SUNBELT SOFTWARE

Cassava Online Gambling Applications
(Software Review)

Sunbelt Software
Research Center

January 9, 2006

Introduction/Overview

Cassava is a Gibraltar-based company that operates a number of online gambling web sites. Cassava makes and distributes software applications that allow customers to access and use its online gambling services. These gambling applications include:

CasinoOnNet	(888.com, casino-on-net.com, casinoonnet.com)
PacificPoker	(pacificpoker.com)
ReefClubCasino	(reefclubcasino.com)

All of these gambling applications are functionally similar and will be referred to collectively as "Cassava's gambling applications."

Distribution & Installation

Cassava's gambling applications are distributed primarily through Cassava's own web sites. When users land on any of Cassava's main web sites, they are immediately confronted with a prompt to "download our free Casino while browsing the site."

Figure 1: CasinoOnNet install prompt at 888.com

Users who click "OK" are then prompted to download and run a stub downloader to their PCs. When executed, this stub downloader downloads and installs the full casino gambling application from one of Cassava's servers.

What is striking about this installation process is not only the aggressive nature of the install prompts that confront users visiting Cassava's web sites but the fact that at no time during the installation process are users ever affirmatively shown an End User License Agreement (EULA) and Privacy Policy or even presented with a simple description of the functionality and behavior of the software.

Cassava also promotes its gambling applications heavily online, often through aggressive pop-ups that appear at third-party web sites. Even more disturbingly, Cassava has promoted its

gambling applications (primarily CasinoOnNet) through pop-up advertising spawned by adware applications that are known to be installed on users' desktops through security exploits as well as other circumstances in which notice and disclosure is poor to non-existent.

Figure 2: 888.com pop-up ad spawned by TheBestOffersNetworks adware program

Figure 3: 888.com pop-up ad spawned by Surf Sidekick 3 adware program

The adware applications that Cassava has been known to use for advertising include:

- Apropos/ContextPlus
- TheBestOffersNetworks (DirectRevenue)
- eXact Advertising (BargainBuddy)
- Look2Me
- Surf Sidekick 3
- VX2/Transponder

Online help forums such as SpywareInfo.com have been filled with complaints from users about incessant, unwanted pop-up advertising for Cassava's gambling applications appearing on their desktop, even while victims are not surfing the internet. Appendix 1 includes a list of links to sample complaints from adware victims regarding unwanted pop-ups for Cassava's software.

Perhaps the most disturbing of these adware applications known to advertise Cassava's gambling program has been Apropos Media/ContextPlus, which used rootkit technology extensively during the latter part of 2005 to hide its files from users and anti-spyware applications, making detection and removal of this pop-up advertising software extremely difficult if not next to impossible. (1) Apropos/ContextPlus victims typically report that unwanted advertising pops up on their desktops as if out of nowhere, even while Internet Explorer is closed, and that they are unable to locate the software responsible for this unwanted, intrusive pop-up advertising anywhere on their PCs.

Still worse, many of these adware-spawned pop-ups have been known to use the same aggressive installation tactics as seen on Cassava's own web sites (see Figure 3 above). Thus, users may be confronted with a prompt to download and install Cassava's gambling software amidst a blitz of other pop-ups as well as on-going installations of other unrequested software -- circumstances which are not only completely typical of many adware installations but which are entirely confusing to users and that do not lend themselves to gaining the informed consent of users to the installation of software.

It should be noted that in the last few weeks the use of pop-ups that aggressively prompt users to download and install Cassava's software appear to have tapered off. The most recently observed adware pop-ups for Cassava's software do not prompt users to install the software; rather, they require users to affirmatively click through the pop-ups to initiate the installation of Cassava's gambling software.

Nonetheless, the very recent and extensive use of aggressive, intrusive adware pop-up advertising does raise the possibility that some Sunbelt customers might have unwittingly installed the software on their systems.

CasinoOnNet was reportedly bundled with the Grokster P2P file sharing application, however, Sunbelt has not observed any installs of Grokster that included Cassava's software in the past year.

Advertising

None of Cassava's gambling applications display or open third-party advertising on users' desktops.

System Reconfiguration

A full installation of any of Cassava's gambling applications consists of around 60 megabytes of files, most of which are media files of one sort of another (image files and sound files). All files (save shortcuts) are installed to a folder in `\Program Files`. Despite the large number of files dropped on the system, Cassava's gambling applications are fairly non-intrusive. They are not configured by default to start with Windows, nor do they make and changes or additions to Internet Explorer or the PC's network configuration. The performance impact on users' systems while the software is not running is negligible.

Data Collection, Transmission, & Sharing

Users who make use of Cassava's gambling applications to gamble online -- either "for practice" or "for money" -- are required to provide personally identifiable information (PII) in order to register for play.

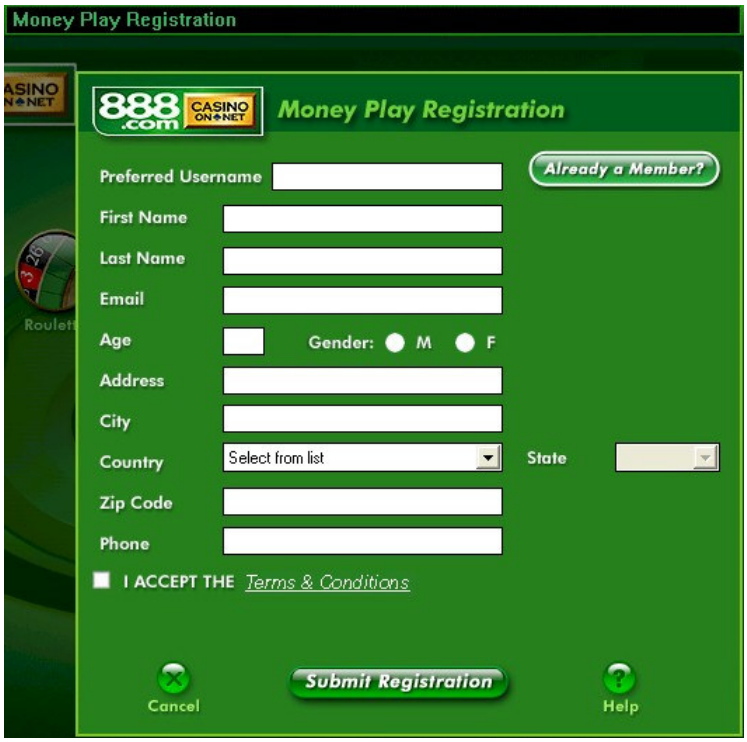

Figure 4: "Money Play Registration" screen

"Money play" registrations understandably require far more PII (including credit card information) than "practice play" registrations.

This collection of PII is perfectly consistent with the voluntary submission of PII by users that would occur with the registration for and/or purchase of other types of online services. There is no evidence that Cassava's gambling applications surreptitiously collect and transmit PII or otherwise track the behavior of users on their computers or online. Moreover, Cassava's data collection and privacy practices are clearly laid out in its privacy policy and EULA:

> Privacy Policy
> http://www.888.com/new888/home.htm?page=fgaprivacy&lang=en
>
> EULA
> http://www.888.com/new888/home.htm?page=aulwarning&lang=en

McAfee reports that Cassava's software does regularly communicate with Cassava's servers both during setup and actual use of the software (2), however, there is no evidence to suggest that these network transmissions consist of PII or other potentially sensitive data from or about users.

Uninstallation

All of Cassava's gambling applications can be uninstalled through an entry in the Add/Remove Programs Control Panel applet. Cassava's uninstallers appear to perform a reasonably complete removal of Cassava's programs.

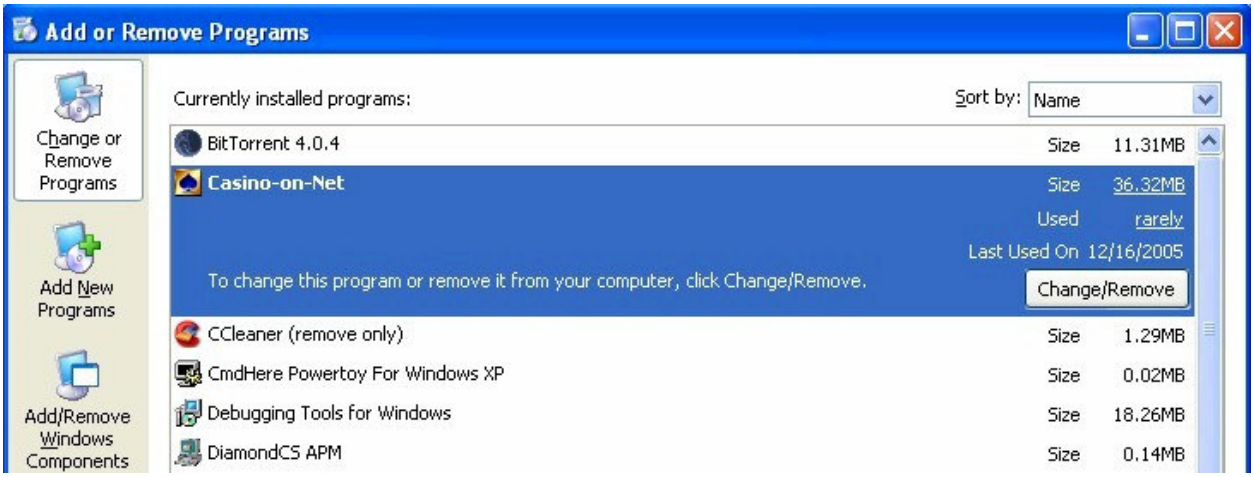

Figure 5: Add/Remove Programs applet

Malware

Cassava's gambling applications are not malware themselves, do not install malware, and are not known to be installed by malware.

Notice, Disclosure, Choice, & Consent

As noted earlier, Cassava's installation practices leave much to be desired. Not only are users never affirmatively shown a EULA or Privacy Policy during installation, but the installation of Cassava's software is often pushed on users through aggressive, incessant pop-up advertising spawned by adware applications that very well may have been installed on users' PCs without proper notice and consent. Moreover, the fact that these pop-ups have been known to employ install prompts that users could mistakenly click through in the confusion of a large adware infestation makes it entirely possible that Cassava's software (most likely CasinoOnNet) could end up on the PCs of Sunbelt customers who never wanted or requested the software.

Sunbelt's Listing Criteria

Cassava's installation practices trip several of Sunbelt's Listing Criteria (http://research.sunbelt-software.com/listing_criteria.cfm):

Distribution & Installation

- installs on users' PCs after providing only substandard, inadequate notice and disclosure, and thus failing to secure users' full, meaningful, and informed consent
- is installed by another functionally separate "adware" program, "spyware" program, or similar program without first providing sufficient notice and choice to users and without securing their full, meaningful, and informed consent
- uses false, misleading, confusing, deceptive, or coercive text or graphics to induce, compel, or cause users to install the software
- uses other installation methods or techniques that most reasonable persons would find objectionable, unfair, misleading, deceptive, or coercive

Notice, Disclosure, Choice, & Consent

- lacks an End User License Agreement and Privacy Policy that is readily accessible before or during installation
- discloses key terms related to advertising, system reconfiguration, and data collection / transmission practices only in an End User License Agreement (EULA) or Privacy Policy or in locations and documents that users are not likely to read during the installation of the software
- uses false, misleading, confusing, deceptive, or coercive text or graphics to induce, compel, or cause users to install the software
- provides notice, disclosure, and choice of such a kind and in such a way that most reasonable persons would find that notice, disclosure, and choice to be inadequate, objectionable, unfair, misleading, deceptive, or coercive

Recommendations

At the time Cassava submitted its request for a software review to Sunbelt, CasinoOnNet was the only gambling application from Cassava to be detected by Sunbelt's CounterSpy anti-spyware

application (setting aside cookies). CasinoOnNet was classified as "Adware," with a threat level of "Elevated" and a default action of "Quarantine."

Given the non-intrusive functionality of CasinoOnNet (as well as Cassava's other gambling applications), this classification is clearly unwarranted. Nonetheless, Cassava's unacceptable installation practices do make Cassava's gambling applications a legitimate detection for Sunbelt to offer its CounterSpy users and customers, given that these installation practices make it possible that users could have unwittingly installed one of Cassava's gambling applications.

Thus, the Sunbelt Research Team recommends the following:

1) Reclassify CasinoOnNet as a "Potentially Unwanted Software," with a threat level of "Low" and a default action of "Ignore."

2) Revise the description of CasinoOnNet in the CounterSpy database to more clearly report the characteristics and behavior of the program.

3) Add Cassava's other gambling applications (PacificPoker, ReefClubCasino) to the CounterSpy database and handle these other applications in the same manner as CasinoOnNet.

In reclassifying Cassava's gambling applications as "Low risk," Sunbelt can continue to offer these detections to users, while still requiring users to affirmatively elect to remove Cassava's gambling applications by changing the selected action in CounterSpy's scan results from "Ignore" to "Quarantine" or "Remove."

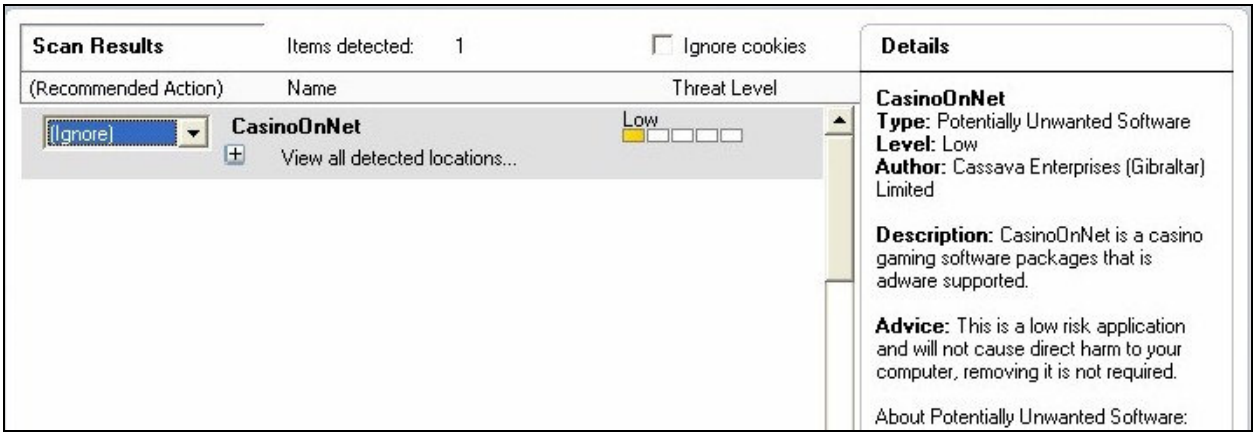

Figure 6: CounterSpy scan results (revised classification)

Users who knowingly installed Cassava's software can continue to use the software without fear that it will be removed by default by CounterSpy, while users who want to remove the software can do so.

At the time of this writing, CasinoOnNet has already been reclassified, and Cassava's other gambling applications are in the process of being added to the database.

Notes:

1. Ryan Narraine. "Where are Rootkits Coming From?" eWeek 7 Dec. 2005. <http://www.eweek.com/article2/0,1895,1897728,00.asp>.

2. McAfee. "CasOnline." <http://vil.nai.com/vil/content/v_133282.htm>.

Appendix 1

Sample complaints from adware victims about unwanted pop-up advertising for Cassava's software on their desktops.

http://castlecops.com/postx137989-0-0.html
http://castlecops.com/t136850-Im_stumped_Spyware_Popups_help.html
http://castlecops.com/t137989-WhenUSave_Cassava_and_other_assortments_of_pop_ups.html
http://www.experts-exchange.com/Miscellaneous/New_Net_Users/Q_21300129.html
http://forums.spywareinfo.com/index.php?showtopic=61144&st=0
http://forums.spywareinfo.com/lofiversion/index.php/t62205.html
http://forums.spywareinfo.com/index.php?showtopic=63189
http://forums.spywareinfo.com/index.php?showtopic=61505
http://forums.spywareinfo.com/index.php?showtopic=62563
http://forums.spywareinfo.com/index.php?showtopic=59841
http://forums.spywareinfo.com/index.php?showtopic=62444
http://forums.spywareinfo.com/index.php?showtopic=62428
http://forums.spywareinfo.com/index.php?showtopic=61144
http://forums.spywareinfo.com/index.php?showtopic=60879
http://forums.spywareinfo.com/index.php?showtopic=64789
http://forums.subratam.org/index.php?showtopic=5941
http://www.geekstogo.com/forum/index.php?showtopic=80409
http://spywarewarrior.com/viewtopic.php?p=104730
http://www.computing.net/windowsme/wwwboard/forum/44227.html

Ben Edelman has documented Cassava's use of eXact Advertising's adware applications to advertise its gambling applications:

eXact Advertising Ads: Gambling
http://www.benedelman.org/spyware/exact-advertisers/ads-gambling.html

CounterExploitation reports that Cassava's gambling applications were advertised through a predecessor to DirectRevenue's BestOffersNetworks application, VX2:

Advertising Spyware: Blackstone Data Transponder and its derivatives
http://www.cexx.org/vx2.htm

Eric L. Howes
Jan. 9, 2006

About Sunbelt Software

Headquartered in Tampa Bay (Clearwater), Fla., Sunbelt Software was founded in 1994 and offers products to protect and secure systems from costly inefficiencies including spam and spyware; as well as enterprise solutions to protect against system downtime and security vulnerabilities.

Sunbelt Software is part of the Sunbelt International Group, which includes Sunbelt Software, Inc. and Sunbelt System Software in Europe. The Sunbelt System Software group has offices in the UK, France, Netherlands, Sweden and Germany.

Primary Media Contacts

Laurie Murrell
lauriem@sunbelt-software.com
888-NT UTILS (688-8457)
Marketing Communications Manager
Sunbelt Software

Heather Kelly
heather@sspr.com
719-634-8274
S&S Public Relations for Sunbelt Software

Jason Ovitt
jovitt@sspr.com
847-415-9326
S&S Public Relations for Sunbelt Software