Sandworm Zero Day Vulnerability | iSIGHT Partners

By By Stephen Ward

Published: 2014-10-14 · Archived: 2026-04-05 22:22:27 UTC

SandWorm Zero Day Vulnerability Team impacting all versions of Microsoft Windows – used in Russian cyber-espionage campaign targeting NATO, European Union, Telecommunications and Energy sectors

---

UPDATE – 10/21/14

Since our disclosure last week of Sandworm Team, the cyber espionage operators who were using the CVE-2014-4114 zero-day, excellent work by others in the community has shed new light on aspects of their behavior we were previously unaware of. We are still uncovering new facets of this campaign, such as targeting, malware, and innovative command and control methods, but perhaps most disconcerting is their interest in the software which runs critical infrastructure.

We have new details of SCADA system targeting – we are still uncovering more information but you can read these details here

---

Last week, (Thursday, October 16, 2014) iSIGHT Partners held a briefing to any interested parties surrounding the Sandworm Team disclosure – you may access the on-demand version of that briefing here.

ALSO – a hat-tip to the team at Recorded Future – an interesting piece of work showing discovery of Sandworm Team IOCs using Recorded Future Maltego transforms…check their piece here

---

Original Post

On Tuesday, October 14, 2014, iSIGHT Partners – in close collaboration with Microsoft – announced the discovery of a zero-day vulnerability impacting all supported versions of Microsoft Windows and Windows Server 2008 and 2012.

Microsoft is making a patch for this vulnerability available as part of patch updates on the 14th – CVE-2014-4114.

Exploitation of this vulnerability was discovered in the wild in connection with a cyber-espionage campaign that iSIGHT Partners attributes to Russia.

Visible Targets

Visibility into this campaign indicates targeting across the following domains. ***It is critical to note that visibility is limited and that there is a potential for broader targeting from this group (and potentially other threat actors) using this zero-day.***

- NATO
- Ukrainian government organizations
- Western European government organization
- Energy Sector firms (specifically in Poland)
- European telecommunications firms
- United States academic organization

Requests for Technical Indicators / For More Information

High level details of this campaign – including iSIGHT's assessment of the actors behind it – can be found below. Further information was provided in a ***briefing to any interested parties*** on Thursday, October 16th at 2:00 p.m. eastern – ***you may access the on-demand version of that briefing here***.

To support organizations in determining their potential exposure to this campaign, ***iSIGHT is making available a broader technical report – inclusive of indicators – through a formal vetting process.***

To request the full technical report, please follow this link and complete the necessary information. Note that you will need to provide professional credentials including work email and telephone and that iSIGHT may contact you to verify those credentials prior to releasing the report.

If you have a media related inquiry regarding this disclosure, please contact iSIGHT at 703.994.9349 or ***by sending email to*** isightpartners@okco.com.

High Level on Sandworm – Cyber Espionage Campaign Attributed to Russia

As part of our normal cyber threat intelligence operations, iSIGHT Partners is tracking a growing drum beat of cyber espionage activity out of Russia.

We are actively monitoring multiple intrusion teams with differing missions, targets and attack capabilities. We are tracking active campaigns by at least five distinct intrusions teams.

For example, we recently disclosed the activities of one of those teams (dubbed Tsar team) surrounding the use of mobile malware. This team has previously launched campaigns targeting the United States and European intelligence communities, militaries, defense contractors, news organizations, NGOs and multilateral organizations. It has also targeted jihadists and rebels in Chechnya.

We are attributing this particular cyber-espionage campaign to a different intrusion team that iSIGHT has dubbed 'Sandworm Team' based on its use of encoded references to the classic science fiction series Dune in command and control URLs and various malware samples.

The team has been previously referred to as Quedach by F-Secure, which detailed elements of this campaign in September 2014 but only captured a small component of the activities and failed to detail the use of the zero-day vulnerability.

iSIGHT Partners has been monitoring the Sandworm Team's activities from late 2013 and throughout 2014 – the genesis of this team appears to be around 2009. The team prefers the use of spear-phishing with malicious document attachments to target victims. Many of the lures observed have been specific to the Ukrainian conflict with Russia and to broader geopolitical issues related to Russia. The team has recently used multiple exploit methods to trap its targets including the use

of BlackEnergy crimeware, exploitation of as many as two known vulnerabilities simultaneously, and this newly observed Microsoft Windows zero-day.

