Microsoft Disrupts APT28 Hacking Campaign Aimed at US Midterm Elections

bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/

Catalin Cimpanu

By
Catalin Cimpanu

- August 21, 2018
- 03:43 AM
- 4

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:

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.

Related Articles:

Microsoft takes down APT28 domains used in attacks against Ukraine

Microsoft finds severe bugs in Android apps from large mobile providers

Microsoft to force better security defaults for all Azure AD tenants

Microsoft: Windows 11 22H2 has reached RTM with build 22621

DuckDuckGo browser allows Microsoft trackers due to search agreement

- APT28
- Cyber-espionage
- Government
- Microsoft
- Senate

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

- 

  Warthog-Fan - 3 years ago

  -
  -

  Everyone blames the Russians for hacking the DNC during the 2016 presidential election. However, since the DNC never allowed any security agency to inspect their servers, there is no actual PROOF that the Russians had anything to do with the release of the Clinton and Podesta emails, and it is just as likely that the emails were leaked by a person working for the Clinton campaign.

- 

  dogood76 - 3 years ago

  -
  -

  CrowdStrike performed an analysis confirming DNC server infiltration (https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/)

- 

  herbman - 3 years ago

  -
  -

  Lisa Page testified under oath 3 weeks ago that the whole Russia narrative was completely made up , Russians were never involved in any hacking and claimed her FBI superiors made her cover up the fact that Russia was never involved.

  She also testified that her superiors purposely altered top secret documents to make sure they covered their tracks .

  Of course the main stream media never reported it and will continue to not report it.

- 

  Warthog-Fan - 3 years ago

  -
  -

  Yes. And now the MSM wants to protect us from "Fake News" by trying to suppress independent creators on YouTube, Facebook, Twitter, etc. They call everyone else "nazis" but they seem to be using the same techniques that the Nazis used to control the media and suppress dissent.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: