Threat profile: Egregor ransomware is making a name for itself

blog.malwarebytes.com/ransomware/2020/12/threat-profile-egregor-ransomware-is-making-a-name-for-itself/

Pieter Arntz December 15, 2020

What is Egregor?

Egregor ransomware is a relatively new ransomware (first spotted in September 2020) that seems intent on making its way to the top right now. Egregor is considered a variant of Ransom.Sekhmet based on similarities in obfuscation, API-calls, and the ransom note.

As we've reported in the past, affiliates that were using Maze ransomware started moving over to Egregor even before the Maze gang officially announced they were calling it quits. Egregor has already targeted some well-known victims like Barnes & Noble, Kmart and Ubisoft.

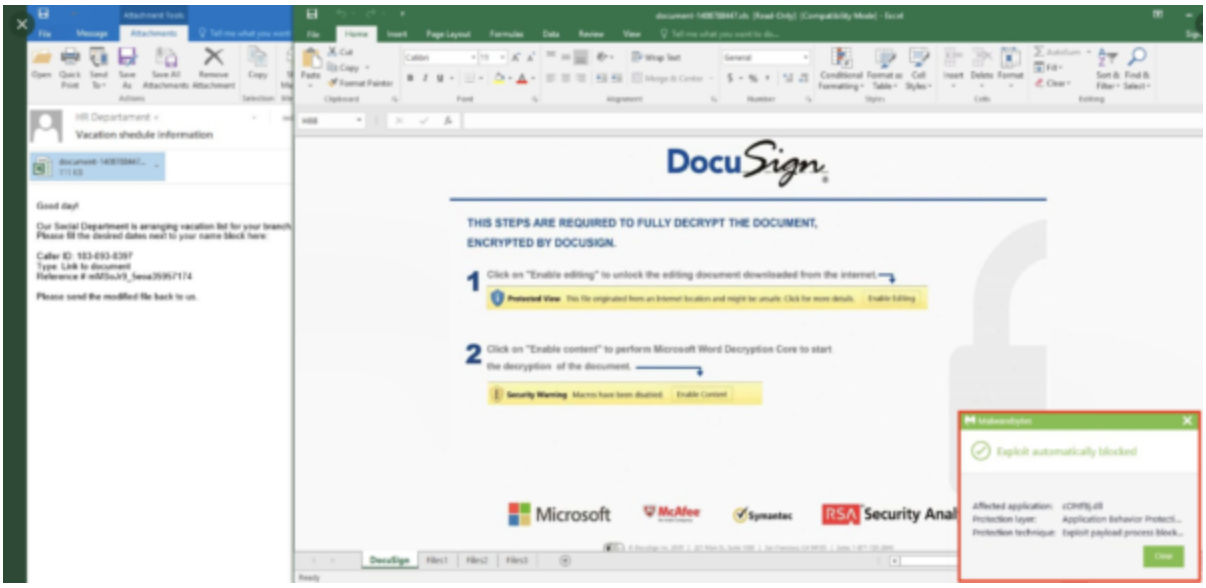
How does Egregor spread?

The primary distribution method for Egregor is Cobalt Strike. Targeted environments are initially compromised through various means (RDP probing, phishing) and once the Cobalt Strike beacon payload is established and persistent, it is then used to deliver and launch the Egregor payloads.

```
------------------

| What happened? |

------------------
Your network was ATTACKED, your computers and servers were LOCKED,

Your private data was DOWNLOADED.
```

First part of the Egregor ransom note

But since Egregor is a ransomware-as-a-service (RaaS) operation with multiple affiliates, the delivery and weaponization tactics can vary. We've also seen it being spread via phishing emails recently. The attack typically unfolds in two steps: initial compromise with email lure that drops Qakbot, followed by the actual Egregor ransomware. The latter is deployed manually by the attackers who have previously gained access as a result of the initial compromise.



There have also been some reports of Egregor utilizing CVE-2020-0688 (a remote code execution flaw in Microsoft Exchange). Some sources also report the possible exploitation of CVE-2018-8174 (VBScript Engine), CVE-2018-4878 (Adobe Flash Player), and CVE-2018-15982 (Adobe Flash Player).

The most common attack method seems to entail an initial spray-and-pray tactic, after which the threat actors make a selection of the available openings. They will obviously go for the easiest and most profitable ones based on primary reconnaissance data from the first stage of the attack. They will then try to enlarge their foothold on the breached network and look for the data and servers that are most critical for the victim. This will give the attackers extra leverage and a bigger chance to cash in their ransom demand.

Egregor does not seem to have a geographical preference, even though Sekhmet has seemed to focus on the US in the past 7 weeks.

Sekhmet attacks in the last 7 weeks per country

Egregor threatens to leak exfiltrated data

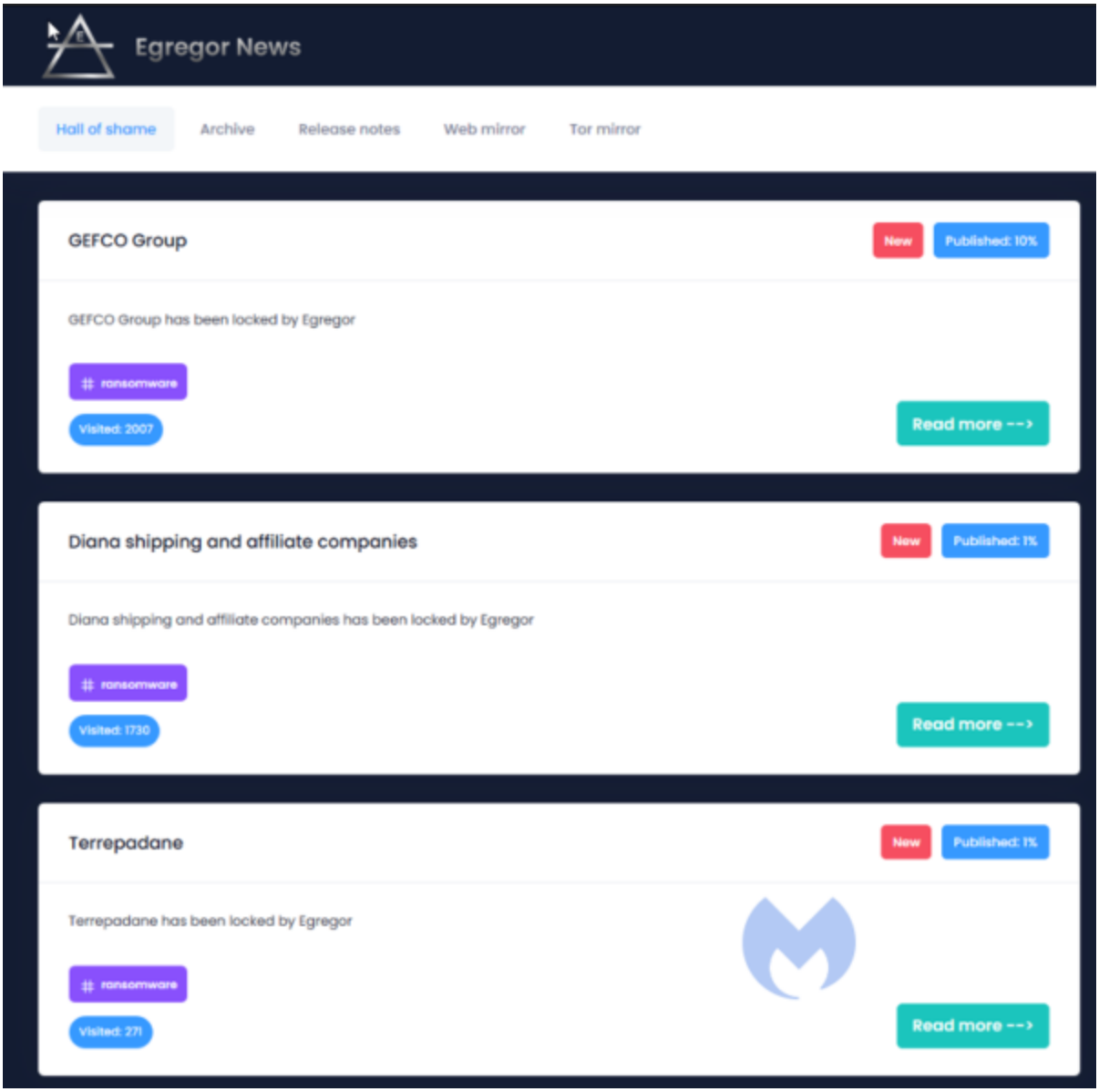
According to the ransom note, if the ransom is not paid by the company within 3 days, and aside from leaking part of the stolen data, the attackers will announce the breach through mass media so the company's partners and clients will know that the company was victimized.

```
----------------------|

| What does it mean? |

----------------------
It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.
--------------------------

| How it can be avoided? |

--------------------------
In order to avoid this,

To avoid this issue you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing AGREEMENT.
-------------------------------------------

| What if I do not contact you in 3 days? |

-------------------------------------------
If you do not contact us in the next 3 DAYS we will begin DATA publication.
```

Part 2

of the Egregor ransom note

In all three the cases we mentioned earlier, the attackers published information on a leak site showing that they had accessed files during the attack, but didn't necessarily reveal source code or anything particularly sensitive.



Announcements of leaked data on the Egregor website

Education by the hands-on experts

A very typical trait of the Egregor ransomware is that the attackers offer to educate their victims in order to help them escape future attacks.

Part 3 of the Egregor ransom note

Cybersecurity advice is promised to those victims that pay the ransom as an extra bonus. What these recommendations look like is unknown at the time of writing. A truthful explanation about how the victim in question was infected, infiltrated, and how data was exfiltrated would certainly help in a forensic investigation of the incident.

Egregor victim Randstad

One of the latest victims seems to be Netherlands-based Randstad, one of the largest recruitment- and head-hunting agencies in the world. In its press release, Randstad specifically calls out Egregor as the attacker.

“We believe the incident started with a phishing email that initiated malicious software to be installed,” a Randstad spokesperson said in an email.

The listing on the Egregor site confirms the attack

The press release confirms the stolen data but is unclear about the exact content.

> “To date, our investigation has revealed that the Egregor group obtained unauthorized and unlawful access to our global IT environment and to certain data, in particular related to our operations in the US, Poland, Italy and France. They have now published what is claimed to be a subset of that data.”

Depending on the stolen data, and given the line of business, the content could be very sensitive and confidential. According to Randstad, the company was able to limit the impact, and the stolen data are in particular related to their operations in the US, Poland, Italy and France.

Third party cybersecurity and forensic experts were engaged to assist with the investigation and remediation of the incident.

IOCs

Tor Onion URLs:

- egregorwiki.top
- wikiegregor.top
- sekhmet.top
- sekhmetleaks.top

SHA256 hashes:

- 4c9e3ffda0e663217638e6192a093bbc23cd9ebfbdf6d2fc683f331beaee0321
- aee131ba1bfc4b6fa1961a7336e43d667086ebd2c7ff81029e14b2bf47d9f3a7

Ransom note:

RECOVER-FILES.txt (some parts of the ransom note can be seen in the article)