security affairs

The FBI requests $38 Million to counter the threat of Going Dark

February 12, 2016 By Pierluigi Paganini

The FBI requests $38 Million to counter the threat of Going Dark, in particular asking more economic resources to break encryption when needed.

The FBI Director James Comey has highlighted in different occasions the difficulties faced by law enforcement when dealing with encryption during their investigations.

Now, the FBI is making its request for budget for the next year, in particular asking more economic resources to break encryption when needed.

Giving a look at the FBI's Fiscal Year 2017 Budget Request document it is possible to find a specific session titled "Going Dark" that reports the following text:

"Going Dark: $38.3 million and 0 positions The requested funding will counter the threat of Going Dark, which includes the inability to access data

analysis, cryptanalytic capability, and forensic tools. Current services for this initiative are 39 positions (11 agents) and 31.0 million."

The FBI asked for $38.3 more million on top of the $31 million already requested in 2015 (a total of $69.3 million) to improve its capabilities to get encrypted data and de-anonymize Internet users.

These numbers demonstrate a significant effort of□ law enforcement to overwhelm the "going dark" problem.

In December, the FBI's Director James Comey called for tech companies currently providing users with end-to-end encryption to review "their business model" and stop implementing it.

The end-to-end encryption allows users to communicate securely on the internet making impossible for law enforcement to eavesdrop the traffic.□

The IT giants implemented the end-to-end encryption in response to the disconcerting revelations of the NSA whistleblower Edward Snowden about mass surveillance operated by the US Government.

"FBI Director James Comey on Wednesday called for tech companies currently offering end-to-end encryption to reconsider their business model, and instead adopt encryption techniques that allow them to intercept and turn over communications to law enforcement when necessary." reported The Intercept.

In the past, the FBI's Director James Comey already requested IT giants to insert a backdoor in their product to allow law enforcement to decrypt data, but the reply of the companies was negative.

The US authorities have been pressuring companies like Apple and Google in public hearings to provide law enforcement access to decrypted communications whenever there's a lawful request.

Given the negative response of the IT companies, it is normal that the FBI and intelligence agencies will opt for hacking techniques to break encryption.

"The days of reliable wiretaps are vanishing. [Hacking] is the next best thing for the FBI," Christopher Soghoian, the principal technologist at the American Civil Liberties Union, told to Lorenzo Bicchierai from MotherBoard.

It is likely the FBI will spend that money to buy hacking tools, including spyware and zero-day exploits, for its investigations.

"38.3 million dollars buys a hell of a lot of malware and zero-day exploits," added Soghoian.

The FBI already used hacking techniques during its investigations, in particular to de-anonymize criminals on the dark web. A few weeks ago emerged more details on the operation conducted against TorMail in 2013.

Pierluigi Paganini

(Security Affairs – Going Dark, FBI)

Share it please ...

encryption FBI Going Dark Hacking Internet law enforcement monitoring surveillance Terrorism

SHARE ON

f g+ in t ✉

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

A replica of AlphaBay market used to steal login credentials

NEXT ARTICLE

UK police arrested teenage hacker who allegedly hacked CIA and FBI officials□

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

[redacted]

[redacted]

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the

ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^