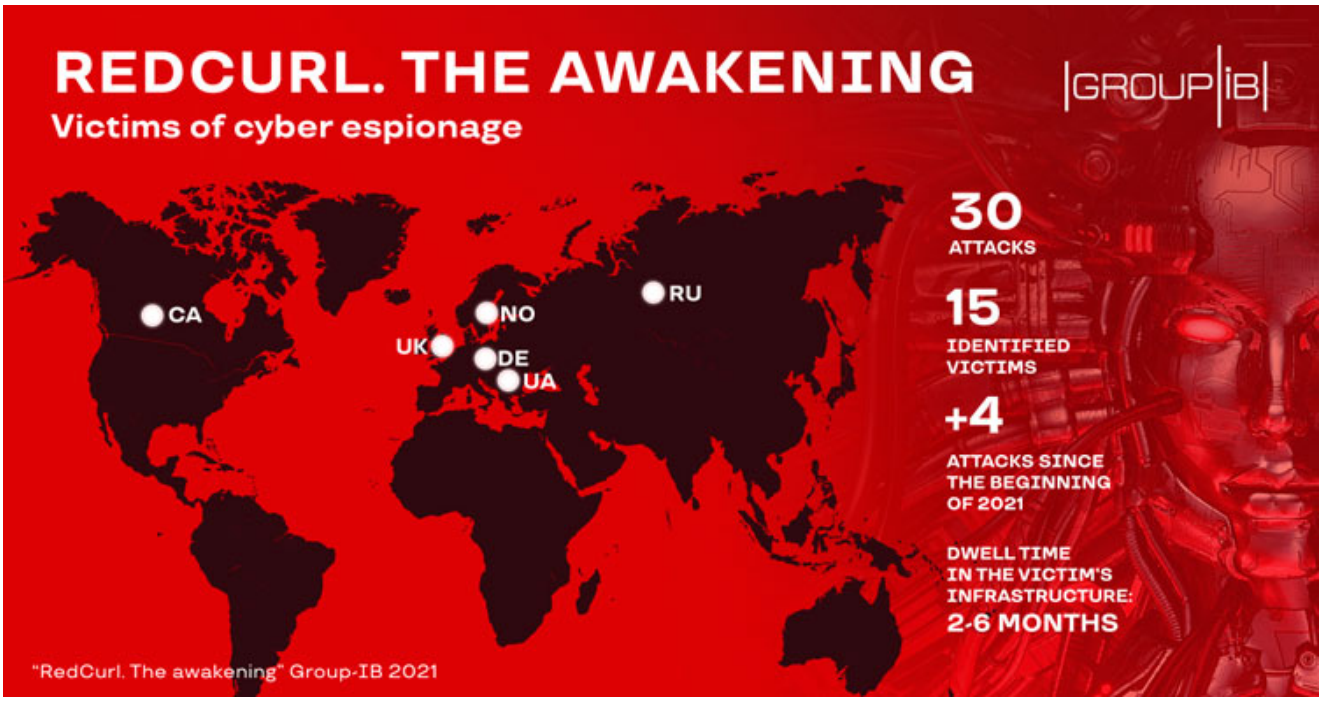
The awakening: Group-IB uncovers new corporate espionage attacks by RedCurl

group-ib.com/media/red-curl-threat-report/

Group-IB, one of the leading solution providers dedicated to detecting and preventing cyberattacks, identifying online fraud, investigating high-tech crimes, and intellectual property protection, detected new attacks by RedCurl, a corporate cyber espionage threat actor targeting companies in various industries. Group-IB's latest report "RedCurl: The awakening" details how the adversary's tactics and tools have evolved. Since the beginning of 2021, RedCurl has carried out four attacks, bringing the total count to 30.



Last year, in the report "RedCurl. The pentest you didn't know about" Group-IB researchers described for the first time a new Russian-speaking hacker group that they had codenamed RedCurl. Between 2018 and 2020, the threat actor carried out at least 26 attacks. Group-IB identified 14 victim organizations across various countries and industries. Victims included companies in the fields of construction, finance, consulting, retail, insurance, and law located in the UK, Germany, Canada, Norway, Russia, and Ukraine. Seven months later, in 2021, RedCurl attacks resumed.

Group-IB Threat Intelligence & Attribution system detected RedCurl's updated arsenal as it appeared: after a long break, the group returned to the corporate cyber espionage

arena. In every attack, the threat actor demonstrates extensive red teaming skills and the ability to bypass traditional anti-virus detection using their own custom malware. This means that more and more companies are likely to fall victim to the group, which conducts well-prepared targeted attacks aimed at stealing internal corporate documentation. Commercial Corporate cyber espionage remains a rare and largely unique phenomenon. We cannot rule out, however, that RedCurl's success could set a new trend in the cybercrime space.

