Agenda Item 2

Featured Start-Up – SecondWrite, LLC
**TOPIC:** Featured Start-Up – SecondWrite, LLC (information item)

**COMMITTEE:** Economic Development and Technology Commercialization

**DATE OF COMMITTEE MEETING:** June 19, 2014

**SUMMARY:** SecondWrite, a company founded by a faculty member from UMCP, has been selected as the featured start-up for the June 19th Committee meeting. Its technology improves computer performance and security.

SecondWrite, LLC, has licensed the first static binary rewriting technology that rewrites binaries without relocation of symbolic information. The software provides wholesale recompilation of the binary including redoing register allocation and instruction selection. The resulting advantages of this novel static binary rewriter are rewriting 100% of binary code with relatively no run-time increase, enforcing security on untrustworthy program codes, bypassing malicious codes hidden in the software, and rewriting obfuscated binary code, thereby preventing future obfuscator use.

**ALTERNATIVE(S):** This item is for information purposes.

**FISCAL IMPACT:** This item is for information purposes.

**CHANCELLOR’S RECOMMENDATION:** This item is for information purposes.

---

**COMMITTEE RECOMMENDATION:**

---

**BOARD ACTION:**

---

**SUBMITTED BY:** Joseph F. Vivona (301) 445-2783
Corporate summary

SecondWrite LLC
June 3, 2014
Company Background

Summary
Spinoff from University of Maryland, College Park
Result of six years of research at UMD
Active operations started July, 2013

Team
Dr Rajeev Barua, CEO
Dr Kapil Anand, CTO
Satish Tamboli, Business Mentor

Advisory Board
Ron Gula, Founder & CEO, Tenable Networks
Rajesh Radhakrishnan, Vice President Application & BPO Services, Americas, HP
Srini Mantripragada, EIR, Foundation Capital

Funding

Markets
Application Performance Monitoring (APM)
Malware Detection
Need for APM in real-world

The average cost per minute increased 41 percent from:

- $5,617 in 2010 to $7,908 in 2013

Ponemon Institute

Online brokerage applications lose $6.4 million for every hour of downtime

Credit card applications lose $2.6 million for every hour of downtime

By: TechCrunch
February 15, 2013 at 00:30 AM EST

Heroku Admits To Performance Degradation Over The Past 3 Years After Criticism From Rap Genius

Thomas Cook: Boosting Online Sales with Performance Monitoring
Leading Travel Services Website Proves the Value of APM

As a result, travel bookings have increased by 30 percent time it takes for problem resolution has been reduced by 97 percent — from 48 hours down to two hours — and the volume of online customer service calls has been cut in half.

apmdigest.com
What is APM?

**GOALS**
- Automatically detect slowdowns and timeouts.
- Automatically pin-point the location of the problem.

**MARKET**
- $2.1 B/year
- $4-5 B/year in next 5 years

**EXISTING SOLUTIONS**
- Only supports interpreted code
  - JAVA, .NET
- No visibility inside binary code
  - C, C++
Multi-tier: Lack of binary code APM

- Application Front-end
- Web Server
- Application Processing
- Data-Bas Processing

Transaction Tracking
Deep-dive Monitoring

Client
Application
Data
Binary Code

Modern Languages with binary mode

Infrastructure Components

Libraries

Language Interpreters

Custom Applications
RapidWrite™: Change binary code during execution

X-ray vision into binary applications

[Patent Pending 2014]
APM Flow Diagram

Dr. Dobb's the world of software development, “Application Monitoring In Complex Multi-Tier Worlds”
The challenge of malware

“$250 billion annual loss to American companies”
Gen. Keith Alexander, NSA Director

“Less than 60% of cyberattacks are stopped”
Taher Elgamal, CTO SalesForce

“Enterprise security market is $9.6 billion/year”
IBIS Report
Sandbox-based detection

Isolated Sandbox Environment

Network Traffic

Unknown Software

Malware detection engine

SAFE

Live System
Leading vendors using Sandbox

- FireEye
- TRENDS MICRO
- DAMBALLA
- lastline
- FORTINET
- cyberpoint
- AhnLab
- norman
- CYPHORT
- Check Point
- McAfee
- paloalto NETWORKS
- GFI
- ThreatGRID
Problem with Sandboxing: Evasive Malware

Isolated Sandbox Environment

Network Traffic → Malware detection engine → SAFE

Live System
Evasive Mechanism

- SLEEP
- USER INPUT
- TIMEBOMB
- ANTI-VM
Evasive malware in the News!

South Korea Cyber Attacks Used Data-Wiping Trojan, Component to Wipe Linux Machines

“Hastati ....activates itself at 2 PM on March 20, 2013. If the sample is monitored in a file-based sandbox before that time and date, it does not execute, evading detection” - FireEye [March 20, 2013]

Trojan Nap Employs Extended Sleep Calls to Neglect Detection by FireEye

“Through prolonged sleep calls - till 10 minutes against the normal few seconds, the Trojan neglect tripping automated examining systems” [Feb 14, 2013]

Trojan Upclicker ties malware to the mouse

“..large-scale “sandbox”-style automated research and malware analysis tools don’t evaluate mouse interactions, hiding there is a convenient way for the malicious code” [Dec 17, 2012]
Anti-evasive tool

“Lie detector for malware”

Initial phase

Malware detection

Monitoring tool

Malware

Analysis phase

Unexplored path determination

Proprietary heuristics to reduce code paths

Path exploration phase

Force execution

Paths to be explored

Sandbox

Malware path 1

Sandbox

Malware path 2

Sandbox

Malware path 3
Thank you!

barua@secondwrite.com