

Peek Inside Cybercrime Monetisation Methods and Volume

Regardless of who you are — an individual at home, the CFO of a publicly-traded company, a government agency or a journalist — your PC is a target for cybercriminals when you are online.

Over the course of the last five years, many reports have surfaced which focus on the motivation behind the actions of today's cybercriminals. The main message in these reports is repetitive; "*Cybercriminals are motivated by money, not by fame.*" Unlike the '*fame-based*' attacks that used to get 'hackers' their 15 minutes of fame, today's cybercriminals are increasingly finding new ways to monetise their criminal activities.

There are various methods utilised by today's cybercriminals to cash-out. Primary methods include:

- Using malware to steal and later selling valuable personal data (e.g. your credit card numbers, SSNs, confidential email communications)
- Trading — buying and selling — your compromised PC

Consumers might be surprised to suddenly find their PCs in a long list of compromised computers that criminals are offering for sale on their auction sites. It doesn't matter if it is a home computer or if it belongs to a C-level executive of a Fortune 500 company, a government agency or news network — each and every compromised PC has its own value and price in the cyber-economy.

AVG monitored 165 domains controlled by cybercriminals, which over two months managed to infect more than 1.2 million computers worldwide out of 12 million users visiting their compromised Web pages — about 10% success rate in infection.

Who might be after your PC? What tools and techniques are they using? How successful are they? Where are they located? What you should do to prevent them from 'owning' your PC? This report will provide insight into these questions along with suggested ways to protect yourself from cyber-criminals.

Overview

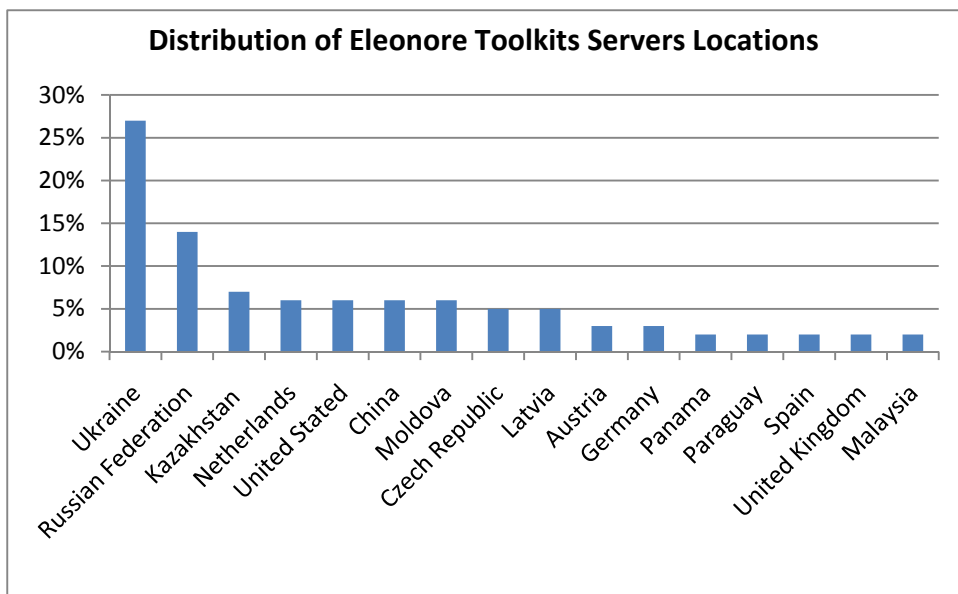
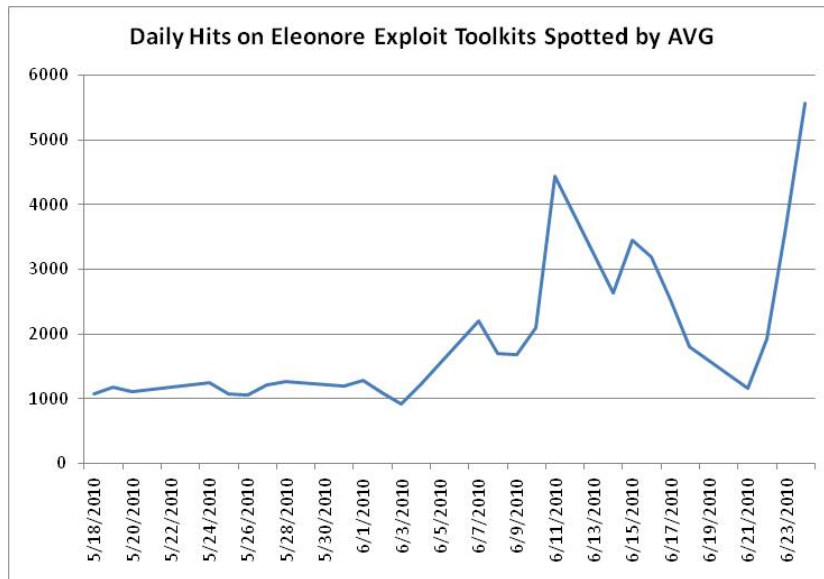
Web-based attacks have increased in volume and in sophistication in the past few years, mostly due to the large amount of money cybercriminals can make. As these attacks have increased in popularity commercial grade tools have been introduced which are designed to assist cybercriminals in accomplishing their goals much easier and faster. These toolkits also enable non-technical people to be 'part of the game' without any knowledge of security. Such tools are known as [Exploit toolkits](#) and are widely used by cybercriminals on the Web today.

The Eleonore Exploits Toolkit Under Research

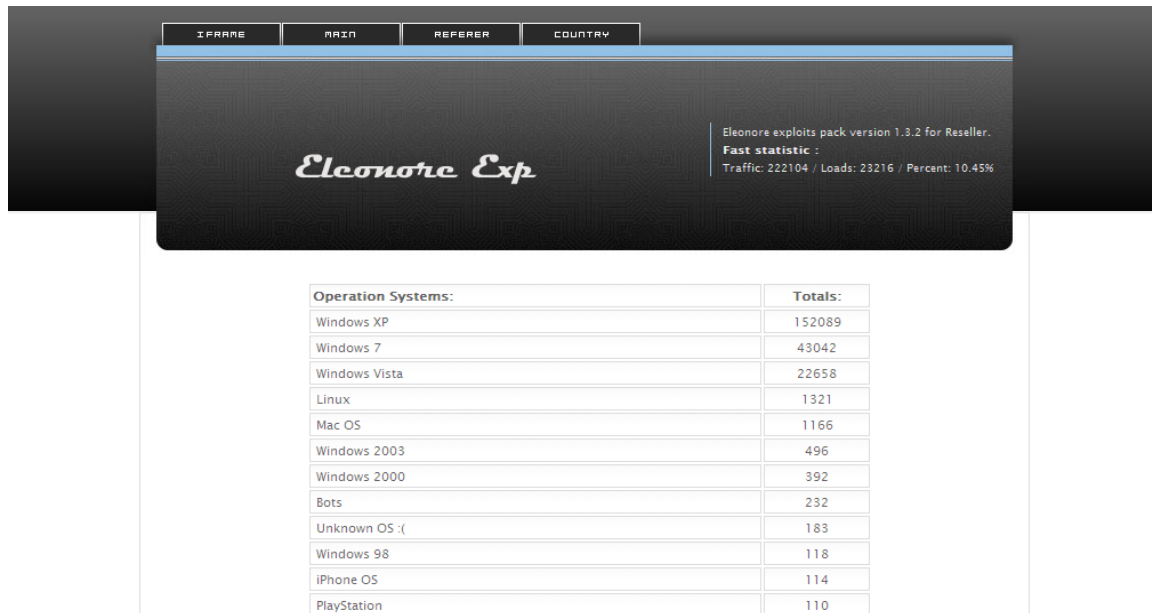
During the last two months, AVG's research team noticed an increase in the use of one specific Exploit toolkit known as Eleonore. Due to this spike in activity AVG directed its Web security team to conduct this study.

During this study, AVG's research team monitored **165** unique domains hosting the Eleonore toolkit and operated by various cybercriminals all around the world. The domains under research grabbed our attention due to a relatively high volume of Web site traffic that the cybercriminals managed to gain by directing innocent users from compromised websites to their malicious domains.

Although you may assume that the cybercriminals making and using these toolkits are software experts, the reality indicates that even malicious code writers leave vulnerabilities in their code. Taking advantage of one of the weaknesses in the Eleonore toolkit, we were able to collect statistics that allow us to gain a better understanding of the magnitude of such attacks and the average success rate in infecting PCs by these toolkits.



The 165 domains AVG researched used the 1.3.2 version of the Eleonore exploit toolkit, although we also found a later version of Eleonore, the v1.4.x.



Operation Systems:	Totals:
Windows XP	152089
Windows 7	43042
Windows Vista	22658
Linux	1321
Mac OS	1166
Windows 2003	496
Windows 2000	392
Bots	232
Unknown OS :(183
Windows 98	118
iPhone OS	114
PlayStation	110

The Eleonore exploit toolkit administration panel under research

The first step to silently infecting users' machine with malware is to exploit a vulnerability in their browser or other applications running on their machine. Successfully exploiting a vulnerability enables the cybercriminal to load and install the actual malware that can steal data and enable the criminal to later auction the PC online as a DDoS bot or a spam sending machine.

