Identifying, Exploring, and Predicting Threats in the Russian Hacker Community

Dr. Thomas J. Holt

Michigan State University
holtt@msu.edu

Dr. Max Kilger, Spartan Devils Honeynet Project
Dr. Deborah Strumsky, UNC-Charlotte
Dr. Olga Smirnova, Eastern Carolina University

Malware and Hacking

- The problem of malware and computer based theft is increasing and becoming more complex
  - The number of unique keyloggers and malware identified by the apwg have increased during 2008
  - CSI/FBI reports that businesses lost over $21 million due to fraud, as well as over $10 million due to various malicious software infections
  - The Department of Justice argues that it is now more profitable to engage in computer crime than drug trafficking

Criminological Research

- Social science research has explored the malware and hacking community to some degree
  - Hackers and malware writers operate within a technology focused subculture that values skill and ability
  - They have relatively loose connections, and sometimes work in teams to create programs or hack systems
- Few systematic examinations of the malware and hacker community have examined social ties and interests
  - Generally no predictive research has been conducted

On-line Resources

- The malware and hacking community utilize on-line resources that can be actively mined for information

- This study will examine the social networks of the malware and hacking community in Russia and Eastern Europe using data generated from social networking blogs
  - Blogs provide important information on:
    - Current and emerging threats
    - The relationships and behavior of attackers
    - Locations, attitudes, beliefs

Self-Report Information

- Each LJ profile allows users to provide information on their:
  - Location
  - Education
  - Biographies sometimes provide useful information on psychological status of the user or whether the journal is friends-only
  - Interests can include political affiliation, geographical location as well as nonsense
  - Friends
    - people whom the users reads and who can have access to ‘friends-only’ entries
  - Also friend of
    - people who read this journal and do not have access to protected entries
  - Mutual friends
    - both users added each other
  - Communities
    - LJ groups that the individual belongs to

Data and Methods

- This study uses a sample of the members of multiple hacker groups that have connected forums known to sell and trade malicious software and stolen data
  - The content of each blog was downloaded and translated by a native speaker
  - Google searching was conducted for each individual to determine their involvement in the hacker community
  - Network analyses were conducted to indicate the centrality of users with high perceived threat level

Membership

Risk Levels By Group					
	0	1	2	3	Total
BH	154	12	34	8	208
CU	24	2	4	2	32
DL	30	8	8	8	54
HN	0	0	0	4	4
HZ	180	12	38	4	234
MF	16	0	8	4	28
RU	10	0	4	4	18
Total	414	34	96	34	578

Extrapolating Data: Location

- Location
  - From current educational listing
  - From ICQ profile or other online contact information
  - From communities – if the user belongs to the communities devoted to finding jobs in particular location
  - From Interests – the user can indicate heightened interests to the particular location
  - Each of these categories is further corroborated by reading the journal entries

Extrapolating Data: Age

- Age
  - Education
    - Assuming the standard Russian educational trajectory, we can assign the age with some margin of error
  - ICQ profiles
  - Journal entries
    - users are congratulated on their birthdays, especially for ages 18-20

Extrapolating Data: Threat

- Threat scores were created and assigned based on:
- Results from google searches on the handle provided
  - 0: no threat
  - 1: computer security blogger
  - 2: low level hacker
  - 3: high level hacker

General Details

- 70% of users with very low perceived risk
- 13% of users did not provide physical locations in profiles
- 6% of users provided locations that do not exist
- 15% friends-only profiles
- **7 females**
- **3 virtual identities**

Example of age identification

- Zdeusz:
  - graduated from high-school in 2002;
  - studied at the university in 2003-2008;
  - he has spent one year somewhere (working or preparing to study in the university).
  - assuming that he has graduated from school as majority of Russians at 16, studied 5 years at the university, then this puts him at 22 years or 1986.

General Educational Information

- About 14% are currently students
- The universities with several representatives studying together:
  - 6 at Scientific Research Institute of Sorcery and Wizardy (NIIFAQ), Solvets, Murmanskaya oblast, Russian Federation (most favorite fake location)
  - 5 at Lomonosov Moscow State University
  - 5 at National Research Nuclear University (Moscow)
  - 4 at Moscow State Technical University n.a. N.E. Bauman (MSTU)
- The typology of schools can be classified as following:
  - At least 7 users study at various schools with language affiliations
  - 3 computer specialists, 3 engineers, 7 mathematics, 6 physics, and 32 study at various polytechnic and technical schools

Location

- The regional distribution is skewed to two prime cities:
  - 31% Moscow
  - 11% St. Petersburg
  - 5% Novosibirsk
  - 53% Other cities
    - Russian Federation (52%), Ukraine* (6%) Unable to locate 30% of users

Geographical distribution of hackers vs. Russian online communities

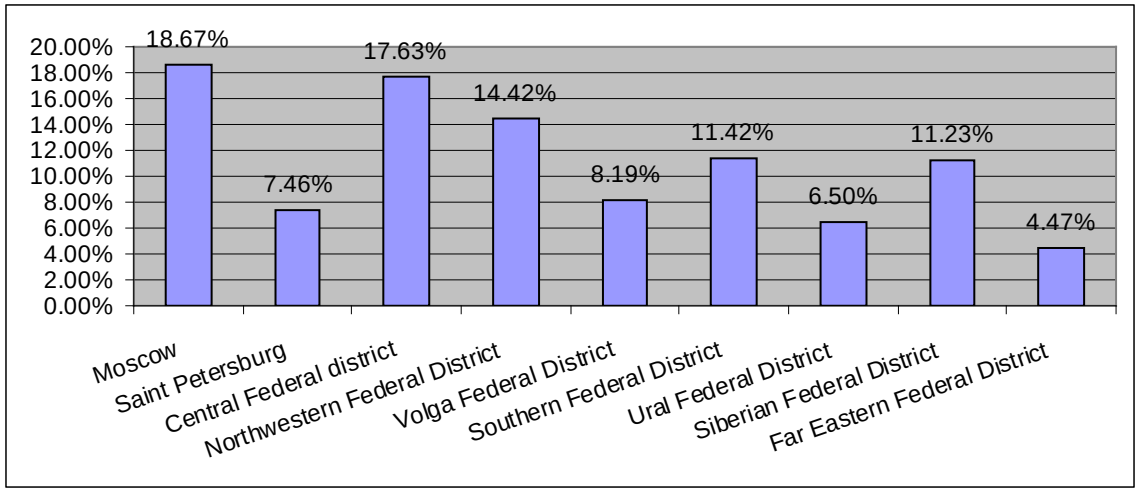
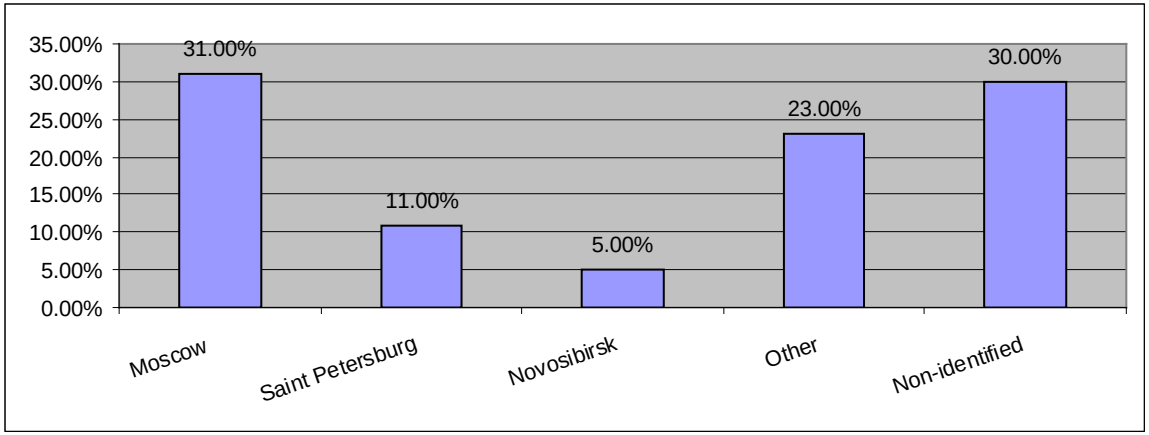
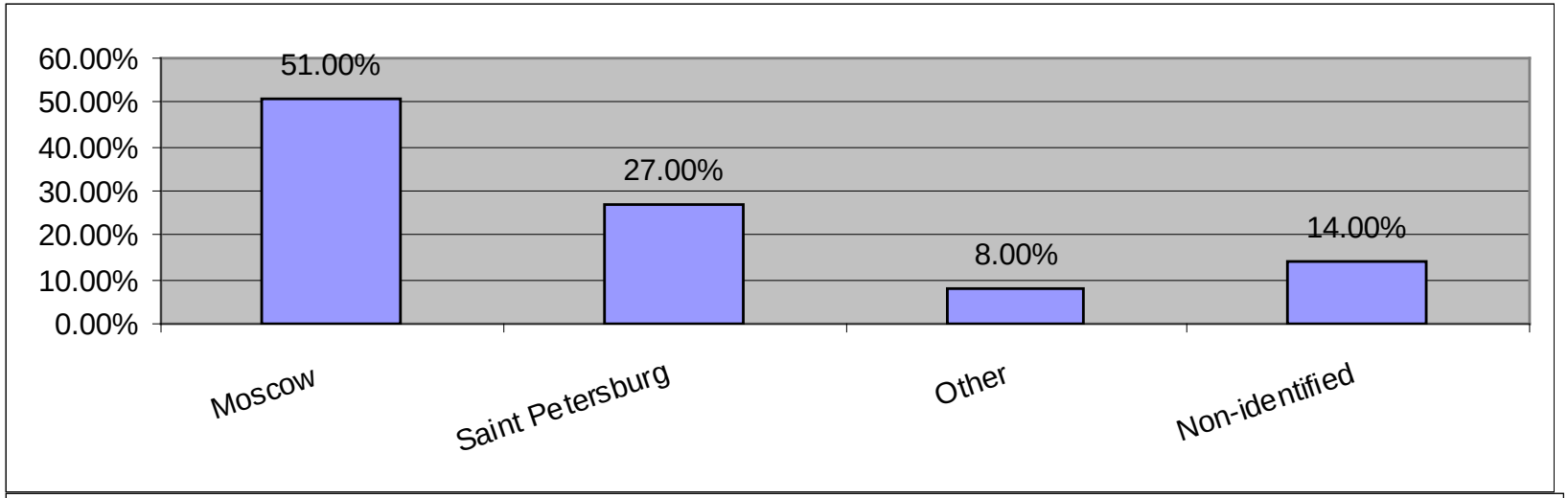


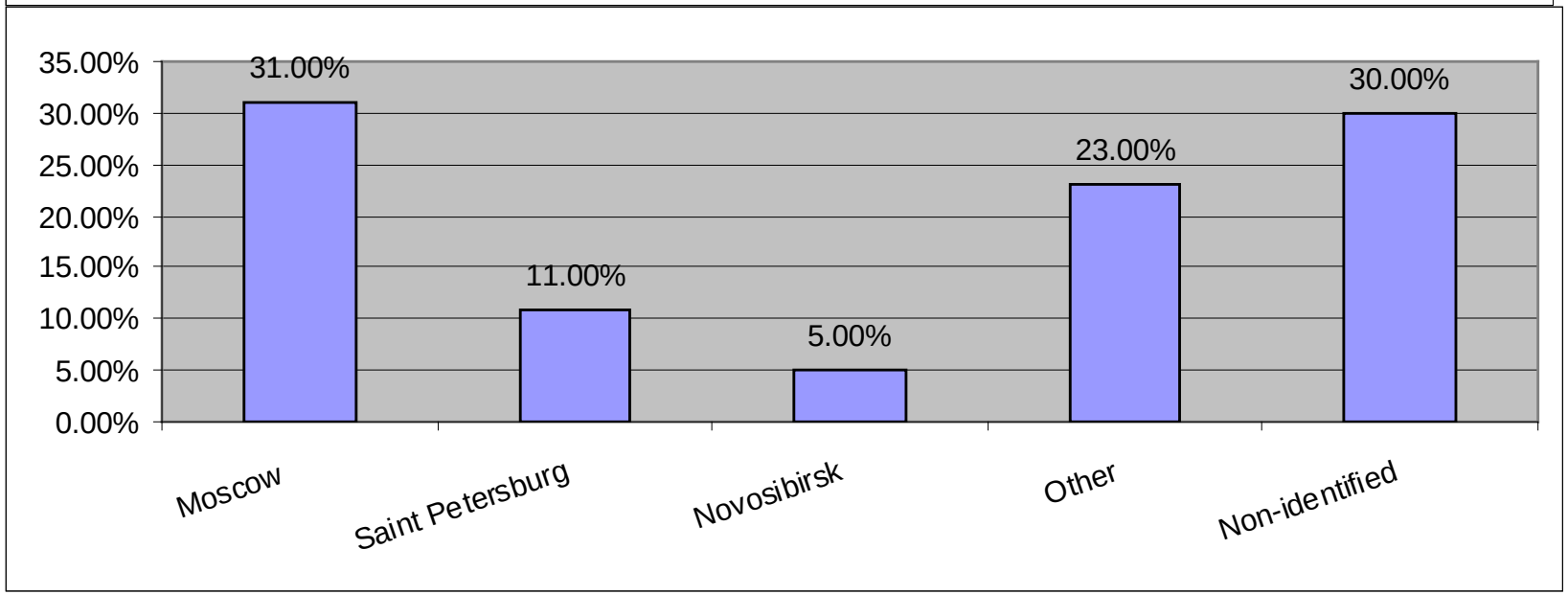
Figure 5 . Geographic distribution of RUnet users.
Source: Solovyeva presentation



Geographic distribution of hackers

Our selection compared with the other hacker conferences





Examples of Location identification

- The most extreme
  - nait-n8 indicates that lives in ValueTown, Zimbabwe and speaks only Albanian
  - arkanoid indicates that his location St.Peteresburg/Moscow which is supported by his entries where he looks for a ride to Saint Petersburg for weekend. He works in Moscow and studies in Saint Petersburg.
  - gayrabbit studied on Cuba, Lithuania, and Tashkent
- The most common – Moscow, Saint Petersburg
- Total unknown
  - About 30%
- Fake locations:
  - “Scientific Research Institute of Sorcery and Wizardry" in Solovets, Murmanskaya oblast‘ (a fictional institution from Strugatskie' book “Monday starts on Saturday”)
  - Hogwarts
- County Locations:
  - 59% indicates that live in Russian Federation
  - 6.6% in Ukraine
  - 1.6% in Belarus
  - 1.3% in Germany

Gender and Virtual Identities

- Examples of females – represent a very small subset of hacker's community, but with the very high degree of diversity. For example,
  - bubnilkin – describes her everyday life
  - kiote-the-one – the journal is called 'serial maniacs' and subscribed to communities devoted to studying serial maniacs, the content is about computer programming (but writes from a female 'podumalA')
  - 13-ya – has a twin sister and uses her diary for communication with friends
- Examples of virtual identities
  - Mrbuggers – gender is listed as female in ICQ profiles, shown everywhere else as male, does not provide identification information in his LJ profile. One of co-founders of BH crew.
  - perajok - the journal is from We not I (somebody and Irena Ponaroshku which translates as Irena Pretending, mostly devoted to music)

Gender and Virtual Identities

Only one high threat female was identified, eas7. She was well connected to many males in the network

WowShell -Remote Shell access program

Netme ^_^- Portmap daemon or service application.

GOSS ^_^- GUI Oracle Security Scanner.

sTask ^_^- Console Service Task Manager/rootkit

Https ^_^- HTTPS - Console http/https downloader.

COSS ^_^- COSS - Console Oracle Security Scanner.

Rootkity ^_^ - Rootkits hidden ports checker.

GUI6011 ^_^- GUI Interface v.1.1.77 for Project6011.

GUI6011 ^_^- network scanner

Memories:: 4 entries

Pictures: fewer than 10 public

Interests: **107:** borland, crack, debug, delphi, exploits, kernels, lesbi, linux, phreak, tasm, unix, water, winnt, ø, anecdotes, anime, scents, pancakes, reciprocity, east, guitar, mountains, mushrooms, walk, money, jam, design, home, friends, zhasminovy tea, greens, winter, dating, invent, caviar, Internet, Arts, History, kamchatka, cafes, cinemas, clubs, computers, cosmetics, coffee, cats, beauty, cooking, wood , Love, medicine, views RRTIMETABLE, fashion, sea, ice cream, moscow, music, sky, tenderness, night, adored, communication, autumn, parachutes, paris, plush bears, beaches, kiss, the tide, nature, psychology, travel, Work, roses, with + +, salads, sahalin, sex, family, network, blue, sweet, juice, sun, sports, style, passion, dancing, morning, fantasy, fiction, fenki, philosophy, movies, felt-tip pen, photo, khaki flowers, tea, chat rooms, sense, champagne, shmotki, chocolate, shopping, japan

Schools: *None listed*

Friends: **521:** View Friends.

Mutual Friends: **403:** **013_van_gog_013,** 01922, 0x0badf00d, 1st_ist, 21karon12, 314159265, 357r1, 3v0luti0n, __jester, _aleksej_, _ashtray_boy_, _bublik_, _marinus_, _n_i_k_, _na_e_dine_, _prometey, _rus2, _zen_it, a1isa, abyss_amph, ach_yhrm, adagio0fwinter, aeriman, afx237_v7, aqneta, akeepaki, akunamatata_ser, al1us, alaniel, alexanderbelov, alexblues, alexeydream, alexxx5, alice_takes, alloff21, andregt, andrej, andrew_belkin, aneksiy, anisiy1981, annushka14, antianisiy, arkanoid, artnick, aruslan, atarix, atfakep, avissin, badnight, bansheezm, bayukov, beched, beezzin, besopodobniy, black_n, boltoon, bonyfacio, boyancheg, burus, bzmrnkt, c0rw1n_datatype, c_alien, casufi, celaz, chaos_code, cheshirabit, chtoosha, chuv1, clbq, click0, codera, cr4sh_0x48k, crazyblondorama, crisisofsilence, cuba_stars, cybeast, cyber_lyric, cyberii, d0xt0r, da_forever, daark_moon, danila_bas, dark_lawyer, dask_net, deep_shaft, dema, derzelle, desruptor, devilos, dgfopad, die_tinte, diksi_, ding_0, disnider, diver, diver_ice, dmitrief, dom_vetra, doubletail, dphq, dr_schmulge, drtr0jan, duke_66rus, dyke_grrl, eag1e, ebanat_kaliya, ebanyipatefon, eithe, ekzistencia, electrohippy, elochkina, elw, emotion_blog, energy_csdx, exitusletaris, familiarity, faye_t, fdoml, festa2007, foriss, freeatnet, freetiger, frixyfran, g3w, gangstasnob, gexxx, ghost_gfxer, ghost_tport, girlschoice, gizmal, glamour_scrap_e, gr3a7, grey_kosh, grif_51, grinders, gt_x, h_hocob, harridan_ly, hellgas, hid, hipoth, hitm4n, hobbit_sun, hromoj, humpty_dumpty, hun7er, i0ngunn3r, i_mry, ice_3000, icqjcnet, idispatch, ilya_samartsev, impr3za, in73r, indeyets, indrik, inf_loa_d, inojmax, insa, iren_myau, iret, itoitocs, itsnotaboutlife, ivlad, janadark, jane_baikal, jerom, jullie, kamarado, kapitern, karnabi, katzpaws, keir_ru, keyptor, killerloo, kiote_the_one, knesya, kolloid, komuna, konsull, koshkofil, koteno4ka, kroshkenstein, kukowa, kvapp, kz_clickf1, l0rda, l33thax0r, lady_charmed, lady_noname, lan_dao, latex_pony, lazycat83, leadmd, lich_ona, ligalizovana, light_guess, lightop, liks_cryptor, lil0k, linoosik, lis_kiss_kiss, liudmyla, lllllll, lo_stregone, loginex, luba_wow, luchcho, lui_abappel, lwen, m104, m3tr0, m_s_m, madkoder, maeror, maesh, maleskiller, malta_69, manyperson, marcell_skyout, maristamina, marixaru, marmeladka_t, martyn_na, masha_lis, mata, matex, matholimp, mavenka, mcdermott_photo, mclap, melkiy_poc, michael25, mihsol, misha, mishok, money4you, moodperson, moonofnovember, morkoff191, mpak_, mrdruid, mt6561, mutogen, n0xi0uzz, n1troza, naftoly_litman, naigovan, ncd0, nemox, neon_lenz, nerezus, net_f0x, netstrelka, netwind, newpsheniy, ni_ten_ichi_ryu, nikolavna, nixxl, nob, nord_soul, nozx, nponeccop, nq_skrju, nsimakova, ny3o, o_cash_o, off_base, old_lis, oldayn, oldmann, olympp, onave, oopstranslation, orbit87, ottenki_serogo, out_rage, oversider_kosma, paflenta2, paqing, pashix, pavlik81, pegasd, pepsin, perebor, peredozo, pereiks, perepiolkina, perlbot, ph3onix, photo_world, pierre_aronax, pigh, poputchik_ru, porosenok_petr, postmonition, privac, prkrust, pseudoart, qwe13, r1zn, rabb_it, radio_radar, radisniy, raspizdyaika, reac7i0n, realloc, rebel_ken, red_buttons, redodepts, reeves11, resv, ria_designer, romashov, roobish, rstghc, ru_line_up, rubinrot, s0larst0ne, samkin, sappfire, sasha_belka, seawoter, shados, shamany, shared_lj, sharpc, shnur0vka, shoppingzone, sidepocket_pro, sirena_evklad, sladkoewka, slonny, smirnovsirozha, smit, snaych, solovets_denis, sonorka, sportloto80, spott, srpspb, sruji, st_shtuchka, stable, stden, t1mreh, taibolinskaia, taka2001, tamagoch, tematic, terminalhead, texno_kot, theodorm, third_lag, thunderdomebaby, tigercup, top_photos, toxa, trak_shell, transistance, trasheng, trashhka, tsw, tutux, u4n, ufonaut, unatine, unkled, unpersonlich, upo, vadim88, veronika_7, vika_sk, visir, voronin, vospitatelnica, vv_olf, vybirayluchshee, webster89, why_g, windowoz, wokoladnaya, x0man, xatkaru, xblp, xdiman, xsaper, yaichnica, yama1, yo_sh, yo_she, yuzvir, z_zelenka, zarifulin, zarincheg, zhenyat, zhoker, zloiuser, zlokk, zoid_hero, zotrix, zxfun, zzfi

Also Friend of: **2:** **000_xyemb,** glamouressa

Member of: **87:** **_hot_lips_,** _urban_photos, ad_fake, alt_girl_love, androgyny_ru, art_by_girls, bad_girlzzz, bce_obo_bcem, beauty_news, bestphotos, blackcats, bmx_photo, cc6, clubmusic, clubnews_ru, complexxx, cow_head_brand, devki_ekonomyat, devki_v_shope, dyke_photo, elektroradio, fashion_ideas, fashion_punk, flash_pc, hack_n_phreak, hackzona_ru, hochu_muzh4inu, iva_nova_band, iwy_model, kosmetichka, krugom_torchki, linuxnews_ru, lookatme_msk, motologia, na_pozitive, nanedele, net_doma, oracle_dba, otdamsya_darom, paidmembers, photo_art_ru, phreakers, pickmybest, pink_shik, polunochnik, rastaman_ru, ru_biketrials, ru_bluejacker, ru_bmx, ru_book, ru_books, ru_drugs, ru_fem, ru_freelance, ru_girls_hack, ru_glamour, ru_hack, ru_hacker, ru_hair, ru_ljabber, ru_makeup, ru_manicure, ru_model, ru_nethack, ru_openbsd, ru_philosophy, ru_pinky, ru_root, ru_sell_things, ru_sql, ru_swine, ru_taxi, ru_tshirt, ru_tutor, ru_utena, ru_whacking, ru_women, shame_les, shopping_msk, sleepers, stavropol, unixgirlonly, unixparty, vmeste_na_diete, vuln_dev, womenintech, wow_people

Account type: Plus Account

Date created: 2004-08-19 09:58:21

Date updated: 2008-07-10 12:09:29, *3 days ago*

Examples of identities which appear to be real people

- There is a small percentage of people who do not hide their real identities, but us Livejournal and Internet for professional or communal connections:
  - puzanov (Puzanov) is a radio host who gives ads for his new radio programs
    - Puzanov can be his last name or nickname
  - stden (Denis Stepulyonok) discusses educational programs at the institution where he works
    - He teaches computer security

BH Crew example

- BHCREW is the separate profile (from BH community) for founders (or the founder) or BH crew. BH stands for Bugger-Hukker Crew.
- One of the latest visible entries in the BH crew community indicates that the community is seeking information on a computer security specialist
  - This might be an example of hackers attack or control marker
- Use their own language and have their own manifesto:
  - “The plans of BHC are simple and trivial like hangover: produce REVOLUTION. Buggers will be the president, Hukkers will be the prime-minister, well and there, *hwat* else is there, everybody gets free coca-cola, golden roller-blades, *freebie* Internet too, and *that's all*!”

