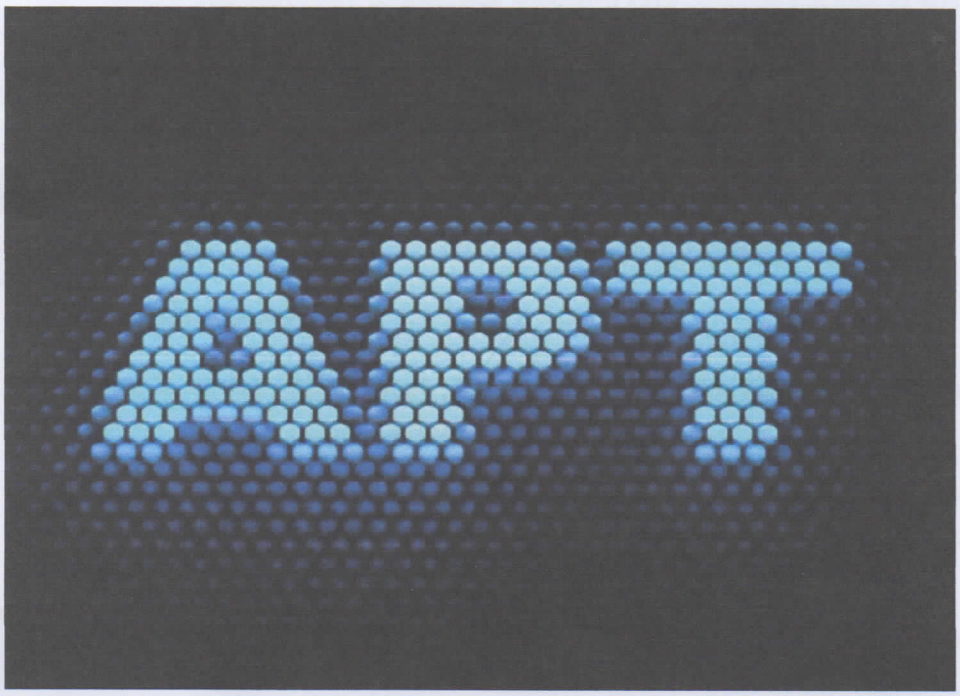
Government Entities sighted as Targets by Sophisticated USB Info-Stealer



Once installed, it scans various paths on the infected device, collecting documents that possess certain extensions," according to the analysis. "These documents are then transferred to USB drives connected to the system. This suggests the malware was designed to reach air-gapped machines, or those that are not directly connected to the internet or any other computer connected to internet.

Modus Operandi

There is a new USB Culprit malware being added as part of the arsenal of an APT known as Cycldek, which targets government entities aimed at reaching air-gapped devices.

Governments in Southeast Asia have been the most common target for Cycldek (a.k.a. Goblin Panda, APT 27 and Conimes). It has been around targeting governments in, based on an analysis by Kaspersky and since its beginning, it still hasn't slowed down but instead it has been steadily adding more sophisticated tools over time.

Added reports indicate that USBCulprit has been deployed against targets in Vietnam, Thailand and Laos

- "It possesses both lateral movement (ability to move through the network to obtain the targeted data) and data-stealing capabilities
- other features suggest that it was built to reach physically isolated machines, where the only way to transfer inbound and outbound data is with removable media such as a USB drive.
- Once installed, it scans various paths on the infected device, collecting documents that possess certain extensions
- These documents are then transferred to USB drives connected to the system. This suggests the malware was designed to reach air-gapped machines, or those that are not directly connected to the internet or any other computer connected to internet.

Malware Behavior

Upon analyzing the code, it was discovered that first build for the binary dates back to 2014, with the latest sample timestamped last year.

attacks would usually start with phishing emails that contain politically themed, boobytrapped RTF documents that exploit known vulnerabilities. Once compromised, the victims are infected with a payload malware called NewCore RAT.

"This malware consists of two variants with advanced data stealing capabilities:

- BlueCore appears to have been deployed against diplomatic and government targets in Vietnam, while
- RedCore was first deployed in Vietnam before being found in Laos."

Both of these "Cores" in turn download USBCulprit (together with other tools, such as a custom backdoor, a tool for stealing cookies and a tool that steals passwords from Chromium based browser databases). The malware is implanted as a side-loaded DLL of legitimate, signed applications.

Such applications included AV components like wsc_proxy.exe (Avast remediation service), qcconsol.exe and mcvsshld.exe (McAfee components), as well as legitimate Microsoft and Google utilities like the resource compiler (rc.exe) and Google Updates (googleupdate.exe). These tools could be used in order to bypass weak security mechanisms like application whitelisting, grant the malware additional permissions during execution or complicate incident response."

References:

https://threatpost.com/info-stealer-air-gapped-devices sb/156262/
https://securityaffairs.co/wordpress/100661/cyber-crime/fin7-usb-teddy-bears-attacks.htmlhttps://securelist.com/usb-threats-from-malware-to-miners/87989/https://www.cynet.com/cyber-attacks/advanced-persistent-threat-apt-attacks/