Zacks Small-Cap Research

September 16, 2014

Lisa Thompson
312-265-9154
lthompson@zacks.com

scr.zacks.com

10 S. Riverside Plaza, Chicago, IL 60606

Finjan Holdings (FNJN-NASDAQ)

FNJN: Zacks Company Report – INITIATION Finjan: A Pure Play in Cybersecurity Licensing

Current Recommendation	**Buy**
Prior Recommendation	N/A
Date of Last Change	9/15/2014
Current Price (09/15/14)	$4.26
Target Price	**$5.80**

OUTLOOK

Finjan Holdings, Inc. is an entity that was created last year to enforce the patents of Finjan Inc., a former cybersecurity vendor from Israel founded in 1997. This new company is pursuing licensing arrangements and/or suing current vendors of cybersecurity hardware and software products it believes infringe upon its patents. The former company was a pioneer in a number of foundational attack prevention technologies such as anti-malware and sandboxing. We believe the company could begin to generate revenues by the end of the year either through a new licensing arrangement, or settlement of one or more of its current lawsuits.

SUMMARY DATA

52-Week High	**$12.61**
52-Week Low	**$3.32**
One-Year Return (%)	**-34.3**
Beta	**0.09**
Average Daily Volume (sh)	**6,449**
Shares Outstanding (mil)	**22**
Market Capitalization ($mil)	**$95**
Short Interest Ratio (days)	**2.08**
Institutional Ownership (%)	**9**
Insider Ownership (%)	**29**
Annual Cash Dividend	**$0.00**
Dividend Yield (%)	**0.00**
5-Yr. Historical Growth Rates	
Sales (%)	**-13.9**
Earnings Per Share (%)	**N/A**
Dividend (%)	**N/A**
P/E using TTM EPS	**N/A**
P/E using 2014 Estimate	**N/A**
P/E using 2015 Estimate	**7.3**
Zacks Rank	**N/A**

Risk Level	**Very High**
Type of Stock	**Small-Growth**
Industry	**Internet-Software**
Zacks Rank in Industry	**N/A**

ZACKS ESTIMATES

Revenue
(in millions of $)

	Q1 (Mar)	Q2 (Jun)	Q3 (Sep)	Q4 (Dec)	Year (Dec)
2012	$0.0 R	$0.0 R	$0.00 R	$0.0R	$2.48 R
2013	$0.0 A	$0.2 A	$0.4 A	$0.2 A	$0.7 A
2014	$0.2 A	$0.6 A	$1.2 E	$0.6 E	$2.6 E
2015					$30.0 E

Earnings per Share
(EPS is operating earnings before non-recurring items)

	Q1 (Mar)	Q2 (Jun)	Q3 (Sep)	Q4 (Dec)	Year (Dec)
2012	NM	NM	NM	NM	-$0.01 A
2013	-$0.04 A	-$0.06 A	-$0.06 A	$0.0 A	-$0.28 A
2014	-$0.09 A	-$0.15 A	-$0.15 E	-$0.15 E	-$0.54 E
2015					$0.58 E

Zacks Projected EPS Growth Rate - Next 5 Years NA

© Copyright 2014, Zacks Investment Research. All Rights Reserved.

KEY POINTS

- Finjan holds a number of pioneering patents for cybersecurity hardware and software that is relevant to dozens of companies in this space.
- While its patents have a limited licensing and enforcement track record, the company has the potential to reap large licensing revenues from the $20 billion market for cybersecurity software, services and appliance market.
- The technology licensing market in the U.S., once an afterthought, has grown from $33 billion in 1994 to $68 billion in 2002 and is likely over $100 billion today.
- The company's has a market cap of $95 million and $20 million in cash but could be worth considerably more if it is successful in its licensing pursuits. Estimating revenues of $30 million in 2015 and an industry multiple of 3.7 times sales, the company could be worth $5.80 by next year.

OVERVIEW

Finjan Holdings is a patent licensing and enforcement firm based in NYC that owns the patents of its predecessor company Finjan Inc., a cybersecurity company that was founded in Israel in 1997. It invented several technologies that are used in current cybersecurity products today. Its three main patent areas:

- Behavior-based methods to detect and prevent threats from the Internet, including email and Web malware
- "Sandboxing" or stripping applications and running potentially malicious code in a safe environment
- Mobile code replacement where the malicious code is stripped and replaced by safe code

The original company did not survive, due to in part to competition that used its technology unlawfully. The patents the company developed however are valuable and have garnered $145 million to date in licensing fees, settlements and judgments, of which $97.5 million was in 2012. The predecessor company paid out most of that money through dividends, and a new company was formed last June that owns the patent rights.

The initial patent enforcement action taken by the former Finjan Inc. was in 2006, when it sued Secure Computing. It won in court and was ultimately awarded $37.9 million. Thereafter, in 2010, the company decided to pursue five other companies, of which two settled (MacAfee—who by then owned Secure Computing, for $85 million and Webroot for $11.3 million) in 2012 and three (Websense, Symantec and Sophos) won in court. The lost case is currently being appealed.

The historical licensing and enforcement by the predecessor company is shown on the chart below:

	COMPANY	DATE	LICENSES & SETTLEMENTS	TYPE
JUDGMENTS	secure computing	March 2008	$37.9 MM	• Established royalty rate 8%-16% • Willfulness found • Injunction granted
LICENSES & SETTLEMENTS	Microsoft	July 2005	$8 MM	• Paid-up, cash • Portfolio • Life of patents
	M86 SECURITY	Nov 2009	25% equity of M86	• Stock • Portfolio • Life of patents
	Trustwave	March 2012	$3.1 MM[1]	• Stock • Portfolio • Life of patents
Webroot	CONFIDENTIAL	April 2012	$11.3 MM	• Confidential • Portfolio • Life of patents
MacAfee	CONFIDENTIAL	Nov 2012	$85 MM	• Confidential • Portfolio • Life of patents

1: Estimated book value representing 224,000 shares of Trustwave
Source: company SEC filings

Revenue strategy

There are a variety of IP companies out there, some of which have a large base and stable revenues such as Rambus (RMBS) and Interdigital (IDCC), and others that are more litigators swinging for the fences. Finjan hopes to be more conservative, preferring licensing over litigation, and would prefer to settle than to go to court. It plans to hit singles and doubles rather than home runs by going to go to trial and hoping for a favorable outcome. This reduces the risk as well as shortens the time period for some revenues to develop. One example of this desire to proceed quickly is the company's strategy to sue in the Northern District of California as that area has more tech savvy judges and even has a patent pilot program to expedite patent cases. While licensing is preferred, there is however a number of companies with whom voluntary licensing has not proven to be possible, and in those cases, the company will enforce its patents through litigation. While the company does not reveal who it is contemplating prosecuting, its current litigation is known. For all its litigation, it uses Kramer Levin as outside counsel. The company has a highly structured fee arrangement with Kramer Levin that consists of (discounted) hourly rates, and a portion of any favorable settlement or judgment.

Business Strategy

In addition to licensing, the company also has a small investment in a Jerusalem Venture Partners' JVP Cyber Labs cybersecurity incubator fund in Israel. They have committed to a $5 million investment in this fund of which $1 million has been funded and the rest will be funded from time to time on demand, as the fund requires. This incubator is investing in cybersecurity startups that Finjan plans to help with expertise and patenting advice. Hopefully some of these investments will be successful and add to Finjan earnings in the future. Companies in JVP's portfolio in the cybersecurity space include:

- nativeflow - Enterprise data protection for BYOD and corporate-owned devices, supporting iOS, Android and Windows 8 devices
- Cyber-Ark - the leader in securing and managing privileged identities and highly sensitive information.
- ThetaRay - developing a disruptive cyber-security product suite that is geared towards prevention of zero-day attacks and advanced persistent threats.

THE FORMER COMPANY ENFORCEMENT

Past Litigation Wins

To date, there have only been three patents owned by Finjan that have been successfully defended in court and in one court case. The court win was against Secure Computing in March 2008, when it was awarded $37.9 million in compensatory damages. Here the jury found willful infringement. The jury awarded this based on a 16% royalty on $49 million in sales of Secure Computing's Webwasher Software and an 8% royalty each on $3.25 million in sales of Webwasher hardware appliances and $13.5 million of Cyberguard TSP hardware appliances, plus punitive damages.

