SandWorm hacking team exploited 0-day against NATO and other Government entities

October 14, 2014 By Pierluigi Paganini

iSIGHT Partners firm uncovered a Russian hacking team dubbed Sandworm that was running a cyber espionage campaign on NATO and other Government entities.

According to a new report issued by the cyber security firm iSIGHT Partners a group of Russian hackers has been exploiting a previously unknown flaw in Microsoft's Windows operating system to spy on NATO, the Ukrainian government, a U.S. university researcher and many other entities. The researchers at ISight dubbed the hacking group SandWorm because of references discovered in its code to the science-fiction novel "Dune."

The experts at iSIGHT Partners have worked in close collaboration with Microsoft during the investigation, the company announced the discovery of a zero-day vulnerability affecting all supported versions of Microsoft Windows and Windows Server 2008 and 2012. The vulnerability has been classified with the code CVE-2014-4114, and according the revelation made by iSIGHT is has been exploited in cyber espionage operation on a large scale by a Russia hacking team, the nature of the target and the tactics, techniques, and procedures (TTP) adopted lead the experts to believe that this is the work of state-sponsored hackers.

"This is consistent with espionage activity," said iSight Senior Director Stephen Ward. "All indicators from a targeting and lures perspective would indicate espionage with Russian national interests."

Microsoft is already working on a security update for the CVE-2014-4114 that will be available in the next patch updates on the October 14th.

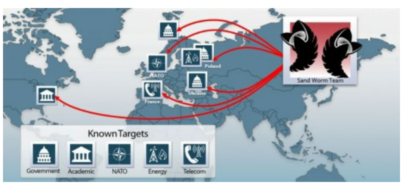
According to the report issued by iSIGHT, the APT has been active since at least 2009, Its targets in the recent campaign also included a Polish energy firm, a Western European government agency and also a French telecommunications firm.

iSIGHT_Partners sandworm timeline_13oct2014

The experts began the investigation in late 2013 when the NATO alliance was targeted by the SandWorm hacking team with exploits other than the zero-day, but they discovered the critical zero-day in August, when the group targeted the Ukrainian government, in the lead-up to the NATO summit in Wales.

"In late August, while tracking the Sandworm Team, iSIGHT discovered a spear-phishing campaign targeting the Ukrainian government and at least one United States organization. Notably, these spear-phishing attacks coincided with the NATO summit on Ukraine held in Wales." states the report published by iSIGHT.

Security experts speculated that the intensification of the cyber dispute between Russian and Ukraine could have increased the likelihood to discover operations that went under the radar for so long.



Below chronological details provided by the researchers on the Sandworm activity:

- *The NATO alliance was targeted as early as December 2013 with exploits other than the zero-day*
- *GlobSec attendees were targeted in May of 2014 with exploits other than the zero-day*
- *June 2014*
  - *Broad targeting against a specific Western European government*
  - *Targeting of a Polish energy firm using CVE-2013-3906*
  - *Targeting of a French telecommunications firm using a BlackEnergy variant configured with a Base64-encoded reference to the firm*

The SandWorm hacking team sent spear-phishing emails with a malicious attachments to compromise the victim's machine, the threat actors mentioned a global security forum on Russia and a purported list of Russian terrorists.

Another element that suggests Russia is responsible for the cyber espionage campaign are codes discovered on the C&C server, located in Germany, that had not been properly secured and that contains Russian-language computer files that had been uploaded by the hackers.

"They could have closed it off, and they didn't," he said of the server. "It was poor operational security."

The investigators noticed that SandWorm apparently re-engineered malware previously by other APT probably to masquerade its campaigns.

Read the full post for further information.

Pierluigi Paganini

(Security Affairs – **Sandworm, cyber espionage)**

Share this...

APT CVE-2014-4114 cyber espionage Cybercrime Hacking NATO Russia Sandworm Ukraine zero-Day

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 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
Reflected File Download attack to spread 0-Day Worm Over Any Social Networks

NEXT ARTICLE
7 million DropBox credentials apparently leaked

YOU MIGHT ALSO LIKE

Trend Micro addresses two issues exploited by hackers in the wild
March 18, 2020 By Pierluigi Paganini

TrueFire Guitar tutoring website was hacked, financial data might have been exposed
March 18, 2020 By Pierluigi Paganini

Yoroi Blog

Copyright 2015 Security Affairs by Pierluigi Paganini All Right Reserved.