Research the dynamic of author activities in threats through to public and private sources

M.E. Burlakov[a]

[a] *Samara National Research University, 443011, 1 Ac. Pavlov street, Samara, Russia*

Abstract

The paper is aimed at researching the dynamic of objects publications in question of threats activity. Analysis of the author activities is lied in public and private sources like the Internet or the shadow global networks like TOR, VPN, Socks, Proxy and Mesh. In paper for analyzing the 10 most popular software are used for Windows operation system. The special program complex called Scan Project is applied for accumulating the messages about vulnerabilities and software mistakes. The 10 most active authors are shown.

Keywords: information threats; vulnerabilities publication; open data sources; private data

1. Introduction

Today, there are many problems associated with the detection of threats and vulnerabilities in information technologies and software systems. More than 87% personal computers are on Windows operating systems (Windows XP, Windows 7, Windows 8 and Windows 10) [1]. On the one hand, that's why many hackers attend this operation system much time always. On the other hand, there are many attention is given to software solutions which worked based on this operation system. For example, according to the Hewlett Packard company report [2], there are more than 500 different classes of vulnerabilities in Windows software.

The most common vulnerabilities are shown by TeamSHATTER command [3]. Such as:

1. the presence of specialized username and password (by default, easily bruteforsed);
2. SQL injection in various implementations interaction databases;
3. incorrectly issued executive rights for user, errors in setting group privileges;
4. weak desired functionality for administration configuration of databases;
5. incorrect settings for all type of configurations;
6. the buffer overflow (stack);
7. privilege escalations;
8. denial of service attack (DDoS);
9. the lack of a timely update database security component;
10. non secure data storage, etc.

There are two ways for creating the vulnerabilities in software: explicit and implicit. The explicit type means that the vulnerabilities are made special for the further destructive activity. This type is a hard nut to crack because it's difficult to predict for any external systems. Often the results of their appearance are motivated acts by developers or development teams. It's aimed at targeted deterioration (even for information security) software. The predicting and correcting explicit type errors are difficult and should be started with the work with the staff, that is, the use of social-oriented approaches.

Implicit errors occur for many reasons. Such as:

- carelessness of software developers;
- incorrect software testing organization;
- small experience;
- using the software and libraries with existing threats and vulnerabilities;
- small outlook of development vision, etc.

Implicit bugs (errors) are founded both software developers and hackers. It's usual situation when the hackers are discover the threat faster than the developers and use this knowledge for the escalating the security policies of computer systems.

There are private and public sources are used for the publication of information about threats and vulnerabilities by hackers. The status of "private" source means that access to information is limited by various kinds of software and hardware solutions. Such as:

- Authentication process limitation:
  - basic authentication;
  - authentication confirmation (email, phone, etc.);
  - two-factor authentication with reference to the phone;
  - other authentication variation, etc.
- Limitation by technologies :
  - virtual private networks;
  - Proxy and Socks servers;
  - Mesh networks;
  - TOR networks (more can be found in [4-7]);

- access through a communication channel with the use of special certificates;
- other technological limitations.

• Other solutions, limiting access to information about threats and vulnerabilities.

The status of "public" source means that the source is not private.

In public and private sources both hackers and developers are exchange information though the messages and reports. They become the authors of these messages and reports about discovered threats and vulnerabilities. These reports and messages are the signals or indicators for computer security specialists of existing for definite software some problems. This paper attempts to research the authors of the threats with making some conclusions.

2. Data analyzing

The 10 most popular software which running on Windows operation system are selected for the researches (Table 1). The selection is made by conclusion about the number of downloads (statistic was taken from Softonic Group report [8]).

Table 1. TOP-10 the most popular software in Windows OS

№	*Software*
1	uTorrent
2	SHAREit
3	VLC media player
4	UC Browser
5	Mozilla Firefox
6	Whatsapp
7	Google Chrome
8	Adobe Reader
9	Adobe Flash Player
10	Internet Downloader Manager

The complex SCAN Project v.1.9.5 (hereinafter SCAN) was used as a tool for research. This complex was developed thanks to R&D project by "Academy Infotecs". It has the number of functions. Such as:

1. the automated collection of information about threats and vulnerabilities in software systems;
2. the allocation of information about the time of threats and vulnerabilities assigned;
3. the release of information about the authors, announced of threats and vulnerabilities.

The analyzed software is shown in Table 1 and the basic OS was selected Windows OS with versions (Windows XP, Windows 7, Windows 8 and Windows 10). The data analysis was conducted for receiving information with the time interval from 1991 to present.

The numbers of analyzed private and public sources are shown in Table 2.

