Australian Government

acma

Australian Communications and Media Authority

ITU

International Training Program 2014

Australian Internet Security Initiative

Julia Cornwell McKean

Australian Internet Security Initiative

- Malware – what is it and what can it do?

Australian Internet Security Initiative

- The AISI – Bot-net mitigation strategy

16 sources of data

Shadowserver

Sorbs

CML

Team Cymru

Microsoft

Australian Internet Security Initiative

- 139 members – Internet Service Providers, educational institutions: covers over 98% of Australian IP space

Australian Internet Security Initiative

- IP address
- Time and date stamp
- Infection type/Category
- Additional information

Australian Internet Security Initiative

Statistics – unique IP addresses with compromises per day

- 2011/12 - 16,517
- 2012/13 - 16,034
- 2013/14 - 25,839

Australian Internet Security Initiative

Zero Access

Click fraud

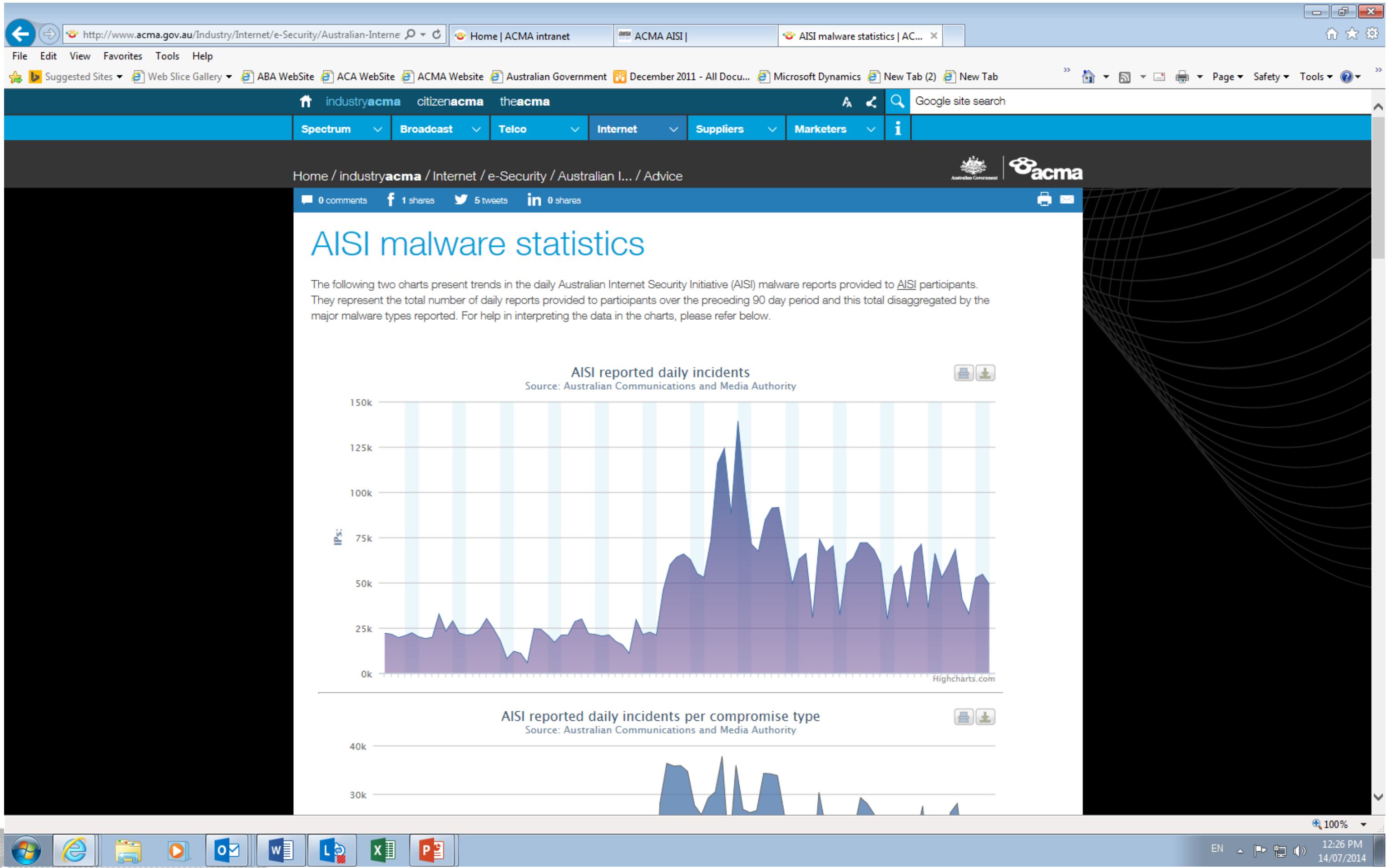
Up to 40% of daily incidents

Zeus

Banking Trojan

Up to 25% of daily incidents

Australian Internet Security Initiative



AISI malware statistics

The following two charts present trends in the daily Australian Internet Security Initiative (AISI) malware reports provided to AISI participants. They represent the total number of daily reports provided to participants over the preceding 90 day period and this total disaggregated by the major malware types reported. For help in interpreting the data in the charts, please refer below.

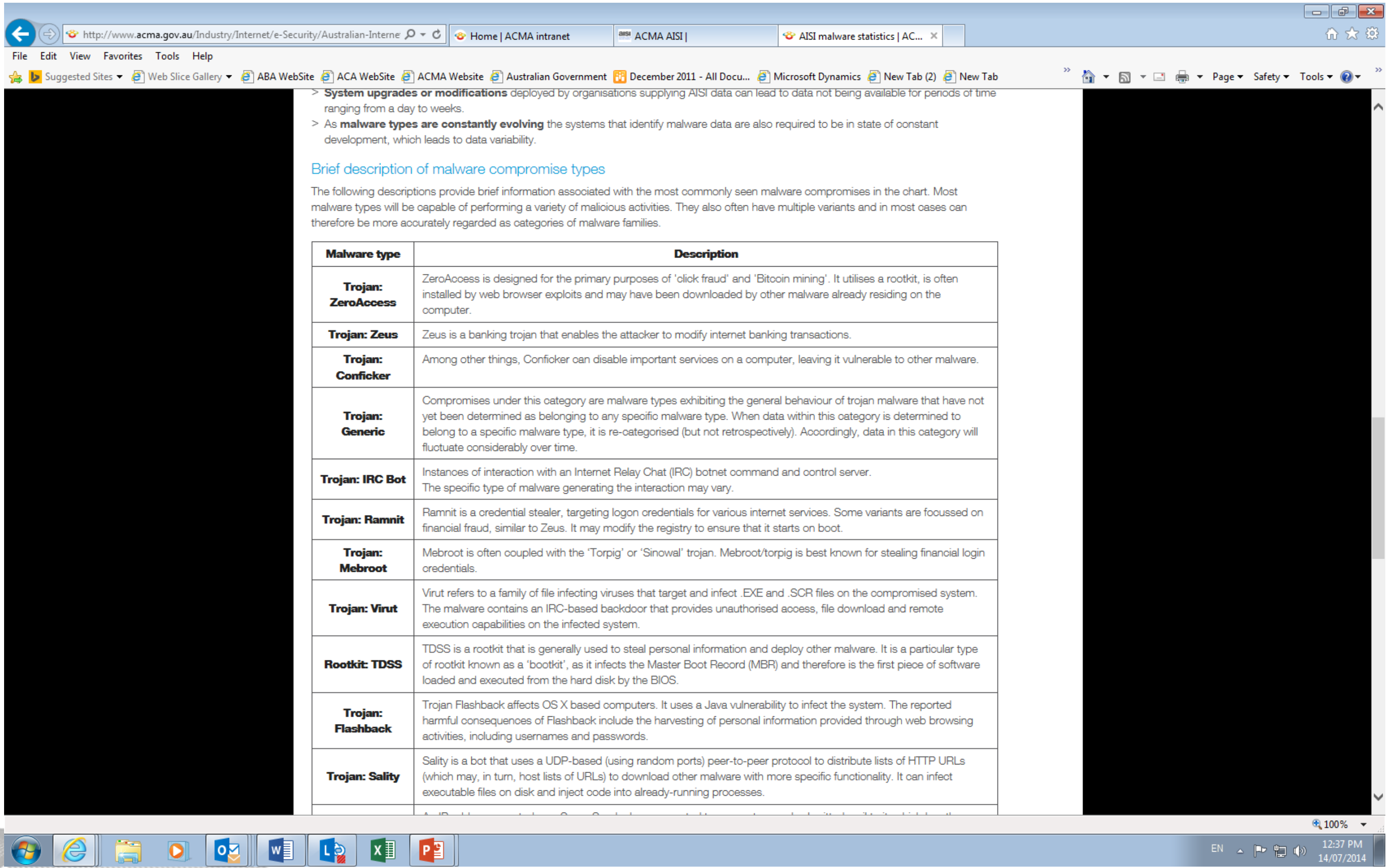
AISI reported daily incidents

Source: Australian Communications and Media Authority

AISI reported daily incidents per compromise type

Source: Australian Communications and Media Authority

Australian Internet Security Initiative



> **System upgrades or modifications** deployed by organisations supplying AISI data can lead to data not being available for periods of time ranging from a day to weeks.

> As **malware types are constantly evolving** the systems that identify malware data are also required to be in state of constant development, which leads to data variability.

Brief description of malware compromise types

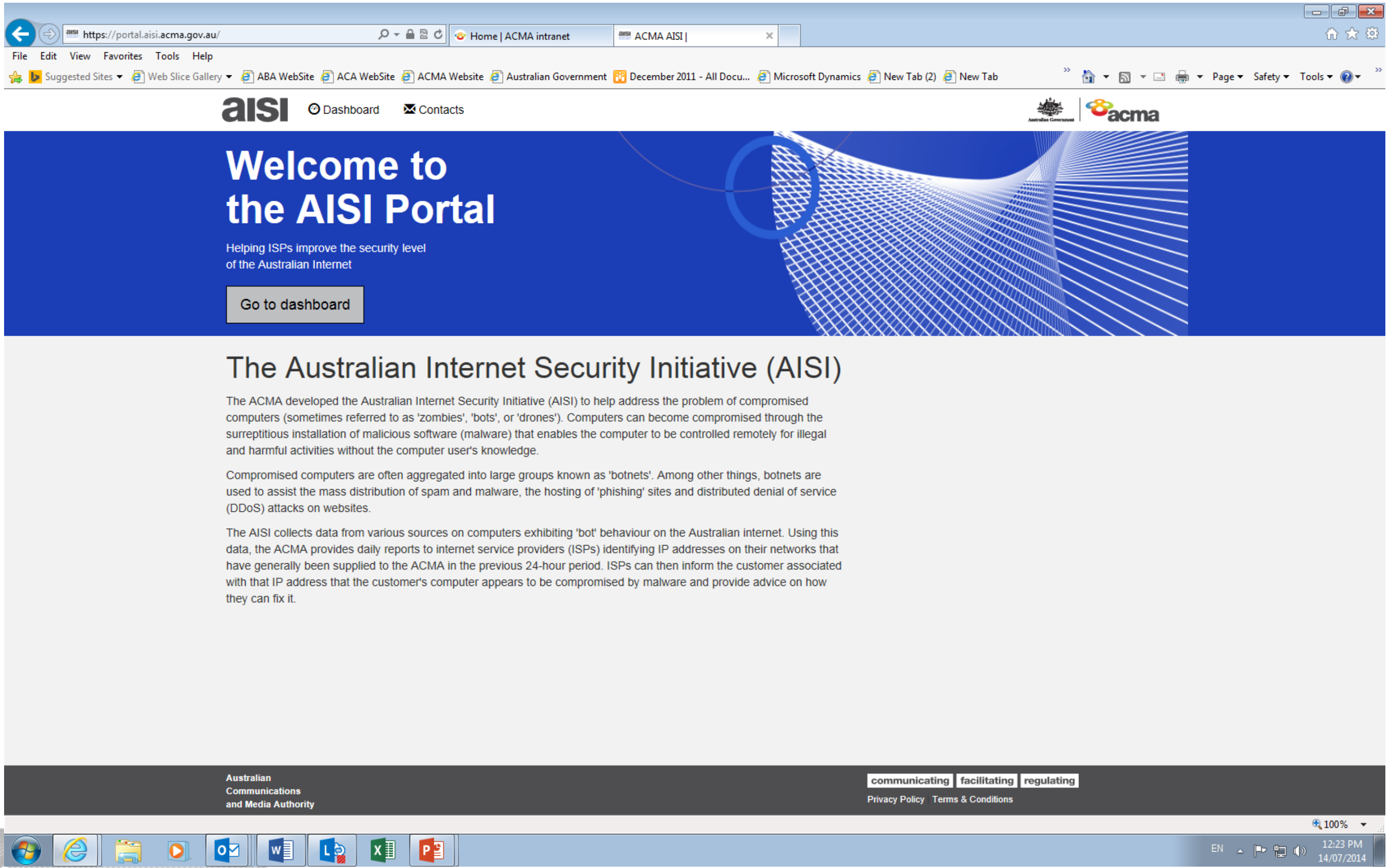
The following descriptions provide brief information associated with the most commonly seen malware compromises in the chart. Most malware types will be capable of performing a variety of malicious activities. They also often have multiple variants and in most cases can therefore be more accurately regarded as categories of malware families.

Malware type	Description
Trojan: ZeroAccess	ZeroAccess is designed for the primary purposes of 'click fraud' and 'Bitcoin mining'. It utilises a rootkit, is often installed by web browser exploits and may have been downloaded by other malware already residing on the computer.
Trojan: Zeus	Zeus is a banking trojan that enables the attacker to modify internet banking transactions.
Trojan: Conficker	Among other things, Conficker can disable important services on a computer, leaving it vulnerable to other malware.
Trojan: Generic	Compromises under this category are malware types exhibiting the general behaviour of trojan malware that have not yet been determined as belonging to any specific malware type. When data within this category is determined to belong to a specific malware type, it is re-categorised (but not retrospectively). Accordingly, data in this category will fluctuate considerably over time.
Trojan: IRC Bot	Instances of interaction with an Internet Relay Chat (IRC) botnet command and control server. The specific type of malware generating the interaction may vary.
Trojan: Ramnit	Ramnit is a credential stealer, targeting logon credentials for various internet services. Some variants are focussed on financial fraud, similar to Zeus. It may modify the registry to ensure that it starts on boot.
Trojan: Mebroot	Mebroot is often coupled with the 'Torpig' or 'Sinowal' trojan. Mebroot/torpig is best known for stealing financial login credentials.
Trojan: Virut	Virut refers to a family of file infecting viruses that target and infect .EXE and .SCR files on the compromised system. The malware contains an IRC-based backdoor that provides unauthorised access, file download and remote execution capabilities on the infected system.
Rootkit: TDSS	TDSS is a rootkit that is generally used to steal personal information and deploy other malware. It is a particular type of rootkit known as a 'bootkit', as it infects the Master Boot Record (MBR) and therefore is the first piece of software loaded and executed from the hard disk by the BIOS.
Trojan: Flashback	Trojan Flashback affects OS X based computers. It uses a Java vulnerability to infect the system. The reported harmful consequences of Flashback include the harvesting of personal information provided through web browsing activities, including usernames and passwords.
Trojan: Sality	Sality is a bot that uses a UDP-based (using random ports) peer-to-peer protocol to distribute lists of HTTP URLs (which may, in turn, host lists of URLs) to download other malware with more specific functionality. It can infect executable files on disk and inject code into already-running processes.

Australian Internet Security Initiative

- AISI 2.0 and the AISI Portal
  - Improved daily reporting
  - Self-service model
  - Enhanced data, including records of all observed infections
  - Searches and reports can be exported

Australian Internet Security Initative



Welcome to the AISI Portal

Helping ISPs improve the security level of the Australian Internet

The Australian Internet Security Initiative (AISI)

The ACMA developed the Australian Internet Security Initiative (AISI) to help address the problem of compromised computers (sometimes referred to as 'zombies', 'bots', or 'drones'). Computers can become compromised through the surreptitious installation of malicious software (malware) that enables the computer to be controlled remotely for illegal and harmful activities without the computer user's knowledge.

Compromised computers are often aggregated into large groups known as 'botnets'. Among other things, botnets are used to assist the mass distribution of spam and malware, the hosting of 'phishing' sites and distributed denial of service (DDoS) attacks on websites.

The AISI collects data from various sources on computers exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to internet service providers (ISPs) identifying IP addresses on their networks that have generally been supplied to the ACMA in the previous 24-hour period. ISPs can then inform the customer associated with that IP address that the customer's computer appears to be compromised by malware and provide advice on how they can fix it.

Australian
Communications
and Media Authority

communicating | facilitating | regulating

Privacy Policy Terms & Conditions

Australian Internet Security Initiative

International Collaboration

- London Action Plan
- ACDC (Europe)