

The UrSnif Family

By Ken Dunham – ISSA member, Boise, ID, USA chapter



UrSnif is a little known malcode family of growing importance in the wild, launching attacks since 2006. It is also known as Papras and Snifula and generically referred to as variants of NTrootkit and Agent. The group behind UrSnif attacks to date is well-organized. Additionally, they have included functionality as a rootkit to sniff network traffic enabling the malcode to jump out of a traditional VMware environment to steal network data from the host machine.

The first notable attack by the UrSnif group took place with Vector Markup Language (VML) attacks in September 2006. VML was a huge exploitation incident at the time, quickly capitalized upon by criminals using the Russian Business Network (RBN) for hosting of remote command and control servers at the time. This first attack proved that a new sophisticated group with important code capabilities was now involved with rapid exploitation of new vulnerabilities in the wild.

The group then struck during another notable period about one year after VML attacks, striking against vulnerabilities in Adobe products in the fall of 2007. During this time unspecified vulnerabilities in Adobe Acrobat and Adobe Acrobat Reader 8.1 (CVE-2007-5020) emerged. Just one day after a patch was released in late October, UrSnif attacks began in the wild. Most computers were not patched at the time, resulting in many infections throughout the fall of 2007. Fall 2007 attacks resulted in the installation of two Windows rootkit files. Shortly after this attack, in November 2007, the RBN was taken offline by upstream providers via public pressure applied to the group over an extended

period of time by multiple security-related organizations and the media.

In 2008 UrSnif attacks have continued as under-the-radar threats regularly distributed in the wild. However, tactics of the group have notably changed. In 2008 emails have been sent to users claiming to be from Comercia Bank asking them to identify their identity with a certificate. Users that followed a link provided in the email were directed to a website that prompted them to download “DC Loader Wizard.” Installation of this code results in the installation of a UrSnif Trojan.

Around the same time frame emails claiming to be from CareerBuilder have been sent out to users claiming to be a “System Update.” Users are told that CareerBuilder offers the ability to sign in using Microsoft Windows Live ID Certification service, with a link titled “Setup Wizard Review.” The HTML of this email sports a yellow background, as seen with others from the group in August and September 2008. By the end of September 2008 similar emails are sent out but with a different background color, changing content filtering options for individuals attempting to block such content.

One of the attacks analyzed in 2008 install files named 9129837.exe and new_drv.sys on a computer. They also modify the Windows registry in multiple locations to install as a rootkit, as a service, and in the standard “Run” directory on the host to run upon Windows startup. In this attack it uses a mutex “__RHaiuy72Mjtex.” The remote C&C is located at pull.dolcebrava.com (124.217.249.5), hosted in Malaysia at the time of attack. CGI scripts are used

to communicate with the remote C&C. Uploads of stolen data are sent in real time to the remote server via a forms.cgi packet. Filenames and C&C servers vary throughout the year with this group continually maturing their attacks and changing each wave of code for maximum success in the wild.

Little is known about the group behind UrSnif attacks to date. They have operated mostly under the radar for at least two years. It is troubling that they have successfully exploited rather rapidly VML and PDF vulnerabilities two years in a row. Now it appears the group is moving towards more of a social engineering approach when vulnerability vectors are not as readily available. One of the former C&Cs used in attacks, while affiliated with the RBN, correlates to former Animated Cursor (ANI) exploitation and CoolWebSearch (CWS) adware abuse. It is possible that the two are related not just by RBN services but authored by the same group.

About the Author

Ken Dunham has more than a decade of experience on the front lines of information security. As Director of Global Response for iSIGHT Partners, he oversees all global cyberthreat response and malcode research operations. He frequently briefs upper levels of federal and private-sector cybersecurity authorities on emerging threats, and regularly interfaces with vulnerability and geopolitical experts to assemble comprehensive malicious code intelligence and to inform the media of significant cyberthreats. He can be reached at ken@kendunham.org.