New Gallmaker APT group eschews malware in cyber espionage campaigns

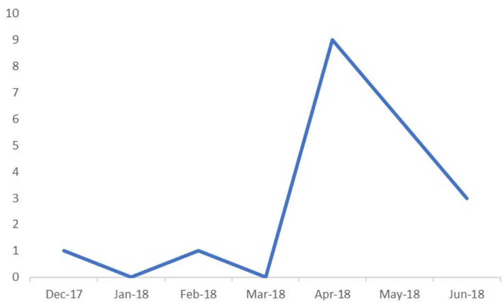
October 11, 2018 By Pierluigi Paganini

A previously unknown cyber espionage group, tracked as Gallmaker, has been targeting entities in the government, military and defense sectors since at least 2017.

A new cyber espionage group tracked as Gallmaker appeared in the threat landscape. According to researchers from Symantec, who first spotted the threat actor, the group has launched attacks on several overseas embassies of an unnamed Eastern European country, and military and defense organizations in the Middle East.

Gallmaker is a politically motivated APT group that focused its surgical operations on the government, military or defense sectors.

Gallmaker been active since at least December 2017, researchers observed a spike in its operations in April and most recent attacks were uncovered in June.



The experts speculate the threat a nation-state actor, it is interesting to note that the APT is relying entirely on code scraped from the public internet.

"This group eschews custom malware and uses living off the land (LotL) tactics and publicly available hack tools to carry out activities that bear all the hallmarks of a cyber espionage campaign," reads the analysis published by Symantec.

"The most interesting aspect of Gallmaker's approach is that the group doesn't use malware in its operations. Rather, the attack activity we observed is carried out exclusively using LotL tactics and publicly available hack tools."

Gallmaker uses spear phishing messages using a weaponized Office document that uses the Dynamic Update Exchange (DDE) protocol to execute commands in the memory of the targeted device.

"These lure documents use titles with government, military, and diplomatic themes, and the file names are written in English or Cyrillic languages. These documents are not very sophisticated, but evidence of infections shows that they're effective." continues Symantec.

"By running solely in memory, the attackers avoid leaving artifacts on disk, which makes their activities difficult to detect."

Once the attackers gain access to a target machine, they use various tools including the reverse_tcp reverse shell from Metasploit, the WindowsRoamingToolsTask PowerShell scheduler, the WinZip console, and an open source library named Rex PowerShell, which helps create PowerShell scripts for Metasploit exploits.

Experts discovered that Gallmaker APT is using three primary IP addresses for its C&C infrastructure, they also noticed the attackers use to delete some of its tools from compromised machines once it is completed the attack, likely to hide traces of their activity.

"The fact that Gallmaker appears to rely exclusively on LotL tactics and publicly available hack tools makes its activities extremely hard to detect. We have written extensively about the increasing use of LotL tools and publicly available hack tools by cyber criminals." concluded Symantec. "One of the primary reasons for the increased popularity of these kinds of tools is to avoid detection; attackers are hoping to "hide in plain sight", with their malicious activity hidden in a sea of legitimate processes."

Pierluigi Paganini

(Security Affairs – Gallmaker, cyber espionage)

Share this...

APT | cyber espionage | Gallmaker | Hacking | Pierluigi Paganini | Security Affairs

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
SAP October 2018 set of patches fixes first Hot News security note for SAP BusinessObjects in 5 years

NEXT ARTICLE
Juniper Networks provides dozens of fix for vulnerabilities in Junos OS

YOU MIGHT ALSO LIKE

Russia-linked APT28 has been scanning vulnerable email servers in the last year
March 20, 2020 By Pierluigi Paganini

Pwn2Own 2020 – Participants hacked Adobe Reader, Oracle VirtualBox, and Windows
March 20, 2020 By Pierluigi Paganini