The patents involved in this judgment were:

6,092,194 "System and method for protecting a computer and a network from hostile downloadables." Filed in 1997, expires in 2017.

6,804,780, “System and method for protecting a computer and a network from hostile downloadables.” Filed in 2000, expires in 2020.

7,058,822, “Malicious mobile code runtime monitoring system and methods.” (Aka sandboxing) Filed in 2001, expires in 2021.

Past Settlements

After this win, the company decided to pursue further enforcement. In 2010, the company sued Websense, Sophos, MacAfee, Webroot Software and Symantec for violating patent numbers:

- 6,480,962 “System and method for protecting a client during runtime from hostile downloadables” filed in 2000.
- 6,804,780: “System and method for protecting a computer and a network from hostile downloadables” filed in 2000.

MacAfee ($85 million) and Webroot ($11.3 million) settled out of court, and Websense, Sophos and Symantec went to trial and Finjan lost. Finjan has appealed this ruling.

Past Licensing

Three companies have licensed Finjan patents at the predecessor company. Microsoft licensed all of them in perpetuity for $8 million after Finjan discovered major security flaws in Windows XP. Later M86 bought the operations and product line of Finjan and negotiated a perpetual license to the technology and a non-compete agreement, while Finjan retained the patents. Trustwave subsequently bought M86 and then increased the licensing arrangement by an additional $3.1 million to include its products in the license.

THE PRESENT COMPANY ENFORCEMENT

Litigation of Newly Formed Company

As soon as the new Finjan was created, it commenced enforcing its patents starting with a lawsuit against FireEye on July 8, 2014. The companies being currently sued with litigation status are shown on the chart below. We have bolded the patent numbers of the patents that were upheld in court in the Secure Computing case. The others have not yet been successfully litigated. Under the company names we have given our estimates of its 2014 calendar year sales, or used consensus estimates for public companies.

Company	Date and Location	Status	Patent numbers
FireEye **($428 m)**	US District Court for the Northern District of California on July 8, 2013	June 6, 2014, the judge entered an Order Granting Motion to Stay Pending Reexamination of certain Finjan patents.	**6,804,780**, 8,079,086, 7,975,305, 8,225,408, **7,058,822**, 7,647,633 and 6,154,844
Blue Coat **(est. >$500m)**	US District Court for the Northern District of California on August 28, 2013	"Markman" Hearing on August 22, 2014. Trial for this action is scheduled for July 20, 2015.	6,154,844, **6,804,780**, 6,965,968, **7,058,822**, 7,418,731, and 7,647,633
Websense **(est. $400m)**	US District Court for the Northern District of California on September 23, 2013 & March 24, 2014	"Markman" Hearing on November 21, 2014. Trial for this action is scheduled for October 5, 2015.	**7,058,822**, 7,647,633, 8,141,154, and 8,225,408
Proofpoint **($186 m)**	United States District Court for the Northern District of California on December 16, 2013	Hearing on the Motion to Stay on August 21, 2014. "Markman" Hearing on May 8, 2015. Trial for this action is scheduled for January 11, 2016.	6,154,844, **7,058,822**, 7,613,918, 7,647,633, 7,975,305, 8,079,086, 8,141,154, and 8,225,408
Sophos **(est. $420 m)**	United States District Court for the Northern District of California on March 14, 2014	"Markman" Hearing on February 13, 2015. No trial date yet.	6,154,844, **6,804,780**, 7,613,918, 7,613,926, 7,757,289, 8,141,154, 8,566,580, 8,677,494
Symantec **($6.7 billion)**	United States District Court for the Northern District of California on July 1, 2014	Case assigned, SYMC not yet responded	7,756,996; 7,757,289; 7,930,299; 8,015,182; 8,141,154
Sophos, Websense and Symantec	Appellate Court on December 10, 2013	Oral argument scheduled for September 9, 2014.	**6,092,194** and 6,480,962

FireEye Inc.

The current poster boy for the cybersecurity business is FireEye (FEYE) of Milpitas, CA founded in 2004. It is a one-year-old IPO with an astronomical valuation due to its rapid growth and position in the industry. Its estimated 2014 revenue is $428 million. The products Finjan claims infringe on its patents are: FireEye's Threat Protection Platform, including the FireEye Malware Protection System (FireEye EX Series), the FireEye Dynamic Threat Intelligence, and the FireEye Central Management System. Two of the patents in this suit were two of those upheld against Secure Computing, one of which is sandboxing. In relation to this lawsuit, FEYE has demanded two of the patents be examined by the patent office. Their status is as follows:

Proceedings before the United States Patent & Trademark Office (USPTO)

Ex Parte Reexamination Proceedings

U.S. Patent No. 7,647,633

- FireEye filed a third party request for *ex parte* reexamination of claims 1-7 and 28-33 of Finjan's U.S. Patent No. 7,647,633 on October 7, 2013.
- The request for reexamination was granted and a non-final Office Action was mailed November 19, 2013. The non-final Office Action included rejections of claims 1-7 and 28-33 under various prior art.
- An in-person Examiner interview was conducted at the USPTO on February 4, 2014, and a timely response to non-final Office Action was filed on February 19, 2014. Additionally, a petition to accept an unintentionally delayed priority claim was also submitted.
- The case is currently awaiting USPTO action.

U.S. Patent No. 7,058,822

- FireEye filed a third party request for *ex parte* reexamination of claims 1-8 and 16-27 of Finjan's U.S. Patent No. 7,058,822 on October 7, 2013.
- The request for reexamination was granted and a non-final Office Action was mailed December 6, 2013. The non-final Office Action included rejections of claims 1-8 and 16-27 under various prior art.
- An in-person Examiner interview was conducted at the USPTO on February 4, 2014, and a timely response to non-final Office Action was filed on March 6, 2014. Additionally, a petition to accept an unintentionally delayed priority claim was also submitted.
- The case is currently awaiting USPTO action.

Blue Coat Systems, Inc.

Blue Coat Systems founded in 1996 in Sunnyvale, CA is a private company with 1,300 employees. It is a leader in Secure Web Gateway and Content Security Management. It has 75 million users and 86% of the Fortune 500 uses its products. Rakuten (JASDAQ: 4755) bought the company for $1.3B in December 2011. In February 2012, the company went private through private equity lead Thoma Bravo for $1.3 billion. In its last reported quarter of October 2011, it did $114 million in revenues. Finjan claims systems and methods on the Blue Coat ProxySG Appliances and Software, ProxyAV Appliances and Software and WebPulse infringe on its patents. Since this lawsuit was filed, Blue Coat has acquired Norman Shark, a leader and early patent holder in sandboxing.

Websense, Inc.

Websense, founded in 1994 is headquartered in San Diego. It also was taken private in May 2013, for $906 million by Vista Equity Partners. It has over 1,500 employees. In its last public quarter of March 2013, it generated $87 million in revenues. On July 12, 2010, Finjan, Inc. filed a complaint that alleges that by making, using, importing, selling and/or offering for sale Websense Web Security Gateway, TRITON Enterprise, TRITON Security Gateway Anywhere, Websense Web Security Gateway Anywhere, Websense Web Security Gateway

Hosted and the Websense V-Series appliances, Websense infringes patent 6,092,194. Finjan lost this case but is appealing it.

Proofpoint, Inc.

Proofpoint (PFPT) headquartered in Sunnyvale, CA, is a SaaS provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance and secure communications to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. The company was founded in 2002 has over 700 employees, and analysts estimate it to do $186 million in sales in 2014. On December 16, 2013, Finjan, Inc. sued Proofpoint and Armorize Technologies, Inc., which had just been bought by Proofpoint in October 2013 for $25 million. Finjan claims that all Proofpoint and Armorize products and services that utilize: Proofpoint's Zero-Hour Threat Detection, Proofpoint's Malware Analysis Service, Proofpoint's Targeted Attack Protection, HackAlert, and CodeSecure, including without limitation on Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials, Proofpoint Protection Server, Proofpoint Messaging Security GatewayHackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert CodeSecure, HackAlert Vulnerability Assessment or SmartWAF, infringe on its patents.

Sophos Ltd.

Sophos is a private company founded in 1985 in Abington, UK and acquired for $830 million by Apex Partners in 2010 with over 1,300 employees worldwide. It is a leader in IT security and data protection focused on the mid-market. It is the only IT security company to be positioned as a leader across three critical security areas: Unified Threat Management (UTM), Mobile Data Protection and Endpoint Protection Platforms according to Gartner. The company has over $150 million in billings in UTM alone and generates $420 million in revenues

Finjan claims that products using Sophos Live Protection, Advanced Threat Protection, and WebLENS, including without limitation on Enduser Protection Suites, Endpoint Antivirus, Endpoint Antivirus Cloud, Sophos Cloud, Unified Threat Management, Next-Gen Firewall, Secure Web Gateway, Secure Email Gateway, and Server Security infringe on its patents.

Symantec Corporation

Symantec (SYMC) the giant anti-virus company was founded in 1982, and is located in Mountain View, CA. It is expected to generate $6.7 billion in revenues in the March 2015 year. The company has over 18,500 employees in 50 countries. It provides security, backup and availability software and services. The company has three segments: Symantec's User Productivity & Protection segment ($2.9 billion) sells products that are under the "Norton" brand name to consumers; Symantec's User Productivity & Protection segment sells under the Symantec brand name to businesses; Symantec's Information Security segment ($1.3 billion) sells products that provide SSL certificates, mail and web security, data center security, data loss prevention and information security services offerings; and Symantec's Information Management segment ($2.5 billion) focuses on backup, recovery and electronic discovery.

Finjan had previously sued Symantec in 2010 for patent infringement of patent numbers 6,092,194 and 6,480,962 and lost. This case is in appeal. On November 29, 2011, Symantec filed a third party request for *Inter Partes* re-examination of all claims 1-55 of Patent **6,480,962**. The request for reexamination was granted and a non-final office action included rejections of claims 1-55 under numerous prior art references and combinations of such references. Finjan and Symantec then both filed a response and the USPTO mailed an Action Closing Prosecution (ACP) on October 2, 2013. Finjan responded to the ACP on December 2, 2013, which included proposed claim amendments for consideration. Symantec responded on January 2, 2014. On June 27, 2014, the USPTO stated that the proposed claim amendments would not be entered and issued a Right of Appeal Notice. Then on July 1, 2014, Finjan filed a notice of appeal of the rejection of Claims 1-55.

Finjan filed a new claim July 1, 2014 that products that use SONAR with Insight, Disarm, Norton Safe Web, Norton Safe Search and Symantec Endpoint Protection Manager, including without limitation on Messaging Gateway, Message Gateway for Service Providers, Message Gateway Small Business Edition, Symantec Endpoint Protection, Symantec Endpoint Protection Small Business Edition, Network Access Control, Norton Internet Security, Norton Anti-Virus, Norton 360, and Safe-Web Lite all infringe on a different group of patents (see previous chart).

CYBERSECURITY MARKET

The market for cyber security products that may use technology covered by Finjan patents is expected to total $20 billion in sales in 2014, according to estimates by Gartner. These types of products include: endpoint and cloud, web gateway and next generation firewall software and hardware products as shown on the following chart.

Relevant Security Markets	2013	2014	2015	2016	2017
Endpoint & Cloud	$11.2 BN	$11.8 BN	$12.5 BN	$13.2 BN	$13.8 BN
Web Gateway	$4.1 BN	$4.4 BN	$4.7 BN	$5.0 BN	$5.3 BN
Next Gen. Firewall	$4.0 BN	$4.0 BN	$4.0 BN	$3.7 BN	$3.4 BN
Total Finjan Technology related Sales	$19.3 BN	$20.2 BN	$21.2 BN	$21.9 BN	$22.5 BN

Source: Gartner, IDC and Finjan estimates

There are several dozens of companies that sell these types of products and Finjan has plans to approach all of them to its technology, except the five already licensed. Examples of companies that we believe to have products that may infringe on Finjan's patents can be found on Gartner's Magic Quadrants for these three types of products.

Gartner Magic Quadrant: Firewalls



Gartner Magic Quadrant: Endpoint Protection



Gartner Magic Quadrant: Web Gateways



Source: Gartner (June 2014)

MANAGEMENT AND DIRECTORS

Phil Hartstein
President and Chief Executive Officer

Phil Hartstein joined Finjan in April of 2013 and has worked in a number of technology and intellectual property related roles. He comes to Finjan from IP Navigation Group where he was a Vice President and managed enforcement programs for clients. Before that he was a managing director at Rembrandt IP Solutions, a patent investment fund. His experience also includes working in IP as an in-house lawyer. Mr. Hartstein earned a BS in industrial technology from California Polytechnic, San Luis Obispo in 2000. He is an active participant in industry organizations, is regularly invited to speak on a number of patent monetization related topics from third-party litigation financing to capital market trends, and is a named inventor and patent holder.

Shimon Steinmetz
CFO and Treasurer

Shimon also joined Finjan in April 2013 after a career as a technology investment banker. He was most recently at Cantor Fitzgerald where he helped launch the technology practice. He has also worked in restructuring, turnarounds, and leveraged finance. He earned and MBA from University of Chicago in 2007 and a BS in Finance and Management from Yeshiva University in NYC in 2001.

Julie Mar-Spinola
VP Legal Operations

Julie joined Finjan in February 2014, as the head lawyer and is responsible for building the Company's IP assets, heading up its legal operations, and overseeing Finjan's enforcement program. She is also a legal consultant for Alta Devices. She has also been the General Counsel for Phoenix Technologies (PTEC), and iolo technologies and worked in the legal department at Atmel (ATML). There she won several major litigations that resulted in $100M in jury awards and a complete defense verdict invalidating each of the asserted patents in suit, as well as defeating the plaintiff's claim for over US $200 million plus enhanced damages. Julie has been a certified mediator for the US District Court for the Northern District of California, specializing in patent disputes since 2011. She earned a JD from Santa Clara University, School of Law in 1987 and a BA in Chemistry from San Diego State in 1984, and is a Patent Attorney registered to practice before the USPTO.

Ivan Chaperot
VP IP Licensing

Ivan joined Finjan in February 2014, from Intel where he was responsible for strategic patent acquisitions and licensing transactions. Before Intel, Ivan was a licensing executive at Intellectual Ventures, an invention marketplace, where he developed and led several IP monetization programs. Prior to Intellectual Ventures, Ivan was at Alcatel Lucent where he was responsible for IP licensing negotiations and the development of a patent sales program. Ivan started his career at Thales in France, where he developed and managed IP portfolios relating to security and embedded electronics markets. He is a member of the Licensing Executive Society (LES) and LES International and a European Patent Attorney and a French Patent Attorney. He earned an ESO at Ecole Superieure d'Optique in 1994, a PhD in Optics and Photonics at the University Paris Sud in 1997, a MA in Industrial Property and Contract Law from Center for International Industrial Property Studies.

Shlomo Touboul
Senior Advisor

Shlomo founded Finjan Software in 1997 and is named as an inventor on a number of Finjan patents covering behavior-based technologies for identifying and deflecting malicious code from accessing endpoint devices across networks and the Internet. He is recognized internationally as a thought leader in the cyber security space as he has both founded and advised a number of companies in the sector. His current involvement includes CUPP Computing, Yoggie Security Systems, and StrategySeeker.com. Shlomo earned a B.Sc. in Computer Science from Technion Israel in 1986.

BOARD OF DIRECTORS

Michael Eisenberg

Michael joined the board of Finjan in January 2002. He joined Benchmark Capital in 2005 and started his own fund, Aleph in 2013. Before Benchmark, Michael was a partner at Israel Seed Partners for eight years. Michael joined Israel Seed in 1997 from Jerusalem Global, where he started and headed the firm's successful investment banking group and partnership with Montgomery Securities. Michael earned a BA in Political Science from Yeshiva University in New York in 1993.

Daniel Chinn

Daniel has been a director of the company since June 2013. He has served as a director of the predecessor company since 2007 and was its CEO from 2010 until April 2014. Since 2011, he has also been a Partner at Tulchinsky Stern Marciano Cohen Levitski & Co., an Israeli law firm. Before that Daniel was the CEO of Seambiotic Ltd., and a partner at Israel Seed IV, LP, an investment company focusing on Israeli information technology and life sciences companies. He earned a BA in Jurisprudence from the University of Oxford in 1986.

Eric Benhamou

Eric became a director of the new company in June 2013 and had been a director of the predecessor company since 2006. He is currently CEO and founder of Benhamou Global Ventures, LLC. Eric is well known as the former CEO and Chairman of 3Com and later the Chairman of Palm, the mobile handset maker. He is also Chairman of Cypress Semiconductor Corporation and on the board of Silicon Valley Bank. He was a director of RealNetworks, Inc., Voltaire Ltd., and Dasient. He is on the board of the Stanford University School of Engineering, and Vice Chairman of the Board of Governors of Ben Gurion University of the Negev. He earned an MS from Stanford University's School of Engineering in 1977, a Diplôme d'Ingénieur and a doctorate from Ecole Nationale Supérieure d'Arts et Métiers, Paris in 1976, and has several honorary degrees.

Alex Rogers

Alex also became a director in June 2013 and also was a director of the predecessor company since 2006. Alex is a MD of HarbourVest (Asia) Limited and HarbourVest Partners LLC, which he joined in 1998. At HarbourVest, he focuses on direct co-investments in growth equity, buyout, and mezzanine transactions in Asia, Europe and emerging markets. He is on the board of Nero AG and FSI. His previous experience includes two years with McKinsey & Company. Alex earned a BA in Economics from Duke University in 1996 and an MBA from Harvard in 2002.

Glenn Daniel

Glenn joined the board of Finjan in April 2014. He was a MD at Houlihan Lokey where he advised boards of directors and independent committees of technology companies on fairness, valuation, and other financial matters in M&A and securities transactions. Mr. Daniel has testified as a financial expert in more than 25 cases in State, Federal, and Bankruptcy Court. He previously worked at Moody's and Lehman Brothers. Mr. Daniel holds a BA in German & Economics and an MS in Finance from the University of Wisconsin, Madison. He is a CFA and a member of the CFA Institute.

Harry Kellogg

Harry also joined the board in April 2014. He is Vice Chairman of the Board of Silicon Valley Bank and Head of Strategic Relationships for SVB Financial Group where he has been since 1986. Additionally Harry serves on the board of organizations: TechNet, Joint Venture: Silicon Valley Network, Financial Executives International, Stanford Institute for Economic Policy Research, The Computer History Museum, California/Israel Chamber of Commerce, Nollenberger Capital Partners, The Tuck Center for Private Equity and Entrepreneurship, Pacific Community Ventures and Grameen Bank. He is an emeritus board member of the Technology Museum of Innovation and earned a BS in Business Administration & Finance from San Jose State University in 1965.

Michael Southworth

Another board member to join in April 2014 is Michael Southworth, the CEO at Contact Solutions LLC, a leading provider of cloud-based and mobile customer self-service solutions that he joined in June 2013. Previously he was SVP of Global Wireless Solutions at Corning and Prior to Corning held senior financial roles at companies including: MobileAccess Networks, Lucent Technologies, and Chromatis. Michael earned a BS in Biology, Business concentration, from the University of California at Berkeley in 2004 and is a CPA.

PATENTS

US PATENTS OWNED BY FINJAN

20140143827	Malicious Mobile Code Runtime Monitoring System and Methods	2014
20140040610	Splitting an SSL Connection Between Gateways	2014
20100251373	SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE	2010
8677494	Malicious mobile code runtime monitoring system and methods	2011
8566580	Splitting an SSL connection between gateways	2013
8225408	Method and system for adaptive rule-based content scanners	2004
8141154	System and method for inspecting dynamically generated executable code	2010
8087079	Byte-distribution analysis of file security	2007
8079086	Malicious mobile code runtime monitoring system and methods	2009
8015182	System and method for appending security information to search engine results	2006
7975305	Method and system for adaptive rule-based content scanners for desktop computers	2004
7930299	System and method for appending security information to search engine results	2006
7757289	System and method for inspecting dynamically generated executable code	2005
7756996	Embedding management data within HTTP messages	2004
20120144485	COMPUTER SECURITY METHOD AND SYSTEM WITH INPUT PARAMETER VALIDATION	2008
20100023756	SPLITTING AN SSL CONNECTION BETWEEN GATEWAYS	2008
20080276320	Byte-distribution analysis of file security	2007
20070143271	System and method for appending security information to search engine results	2006
7647633	**Malicious mobile code runtime monitoring system and methods**	**2005**
7613926	Method and system for protecting a computer and a network from hostile downloadables	2006
7613918	System and method for enforcing a security context on a downloadable	2006
7418731	Method and system for caching at secure gateways	2004
7058822	**Malicious mobile code runtime monitoring system and methods**	**2001**
6965968	Policy-based caching	2003
6804780	**System and method for protecting a computer and a network from hostile downloadables**	**2000**
6480962	System and method for protecting a client during runtime from hostile downloadables	2000
6167520	System and method for protecting a client during runtime from hostile downloadables	1997
6154844	**System and method for attaching a downloadable security profile to a downloadable**	**1997**
6092194	System and method for protecting a computer and a network from hostile downloadables	1997

INTERNATIONAL PATENTS OWNED BY FINJAN

GRANTED

PCT Application PCT/IB98/02151
PCT Application PCT/IB97/01626
PCT Application PCT/IB01/01138
PCT Application PCT/IL2005/000915
Israel Patent No. 129,729
PCT Application PCT/IL2006/001430
PCT Application PCT/IL2006/001385
PCT Application PCT/IB2007/002108
Japanese Patent No. 3,952,315
United Kingdom Patent No. UK 0 965 094 B1
Netherlands Patent No. NL 0 965 094 B1
Italian Patent No. IT 0 965 094 B1
German Patent No. DE 0 965 094 B1
French Patent No. FR 0 965 094 B1
EP Patent No. 0 965 094 B1

Canadian Patent No. 2,275,771
Israel Patent No. 147,712
Israel Patent No. 190,518

PENDING

Israel Application No. 181,611
EP Application No. 05775457.4
Canadian Application No. 2,578,792
EP Application No. 06821605.0

VALUATION

Valuation of an IP company, even with a track record is very difficult and even more so with a company like Finjan that has only one court victory and no recent licensing arrangements. We can however look at other IP companies to see how the market values them to make some comparisons. There seems to be two different types of companies in this space, the older stable revenue generating companies like Rambus, and the upstarts that trade on events and potential. We can see from the table below, these range from values Inventergy Global with a $52 million enterprise value to Rambus with an enterprise value of $1.3 billion and $300 million in sales expected this year. On average the companies with revenues trade at an average of 3.7X revenues or an EV/EBITDA of 7.6X. We think that Finjan may start generating revenues in the next few months but it will be years before it reaches its maximum potential.

Using a valuation based on enterprise value to sales is easier for pre-revenue companies. If Finjan were to generate $30 million in sales in 2015, we could see the market putting a 3.7 times sales multiple on it as shown in the industry average below. Using that and working back to enterprise value per share, we see that given those revenues, Finjan could be worth $5.81 per share by next year, assuming it still has the same amount of cash on the balance sheet as today.

IP Industry Comparable Public Companies

IP Companies

	Ticker	Revenue		EV/	EBIDTA	Enterprise Value / Sales		Included	Enterprise
Company		2014E	LTM	EBITDA	Margin	2014E	LTM	in Average?	Value
Interdigital	IDCC	$401	$462	4.9	54%	3.1x	2.7x	y	1,230
Inventergy Global	INVT	NA	$47	NM	NM	NM	1.1x	n	52
Neonode	NEON	$5	$4	NM	NM	21.8x	25.9x	n	103
Parkervision	PRKR	$5	$0	NM	NM	21.1x	NM	n	105
Pendrell	PCO	$47	$42	NM	NM	3.3x	3.7x	y	157
Rambus	RMBS	$300	$302	10.4	42%	4.4x	4.4x	y	1,330
RPX	RPXC	$259	$245	2.8	71%	1.8x	1.9x	n	476
Tessera	TSRA	$262	$219	13.3	39%	4.4x	5.2x	y	1,150
Unwired Planet	UPIP	$39	$36	27.0	11%	2.8x	3.0x	y	111
VirnetX	VHC	$197	$2	NM	NM	3.8x	309.9x	y	744
Vringo	VRNG	$0	$1	NM	-2600%	618.0x	58.9x	n	62
Wi-Lan	WILN	$96	$102	5.2	70%	3.8x	3.6x	y	370
Average				**7.6**	**31%**	**3.7x**	**47.5x**		**$727**

	Revenue		EBITDA	Enterprise Value / Sales		Valuation Range	
	2015E	LTM	Margin	2015E	LTM	Low	High
FinJin	**$30**	**$0**		**3.7x**	**47.5x**	**$0**	**$110**

Conclusion of Enterprise Value	**$110,045,737**
Market Value	**$130,045,737**
Shares Outstanding	22,400,000
Price per Share	**$5.81**

It is impossible to predict what Finjan's long term revenues could be, but we can put parameters around what an investor could expect near term and long term. The industry it is targeting is expected to grow to $22.5B by 2017. Taking out Microsoft and MacAfee lets say $20B. Then Finjan can attempt to license to the rest. 2% of $20B is $400 million per year. We estimate the average EBITDA for revenue producing IP companies is 50%, and the average EV/EBIDTA is 7.6 times, we get a maximum EV for Finjan of $1.5B years in the future.

Near term however, there is no way to predict if the company will successfully license, settle or win any cases. We can take a look at the current companies being approached and their revenues. Since only a portion of revenues will apply to the products that are covered by the patents, we apply a discount to revenues. Then we show the potential license revenues at various royalty rates. Assuming the industry average of 50% EBITDA margins, and an industry average of EV to EBITDA multiple of 7.6x, we can estimate the enterprise value per share of Finjan if it were to reach those revenues and EBITDA longer term. This can be later refined as Finjan starts to produce revenues and we get a better sense of what it can achieve and how much it plans to spend.

Near Term Scenarios

			Royalty Rate			
	Revenues	% Relevant	16%	8%	2%	1%
FireEye	$428	30%	$21	$10	$3	$1
Blue Coat	500	10%	8	4	1	0.5
Websense	400	20%	13	6	2	0.8
Proofpoint	186	50%	15	7	2	0.9
Sophos	420	25%	17	8	2	1.1
Symantec (2 segments)	4,200	30%	202	101	25	12.6
TOTAL			$275	$137	$34	$17
EBITDA			$137.31	$68.66	$17.16	$8.58
Avg. EBITDA Multiple			7.6	7.6	7.6	7.6
Enterprise Value			1,044	522	130	65
Price Per Share			$47.44	$23.72	$5.93	$2.96

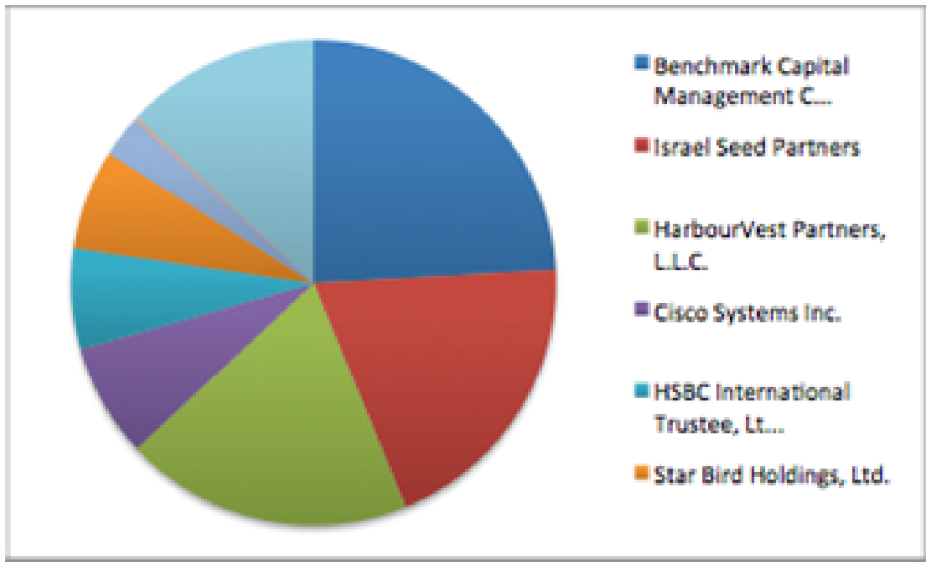
RISKS

- The company has a limited track record with which to set expectations.
- Finjan's patents have only prevailed in court once and only two patents in the portfolio have been upheld thus far.
- There is no way to predict the timing of lawsuit settlements or licensing agreements, or even the length of a lawsuit.

- As the current company burns cash and has no current licensing revenue, it may not generate enough revenues to cover costs and continue operations unless it generates income or receives further financing.
- The stock is high risk and is expected to have wide swings in stock price depending on unpredictable events.
- Government is expected to legislate new laws on patent enforcement that could affect the company's ability to monetize its patents as it currently expects.

FLOAT AND OWNERSHIP

Of the 22 million shares outstanding, only 17% is in the float.



BALANCE SHEET

$ in Thousands	June 30, 2014	Mar. 31, 2014	Dec. 31, 2013	% Change June-Dec
Current assets:				
Cash and cash equivalents	$20,559	$23,549	$24,598	-16%
Accounts receivable, net	254	51	50	408%
Inventories	80	61	34	135%
Prepaid expenses and other current assets	239	214	150	59%
Total current assets	21,132	23,875	24,832	-15%
Property and equipment, net	862	958	953	-10%
Intangible assets, net	1,192	1,253	1,333	-11%
Goodwill	306	306	306	0%
Investments	1000	500	500	100%
Other non-current assets	23	23	23	0%
Total Assets	24,515	26,915	27,947	-12%
Current Liabilities:				
Accounts payable	1,030	873	495	108%
Accounts payable - related parties	13	19	15	-13%
Accrued expenses	957	591	336	185%
Accrued income taxes	4	5	4	0%
Other current liabilities	15	32	35	-57%
Total current liabilities	2,019	1,520	885	128%
Deferred tax liabilities	35	37	39	-10%
Total Liabilities	2,054	1,557	924	122%
Commitments and contingencies				
Stockholders' Equity				
Common stock	2	2	2	0%
Additional paid-in capital	22,461	21,884	21,546	4%
Retained earnings	222	3,472	5,475	-96%
Total Stockholders' Equity	22,461	25,358	27,023	-17%
Total Liabilities and Stockholders' Equity	$24,515	$26,915	$27,947	-12%

INCOME STATEMENT

	2013				2014						
In Thousands	**Q1A**	**Q2R**	**Q3A**	**Q4A**	**Q1A**	**Q2A**	**Q3E**	**Q4E**	**2013**	**2014E**	**2015E**
Licensing	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$30,000
Fertilizer	0	198	394	152	175	636	1,200	600	744	2,611	2,700
Total Revenues	0	198	394	152	175	636	1,200	600	744	2,611	32,700
Cost of revenues	0	148	576	38	134	332	1,300	250	762	2,016	2,700
Gross profit	0	50	(182)	114	41	304	(100)	350	(18)	595	30,000
Gross Margin		25%	-46%	75%	23%	48%	-8%	58%	-2%	23%	92%
Operating Expenses:											
SG&A	847	1,493	1,197	$3,152	3,123	3,564	3,600	3,600	6,689	13,887	17,000
Transaction costs	0	790	0	$0		0	0	0	790	0	0
Total operating expenses		2,283	1,197	$3,152					7,479	13,887	17,000
	847				3,123	3,564	3,600	3,600			
Loss from operations	(847)	(2,233)	(1,379)	($3,038)	(3,082)	(3,260)	(3,260)	(3,260)	(7,497)	(12,862)	13,000
Other Income											
Gain on settlements		1,000			1,000	0	0	0	1,000	1,000	0
Other income		17			12	5	0	0	9	17	0
Interest income	80	31	7	$35	68	6	6	5	153	85	100
Total other income	80	1,048	7	$27	1,080	11	11	11	1,162	1,113	100
Loss before taxes	(767)	(1,185)	(1,372)	($3,011)	(2,002)	(3,249)	(3,249)	(3,249)	(6,335)	(11,749)	13,100
Income taxes		7	0	$0	1	(2)	(2)	(2)	(263)	(5)	0
Net Loss	(767)	(1,192)	(1,372)	($3,011)	(2,003)	(3,247)	(3,247)	(3,247)	(6,072)	(11,744)	13,100
Net Loss Per Share:											
Basic and Diluted	($0.04)	($0.06)	($0.06)	($0.13)	($0.09)	($0.15)	($0.15)	($0.15)	($0.28)	($0.52)	$0.58
Basic and Diluted Shares	20,591	21,093	22,348	22,350	22,368	22,379	22,379	22,379	21,602	22,376	22,500

STOCK PRICE CHART



Source: Yahoo! Finance

APPENDIX

Summary of The Four Main Patents That have been Successfully Defended in Court:

November 6, 1997

PATENT 6,092,194: System and method for protecting a computer and a network from hostile downloadables

ABSTRACT

A system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

CLAIMS (68)

What is claimed is:

A computer-based method, comprising the steps of:

- Receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client;
- Comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated;
- And preventing execution of the Downloadable by the client if the security policy has been violated.

