AutoIt-Compiled Worm Sends Fileless BLADABINDI/njRAT

By Carl Maverick Pascual, Michael Jhon Ofiaza, Patrick Angelo Roderno (words)

Published: 2018-11-27 · Archived: 2026-04-06 01:37:02 UTC

BLADABINDI, also known as njRAT/Njw0rm, is a remote access tool (RAT) with a myriad of backdoor capabilities — from keylogging to carrying out distributed denial of service (DDoS) — and has been rehashed and reusedopen on a new tab in various cyberespionage campaigns since it first emerged. Indeed, BLADABINDI's customizabilityopen on a new tab and seeming availabilitynews- cybercrime-and-digital-threats in the underground make it a prevalentopen on a new tab threat. Case in point: Last week, we came across a worm (detected by Trend Micro as Worm.Win32.BLADABINDI.AA) that propagates through removable drives and installs a fileless version of the BLADABINDI backdoor.

While it is still unknown how the malicious file actually arrives in the infected system, its propagation routine suggests that it enters systems through removable drives. Apart from being a flexible and easy-to-use scripting language, BLADABINDI's use of AutoIt is notable. It uses AutoIt (the *FileInstall* command) to compile the payload and the main script into a single executable, which can make the payload — the backdoor — difficult to detect.

Figure 1: Screenshot showing a common indicator of a compiled AutoIt script (highlighted)

Technical analysis

We used an AutoIt script decompiler to break down the executable's AutoIt script and found that the script's main function first deletes any file named *Tr.exe* from the system's %TEMP% directory so it can install its own version of *Tr.exe* on it. The dropped file is executed after terminating any process with the same name. It will also drop a copy of itself in the same directory. For persistence, it adds a shortcut for the file at the *%STARTUP%* directory.

For propagation, it installs a hidden copy of itself on any removable drive found on the infected system. It will also drop a shortcut file (.LNK) and move all original files of the removable drive from its root to a created folder named *sss*.

Figure 2: Code snapshot showing the decompiled script

Figure 3: Code snapshot showing how the AutoIt's FileInstall command is used to bundle an AutoIt script with any file then load the file during the script's execution

Figure 4: Code snapshots showing how the shortcut is added (top) and how it propagates through removable drives (bottom)

The dropped *Tr.exe* is actually another AutoIt-compiled executable script (Trojan.Win32.BLADABINDI.AA). Decompiling it reveals that it contains a base-64 encoded executable, which it will write in a registry value named *Valuex* in the registry HKEY_CURRENT_USER\Software.

It will also create another value for persistence. It will use an auto-run registry (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run) named *AdobeMX* that will execute PowerShell to load the encoded executable via reflective loading (loading an executable from memory rather than from the system's disks).

Since the executable is loaded directly from the registry to the memory of PowerShell, we were able to dump the specific address where the malicious executable is located. And we found out that it is .NET-compiled, which uses a commercial code protector software for obfuscation.

Figure 5: Screenshots showing PowerShell loading the encoded executable

BLADABINDI/njRAT payload

The variant of the BLADABINDI backdoor uses *water-boom[.]duckdns[.]org* as its command-and-control (C&C) server, on port 1177. As with other and previousopen on a new tab iterations of BLADABINDI, this fileless version's C&C-related URL uses dynamic domain name system (DNS). This could potentially allow the attackers to hide the server's actual IP address or change/update it as necessary.

All files downloaded from C&C server are stored in the %TEMP% folder as *Trojan.exe*. It uses the string 5cd8f17f4086744065eb0992a09e05a2 as its mutex as well as its registry hive in the affected machine. It uses the value *tcpClient_0* as its HTTP server, where it will receive all stolen information from the infected machine. However, since the value was set to null, all stolen information will be sent to the same C&C server.

When the backdoor runs, it creates a firewall policy that adds PowerShell's process to the list of allowed programs in the system. BLADABINDI's backdoor capabilities are shown in Figure 7, which includes keylogging, retrieving and executing files, and stealing credentials from web browsers.

Figure 6: Code snapshots showing the configurations of the BLADABINDI variant (top) and how it creates a firewall policy to add PowerShell to the list of programs allowed to run (bottom)

 Figure 7: The backdoor capabilities of the BLADABINDI variant

Best practices and Trend Micro solutions

The worm's payload, propagation, and technique of filelesslynews article delivering the backdoor in the affected system make it a significant threat. Users and especially businesses that still use removable media in the workplace should practice security hygiene. Restrict and secure the use of removable media or USB functionality, or tools like PowerShell (particularly on systems with sensitive data), and proactively monitor the gateway, endpoints, networks, and servers for anomalous behaviors and indicators such as C&C communication and information theft.

Users and businesses can also use Trend Micro endpoint solutions such as Trend Micro™ Securityproducts, Smart Protection Suitesproducts, and Worry-Free Business Security all include behavior monitoring to detect fileless malware attacks. This helps organizations look out for malicious behavior that can block the malware before the behavior is executed or performed. OfficeScan can also include a device controlopen on a new tab feature that can prevent USB and optical drives from being accessed, preventing an attack similar to the one discussed in this post. Trend Micro™ OfficeScan™ with XGen™ endpoint security infuses high-fidelity machine learning with other detection technologies and global threat intelligence for comprehensive protection against advanced malware.

Indicators of Compromise (IOCs)

Related hashes (SHA-256):

- c46a631f0bc82d8c2d46e9d8634cc50242987fa7749cac097439298d1d0c1d6e — Worm.Win32.BLADABINDI.AA
- 25bc108a683d25a77efcac89b45f0478d9ddd281a9a2fb1f55fc6992a93aa830 — Win32.BLADABINDI.AA

Related malicious URL:

- water[-]boom[.]duckdns[.]org (C&C server)

Source: https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-worm-affecting-removable-media-delivers-fileless-version-of-bladabindi-njrat-backdoor/