Oct 21, 2022 08:01 BST

NCC Group Monthly Threat Pulse – September 2022

- Ransomware attacks on the rise in September, with 26% increase on previous month
- Lockbit 3.0 steals a march (105 victims), followed by BlackBasta (19 victims)
- IceFire goes quiet and new threat actor, Sparta, emerges
- Industrials (28%), Consumer Cyclicals (14%), and Technology (9%) remain most targeted sectors

Analysis from NCC Group's Global Threat Intelligence team showed a marked

increase in ransomware attacks in September with 202 attacks - a 26% increase from the 160 reported in August.

The Monthly Threat Pulse also revealed further turbulence amongst threat actors, months after Conti disbanded and Lockbit rebranded. In September, Lockbit 3.0 was responsible for 52% of all attacks, a 62% increase in attacks compared to August. Its total of 105 incidents marks the largest increase in total victims for the group since January - suggesting Lockbit 3.0 is ramping up its activity.

Though dwarfed by Lockbit 3.0's victim count, BlackBasta claimed second position this month with 19 attacks.

Despite only emerging in March, IceFire was not present in September's analysis and with its leak site currently inaccessible, it is thought the group has discontinued operations or has been forced offline by law enforcement.

Claiming the fourth most active spot, just behind BlackCat was new entrant Sparta. With 12 victims reported in one day and 14 over the course of the month, the group has emerged onto the ransomware scene with an explosive start. Observations suggest it is currently solely targeting Spain-based entities, suggesting it is a Spanish-speaking organised crime group.

Sector trends remained consistent with previous months, with Industrials continuing to be the most targeted sector with 57 incidents (28%), followed by Consumer Cyclicals with 29 incidents (14%), and Technology with 19 (9%).

Taking a regional perspective, Europe claimed the spot for most attacks this month with 85 incidents (42%), with North America suffering 72 (35%), and Asia 23 attacks in total (11%).

Spotlight on China

September saw concerted efforts from China to adopt widespread cyber espionage campaigns to push nationalistic objectives forward. Security research reports, news headlines, and strategic decisions by Governments, suggest that the threat posed by Chinese APTs (Advanced Persistent Threats) is apparent and present.

In September we also released research analysing a recent incident response engagement exploiting ShadowPad malware. This malware is closely associated with Chinese threat actors, and leading researchers can assume with confidence that the malware case involved Chinese APT actors.

Much of the activity reported by researchers and news headlines has been attributed to the Chinese nation state actors, APT40 and APT41 - both groups having a highly expansive reach on capabilities and objectives. Observations show APT41 is an advanced and persistent threat group believed to be working under the instruction of the Chinese Ministry of State Security (MSS).

Matt Hull, Global Head of Threat Intelligence at NCC Group, said:

“Against a backdrop of continuous change for threat actor groups, ransomware attacks are once again on the rise. In particular, it’s clear Lockbit 3.0 is growing stronger in its operations, and it doesn’t seem likely it will disappear from the threat scene anytime soon.

“Meanwhile, the emergence of Sparta – replacing the fairly short-lived new entrant IceFire – reminds us yet again the need for close monitoring and vigilance against new groups, as we get to grips with their preferred methods of attack. With reports already showing it conducted 12 attacks in one day, it will be interesting to see how this develops over the next few months.

“Our research into the exploitation of ShadowPad malware was also revealing, as China’s cyber espionage efforts ramp up. As always, we will monitor these situations closely, to support the efforts to remain vigilant against attack.”

Keep up to date with our latest insights

Never miss a threat intelligence update - sign up to receive our monthly insights into the emerging advances in threat landscape and for our next quarterly Threat Monitor webinar here.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970