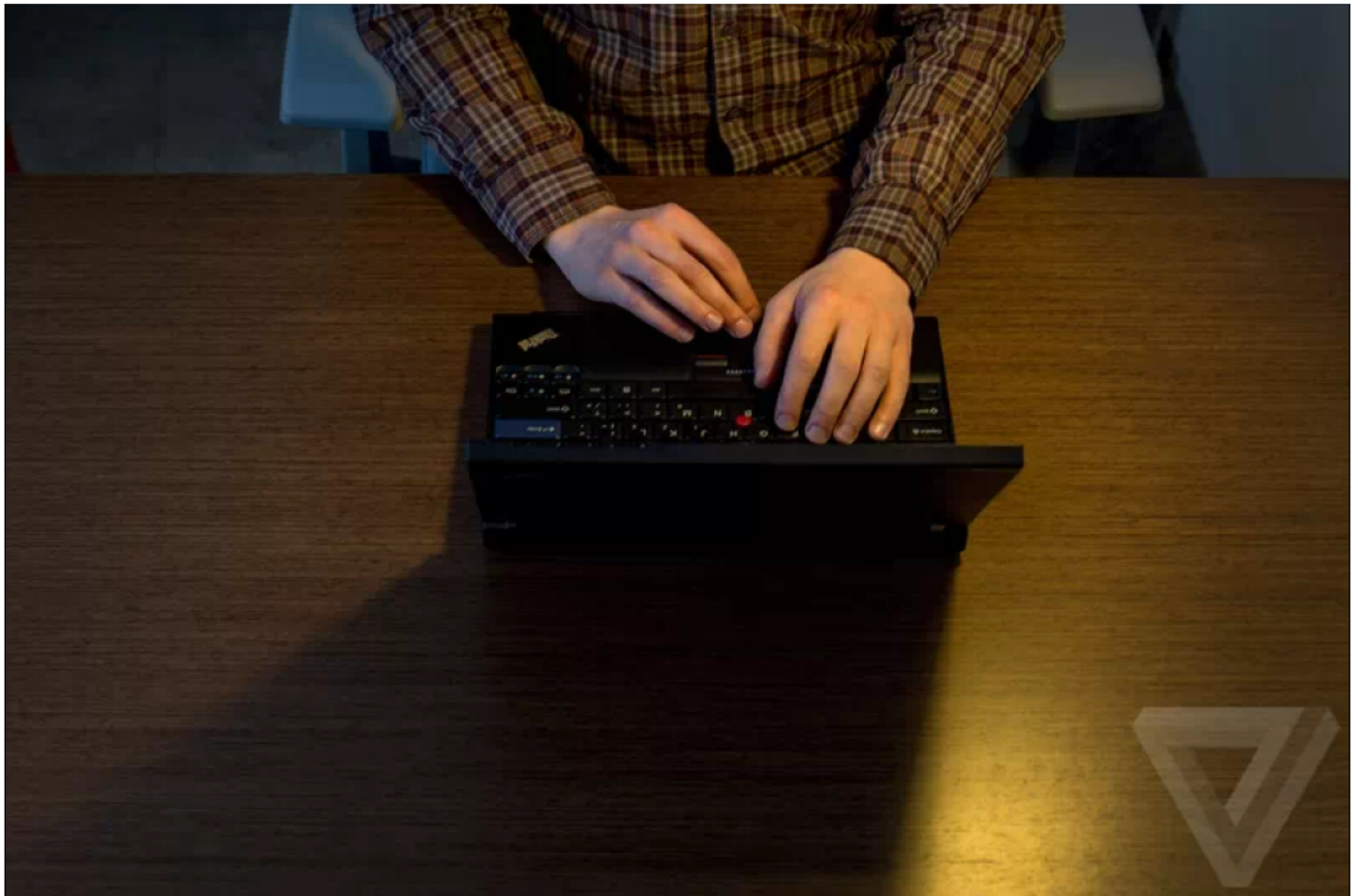


Who hid a backdoor in a popular corporate VPN program?

By [Ashley Carman](#) on December 22, 2015 08:33 am



For years, attackers may have unmasked and read sensitive digital communications between users and corporate entities around the world. Last week, their efforts were finally detected in the form of recently discovered backdoors, raising troubling new questions about state efforts to break network security.

