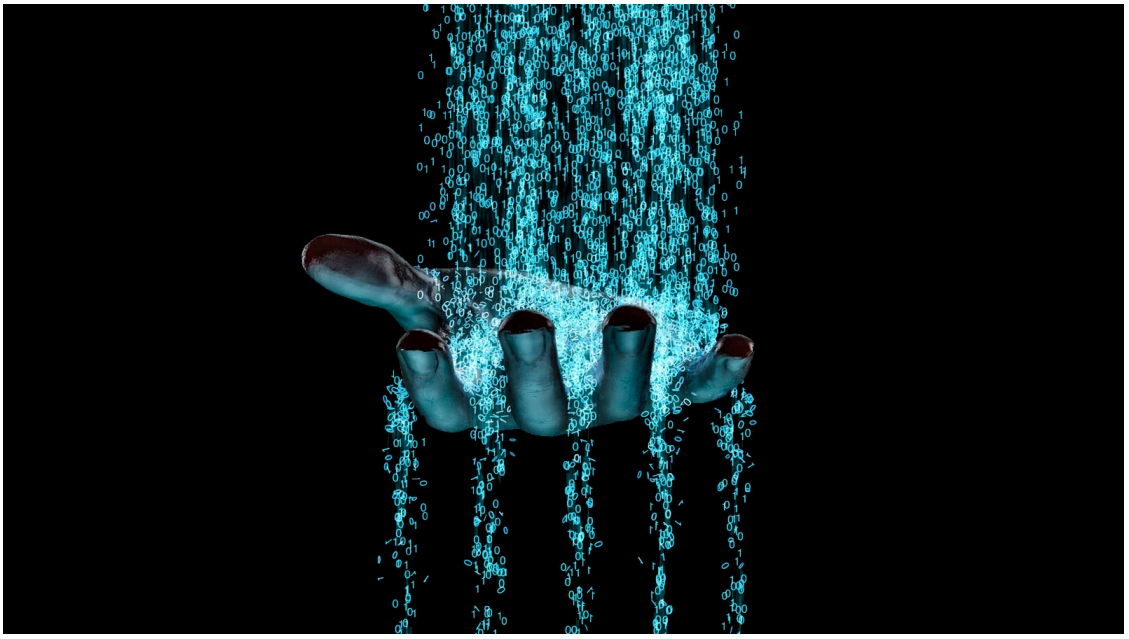
Gamaredon hackers start stealing data 30 minutes after a breach

By Bill Toulas

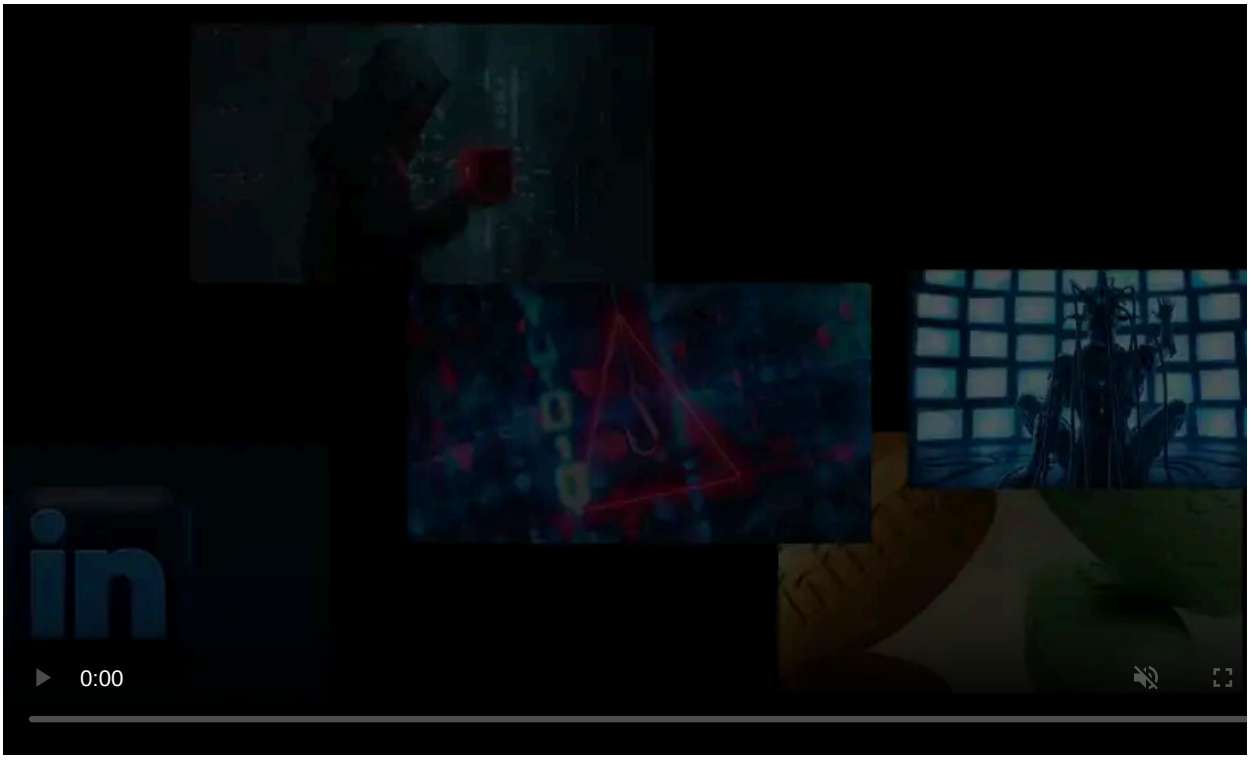
Published: 2023-07-15 · Archived: 2026-04-05 18:52:50 UTC

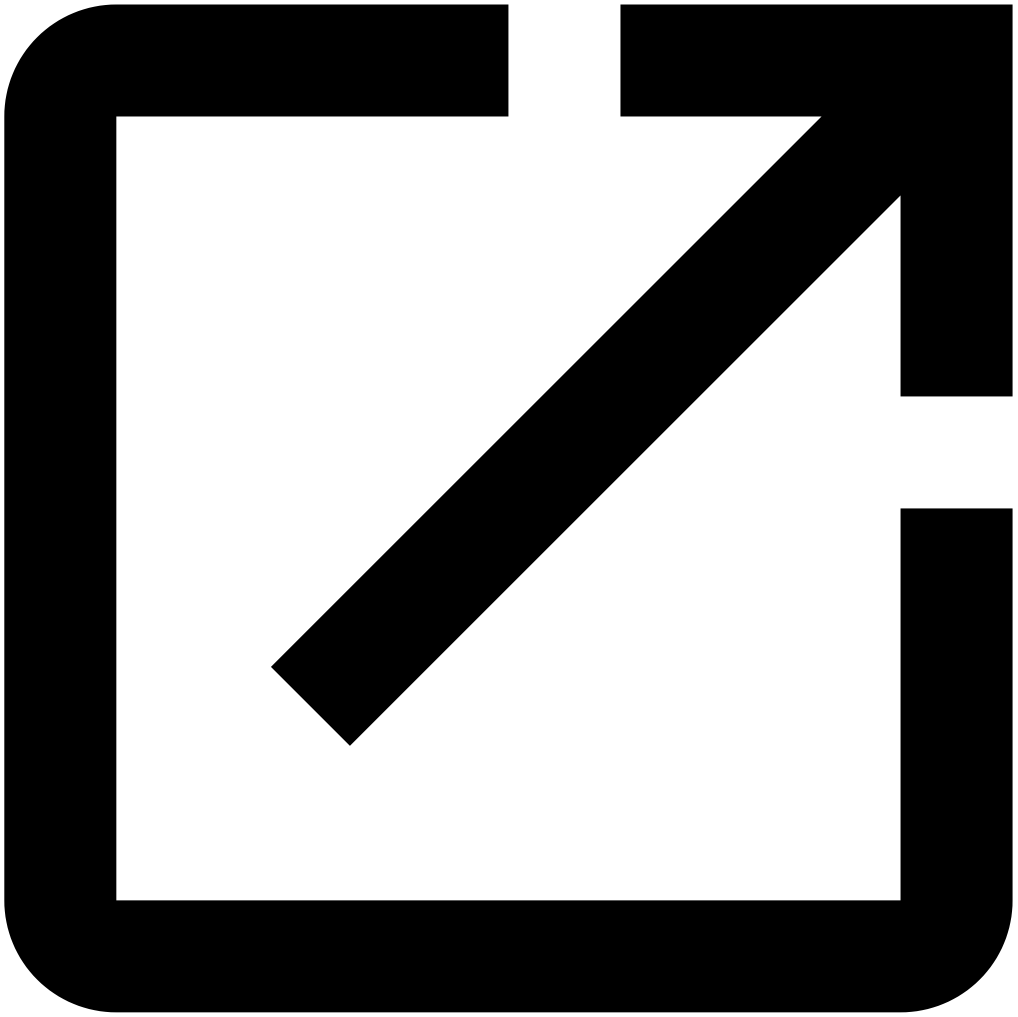


Ukraine's Computer Emergency Response Team (CERT-UA) is warning that the Gamaredon hacking operates in rapid attacks, stealing data from breached systems in under an hour.

Gamaredon, aka Armageddon, UAC-0010, and Shuckworm, is a Russian, state-sponsored cyber-espionage hacking group with cybersecurity researchers linking them to the FSB (Russian Federal Security Service) and having members who are former SSU officers who defected to Russia in 2014.

Since the start of the Russian invasion, the threat actors are believed to be responsible for thousands of attacks against the government and other critical public and private organizations in Ukraine.


0:00



The accumulation of data from these attacks has enabled CERT-UA to outline the group's attacks, which it shares to help defenders detect and stop network infiltration attempts.

Gamaredon attack traits

Gamaredon attacks commonly start with an email or message sent to targets via Telegram, WhatsApp, Signal, or other IM apps.

The initial infection is achieved by tricking the victim into opening malicious attachments such as HTM, HTA, and LNK files disguised as Microsoft Word or Excel documents.

Once the victim launches the malicious attachments, PowerShell scripts and malware (usually 'GammaSteel') are downloaded and executed on the victim's device.

The initial infection step also modifies Microsoft Office Word templates so that all documents created on the infected computer carry a malicious macro that can spread Gamaredon's malware to other systems.

The PowerShell script targets browser cookies containing session data to enable the hackers to take over online accounts protected by two-factor authentication.

Regarding GammaSteel's functionality, CERT-UA says it targets files with a specified list of extensions that are: .doc, .docx, .xls, .xlsx, .rtf, .odt, .txt, .jpg, .jpeg, .pdf, .ps1, .rar, .zip, .7z, .mdb.

If the attackers are interested in the documents found on a breached computer, they exfiltrate them within 30-50 minutes.

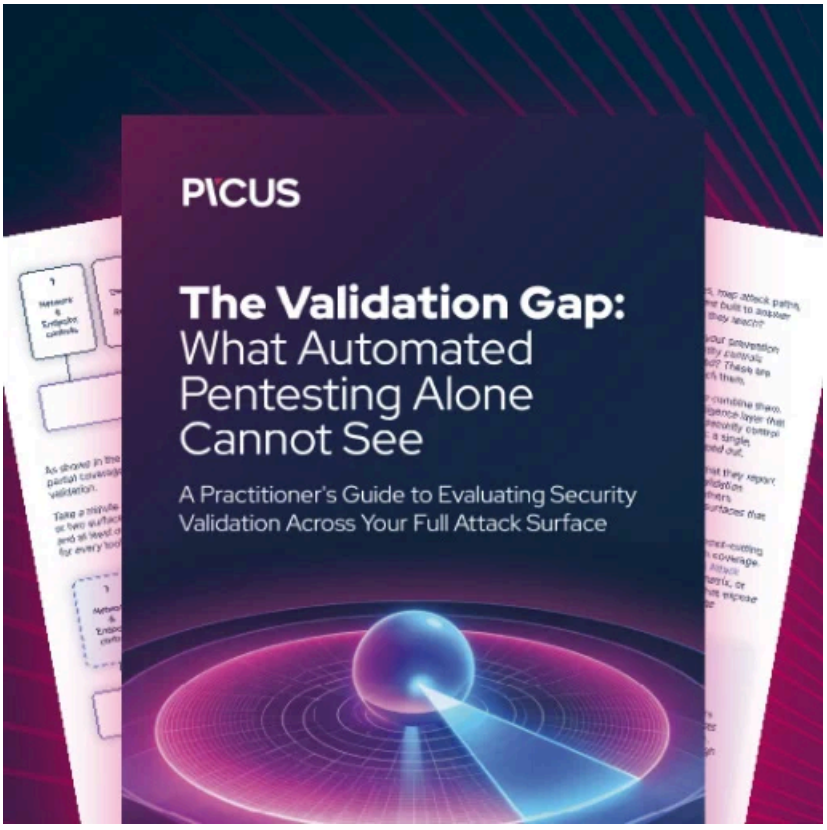
Another interesting aspect of Gamaredon infections is that the threat actors plant as many as 120 malicious infected files per week on the compromised system to increase the likelihood of re-infection.

"If during the disinfection process, after cleaning the operating system registry, deleting files, scheduled tasks, etc., at least one infected file or document is left on the computer (quite often users reinstall the OS and transfer "necessary" documents without checking), then the computer will likely be infected again." explains CERT-UA (machine translated).

Any USB sticks inserted on the ports of an infected computer will also be automatically infected with Gamaredon's initial compromise payloads, potentially furthering the breach to isolated networks.

Finally, the hackers change the IP addresses of intermediate victim command and control servers three to six times daily, making it harder for defenders to block or trace their activities.

At this time, CERT-UA says the best way to limit the effectiveness of Gamaredon attacks is to block or restrict the unauthorized execution of mshta.exe, wscript.exe, cscript.exe, and powershell.exe.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
