Computer scientist forges new line of defense against malicious traffic

November 5 2007

Paul Barford has watched malicious traffic on the Internet evolve from childish pranks to a billion-dollar "shadow industry" in the last decade, and his profession has largely been one step behind the bad guys.

Viruses, phishing scams, worms and spyware are only the beginning, he says.

"Some of the most worrisome threats today are things called 'botnets' - computers that are taken over by an outside party and are beyond the user's control," says Barford, a computer scientist at the University of Wisconsin-Madison. "They can do all sorts of nasty things: steal passwords, credit card numbers and personal information, and use the infected machine to forward spam and attack other machines.

"Botnets represent a convergence of all of the other threats that have existed for some time," he adds.

One of the most menacing aspects of botnets is that they can go largely undetected by the owner of a personal computer. That feature has allowed botnets to grow exponentially online, with millions of infected computers bought and traded on an underground market that one security company estimates has surpassed $1 billion in activity, Barford says.

Motivated by this growing threat, Barford is developing a new technology that may head off hackers at the pass.

In June 2007, Barford and colleagues opened a spinoff company at the MG&E Innovation Center of University Research Park called Nemean Networks, LLC. The company is developing a new approach to detecting network intrusions that offers a significant improvement over the current state of the art. Nemean is based on four distinct patents that are either filed or are in process with the Wisconsin Alumni Research Foundation (WARF).

Nemean is named after the first of Hercules' 12 labors, in which Hercules must kill the Nemean lion whose coat was impenetrable by weapons. It's an apt metaphor for the technology, which seeks to hunt down a slight vulnerability in malicious traffic: the unique "signature" such traffic generates.

Most network-intrusion systems today are comparing traffic against a database, collected by hand, of previously recognized attack signatures. The innovation with Nemean is a method to automatically generate intrusion signatures, making the detection process faster and more precise.

The Achilles' heel of current commercial technology is the number of false positives they generate, Barford says. Hackers have become so adept at disguising malicious traffic to look benign, security systems now generate literally thousands of false positives for each genuine intrusion they find. Nemean virtually eliminates false positives.

In a test comparing Nemean against a current technology on the market, both had a high detection rate of malicious signatures - 99.9 percent for Nemean and 99.7 for the comparison technology. However, Nemean had zero false positives, compared to 88,000 generated by the other technology during the same time frame.

"The technology we're developing here really has the potential to

transform the face of network security," says Barford. "Our objective is to build this company into a world leader in network security solutions."

Barford's research is supported by the National Science Foundation, the Army Research Office and the Department of Homeland Security. Nemean was developed and tested on the Wisconsin Advanced Internet Laboratory (WAIL), a unique test bed for examining complex behavior on the Internet. WAIL provides researchers with a microcosm of the Internet, allowing them to study security, speed, efficiency of transfer and other Internet issues. Funded by Cisco Systems CEO John Morgridge, WAIL is a computer science parallel to the model organism in biology.

While Barford has high hopes for Nemean, he says Internet security is a continuous process and there will never be a single cure-all to the problem. "This is an arms race and we're always one step behind," he says. "We have to cover all the vulnerabilities. The bad guys only have to find one."

Nemean is funded by an angel investment group composed of UW-Madison alumni who are working to foster technology transfer from the campus. The company also is working in close partnership with the Department of Information Technology (DOIT) at UW-Madison to test and evaluate the research prototype version of its first product.

Source: UW-Madison