Last week, Juniper Networks issued an **out-of-cycle security advisory** for thousands of its devices, based on two vulnerabilities in its ScreenOS product. The vulnerabilities would allow an attacker to gain access to devices or monitor and decrypt protected VPN traffic. And unlike most vulnerabilities, this weakness appears to have been deliberately inserted in the code, designed to be overlooked and kept secret for as long as possible.

JUNIPER ONLY BECAME AWARE OF ITS EXISTENCE RECENTLY

Why would someone want to plant a backdoor in corporate VPN software? While it's not a household name, Juniper VPNs protect hundreds of corporate networks, exactly the kind of capability sought by intelligence agencies around the world. Compromising these connections would yield access to highly sensitive information and communications, said HD Moore, chief research officer at Rapid7, in an interview with *The Verge*. **Some estimates** put the number of devices vulnerable to Juniper's backdoors at around 26,000, smaller than most vulnerabilities but more lucrative for spies with specific targets.

While the FBI looks into Juniper's unauthorized code, plenty of people are investigating on their own, and in their minds, state-sponsored adversaries are likely to blame for the backdoors. It's easy to see why. The NSA, GCHQ, China, Russia, Iran, and plenty of other countries routinely conduct cyber-espionage. The US and China, for instance, **just reached** an agreement about corporate cyber-espionage, without addressing state spying. It isn't hard to imagine that at least one, if not multiple countries are behind Juniper's backdoors. Researchers have provided compelling evidence for each case.

One early suspect is the NSA, thanks to a quirk of the backdoor itself. The mysterious code worked through a faulty random number generator, a modified version of an NSA-linked generator called Dual_EC_DRBG. The NSA is thought

to have **built a backdoor into Dual_EC_DRBG** in 2006, ultimately paying security company RSA \$10 million **to build it into products**. But while Juniper's backdoors resemble Dual_EC's, the tactics have been public for years and it's more likely that a malicious attacker or group copied them, Mitchel Sahertian, a senior security expert at Fox-IT, told *The Verge*. Others have also expressed skepticism, like respected cryptologist Matt Blaze.



Other aspects of the attack point to Britain's surveillance agency, the GCHQ. **In 2010**, the agency broke into the computer systems of Belgium's largest telecommunications provider, Belgacom, breaking through a number of Juniper VPN gates along the way. Despite extensive documents leaked by Edward Snowden, it's never been entirely clear how the GCHQ broke through, but a tool like the ScreenOS backdoor would have given them easy access to the company's internal networks. There's still no firm evidence linking the GCHQ to the hack, but the coincidence has raised a number of eyebrows in the security world.



At the same time, others are pointing at China. *The Register* cited a tip from a former Juniper staffer to make the case for Chinese actors. In 2004, Juniper acquired NetScreen, which was founded by Chinese nationals, and it's reasonable to believe that some ScreenOS code could have originated in the country, too. Juniper wouldn't say whether any of its code came from its Beijing offices, and *The Register* didn't draw further connections beyond pointing out a possible Chinese link.

JUNIPER WOULDN'T SAY WHETHER ANY OF ITS CODE CAME FROM ITS BEIJING OFFICES

But while researchers are still looking for clues as to who planted the backdoor, it's already clear they were sophisticated actors, and knew exactly what they were up to. The code stayed secret for three years because it was well hidden. According to Moore, its password was designed to look like the rest of the OS's. One remote access vulnerability is difficult to keep hidden, he says, but add in another backdoor and it's "hard to pull off." He says Juniper needs to "document how the [VPN] backdoor went undetected for so long," although it is doing at least a decent job at transparency already. As the company continues to release information on the apparent attack and researchers scrutinize Juniper's products, Moore warns more vulnerabilities will likely be discovered.

"The only thing I can say is patch," he says.

CrunchBase

Juniper Networks

Overview

Timeline

Followers

Contributors

STATISTICS

★
28

👁️
10K

ADD TO THIS PROFILE
TOP CONTRIBUTORS

⊕
CONTRIBUTE

Overview

UPDATE

Acquisitions

11 Acquisitions

IPO / Stock

Went Public on Jun 25, 1999 / NASDAQ:JNPR

Headquarters:

Sunnyvale, CA

Description:

Juniper Networks is a news network that designs, develops, and sells products and services, along with network infrastructure.

Founders:

Pradeep Sindhu

Categories:

Security, Technology, Communications Hardware

Website:

http://www.juniper.net

Social:



Company Details

UPDATE

Founded:

February 6, 1996

Contact:

social-media@juniper.net | (888) 586-4737

Employees:

5k - 10k | [46 in CrunchBase](#)

Juniper Networks is a news network that designs, develops, and sells products and services, which together provide its customers with network infrastructure. Its aim is to create innovative products and solutions that meet the growing demands of the connected world. The company has 9,000 employees in 70 countries and nearly 5 billion U.S. dollars in revenue. Its customers include the top 100 global service providers and 30,000 enterprises, including the Global Fortu ...

[See More](#)

Funding Rounds (2) - \$120.61M

UPDATE

Date	Amount / Round	Valuation	Lead Investor	Investors
Jan, 2014	\$18.85M / Post Ipo Equity	—	—	0
Dec, 2012	\$101.76M / Post Ipo Equity	—	—	0

Acquisitions (11)

UPDATE

Date	Acquired	Amount
Dec 16, 2013	Wandl	\$60M (terms undisclosed)

Feb 8, 2013	Webscreen Technology	Unknown
Dec 13, 2012	Contrail Systems	\$176M in Cash & Stock
Feb 22, 2012	Mykonos Software	\$80M in Cash
Dec 6, 2010	Altor Networks	\$95M in Cash
Nov 18, 2010	Blackwave	Unknown
Nov 16, 2010	Trapeze Networks	\$152M in Cash
Jul 27, 2010	SMobile Systems	\$70M (terms undisclosed)
Apr 8, 2010	Ankeena Networks	Unknown
Mar 29, 2005	Kagoor Networks	\$67.5M in Cash

ALL ACQUISITIONS

Investments (25)

Vectra investors include Accel Partners, Intel, Juniper Networks - All Spy State Cartel Members

Date	Invested In	Round	Partner(s)
Sep, 2015	Vectra Networks	\$35M / Series D	—
Jan, 2015	Fastback Networks	\$15M / Series C	Jeff Lipton
Aug, 2014	Vectra Networks	\$25M / Series C	—
Jul, 2014	Vidyo	\$20M / Series E	—
Jun, 2014	Wickr Inc.	\$30M / Series B	—
Apr, 2014	Enplug	\$2.5M / Seed	—
Jan, 2014	Gainspeed	\$10M / Series B (Lead)	Frank Marshall
May, 2013	Cloudscaling	\$10M / Series B	—
May, 2013	Fastback Networks	\$15M / Series B	Jeff Lipton
Jan, 2013	Illumio	\$8M / Series A	—
Jan, 2013	FireEye	\$50M / Series F	—
Aug, 2012	Typesafe	\$14M / Series B	—
May, 2012	Vidyo	\$2M / Venture	—
Mar, 2012	Violin Memory	\$50M / Series D	Iqbal Ottamalika
Jun, 2011	Cotendo	\$17M / Series D	—

Feb, 2011	Violin Memory	\$35M / Series B	Iqlas Ottamalika
Dec, 2010	Sentrigo	\$6M / Series C	—
Mar, 2010	Altor Networks	\$10M / Series B	—
Sep, 2009	BLADE Network Technologies	\$10M / Series B	—
May, 2008	FireEye	\$14.5M / Series C	—
Nov, 2006	Apigee	\$16M / Series B	—
Aug, 2006	Trapeze Networks	\$30M / Series D	—
Aug, 2006	FireEye	\$14.5M / Series B	—
May, 2002	Nominum	\$10M / Series B	—
Nov, 2001	Zambeel,Inc.	\$52.6M / Series B	—

ALL INVESTMENTS ➔

Current Team (46)

UPDATE

Luis Avila-Marco
EVP, Strategy & Corporate Development

Bindurani Bali
Talent Acquisition

Michael Banic
Team Member

Mike Banic
VP, Product Marketing, Ethernet Switching

Taps Barclays
CEO

ALL CURRENT TEAM ➤

Board Members and Advisors (10)

