The Cobalt group is exploiting the CVE-2017-11882 Microsoft Office flaw in targeted attacks

November 26, 2017 By Pierluigi Paganini

A few days after details about the CVE-2017-11882 Microsoft Office flaw were publicly disclosed, the firm Reversing Lab observed Cobalt group using it.

A few days after details about the CVE-2017-11882 Microsoft Office vulnerability were publicly disclosed, security experts from firm Reversing Lab observed criminal gang using it in the wild.

The gang is the notorious Cobalt hacking group that across the years targeted banks and financial institutions worldwide.

The flaw is a memory-corruption issue that affects all versions of Microsoft Office released in the past 17 years, including the latest Microsoft Office 365. The vulnerability could be triggered on all versions of Windows operating system, including the latest Microsoft Windows 10 Creators Update.

The CVE-2017-11882 flaw was discovered by the security researchers at Embedi, it affects the MS Office component EQNEDT32.EXE that is responsible for insertion and editing of equations (OLE objects) in documents.

The component fails to properly handle objects in the memory, a bug that could be exploited by the attacker to execute malicious code in the context of the logged-in user.

The EQNEDT32.EXE component was introduced in Microsoft Office 2000 seventeen years ago and affects Microsoft Office 2007 and later because the component was maintained to maintain the backward compatibility.

According to Reversing Labs, the Cobalt group is now targeting organizations with malicious email using specifically crafted RTF documents that trigger the CVE-2017-11882 flaw.

The availability online of many exploits of the of CVE-2017-11882 will allows threat actors to rapidly use the hacking code in their operations.

Other proof of concept (PoC) exploits are available online:

- https://github.com/embedi/CVE-2017-11882
- https://github.com/Ridter/CVE-2017-11882
- https://github.com/unamer/CVE-2017-11882

The infection chain would go through multiple steps, in the final stage the malware would download and load a malicious DLL file.

"The starting point of our analysis was an RTF seen in the wild:
bc4d2d914f7f0044f085b086ffda0cf2eb01287d0c0653665ceb1ddbc2fd3326

Using MS Equation CVE-2017-11882, it contacted
hxxp://104.254.99[.]77/x.txt
for first-stage payload, executed through MSHTA" reads the analysis published by ReversingLabs.

"When run, it downloads the next stage payload from
hxxp://104.254.99[.]77/out.ps1"

The script drops the embedded final second-stage payload – Cobalt, one 32-bit or second 64-bit DLL, depending on the system architecture:
d8e1403446ac131ac3b62ce10a3ee93e385481968f21658779e084545042840f (32-bit)
fb97a028760cf5cee976f9ba516891cbe784d89c07a6f110a4552fc7dbfce5f4 (64-bit)

The analysis published by the security firm includes IoCs and also Yara rules to detect the threat.

The Cobalt group has already exploited Microsoft bugs in past campaigns, for example the RCE vulnerability tracked as CVE-2017-8759 that was fixed by Microsoft in the September 2017 Patch Tuesday.

The Cobalt group was first spotted in 2016 when it was spotted targeting ATMs and financial institutions across Europe, later it targeted organizations in the Americas and Russia.

To protect their systems, administrators should apply the Windows updates KB2553204, KB3162047, KB4011276, and KB4011262, included in the November 2017 Patch Tuesday.

Pierluigi Paganini

(Security Affairs – Cobalt group, hacking)

Share this...

banking | Cobalt group | CVE-2017-11882 | Cybercrime | Hacking

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
A new Mirai variant is rapidly spreading, around 100,000 IPs running the scans in the past 60 hours

NEXT ARTICLE
Security Affairs newsletter Round 138 – News of the week

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