were posted to this article. One reader named kaa said he "laughed for a long time." Someone named buggzy called Stealth a "totalitarian sect," while another respondent named CyberNeg denounced the article as "full of nonsense" and saw a possible conspiracy at work.

As for LG, CyberNeg said, "He is one of the most popular virus-makers in the former Soviet Union. If there is any group where everything is thrown into a fund and where they have their own leader, then even the government can call this a sect!"[21]

Exposing the Cult

TS, the author of the exposé on Stealth and LovinGOD, records the following conversation, which is an example of cult-like behavior by the leader of the group:

```
LG:   "You have not adjusted to life!"
TS:   "And why do you think you have the right to
      humiliate me?"
LG:   "I humiliate you for your own good. I am working
      with you in debug-mode. You are unstable…"
TS:   "Thanks, but I don't need such 'good'… When I find
      out where I can still blend in, I can leave."
LG:   "Well, and you can vanish psychologically; you will
      sink into strange obsessions! Without me you will
      not be able to live!"
```

TS said that he was regularly beaten by LG. He records one incident during which he was reportedly struck 30 times. This was followed by a threat: "If you don't submit, we will wring you by brute force." In spite of all this, TS stayed with the organization and later said he worked

[20] iDEFENSE Intelligence Report ID# 109785, June 10, 2002.
[21] Responses were posted June 7-10, 2002, on the xakep.ru website.

Copyright © 2002, iDEFENSE Inc.

on a polymorphic virus during some of this time. TS later left Kiev, where these events occurred, and relocated to Moscow.

At another time, Stealth member Gart suggested that the group adopt a ritual that he said was adapted from the Mayans. After a battle several men would cut themselves and drink each other's blood. LG immediately adopted the ritual for themselves and responded as follows:

```
LG:   "You understand, that this is binding … No one can
      be allowed to turn into a Philistine. Is everyone
      agreed on the conditions of the oath?"
Gart: "Well, if I turn into a Philistine, then it is only
      externally and only because it would be very
      advantageous to me…"
TS:   "And what is the harm in this…?"
Gart: "Well, everyone understands this…."
TS:   "Generally, I am agreed."
LG:   "If you break the oath – they will kill you."
```

At this point, the assembled group cut themselves, poured blood into a glass, added vodka, and drank to this oath, although to what they were agreeing is not exactly clear.

The TS exposé contains dozens of pages chronicling LG's paranoia and desire for maniacal control of his hacker organization. In a history that goes back to December 2001, TS describes a series of events within the group in which LG repeatedly tried to manipulate, cajole, deceive, beat, or use whatever means necessary to exert his absolute will over his group of virus-writers.

The relationships among members of Stealth Group deteriorated significantly over time. Death threats, mind games, backstabbing, and double-dealing abounded within a culture of psychological and emotional domination. TS allegedly tried to kill LG eventually — unsuccessfully. TS also developed suicidal tendencies.

Virus-Makers' Convention

Several postings on the Siberian Bears Virus Club (SBVC) website in early April 2002, refer to a so-called "Convention of the Association of Virus-Makers." The SBVC itself is a prominent and active club of malicious code authors.[22] Those who posted messages assumed that LovinGOD was the person behind the "virus-makers convention." One was not very complimentary: "This [*expletive deleted*] convention was written by LovinGOD, look, it's 100 percent him."[23]

It is clear from the TS exposé that the Stealth Group became deeply splintered internally. However, LG may now be in the process of regrouping his organization. TS closed his exposé by expressing concern over this idea. He said he hopes that there will not be a new group of "young virus-writers" that "LG will turn into zombies." He warned that LG may be "creating a new group by now."

[22] iDEFENSE Intelligence Report ID# 108291, March 27, 2002.
[23] According to a SBVC posting on the computer viruses forum from April 8, 2002.

Copyright © 2002, iDEFENSE Inc.

Copyright © 2002, iDEFENSE Inc.

FUTURE THREATS

The TS exposé demonstrates some of the dangers of this group. Although Stealth Group is currently splintered, LovinGOD appears capable of reorganizing the group, and he may already be in the process of doing so. A posting attributed to LG dated March 3, 2002, said the group has a new message board. He directed all questions to that board. He also urged all responders to use PGP encryption in communications to him.

Some handles of hackers and virus-makers communicating with Stealth Group and LG during the period of December 2001 to May 2002 include CreedHead, Skull, MeTrA, MYSTIQUE, philet0ast3r, cooluser, Max_Z, Qwazar, iKaR, X3, Naginata, Flash//DR, mogi, Art, Dolphin, and many others. A great number of these messages complimented LG on his organization and asked how to become a member.