Some chronological details on Sandworm's targeting…

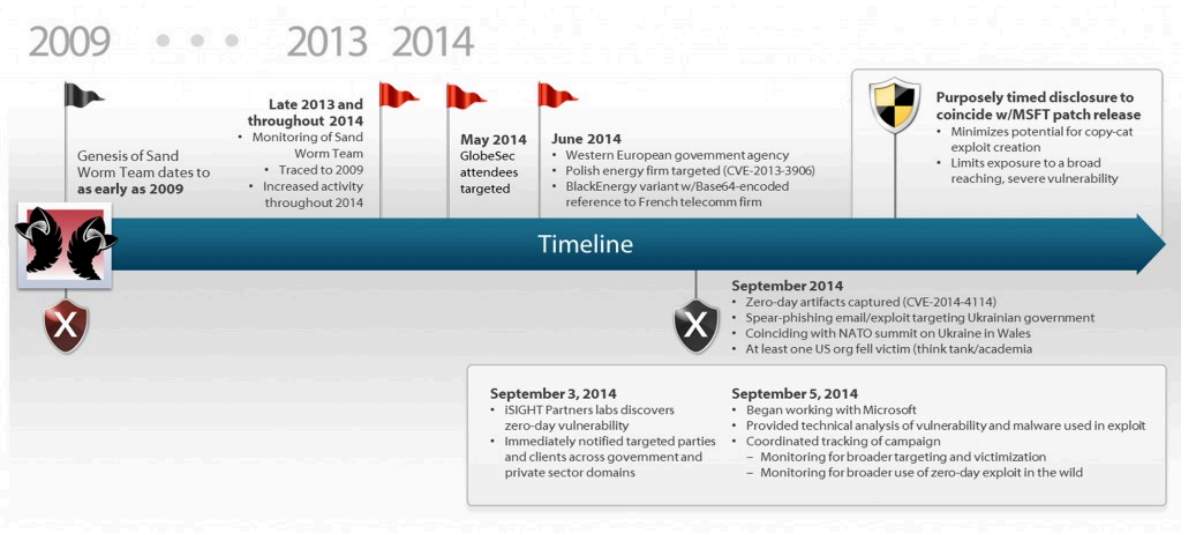
- The NATO alliance was targeted as early as December 2013 with exploits other than the zero-day
- GlobSec attendees were targeted in May of 2014 with exploits other than the zero-day
- June 2014
    - Broad targeting against a specific Western European government
    - Targeting of a Polish energy firm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

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.

On September 3rd, our research and labs teams discovered that the spear-phishing attacks relied on the exploitation of a zero-day vulnerability impacting all supported versions of Microsoft Windows (XP is not impacted) and Windows Server 2008 and 2012. A weaponized PowerPoint document was observed in these attacks.

Though we have not observed details on what data was exfiltrated in this campaign, the use of this zero-day vulnerability virtually guarantees that all of those entities targeted fell victim to some degree.

We immediately notified targeted entities, our clients across multiple government and private sector domains and began working with Microsoft to track this campaign and develop a patch to the zero-day vulnerability.



Working with Microsoft, we discovered the following:

- An exposed dangerous method vulnerability exists in the OLE package manager in Microsoft Windows and Server
    - Impacting all versions of the Windows operating system from Vista SP2 to Windows 8.1
    - Impacting Windows Server versions 2008 and 2012
- When exploited, the vulnerability allows an attacker to remotely execute arbitrary code
- The vulnerability exists because Windows allows the OLE packager (packager .dll) to download and execute INF files. In the case of the observed exploit, specifically when handling Microsoft PowerPoint files, the packagers allows a Package OLE object to reference arbitrary external files, such as INF files, from untrusted sources.
- This will cause the referenced files to be downloaded in the case of INF files, to be executed with specific commands

- An attacker can exploit this vulnerability to execute arbitrary code but will need a specifically crafted file and use social engineering methods (observed in this campaign) to convince a user to open it

Coordinated Disclosure

Over the past 5 weeks, iSIGHT Partners worked closely with Microsoft to track and monitor the exploitation of this vulnerability in the wild, share technical information to assist in the analysis of the vulnerability and the development of a patch, and coordinate disclosure to the broader security community.

Although the vulnerability impacts all versions of Microsoft Windows – having the potential to impact an enormous user population – from our tracking it appears that its existence was little known and the exploitation was reserved to the Sandworm team.

Given that affected parties were notified and that we did not witness a major surge / broader propagation of the exploit based upon our visibility into the team's command and control infrastructure, we elected to time the disclosure to the availability of a patch. This timing minimizes the potential for other bad actors to take advantage of the vulnerability.

Should we have witnessed a major change, both Microsoft and iSIGHT Partners were ready to release this information in advance of the patch.

The application of this patch should be done as soon as humanly possible given the potential for further exploitation by this cyber espionage team and others in the threat actor community.

Microsoft is detailing a list of workarounds to the vulnerability as part of its bulletin – these workarounds should help mitigate the risk of exploitation while the patching process unfolds for your firm.

Requests for Technical Indicators

As mentioned at the beginning of this blog, iSIGHT is providing indicators of compromise to all concerned parties through a vetting process to assist organizations in analyzing their potential exposure. To request the technical report click here.

Tags active cyber espionage campaigns blackenergy malware crimeware CVE-2014-4114 cyber crime cyber espionage cyber intel cyber intelligence cyber readiness cyber risk assesment cyber risk reduction cyber threat intelligence cyber threats fusing threat intelligence isight partners russian cyber espionage ukraine sandworm team threat intel threat intelligence zero day windows zero-day discovery zero-day malware zero-day windows malware

---