November 24th, 2020

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* looks at what the announcement of the United Kingdom's (U.K.) National Cyber Force means for the country, for malicious cyber actors, and possibly for international cyber norms. Next, we examine Symantec's breakdown of an enormous Chinese state-sponsored cyber campaign against Japanese-linked organizations, and we provide our thoughts on what healthcare organizations might learn from it. Finally, we recap a newly released ransomware resiliency report and highlight considerations healthcare organizations may wish to address. Welcome back to *Hacking Healthcare*.

1. The U.K. Publicly Acknowledges its National Cyber Force

Cybercriminals and nation-state actors continue to proliferate and become more sophisticated in their methods. As such, organizations are understandably concerned that the already arduous task of adequately defending themselves, especially from determined state-sponsored actors, is becoming harder instead of easier. In response, nation-state governments are increasingly under pressure to move beyond cybersecurity strategies that are rooted in response and recovery and towards being seen as publicly proactive in imposing costs on malicious actors and reducing threats. Last week, the U.K. appears to have taken a step toward normalizing this more proactive approach.

On November 19th, in a statement to the House of Commons, U.K. Prime Minister Boris Johnson publicly affirmed the existence and effective operation of the country's National Cyber Force (NCF) by stating that is "already operating in cyberspace against terrorism, organised crime and hostile state activity."[1] While reports of the NCF's formation date back some time, and it has officially been operational since April, Prime Minister Johnson's statement was its first public confirmation by the U.K government.[2] According to GCHQ, the U.K.s intelligence and security organization, the NCF is a joint partnership between GCHQ and the Ministry of Defence (MoD) and draws personnel from GCHQ, MoD, "the Secret Intelligence Service (MI6) and the Defence Science and Technology Laboratory (DSTL) under one unified command for the first time."[3]

Government officials responded to the announcement by stating that the NCF would give the "UK a world class ability to conduct cyber operations" and that it "means we are growing a potent national capability to deter our adversaries, defend our forces on operations and protect our digital homeland."[4] Others made assurances that it would be a "force for good, capable of conducting targeted, responsible cyber operations" that were "in line with UK and international law."[5] GCHQ also made sure to highlight that while they may work together, the NCF is separate from the National Cyber Security Center (NCSC), the well-known U.K. defensive agency that is more akin to the Cybersecurity and Infrastructure Security Agency (CISA) within the United States.

Action & Analysis
H-ISAC Membership Required

2. Researchers Allege Large Scale Attacks on Companies with Japanese Links

In a blog post published last week, security researchers at Symantec detailed a "long-running and sophisticated attack campaign" against organizations with Japanese links.[6] Symantec was confident enough of their evidence to ultimately attribute the attacks to the Cicada group, also known as APT10, Stone Panda, and Cloud Hopper.

This threat group, which has strong links to the Chinese government, apparently targeted numerous organizations across 17 regions and in a wide range of industries, including pharmaceuticals.[7] Symantec believes that the campaign began at least in October 2019 and continued up until October 2020. While its overall goal is unknown, Symantec estimates that the campaign is primarily an intelligence gathering operation, which would align with some operations previously attributed to the Cicada group.[8]

According to Symantec, the organizations that were targeted are "in the main, large, well-known organizations, many of which have links to Japan or Japanese companies."[9] This focus on Japan appears consistent with previous attacks attributed to the group and once again reiterates how geopolitics can be a major factor in determining targets for state-sponsored entities. In Symantec's conclusion, they warned *all* Japanese linked organizations to be wary. That's a pretty big list of potential targets.

Action & Analysis
H-ISAC Membership Required

3. Resiliency Report Sheds Light on the State of Ransomware Preparedness

As ransomware runs rampant, a new report from data management company Veritas helps put things into perspective. Released last week, the *2020 Ransomware Resiliency Report* sought to "understand [companies'] level of ransomware resiliency, how deeply they had been impacted by ransomware attacks and how much was their cloud strategy increasing their IT complexity, potentially putting them at risk."[10] To do so, Veritas' surveyed 2,690 IT professionals and executives across 21 countries from North America, Europe, Asia, Africa, and Australia.[11] All companies employed at least 1,000 individuals and no mention was made of their industry or sector.

While the 13-page report covers a lot of ground, some of the more interesting findings include:[12]

- ~65% of respondents say their company's IT infrastructure is at least half on the public cloud
- ~64% of respondents say their company at least partially struggles with getting their security measures to keep pace with the added complexity brought about by the cloud
- Only ~46% of respondents say their company's security budget has increased since COVID-19 started
- Despite the prevalence of ransomware, roughly 20% of respondents say their companies employ just one or two ransomware protection measures
- The percentage of respondent companies who experienced at least one ransomware attack was equal (~43%) regardless of whether an organization's infrastructure was mostly in the cloud or mostly on-premises
- There was an appreciable gap between how CIOs (43%) and IT Directors (%33) felt about their organization's ability to recover quickly from a ransomware incident within 5 days

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, November 24th:
- No relevant hearings

Wednesday, November 25th:
- No relevant hearings

Thursday, November 26th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Sundries –

Brazilian government recovers from "worst-ever" cyberattack
https://www.zdnet.com/article/brazilian-government-recovers-from-worst-ever-cyberattack/

November 24th, 2020

Biden Team Highlights Cybersecurity Focus With First Cabinet Picks

https://www.nextgov.com/cybersecurity/2020/11/biden-team-highlights-cybersecurity-focus-first-cabinet-picks/170274/

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.gov.uk/government/speeches/pm-statement-to-the-house-on-the-integrated-review-19-november-2020

[2] https://www.bbc.com/news/technology-55007946

[3] https://www.gchq.gov.uk/news/national-cyber-force

[4] https://www.gchq.gov.uk/news/national-cyber-force

[5] https://www.gchq.gov.uk/news/national-cyber-force

[6] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

[7] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

[8] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

[9] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

[10] https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf

[11] https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf

[12] https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf