Sandworm APT Team Found Using Windows Zero Day Vulnerability

Author:
Dennis Fisher
October 14, 2014
/ 6:11 am

3 minute read

Share this article:

A cyberespionage team, possibly based in Russia, has been using a Windows zero day vulnerability to target a variety of organizations in several countries, including the United States, Poland, Ukraine and western Europe.

UPDATE–A cyberespionage team, possibly based in Russia, has been using a Windows zero day vulnerability to target a variety of organizations in several countries, including the United States, Poland, Ukraine and western Europe. The vulnerability, which will be patched today by Microsoft, is trivially exploitable and researchers say that the team behind the attacks has been using it since August to deliver the Black Energy malware.

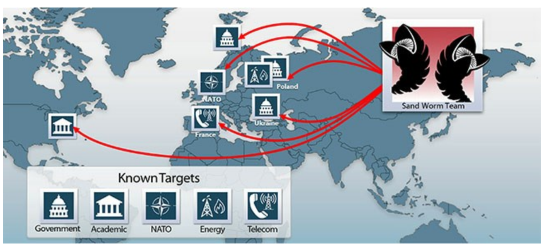
Researchers at iSIGHT Partners said that the team, which they've dubbed Sandworm, likely has been active since 2009 and has been using the Windows vulnerability CVE-2014-4114 in conjunction with a series of other flaws in order to compromise users at government agencies, NATO, academic institutions, a telecom, defense and energy firms. The attackers use highly targeted spearphishing emails in order to lure users into opening a rigged PowerPoint file that contains the exploit code for the vulnerability. Once the exploit code fires, it then downloads the Black Energy malware and begins gathering sensitive data for exfiltration.

Researchers at iSIGHT said that the malware steals sensitive documents, SSL keys and code-signing certificates, among other things. The Windows zero day affects all currently supported versions of Windows and researchers said that exploiting the bug is extremely simple. The exploit code can be loaded into any Office document and when it executes, the machine doesn't crash, so the user is likely unaware of the attack.

"It is extremely easy to recreate. This requires a low level of technical expertise to recreate," said Drew Robinson, senior technical analyst at iSIGHT.

The iSIGHT researchers reported the Windows vulnerability to Microsoft on Sept. 5, and also began notifying its partners and customers in various sectors about the ongoing Sandworm campaign.

The spearphishing emails sent to victims are highly customized to appeal to the recipients' interests, such as a white paper targeted at attendees of the GlobeSec conference. Other documents are specifically targeted at users in countries such as Poland and Ukraine, Robinson said. The iSIGHT researchers said the company has seen about 12 organizations targeted with the Windows zero day thus far, beginning in August. In each case, the attack results in the installation of Black Energy, a venerable Trojan that's been used in a variety of attacks for several years.



"Everything we're seeing is Black Energy," Robinson said. "It's probably in part because it's a modular framework and they can do whatever they want on victims' computers."

Black Energy has gone through several iterations and iSIGHT said that the Sandworm attackers are using Black Energy 2, an intermediate version that includes DDoS capabilities and the ability to steal financial credentials.

Researchers at Kaspersky Lab have been looking at the Black Energy 2 malware attacks for a long time, and Alex Gostev, chief security expert of the GReAT Team at Kaspersky, said identifying these attackers as Russian could be premature.

"The number of cyber espionage operations is growing from one month to the next. Some of these operations stand out for various reasons: sophisticated malware, skills of the cybercriminals, or the resources that enable them to continue their espionage activities for a long period or buy expensive zero-days. Any of the above may indicate that an espionage operation is connected with the work of government-controlled structures but proving this connection is extremely difficult – it is the work of investigation agencies, rather than IT security companies," Gostev said.

"Cybercriminals may leave traces indicating that they speak a certain language or belong to a certain ethnic group in order to mislead investigators. Moreover, people in many post-Soviet countries communicate in Russian, particularly in the information technology sector. Therefore, making conclusions about a 'Russian' trace based on this evidence is ill-advised. The files/documents that the cybercriminals are after do not provide sufficient evidence from which to draw firm conclusions either."

The team using the CVE-2014-4114 zero day has been active for a number of years, and iSIGHT researchers said that the attacks identified most recently have similarities to older operations and has been observed using traditional crimeware tactics in the past. The attack infrastructure the Sandworm team used in these recent attacks also overlaps in some cases with proxies used in other operations. Robinson said that the Sandworm team most likely is based in Russia, a conclusion based on the group's target selection, the use of Black Energy and technical details in the attacks.

Despite some similarities, iSIGHT researchers said that the Sandworm team doesn't appear to be related to the Energetic Bear attackers who have been tied to other APT campaigns recently.

This article was updated on Oct. 14 to add the comments from Gostev.

Image from Flickr photos of Mark Skeet.

Share this article:

Critical Infrastructure Government Hacks Malware Vulnerabilities

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 15, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

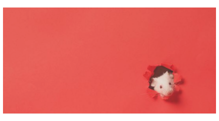
Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

The Case for Cyber-Risk Prospectuses
December 24, 2019 1

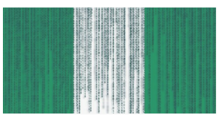
Twitter
RT @Techmeme: Study: Microsoft Edge sends frequent hashed IDs tied to hardware to its back-end servers, making it one of the least private...
12 mins ago
Follow @threatpost

SUGGESTED ARTICLES



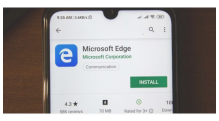
APT36 Taps Coronavirus as 'Golden Opportunity' to Spread Crimson RAT

The Pakistani-linked APT has been spotted infecting victims with data exfiltration malware.
March 17, 2020



Activities of a Nigerian Cybercriminal Uncovered

Rise and fall of a Nigerian cybercriminal called 'Dton,' who made hundreds of thousands of dollars in a 7-year campaign, outlined in new report.
March 17, 2020



Microsoft Edge Shares Privacy-Busting Telemetry, Research Alleges

An academic study found Microsoft's Edge browser to be the least private, due to it sending device identifiers and web browsing pages to back-end servers.
March 16, 2020

DISCUSSION