theguardian

WikiLeaks publishes 'biggest ever leak of secret CIA documents'

The 8,761 documents published by WikiLeaks focus mainly on techniques for hacking and surveillance

US consulate in Frankfurt, Germany is home to a 'sensitive compartmentalised information facility', according to the leaked documents. Photograph: Boris Roessler/AP

Ewen MacAskill Defence and security correspondent, Sam Thielman in New York, and Philip Oltermann in Berlin

Tuesday 7 March 2017 16.42 GMT

The US intelligence agencies are facing fresh embarrassment after WikiLeaks published what it described as the biggest ever leak of confidential documents from the CIA detailing the tools it uses to break into phones, communication apps and other electronic devices.

The thousands of leaked documents focus mainly on techniques for hacking and reveal how the CIA cooperated with British intelligence to engineer a way to compromise smart televisions and turn them into improvised surveillance devices.

The leak, named “Vault 7” by WikiLeaks, will once again raise questions about the inability of US spy agencies to protect secret documents in the digital age. It follows disclosures about Afghanistan and Iraq by army intelligence analyst Chelsea Manning in 2010 and about the National Security Agency and Britain’s GCHQ by Edward Snowden in 2013.

The new documents appear to be from the CIA's 200-strong Center for Cyber Intelligence and show in detail how the agency's digital specialists engage in hacking. Monday's leak of about 9,000 secret files, which WikiLeaks said was only the first tranche of documents it had obtained, were all relatively recent, running from 2013 to 2016.

The revelations in the documents include:

CIA hackers targeted smartphones and computers.

The Center for Cyber Intelligence, based at the CIA headquarters in Langley, Virginia, has a second covert base in the US consulate in Frankfurt which covers Europe, the Middle East and Africa.

A programme called Weeping Angel describes how to attack a Samsung F8000 TV set so that it appears to be off but can still be used for monitoring.

The CIA declined to comment on the leak beyond the agency's now-stock refusal to verify the content. "We do not comment on the authenticity or content of purported intelligence documents," wrote CIA spokesperson Heather Fritz Horniak. But it is understood the documents are genuine and a hunt is under way for the leakers or hackers responsible for the leak.

WikiLeaks, in a statement, was vague about its source. "The archive appears to have been circulated among former US government hackers and contractors in an unauthorised manner, one of whom has provided WikiLeaks with portions of the archive," the organisation said.

The leak feeds into the present feverish controversy in Washington over alleged links between Donald Trump's team and Russia. US officials have claimed WikiLeaks acts as a conduit for Russian intelligence and Trump sided with the website during the White House election campaign, praising the organisation for publishing leaked Hillary Clinton emails.

Asked about the claims regarding vulnerabilities in consumer products, Sean Spicer, the White House press secretary, said: "I'm not going to comment on that. Obviously that's something that's not been fully evaluated."

Asked about Trump's praise for WikiLeaks during last year's election, when it published emails hacked from Clinton's campaign chairman, Spicer told the Guardian: "The president said there's a difference between Gmail accounts and classified information. The president made that distinction a couple of weeks ago."

Julian Assange, the WikiLeaks editor-in-chief, said the disclosures were "exceptional from a political, legal and forensic perspective". WikiLeaks has been criticised in the past for dumping documents on the internet unredacted and this time the names of officials and other information have been blacked out.

WikiLeaks shared the information in advance with Der Spiegel in Germany and La Repubblica in Italy.

Edward Snowden, who is in exile in Russia, said in a series of tweets the documents seemed genuine and that only an insider could know this kind of detail. He tweeted:

The document dealing with Samsung televisions carries the CIA logo and is described as secret. It adds "USA/UK". It says: "Accomplishments during joint workshop with MI5/BTSS (British Security Service) (week of June 16, 2014)."

It details how to fake it so that the television appears to be off but in reality can be used to monitor targets. It describes the television as being in "Fake Off" mode. Referring to UK

involvement, it says: “Received sanitized source code from UK with comms and encryption removed.”

WikiLeaks, in a press release heralding the leak, said: “The attack against Samsung smart TVs was developed in cooperation with the United Kingdom’s MI5/BTSS. After infestation, Weeping Angel places the target TV in a ‘Fake Off’ mode, so that the owner falsely believes the TV is off when it is on. In ‘Fake Off’ mode the TV operates as a bug, recording conversations in the room and sending them over the internet to a covert CIA server.”

The role of MI5, the domestic intelligence service, is mainly to track terrorists and foreign intelligence agencies and monitoring along the lines revealed in the CIA documents would require a warrant.

The Snowden revelations created tension between the intelligence agencies and the major IT companies upset that the extent of their cooperation with the NSA had been exposed. But the companies were primarily angered over the revelation the agencies were privately working on ways to hack into their products. The CIA revelations risk renewing the friction with the private sector.

The initial reaction of members of the intelligence community was to question whether the latest revelations were in the public interest.

A source familiar with the CIA’s information security capabilities took issue with WikiLeaks’s comment that the leaker wanted “to initiate a public debate about cyberweapons”. But the source said this was akin to claiming to be worried about nuclear proliferation and then offering up the launch codes for just one country’s nuclear weapons at the moment when a war seemed most likely to begin.

Monday’s leaks also reveal that CIA hackers operating out of the Frankfurt consulate are given diplomatic (“black”) passports and US State Department cover. The documents include instructions for incoming CIA hackers that make Germany’s counter-intelligence efforts appear inconsequential.

The document reads:

“Breeze through German customs because you have your cover-for-action story down pat, and all they did was stamp your passport.

Your cover story (for this trip):

Q: Why are you here?

A: Supporting technical consultations at the consulate.”

The leaks also reveal a number of the CIA’s electronic attack methods are designed for physical proximity. These attack methods are able to penetrate high-security networks that are disconnected from the internet, such as police record databases. In these cases, a CIA officer, agent or allied intelligence officer acting under instructions, physically infiltrates the targeted workplace. The attacker is provided with a USB stick containing malware developed for the CIA for this purpose, which is inserted into the targeted computer. The attacker then infects and extracts data.

A CIA attack system called Fine Dining provides 24 decoy applications for CIA spies to use. To witnesses, the spy appears to be running a programme showing videos, presenting slides,

playing a computer game, or even running a fake virus scanner. But while the decoy application is on the screen, the system is automatically infected and ransacked.

The documents also provide travel advice for hackers heading to Frankfurt: “Flying Lufthansa: Booze is free so enjoy (within reason).”

The rights group Privacy International, in a statement, said it had long warned about government hacking powers. “Insufficient security protections in the growing amount of devices connected to the internet or so-called ‘smart’ devices, such as Samsung smart TVs, only compound the problem, giving governments easier access to our private lives,” the group said.

More
WikiLeaks
CIA Julian Assange news