

# APT39 Hacking Group Launch Widespread Attack Focused on Personal Information

By GURUBARAN S - January 31, 2019 0



Iranian cyber espionage group APT39 focus on stealing on personal information o perform monitoring, tracking, or surveillance operations against specific individuals.

The group carrying a widespread campaign focused their operations in the Middle East, the U.S. and South Korea. Following are the industries targeted including telecommunications, travel industries, high-tech industry, and government entities.

"We have moderate confidence APT39 operations are conducted in support of Iranian national interests based on regional targeting patterns focused in the Middle East, infrastructure, timing, and similarities to APT34", reads [FireEye report](#).

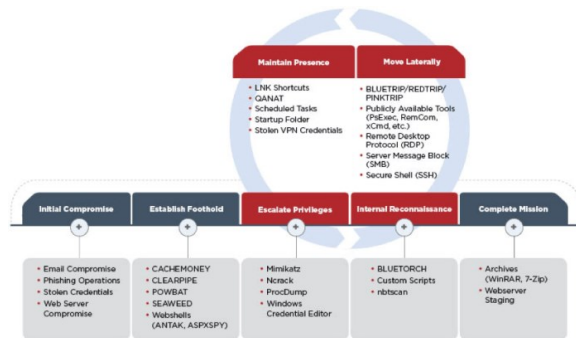
## Focused Attack – APT39

The attack starts with spear phishing emails, stolen credentials, and web server compromise. Phishing emails carry malicious attachments resulting in downloading the POWBAT malware.

For C2 server communications the hacker group register domains that pose as a legitimate one and relevant to organizations.

Also, the group compromise web servers with know vulnerabilities of the targeted organizations and inject web shells such as ANTAK and ASPXSPY. Stolen credentials used to gain access to the email accounts.

APT39 uses custom backdoors such as SEAWEEED, CACHEMONEY variants of POWBAT to gain access to the target organizations and to escalate privileges using freely available tools such as Mimikatz and Ncrack.



Lateral movement carried out through popular tools such as Remote Desktop Protocol (RDP), Secure Shell (SSH), PsExec, RemCom, xCmdSvc and with custom tools REDTRIP, PINKTRIP, and BLUETRIP.

To archive, the stolen data the APT 39 group uses WinRAR or 7-Zip and they use a modified version of Mimikatz to evade anti-virus detection.

Telecommunication and travel industries are the prime targets for the group as they store large amounts of personal and customer information,

"APT39's targeting not only represents a threat to known targeted industries, but it extends to these organizations' clientele, which includes a wide variety of sectors and individuals on a global scale," researchers concluded.

**You can follow us on [LinkedIn](#), [Twitter](#), [Facebook](#) for daily Cybersecurity updates also you can take the [Best Cybersecurity courses online](#) to keep your self-updated.**

Related Read

### Newsletter

Signup to get Hacking News & Tutorials to your Inbox

Name

Email\*

Subscribe

### Penetration Testing as a Service

**TWINTech**  
Penetration Testing as a Service (PTaaS)  
We will test the effectiveness of your own security controls before malicious parties do it for you.  
[Enquire More](#)





### Brexit ebook

**ManageEngine**  
Guide to overcoming **BREXIT'S** Data management challenges.  
[Grab your copy](#)

### Cyber Security Courses

**Learn Cyber Security Courses Online**  
Upto 70% Offer On all Courses  
[Enroll Now](#)

### Computer Security

-  CoronaVirus Cyber Attack Panic - Threat Actors Targets Victims Worldwide  
March 16, 2020
-  Microsoft Released Patches for Wormable Windows SMBv3 RCE Flaw - More...  
March 13, 2020
-  Unpatched Wormable Windows SMBv3 RCE Zero-day Flaw Leaked in Microsoft ...  
March 12, 2020
-  Best and Effective Ways to Keep Your Files Safe From Hackers...  
February 26, 2020

APT Group Actively Exploiting Internet-facing Vulnerable ColdFusion Server and Uploading Webshell

APT Group Uses Datper Malware To Launch Cyber Attack on Asia Countries by Executing Shell Commands

APT28 Hacking Group's New Espionage Operations Targets Military and Government Organizations

Share and Support Us :



TAGS APT39 computer security Cyber Attack hacker group Malware



GURUBARAN S

<http://gbhackers.com>

Gurubaran is a PKI Security Engineer. Certified Ethical Hacker, Penetration Tester, Security blogger, Co-Founder & Author of GBHackers On Security.



RELATED ARTICLES

MORE FROM AUTHOR



Computer Security  
CoronaVirus Cyber Attack Panic – Threat Actors Targets Victims Worldwide



Cyber Attack  
Chinese APT Hackers Exploit MS Word Bug to Drop Malware Via Weaponized Coronavirus Lure Documents



Android  
Cookie Thief – Android Malware that Gains Root Access to Steal Browser & Facebook App Cookies



Leave a Reply

Enter your comment here



#### ABOUT US

GBHackers on security is a Cyber Security platform that covers daily Cyber Security News, Hacking News, Technology updates and Kali Linux tutorials. Our mission is to keep the community up to date with happenings in the Cyber World.

Contact us: [admin@gbhackers.com](mailto:admin@gbhackers.com)

#### FOLLOW US



What is DNS Attack and How Does it Works?  
February 26, 2020

Load more

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it.

OK

Learn More