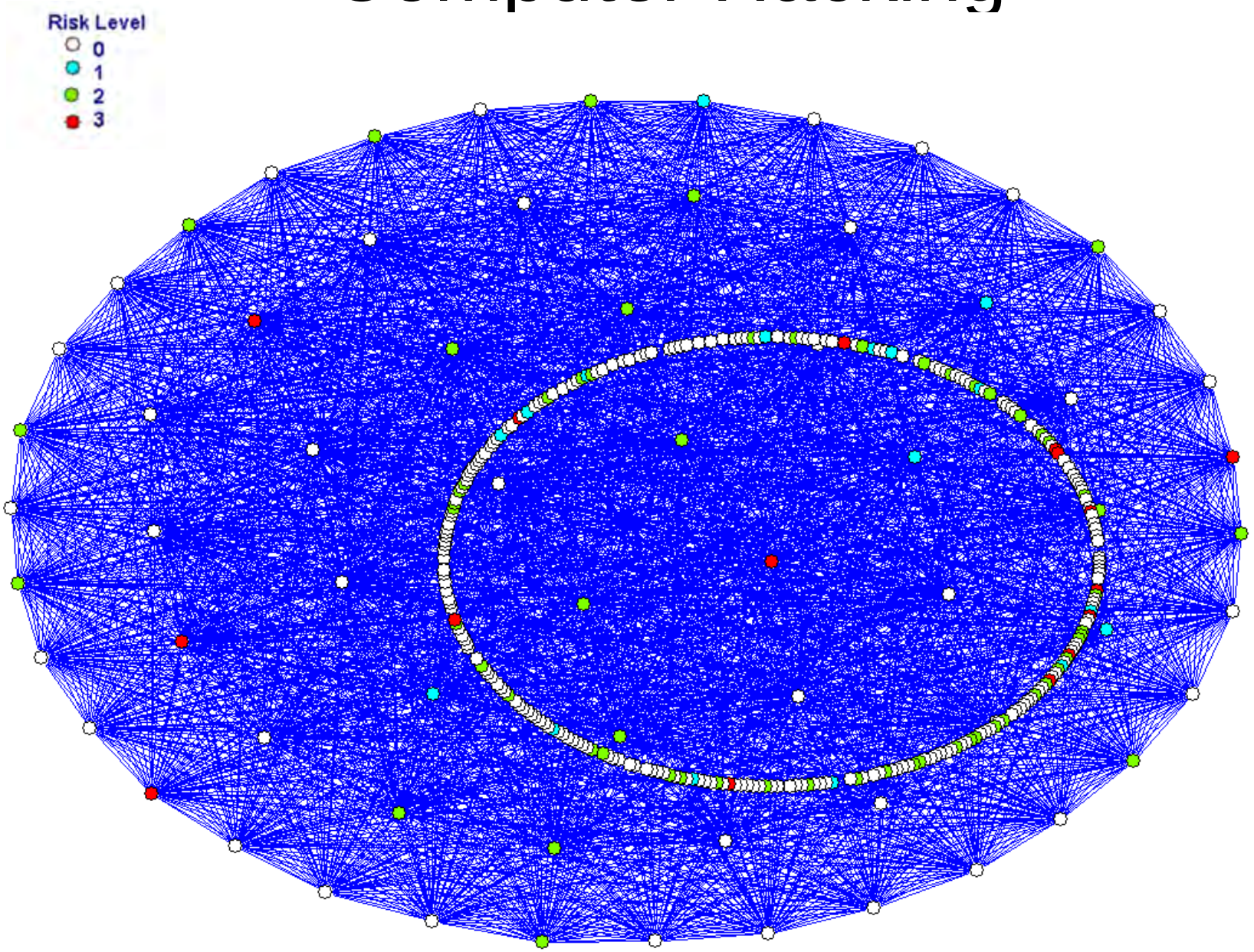
Examples of other uses of journals

- diaries
  - bubnilkin
- accessory to work
  - bukva_b asks different surveys-questionnaires
- collection of materials found in the Internet
  - cyberozzman
- Communication means
  - BH crew/ other hacker communities
- medium for distributing important information
  - BH_crew – posting news about group activities
- mass media type journals with large number of very popular for reading entries

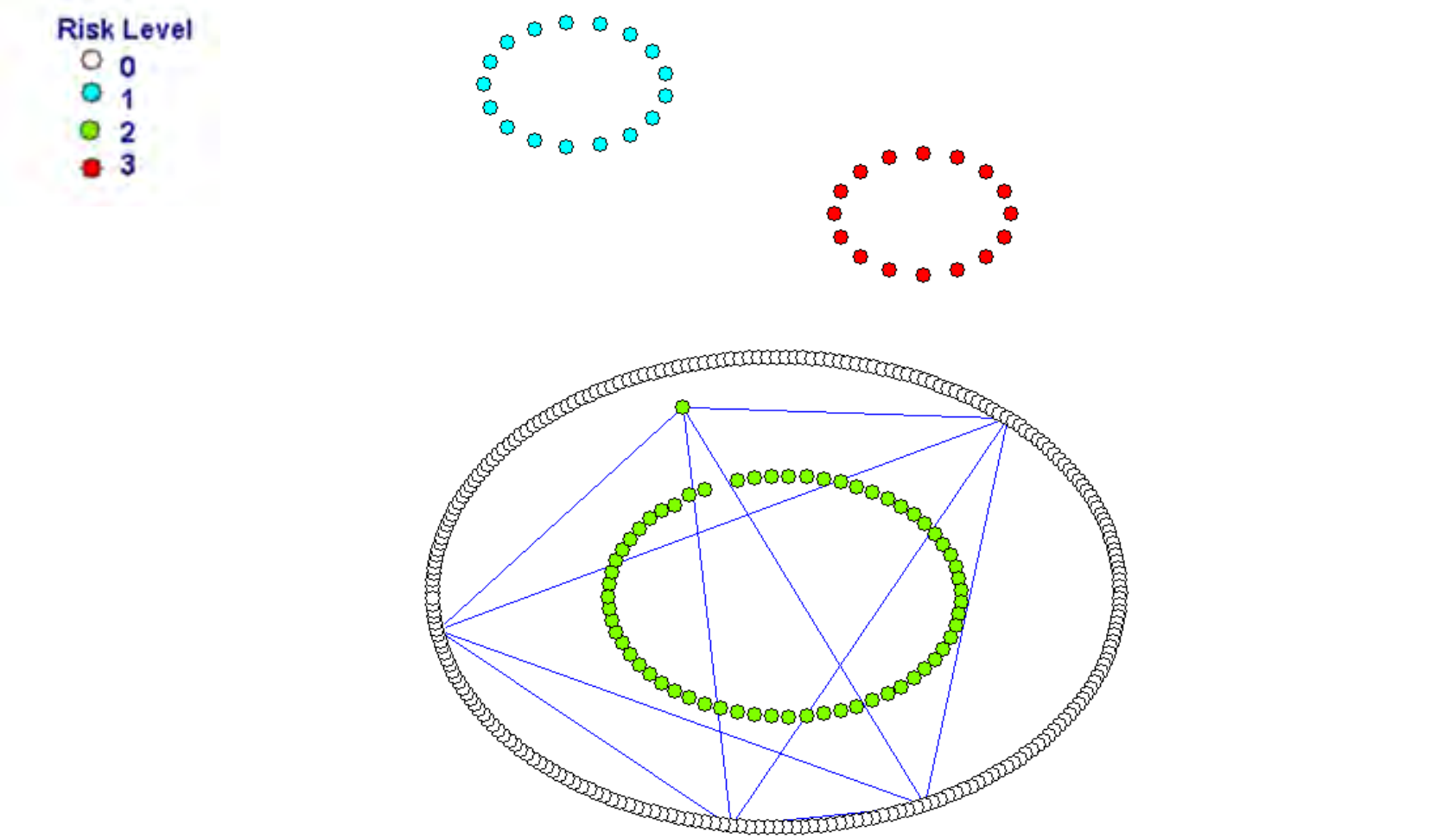
Depression and Affect

- Heightened levels of depression and aggression are noted in user blogs, as well as deviant behavior in general
  - lisnake posted in an online photo-resource under the title: “The Perfect Day for Suicide”
  - Crash’s blog titled “My Aimless Life”
  - 4kella indicates that he wants to commit suicide, and receives the comment: “The suicide is for weak – you have to leave”

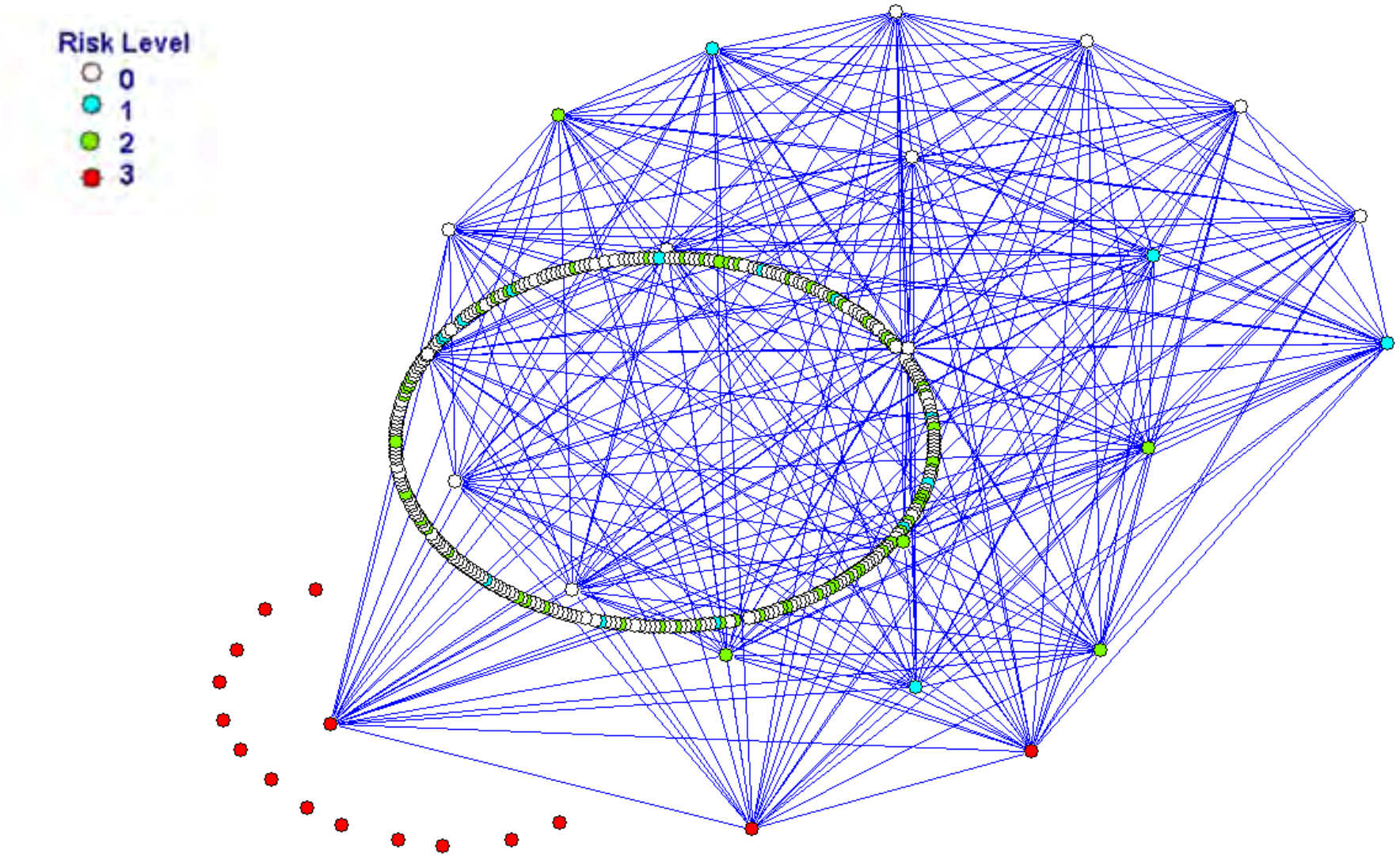
Computer Hacking



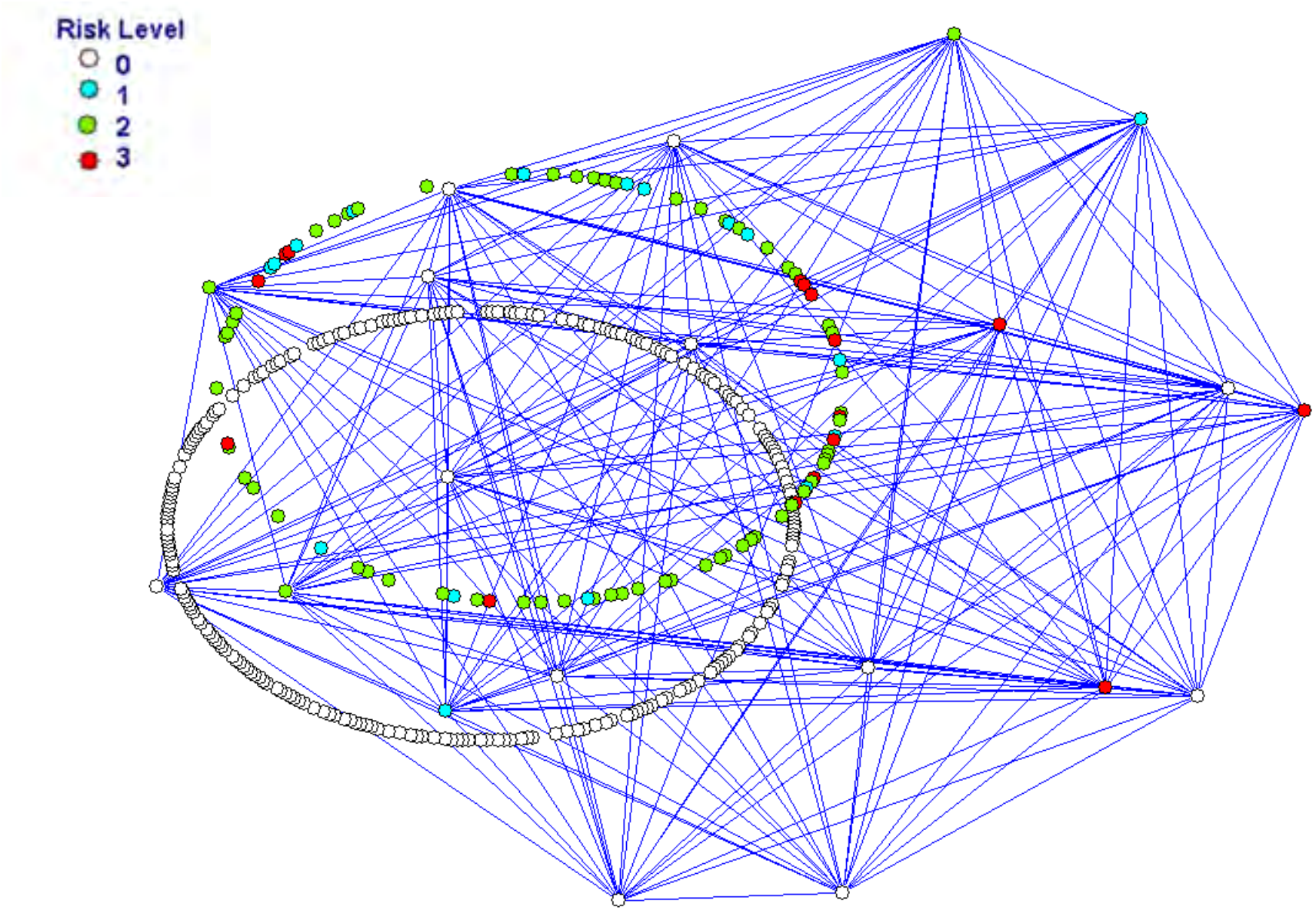
ASSEMBLY/HIGH LEVEL PROGRAMMING



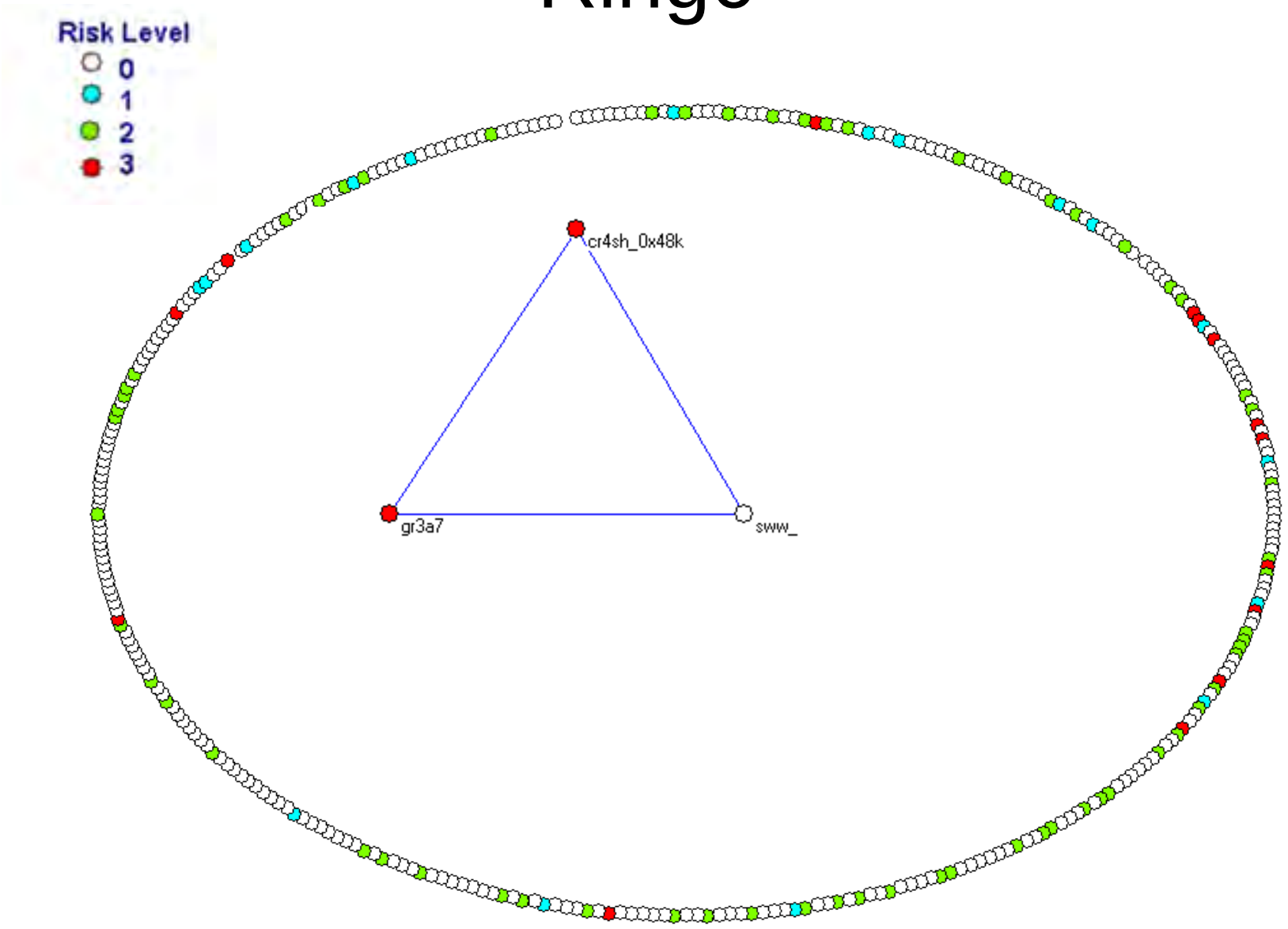
Computer Security



General Malware



Ring0



Initial Predictive Analysis

- An Anova analysis was conducted based on frequency of interests in various categories
  - Malware
  - Operating Systems
  - Drugs & Alcohol
  - Assembly Language

- Anova Class based on individuals verified as having created, attempted, or sold malware

  0 = no history of hacks/malware

  1 = security writer or blogger

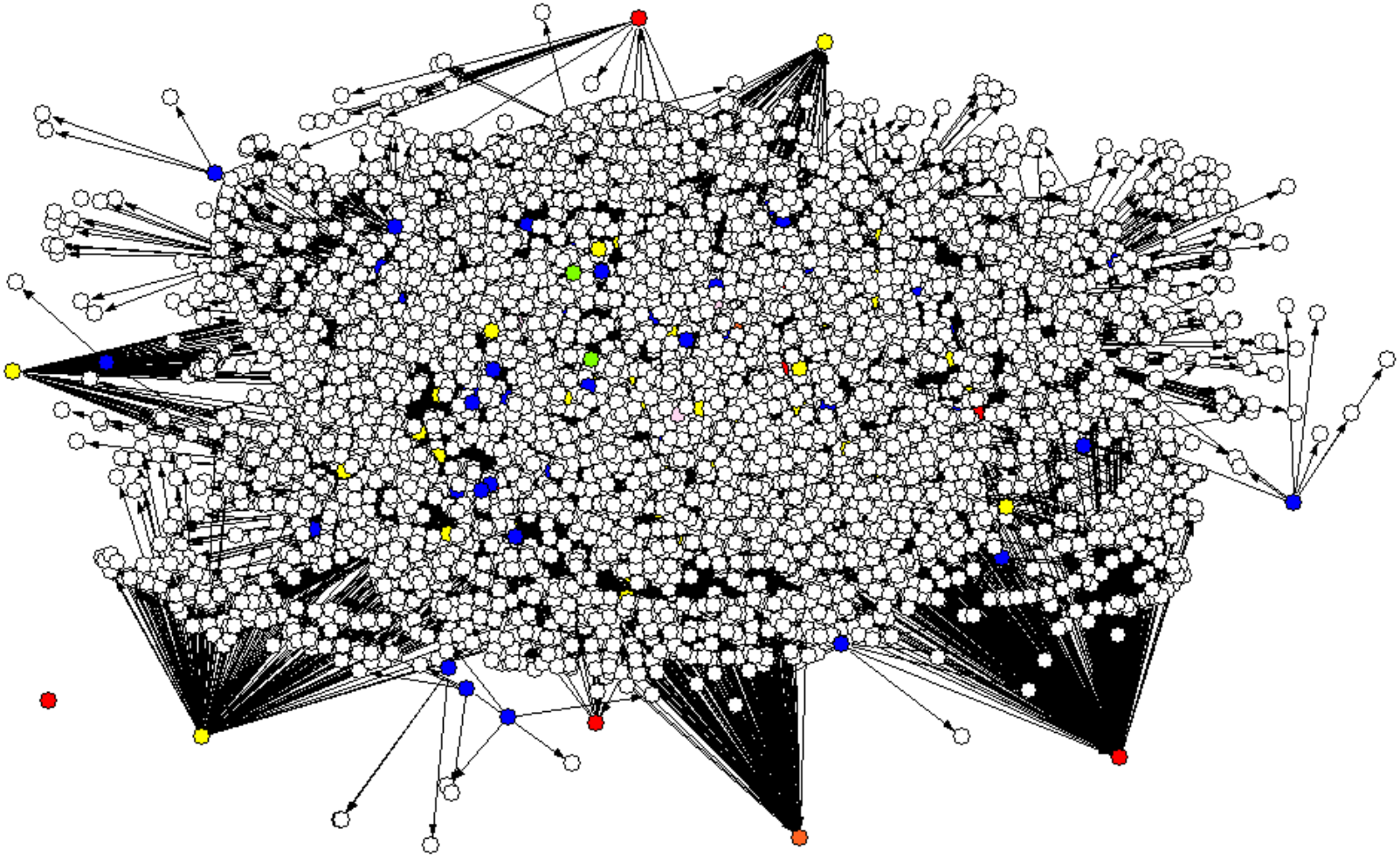
  2 = script kiddie, hacker or malware creator

Initial Predictive Analysis

Interests	ANOVA	F-Statistic
Malware	Significant	0.0282
Operating Systems	Significant	0.0135
Drugs & Alcohol	Not Significant	0.4703
Assembly Language	Not Significant	0.4881

- Individuals with higher threat levels express more specific and detailed interests in software techniques and methods, rather than general topics of interests.
  - Threat Level = 0 might list “hacks” as a general interest
  - Threat Level = 2 or 3 may list all of the following “botnets, buffer overflows, ios kernel hack, phreaking, rootkits, immunity debugger”

Mutual Friends Networks



The complete network of all members & friends.

Mutual Friends Networks

Red- Damagelab

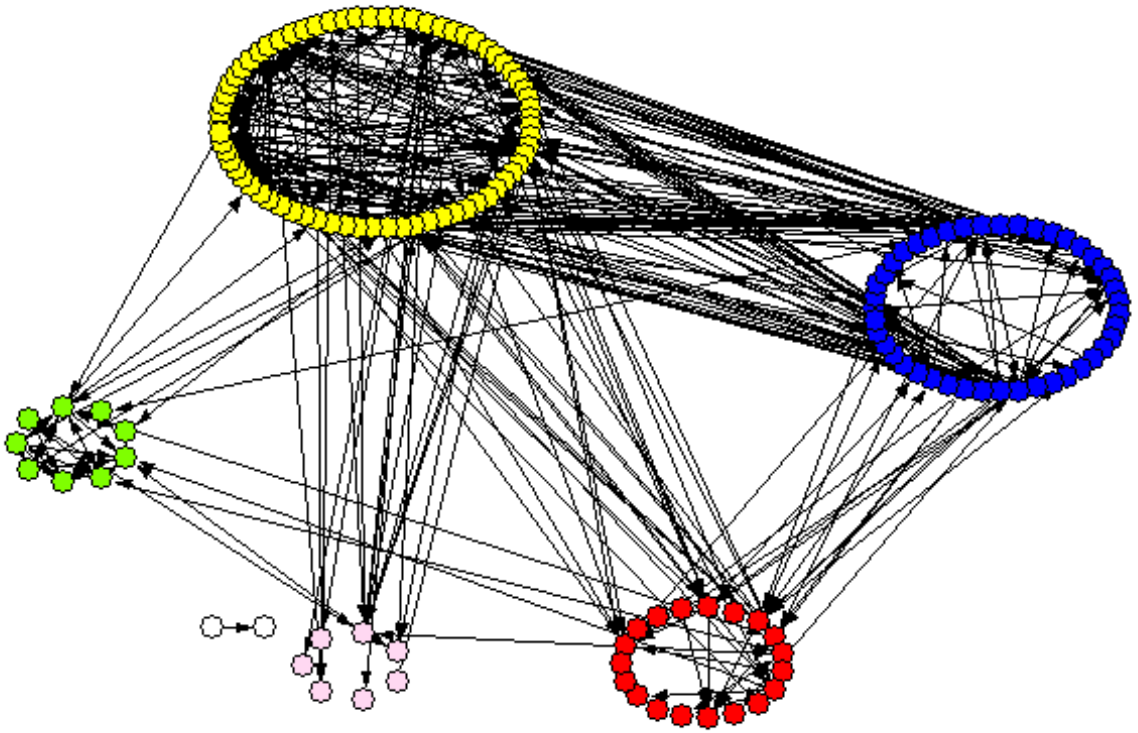
Yellow- BH Crew

Green- Cup

Blue- HZ

Purple- MF

White- HK



The level of interaction between the groups is fairly high.

Mutual Friends Networks

Red- Damagelab

Yellow- BH Crew

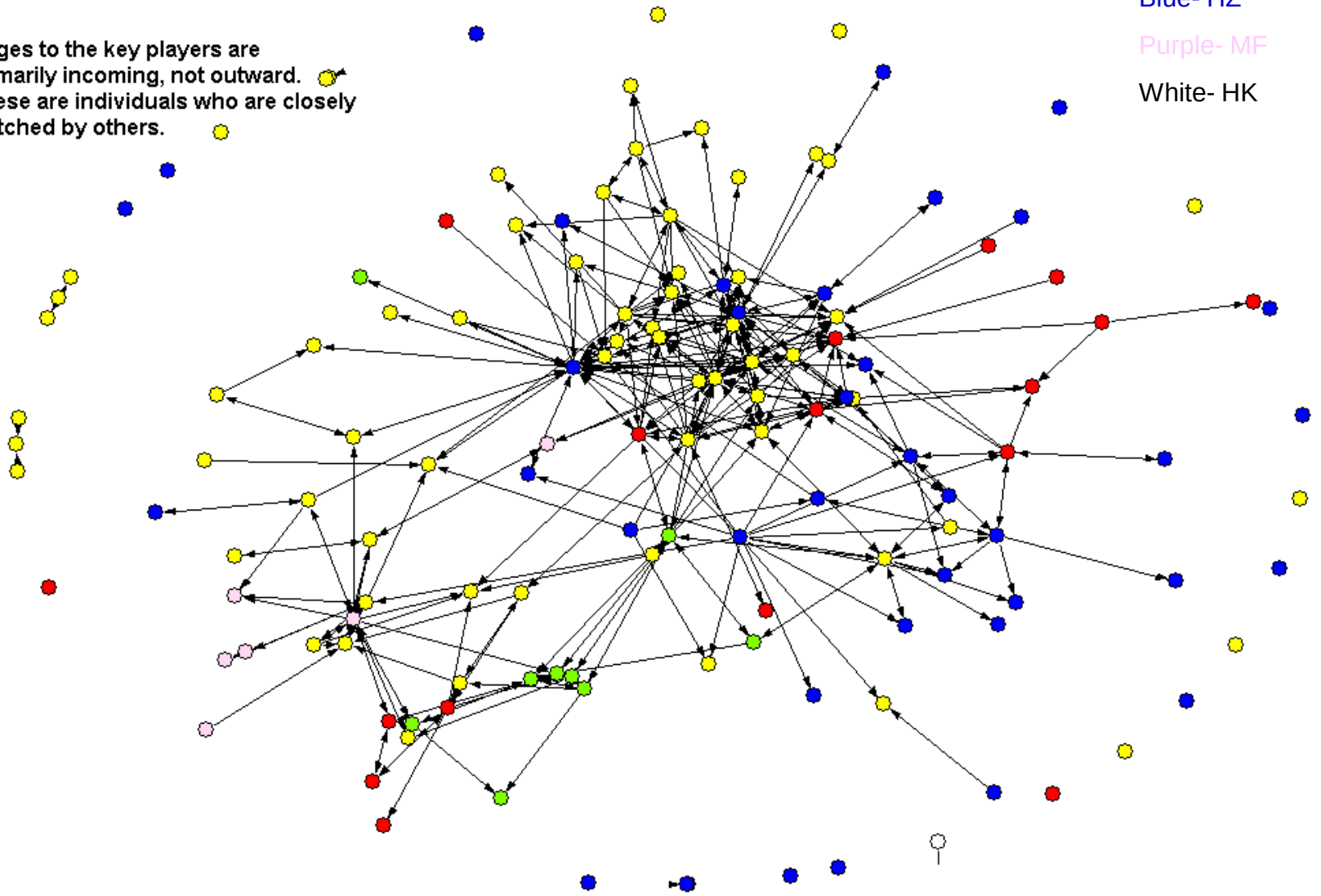
Green- Cup

Blue- HZ

Purple- MF

White- HK

Edges to the key players are primarily incoming, not outward. These are individuals who are closely watched by others.



Mutual Friends Networks

Red- Damagelab

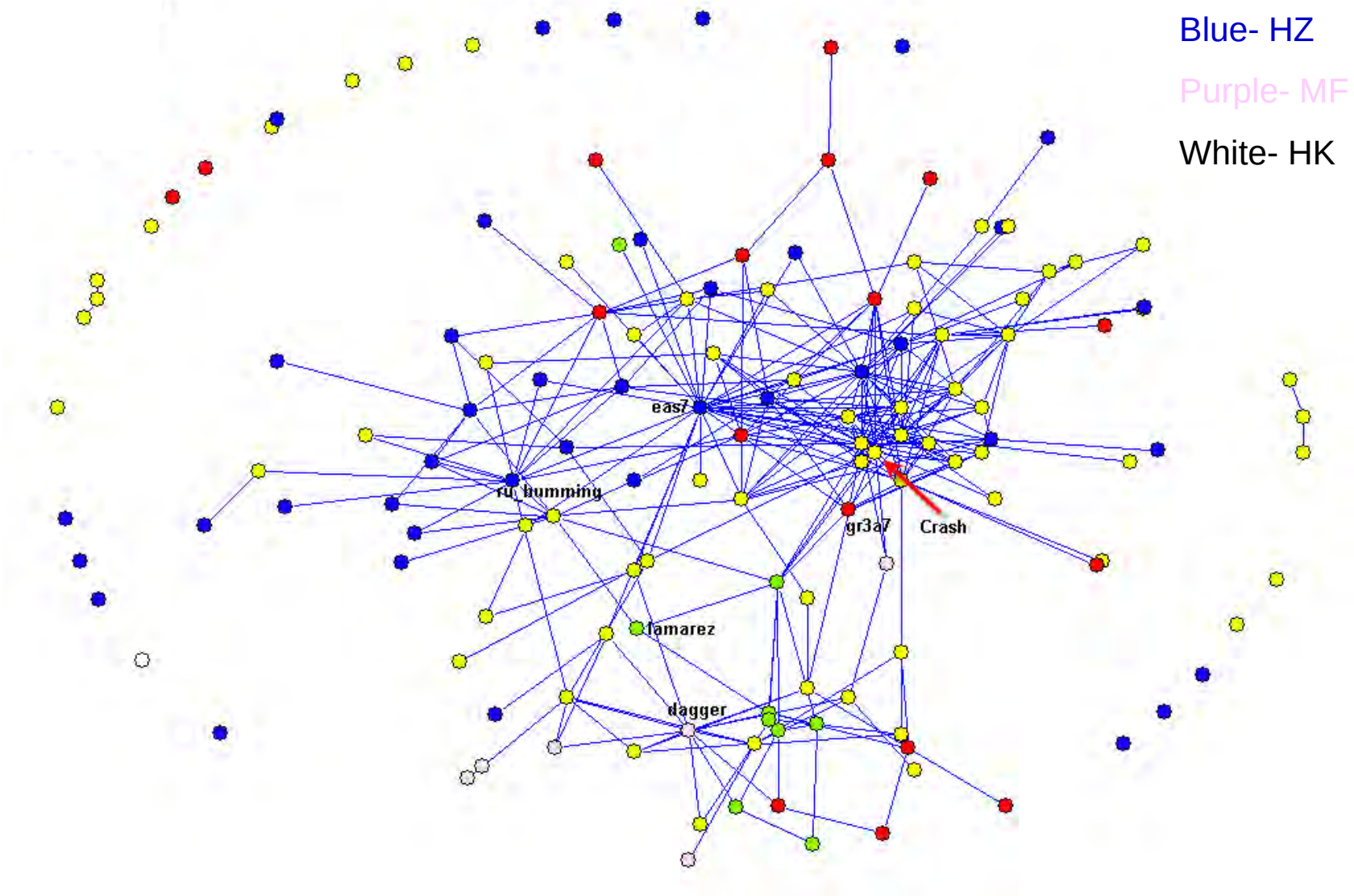
Yellow- BH Crew

Green- Cup

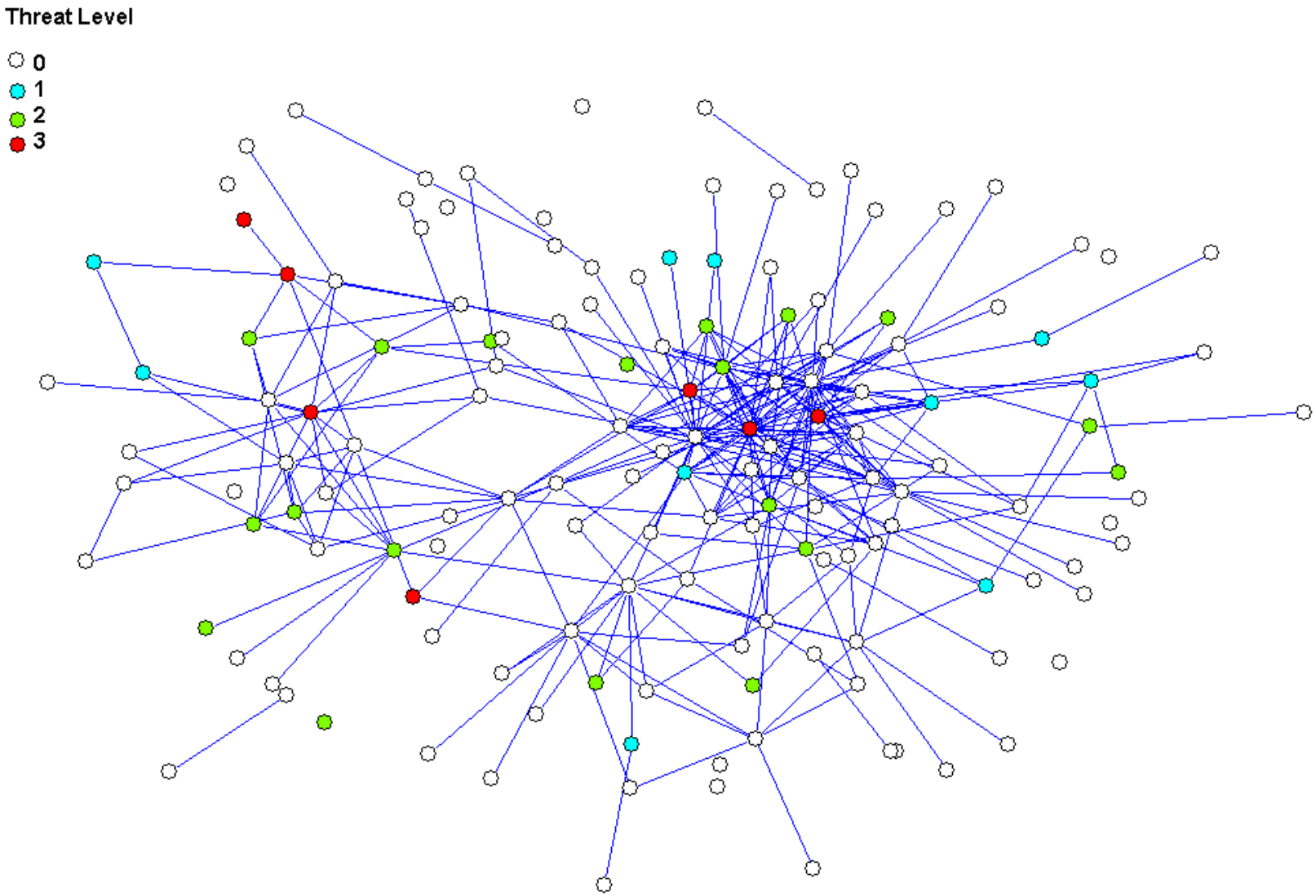
Blue- HZ

Purple- MF

White- HK



Mutual Friends Networks



Discussion and Conclusions

- A significant amount of information can be generated from social networking data
- The Russian hacker community is relatively centrally located in Moscow and St. Petersburg
  - Gender and education reflect general research on the community
- Groups are well connected, and particularly threatening hackers are densely connected
  - A small percentage of the members appear to be overtly involved in hacking and malware

Discussion and Conclusions

- Groups are densely connected and redundant networks exist
  - Indicates insulation which may be why so many tools and attacks are continuously recycled and pushed from skilled to unskilled
- Interests may be a critical predictor of hacker behavior
  - Multinomial regression models can be developed to identify factors that help to determine threat level of hackers
  - Test computer simulations of hacker-networks behavior

Thank You!

- Comments or Questions?
- Dr. Thomas J. Holt
  Assistant Professor
  School of Criminal Justice
  Michigan State University
  holtt@msu.edu