NSA has 'industrial scale' malware for spying

March 12 2014

The National Security Agency (NSA) headquarters at Fort Meade, Maryland, as seen from the air, January 29, 2010

The National Security Agency has developed malware that allows it to collect data automatically from millions of computers worldwide, a report based on leaked documents showed Wednesday.

The report co-authored by former Guardian reporter Glenn Greenwald for the online news site The Intercept said the program has dramatically expanded the US spy agency's ability to covertly hack into computers on a mass scale.

The report is based on classified documents provided by former NSA contractor Edward Snowden.

It said the surveillance technology allows the NSA to infect potentially millions of computers worldwide with malware "implants" which can help the agency extract data from overseas Internet and phone networks.

The report by Greenwald and reporter Ryan Gallagher said these implants were once reserved for a few hundred hard-to-reach targets whose communications could not be monitored through traditional wiretaps but that the NSA has expanded this to "industrial scale," according to the documents.

The automated system codenamed TURBINE expands the ability to gather intelligence with less human oversight, according to the report.

The report was the first by Greenwald based on leaked documents since he joined First Look Media, an organization backed by tech entrepreneur Pierre Omidyar that includes The Intercept.

Greenwald was among the first journalists to publish documents leaked by Snowden describing the vast surveillance programs of the NSA and other intelligence services, sparking a massive outcry.

Wednesday's report said the covert infrastructure that supports TURBINE operates from the NSA headquarters in Maryland, and from eavesdropping bases in Britain and Japan and that the British intelligence agency GCHQ appears to have played an important role in the effort.

The report said that in some cases the NSA has used a decoy Facebook server to infect a target's computer and exfiltrate files.

It said the malware can also covertly record audio from a computer's

microphone and take snapshots with its webcam.

The Intercept said the malware has been in existence since 2004 but that the automated program expanding its use appears to have begun in 2010.

The malware can be installed in as little as eight seconds, according to the documents.

Because people have become suspicious of email attachments, the report said the NSA has had to resort to new tools to install the malware such as "man-in-the-middle" and "man-on-the-side" attacks through Internet browsers.

The NSA, queried by AFP, did not directly respond to the report. But an NSA official reiterated policy that its operations are conducted "exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes."