SECRET

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 43) July 18**

1. **Introduction.** The IT security researchers have discovered an adware **"PBot (PythonBot)"** written in **Python language** targeting **Windows-based** computers. The adware spams an infected computer with **advertisements** and also installs **cryptocurrency miner** and ad extensions in the browser.

2. **Technical Analysis.**

a. **Adware's** are Programs designed to launch advertisements on infected computers and/or to re-direct search engine results to promotional web sites.

b. Malware **developers** are constantly releasing new **versions,** each of which complicates the script of **obfuscation,** important added feature is the presence of a module that **updates scripts** and **downloads** fresh **browser** extensions.

c. The browser **extension** is used to spam banners on the page visited by the victim which redirects them to advertising sites to generate revenue, while the **cryptominer** uses computing power (CPU) of the system to generate crypto currency.

d. **Pbot** might also cause below mentioned damage s described under:-

(1) The loss of important data.

(2) Serious system malfunction because of crypto *mining.*

(3) Continuous pop-up ads and redirects while browsing the Internet.

(4) Making the system vulnerable to other this.

(5) Leading its victims to money loss or eve unity theft.

e. **Information tracking** is also implemented PythonBot, which typically collects users' **search terms, mostly visited** On names, **'computer's IP** address, its **location** and **similar data.**

3. **Distribution Method.**

a. **PBot** is generally **distributed** through **partner sites** whose implement scripts to **redirect** users to sponsored links. Details of the standard **PBot propagation scheme** as under-

(1) The user visits the partner site.

(2) When any point on the page is clicked, a new browser window pops up that opens an intermediate link.

(3) The **intermediate link redirects** the user to the **PBOt ,download** page, which is tasked with downloading and running the adware on the victim computer.

4. **Mitigation Measures.** Following best practices are suggested in this regard:-

a. It is advised to be vigilant while browsing and refrain from visiting unknown sites or clicking links sent by unknown senders.

b. **Anti-malware** solution (e.g. Reimage, Plumbytes Anti-Malware, Malwarebytes) is required to remove **PBot** virus as there is **no manual** method to rernove it.

c. After removal of malware, it is strongly recommended to **refresh computer system** and **browsers.** Malicious content can still be hiding and waiting for its chance recover.

d. Don't open any word document received via **email** or any **unknown resource.**

e. Use **latest** and **updated** version of **Microsoft office.**

f. **Install and UPDATE well reputed antiviruses** such as Kaspersky, Bitdefender, Nod 32, Avast etc.

5. **Recommendations.**

a. It is advised to strictly follow all **mitigation measures** discussed at para 4.

b. Keep all the **software's** and **operating system** (OS) up-to-date.

c. Train employees on **web browser security** and educate with basic **awareness** of **cyber security.**