Hackers Reveal Underground Digital Threats Targeting Financial Industry at HackMiami 2013 Conference

Malware research scientist Christopher Elisan will demonstrate how new configuration and obfuscation techniques can be used on well known financial malware suites to bypass even the most updated antivirus protection.

Miami Beach, FL (PRWEB) April 24, 2013

Hackers and information security professionals are scheduled to speak in Miami Beach, Florida about the latest threat intelligence regarding the evolution of sophisticated banking malware campaigns. The HackMiami 2013 Hackers Conference will take place on May 17-19, 2013, at the Miami Beach Holiday Inn Oceanfront Hotel.

HackMiami 2013 Hackers Conference
May 17-19, 2013

"The public availability of these formerly proprietary crimeware suites has provided a new marketplace for underground coders to develop and sell obfuscation tools, modules and plugins."

Malware research scientist Christopher Elisan will demonstrate how new configuration and obfuscation techniques can be used on well known malware suites to bypass even the most updated antivirus protection. Elisan is the author of, "Malware, Rootkits & Botnets, A Beginner's Guide." Elisan will demonstrate how banking malware suites such as Zeus and SpyEye are still being used to this day to infect corporate enterprise workstations on a mass scale.

These families of financial malware have plagued online banking users for years, despite prolifically available virus signatures and publicly available leaked source code. Elisan will discuss how the creation, obfuscation, and deployment of crimeware payloads can be automated to evade detection.

Elisan explains, "As detailed in my book, the availability of leaked crimeware kits makes it easy for researchers and reverse engineers to understand the inner workings of the kits, as well as assist in the formulation of solutions. On the other hand, attackers can modify and even improve these kits and use them on their attack campaign or resell them under a different name."

An example of this is the Zeus Trojan, which had its complete source code was leaked in 2011. Since then, it has spawned proprietary licensed incarnations such as ICE IX. The same is true of SpyEye, which had its source code leaked in 2011.

"The public availability of these formerly proprietary crimeware suites has provided a new marketplace for underground coders to develop and sell obfuscation tools, modules and plugins," stated Alex Heid, President of HackMiami. "The exposure allows the underground ecosystem to learn from itself, so when one family of malware may go obsolete, either by a leak, technical flaw, or takedown action, dozens more be ready and waiting to replace it."

Crimeware kits such as Zeus, SpyEye, and ICE IX provide an incredibly simple way for hackers and other malicious actors to build silent botnets which give no indication of infection to the end user. Mean-

while, the botnet administrator is able to obtain credit cards data, usernames, passwords, and most importantly, the credentials needed to activate international wire transfers.

Modern criminals are still taking advantage of traditional signature based detection methods in use by modern antivirus software for evasion, while at the same time taking advantage of increasingly sophisticated client side exploitation methodologies as vectors for infection.

These forms of financial malware campaigns are also migrating into the mobile arena. In addition to Christopher Elisan's talk about malware automation and obfuscation, the HackMiami 2013 Hackers Conference will also feature content that delves into how mobile operating systems and browsers are exploited and leveraged in these types of campaigns.

About HackMiami 2013 Hackers Conference

The HackMiami 2013 Hackers Conference seeks to bring together the brightest minds within the information security industry and the digital underground. This conference will showcase cutting edge hacking tools, techniques, and methodologies that are at the forefront of the global threatscape.

This hacking conference features three days of multiple tracks, comprehensive all day training courses, competitive tournaments, and informational events. Tickets for the conference and trainings are now available at HackMiami.com. In addition to credit cards and other standard payment methods, the HackMiami 2013 Conference is the first hacker conference to accept Bitcoin as an alternative form of payment.

About HackMiami

HackMiami is the premier resource in South Florida for highly skilled hackers that specialize in vulnerability analysis, penetration testing, digital forensics, and all manner of information technology and security. Members of HackMiami have been involved in the research projects regarding the Zeus trojan as far back as 2009.

HackMiami seeks to develop and harness the participation of the information security community through regular events, presentations, labs, and competitions. These events allow the hacker community a forum in which to present their research, develop new techniques and methodologies and at the same time provides a valuable networking resource for contracting opportunities.

MEDIA CONTACT:
HackMiami Media Desk
info@HackMiami.com
https://www.hackmiami.com
Twitter: @hackmiami
Telephone: 786-505-4225