2. The method of claim 1, further comprising the step of decomposing the Downloadable into the Downloadable security profile data.

3. The method of claim 2, wherein the security policy includes an access control list and further comprising the step of comparing the Downloadable security profile data against the access control list.

4. The method of claim 1, further comprising the steps of scanning for a certificate and comparing the certificate against a trusted certificate.

5. The method of claim 1, further comprising the step of comparing the URL from which the Downloadable originated against a known URL.

6. The method of claim 5, wherein the known URL is a trusted URL.

7. The method of claim 5, wherein the known URL is an untrusted URL.

8. The method of claim 1, wherein the Downloadable includes a Java™ applet.

9. The method of claim 1, wherein the Downloadable includes an ActiveX™ control.

10. The method of claim 1, wherein the Downloadable includes a JavaScript™ script.

11. The method of claim 1, wherein the Downloadable includes a Visual Basic script.

12. The method of claim 1, wherein the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

13. The method of claim 1, wherein the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

14. The method of claim 1, wherein the client belongs to a particular group, and the security policy includes a specific security policy corresponding to the particular group.

15. The method of claim 1, further comprising, after preventing execution of the Downloadable, the step of sending a substitute non-hostile Downloadable to the client for informing the client.

16. The method of claim 1, further comprising, after preventing execution of the Downloadable, the step of recording the violation in an event log.

17. The method of claim 1, further comprising the step of computing a Downloadable ID to identify the Downloadable.

18. The method of claim 16, further comprising the steps of fetching components identified by the Downloadable and including the fetched components in the Downloadable.

19. The method of claim 18, further comprising the step of performing a hashing function on the Downloadable to compute a Downloadable ID to identify the Downloadable.

20. The method of claim 18, further comprising the step of fetching all components identified by the Downloadable.

21. The method of claim 1 further comprising the step of examining the intended recipient user ID to determine the appropriate security policy.

22. The method of claim 20, wherein the appropriate security policy includes a default security policy.

23. The method of claim 1, further comprising the step of examining the Downloadable to determine the appropriate security policy.

24. The method of claim 1, further comprising the step of comparing the Downloadable against a known Downloadable.

25. The method of claim 24, wherein the known Downloadable is hostile.

26. The method of claim 24, wherein the known Downloadable is non-hostile.

27. The method of claim 24, further comprising the step of including a previously received Downloadable as a known Downloadable.

28. The method of claim 27, wherein the security policy identifies a Downloadable to be blocked per administrative override.

29. The method of claim 28, wherein the security policy identifies a Downloadable to be allowed per administrative override.

30. The method of claim 1, further comprising the step of informing a user upon detection of a security policy violation.

31. The method of claim 1, further comprising the steps of recognizing the incoming Downloadable, and obtaining the Downloadable security profile data for the incoming Downloadable from memory.

32. A system for execution by a server that serves as a gateway to a client, the system comprising: a security policy; an interface for receiving an incoming Downloadable addressed to a client; a comparator, coupled to the interface, for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against the security policy to determine if the security policy has been violated; and a logical engine for preventing execution of the Downloadable by the client if the security policy has been violated.

33. The system of claim 32, wherein the Downloadable includes a Java™ applet.

34. The system of claim 32, wherein the Downloadable includes ActiveX™ control.

35. The system of claim 32, wherein the Downloadable includes a JavaScript™ script.

36. The system of claim 32, wherein the Downloadable includes a Visual Basic script.

37. The system of claim 32, wherein the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

38. The system of claim 32, wherein the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

39. The system of claim 32, wherein the client belongs to a particular group, and the security policy includes a specific security policy corresponding to the particular group.

40. The system of claim 32, further comprising an ID generator coupled to the interface for computing a Downloadable ID identifying the Downloadable.

41. The system of claim 40, wherein the ID generator pre-fetches all components of the Downloadable and uses all components to compute the Downloadable ID.

42. The system of claim 41, wherein the ID generator computes the digital hash of all the pre-fetched components.

43. The system of claim 32, further comprising a policy finder for finding the security policy.

44. The system of claim 43, wherein the policy finder finds the security policy based on the user.

45. The system of claim 43 wherein the policy finder finds the security policy based on the user and the Downloadable.

46. The system of claim 43, wherein the policy finder obtains the default security policy.

47. The system of claim 32 wherein the comparator examines the security policy to determine which tests to apply.

48. The system of claim 47 wherein the comparator compares the Downloadable against a known Downloadable.

49. The system of claim 48, wherein the known Downloadable is hostile.

50. The system of claim 48, wherein the known Downloadable is non-hostile.

51. The system of claim 32, wherein the security policy identifies a Downloadable to be blocked per administrative override.

52. The system of claim 32, wherein the security policy identifies a Downloadable to be allowed per administrative override.

53. The system of claim 32, wherein the comparator sends a substitute non-hostile Downloadable to the client for informing the client.

54. The system of claim 32, further comprising a code scanner coupled to the comparator for decomposing the Downloadable into the Downloadable security profile data.

55. The system of claim 54, further comprising an ACL comparator coupled to the code scanner for comparing the Downloadable security profile data against an access control list.

56. The system of claim 32, further comprising a certificate scanner coupled to the comparator for examining the Downloadable for a certificate.

57. The system of claim 56, further comprising a certificate comparator coupled to the certificate scanner for comparing the certificate against a trusted certificate.

58. The system of claim 32, further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL.

59. The system of claim 58, wherein the known URL identifies an untrusted URL.

60. The system of claim 58, wherein the known URL identifies a trusted URL.

61. The system of claim 31, wherein the logical engine responds according to the security policy.

62. The system of claim 31, further comprising a record-keeping engine coupled to the comparator for recording results in an event log.

63. The system of claim 32, further comprising memory storing the Downloadable security profile data for the incoming Downloadable.

64. A system for execution on a server that serves as a gateway to a client, comprising: means for receiving an incoming Downloadable addressed to a client; means for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security

policy has been violated; and means for preventing execution of the Downloadable by the client if the security policy has been violated.

65. A computer-readable storage medium storing program code for causing a server that serves as a gateway to a client to perform the steps of: receiving an incoming Downloadable addressed to a client; comparing Downloadable security profile data pertaining to the Downloadable against a security policy to determine if the security policy has been violated; and preventing execution of the Downloadable by the client if the security policy has been violated.

66. A method, comprising: receiving a Downloadable; decomposing the Downloadable into Downloadable security profile data; the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, comparing the Downloadable security profile data against a security policy; and preventing execution of the Downloadable if the Downloadable security profile data violates the security policy.

67. The method of claim 66, further comprising: fetching all components referenced by the Downloadable; performing a hashing function of the Downloadable and the components fetched to compute a Downloadable ID; and storing the Downloadable security profile data and the Downloadable ID in memory.