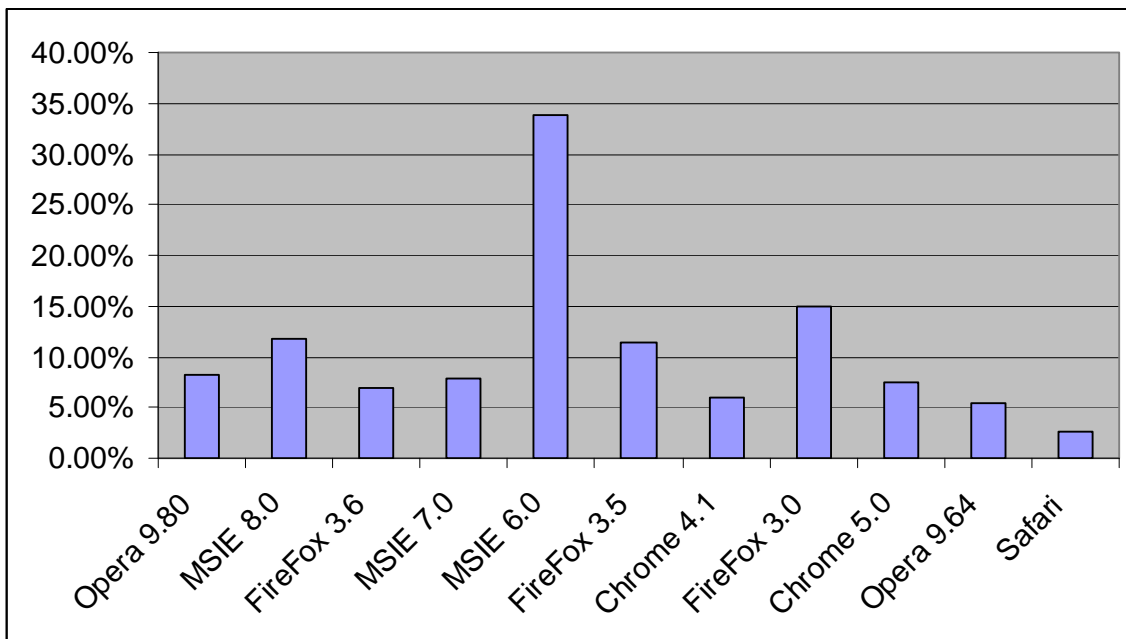
Eleonore exploit toolkit utilises the following vulnerabilities to exploit PCs:

- Sun JVM Vulnerabilities
- Adobe Acrobat Reader Vulnerabilities
- Various IE6 Vulnerabilities
- Various IE7 Vulnerabilities
- Various FireFox Vulnerabilities

How Many PCs were Infected by These Cybercriminals?

According to the toolkit statistics pages, these 165 domains managed to infect more than 1.2 million machines by attacking more than 12 million machines with a 10 percent success rate. These are impressive numbers for a single Exploit toolkit type, knowing there are dozens more out there doing the same thing.

The success rate of attacks is dependent on the browser that was attacked. Eleonore exploits were most successful when attacking IE6 with 33.8 percent success rate while against Safari had the lowest success rate of only 2.78 percent.



Web browser vendors are not always to be blamed for infections, in fact, as noted in the table below, the most effective attacks were conducted by exploiting vulnerabilities in cross browser applications, namely Sun Java Virtual Machine (JVM) and Adobe Acrobat Reader.

Exploit Name	Infection Ratio
Sun JVM Vulnerabilities	36%
Adobe Acrobat Reader Vulnerabilities	36%
Various IE6 Vulnerabilities	22%
Various IE7 Vulnerabilities	5%
Various FF Vulnerabilities	1%

Looking at the geographic distribution of the infected machine we found the following results:

Country	Traffic	Infections
Russian Federation	8,906,025	916,430
Ukraine	609,546	62,722
United States	490,776	50,501
United Kingdom	472,563	48,627
Vietnam	297,414	30,604
Unknown	260,794	26,836
Germany	217,696	22,401
Spain	185,509	19,089
Kazakistan	156,234	16,076
Portugal	144,969	14,917

What Should You do to Protect Yourself From These Attacks?

Cybercriminals are getting smarter and smarter at utilising sophisticated techniques to evade detection by traditional URL filtering and database driven security products. Protecting yourself from these attacks requires innovative Web security products that can scan the Web content you view in real-time for threats.

AVG provides this technology for FREE to anyone who wants it. By [downloading AVG's free product](#) users are equipped with award winning anti-virus software, in addition to the innovative Web security product, AVG LinkScanner® which is available separately for both Windows and Mac based systems.