Beware! Undetectable CrossRAT malware targets Windows, MacOS, and Linux systems

By The Hacker News

Published: 2018-01-25 · Archived: 2026-04-05 18:50:22 UTC

Are you using Linux or Mac OS? If you think your system is not prone to viruses, then you should read this.

Wide-range of cybercriminals are now using a new piece of 'undetectable' spying malware that targets Windows, macOS, Solaris and Linux systems.

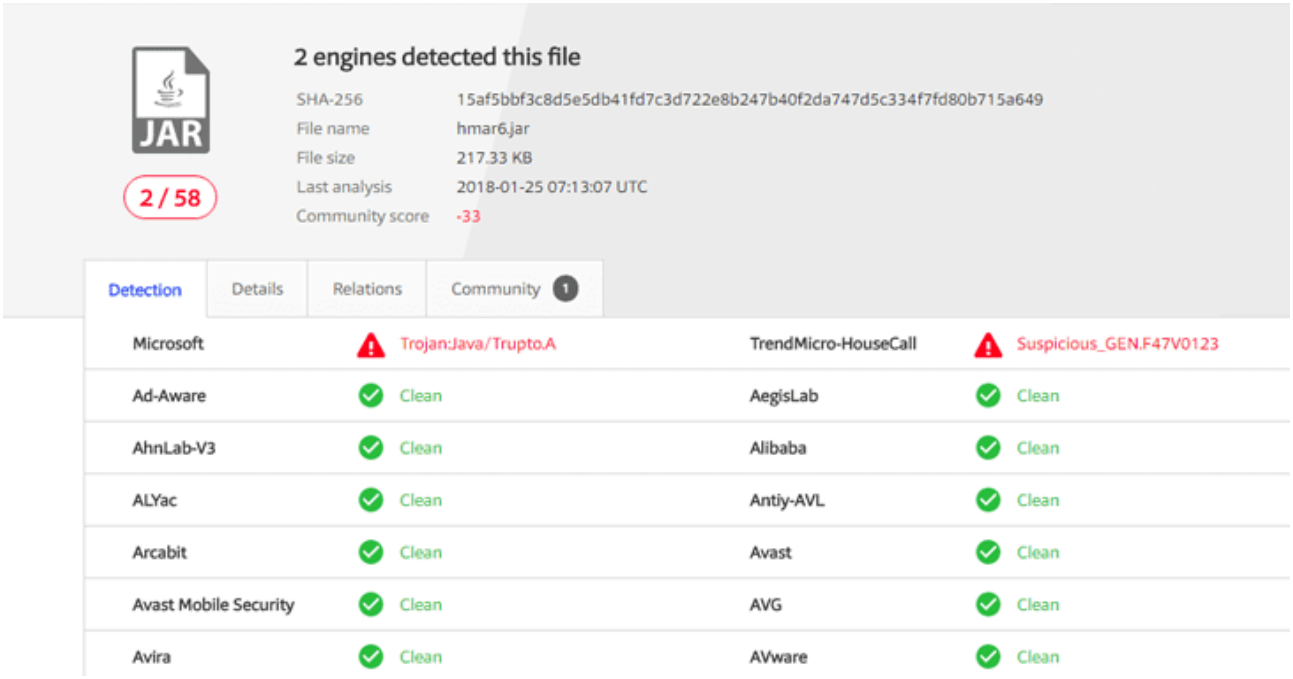
Just last week we published a detailed article on the report from EFF/Lookout that revealed a new advanced persistent threat (APT) group, called Dark Caracal, engaged in global mobile espionage campaigns.

Although the report revealed about the group's successful large-scale hacking operations against mobile phones rather than computers, it also shed light on a new piece of cross-platform malware called **CrossRAT** (version 0.1), which is believed to be developed by, or for, the Dark Caracal group.

CrossRAT is a cross-platform remote access Trojan that can target all four popular desktop operating systems, Windows, Solaris, Linux, and macOS, enabling remote attackers to manipulate the file system, take screenshots, run arbitrary executables, and gain persistence on the infected systems.

According to researchers, Dark Caracal hackers do not rely on any "zero-day exploits" to distribute its malware; instead, it uses basic social engineering via posts on Facebook groups and WhatsApp messages, encouraging users to visit hackers-controlled fake websites and download malicious applications.

CrossRAT is written in Java programming language, making it easy for reverse engineers and researchers to decompile it.



Since at the time of writing only two out of 58 popular antivirus solutions (according to VirusTotal) can detect CrossRAT, ex-NSA hacker **Patrick Wardle** decided to analyse the malware and provide a comprehensive technical overview including its persistence mechanism, command and control communication as well as its capabilities.

CrossRAT 0.1 — Cross-Platform Persistent Surveillance Malware

Once executed on the targeted system, the implant (*hmar6.jar*) first checks the operating system it's running on and then installs itself accordingly.

Besides this, the CrossRAT implant also attempts to gather information about the infected system, including the installed OS version, kernel build and architecture.

Moreover, for Linux systems, the malware also attempts to query systemd files to determine its distribution, like Arch Linux, Centos, Debian, Kali Linux, Fedora, and Linux Mint, among many more.

CrossRAT then implements OS specific persistence mechanisms to automatically (re)executes whenever the infected system is rebooted and register itself to the C&C server, allowing remote attackers to send command and exfiltrate data.

As reported by Lookout researchers, CrossRAT variant distributed by Dark Caracal hacking group connects to '*flexberry(dot)com*' on port 2223, whose information is hardcoded in the 'crossrat/k.class' file.

CrossRAT Includes Inactive Keylogger Module

```
// Server command prefixes
public static String m = "@0000"; // Enumerate root directories on the system. 0 args
public static String n = "@0001"; // Enumerate files on the system. 1 arg
public static String o = "@0002"; // Create blank file on system. 1 arg
public static String p = "@0003"; // Copy File. 2 args
public static String q = "@0004"; // Move file. 2 args
public static String r = "@0005"; // Write file contents. 4 args
public static String s = "@0006"; // Read file contents. 4 args
public static String t = "@0007"; // Heartbeat request. 0 args
public static String u = "@0008"; // Get screenshot. 0 args
public static String v = "@0009"; // Run a DLL 1 arg
```

The malware has been designed with some basic surveillance capabilities, which get triggered only when received respective predefined commands from the C&C server.

Interestingly, Patrick noticed that the CrossRAT has also been programmed to use 'jnativehook,' an open-source Java library to listen to keyboard and mouse events, but the malware does not have any predefined command to activate this keylogger.

> "However, I didn't see any code within that implant that referenced the jnativehook package—so at this point it appears that this functionality is not leveraged? There may be a good explanation for this. As noted in the report, the malware identifies it's version as 0.1, perhaps indicating it's still a work in progress and thus not feature complete," Patrick said.

How to Check If You're Infected with CrossRAT?

Since CrossRAT persists in an OS-specific manner, detecting the malware will depend on what operating system you are running.

For Windows:

- Check the 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run\' registry key.
- If infected it will contain a command that includes, java, -jar and mediamgrs.jar.

For macOS:

- Check for jar file, mediamgrs.jar, in ~/Library.
- Also look for launch agent in /Library/LaunchAgents or ~/Library/LaunchAgents named mediamgrs.plist.

For Linux:

- Check for jar file, mediamgrs.jar, in /usr/var.
- Also look for an 'autostart' file in the ~/.config/autostart likely named mediamgrs.desktop.

How to Protect Against CrossRAT Trojan?

Only 2 out of 58 antivirus products detect CrossRAT at the time of writing, which means that your AV would hardly protect you from this threat.

> "As CrossRAT is written in Java, it requires Java to be installed. Luckily recent versions of macOS do not ship with Java," Patrick said.

> "Thus, most macOS users should be safe! Of course, if a Mac user already has Java installed, or the attacker is able to coerce a naive user to install Java first, CrossRAT will run just dandy, even on the latest version of macOS (High Sierra)."

Users are advised to install behaviour-based threat detection software. Mac users can use BlockBlock, a simple utility developed by Patrick that alerts users whenever anything is persistently installed.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2018/01/crossrat-malware.html