
Moderator
Tim Williams
Vice Chairman
Pinkerton Global Security Services

Panelist
Kevin O’Brien
Director, Global Data Center Security
Google

Panelist
Dave Tyson
CEO
CISO Insights
SNG
SECURING NEW GROUND
SIA EXECUTIVE CONFERENCE | OCT. 26 – 27 | NEW YORK
#SIASNG17
The Cyber Evolution: What You Need to Know

John McClurg
Vice President in the Office of Security and Trust (OST), Cylance / former CSO of Dell
“May you Live in Interesting Times”

Old Chinese Curse
Traditional boundaries of interest grow ever more porous

- Cyber / Physical
- Domestic / International
- Public / Private
- Church / State
- Business / Security
With increasing connectivity comes an increase in the number of Threat Vectors, Avenues of Attack, open to an adversary.
Proactive Prevention

Versus

Reactive Detection

“The fence at the top of the cliff or the ambulance at the bottom.”
“Those who cannot remember the past are condemned to repeat it.”

George Santayana
A lesson from the Past – WWII V-Weapons Defense Strategies

Proactive Prevention
Operation Crossbow
Reaping the Reactive Life:

Counterterrorism – Lockerbie, Oklahoma City, Unabomber
Pheakers & Hackers – Dark Dante
Counterespionage - Harold “Jim” Nicholson
Corporate Life – “Not If But When”
Elaborate “Defense In Depth” Structures
  Complex
  Costly
  Reactive: Post-execution

A call for new paradigms
Emergence of the Proactively Predictive:

Snowden
US Government Requirement – Viable Trusted Insider Program
Big Data Analytics – AI’s Machine Learning & Mathematical Algorithms

We Had To Do Better
“Their Spies!”
Reactive Detection Versus Prevention

Reactive Detection
• “Big Data” problem: Early indicators too numerous and distributed, across too many repositories

Prevention
• Software that allows us to pull data into algorithms that could be fed from numerous repositories across diverse environment
Security

No longer a *distasteful* cost of doing business; Now an indispensable and inextricable *aspect* of advancing it.

No longer just the guns, gates, guards, and geeks of yesterday; Now a duty owned by all.
Wetware: Individual Users

- Spear-phishing draped in “Beguiling Specificity”

“Here’s a picture of your daughter kicking the winning goal at last Saturday’s soccer game!”

Malware embedded
Not if, but when...

1) How well are critical assets identified
2) Enclaved those assets
3) Detected the compromise
4) Contained it
5) Expelled it
6) Leverage new insights gained

Only 19% Detected
No more sacrificing at least one endpoint or employee’s computer for the greater good—for the creation of a signature---NO MORE SACRIFICIAL LAMBS.
March 2015

I still remember that day...

460 had never been seen by commodity antivirus or virus listing sites

3,700 total pieces of malware
THE RESULTS

Res Ipsa Loquitor

\[
\frac{12}{4,160} = 99.7\%
\]

EFFICACY
How it Works

Determine if a file is good or bad purely on the information contained in the file replicated on a sustainable massive scale.

Patterns have emerged of how specific files are constructed.

Prediction based on properties learned from earlier data to differentiate malicious files from safe ones.

99.7% Effective

Humans are simply incapable.
Proactively Predictive: AI’s Machine Learning

- ML is a type of artificial intelligence (AI) that provides computers with the ability to learn—without being explicitly programmed, without the assistance or intervention of humans.

- AI provides the opportunity to develop pre-execution, malware prevention—more disruptive than anything I’ve seen in the last two decades.
Having mapped the genomic structure of the files making up the internet, We make software that predicts, then blocks Cyberattacks, on the endpoint, in real time, using pre-execution artificial intelligence algorithms.
Well...It’s Groundhog Day again?!
THE Groundhog is Dead!

Battling the entrenched security paradigm of the last two decades
The dawn of a new age!
A Paradigm Shift...Galileo Lives Again!
“Prove for one’s self.”
“May you Live in Interesting Times”

A New Paradigm Benediction
QUESTIONS AND ANSWERS

JOHN E McCLURG | VP & AMBASSADOR-AT-LARGE
jmcclurg@Cylance.com