RedCurl cybercrime group has hacked companies for three years

By Written by Catalin Cimpanu, ContributorContributor Aug. 13, 2020 at 12:00 a.m. PT

Archived: 2026-04-05 15:38:13 UTC

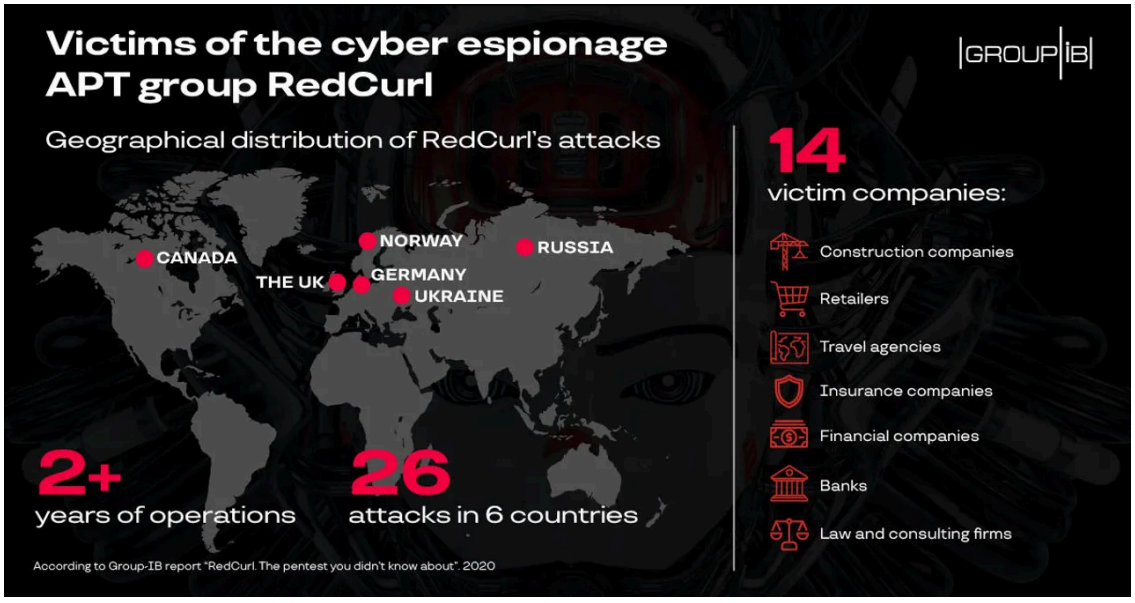

Image: Group-IB

Security

Security researchers have uncovered a new Russian-speaking hacking group that they claim has been focusing on the past three years on corporate espionage, targeting companies across the world to steal documents that contain commercial secrets and employee personal data.

Named RedCurl, the activities of this new group have been detailed in a 57-page report released today by cyber-security firm Group-IB.

The company has been tracking the group since the summer of 2019 when it was first called to investigate a security breach at a company hacked by the group.

Since then, Group-IB said it identified 26 other RedCurl attacks, carried out against 14 organizations, going as far back as 2018.

Victims varied across countries and industry sectors, and included construction companies, retailers, travel agencies, insurance companies, banks, and law and consulting firms from countries like Russia, Ukraine, Canada, Germany, Norway, and the UK.

Spear-phishing and PowerShell

But despite the prolonged three-year hacking spree, the group didn't use complex tools or hacking techniques for their attacks. Instead, the group heavily relied on spear-phishing for initial access.

"RedCurl's distinctive feature, however, is that the email content is carefully drafted," researchers said today. "For instance, the emails displayed the targeted company's address and logo, while the sender address featured the company's domain name.

"The attackers posed as members of the HR team at the targeted organization and sent out emails to multiple employees at once, which made the employees less vigilant, especially considering that many of them worked in the same department," they added.

The emails included links to malware-laced files that victims had to download. Once victims ran the content of the boobytrapped archives, they got infected with a collection of PowerShell-based trojans.


redcurl-schema.jpg
Image: Group-IB

Group-IB said the trojans were unique to the group and allowed RedCurl operators access to basic operations, such as searching systems, downloading other malware, or uploading stolen files to remote servers.

RedCurl hid in hacked networks between two and six months

Where possible, the group also attempted to move laterally through infected networks by accessing network shared drives and replacing original files with boobytrapped LNK (shortcut) files that would infect other employees if they executed the files.

Group-IB researchers say that this phase usually lasted between two and six months.

"The stage of spreading over the network is significantly extended in time as the group strives to remain unnoticed for as long as possible and does not use any active Trojans that could disclose its presence," the company said.

One particular thing that stood out about RedCurl was the use of the WebDAV protocol as a data exfiltration channel, similar to other hacking groups like CloudAtlas and RedOctober. However, Group-IB said it did not find any other major overlaps between the three, and believes they are separate operations based on the current evidence.


redcurl-comparrison.png
Image: Group-IB

The biggest Internet of Things, smart home hacks of 2019

Security
