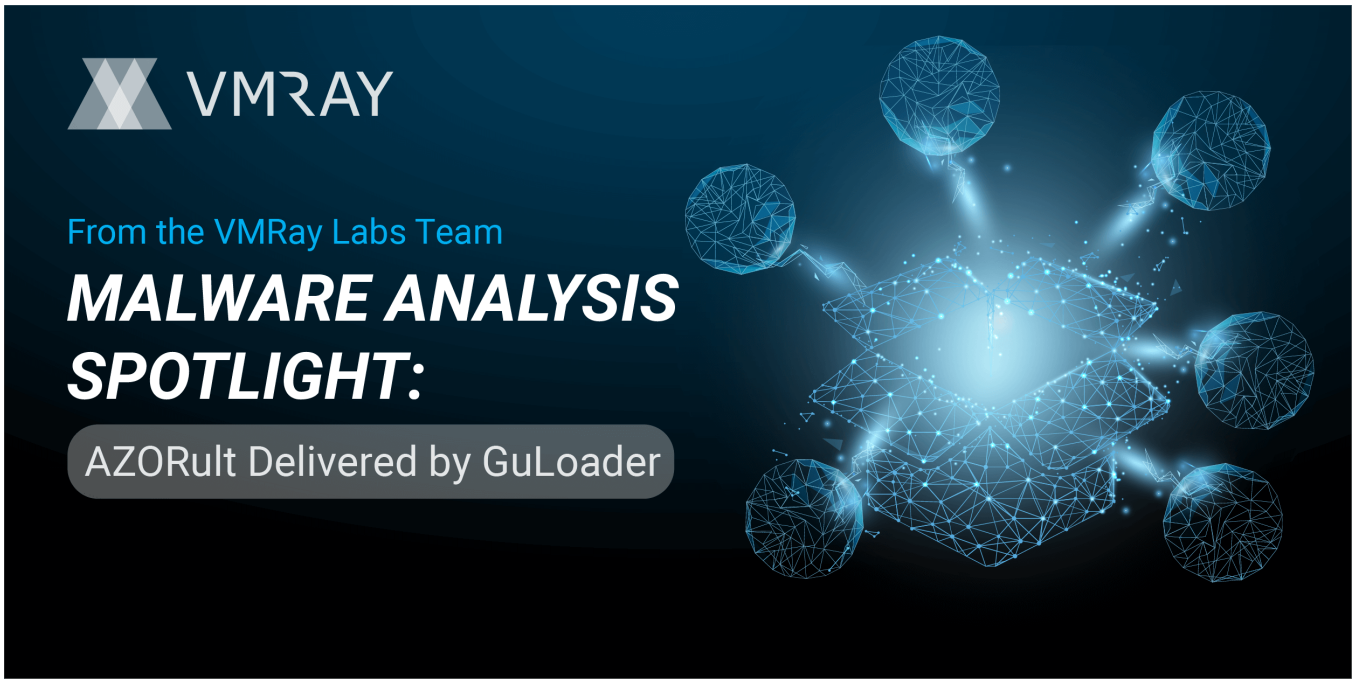
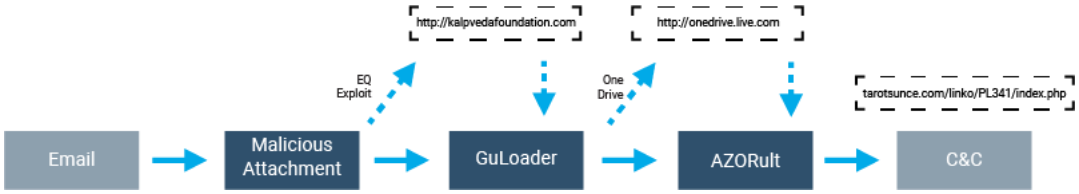
Malware Analysis Spotlight: AZORult Delivered by GuLoader

vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/





Earlier this year, in one of our blog posts we covered GuLoader, a downloader outfitted with advanced anti-analysis techniques that has delivered FormBook, NanoCore, LokiBot, and Remcos among others. Recently, we've observed GuLoader delivering AZORult.

Active for many years, AZORult is an information stealer that has seen many iterations and is typically spread via spam emails or malicious software.

GuLoader's evasive techniques coupled with AZORult's information-stealing capabilities make this an interesting combination for an attacker to hit their target.

In this Malware Analysis Spotlight, we will analyze a delivery chain that uses malicious e-mail attachments and GuLoader to spread AZORult.

Analysis of the AZORult Delivery Chain

Our investigation started from a single sample that matched our AZORult v3 network communication YARA rule. We decided to get more background information and look for the delivery method. The delivery payload turned out to be an RTF document delivered as an email attachment (Figure 1) and exploiting a vulnerability in one of Microsoft's Office products.

Starting from the email, the attack actually contained three steps and downloaded two payloads during its execution. At least one of the payloads was AZORult. We also investigated the other parts of the executions chain and it turned out that the infamous GuLoader was used as one of the links in the execution chain.

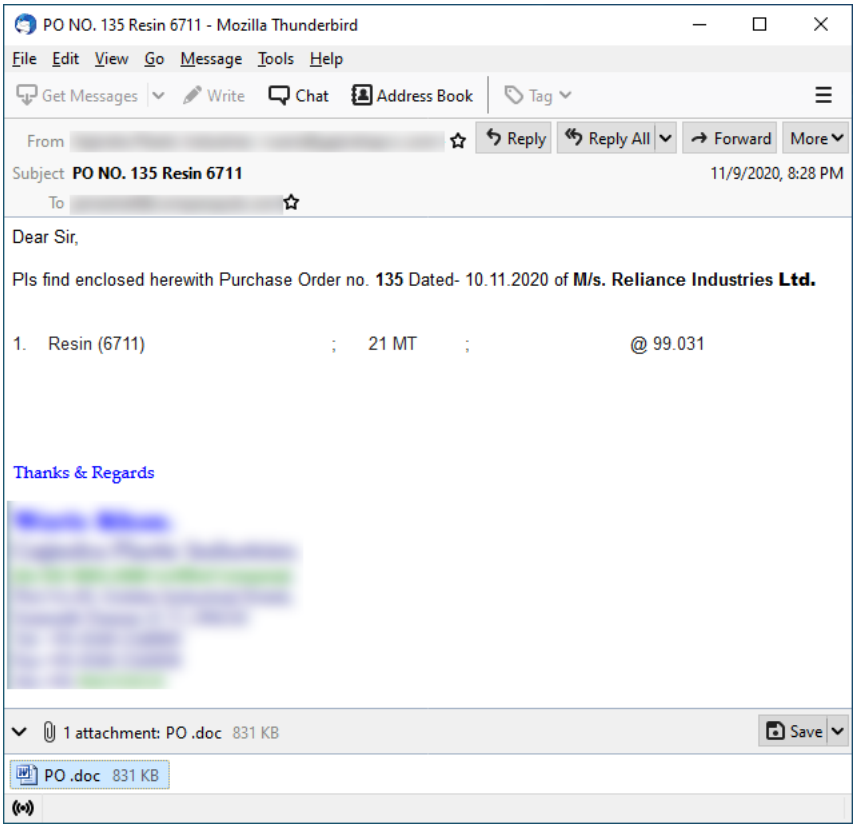


Figure 1: Spam email that delivers the malicious RTF document.

The document is abusing the equation editor (CVE-2017-11882) vulnerability to achieve execution on the victim's machine. This leads to the download and execution of the next payload which is GuLoader (Figure 2).

In our investigation, we found multiple unique domains responsible for hosting the GuLoader payload (see list of IOCs) associated with similar spam emails leveraging this type of execution chain.

Host Behavior

File (1)

Operation	Filename	Additional Information	Success	Count	Logfile
Create	C:\Users\aETAdzjz\AppData\Roaming\fghvhghvgfdgfhchfg.exe	desired_access = GENERIC_WRITE, file_attributes = FILE_ATTRIBUTE_NORMAL	✓	1	FN

Process (1)

Operation	Process	Additional Information	Success	Count	Logfile
Create	C:\Users\aETAdzjz\AppData\Roaming\fghvhghvgfdgfhchfg.exe	cmd_line = C:\Users\aETAdzjz\AppData\Roaming \fghvhghvgfdgfhchfg.exe, show_window = SW_SHOWNORMAL	✓	1	FN

Figure 2: VMRay Analyzer – Download of the next GuLoader payload by exploiting a vulnerability in the equation editor.

As we have described in one of our previous Threat Bulletin, GuLoader is equipped with advanced anti-analysis, sandbox detection, and evasion techniques to increase its chances of delivering malware to its intended target.

In the VMRay Analyzer Report, we observed the typical behavior of GuLoader, using shellcode in two instances (processes). The shellcode uses its advanced techniques to thwart dynamic analysis followed by the final payload downloaded from a publicly available cloud provider.

Compared to the previously analyzed GuLoader samples, this one shows additional behavior in the enumeration of products currently advertised/installed (MsiEnumProductsA) and services (EnumServicesStatusA) (Figure 3). This might be an indicator of further detection or evasion techniques present in this GuLoader sample.

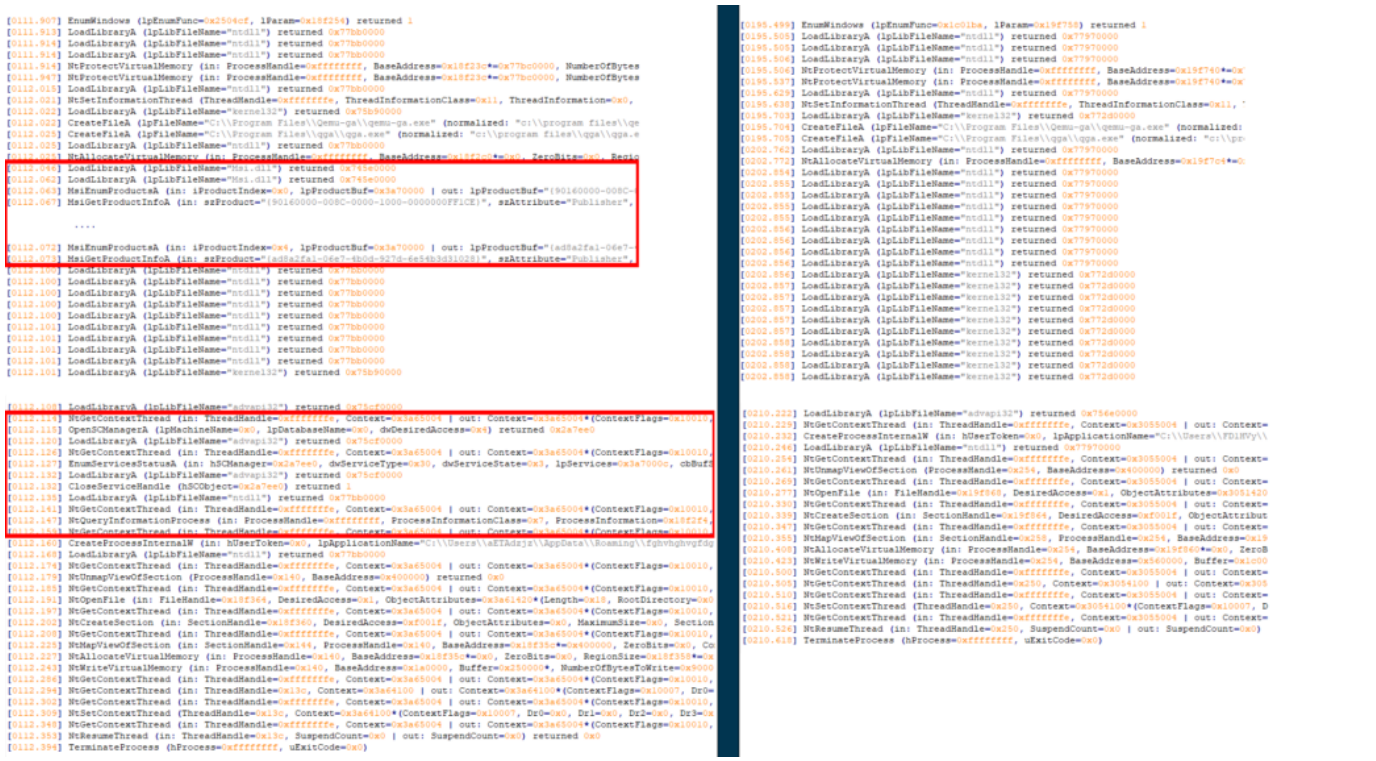


Figure 3: VMRay Analyzer's function log – Comparison of GuLoader's new behavior (left) with previously analyzed samples (right)

Last, it downloads the final AZORult stealer payload, maps it into its own process, and transfers control flow (Figure 4).

HTTP Session #3

Information	Value
Server Name	onedrive.live.com
Server Port	80
Total Data Sent	232 bytes
Total Data Received	977 bytes

Operation	Information	Success	Count	Logfile
Open Session	user_agent = Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko, access_type = INTERNET_OPEN_TYPE_PRECONFIG	✓	1	FN
Open Connection	protocol = http, server_name = onedrive.live.com, server_port = 80	✓	1	FN
Open HTTP Request	http_verb = GET, http_version = HTTP 1.1, target_resource = /download, flags = INTERNET_FLAG_PRAGMA_NOCACHE, INTERNET_FLAG_NO_CACHE_WRITE, INTERNET_FLAG_RELOAD	✓	1	FN
Send HTTP Request	headers = WINHTTP_NO_ADDITIONAL_HEADERS, url = http://onedrive.live.com /download?cid=4C3F5C65A99DA195&resid=4C3F5C65A99DA195%21241& authkey=AGyBKeKMs6qKShY	✓	1	FN
Read Response	size = 65536, size_out = 65536	✓	1	FN DATA
Read Response	size = 65536, size_out = 49216	✓	1	FN DATA
Read Response	size = 65536, size_out = 0	✓	1	FN
Close Session		✓	1	FN

AZORult's Behavior

From this point on, the behavior of AZORult is visible. AZORult is an information stealer that targets login credentials, cookies, cryptocurrency wallets, and more (Figure 5).

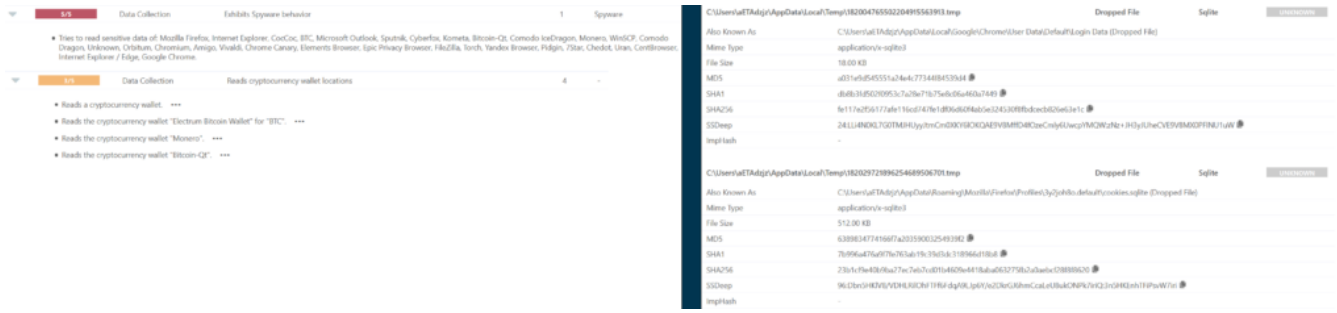


Figure 5: VMRay Analyzer – AZORult's data collection

AZORult v3 always appends the XOR key used to encrypt the following message sent to its C&C at the beginning of the message. Thus, the initial communication always starts with three NUL bytes followed by an XOR encrypted ID hash (Figure 6). In our investigation, we found multiple servers used as its C&C (see IOCs) that all contain the same path.

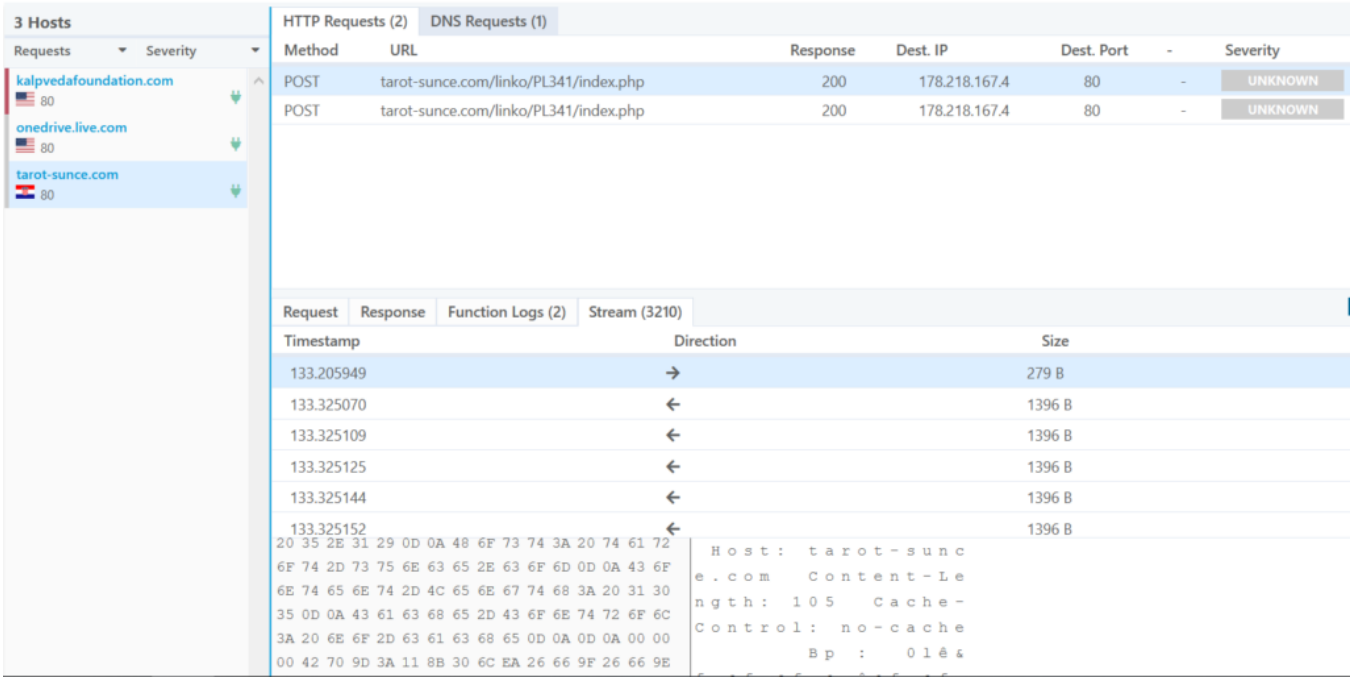


Figure 6: VMRay Analyzer – AZORult's initial message sent to its C&C server.

Conclusion

By using GuLoader in the delivery chain, the attackers can profit from the many features provided by GuLoader that are not offered by AZORult on its own. This obstructs dynamic analysis, complicates manual analysis and provides a flexible, easy distribution of tasks to the attacker without the requirement of advanced specialized knowledge. Despite all that, the VMRay Analyzer monitored the complete delivery chain from the initial RTF document to the final payload.

As mentioned before, these documents are sent via spam emails which are typical attack vectors that attackers use as an entry into the network. Including the VMRay Email Threat Defender (ETD) in the network helps to detect and prevent such attacks.

IOCs

Documents	5ff8a87fd7626d4beab7a5be7f285f1d1d64478509f27aca6fd9de
9a5f4116b1be763a38e25cb14869b57daf9ae4fe1c2e72adc433eccc95d5f539	
08df240668051225b392d88174dadd0db2703ee1ba93c62e3b020cb2be188c17	
6a39c54717f2c9f76f5cf9bde58ca256ab1ed77985b3f590d3797fd6655c19ac	
f0fb1c2a2150e9a33488974952af6c8f0cd52d463ab656e36d17b7d224d04f8e	

cc88795da896ebd8df6fdd996179ae53285c021b0d7437fa9bffca4e5fbc0473	
d0f83c5b91494e26b3c0cc108aa43f6865a17eee870a28f1f7d89669e177d279	
3bd6858a664535a00192021b4b89ab96d47fcf08c32fee5ea97ded3099e39ba8	
GuLoader using MsiEnumProducts	e000b0cae7df0753ea12d97175e393bacf905613eef1a59d7e17
1e6a09e38553c090a119156022d61670adf96f8a635a3dac11f11dd395c107ba	
4487e0798fb74f9891c48625b3a189dbd1e05e2c400cd710f4ea0bdf03b9adbd	
c256466dc256d55f7cba0f1c2201f208b82deabd903dd3a71a4e7989e6a61ff7	
c87290bb28696eddacaadc0f01805f841bda964d55efa9c39d0a06f1d31ede3b	
1623c45e067729ec3b334294da18855e0e5312fd4d9d28f95d4e38b074255892	
b5389059c8b005b1968197bb1bb38edc024501c02bf8941d287b1c01358b121a	
e97e14f57e6f9ad987e4b5079b7ba8a387115b89784958d40d1f65d79d027315	
Domains hosting GuLoader	kalpvedafoundation[.]com
cieloabiertocasahogar[.]com	
www[.]cecadperu[.]com	
AZORult C&Cs	skilldrivinget[.]com/ojman/PL341//index[.]php
laninesolution[.]com/roky/PL341/index[.]php	
tarot-sunce[.]com/linko/PL341/index[.]php	
eksodus[.]id/ghytoja/PL341/index[.]php	
laninesolution[.]com/roky/PL341/index[.]php	