# How Turla and "worst breach of U.S. military computers in history" are connected

**Abingdon, 12 March 2014**

Experts from G-Data and BAE Systems recently released information about a persistent cyber espionage operation codenamed Turla (also referred to as Snake or Uroburos). Further to this, Kaspersky Lab's research and analysis team have now found an unexpected connection between Turla and an existing piece of malware known as Agent.BTZ.

In 2008, Agent.BTZ infected the local networks of the United States Central Command in the Middle East, and was called at the time the 'worst breach of U.S. military computers in history'. It took specialists at the Pentagon some 14 months to completely disinfect Agent.BTZ from military networks, and it was this experience that lead to the creation of the US Cyber Command. The worm, thought to have been created around 2007, has the ability to scan computers for sensitive information and send data to a remote command and control server.

**Source of inspiration**

Kaspersky Lab first became aware of the Turla cyber espionage campaign in March 2013, when the company's experts were investigating an incident involving a highly sophisticated rootkit. Originally known as the 'Sun rootkit', based on a filename used as a virtual file system 'sunstore.dmp', it is also accessible as '\\.\Sundrive1' and '\\.\Sundrive2'. The 'Sun rootkit' and Snake are in fact one and the same.

It was during this research that Kaspersky Lab's experts found some interesting links between Turla, a highly sophisticated, multifunctional program and Agent.btz. The Agent.btz worm seems to have served as an inspiration for the creation of a range of the most sophisticated cyber espionage tools to date, including Red October, Turla and Flame/Gauss:

- **Red October** developers clearly knew about Agent.btz's functionality as their USB Stealer module (created in 2010-2011) searches for the worm's data containers ('mssysmgr.ocx' and 'thumb.dd' files) which hold information about infected systems and activity logs, and then steal it from the connected USB drives.
- **Turla** uses the same file names for its logs ('mswmpdat.tlb', 'winview.ocx' and 'wmcache.nld') whilst stored in the infected system, and the same XOR key for encrypting its log files as Agent.btz.
- **Flame/Gauss** use similar naming conventions such as '*.ocx' files and 'thumb*.db'. Also, they use the USB drive as a container for stolen data.

**A question of attribution**

Considering these facts, it is obvious that developers of the four cyber espionage campaigns studied Agent.btz in detail to understand how it works, the file names it uses, and used this information as a

model for the development of the malware programs, all of which had similar goals. But does this mean that there is a direct link between developers of these cyber espionage tools?

“It is not possible to draw such a conclusion based on these facts alone”- says Aleks Gostev, Chief Security Expert at Kaspersky Lab. “The information used by developers was publicly known at the time of Red October and Flame/Gauss’ creation. It is no secret that Agent.btz used ‘thumb.dd’ as a container file to collect information from infected systems and in addition, the XOR key used by the developers of Turla and Agent.btz to encrypt their log files was also published in 2008. We do not know when this key was first used in Turla, but we can see it for certain in the latest samples of the malware, which were created around 2013-2014. At the same time, there is some evidence which points towards Turla's development starting in 2006 – before any known sample of Agent.btz; which leaves the question open.”

**Agent.btz – to be continued?**

There have been numerous modifications of the Agent.btz worm. Today, our products detect all of its forms within the main verdict of Worm.Win32.Orbina. Due to its replication method (via USB flash drives) it has become widespread globally. From Kaspersky Lab's data it is possible to see that in 2013, Agent.btz was discovered on 13,800 systems across 100 countries. This leads us to conclude that there are probably tens thousands of USB drives around the world infected with Agent.btz, containing the ‘thumb.dd’ file with information about infected systems.

Read more details at Securelist.com.

## About Kaspersky Lab

*Kaspersky Lab is the world’s largest privately held vendor of endpoint protection solutions. The company is ranked among the world’s top four vendors of security solutions for endpoint users*. Throughout its more than 16-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide. Learn more at www.kaspersky.com.*

---

** The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.*