Iranian intel cyber suite of malware uses open source tools

cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

January 12, 2022

FORT MEADE, Md. –
To better enable defense against malicious cyber actors, U.S. Cyber Command's Cyber National Mission Force has identified and disclosed multiple open-source tools that Iranian intelligence actors are using in networks around the world.

These actors, known as MuddyWater in industry, are part of groups conducting Iranian intelligence activities, and have been seen using a variety of techniques to maintain access to victim networks.

MuddyWater is an Iranian threat group; previously, industry has reported that MuddyWater has primarily targeted Middle Eastern nations, and has also targeted European and North American nations.

MuddyWater is a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS). According to the Congressional Research Service, the MOIS "conducts domestic surveillance to identify regime opponents. It also surveils anti-regime activists abroad

through its network of agents placed in Iran’s embassies."

Should a network operator identify multiple of the tools on the same network, it may indicate the presence of Iranian malicious cyber actors.

Below are some technical aspects of how the threat actor could be leveraging malware in networks.

These include side-loading DLLs in order to trick legitimate programs into running malware and obfuscating PowerShell scripts to hide command and control functions. New samples showing the different parts of this suite of tools are posted to Virus Total, along with JavaScript files used to establish connections back to malicious infrastructure.

www.Virustotal.com/en/user/CYBERCOM_Malware_Alert

- **Previous PowGoop Sample**:
    - These three samples are all part of the same PowGoop instance. They were identified in a folder with several other legitimate executables and DLLs. Goopdate.dll uses DLL side-loading to run when a the non-malicious executable GoogleUpdate.exe is run. goopdate.dll will then de-obfuscate goopdate.dat, which is a PowerShell script used to de-obfuscate and run config.txt. Config.txt is a PowerShell script that establishes network communication with the PowGoop C2 server. It uses a modified base64 encoding mechanism to send data to and from the C2 server. The IP of the C2 server is often hardcoded in config.txt
    - Goopdate.dll hides comms with malicious cyber actors’ C2 servers by executing with Google Update service.
- **Additional PowGoop DLL Side-Loading variants:**
    - Uses same technique to de-obfuscate .dat file, which is a PowerShell script to decode another PowerShell script with .txt file extension
    - **This** open source code has been used for espionage & ransomware-- libpcre2-8-0.dll & vcruntime140.dll (PowGoop variant) leverage different naming conventions to avoid antivirus & manual detection.
- **Additional PowGoop Loader variants:**
    - Any instances of these files may indicate an attacker in the network: Open-source cyber research found PowGoop Loader variants in compromised networks, de-obfuscating a PowerShell script that allows an attacker command and control functions.
    - De-obfuscates .txt file, which is another PowerShell script and main C2 functionality

- **Additional PowGoop C2 Beacon variants:**
  - These malware reach out from victim networks & contact malicious infrastructure. If you see these files, MCAs are likely seeing their beacon too.
  - Each sample reaches out from the victim network and contacts malicious infrastructure. If you see these files on the network, chances are they are seeing their beacon as well.
- **JavaScript samples:**

  The samples issue a GET request to malicious servers. The JavaScripts are associated with groups also employing PowGoop.
- **Mori Backdoor sample:**
  - This sample is an indicator that a network has been compromised – this is the Mori Backdoor and is employed by malicious cyber actors for espionage. This malware uses DNS tunneling to communicate to its C2 infrastructure.
  - This sample is a likely Mori Backdoor. This sample utilizes regsvr32.dll to run. Key IOCs are the creation of the Mutex 0x50504060 and creation of the registry key HKLM\SOFTWARE\NFC