DCRat backdoor returns

securelist.com/new-wave-of-attacks-with-dcrat-backdoor-distributed-by-maas/115850/

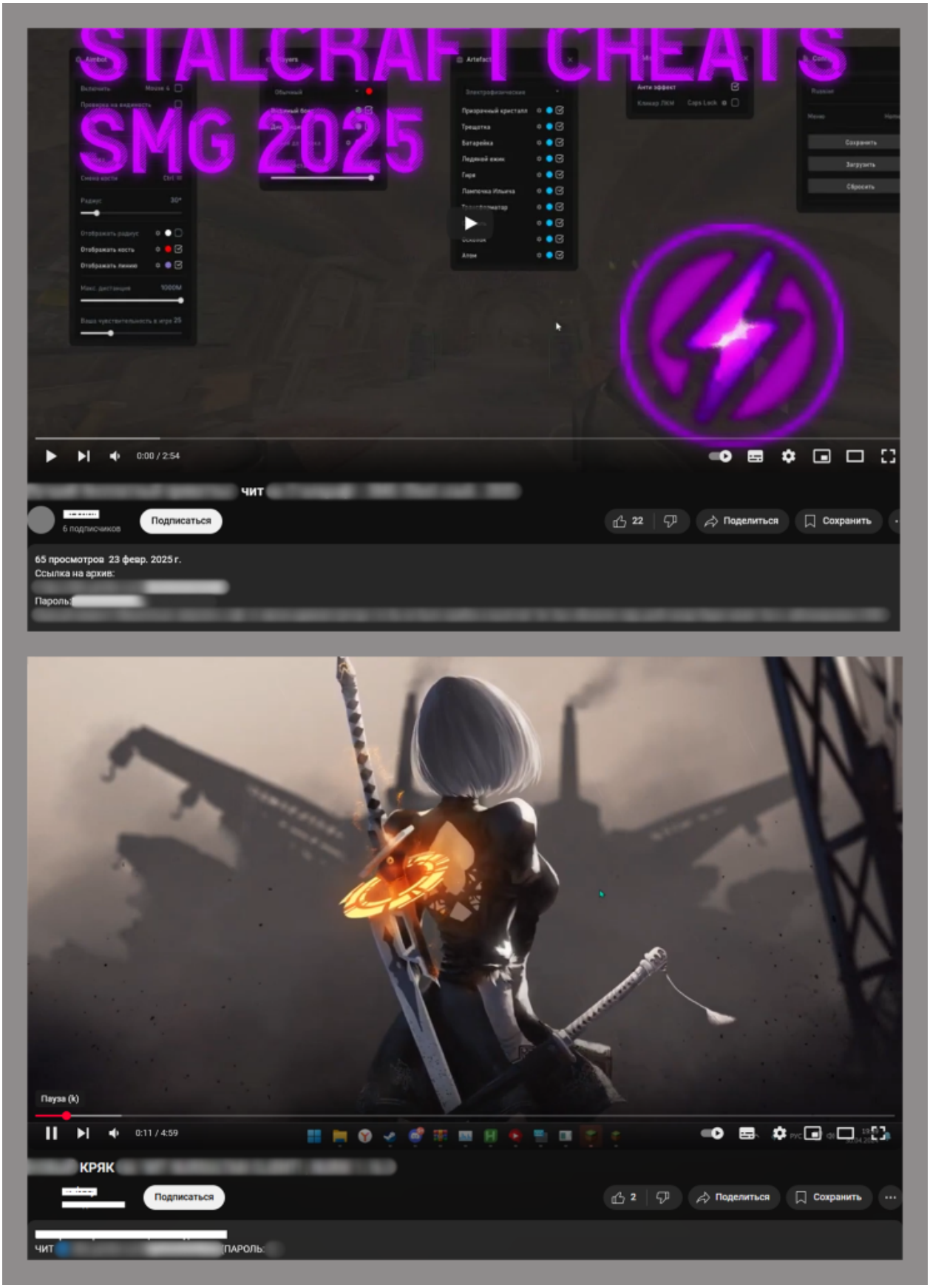
Authors

Expert AMR

Since the beginning of the year, we've been tracking in our telemetry a new wave of DCRat distribution, with paid access to the backdoor provided under the Malware-as-a-Service (MaaS) model. The cybercriminal group behind it also offers support for the malware and infrastructure setup for hosting the C2 servers.

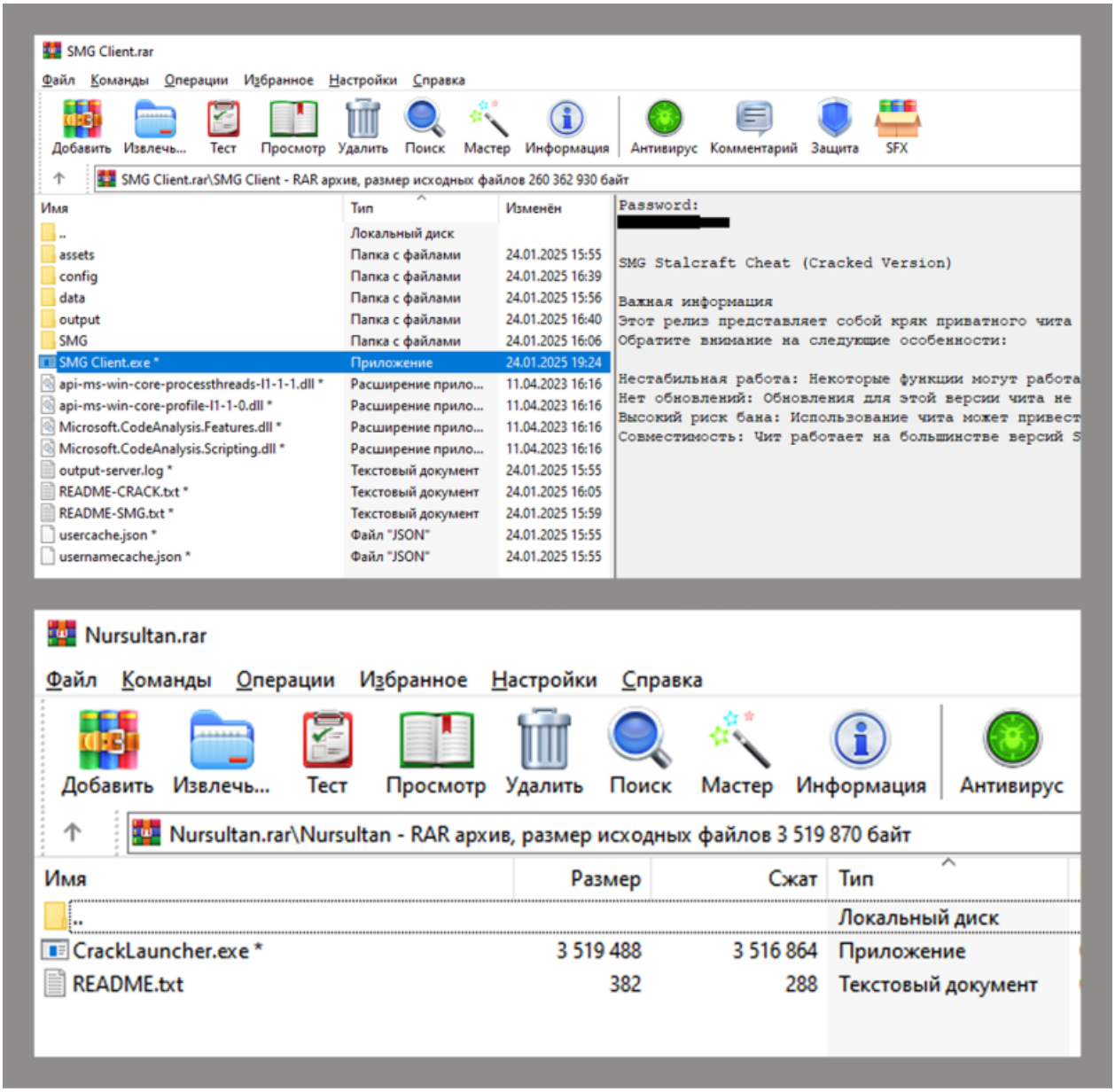
Distribution

The DCRat backdoor is distributed through the YouTube platform. Attackers create fake accounts or use stolen ones, then upload videos advertising cheats, cracks, gaming bots and similar software. In the video description is a download link to the product supposedly being advertised. The link points to a