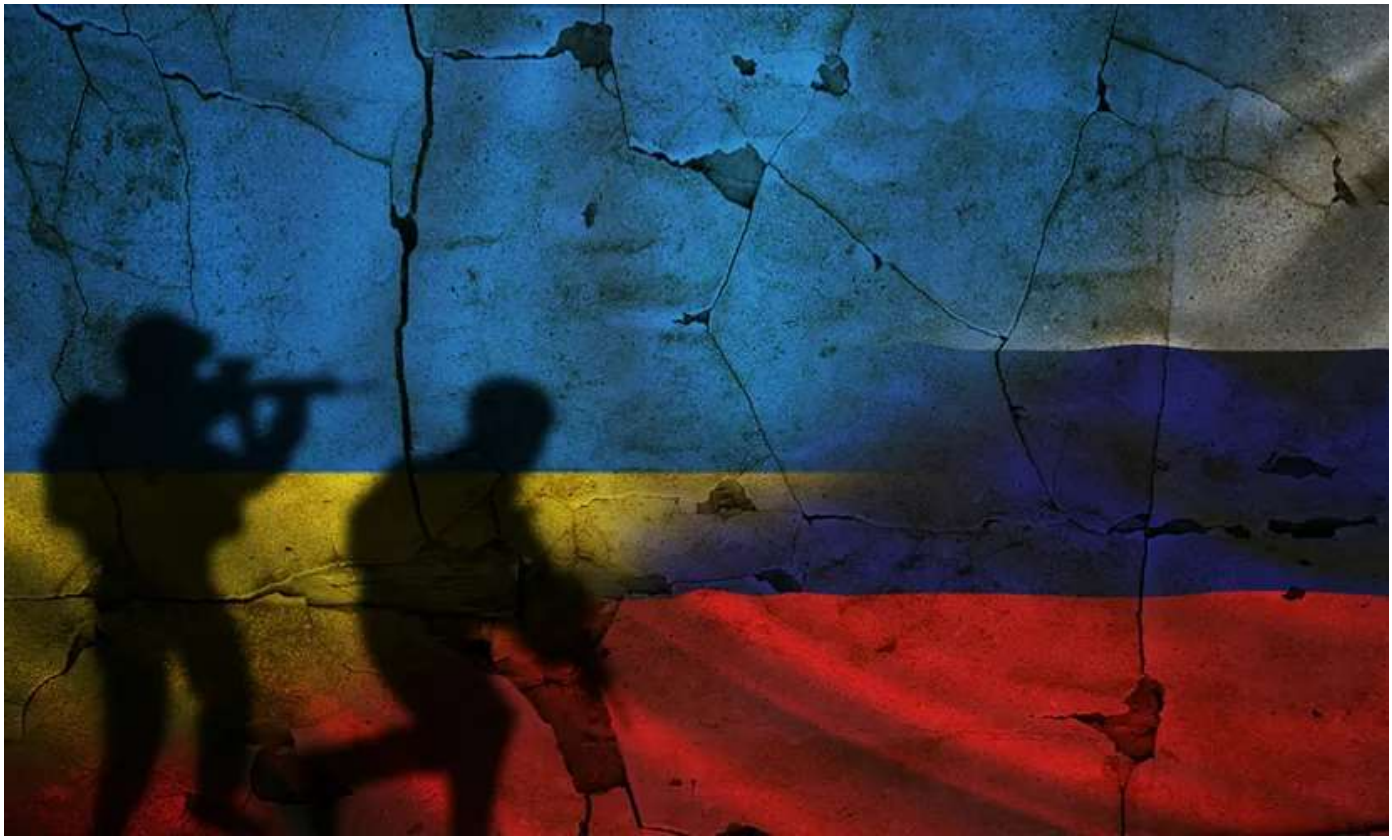
Threat Intelligence

Russia's APT29 intensifies espionage operations

Simon Hendery September 25, 2023



APT29 – also known ask Cozy Bear – increased its phishing attacks on foreign embassies in Ukraine, including targeting those of Russia's partners, Mandiant researchers said. (Image credit: IherPhoto via Getty)

APT29, the threat group linked to the Russia's Foreign Intelligence Service (SVR) and responsible for the SolarWinds supply chain hack, has ramped up the scope and frequency of its espionage attacks this year as the Kremlin sought more intel to assist Russia's war on Ukraine.

The group has made substantial changes to its tooling and tradecraft in a move

embassies in Ukraine, including targeting those of Russia's partners, Mandiant researchers Luke Jenkins, Josh Atkins and Dan Black said in the post.

It was the first time Mandiant had observed the threat group pursuing governments strategically aligned with Moscow, the researchers said.

At the same time, APT29 has also increased its "more routine espionage operations" against diplomatic entities in other parts of the world, they said.

"Across these malware delivery operations, APT29 continues to prioritize European Ministries of Foreign Affairs and embassies, but it has also sustained operations that are global in scope and illustrative of Russia's far-reaching ambitions and interests in other regions."

The threat actor was also continuing an ongoing initial access campaign targeting Microsoft cloud-based services. Mandiant said while the diplomatic and Microsoft campaigns are very different, there is evidence to suggest that once APT29's initial access teams penetrated a victim's environment, they handed off follow-on operations to a separate, centralized exploitation team responsible for data

But as the group's workload has increased this year, its tactics, techniques, and procedures (TTPs) have evolved.

The most visible change to its malware delivery chain observed this year was a shift to hosting its first-stage payloads on compromised web services such as WordPress sites.

"Migrating the first-stage payload server side has likely provided APT29 a greater degree of control over its malware delivery chain and allowed the group to be more judicious about the exposure of its later-stage capabilities," the researchers said.

The change also reduced the number of forensic artifacts the threat actor leaves on compromised networks, meaning less evidence for security teams and researchers to later detect and analyze.

In March the group added a new layer of obfuscation to a campaign, using the TinyURL shortening service to generate malicious phishing links.

Other new techniques seen this year included containing Rootsaw within a PDF document for the first time. When opened, the malicious PDF writes an HML file to disk, which in turn beacons to a domain controlled by the group to profile the victim's information.

Mandiant said APT29's faster pace of operating, and changes including its split into initial access and centralized exploitation teams, "likely reflect a growing mission and pool of resources dedicated to collecting political intelligence."

The threat group "will almost certainly continue to pose a high severity threat to governments and diplomatic entities globally," the researchers said.

Related

THREAT INTELLIGENCE

Novel infostealer spread via Windows Defender SmartScreen flaw

SC Staff January 15, 2024

Attacks leveraging an already patched Windows Defender SmartScreen bypass flaw.

MALWARE

Updated Atomic Stealer malware emerges

SC Staff January 12, 2024

Several updates have been introduced to the Atomic Stealer macOS information-stealing malware, also known as AMOS, including the integration of payload encryption to better evade security software detection, The Hacker News reports.

ENDPOINT/DEVICE SECURITY

US, others potentially targeted by new Volt Typhoon attacks exploiting Cisco router bugs

SC Staff January 12, 2024

The U.S., Australia, India, and the UK are having their government institutions subjected to new attacks by Chinese advanced persistent threat operation Volt Typhoon leveraging a pair of critical vulnerabilities in end-of-life Cisco small business RV320/325 VPN routers, tracked as CVE-2019-1652 and CVE-2019-1653, according to SecurityWeek.

Related Events

ESUMMIT

Threat intelligence: Unleashing the full potential of your security arsenal

TUE FEB 27