If or when a reorganization occurs, the group may likely be compelled to publicly demonstrate its virus-making prowess in some way, especially to counter any impact of the TS exposé. A reconstituted Stealth Group would likely unleash one or more powerful destructive viruses at some unknown point in the future.

Most disturbing at present is LovinGOD's alleged tacit support of al Qaeda's terrorism (according to the TS exposé).[24] LG has reportedly referred to al Qaeda terrorists as his "terrorist-colleagues." While there is no direct proof of a tie between LG or Stealth Group and al Qaeda, LG's extreme anarchism and destructive nature might precipitate a move toward establishing contact with the terrorist group. On the other hand, care must be taken not to build too much on this premise without more evidence as this speculation is based entirely on an alleged statements presented by a disaffected former insider.

What Might This Mean for al Qaeda?

Nevertheless, the seriousness of the claim requires follow-up through to its logical end. A recent major article in the *Washington Post* discussed the possibility that al Qaeda operatives might be planning a future cyber attack on critical US infrastructure, including worrisome probes "routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan."[25] Whether al Qaeda has that capability or not, sympathetic hacker groups that *are* highly sophisticated — such as this one — could make their expertise and resources available to al Qaeda terrorists. Given that possibility, it is vitally important that the virus-making capabilities and contacts of the Stealth Group and any future group founded by LG be carefully assessed and monitored.

[24] iDEFENSE Intelligence Report ID #109900, June 17, 2002.
[25] Gellman, Barton. "Cyber Attacks by Al Qaeda Feared." *Washington Post*. June 26, 2002.

Copyright © 2002, iDEFENSE Inc.

ACKNOWLEDGEMENTS

Thanks to the following individuals for their efforts:

- Michael Cheek and Andrew Schmidt, iDEFENSE Inc.
- David Endler, iDEFENSE Inc.
- Mickey McCarter, Newspoint Inc.

Copyright © 2002, iDEFENSE Inc.

APPENDIX A: RUSSIAN VOCABULARY

kiberanarkhiya: Cyber anarchy

kiberfashizm: Cyber fascism

lamerstvo: The Russian word for being “lame” or promoting “lameness” in computer-related activity

polimorfika: A polymorphic virus

virmeiker: Russian slang for “virus-maker”

virusologiya: The study and development of computer viruses

Copyright © 2002, iDEFENSE Inc.

APPENDIX B: REFERENCES

- Climentieff, Constantin E. (aka DrMad). *Obxod rezidentnykh antivirusnykh monitorov pryamym obrashcheniyem k DOS*. ("Evading Resident Anti-Virus Monitors by Direct Transformation to DOS.") 1998. MoonBug 5. Available at http://www.ussr.to/Russia/drmad/antires.htm.
- Climentieff, Constantin E. (aka DrMad). *Zanimatel'naya virusologiya Chast' 3*. ("Interesting Virusology. Part 3.") Accessed on Aug. 1, 2002 at http://drmad.chat.ru/virus3.htm.
- "Entrance Examination." Russian Civil Hackers' School Website. 1999. Available at http://hscool.netclub.ru/exams/99/EE99.html.
- Gellman, Barton. "Cyber Attacks by Al Qaeda Feared." *Washington Post.* June 26, 2002. Available at http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html.
- *Infected Voice* and *Infected Moscow.* Virus e-zines. 1999-2002. Available at http://vx.netlux.org/dat/zi01.shtml. (*Infected Voice* #15, posted December 2000, appears to be the last issue.)
- "Interview of LovinGOD for TI#1 e-zine." March 20, 1999. Available at http://vx.netlux.org/texts/html/rus/i/lg1.html.
- Siberian Bears Virus Club. "Convention of the Association of Virus Makers." April 2002. Available at http://sbvc.host.sk/forum2/threads/90.php.
- "Stealth." Hackworld 2001. Oct. 28, 1998. Available at http://hackworld2001.narod.ru/stealth.html. (LovinGOD appears to be the author of this assessment.)
- Stealth Group Website (Old). May 2000. Available at http://web.redline.ru/~one/rnp.htm.
- Stealth Group, New Guestbook Entries. July 26, 2002. Available at http://mercury.beseen.com/guestbook/r/180266/guestbook.html.
- TS. "True Face of Evil: Real History, Real Dirt…" (Exposé on LovinGOD and Stealth Group). June 3, 2002. Available at http://xaoc.void.ru/ctcp/lg.txt.
- Xakep.ru. *Na Ukraine est' komp'yuternaya sekta.* ("In Ukraine There Is a Computer Sect.") June 6, 2002. Available at http://www.xakep.ru/post/15462/default.htm.

Copyright © 2002, iDEFENSE Inc.