BITTER APT Targets Chinese Government Agency

⋮ 3/28/2024

March 28, 2024 | **NSFOCUS**

On February 1, 2024, the APT Group BITTER launched a spear-phishing attack on a Chinese government agency.

BITTER, also known as APT-C-08 or T-APT-17, has been actively targeting countries such as China and Pakistan, focusing on industries like government, power, and military to steal sensitive information, driven by strong political motives.

In this incident, the BITTER threat actor sent spear-phishing emails to specific key personnel. Once the email was opened, a scheduled task was created on the victim's computer, activating every 18 minutes. This allowed the Trojan file to control the target host completely and carry out data theft.

Incident Discovery, Analysis, and Identification

The agency detected abnormal external connections in its internal network system and suspected that a computer was remotely controlled. The agency contacted NSFOCUS for emergency investigation and analysis.

The NSFOCUS emergency response team, through internet behavior management and firewall records, found access records to a malicious domain "northgenstudios.com" during the critical time period. However, no other malicious activities related to this domain were discovered.

The query result from NSFOCUS Threat Intelligence shows that the malicious domain was traced to the IP address 195.230.22.7. This is a cluster platform mapping over a thousand domains. Expanding the search timeframe revealed an abnormal outbound connection from a host IP address 10.11.x.x within the client's office intranet, along with six instances of external connections to the malicious domain. Upon careful inspection, multiple msi xxx.tmp files were found in the anti-virus engine's logs of the host, and two malicious samples that were successfully identified unveiled the entire attack chain:

The threat actor used the CHM format as an attachment to entice employees in core key positions to open it and create scheduled tasks. Subsequently, the task accessed the malicious domain "northgenstudios.com" and downloaded msixxx.tmp files. These tmp. files were implanted with the Havoc Trojan and then connected to dtzappaccount.com, corresponding to the IP address 45.66.248.66.

Correlation analysis with historical samples indicated that this APT attack was carried out by the APT Group BITTER.

Attack Event Reconstruction

Based on log and sample analysis, the emergency response team reconstructed the entire attack and response process:

1. **Targeted Email Delivery:** On January 23, 2024, a core employee of the government agency received a phishing email disguised as being from a higher-level government department.
2. **Trojan Implantation:** The victim opened the attachment, making the Trojan be implanted successfully and first automatically accessed the remote C2 server, then implanted a new Trojan.
3. **Data Theft:** The victim's host accessed the remote control server for data transmission, causing an abnormally large increase in traffic volume, which went unnoticed by the client unfortunately.
4. **Clue Discovery:** The NSFOCUS emergency response team received a call for help and conducted an urgent inspection. Leveraging NSFOCUS threat intelligence, abnormal external connections were detected.
5. **Attack Source Tracking:** Through forensic analysis on the host side, extraction of Trojan files, and sample behavior analysis, the NSFOCUS emergency response team identified that APT Group BITTER carried out the attack. Immediate action was taken to remove the Trojan and reinforce the system.