October 14, 2014

‘Sandworm Team’ exploits zero-day bug in espionage campaign

Adam Greenberg

iSIGHT is calling the group “Sandworm Team” after observing various references to science fiction novel Dune during their research.

A group of cybercriminals believed to be Russian are leveraging vulnerabilities – including a zero-day vulnerability impacting multiple versions of Microsoft Windows – to deliver malware and gather information from various organizations around the world, according to cyber threat intelligence firm iSIGHT Partners.

The North Atlantic Treaty Organization (NATO), a university in the U.S., a Polish energy firm, a French telecommunications firm, a Western European government agency, and public and private sector organizations in Poland and Ukraine are among those targeted by the group, which iSIGHT is referring to as “Sandworm Team” after observing various references to science fiction novel *Dune* during their research, according to an iSIGHT Partners report emailed to SCMagazine.com on Tuesday.

“One thing to note, we only have limited visibility into [the group],” John Hultquist, iSIGHT Cyber Espionage Threat Team senior manager, told SCMagazine.com on Tuesday. “We have confirmed a few targets, but we anticipate that the scope is far greater than we can see.”

Spear phishing is the number one vector of attack being used by Sandworm Team, Drew Robinson, senior technical analyst at iSIGHT, told SCMagazine.com on Tuesday. The group crafts fairly well formatted emails that are of interest to the victim, he said, explaining the messages typically contain an attachment that, when opened, exploits a vulnerability and delivers BlackEnergy malware.

BlackEnergy is a plugin-based trojan, meaning plugins can be written and used for nearly any purpose, including keylogging, audio recording, and screenshot grabbing, Robinson said. Sandworm Team uses variants of the malware referred to as BlackEnergy 2 and BlackEnergy 3, or BlackEnergy Lite, Hultquist said.

“What’s different from [other groups is] what’s being taken here,” Hultquist said. “They’re taking email, they’re taking documents, they’re taking knowledge – not data. It’s about esoteric knowledge an attacker can take to gain an advantage.”

Among the exploits being used by Sandworm Team to deliver BlackEnergy and gain footholds in organizations is CVE-2014-4114, a zero-day vulnerability in Windows OLE that impacts multiple versions of the operating system and could enable remote code execution. On Tuesday, Microsoft addressed the issue, which was deemed fairly dangerous by Robinson.

Other vulnerabilities being used include CVE-2010-3333, CVE-2012-0158, CVE-2013-3906, and CVE-2014-1761, all of which enable the group to remotely execute arbitrary code, according to the report, which adds that WinRAR bug OSVDB-62610 was also exploited.

Sandworm Team has been operating since 2009 and has stayed under the radar for so long due to careful planning, which includes compressing and encrypting their malware and employing HTTPS to hide their traffic, Robinson said. Hultquist added that access to a zero-day vulnerability helps.

“I think it’s possible that they have access to other zero-day’s,” Hultquist said.

TOPICS: CRITICAL INFRASTRUCTURE CYBER ESPIONAGE GOVERNMENT MALWARE PATCH RESEARCH

Related Articles

Group infects more than 500K systems, targets banking credentials in U.S.

APT ‘Nitro’ group attacks again in 2014

‘Moafee’ and ‘DragonOK’ APT groups leverage similar attack tools, techniques

MOST POPULAR

Popular Emailed Recent

Coronavirus, Trump threats, geopolitical campaigns - how they affect your business & what you should do

Cymatic offers free cybersecurity tool for schools for remote learning

Coronavirus tracking app locks up Android phones for ransom

Checkmarx sold for $1.15 billion

Years-long malware operation hides njRAT in cracked hacking tools