68. A method, comprising: providing memory storing known-Downloadable security profile data and a that includes a list a suspicious computer operations that may be attempted by a Downloadable known-Downloadable ID corresponding to the Downloadable security profile data; receiving an incoming Downloadable; fetching all components referenced by the incoming Downloadable; performing a hashing function of the Downloadable and the components to compute an incoming-Downloadable ID; comparing the known-Downloadable ID against the incoming-Downloadable ID; retrieving the Downloadable security profile data if the known-Downloadable ID and the incoming-Downloadable ID match; and comparing the Downloadable security profile data against a security policy to determine if the incoming Downloadable violates the security policy.

March 30, 2000

Patent No. 6,804,780: System and method for protecting a computer and a network from hostile downloadables

ABSTRACT

A computer-based method for generating a Downloadable ID to identify a Downloadable, including obtaining a Downloadable that includes one or more references to software components required by the Downloadable, fetching at least one software component identified by the one or more references, and performing a function on the Downloadable and the fetched software components to generate a Downloadable ID. A system and a computer-readable storage medium are also described and claimed.

PRIORITY REFERENCE TO RELATED APPLICATION
This application is a continuation of and hereby incorporates by reference U.S. patent application Ser. No. 08/964,388, entitled “System and Method for Protecting a Computer and a Network from Hostile Downloadables,” filed Nov. 6, 1997, which is now U.S. Pat. No. 6,092,194, which claims priority to provisional application Serial No. 60/030,639, entitled “System and Method for Protecting a Computer from Hostile Downloadables,” filed on Nov. 8, 1996, by inventor Shlomo Touboul.

CLAIMS (18)

What is claimed is:
1. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising: obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; fetching at least one software component identified by the one or more references; and performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

2. The method of claim 1, wherein the Downloadable includes an applet.

3. The method of claim 1, wherein the Downloadable includes an active software control.

4. The method of claim 1, wherein the Downloadable includes a plugin.

5. The method of claim 1, wherein the Downloadable includes HTML code.

6. The method of claim 1, wherein the Downloadable includes an application program.

7. The method of claim 1, wherein said fetching includes fetching a first software component referenced by the Downloadable.

8. The method of claim 1, wherein said fetching includes fetching all software components referenced by the Downloadable.

9. A system for generating a Downloadable ID to identify a Downloadable, comprising: a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and an ID generator coupled to the communications engine that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

10. The system of claim 9, wherein the Downloadable includes an applet.

11. The system of claim 9, wherein the Downloadable includes an active software control.

12. The system of claim 9, wherein the Downloadable includes a plugin.

13. The system of claim 9, wherein the Downloadable includes HTML code.

14. The system of claim 9, wherein the Downloadable includes an application program.

15. The system of claim 9, wherein the ID generator fetches a first software component referenced by the Downloadable.

16. The method of claim 9, wherein the ID generator fetches all software components referenced by the Downloadable.

17. A system for generating a Downloadable ID to identify a Downloadable, comprising: means for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; means for fetching at least one software component identified by the one or more references; and means for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

18. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

- Obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;
- Fetching at least one software component identified by the one or more references;
- And performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

”SANDBOXING”

May 17, 2001

PATENT 7,058,822: Malicious mobile code runtime monitoring system and methods

ABSTRACT

Protection systems and methods provide for protecting one or more personal computers (“PCs”) and/or other intermittently or persistently network accessible devices or processes from undesirable or otherwise malicious operations of Java™ applets, ActiveX™ controls, JavaScript™ scripts, Visual Basic scripts, add-ins, downloaded/uploaded programs or other “Downloadables” or “mobile code” in whole or part. A protection engine embodiment provides, within a server, firewall or other suitable “re-communicator,” for monitoring information received by the communicator, determining whether received information does or is likely to include executable code, and if so, causes mobile protection code (MPC) to be transferred to and rendered operable within a destination device of the received information, more suitably by forming a protection agent including the MPC, protection policies and a detected-Downloadable. An MPC embodiment further provides, within a Downloadable-destination, for initiating the Downloadable, enabling malicious Downloadable operation attempts to be received by the MPC, and causing (predetermined) corresponding operations to be executed in response to the attempts, more suitably in conjunction with protection policies.

PRIORITY REFERENCE TO RELATED APPLICATIONS
This application claims benefit of and hereby incorporates by reference provisional application Ser. No. 60/205,591, entitled “Computer Network Malicious Code Run-time Monitoring,” filed on May 17, 2000 by inventors Nimrod Itzhak Vered, et al. This application is also a Continuation-In-Part of and hereby incorporates by reference patent application Ser. No. 09/539,667, now U.S. Pat. No. 6,804,780, entitled “System and Method for Protecting a Computer and a Network From Hostile Downloadables” filed on Mar. 30, 2000 by inventor Shlomo Touboul. This application is also a Continuation-In-Part of and hereby incorporates by reference patent application Ser. No. 09/551,302, now U.S. Pat. No. 6,480,962, entitled “System and Method for Protecting a Client During Runtime From Hostile Downloadables”, filed on Apr. 18, 2000 by inventor Shlomo Touboul.

CLAIMS (18)

What is claimed is:

A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:

- obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;
- fetching at least one software component identified by the one or more references;
- And performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

2. The method of claim 1, wherein the Downloadable includes an applet.

3. The method of claim 1, wherein the Downloadable includes an active software control.

4. The method of claim 1, wherein the Downloadable includes a plugin.

5. The method of claim 1, wherein the Downloadable includes HTML code.

6. The method of claim 1, wherein the Downloadable includes an application program.

7. The method of claim 1, wherein said fetching includes fetching a first software component referenced by the Downloadable.

8. The method of claim 1, wherein said fetching includes fetching all software components referenced by the Downloadable.

9. A system for generating a Downloadable ID to identify a Downloadable, comprising:
- A communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;
- And an ID generator coupled to the communications engine that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

10. The system of claim 9, wherein the Downloadable includes an applet.

11. The system of claim 9, wherein the Downloadable includes an active software control.

12. The system of claim 9, wherein the Downloadable includes a plugin.

13. The system of claim 9, wherein the Downloadable includes HTML code.

14. The system of claim 9, wherein the Downloadable includes an application program.

15. The system of claim 9, wherein the ID generator fetches a first software component referenced by the Downloadable.

16. The method of claim 9, wherein the ID generator fetches all software components referenced by the Downloadable.

17. A system for generating a Downloadable ID to identify a Downloadable, comprising:
- Means for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;
- Means for fetching at least one software component identified by the one or more references; and
- Means for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

18. A computer-readable storage medium storing program code for causing a computer to perform the steps of:
- Obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;
- Fetching at least one software component identified by the one or more references;
- And performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

April 18, 2000

Patent No. 6480962 B1: System and method for protecting a client during runtime from hostile downloadables

ABSTRACT

A system protects a client from hostile Downloadables. The system includes security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.

CLAIMS(51)

What is claimed is:

1. A computer-based method, comprising:
- monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;
- interrupting processing of the request;
- comparing information pertaining to the Downloadable against a predetermined security policy;
- and performing a predetermined responsive action based on the comparison.

2. The method of claim 1, wherein monitoring the operating system includes monitoring a request sent to a Downloadable engine.

3. The method of claim 2, wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and wherein monitoring the operating system includes monitoring each Java™ class for receipt of the request.

4. The method of claim 2, wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and wherein monitoring the operating system includes monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

5. The method of claim 1, further comprising determining whether information pertaining to the Downloadable violates a security rule.

6. The method of claim 5, further comprising determining whether violation of the security rule violates the security policy.

7. The method of claim 1, further comprising:
- comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable;
- and performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

8. The method of claim 1, wherein the predetermined responsive action includes storing results of the comparison in an event log.

9. The method of claim 1, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

10. The method of claim 1, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

11. The method of claim 1, wherein the predetermined responsive action includes discarding the Downloadable.

12. A system, comprising:
- a security policy;
- a plurality of operating system interfaces operating substantially in parallel, each interface for recognizing a runtime event in a subsystem of the operating system caused from a request made by a Downloadable;
- a first comparator coupled to the interfaces for comparing information pertaining to the received Downloadable with the security policy; and
- a response engine coupled to the first comparator for performing a predetermined responsive action based on the comparison with the security policy.

13. The system of claim 12, wherein the interfaces-include a Java™ class extension for monitoring a Java™ class in a Java™ virtual machine for receipt of a request.

14. The system of claim 12, wherein the interfaces include an AppletX™ extension for monitoring a message engine, a dynamic-data-exchange and a dynamically-linked library in an AppletX™ environment for receipt of a request.

15. The system of claim 12, further comprising a security rule; and a second comparator, coupled to the interfaces and to the response engine, for determining whether information pertaining to the Downloadable violates the security rule.

16. The system of claim 15, wherein the first comparator determines whether violation of the security rule violates the security policy.

17. The system of claim 12, further comprising a predetermined suspicious Downloadable; and
a second comparator coupled to the interfaces for comparing information pertaining to the Downloadable with information pertaining to the predetermined suspicious Downloadable; wherein the response engine is further coupled to the second comparator and performs the responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

18. The system of claim 12, further comprising an event log coupled to the first comparator for storing results of the comparison.

19. The system of claim 12, further comprising a user interface coupled to the first comparator.

20. The system of claim 12, further comprising a suspicious Downloadable database for storing information on known and previously-deemed suspicious Downloadables.

21. The system of claim 12, wherein the predetermined suspicious action includes discarding the Downloadable.

22. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:
- means for monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;
- means for interrupting processing of the request;
- means for comparing information pertaining to the Downloadable against a predetermined security policy; and
- means for performing a predetermined responsive action based on the comparison.

23. The system of claim 22, wherein the means for monitoring the operating system includes means for monitoring a request sent to a Downloadable engine.

24. The system of claim 23, wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and wherein the means for monitoring the operating system includes means for monitoring each Java™ class for receipt of the request.

25. The system of claim 23, wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and wherein the means for monitoring the operating system includes means for monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

26. The system of claim 22, further comprising means for determining whether information pertaining to the Downloadable violates a security rule.

27. The system of claim 26, further comprising means for determining whether violation of the security rule violates the security policy.

28. The method of claim 22, further comprising:

- means for comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable;
- and means for performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

29. The system of claim 22, wherein the predetermined responsive action includes storing results of the comparison in an event log.

30. The system of claim 22, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

31. The system of claim 22, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

32. The system of claim 22, wherein the predetermined responsive action includes discarding the Downloadable.

33. A computer-readable storage medium storing program code for causing a computer to perform the steps of: monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request; comparing information pertaining to the Downloadable against a predetermined security policy; and performing a predetermined responsive action based on the comparison.

34. The medium of claim 33, wherein monitoring the operating system includes monitoring a request sent to a Downloadable engine.

35. The medium of claim 33, wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and wherein monitoring the operating system includes monitoring each Java™ class for receipt of the request.

36. The medium of claim 35, wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and wherein monitoring the operating system includes monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

37. The medium of claim 33, further comprising determining whether information pertaining to the Downloadable violates a security rule.

38. The medium of claim 37, further comprising determining whether violation of the security rule violates the security policy.

39. The medium of claim 33, further comprising:
- comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable;
- and performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

40. The medium of claim 33, wherein the predetermined responsive action includes storing results of the comparison in an event log.

41. The medium of claim 33, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

42. The medium of claim 33, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

43. The medium of claim 33, wherein the predetermined responsive action includes discarding the Downloadable.

44. The system of claim 1, wherein each subsystem includes one of a file system, network system, process system or memory system.

45. The system of claim 12, wherein each subsystem includes one of a file system, network system, process system or memory system.

46. The system of claim 22, wherein each subsystem includes one of a file system, network system, process system or memory system.

47. The system of claim 33, wherein each subsystem includes one of a file system, network system, process system or memory system.

48. A method, comprising:
- intercepting, by an operating system probe associated with an operating system function, an operating system call being issued by a downloadable to an operating system and associated with the operating system function;
- comparing, by a runtime environment monitor, the operating system call against a predetermined security policy before allowing the operating system to process the operating system call;
- blocking, by a response engine, operating system calls that are forbidden according to the security policy; and
- allowing, by the response engine, operating system calls that are permitted according to the security policy.

49. The method of claim 48, wherein the Downloadable is one of a Java component, an ActiveX control, executable code, or interpretable code.

50. A system, comprising:
- an operating system probe associated with an operating system function for intercepting an operating system call being issued by a downloadable to an operating system and associated with the operating system function;
- a runtime environment monitor for comparing the operating system call against a predetermined security policy before allowing the operating system to process the operating system call;

- and a response engine for blocking operating system calls that are forbidden according to the security policy, and for allowing operating system calls that are permitted according to the security policy.
-

51. The system of claim 50, wherein the Downloadable is one of a Java component, an ActiveX control, executable code, or interpretable code.

DISCLOSURES

The following disclosures relate to relationships between Zacks Small-Cap Research ("Zacks SCR"), a division of Zacks Investment Research ("ZIR"), and the issuers covered by the Zacks SCR Analysts in the Small-Cap Universe.

ANALYST DISCLOSURES

I, Lisa Thompson, hereby certify that the view expressed in this research report accurately reflect my personal views about the subject securities and issuers. I also certify that no part of my compensation was, is, or will be, directly or indirectly, related to the recommendations or views expressed in this research report. I believe the information used for the creation of this report has been obtained from sources I considered to be reliable, but I can neither guarantee nor represent the completeness or accuracy of the information herewith. Such information and the opinions expressed are subject to change without notice.

INVESMENT BANKING, REFERRALS, AND FEES FOR SERVICE

Zacks SCR does not provide nor has received compensation for investment banking services on the securities covered in this report. Zacks SCR does not expect to receive compensation for investment banking services on the Small-Cap Universe. Zacks SCR may seek to provide referrals for a fee to investment banks. Zacks & Co., a separate legal entity from ZIR, is, among others, one of these investment banks. Referrals may include securities and issuers noted in this report. Zacks & Co. may have paid referral fees to Zacks SCR related to some of the securities and issuers noted in this report. From time to time, Zacks SCR pays investment banks, including Zacks & Co., a referral fee for research coverage.

Zacks SCR has received compensation for non-investment banking services on the Small-Cap Universe, and expects to receive additional compensation for non-investment banking services on the Small-Cap Universe, paid by issuers of securities covered by Zacks SCR Analysts. Non-investment banking services include investor relations services and software, financial database analysis, advertising services, brokerage services, advisory services, equity research, investment management, non-deal road shows, and attendance fees for conferences sponsored or co-sponsored by Zacks SCR. The fees for these services vary on a per client basis and are subject to the number of services contracted. Fees typically range between ten thousand and fifty thousand USD per annum.

POLICY DISCLOSURES

Zacks SCR Analysts are restricted from holding or trading securities placed on the ZIR, SCR, or Zacks & Co. restricted list, which may include issuers in the Small-Cap Universe. ZIR and Zacks SCR do not make a market in any security nor do they act as dealers in securities. Each Zacks SCR Analyst has full discretion on the rating and price target based on his or her own due diligence. Analysts are paid in part based on the overall profitability of Zacks SCR. Such profitability is derived from a variety of sources and includes payments received from issuers of securities covered by Zacks SCR for services described above. No part of analyst compensation was, is or will be, directly or indirectly, related to the specific recommendations or views expressed in any report or article.

ADDITIONAL INFORMATION

Additional information is available upon request. Zacks SCR reports are based on data obtained from sources we believe to be reliable, but are not guaranteed as to be accurate nor do we purport to be complete. Because of individual objectives, this report should not be construed as advice designed to meet the particular investment needs of any investor. Any opinions expressed by Zacks SCR Analysts are subject to change without notice. Reports are not to be construed as an offer or solicitation of an offer to buy or sell the securities herein mentioned.

ZACKS RATING & RECOMMENDATION

ZIR uses the following rating system for the 1,116 companies whose securities it covers, including securities covered by Zacks SCR:
Buy/Outperform: The analyst expects that the subject company will outperform the broader U.S. equity market over the next one to two quarters.
Hold/Neutral: The analyst expects that the company will perform in line with the broader U.S. equity market over the next one to two quarters.
Sell/Underperform: The analyst expects the company will underperform the broader U.S. Equity market over the next one to two quarters.

The current distribution is as follows: Buy/Outperform- 16.6%, Hold/Neutral- 76.7%, Sell/Underperform – 5.9%. Data is as of midnight on the business day immediately prior to this publication.