

# Microsoft Disrupts APT28 Hacking Campaign Aimed at US Midterm Elections

By Catalin Cimpanu

Published: 2018-08-21 · Archived: 2026-04-05 13:33:26 UTC

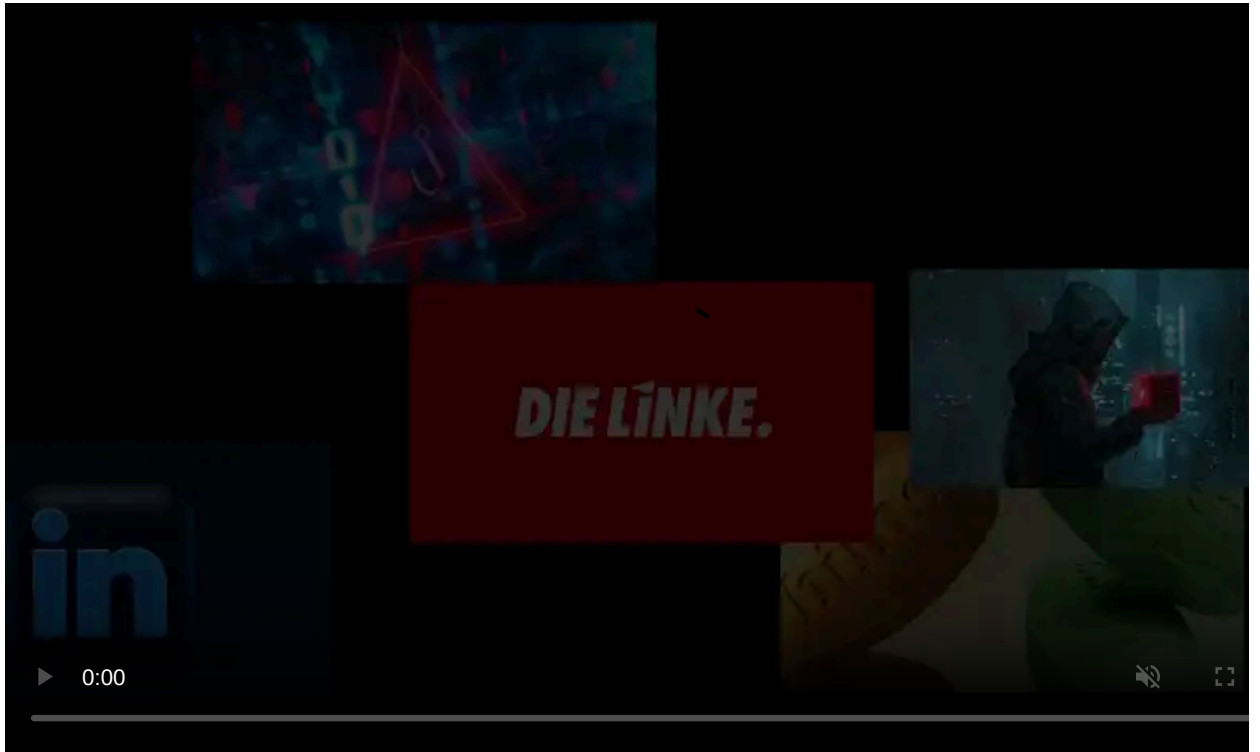


Microsoft revealed last night that it successfully disrupted a hacking campaign associated with the Russian military intelligence service GRU.

The group is known in infosec industry circles as APT28, Fancy Bear, or Strontium, and has been previously linked to cyber-espionage campaigns aimed at numerous governments around the world, including to the hack of the Democratic National Committee ahead of the 2016 US Presidential Election.

## Microsoft takes over six APT28 domains

Microsoft President Brad Smith said that Microsoft's Digital Crimes Unit (DCU) successfully executed a court order to transfer control of six internet domains created by the group. The six domains are:



Visit Advertiser website [GO TO PAGE](#)

my-iri.org  
hudsonorg-my-sharepoint.com  
senate.group  
adfs-senate.services  
adfs-senate.email  
office365-onedrive.com

The first domain was registered to look like a domain for the International Republican Institute, which promotes democratic principles. The second was registered to mimic the Hudson Institute, an organization known for its discussions on election cybersecurity. The last four were blatant attempts at mimicking domains part of the US Senate's IT infrastructure. Microsoft said it notified all three organizations.

## Microsoft has now taken over 84 APT28 domains

Based on their format, the domains were most likely supposed to be used as part of spear-phishing operations.

Microsoft says it managed to gain ownership of the domains before they were used in any attacks.

The OS maker said this was the twelfth time they used a court order to take control of domains they believed to be associated with APT28's attack infrastructure. Smith said they have now taken control of 84 APT28 domains in the last two years.

"Despite last week's steps, we are concerned by the continued activity targeting these and other sites and directed toward elected officials, politicians, political groups and think tanks across the political spectrum in the United States," Smith [said](#). "Taken together, this pattern mirrors the type of activity we saw prior to the 2016 election in the United States and the 2017 election in France."

Last week, Reuters [reported](#) that the FBI was investigating cyber-attacks on the congressional campaign of a Democratic candidate in California, albeit there's no evidence that Microsoft's intervention is tied to that investigation.

Speaking at a conference in mid-July, Tom Burt, Corporate Vice President for Customer Security and Trust, Microsoft, said Microsoft had blocked at the time [the first cyber-attacks on the US 2018 midterm elections](#).

[In May this year](#), the FBI also intervened in a similar fashion to take control of domains that the APT28 group was using to control the VPNFilter IoT botnet.

## Microsoft officially launches AccountGuard service

While announcing Microsoft's intervention to take down the six APT28 domains, Smith also [announced](#) the launch of the AccountGuard service designed to help US election and campaign entities secure their IT infrastructure against nation-state attacks.

Bleeping Computer first broke the story about Microsoft's new AccountGuard service at the start of the month —more details [here](#).

After Microsoft revealed its takeover of the six APT28 domains, Google also issued a [security advisory](#) on its blog about the dangers of government-backed phishing operations. Last week, Google added support for controlling the behavior of ["Government backed attacks" alerts inside the G Suite service](#).



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

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.

---

Source: <https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/>