Feature

The Underground Threat

Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CBCP, CDP, CISSP, ITIL V3, is a senior associate at the Veris Group LLC, and has more than 15 years of experience in IT security. Wlosinski has been a speaker on a variety of IT security topics at US government and professional conferences and meetings and has written numerous articles for professional magazines and newspapers.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

The numbers are astounding. According to the Symantec *Internet Security Threat Report (ISTR) 2014*, the annual cost of cybercrime to consumers in the US is more than US $38 billion; in China it is more than US $37 billion; and in Europe it is more than US $13 billion.[1] On average, there are about 28 billion spam emails per day,[2] and the majority have a malicious intent. According to the *2012 Norton Cybercrime Report*, the highest number of cybercrime victims are in Russia (92 percent), China (84 percent) and South Africa (80 percent).[3] According to the 2014 Trustwave Global Security Report, the top three malware hosting countries are the US (42 percent), Russia (13 percent) and Germany (9 percent).[4] The top three spam hosting countries are the US, Canada and the UK.[5]

How did it get so bad that it is a worldwide problem that affects almost everyone? How did all those computers (i.e., desktops, workstations, laptops, mobile devices) get infected? Who is responsible for infecting all these machines? What are the costs to businesses, financial institutions and society in general? Can this malicious activity be stopped and assets be protected?

HOW DID IT GET SO BAD?

Malware can exist in a variety of forms, including key loggers, computer viruses, worms, Trojan horse, ransomware, spyware, adware and botnets, to name a few. Malware can be embedded in files that are accessed, and it can be activated by simply clicking a malicious file or link in an email. It can be planted, purposely or by accident, on web sites. It can be spread via communications software (e.g., email, Internet relay chats, spam), movable media (e.g., thumb drives, CDs, diskettes), wirelessly by infected mobile devices and by itself within an infected network.

Malware exists because of weaknesses and vulnerabilities in software systems at the operating system (OS), application, software utilities and hardware levels (i.e., computer chips). The complexity of software provides an advantage to those who develop the malware. Sophisticated malware, and those who use it, can hide their activities and cover their tracks by providing false addresses, redirecting traffic, erasing their activities (i.e., deleting files and information in log files), planting false information and working outside of the country in which the malicious activity is being conducted. Polymorphic malware even changes its signatures (i.e., file names and locations) so that antivirus software cannot identify the program components and remove them. Some types of malware make it very difficult to remove them because they can hide by changing file and directory permission settings. In some cases, malware can appear to be removed, but then reinstall itself upon restart.

Malware has grown from simply annoying events to software and systems that can take down government computers, capture access information or steal an individual's money. Those who control malware can obtain personal and financial information, cause havoc within commercial industries and financial institutions, and threaten people's livelihoods and personal wealth.

HOW DID ALL THOSE COMPUTERS GET INFECTED?

As a result of the efforts of cybercriminals, software developers have created malware to control other malware and computers. These systems are called botnets and they have command and control (C&C) centers.

Some of the uses of a bot or botnet include:

- Running a distributed denial-of-service (DDoS) attack that can send large streams of User Datagram Protocol (UDP) packets, Internet Control Message Protocol (ICMP) requests or Transmission Control Protocol (TCP) sync requests
- Infecting other computers on a network by taking complete control of a victim machine
- Utilizing and sharing large amounts of bandwidth among hacker communities
- Installing a backdoor to maintain access after an exploit
- Hosting illegal data on a system by making the data part of a file-sharing network to host illegal files (e.g., software, pirated movies)

To infect or compromise a computer system, a cyberattack goes through three phases:

1. **Precompromise**—This phase consists of:
   - Reconnaissance of the target or intended victim
   - Customizing the malware as a weapon to cause damage, obtain data and spy on the target
   - Establishing a means of access
2. **Compromise**—In this phase, the target system is exploited to the hacker's advantage and, subsequently, the malware is installed on vulnerable systems on the network or computer.
3. **Postcompromise**—Once compromised, the attacker establishes a C&C center to direct future cyberactivities and perform actions to further his/her intent.

Cybercriminals not only use malware to gain access to proprietary, sensitive and personal information, but they piggyback on personal activities to learn about targets and their employer organizations. These activities include:

- Capturing online banking access information
- Emailing source and target Internet Protocol (IP) and email lists
- Manipulating online gaming sites to their advantage
- Monitoring bad patching practices
- Studying a target's browsing routines and habits
- Capturing a target's mobile browsing activities
- Studying social networking and messaging sites

To make the problem even worse, time and bad programming practices have allowed cybercriminals to become organized. They know that not everyone has the best security in place, so they prey on the unaware, untrained and unprepared.

CRIMINAL BUSINESS MODELS

According to Trend Micro, cybercriminals can be viewed as having four models (or classifications)[6] (**figure 1**). The commercial model is about selling their services and software. Organized crime is about exploiting the weak and taking their money. The outsourcing model is about obtaining and using criminals with software development skills for their benefit, and the mentors/apprentices model is about those who want to become better at their criminal activities to advance their financial gains.

To develop malware, one may need to incorporate the following tools, resources and services: tool kits (e.g., Structured Query Language [SQL] injection, exploit), bulletproof hosting sites, compromised web sites, bot resellers, cryptography experts, existing malware (i.e., worm, virus, Trojan horse), programmers, information about the target (e.g., IP addresses/ranges, operating system[s], defenses) and testers.

WHO IS RESPONSIBLE FOR INFECTING ALL THESE MACHINES?

Cybercriminals thrive in forums and chat rooms. They not only share their programs and resources, but also brainstorm and share ideas. It is here that they plan cyberattacks, new malware, new approaches to identity theft, phishing schemes, and other ways to make money or gain information. They include specialists who deploy sophisticated malware, design private botnets, design fake antivirus software, poison and hijack web sites, and develop exploit tool kits. Their methods of promotion include Internet job boards, hacking message forums and the Underground Internet Relay Chat (IRC) channel.

Figure 1—Four Models of Cybercriminals

Model	Description	Sample Activities
Commercial	Sell information, tools and resources	• Sell acquired databases (e.g., credit cards) • Sell malware • Sell services to write malware • Conduct DDoS attacks
Organized crime	Work as groups for specific purposes	• Launder stolen property • Participate in malicious activities (e.g., emptying automated teller machine [ATM] accounts, buying gift certificates)
Outsourcing	Hire programmers to join their group, perform malware development or provide services	• Outsource parts of the malware development process • Request DDoS attacks • Use white hat proof of concept to build malware
Mentors/apprentice	Hire more skilled criminals to learn their craft	• Have skilled programmers teach novices

Source: Larry G. Wlosinski. Reprinted with permission. Content based on: Trend Micro, "Cybercriminal Underground Works in Business Models," 10 May 2014, *www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-underground-works-in-business-models*

Cybercriminals use social networks with escrow services. Like normal businesses, they license malware and receive technical support. Botnets can be rented by the hour. There are even infection services and sources for zero-day exploit information. According to Trend Micro, the main underground cybercriminals groups responsible for most malicious activity are located in Russia, China and Brazil.[7]

UNDERGROUND COMPARISON

Figure 2 provides a summary comparison of the malware products and service offerings of Russia, China and Brazil. It is not all-inclusive, but it does provide a high-level view of the underground criminal business offerings.

The overall underground economy that has resulted from cybercriminals' activities is driven by malware authors, organized crime, money-mule networks, third-party enablers, corporate enablers, insiders, and C&C systems and those who control them.

The consequences of their actions on society include:

- Data loss to governments, commercial businesses, financial institutions and individuals

Figure 2—Comparision of Malware Products and Services From Russia, China and Brazil

Service	Russia	China	Brazil
Denial of service (DoS)	• By email • By land line • By text message	• By SYN traffic • By Hypertext Transfer Protocol (HTTP) Get • Domain Name System (DNS) Server • DDoS tool kit rental	
Botnets		• Windows XP bots • Windows Server 2003/2008 bots • By number of bots	
Banking Trojans		• By level of importance • Account stealers	• Selling builder Trojan • Selling source code
Server hosting	• Virtual private network (VPN) with one exit point • With unlimited exit points and traffic	• By proxy addresses per month • VPN by month(s) or year	
Hacking	By target: • Facebook • Gmail • Hotmail • Others		
Cracking		Encrypted files Software with: • Dongle protection • Registration code • User number limit protection	
Email	Spamming by quantity: • Generic (public database) • Short Message Service (SMS)/texting • ICQ • Skype	Spamming by quantity of email addresses	Phishing of popular banks and financial service providers
Social media			Number of likes for: • Facebook • Instagram • Twitter • YouTube

Figure 2—Comparision of Malware Products and Services From Russia, China and Brazil *(cont.)*

Service	Russia	China	Brazil
Other product offerings	• Trojan horses—Self-replicating software that contains malicious code • Exploits and exploit bundles • Rootkits—Hide existence of malicious processes or programs • Crypters—File encryption and extraction software • Fake documents, e.g., passports • Stolen credit card and other credentials (e.g., VISA, MasterCard, gaming account)	• System exploit kit to fully utilize administrator capabilities • Fake post/comment/view/follower to inflate counts of postings, comments, video views and followers • Fake site, e.g., malicious online game site • Scanned fake document—Passports for China, the US and Canada • Software serial keys for Microsoft, Adobe and AutoCAD products • Traffic monitoring software—IP addresses per day (priced by tiered quantity) • Trojan horse software—Account stealers and bank Trojan tool kits	• Business application account credentials • Credit card credentials • Credit card number generators and testers • Crypters • Social media followers • Online service account credential checkers • Phishing pages • Phone number lists by town or city • Social media followers/views/likes • SMS (texting) spamming software
Other service offerings	• Dedicated server hosting—Servers rented for malicious activity • Proxy server hosting—Used to ensure anonymity • VPN—Encrypted tunnel that can misdirect traffic analysis (e.g., Tor—an encrypted communications tunnel used by cybercriminals) • Pay-per-install (PPI) of select malware—Free applications bundled with adware • Phishing and spamming—Sending quantities of unsolicited messages/email • Malware checking against security software—To test software effectiveness • Social engineering—Manipulating people to give up sensitive information • Brute-force attacks of email and access accounts • System abuse services • Account hacking services • Blackhat search engine optimization (SEO) services • C&C system server activity-related services • Carding (investigation) services • Crypting services (i.e., encryption and decryption)	• Use a compromised host as a malware or spam distributor • Use a compromised host to run complex computing tasks • Cracking of files (e.g., encrypted, RAR, .ZIP, DOC, XLS, EXE) and software (e.g., software key protection, registration code, user limit protections) • Fake document rework • Hacking of forum, email and other account types • Malware checking against various software (including security software) • Programming, development of Remote Access Toolkit (RAT) Trojan • HTTP SOCKS proxy server hosting (by tiered quantity of IP addresses) • RAT rental to function as a system administrator • Trojan attack—One online game per day • VPN server hosting by month(s) or year	• Malware checking against security software services • SMS spamming services • Training services (crypter programming and fraud) • Provide fraud training by selling how-to videos • Provide support via Skype

Figure 2—Comparision of Malware Products and Services From Russia, China and Brazil *(cont.)*

Service	Russia	China	Brazil
Other service offerings *(cont.)*	• Electronic-payment-related services • Money-laundering and mule-related services • Obfuscation services • PPI services • Programming services • Messaging fraud-related services		

Source: Larry G. Wlosinski. Reprinted with permission. Based on content from: Goncharoc, M; "Russian Underground Revisited," Trend Micro Cybercriminal Underground Economy Series, 2014, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf*. Gu, L.; *The Chinese Underground* in 2013, Trend Micro Cybercriminal Underground Economy Series, 2014, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf.* Merces, F.; *The Brazilian Underground Market*, Trend Micro Cybercriminal Underground Economy Series, 2014, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf*

- Identity theft (e.g., stolen credit cards, theft under the names of those affected)
- Online fraud (i.e., theft of account holdings by deception)
- Computer extortion (e.g., ransomware)
- Unauthorized access to networks and personal computing devices
- Copyright infringement that affects commercial businesses and government contractors
- DDoS attacks against businesses, government networks and web sites, rendering systems unavailable
- Data destruction, which can affect data availability and business continuity
- Damage to brand names, which can undermine an entire business and put those who work for it out of a job

To summarize, the results of cybercriminals' malicious actions threaten governments, businesses, individuals and the global economy. The resulting cost to society and the world's economy is high.

WHAT ARE THE COSTS TO BUSINESSES, FINANCIAL INSTITUTIONS AND SOCIETY IN GENERAL?

To calculate the costs, one must first quantify the direct and indirect losses and costs of cybersecurity-related defensive actions. The total cost is the sum of the direct losses, indirect losses and defense costs (**figure 3**).

Figure 3 represents just some of the costs. Even with this small list, it is apparent how powerful the underground has become as a threat and how important it is that work is undertaken to at least minimize the effect.

Figure 3—Losses and Costs of Cybersecurity-related Defensive Actions

Direct Losses	Indirect Losses	Defensive Action Costs
• Money withdrawn from victim accounts • Time and effort to reset account credentials (for both banks and consumers) • Distress suffered by victims • Secondary costs of overdrawn accounts, e.g., deferred purchases, inconvenience of not having access to money when needed	• Lost attention and bandwidth caused by spam messages • Missed business opportunity for banks to communicate with their customers by email • Reduced uptake by citizens of electronic services as a result of lessened trust in online transactions • Efforts to clean up all types of computers infected with the malware	• Loss of trust in online banking, leading to reduced revenues from electronic transaction fees and higher costs for maintaining branch staff and check-clearing facilities • Security products such as spam filters, antivirus and browser extensions to protect users • Security services provided to individuals, such as training and awareness measures • Security services provided to industry to protect against web site takedowns • Fraud detection, tracking and recuperation efforts • Law enforcement • Inconvenience of missing an important message falsely classified as spam

Source: Larry G. Wlosinski. Reprinted with permission.

CAN IT BE STOPPED?

The threat cannot be stopped, but the risk can be assessed, decisions on how to handle the threat made and countermeasures implemented. When determining the risk, it needs to be decided if each risk factor can be accepted, avoided/removed, minimized (plan for remediation), researched for a solution or transferred (e.g., insurance).

> “Stopping all threat sources is a monumental task that requires the cooperation of many countries and organizations.”

The problem with the underground threat is not at the organization’s enterprise or system level; rather, it is a world threat. While there are three main sources of underground threat, as described previously, there are others who are not as organized but perform similar, if not the same, malicious actions. Stopping all threat sources is a monumental task that requires the cooperation of many countries and organizations.

COUNTERMEASURES

In addition to the IT security defenses and best practices already in place, the following countermeasures could be implemented at the global level:

1. **Reinvent Internet defenses to block malicious activity coming from outside the country.** The reason for this is that some countries will not allow for extradition or do not have the will/capability to stop criminal organizations from conducting cybertraffic. To accomplish this, network monitors and reporting programs need to be implemented at each country’s entry point.
2. **Add sensors not only to monitor critical networks and systems but also to track places of origin.** This is needed to better locate the source and minimize the effect of address spoofing. Sensors should be able to verify source addresses before they are permitted to spread or cause DDoS and other malware attacks.
3. **Develop defensive software systems.** That is, applications should be self-monitoring such that if someone attempts changes without permission, the system would send an alert and not allow it. The system would also have the ability to correct itself by reverting back to its baseline.
4. **Develop nonstandard systems.** Developers should be able to create applications with the freedom to design how they see fit. Presently, the programming approach is according to proven best practices. What if programmers could assign code to dynamic memory locations, place files in random locations and create systems that appear random (i.e., at the programmers’ choosing) to make it more difficult for cybercriminals? Is this not what cybercriminals are doing? Perhaps learning from virus writers is a means of helping to avoid malicious activities.
5. **Create software viruses that can attach themselves to a malicious virus and remove the malware that was installed.** This would require understanding the malicious virus and setting a trap where the cleaning virus would attach to the bad virus.
6. **Develop an inventory system that would document what it discovers.** It would be a combination of a vulnerability scanner and a patch management system, but it would produce reports that define the system boundary and provide the basis for a system assessment. The system would be designed so that additional information could be added (e.g., location, serial number, purpose) and custom reports created.
7. **Have those who use encryption employ something that cannot be broken.** This concept suggests that each organization develop an internal proprietary encryption formula. Examples of proprietary encryption could be a simple enhancement to normal encryption such as adding to it, multiplying it, applying some polynomial to it or employing some mathematical formula to it that works for the single organization only.
8. **Encrypt sensitive information at the field level.** If the information is a personal identifier (e.g., social security number) or personally identifiable information (PII), at least encrypt these while at rest or in transit. This may require new retrieval and display routines, but the data are important enough to implement more secure measures for customers.

Are there other ways to reduce the threat and the level of risk? Here are some other things to consider:

- **Training**—From where are criminal programmers coming? Are international students trained in how to compromise specific systems? Where are criminally inclined programmers being taught? Is it possible that universities discard these programmers and developers if they are not good enough? What circumstances are pushing them to find an alternative and, possibly, a more lucrative job in the criminal world?

- **Blackmail**—Are those who become part of the cybercriminal world being forced to work for criminal enterprises for fear of reprisals to them and/or their family and friends? Do they have a way out?
- **Punishment**—Are more prisons needed? Are the laws (in all countries) sufficient to be a deterrent? Can smaller countries work together to share the burden of enforcement?
- **Location**—How are criminals who hide behind distance and anonymity reached? How can other governments be convinced that the malicious cyber-related actions of their people affect the world economy and they need to do the responsible thing?
- **Laws**—How can countries be convinced that their laws need to be adjusted to handle cyberactivities? New laws are needed for the cybercriminal sector and there need to be new rules of interconnectivity.
- **Web security**—How is the problem of a web site with weak security addressed? This refers not only to web sites that have been abandoned, but also to those owned by small businesses that have created company web sites but do not monitor them. These problems can be attributed to weak software patching programs, nonexistent malware scanning and removal, and configuration weaknesses. Should web sites have an automatic retirement/closure capability by default?
- **Reactive measures**—Should the good guys hack and disrupt the bad guys' web sites? Should someone teach them right from wrong? Should there be countermeasures and repercussions against those who work to harm society and the governments of all countries?
- **Businesses**—Should businesses have an incentive to monitor their employees' computers for malware? Business incentives could include tax credits and reduced credit rates (but this would require monitoring and enforcement).
- **Accountability**—Do the countries that harbor cybercriminals need accountability for the malicious cyberactivity they allow? How can transactions be tracked in places that do not capture or report malicious or suspicious activity? Should countries that do not follow honorable practices be removed from the global economic enterprise?

CONCLUSION

Everyone must be encouraged to work together to develop solutions. The threat is so large that entire economies are affected. This, in turn, affects banks (i.e., those who lend money, pay interest on accounts and pay for malicious intrusions), employing organizations and individual prosperity.

Governments, financial institutions, software vendors, system developers and users must work together to take back the economy or things will continue to get worse. Current cyber-related controls and strategies are not acceptable—cybercriminals are getting rich from the hard work of others and the lack of a united cybersecurity front on everyone's part.

ENDNOTES

[1] Symantec, *Internet Security Threat Report (ISTR) 2014*, 2014, *www.symantec.com/security_response/publications/threatreport.jsp?&om_sem_cid=biz_sem_s186232479297029|pcrid|51284528675|pmt|b|plc||pdv|c*

[2] Symantec, *Internet Security Threat Report (ISTR) 2015*, vol. 20, 2015, *www.symantec.com/security_response/publications/threatreport.jsp*

[3] Norton, *2012 Norton Cybercrime Report*, 2012, *http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf*

[4] Trustwave, *Uncovered: Targets, Methods and Motivations of Cybercrime*, 2014 Trustwave Global Security Report, 2014, *www2.trustwave.com/GSR2014.html?utm_source=redirect&utm_medium=web&utm_campaign=GSR2014*

[5] McAfee, *McAfee Labs Threats Report June 2014*, 2014, *www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf*

[6] Trend Micro, "Cybercriminal Underground Works in Business Models," 10 May 2014, *www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-underground-works-in-business-models.* The report includes lists of malware products available in Russia, China and Brazil.

[7] *Ibid.*