**What is a RAT?**

Remote Access Trojans are programs that provide the capability to allow covert surveillance or the ability to gain unauthorized access to a victim PC. Remote Access Trojans often mimic similar behaviours of keylogger applications by allowing the automated collection of keystrokes, usernames, passwords, screenshots, browser history, emails, chat lots, etc. Remote Access Trojans differ from keyloggers in that they provide the capability for an attacker to gain unauthorized remote access to the victim machine via specially configured communication protocols which are set up upon initial infection of the victim computer.  This backdoor into the victim machine can allow an attacker unfettered access, including the ability to monitor user behaviour, change computer settings, browse and copy files, utilize the bandwidth (Internet connection) for possible criminal activity, access connected systems, and more.

RAT remain as one of the most prevalent forms of malware and are leveraged in many different types of cyber-attacks. Various flavors and versions of these RATs are freely available and easily modified to fit the unique requirements of any given attack. The primary purpose of using RATs is to gain unauthorized remote access to the victim’s device after the initial infection of the machine. Once an attacker gains access to the machine using these RATs, they can try to collect keystrokes, usernames, passwords, browser history, emails, screenshots, etc. A few examples from a much larger list of popular RATs include Poison-Ivy, JRAT, NjRAT, Orcust-RAT, CyberGate, DarkComet, DreamWare, BlackShades, NetWire.

**What is NanoCore RAT?**

NanoCore is a high-risk RAT that provides attackers with details on the device name and OS. This information is used to carry out various malicious activities, such as manipulating confidential files, hijacking webcam and microphone, stealing login credentials and more.

NanoCore comes with base plugins that expand the performance capability of the malware, inciting specific malicious attacks. Since its discovery in 2013, NanoCore has gone through multiple versions over the years.

NanoCore RAT comes with a few base plugins and the ability to expand its functionality, so threat actors can develop additional features for other malicious actions. There is already a wide range of NanoCore plugins available online that can be used for cryptocurrency mining, ransomware attacks, and more.

**Distribution Methods**

The most common initial delivery method today is via attachments in spam emails and web download links. Previously security researchers found MS Word documents with malicious auto-executable VBA code and a fake invoice in PDF format that can install the NanoCore *RAT*.

The first delivery method we identified is using the actual compiler, Autoit3.exe (version 3.3.8.1) which was used by renaming the legitimate **AutoIT Script** interpreter to cxf.exe to bypass basic script control based solutions. Additionally, the malicious code was executed as a script instead of as an actual AutoIT executable to further evade detection from AV. The malicious script demonstrates advanced support for process hollowing for both 32 and 64-bit architectures, VM evasion, and the use of advanced shellcodes such as RunPE. Here we will investigate the functionality of the script and how it delivers and executes the NanoCore RAT. A similar type of attack was previously reported by [TALOS](https://blogs.cisco.com/security/talos/sysadmin-phish) and [HornetSecurity](https://www.hornetsecurity.com/en/security-information/creative-distribution-of-an-old-acquaintance), but with a different primary source of the attack and a different file type for the config file.

Yara Rule:

