Russian APT 'BlueCharlie' Swaps Infrastructure to Evade Detection

darkreading.com/attacks-breaches/russian-apt-bluecharlie-swaps-infrastructure-to-evade-detection

Nate Nelson August 2, 2023

Attacks/Breaches
3 MIN READ

NEWS
Despite being outed earlier this year, the advanced persistent threat group is trying to sneak past researchers again.

August 02, 2023

Source: Chris Van Lennep via Alamy Stock Photo

In a futile attempt to evade detection, the Russian espionage group "BlueCharlie" has swapped out all of its old infrastructure for a network of 94 new domains.

BlueCharlie — aka "Calisto," "COLDRIVER," "SEABORGIUM," and "StarBlizzard" — is a threat actor linked to groups that have been active since at least 2017. In the past, it has targeted organizations across the government, defense, education, and political sectors, as well as NGOs, think tanks, and journalists. Though focused on espionage, it has also been known to perform hack-and-leak operations.

At the turn of the year, one by one, researchers began to out BlueCharlie — describing its campaigns, its impact on the Russia-Ukraine war, breaking down its infrastructure, and even attributing a specific person running the show.

According to Recorded Future, in BlueCharlie's latest campaign, the group completely switched up its infrastructure, creating nearly 100 new domains from which to perform credential harvesting and follow-on espionage attacks.

BlueCharlie's New Domains

In prior campaigns, BlueCharlie used a tool called Evilginx to help name their phishing domains. A threat intelligence analyst at Recorded Future's Insikt Group, who chose to remain anonymous for this story, explains how.

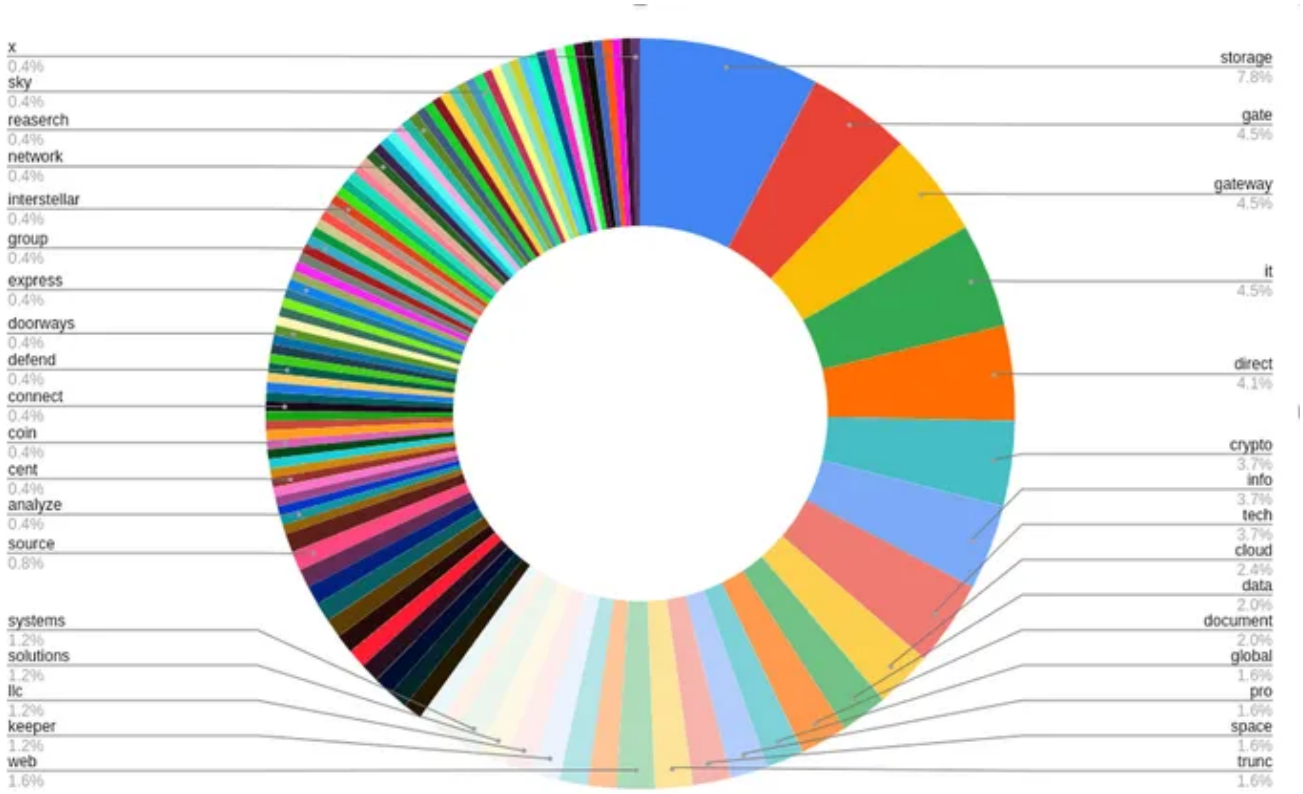
"This framework uses any arbitrarily defined, user-supplied domain, and appends a victim-specific URL to the end of that domain. For example, if a threat actor creates a phishing domain, *goo-ink[.]online*, emulating a Google domain, they can then append a URL structure, like *adfs[.]llnl[.]gov* — which emulates the Microsoft Active Directory of Lawrence Livermore National Laboratory — to create the full phishing URL of *http[:]//goo-ink[.]online/adfs[.]llnl[.]gov*," in order to dupe a Lawrence Livermore National Lab employee into believing the link is legitimate. Lawrence Livermore became a target of BlueCharlie last year.

In rare cases, they add, "the group did employ fully emulated domains of victims," in line with more traditional phishing.

In its latest activity, BlueCharlie used neither the tailing URL structure nor fully emulated domains. Instead, the group named its domains by combining two, seemingly random IT-related terms — say, "storage" and "gateway" — with a hyphen in the middle.

Changing TTPs to Evade Researchers

"People would be less likely to fall for general IT-related domains," the Recorded Future analyst acknowledged, adding fuel to the theory that these changes were made primarily for the sake of change itself.



Breakdown of terms used in BlueCharlie activity since November 2022. (Source: Recorded Future)

"Historically speaking, certain Russian state-sponsored groups such as BlueBravo, BlueDelta, and more have evolved their TTPs extremely quickly," the analyst explains. This time, though, the attackers may simply have adjusted their TTPs in direct response to their prior TTPs being exposed.

"On numerous past occasions, we have directly observed threat actors changing their infrastructure or TTPs in short order following exposure, and that this isn't unique to BlueCharlie/Russian groups — we've seen it from other APT groups as well, so we are confident that they are reacting to exposure," they say.

To defend against ever-changing APT tactics, the authors of the report recommended that organizations practice general cyber hygiene — training employees, disabling macros, and using FIDO2-compliant MFA tokens. "BlueCharlie has demonstrated the ability to adapt and evolve over time to public reporting," the authors wrote, "and will likely continue to change their TTPs based on past precedent."