



The 31 page Damballa report titled “The Command Structure of the Aurora Botnet: History, Patterns and Findings,” reveals that most of what has been reported to-date understates the breadth and ordinariness of the attack. Key findings include:

- At the time the attack was first noticed by Google in December 2009, systems within at least seven countries had already been affected. By the time Google made the public disclosure of the attack on January 12, 2010, systems in over 22 countries had been affected and were attempting to contact the CnC servers - the top five countries being the United States, China, Germany, Taiwan and the United Kingdom.
- The Trojan.Hydraq malware, which has been previously identified as the primary malware used by the attackers, is actually a later staging of a series of malware used in the attacks which consisted of at least three different malware ‘families’. Two additional families of malware (and their evolutionary variants) have been identified, and they were deployed using fake antivirus infection messages tricking the victim into installing the malicious botnet agents.
- The attacks that eventually targeted Google can be traced back to July 2009, with what appears to be the first testing of the botnet by its criminal operators. The analysis identifies the various CnC testing, deployment, management and shutdown phases of the botnet CnC channels.
- The botnets used dozens of domains in diverse Dynamic DNS networks for CnC. Some of the botnets focused on victims outside of Google, suggesting that each set of domains might have been dedicated to a distinct class or vertical of victims.
- Some of the CnC domains appear to have been dormant for a period of time after they had infected a number of victim systems. This can occur after the botnet operator has updated the botnet malware with new (more powerful) variants or when the criminal operator sells/trades a segment of the botnet to another criminal operator.
- There were network artifacts that suggest that the botnet malware operating with the US-based victims’ networks made use of email services to extract the stolen data from the breached organizations.
- There is evidence that there were multiple criminal operators involved, and that the botnet operators were of an amateur level. The botnet has a simple command topology and makes extensive use of Dynamic DNS CnC techniques. The construction of the botnet would be classed as “old-school”, and is rarely used by professional botnet criminal operators today.

“Trojan.Hydraq would have been just another piece of dumb malicious software if it did not have the ability to connect to a CnC server and receive new instructions or allow its criminal operators interactive control over its victims,” states Ollmann. “CnC infrastructure is the critical element in all botnet campaigns.”

“Our team published this report to alert enterprises as to the pervasive and relentless nature of botnets and APTs,” said Val Rahmani, CEO at Damballa. “It is essential that corporations understand the origin and elements of these criminal operators to better arm themselves against these attacks. It is clear that traditional defense-in-depth measures,

even those taken by some of the most advanced companies in the world, are incapable of stopping these criminal operators. At Damballa, we have demonstrated that the only way to ensure that these threats are contained is to detect and terminate malicious command-and-control activity.”

The Damballa research paper can be downloaded at:

<http://www.damballa.com/research/aurora>.

**About Damballa, Inc.**

Damballa stops crimeware threats that exploit enterprise networks by finding and disrupting the hidden communications channels used to control internal assets. By focusing on malicious remote control, Damballa solutions identify advanced network threats, terminate criminal activity and provide remediation guidance. Damballa customers include major banks, Internet service providers, government agencies, educational organizations, manufacturers and other companies typically targeted by organized cybercrime. Privately held, Damballa is headquartered in Atlanta, GA.

###