Bifrost Burned: Dissecting Asgard Protector's Defenses

By James

Published: 2025-10-01 · Archived: 2026-04-05 17:09:03 UTC

SpyCloud Labs analysts have been busy reversing Asgard Protector, one of the crypters recommended by the sellers of LummaC2. At the time of writing this publication, LummaC2 is the most prominent commodity infostealer available.

Crypters are tools used by cybercriminals that allow them to hide malicious payloads in seemingly nonmalicious wrappers or "packed" samples, allowing them to easily bypass antivirus (AV) software and other protections. Asgard Protector leverages Nullsoft package installations, hidden AutoIt binaries, and compiled AutoIt scripts in order to inject encrypted payloads into memory, which are decrypted in memory and executed.

All told, the combination of LummaC2 and Asgard Protector represents a potent union for evading detection and stealing data from devices and networks.

Asgard Protector advertises itself as an AUTOcrypt service, meaning that stubs are generated automatically for malware submitted to its crypting service (a Telegram bot). We have observed advertisements for Asgard Protector on XSS dating back to at least 2023. As we can see from these advertisements, (see **Image 1** below), the Telegram bot also allows for a wide variety of customizable options to be added to the crypt such as:

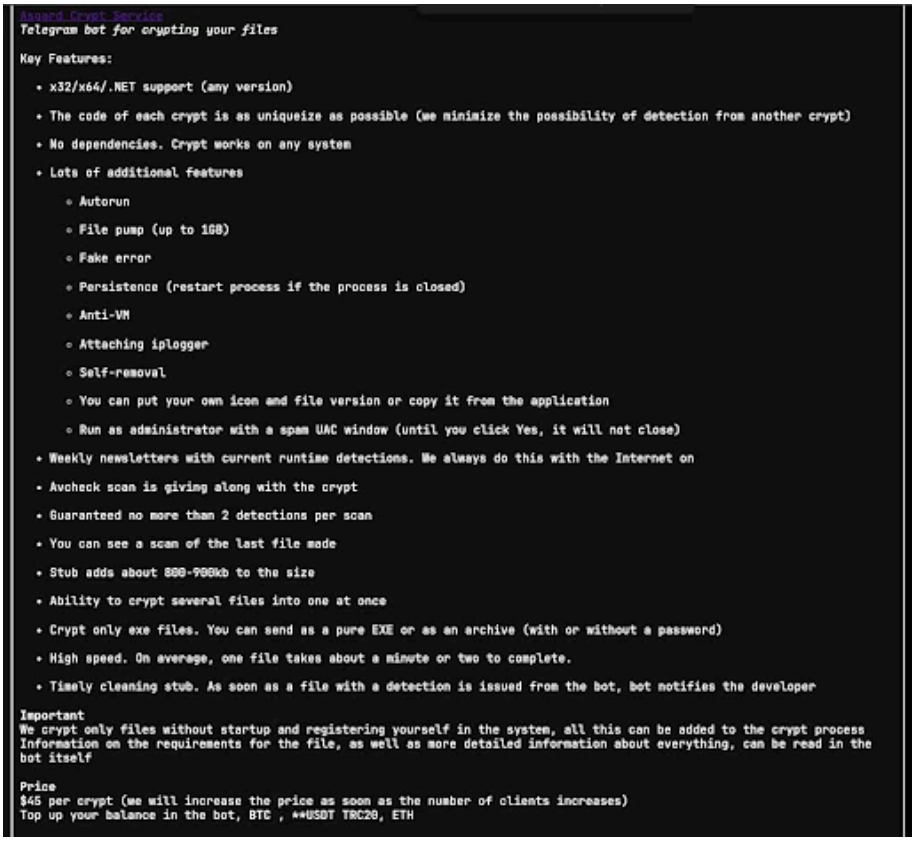

Image 1: Screenshots of the Asgard Protector ad, which appeared on XSS.

Installation

Asgard Protector crypted binaries arrive on systems as Nullsoft Installation Binaries, which are essentially self-extracting RAR files with installation scripts that run once the contents are extracted.

For Asgard Protector, the Nullsoft binary simply extracts all files into %temp%, before locating the .bat file that it uses for its installation routine, and then executing it. As observed in **Image 2**, Asgard Protector leverages mismatched file extensions in order to better hide. The .bat file it looks for is the ASCII text file, or in this sample, Belgium.pst.

Image 2: File listing of an Asgard Protector Nullsoft installation binary.

As observed in **Image 3**, the *.bat* file used by Asgard Protector for installation is fairly obfuscated, making reading and understanding it challenging.

The obfuscated .bat file used by Asgard Protector for installation.

However, analysts at SpyCloud have developed in-house tooling to help deobfuscate these scripts, making them much easier to read and understand. A deobfuscated version of the same script that appears above can be observed in **Image 4** below.

The deobfuscated .bat file used by Asgard Protector.

The batch script has some basic AV checking that it conducts in order to determine if it's a safe environment for the malware to run *(i.e.: a vulnerable endpoint)*. This behavior is present in all samples of Asgard Protector that we have analyzed as of the date of publication.

One interesting technique used by the script is the piecemeal assembly of an autoit.exe binary, using the files contained in the .cab file, as observed in **Image 2**, as well as a hardcoded MZ, which is tacked on by the script. What's unique is that in order to find the PE header, findstr is used to find a file offset in one of the embedded files, and then everything is copied over past that offset. This file can partially be observed in **Image 5**, below.

Image 5: The partial AutoIt binary used by Asgard Protector.

Additionally, the script assembles a compiled AutoIt script file using the remaining .pst files (listed as "data" files in **Image 2**), which is then executed by the assembled AutoIt binary. It should be noted that unique crypts using Asgard Protector result in different file extensions for the malware to masquerade as, however, the runthrough is always the same.

AutoIt script

At this point in the infection process, the compiled AutoIt script file is executed by the rebuilt AutoIt binary. This script file handles the extra customizable behavior of the crypter, such as the autorun functionality or the IP logger. Using tools like autoit-ripper, SpyCloud Labs analysts were able to decompile the AutoIt script file to get the raw script source file, as observed in **Image 6**.

Image 6: The obfuscated AutoIt script used by Asgard Protector for malware install

The decompiled script file is horrendously obfuscated, using both a basic state machine and string hiding in order to mask the true functionality of the script. Luckily, using more in-house developed tooling, we were able to deobfuscate the AutoIt scripts as well, as observed in **Image 7**.

Image 7: The deobfuscated version of Asgard Protector's AutoIt install script

This script handles all of the additional features of Asgard Protector, in addition to the actual injection of the malware binary into memory. Asgard Protector normally injects the malware payload into explorer.exe, which helps the malware to evade detections. The malware sits encrypted in the AutoIt script and is decrypted in memory using RC4. Additionally, the AutoIt script decompresses the malware binary once it is in memory, using RTLDecompressFragment and the LZNT1 compression algorithm.

A particularly interesting feature of Asgard Protector is its sandbox detection process, which uses pings to domains that should not provide a response. This can be observed in **Image 7** with a ping to a randomly generated domain that should return null. If this ping receives a response however, Asgard Protector will immediately exit, as it knows that it is running in an environment that is blocking outbound connection attempts and mimicking network traffic.

Pivoting off of Asgard Protector crypted binaries in Virustotal, SpyCloud Labs analysts discovered over 1,200 samples, which helped to determine the most commonly crypted malware families. We then worked to identify a small subset of the samples found in order to determine usage statistics.

As can be observed in **Chart A**, LummaC2 accounted for over **69%** of the more than 200 samples that we identified as having been crypted using Asgard Protector. Interestingly, Rhadamanthys was the next highest family, coming in at just over **11%**.

Chart A: Asgard Protector usage breakdown

We also observed a fairly low percentage of unidentified malware, with only four of the total identified samples consisting of malware that SpyCloud analysts could not immediately identify as a named family.

Additionally, while identifying malware for this crypter, we noticed that many AV providers automatically identified this crypter as CypherIT, despite it not in fact being CypherIT. Looking at past analyses of CypherIT, we note that CypherIT and Asgard Protector are similar in functionality, potentially suggesting a link between these two crypters.

As mentioned previously in this analysis, Asgard Protector drops all of its files into %temp% before running the dropped .bat file via the Nullsoft installation binary, and then installing the malware. However, that behavior by itself may not be anomalous enough for defenders to properly locate the malware, as many nonmalicious executables write to %temp% often.

Instead, defenders should look at the commands Asgard Protector runs during the .bat file execution, as those are more anomalous and can be used to identify malicious behavior. Some commands to look out for are:

Asgard Protector is a malware crypter recommended by the sellers of LummaC2. In the crypted malware samples we analyzed:

Other interesting findings from our analysis include:
