

Cybercrime and the Cloud

Paul J.S. Oliveria



Founded 1988, United States
Headquarters Tokyo, Japan
Market Cap \$5B USD
2016 Sales \$1.2B USD
Customers 500,000 businesses,
Millions of consumers



5200+ Employees,
38 Business units worldwide



Consumers



Small Business

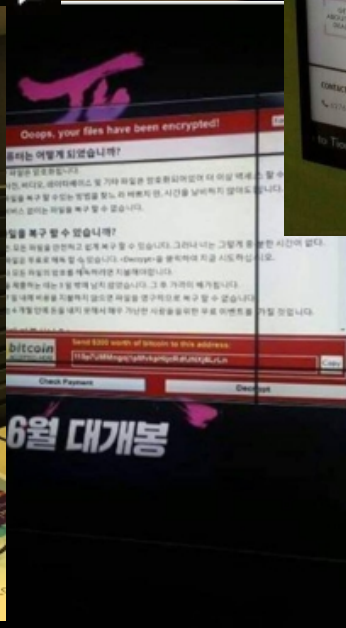
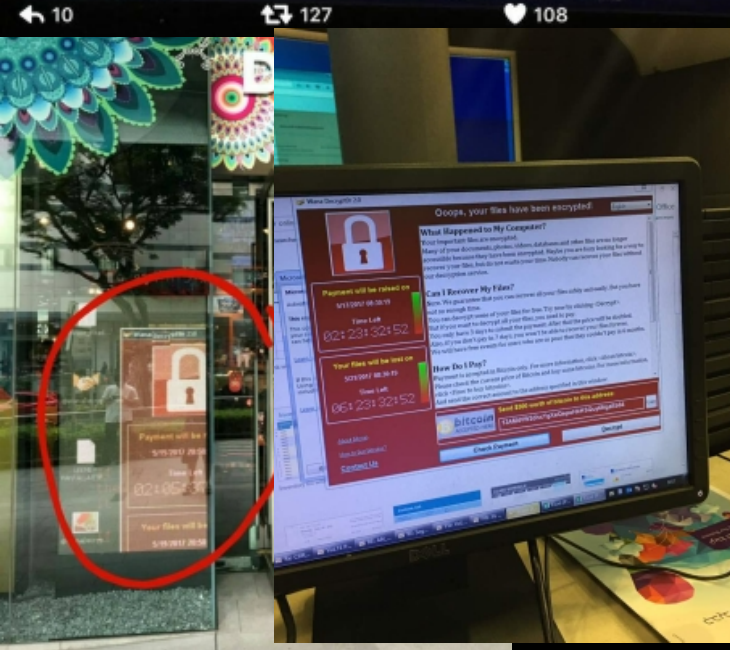
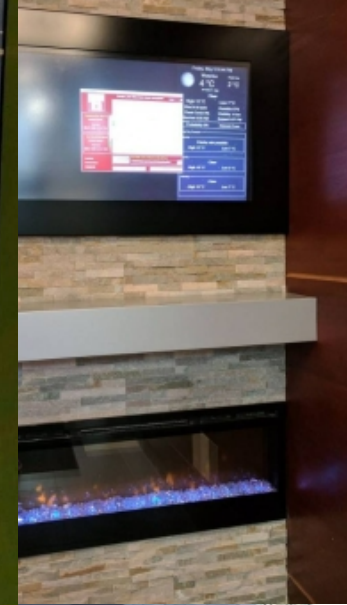
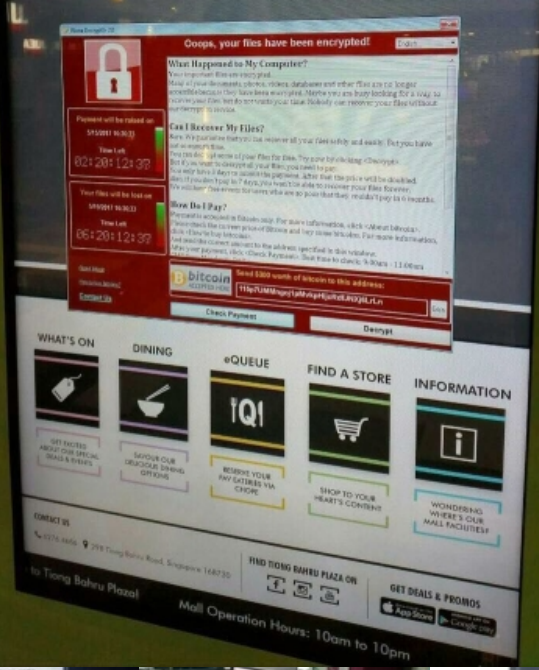
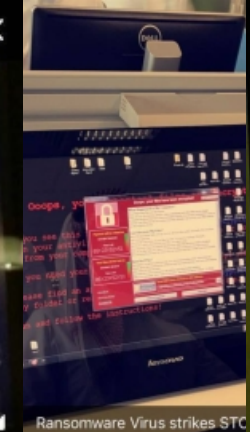
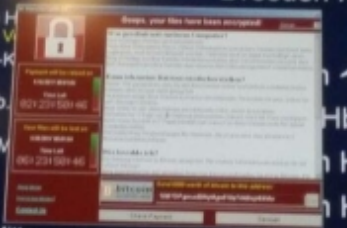


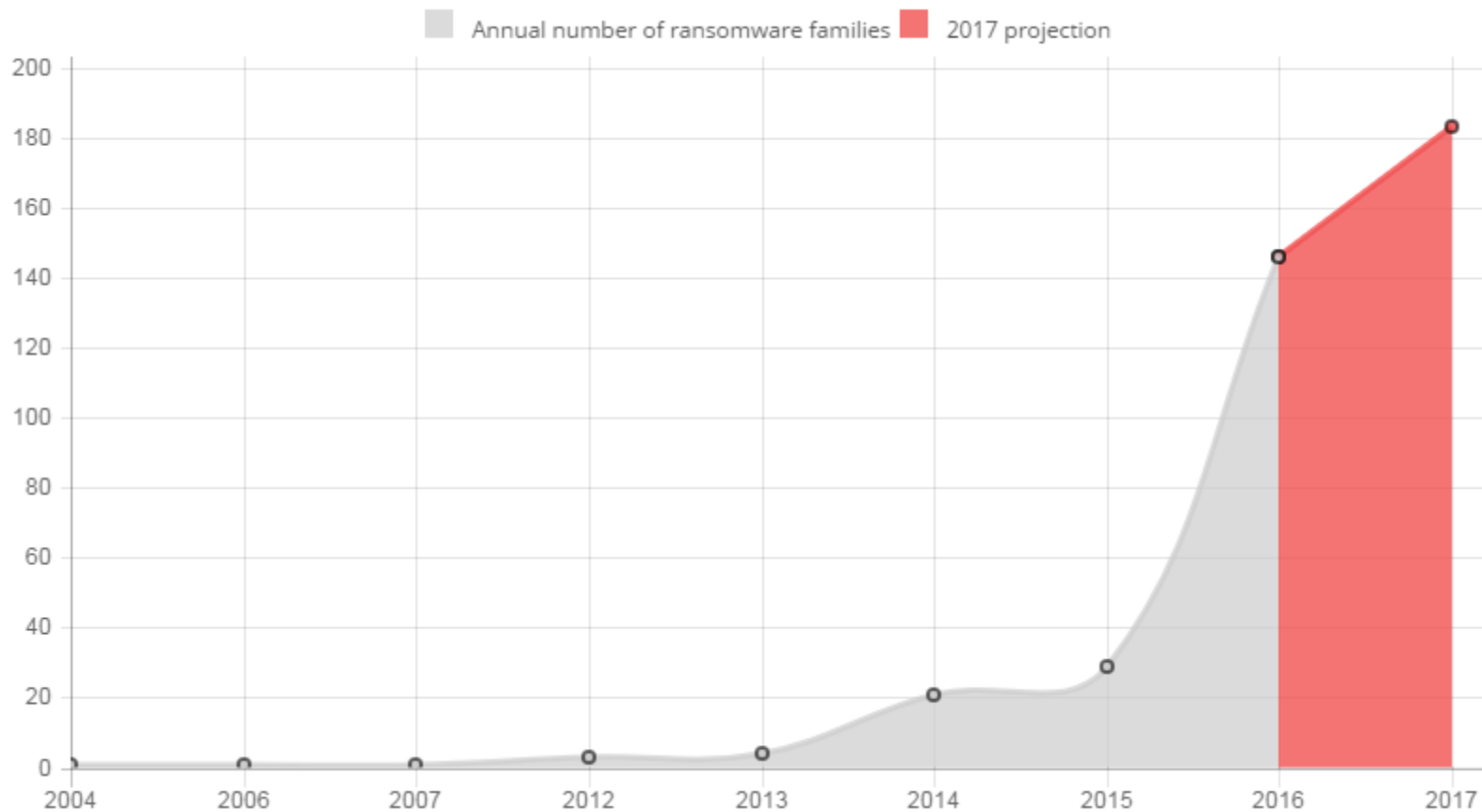
Midsize Business




Enterprise

Zeit	Über	22:10 DB	Nach	Gle
22:15 RB61	Dresden Mitte		Dresden Hbf	8
22:20 S1	Dresden Hbf			2
22:25 S2	Dresden-K			1
22:25 RE50	Coswig (b. Dre)		Hbf	6
22:25 RE50	Dresden M		Hbf	3
22:29 IC 2045	Dresden M		Hbf	7
22:32 S2	Dresden Mitte		Dresden Hbf	2
22:37 S1	Radebeul Ost - Coswig (b. Dre)		Meißen Trieb	1







An urgent e-mail subject requesting immediate fund transfers

BEC scams typically use subject lines that imply urgency regarding payment inquiries or fund transfers.

A spoofed sender domain

CEO fraudsters usually register a domain similar to its target.

Reply Reply All Delete

 **Dennis** <dennis@financialbest.net.au> ←
To: Susan <susan@financialbest.com>
Subject: Quick Request

Wednesday, January 4, 2018 11:00 PM

Hi! Are you available? I need you to take care of a same day domestic transfer for me today. Please let me know the details you need. ←
Get back to me as soon as possible.

Thanks,
Dennis
Chief Executive ←

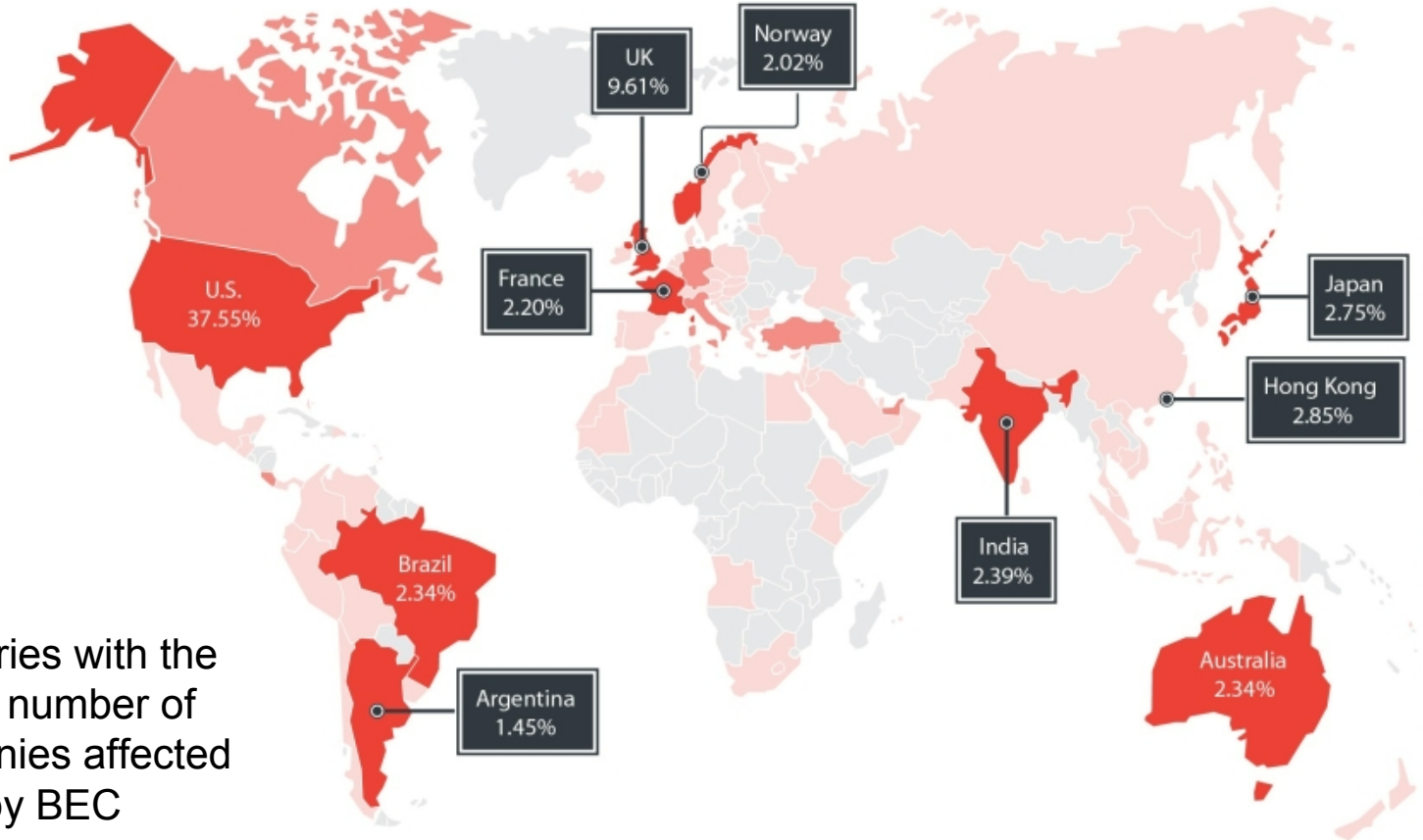
Body of the E-mail

Scammers make it appear as if the fund transfer is urgently needed and should be executed as soon as possible.

Position of the e-mail sender

Cybercriminals employing CEO fraud typically pose as someone influential in an organization.

Countries with the most number of companies affected by BEC



>1.44%

1.44% - 1%

<1%

Unspecified country domains


by Bradley Barth, Senior Reporter

August 01, 2016

Don't be like 'Mike': Authorities arrest mastermind of \$60M online scam operation

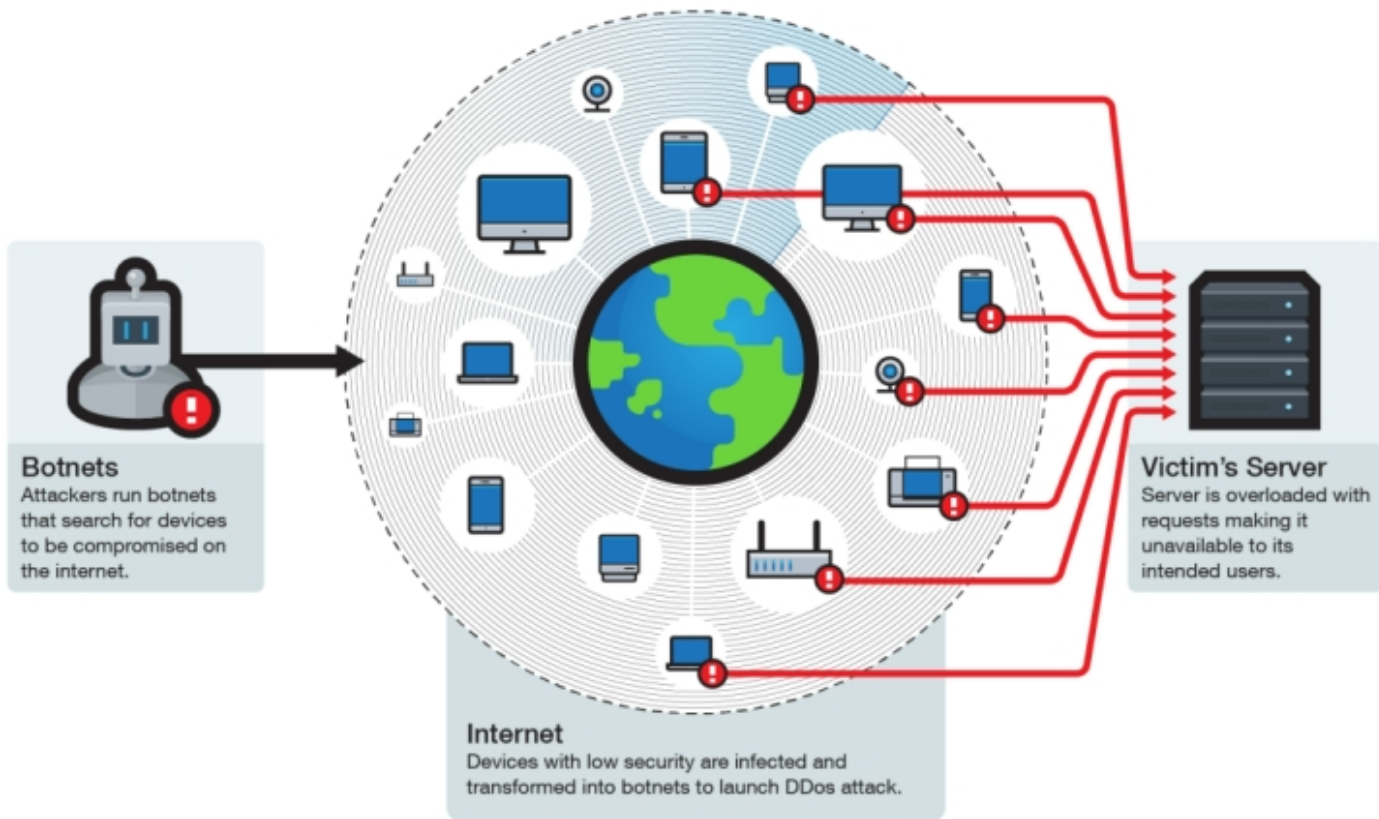


A 40-year-old Nigerian national and alleged online scam artist, accused of bilking his victims out of more than \$60 million, was arrested in Port Harcourt, Nigeria in a joint operation involving **Interpol** and the Nigerian Economic and Financial Crime Commission (EFCC).



Source: <https://www.scmagazine.com/dont-be-like-mike-authorities-arrest-mastermind-of-60m-online-scam-operation/article/529972/>





Home » [Internet of Things](#) » [Persirai: New Internet of Things \(IoT\) Botnet Targets IP Cameras](#)

Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras

Posted on: [May 9, 2017](#) at 5:03 am Posted in: [Internet of Things](#) Author: [Trend Micro](#)



By [Tim Yeh](#), [Dove Chiu](#) and [Kenney Lu](#)

A new Internet of Things (IoT) botnet called Persirai (Detected by Trend Micro as [ELF_PERSIRAI.A](#)) has been discovered targeting over 1,000 Internet Protocol (IP) Camera models based on various Original Equipment Manufacturer (OEM) products. This development comes on the heels of Mirai—an open-source backdoor malware that [caused some of the most notable incidents of 2016](#) via Distributed Denial-of-Service (DDoS) attacks that [compromised IoT devices such as Digital Video Recorders \(DVRs\) and CCTV cameras](#)—as well as the



- Evolving techniques and routines
- Abuse of legitimate services
- Underground economies
- User preparedness/capacity building

- Cybercriminals are stepping up their game and are **capitalizing on industries and economies** that are still behind in terms of cybersecurity
- Due diligence in **understanding information flow** from different sensors to spot anomalies
- Harden overall organizational **business process security**

Thank You!

PAUL_OLIVERIA@TRENDMICRO.COM