July 20th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by providing a brief update on REvil and its apparent disappearance. Next, we break down the United States (US) government's new one-stop-shop for ransomware information and guidance. We then highlight some troubling new vulnerability disclosure regulations coming out of China and how they may impact cybersecurity. Finally, we examine the cyber risk associated with using a Managed Service Provider (MSP) and offer some advice on how to minimize it. Welcome back to *Hacking Healthcare*.

1. REvil Goes Quiet

Following weeks of increasingly stern public statements from the Biden administration warning that it may have to take matters into its own hands if Russia failed to take action against malicious cybercriminals operating within their borders, REvil, the infamous cybercriminal group claiming responsibility for the JBS and Kaseya attacks, has gone quiet. The group's blog, data leak site, and payments site are all down as of this writing.[1] The cause of the group's disappearance has not been definitively attributed.

Some have speculated that the US has taken offensive action towards Russia by finally cracking down on a group that has crossed the line. However, one of the more probable scenarios may be that REvil backed away on its own initiative to let things settle down before eventually reappearing. We will continue to monitor developments and keep you informed as the situation develops.

2. The US Government's new "One-Stop Ransomware Resource"

On July 15th, a Department of Justice (DOJ) Office of Public Affairs press release announced the creation of a "one-stop hub for ransomware resources for individuals, businesses and other organizations."[2] The website (https://www.cisa.gov/stopransomware or StopRansomware.gov) is the product of a collaborative effort between DOJ, the U.S. Department of Homeland Security (DHS), and other federal partners and comes as the Biden administration struggles to find ways to mitigate the damage of ransomware attacks on the public and private sector.

The website itself contains numerous sections, including:

- **Fact Sheets & Information**, with a specific section on healthcare
- **Ransomware 101**, with basic information and links to more in-depth analysis

- **Ransomware Guide**, with links to the Cybersecurity and Infrastructure Security Agency's (CISA) guides
- **Services**, with links for State, Local, Tribal, and Territorial organizations and others
- **Training**, with information for technical and non-technical audiences
- **Webinars**, with links to numerous ransomware topics
- **Bad Practices**, with an explanation of CISA's new initiative to highlight truly egregious practices
- **Campaigns**, with a link to CISA's "Reduce the Risk of Ransomware" initiative
- **Sector Risk Management Agencies**, with links to the sector-specific lead agency for each critical infrastructure sector

In addition creating this resource, is has been reported that the State Department will begin to offer rewards up to $10 million for "information leading to the identification of anyone engaged in foreign state-sanctioned malicious cyber activity, including ransomware attacks, against critical U.S. infrastructure."[3] Funding for these payouts will reportedly come from the State Department's "Rewards for Justice" program and will allegedly "offer a tips-reporting mechanism on the dark web to protect sources who might identify cyber attackers and/or their locations."[4]

This collection of ransomware information doesn't break much new ground, but the consolidation of what has been disparate agency guidance into a single place will certainly help bring speed and efficiency to those looking for guidance and aide. Having a more centralized mechanism to distribute information will also hopefully help bring continuity to government outreach efforts and encourage agencies to ensure that guidance and alerts don't conflict with one another.

It is also encouraging to see the State Department effectively incentivize the provision of information leading to the identification of "foreign state-sanctioned malicious cyber activity" against critical infrastructure. However, it remains to be seen how effective this strategy may end up being, as clearly identifying an individual's involvement while also definitively attributing it to a state-sanctioned cyber effort is no small feat. These steps by themselves are unlikely to radically alter the current threat landscape, but it is encouraging that the Biden administration is making serious efforts to improve the situation.

3. New Concerning Chinese Vulnerability Disclosure Regulations

The Chinese government has announced a new set of vulnerability regulations that will have a significant immediate impact on organizations operating within China, security researchers, and software vendors. Critics are already noting serious concerns with the approach and have highlighted the potential long-term impacts to security research.

Based on reports that began to circulate last week, the new Chinese regulations appear to threaten penalties for researchers and organizations that fail to comply with numerous new restrictions and requirements surrounding vulnerability disclosure.

Recorded Future has helpfully summarized some of the more important articles of the new *Regulations on the Management of Security Vulnerabilities in Network Products* that was published by the Cyberspace Administration of China:[5]

- **Article 4:** Makes it illegal for individuals or organizations to "collect, sell, or publish information on network product security vulnerabilities."
- **Article 5:** Mandates that any organizations or network operators must set up to receive vulnerability reports and keep logs for at least six months.
- **Article 7, (2):** All vulnerability reports must be reported to the Ministry of Industry and Information Technology (MIIT) within two days.
- **Article 7, (3):** Encourages network operators and product vendors to set up a reward mechanism for reported vulnerabilities.
- **Article 9, (1):** Prohibits security researchers from disclosing bug details before a vendor had a reasonable chance to patch. Exceptions to go public can be negotiated with MIIT's approval.
- **Article 9, (3):** Prohibits researchers from exaggerating risks associated with security flaws or using a vulnerability to extort vendors.
- **Article 9, (4):** Prohibits the publication of programs and tools to exploit vulnerabilities and put networks at risk.
- **Article 9, (7):** Prohibits disclosing vulnerability details to "overseas organizations or individuals other than network product providers."
- **Article 10:** Mandates that all network operators and product vendors to register their vulnerability reporting platforms with the MIIT.

Organizations will not have long to assess this new development, as these regulations are slated to go into effect beginning on September 1, 2021.[6]

Action & Analysis
Included with H-ISAC Membership

4. Kaseya Highlights Managed Service Provider Cybersecurity Considerations

Managed Service Providers (MSPs) are often a sensible and economical alternative to handling numerous day-to-day IT tasks in-house. This is especially true for small and medium sized businesses who lack resources or the expertise to confidently manage vital IT infrastructure and systems. However, as the cyberattack against Kaseya highlights, relying on an MSP carries its own set of risks.

On July 2nd, Kaseya announced a potential attack against its Virtual Systems Administrator (VSA) software that was soon confirmed to be compromised.[7] For those unfamiliar, VSA is used by an organization to help remotely manage and monitor systems that are part of their own or a client's infrastructure. Kaseya's VSA was in use by dozens of MSPs and by compromising it, malicious actors were able to compromise 50-60 MSPs and then further compromise many of those MSPs' clients .[8, 9] This cascading effect has negatively impacted an estimated 1,500 organizations, many of which were affected due to their MSP being compromised. This should all sound unfortunately familiar given the recent attack against SolarWinds and its customers, which followed a similar pattern and had a similar outcome.

Attacks that directly or indirectly target MSPs are not new or exceptionally rare. A 2020 report produced by Perch Security found that 73% of MSPs reported at least one security incident in the past 12 months.[10] With the possibility that a single MSP compromise could open the door to tens, hundreds, or many thousands of their clients, the incentive to attack MSPs is obvious. For those organizations using or thinking of using an MSP, it is important to consider the kinds of risks associated with them.

Action & Analysis
Included with H-ISAC Membership

Congress –

Tuesday, July 20th:
- House of Representatives - Permanent Select Committee on Intelligence: STAR Subcommittee Hearing - Microelectronics: Levers for Promoting Security and Innovation

- House of Representatives - Committee on Energy and Commerce: Hearing: "Stopping Digital Thieves: The Growing Threat of Ransomware"

Wednesday, July 21st:
- Senate – Committee on the Environment and Public Works: Hearings to examine cybersecurity vulnerabilities facing our nation's physical infrastructure.

Thursday, July 22nd:
- No relevant meetings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

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

[1] https://fortune.com/2021/07/13/revil-ransomware-offline-dark-web/
[2] https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov
[3] https://apnews.com/article/technology-joe-biden-europe-business-government-and-politics-cd21d84b5fd070421f871610b40e91d0
[4] https://apnews.com/article/technology-joe-biden-europe-business-government-and-politics-cd21d84b5fd070421f871610b40e91d0

[5] https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/
[6] https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/
[7] https://www.kaseya.com/potential-attack-on-kaseya-vsa/
[8] https://www.kaseya.com/company/
[9] https://www.welivesecurity.com/2021/07/13/msp-kaseya-incident-third-party-cyber-risk/
[10] https://www.msspalert.com/cybersecurity-research/perch-threat-report-msps-report-security-incidents/