Campagne di attacco CVE-2017-11882 - Backdoor/Cobalt

Proto: N061117.

Con la presente Yoroi desidera informarLa riguardo al recente rilevamento di **pericolose campagne di attacco** basate su email fraudolente contenenti documenti malevoli in grado di sfruttare la recente vulnerabilità CVE-2017-11882 "*Skeleton in the closet*": criticità legata al componente EQNEDT32.EXE presente all'interno di molteplici versioni della suite Microsoft Office da circa 17 anni. Per ulteriori dettagli a riguardo si rimanda all'*Early Warning N031117*.

Ricercatori di terze parti hanno rilevato tentativi di attacco volti alla compromissione degli host vittima con impianti malware avanzati in grado di instaurare backdoor all'interno del sistema. Il ciclo di infezione prevede le seguenti fasi:

- Sfruttamento di **CVE-2017-11882** all'interno di documento doc oppure RTF malevoli (dropper - stage1)
- Scaricamento automatico di ulteriore file swf/hta offuscato (dropper - stage2)
- Scaricamento e lancio di script Powershell in grado mettere in esecuzione la **backdoor Cobalt**, potenzialmente legata al gruppo "*Cobalt Group*" correntemente attivo in ambito cyber-crime. (payload)

Di seguito si riportano gli indicatori di compromissione legati alla campagna di attacco in oggetto:

- Dropurl:
  - hxxp ://104.254 .99.77/x.txt
  - hxxp ://104.254 .99.77/out.ps1
- C2:
  - 104.144.207 .207 (porta 443)
  - mta14 .veiligheidsprotocol .info
  - hxxps ://104.144.207 .207/submit.php
  - hxxps ://104.144.207 .207/j.ad
  - 93.113.131 .162 (porta 443)
  - updatesupermaster .info
  - updatemaster .info
  - hxxps ://93.113.131 .162/submit.php
  - hxxps ://93.113.131 .162/cx
  - hxxps ://93.113.131 .162/push
  - hxxps ://93.113.131 .162/BrVR
  - hxxps ://updatesupermaster .info/push
  - hxxps ://updatesupermaster .info/cx
  - hxxp ://updatesupermaster .info/a
- User-Agent:
  - Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)
  - Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
  - Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)
- Hash analizzati:
  - bc4d2d914f7f0044f085b086ffda0cf2eb01287d0c0653665ceb1ddbc2fd3326
  - 5f434901d4f186bdc92ee679783bdfad80281423848462e445704d5a10b0dc20
  - 677426cdd9c6945de3a3858f12fae62914e4d914a24f51475b859f2bcb545095
  - fb97a028760cf5cee976f9ba516891cbe784d89c07a6f110a4552fc7dbfce5f4
  - d8e1403446ac131ac3b62ce10a3ee93e385481968f21658779e084545042840f
  - 8b3da94f633f801cafbcb8a84bdc8998445cdaf04c5cef941048a166538a87ad
  - e8bba715014d5fc63223ddc9942100e93788039fe068f5905988e728ec5e3dea

A questo proposito, Yoroi consiglia di applicare le azioni preventive riportate nel precedente *Early Warning N031117* al fine di ridurre il rischio di eventuali compromissioni a seguito dello sfruttamento della vulnerabilità CVE-2017-11882, in dettaglio: aggiornamento delle suite Microsoft Office e/o disabilitazione componente EQNEDT32 vulnerabile.

Yoroi consiglia di mantenere alto il livello di guardia all'interno della vostra organizzazione, monitorare potenziali rischi di sicurezza, mantenere signature e sandbox aggiornate e verificare periodicamente la sicurezza degli apparati di rete. Yoroi consiglia infine di mantenere alto il livello di consapevolezza degli utenti, avvisandoli periodicamente delle minacce in corso e di utilizzare un team di esperti per salvaguardare la sicurezza del perimetro "cyber".
Per avere un indice di minaccia in tempo reale si consiglia di visitare il seguente link: Yoroi Cyber Security Index

Yoroi S.r.l.
Via Giovanni Battista Martini 6,
Roma RM, 00198

info@yoroi.company
+39 051 0301005

P.IVA. 03407741200 - R.E.A. RM 1559639 - Codice Fiscale 03407741200 - Capitale Sociale: Euro 50.000 IV