UPDATE

Bob Calderoni
Interim CEO & President @ Citrix Systems
Member of the Board of Directors (since 2003)

Gary Daichendt
Founder @ Theory R Properties
Member of the Board of Directors (since 2014)

Kevin DeNuccio
President & CEO @ Violin Memory
Member of the Board of Directors (since 2014)

Jim Dolce
CEO @ Lookout
Member of the Board of Directors (since 2015)

ALL BOARD MEMBERS AND ADVISORS ➤

News (1,777)

UPDATE

Date	News
Dec 22, 2015	Financial Express - Cisco reviews code after Juniper breach; more scrutiny expected
Dec 22, 2015	DSL Reports - Juniper Backdoor Deflates US Government Demand For Backdoors
Dec 22, 2015	The Verge - Who hid a backdoor in a popular corporate VPN program?
Dec 11, 2015	Business Wire - Research and Markets: The Big Data Market: 2015 - 2030 - Growth of 14% Over Next 5 Years
Dec 11, 2015	iAM Wire - LocalCircles Raises Funding from Anand Mahindra
Dec 11, 2015	Business Wire - Research and Markets: Global Threat Intelligence Security Market Worth USD \$5,860.5 Million by 2020 - Analysis, Trends & Forecast 2015-2020
Dec 10, 2015	PRNewswire All - Predictive Analytics Market: 27% CAGR Forecast to 2020 with North America Leading Revenue Generation
Dec 10, 2015	PRNewswire UK All - Global Social Media IT Spending Market 2015-2019 - Leading Vendors are IBM, HP, Oracle, Dell, Cisco, Salesforce & HubSpot

ALL NEWS 

@JuniperNetworks

Loading JuniperNetworks's tweets...

JUNIPER NETWORKS ON TWITTER 

Competitors (7)

UPDATE

Alcatel-Lucent

Alcatel-Lucent provides IP and cloud networking and ultra-broadband fixed and wireless access solutions for service providers.

Check Point Software Technologies

Check Point Software Technologies provides network and IT security software and hardware.

Cisco

Cisco Systems is an American multinational corporation that designs, manufactures and sells networking equipment.

Extreme Networks

Extreme Networks of Santa Clara, Calif., founded in 1996, is a publicly listed company that designs, builds, and installs sophisticated

Fortinet

Fortinet is a provider of network security appliances that include firewalls, security gateways, and complementary products.

Huawei Technologies

Huawei Technologies provides infrastructure application software and devices with wireline, wireless, and IP technologies.

Palo Alto Networks

Palo Alto Networks produces hardware firewall products that take an app-centric method for traffic classification and enable app visibility.

Palo Alto Investor = Greylock (Reid Hoffman, LinedIn, Facebook, Accel Partners, James W. Breyer);
Therefore, Palo Alto IS NOT A COMPETITOR, but rather a crony.

Offices/Locations (1)

UPDATE

Headquarters

1194 North Mathilda Avenue
Sunnyvale, CA 94089-1206
USA

Past Team (115)

UPDATE

Rahul Aggarwal

David A. Koretz
Director @ [EarthLink](#)

Kirk Appelman
Senior Vice President, Sales @ [CounterTack](#)

ALL PAST TEAM ➔

Event Appearances (11)

UPCOMING EVENT APPEARANCES (1)



Mobile World Congress 2016



February 22, 2016 - February 25, 2016



Fira Gran Via , Av. Joan Carles I, 64 08908 L'Hospitalet de Llobregat, Barcelona, Catalonia, Spain

This will convene industry leaders, visionaries and innovators to explore the trends that will shape mobile in the years ahead.

[Sponsor](#)

[Exhibitor](#)

PAST EVENT APPEARANCES (10)



SC15 on Nov 15, 2015

[Exhibitor](#)



IBM Insight 2015 on Oct 25, 2015

[Sponsor](#)

[Exhibitor](#)



GITEX Technology Week 2015 on Oct 18, 2015


[Sponsor](#)

ALL EVENT APPEARANCES 

Images (1)

UPDATE



 Add Products

 Add Sub Organizations

 Add Memberships

 Add Customers

 Add Partners

 Add Videos