Negasteal/Agent Tesla, Ave Maria Delivered via Malspam

By Miguel Carlo Ang, Earle Maui Earnshaw (words)

Published: 2019-10-25 · Archived: 2026-04-05 22:33:10 UTC

We recently saw a malicious spam campaign that has AutoIT-compiled payloads – the trojan spy Negasteal or Agent Tesla (detected by Trend Micro as TrojanSpy.Win32.NEGASTEAL.DOCGC), and remote access trojan (RAT) Ave Maria or Warzone (TrojanSpy.Win32.AVEMARIA.T) – in our honeypots. The upgrading of payloads from a typical trojan spy to a more insidious RAT may indicate that the cybercriminals behind this campaign are moving towards deploying more destructive (and lucrative) payloads, such as ransomware, post-reconnaissance.

This campaign uses AutoIT-obfuscated ISO image filesnews- cybercrime-and-digital-threats as well as RAR- and LZH-compressed archive attachments to evade detection. ISO images, specifically, can be used to bypass spam filters, and the file format is also easier to mount on more recent Windows versions. We observed that this spam campaign was sent using a possibly compromised webmail address.

Technical analysis

The AutoIT-obfuscated malware strains are delivered via malicious spam emails. The malspam emails we saw associated with this campaign included a fake shipment advisory and a financial document.

Figure 1. A fake shipment advisory spam email that has a .RAR attachment containing Negasteal

Figure 2. A fake down payment notification email that has an .LZH attachment containing the Ave Maria RAT

The downloaded malicious attachments will then extract the AutoIT-obfuscated malware strains of Negasteal and Ave Maria.

AutoIT, a scripting language that is originally intended to automate basic tasks in Windows GUI, has been abused by cybercriminals in the past to obfuscate malware binaries. In the case of Negasteal and Ave Maria, the AutoIT obfuscation technique has two layers: The actual malware binaries are obfuscated into AutoIT scripts (.au3), after which the scripts are compiled into an executable using an AutoIT compiler like Aut2Exe.

Because of the malicious attachments' highly obfuscated nature, endpoints without cybersecurity solutions equipped with behavior monitoring powered by machine learning will not be able to proactively detect and defend against these threats.


Figure 3. Infection flow of the Negasteal (top) and Ave Maria (bottom)

Once the malicious attachment is downloaded, it will proceed to extract an AutoIT-obfuscated malware strain to the machine.

The attachments contain an AutoIT-based packer or crypter that executes a script that decrypts and loads version 5 of the Frenchy shellcode. We deobfuscated the "Frenchy_shellcode_005" script by:

- Extracting the .au3 file from the binary.
- Finding the variable in the AutoIt script where the shellcode is assembled.Writing the content of the variable to a file.

Trojan spies are popular malspam payloads. The same is true for this particular campaign, at least initially. The first payload is a Negasteal/Agent Tesla variant. Typical of previously seen Negasteal/Agent Tesla variants, the one used in this campaign is able to log and monitor keystrokes, webcam and screen captures, as well as collect information saved on clipboards. It is also able to collect system information and saved usernames and passwords from browsers and mail clients, among many others.

We observed that later versions of this campaign, which uses the same double-layered AutoIT-obfuscation technique, have upgraded its payload from Negasteal/Agent Tesla to the Ave Maria RAT.

We observed that the Ave Maria RAT variant in this campaign is armed with more functions than the typical trojan spy. It uses UAC bypass and process tokens to elevate its privileges. Once it has done that, it will execute the PowerShell **Add-MpPreference –ExclusionPath** cmdlet, which allows the modification of Windows Defender's settings to exclude specific paths from being scanned in real-time.

The malware is also configured to establish a connection to a command-and-control (C&C) server.

Figure 4. Screen capture of Ave Maria's code establishing a C&C connection after its privileges have been elevated

Regardless of whether privilege escalation occurs or not, if Ave Maria is able to create a registry key in the system or drop a copy of itself in **"%Program Data%"** directory, it will create a *cmd.exe* process and, afterward, inject malicious code into it. If that still fails, it will execute *explorer.exe* for code injection.

Figure 5. Screen capture of Ave Maria's code executing *explorer.exe* for code injection

Once successfully running in a compromised system, Ave Maria can log users' keystrokes as well as steal usernames and passwords from the following protocols and applications:

Protocols:

- HTTP
- IMAP
- POP3
- SMTP

Applications:

- Microsoft Outlook (1997-2010, 2013, and 2016 versions)
- Windows Messaging
- Internet Explorer
- Google Chrome
- Foxmail
- Thunderbird
- Firefox

Ave Maria can also modify, drop, and create arbitrary files in a compromised system, as well as enumerate processes, files, directories, and drives. It is also able to terminate running processes, delete files, and uninstall itself.

Security Recommendations

Here are some of the best practices businesses and users can adopt to protect against Negasteal, Ave Maria, and other highly obfuscated threats:

- ***Secure the email gateway.*** Because Negasteal and Ave Maria are delivered via malicious spam emails, it's important to be aware of social engineering tactics so as not to fall for them. Practicing cybersecurity hygienenews-cybercrime-and-digital-threats, both in the workplace and at home, e.g., identifying red flags in phishing emails, helps just as much as deploying security solutions.
- ***Think before you click.*** Refrain from opening email attachments from unverified sources.
- ***Enforce the principle of least privilege.*** Ave Maria abuses legitimate tools such as PowerShellnews article as part of its attack chain. Disabling, restrictingnews article, or securingnews- cybercrime-and-digital-threats its use can significantly deter the threat from abusing them.
- ***Observe, monitor, and log.*** Keep comprehensive records of what happens within the network to enable IT personnel to track suspicious activities like traffic from malicious URLs.
- ***Proactively monitor the organization's online infrastructure.*** For organizations, a multilayered approach can help defend against highly obfuscated threats. Firewallsnews article and intrusion detection and prevention systems help detect and block suspicious traffic or malicious network activities. Application control and behavior monitoring prevent anomalous executables and malware-related routines from running, while URL filtering helps block malicious URLs and websites that may be hosting malware.

Trend Micro solutions

intelUsers and organizations are protected from highly obfuscated threats such as the AutoIT-compiled Negasteal and Ave Maria malware strains with Trend Micro's multilayered proactive and reactive approaches to cybersecurity.

- At the email level, the Trend Micro™ Anti-Spam Engine (TMASE)™ and Hosted Email Security (HES)™ solutions block spam emails, such as the fake shipment advisory and financial document in this campaign, from reaching users and organizations. Both solutions use machine learning technologies that include statistical analysis, advanced heuristics, whitelists and blacklists, as well as signature filtering.
- Malicious files, scripts, and messages like the Negasteal- and Ave Maria-containing ISO, LZH, and RAR attachments are proactively detected by Trend Micro's behavior monitoring technology, a key component in its endpoint solutions such as the Smart Protection Suites productsand Worry-Free™ Business Security
- Two robust reactive layers of protection from the Smart Protection Suites and the Trend Micro Deep Discovery™products solution detect Negasteal and Ave Maria's remote scripts even if they are not being downloaded on the physical endpoints.
- The Trend Micro Deep Discovery Inspector productsprotects customers by detecting suspicious network traffic and preventing Negasteal and Ave Maria from connecting to C&C servers, which may lead to data exfiltration, via these DDI rules:
  - **Rule 4248: WARZONE – DNS (Response)**
  - **Rule 4249: NEGASTEAL - SMTP (Request)**

Indicators of Compromise (IoCs)

SHA-256 Hash	Trend Micro Predictive Machine Learning Detection	Trend Micro Pattern Detection
Bc077b31c61d61d5d077b68b7f0b110efe85d138	Troj.Win32.TRX.XXPE50FFF032	TrojanSpy.Win32.NEGASTEAL.DOCC
224f6e0c21145534ec2bab670bcb1b690c08a26d	Troj.Win32.TRX.XXPE50FFF032	TrojanSpy.Win32.AVEMARIA.T

Source: https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-negasteal-agent-tesla-ave-maria-delivered-via-malspam/