GitHub - cert-orangecyberdefense/edam: Edam dropper

By Mar-Pic

Archived: 2026-04-05 21:35:09 UTC

While monitoring new Emmenhtal iterations, our World Watch team encountered samples likely associated to a politically-aligned malicious campaign, strongly differing from usual financially motivated Emmenhtal distributions leading to commodity infostealers. This confirms the existence of multiple Emmenhtal affiliates, as well as a potential pro-Russian alignment for some of them.

Around mid-October, an infection chain leveraged lure documents related to the 21st Gas Infrastructure Europe (GIE) conference in Munich, possibly targeting organizations in the European energy sector.

Threat actors distributed LNK files (likely through spear phishing) in order to deploy the Emmenhtal loader. These LNK launch an embedded PowerShell script which spawns an execution of the LOLBIN mshta.exe to read an HTA concatenated to a legitimate PE file downloaded from an attacker-controlled C2. The malicious HTA data located in the padding of this PE file corresponds to Emmenhtal‘s first stage, which is then followed by additional consecutive Javascript and Powershell stages. The loader then downloads from two distinct C2 servers a decoy PDF as well as malicious DLL we dubbed Edam Dropper.

Edam is written in C++ and its PDB path indicates it is called "droper_dll". It is capable of establishing persistence by setting up a Run key as Setting App which points towards its own file and then of downloading from another C2 a final stage using HTTP GET.

In this cluster, the C2 were hosted on compromised WordPress infrastructure based in Ukraine and Poland. Similarly to the decoy documents, this infrastructure masqueraded as related to the 21st Gas Infrastructure Europe Annual Conference in Munich.

The campaign we analyzed was also detailed by researchers from StrikeReady last week. It could be related to Sandworm (APT44). This operation does indeed coincide with Sandworm’s reported proclivity for using criminally sourced malware variants, as well as its longstanding interest in the European energy sector.

Links: https://www.orangecyberdefense.com/global/blog/cert-news/emmenhtal-a-little-known-loader-distributing-commodity-infostealers-worldwide https://malpedia.caad.fkie.fraunhofer.de/details/win.emmenhtal https://strikeready.com/blog/ru-apt-targeting-energy-infrastructure-unknown-unknowns-part-3/
