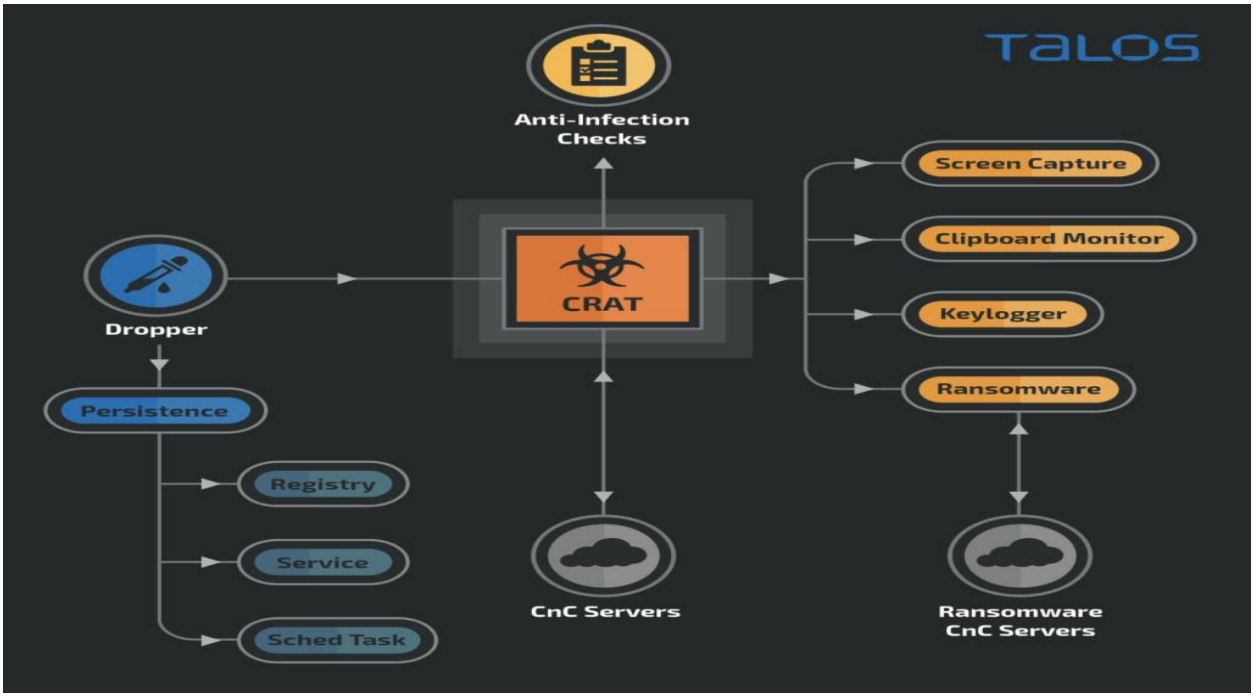
New CRAT Version Is Storming the Endpoints While Evading Detection



- **A new version of the CRAT malware is out, and it comes with additional plugins and obfuscation.**
- **It appears that Lazarus is still the hacker group that is pulling the strings behind CRAT.**
- **The ransomware used by CRAT is following an atypical process of locking files in archives.**

A new version of the CRAT malware is circulating, hitting vulnerable endpoints, fetching and deploying additional plugins, and managing to do all that without being detected. CRAT is a malware family that has been previously linked with the Lazarus APT group (North Korea), a highly skillful and knowledgeable group of hackers who are using custom and powerful tools.

The new version of the CRAT was captured and analyzed by researchers of Cisco Talos, and they report seeing new plugins, as well as a new set of detection-evasion techniques. Their latest investigation also reveals indicators, tactics, and procedures that were previously seen in Lazarus campaigns, so this could mean that CRAT is still used exclusively by the North Koreans.

The researchers couldn't discern the distribution vector of the new campaign, but it could be a document carrying malicious macros again. The additional plugins fetched directly from the C2 servers include ransomware, screen-capture tools, clipboard monitoring components, and even keyloggers. That makes CRAT very powerful and versatile, so the only thing that remains is to make it stealthy.

According to Talos, this is exactly the case with the new CRAT, as it comes with multiple levels of obfuscation, extensive evasion techniques, sophisticated masquerading, and anti-infection checks. For example, the API resolution is done dynamically to hinder analysis by hiding API call sequences. Also, there's an "on-the-fly" patching system that takes place during runtime, masking subroutines/functions so that scanners don't detect malicious code and strings.

The attack from the endpoints is taking place in a sophisticated manner, too, with the implant checking a set of criteria beforehand to see if the process is being debugged or not. If the infected endpoint is suspicious, the execution is aborted.

Among the various problems that CRAT can bring on a target system, ransomware encryption is maybe the worst possible scenario. For this aspect, CRAT fetches a module of the "Hansom" ransomware, locking the files inside archives protected by randomly generated passwords. These passwords are then encrypted using an embedded public key, not the files themselves.

To defend against the new CRAT, a combination of precautionary measures is required. Talos suggests static and network-based detection coupled with system behavior analysis and the deployment of an advanced endpoint protection solution. It is evident that skillful actors go for well-hiding modular tools that combine everything into a single piece, so timely detection is becoming key.

References:

- https://www.technadu.com/new-crat-version-storming-endpoints-evading-detection/224621/
- https://blog.talosintelligence.com/2020/11/crat-and-plugins.html