legitimate file-sharing service where a password-protected archive awaits, the password for which is also in the video description.



YouTube video ad for a cheat and crack

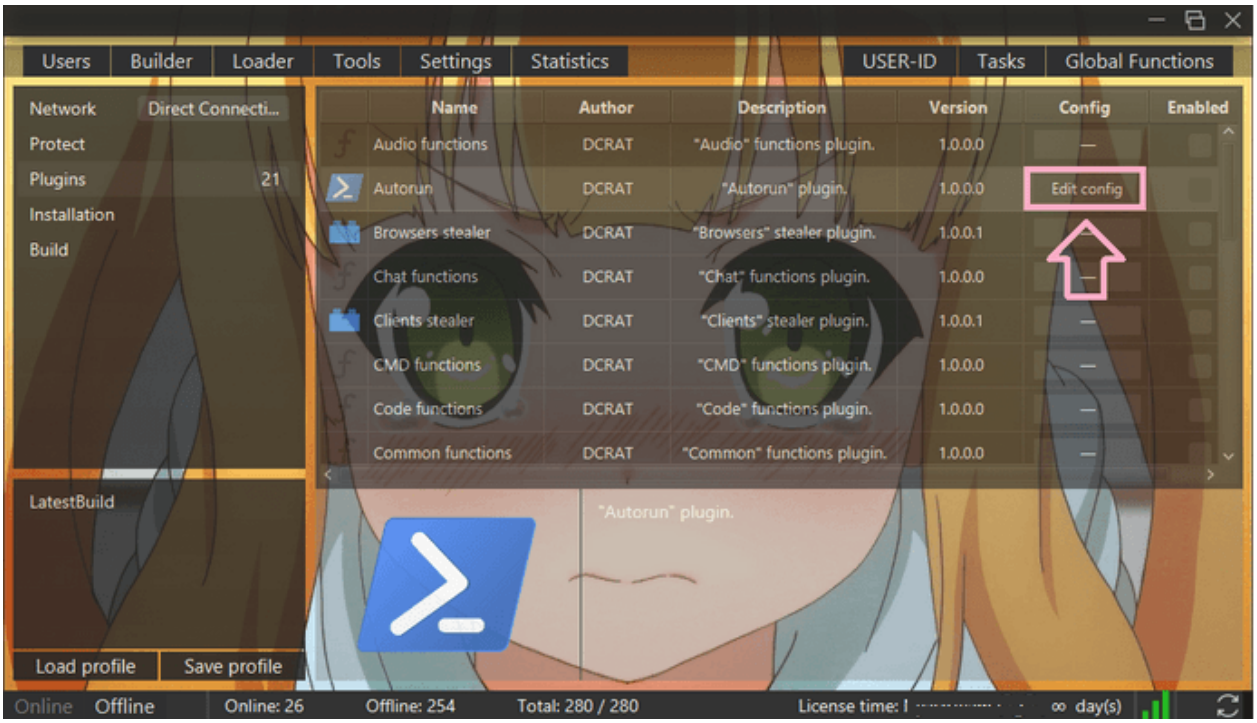
Instead of gaming software, these archives contain the DCRat Trojan, along with various junk files and folders to distract the victim's attention.



Archives with DCRat disguised as a cheat and crack

Backdoor

The distributed backdoor belongs to a family of remote access Trojans (RATs) dubbed Dark Crystal RAT (DCRat for short), known since 2018. Besides backdoor capability, the Trojan can load extra modules to boost its functionality. Throughout the backdoor's existence, we have obtained and analyzed 34 different plugins, the most dangerous functions of which are keystroke logging, webcam access, file grabbing and password exfiltration.



DCRat builder plugins on the attackers' site

Infrastructure

To support the infrastructure, the attackers register second-level domains (most often in the RU zone), which they use to create third-level domains for hosting the C2 servers. The group has registered at least 57 new second-level domains since the start of the year, five of which already serve more than 40 third-level domains.

A distinctive feature of the campaign is the appearance of certain words in the second-level domains of the malicious infrastructure, such as “nyashka”, “nyashkoon”, “nyashtyan”, etc. Users interested in Japanese pop culture will surely recognize these slang terms. Among anime and manga fans, “nyasha” has come to mean “cute” or “hon”, and it’s this word that’s most often seen in the second-level domains.

Host name	Host name	Host name	Host name
268761cm.nyanyash.ru	251037cm.nyashk.ru	322461cm.shnyash.ru	260348cm.nyashnyash.ru
140061cm.nyanyash.ru	901125cm.nyashk.ru	289098cm.shnyash.ru	120149cm.nyashnyash.ru
389920cm.nyanyash.ru	253753cm.nyashk.ru	136601cm.shnyash.ru	392013cm.nyashnyash.ru
723360cm.nyanyash.ru	753333cm.nyashk.ru	568327cm.shnyash.ru	557844cm.nyashnyash.ru
542148cm.nyanyash.ru	879351cm.nyashk.ru	334407cm.shnyash.ru	233713cm.nyashnyash.ru
047506cm.nyanyash.ru	802142cm.nyashk.ru	428982cm.shnyash.ru	874381cm.nyashnyash.ru
446068cm.nyanyash.ru	851078cm.nyashk.ru	679356cm.shnyash.ru	831632cm.nyashnyash.ru
844666cm.nyanyash.ru	758430cm.nyashk.ru	809172cm.shnyash.ru	294210cm.nyashnyash.ru
946786cm.nyanyash.ru	947002cm.nyashk.ru	127004cm.shnyash.ru	463313cm.nyashnyash.ru
835725cm.nyanyash.ru	103705cm.nyashk.ru	524871cm.shnyash.ru	723486cm.nyashnyash.ru
593412cm.nyanyash.ru	908457cm.nyashk.ru	317827cm.shnyash.ru	222390cm.nyashnyash.ru
714280cm.nyanyash.ru	348309cm.nyashk.ru	192592cm.shnyash.ru	704249cm.nyashnyash.ru
148098cm.nyanyash.ru	966489cm.nyashk.ru	657355cm.shnyash.ru	532551cm.nyashnyash.ru
776437cm.nyanyash.ru	800811cm.nyashk.ru	024363cm.shnyash.ru	025813cm.nyashnyash.ru
367533cm.nyanyash.ru	623127cm.nyashk.ru	856748cm.shnyash.ru	741300cm.nyashnyash.ru
821518cm.nyanyash.ru	460629cm.nyashk.ru	045849cm.shnyash.ru	937946cm.nyashnyash.ru
285857cm.nyanyash.ru	008529cm.nyashk.ru	430922cm.shnyash.ru	137777cm.nyashnyash.ru

C2 server addresses with characteristic naming approach

Victims

Based on our telemetry data since the beginning of 2025, 80% of DCRat samples using such domains as C2 servers were downloaded to the devices of users in Russia. The malware also affected a small number of users from Belarus, Kazakhstan and China.

Conclusion

Kaspersky products detect the above-described samples with the verdict Backdoor.MSIL.DCRat.

Note that we also encounter campaigns distributing other types of malware (stealers, miners, loaders) through password-protected archives, so we strongly recommend downloading game-related software only from trusted sources.

DCRat backdoor returns

Your email address will not be published. Required fields are marked *