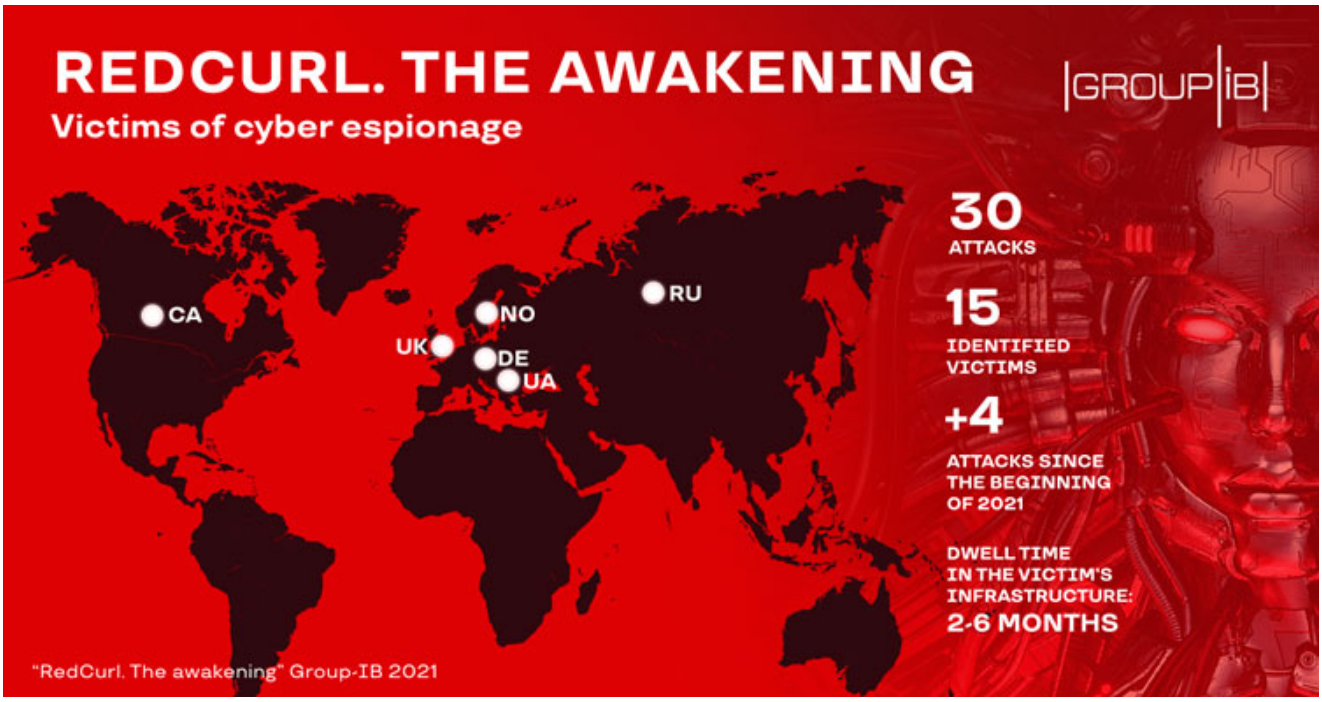
Ivan Pisarev

Head of the Dynamic Malware Analysis Team at Group-IB

Wholesale and retail attacks

Since the beginning of 2021, Group-IB Threat Intelligence team has identified four attacks. One of the victims was a Russian wholesale company, which RedCurl attacked twice. The location of the two other victims remains unknown. Immediately after discovering traces of the attack, Group-IB specialists contacted the identified victim, shared all the relevant information, and provided recommendations to contain the incident and prevent it from spreading.

During the lull in its activities, the group significantly improved their arsenal used during thoroughly prepared cyber espionage attacks that can only be detected by a highly qualified cybersecurity team. For example, analysis of RedCurl's latest attacks revealed that the kill chain for "patient zero" (between receiving the phishing email and launching the module responsible for executing) had grown from three to five stages. Among other improvements, the group added a new reconnaissance tool whose code shares many similarities with the FirstStageAgent module (Group-IB named the tool FSABIN), as well as a PowerShell downloader for the tool. The overall kill chain is as follows:



Before an attack, RedCurl examines their victim thoroughly by collecting information about the target from public sources. The group's signature move is sending spear phishing emails purporting to come from the victim organization's HR department. RedCurl actively uses social engineering: as a rule, email headers contain information about changes to staff incentive programs or other company news. Employees are often lured into clicking on a link with the promise of bonuses.

After infecting a computer in the victim's network, RedCurl collects information about its infrastructure. The hackers are mainly interested in the name and version of the infected system, the list of network and logical drives, and the list of passwords. Group-IB Threat Intelligence team discovered that information from the infected device, the IP address, and the time that the request was received were saved in a separate file on the server side.
It is noteworthy that before the latter took place, the time was adjusted according to the time zone in Minsk (UTC+3).

Slow but steady

RedCurl is known for its patience: the time from "patient zero" becoming infected to data being stolen can be anywhere from two to six months. The group does not use popular post-exploitation tools such as CobaltStrike and Meterpreter. Moreover, they have never been seen using typical ways of controlling compromised devices remotely. Instead, the hackers use self-developed tools and some publicly available programs to gain initial access, achieve persistence, move laterally, and exfiltrate sensitive documentation. All this means that RedCurl's modus operandi remains unique.

Group-IB has noted that despite a high level of control over the victim's network, RedCurl does not encrypt infrastructure, withdraw money from accounts, or demand ransoms for stolen data. This most likely indicates that the group monetizes on its attacks in a different way. The group strives to obtain valuable information as covertly as possible. RedCurl is mainly interested in the following types of files: business emails, staff records, documents relating to various legal entities, court records, and other internal information. Even after the attack has ended, victims could remain unaware that confidential information has been exfiltrated to RedCurl's servers.

Group-IB's new report offers recommendations that IT and cybersecurity teams should follow regardless of a company's size and industry. To better understand RedCurl's techniques, tactics, and procedures (TTPs), Group-IB publishes the MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) matrix based on Group-IB's experience in responding to and analyzing the group's attacks.