New Microsoft Office “Follina” zero-day Already Shared on Ransomware Forums

May 31, 2022 | Minerva Labs Research Team

The new zero-day MS Word vulnerability recently discovered by Nao_Sec on May 27, 2022, titled 'Follina' (CVE-2022-30190) targeting Microsoft Office is being actively utilised, Minerva researchers found. The exploit targets a vulnerability in Microsoft’s Windows Support Diagnostic Tool (MSDT) that occurs due to the ms-msdt MSProtocol URI scheme which could load code and execute via PowerShell despite macros being disabled. Successful exploitation of the CVE enables an attacker to execute arbitrary code on the targeted host. However, the attacker must socially engineer the victim into opening a specially crafted file to exploit this issue which requires a targeted effort to succeed making the vulnerability less prominent to unskilled actors but highly relevant to ransomware gangs such as CONTI, CL0P and ALPHV. To combat this new threat businesses must focus on threat prevention—an approach in which Minerva excels.

An Exploit Tailored to Ransomware Operators

The CVE is already being discussed on key underground dark-web forums catering to ransomware groups and the Ransomware-as-a-Service (RaaS) model including RAMP. Since the announcement by Nao Sec, Minerva analysts have observed multiple dark web actors discussing the CVE including actors on key Russian underground forums, Telegram, Discord and English language forum Breached. The malicious operator DarckSol, a respected and active member of a Russian language forum, shared a link in a thread dedicated to the CVE containing PoC and guidance on weaponization.

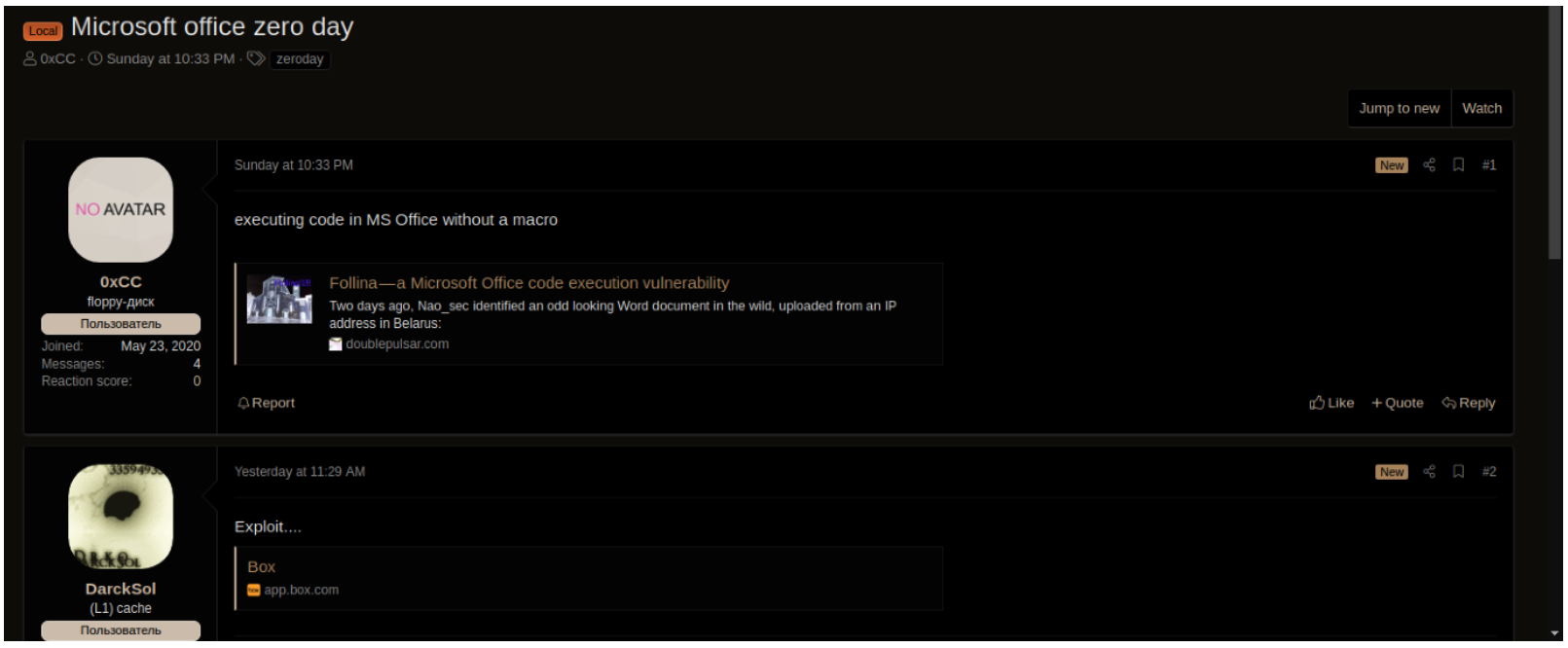

Figure 1: DarckSol sharing download link for Follina on a Russian language forum.

That multiple underground actors already possess the PoC and weaponization guidance is problematic as the overall time from a threat emerges on underground forums to weaponization by ransomware groups is diminishing while ransomware encryption is also becoming faster.

Exploited in the Wild

Although Microsoft has assigned Follina an Exploitability Index (EI) rating of "0 — Exploitation Detected" the exploit already been exploited in the wild. As the exploit targets MS Office and relies on social engineering and has already been exploited in the wild it is highly likely that ransomware operators are racing to use the CVE as part of their toolkit, and some are likely to already operate a working exploit.

Minerva Armor — our anti-ransomware platform - blocks this vulnerability already and has done so for more than a year (policies updated since March 2021) through our malicious document prevention module. This is part of the protection offered by the agent and supports our mission to actively prevent ransomware before it starts.

Advice on Mitigation

• A standard mitigating tactic to this type of vulnerability is to not accept files from unknown or untrusted sources. • Deploy the Minerva Armor agent and ensure your policy has been updated in the last 1.5 years. • Blocking MSDT via AppLocker exceptions to mitigate against this vulnerability. • Educate employees on common Social Engineering lures and warning signs.

« Previous Post