Table 2. Public and private sources

Name of source	*Link*	*Type*
Security Lab	http://www.securitylab.ru/	public
Exploit-DB	https://www.exploit-db.com/	public
CVE Detail	http://www.cvedetails.com/	public
Malwarebytes.org	https://ru.malwarebytes.com/trial/	private
Htbridge.com	https:// htbridge.com	private
web.nvd.nist.gov	https://nvd.nist.gov/	private
0 day	Onion TOR	private
Seclists.org	http://seclists.org/	private
Stackoverflow	Stackoverflow.com	public

The total numbers of threats are equal to 269419. The total number of vulnerabilities with the authorship is 124049.

The total number of authors who have declared about the vulnerabilities is 24975 (averaging out at 5 threats for each author). The numbers of authors have declared at least one threat - 18704. Thus, there are near 75% of all threats are declared by different authors (the difference in terms of logins under the author reserved the information). So, the personalization is very high in finding the vulnerabilities. From these calculations it follows that the 6271 author stated threats 105345, an average of 16.7 each. Thus 33.5% of authors responsible for the 84.9% declared threats that logically corresponds the Pareto principle. There is system work which means that when the author find the one vulnerability there is high probability to find several vulnerabilities.

In Table 3 there are the top 10 most active authors which declared about submitted software vulnerabilities.

Table 3. TOP-10 authors declared the submitted software vulnerabilities

№	*Author*	*Numbers of vul.*	*Author information*	*Country*
1	*CONFIRM*	16295	The numbers of developers which founded themselves vulnerable and declared about them.	-
2	*BID*	10001	Non-commercial community of information security specialists named *SecurityFocus*, engaged in the search for vulnerabilities and threats to further declaring to developers. Site: http://www.securityfocus.com.	USA
3	*XF*	9227	The specialists of IBM X-Force Research team from IBM company which provide services in information security. Site: http://www-03.ibm.com/security/xforce/	USA
4	*MISC*	7864	Private community of experts in information security called *LEGAL HACKERS* which deal with issues of information security, "ethical" hacking and penetration testing of information systems. Site: http://legalhackers.com/	-
5	*BUGTRAQ*	5680	The mailing list of vulnerabilities called *Bugtraq Mailing List*. It's free information source. It's aggregate the information from other sources. Site: http://seclists.org/bugtraq/	USA
6	*VUPEN*	3445	The commercial structure, which is a leading provider of defensive and offensive technologies for exploration in cyber security. Site: http://vupen.com	USA
7	*SECTRACK*	2848	The commercial structure called *SecurityTracker*, which develops and provides the information security software (Vulnerability Notification Service). Site: http://securitytracker.com/	USA
8	*MLIST*	1980	The public community of developers and information security specialists called *Openwall*. Site: http://www.openwall.com/	-
9	*MILW0RM*	1826	The public community of information security researches (hackers). The aggregator of other sources. Site: http://www.milw0rm.com/	-
10	*MS*	1567	The center of security by Microsoft company called TechCenter. Separate unit created to investigate and detect threats associated with the Windows OS. Site: https://technet.microsoft.com	USA

Thus, the 6 from 10 authors has private structure with the location from USA. The Fig. 1 shows the distribution the number of threats detected among the top 50 authors.

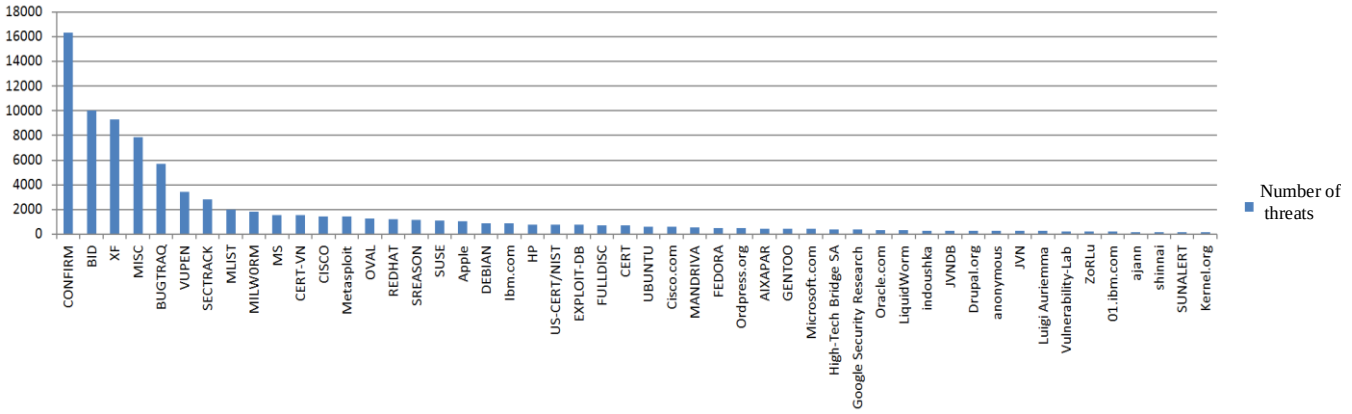

Fig. 1. TOP-50 authors threats destibution.

The Table 4 shows the top 10 most active authors in the last 5 years.

Table 4. TOP-10 the most active authors with the count of declared threats

2012	**2013**	**2014**	**2015**	**2016**
CONFIRM(1493)	CONFIRM(1611)	CONFIRM(2082)	CONFIRM(2587)	CONFIRM(3210)
MISC(782)	MISC(429)	MISC(1665)	MISC(808)	MISC(390)
XF(531)	CISCO(330)	CERT-VN(765)	MS(425)	MS(365)
BID(490)	XF(300)	Ibm.com(598)	CISCO(400)	CISCO(268)
MLIST(340)	MLIST(213)	BID(594)	SECTRACK(262)	Google Security Research(213)
Metasploit(231)	SUSE(212)	XF(423)	APPLE(262)	MLIST(197)
Ordpress.org(175)	BID(206)	MLIST(328)	MLIST(259)	BID(159)
SECTRACK(174)	REDHAT(199)	SECTRACK(268)	Google Security Research(164)	APPLE(114)
OVAL(167)	Metasploit(193)	Cisco.com(223)	BID(158)	SUSE(105)
Drupal.org(134)	OVAL(193)	MS(207)	BUGTRAQ(140)	SECTRACK(101)

Based on these data, the 4 communities maintain a constant work in researching of vulnerabilities and threats: CONFIRM, MISC, BID and MLIST (fig. 2 and fig. 3).

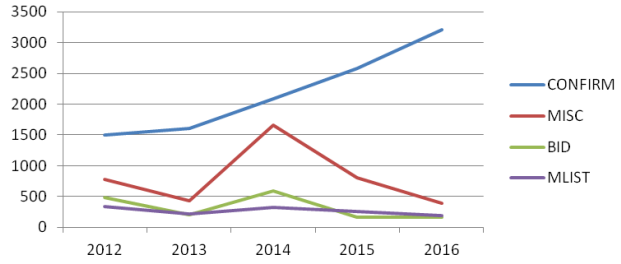

Fig. 2. The number of threats founded by CONFIRM, MISC, BID and MLIST.

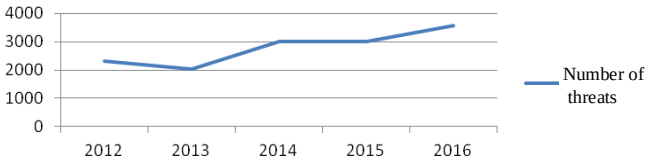

Fig. 3. The total count of threats founded by CONFIRM, MISC, BID and MLIST.

Conclusion

There are definite conclusions based on getting data. Such as:

1. The number of threats is increased from year to year. It indicates the systemic problems in software development and shows the growth of qualification of hackers.
2. The 6 of 10 communities which found the maximum number of threats in 2016 are the private companies from USA.
3. The number of developers which are not involved in analysis of vulnerability at the community is large, but it does not have a decisive impact on the number of detected threats.
4. The impact of public community is large and the number of declared threats is growing.
5. The corporate sector (Microsoft, IBM, etc.) develop the security information and auditing of computer networks and software systems brunch actively.

Acknowledgements

This research was made by the grant through R&D “Academy Infotecs”.

References

[1] W3Schools. OS Platform Statistics [Electronic resource]. — Access mode: http://www.w3schools.com/browsers/browsers_os.asp (30.01.2017)
[2] HP. The collateral damage of cybercrime [Electronic resource]. — Access mode: http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/ (30.01.2017)
[3] Trinidad Mark. Top 10 Database Vulnerabilities and Vulnerabilities and Misconfigurations [Electronic resource]. — Access mode: http://www.sifma.org/uploadedfiles/societies/sifma_internal_auditors_society/top10-database-vulnerabilities-and-misconfigurations.pdf (30.01.2017)
[4] Applebaum, J. A Model of Outbound Client Traffic on The Tor Anonymity Network / J. Applebaum // Wesleyan University . – 2013. – P. 54-58.
[5] Ivanov, M. Cryptographic methods of information protection in computer systems and networks / M. Ivanov – Moscow: KUDIC-OBRAZ, 2001. – 390 p. – (in Russian).
[6] Oliver, V. Computer networks. Principles, technologies, protocols / V. Oliver, N. Oliver – Spb: Piter, 2001. – 672 p. – (in Russian).
[7] Stollings, V. Network Security Essentials. Applications and Standards / V. Stollings – Moscow: Williams, 2002. – 450 p. – (in Russian).
[8] Softonic. Top downloads [Electronic resource]. — Access mode: http://en.softonic.com/windows/top-downloads (30.01.2017)