Chinese Cyber-Espionage Group Hacked Government Data Center

By Catalin Cimpanu

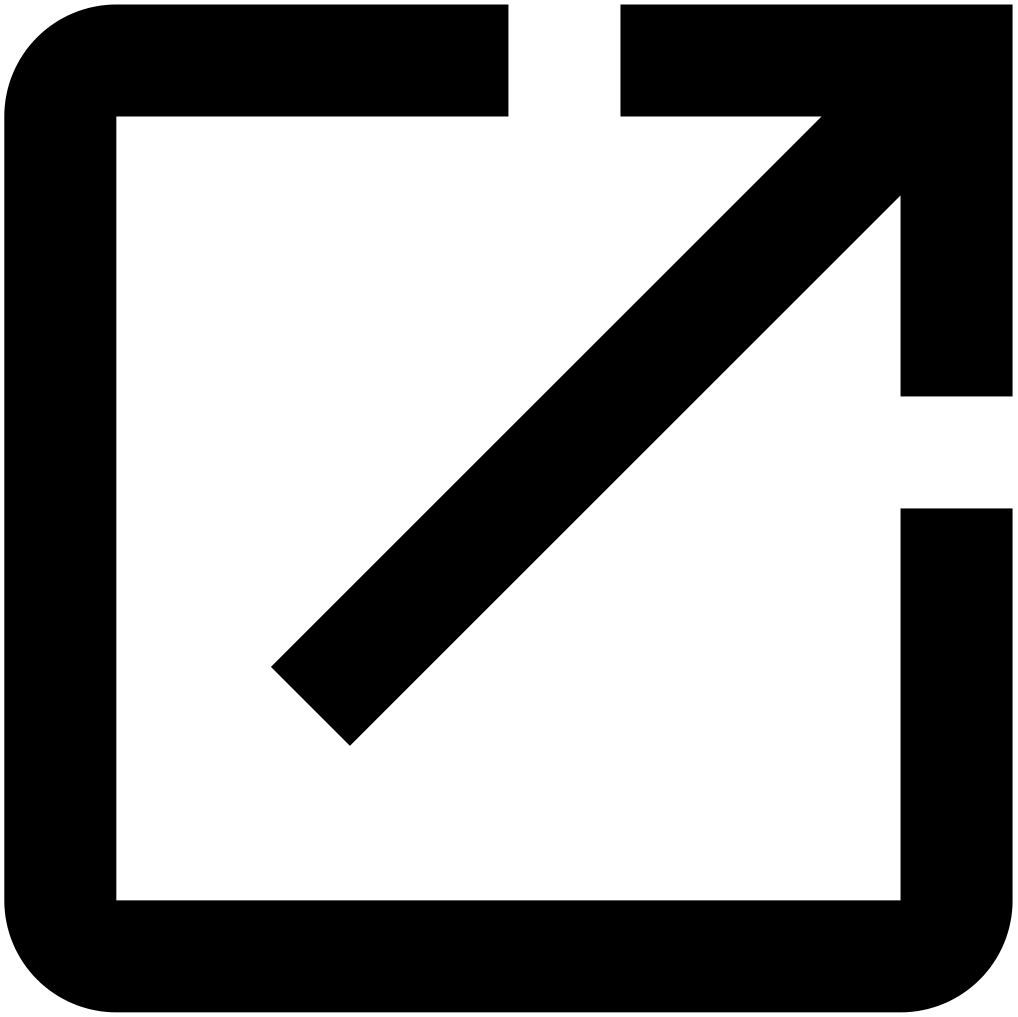
Published: 2018-06-15 · Archived: 2026-04-05 13:06:15 UTC

A Chinese-linked cyber-espionage unit has hacked a data center belonging to a Central Asian country and has embedded malicious code on government sites.

The hack of the data center happened sometime in mid-November 2017, according to a report published by Kaspersky Lab earlier this week.

Experts assigned the codename of LuckyMouse to the group behind this hack, but they later realized the attackers were an older Chinese threat actor known under various names in the reports of other cyber-security firms, such as Emissary Panda, APT27, Threat Group 3390, Bronze Union, ZipToken, and Iron Tiger [1, 2, 3, 4, 5].


DIE LINKE.
0:00



Hackers redirected visitors of government sites to malware

Kaspersky researchers say LuckyMouse used access to the data center to add JavaScript code to government sites, which redirected users to malicious sites hosting exploitation tools such as ScanBox and BEeF (Browser Exploitation Framework).

On these sites, these tools would attempt to infect users with HyperBro, a remote access trojan that operated via an "in-memory" state, leaving minimal traces on disk that could be identified by antivirus solutions.

Researchers say they found evidence of this end-user infection campaign taking place from December 2017 to January 2018.

Kaspersky didn't name the Central Asian country, but they did say LuckyMouse targeted it before in previous campaigns.

The Russian antivirus vendor also didn't say how hackers breached the data center hosting government sites, as they didn't have enough evidence to formulate a conclusion.

LuckyMouse hacked a MikroTik router to host their C&C server

Another detail that also stood out was that LuckyMouse appears to have hacked a MikroTik router to host the command and control server of the HyperBro RAT. Attackers would use this router to control and retrieve data from infected victims, putting an additional layer of anonymity between them, victims, and forensic investigators.

This is not the first time that nation-state hackers have used routers as part of their attack infrastructure, this being a very popular trend recently (let's not forget VPNFilter), but it is the first time they hosted a C&C server on one.

"The most unusual and interesting point here is the target. A national data center is a valuable source of data that can also be abused to compromise official websites," Kaspersky expert Denis Legezo explained. "Another interesting point is the Mikrotik router, which we believe was hacked specifically for the campaign."

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
