H-ISAC™
HEALTH - ISAC

THREAT BULLETINS

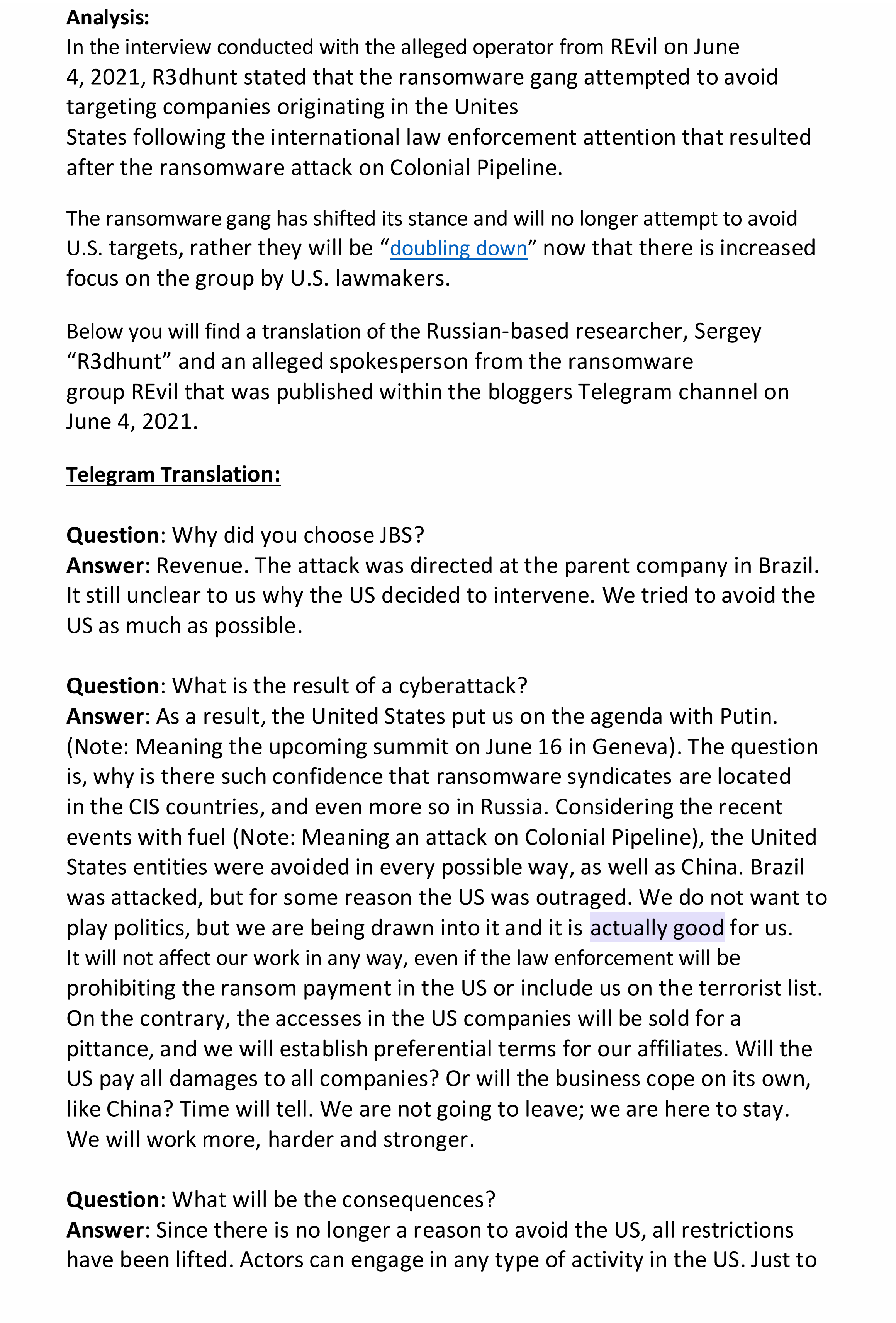
Alleged REvil Ransomware Operator Says All U.S. Entities Can Now Be Targeted

○○○ TLP:WHITE

Jun 07, 2021

On June 4, 2021, multiple intelligence sources reported on an interview that took place with a Russian-based researcher, Sergey “R3dhunt” and an alleged spokesperson from the ransomware group REvil. Sergey “R3dhunt” operates under the Twitter handle Russian OSINT and maintains a presence on YouTube under the same handle.
It has been assessed with medium to high confidence that the interview conducted is legitimate.

Critical infrastructure sectors, including healthcare, may see increased ransomware attacks due to threat actors eliminating any ban on target types.



Analysis:

In the interview conducted with the alleged operator from REvil on June 4, 2021, R3dhunt stated that the ransomware gang attempted to avoid targeting companies originating in the Unites States following the international law enforcement attention that resulted after the ransomware attack on Colonial Pipeline.

The ransomware gang has shifted its stance and will no longer attempt to avoid U.S. targets, rather they will be "doubling down" now that there is increased focus on the group by U.S. lawmakers.

Below you will find a translation of the Russian-based researcher, Sergey "R3dhunt" and an alleged spokesperson from the ransomware group REvil that was published within the bloggers Telegram channel on June 4, 2021.

Telegram Translation:

Question: Why did you choose JBS?
Answer: Revenue. The attack was directed at the parent company in Brazil. It still unclear to us why the US decided to intervene. We tried to avoid the US as much as possible.

Question: What is the result of a cyberattack?
Answer: As a result, the United States put us on the agenda with Putin. (Note: Meaning the upcoming summit on June 16 in Geneva). The question is, why is there such confidence that ransomware syndicates are located in the CIS countries, and even more so in Russia. Considering the recent events with fuel (Note: Meaning an attack on Colonial Pipeline), the United States entities were avoided in every possible way, as well as China. Brazil was attacked, but for some reason the US was outraged. We do not want to play politics, but we are being drawn into it and it is actually good for us. It will not affect our work in any way, even if the law enforcement will be prohibiting the ransom payment in the US or include us on the terrorist list. On the contrary, the accesses in the US companies will be sold for a pittance, and we will establish preferential terms for our affiliates. Will the US pay all damages to all companies? Or will the business cope on its own, like China? Time will tell. We are not going to leave; we are here to stay. We will work more, harder and stronger.

Question: What will be the consequences?
Answer: Since there is no longer a reason to avoid the US, all restrictions have been lifted. Actors can engage in any type of activity in the US. Just to

mention, our servers have not been disconnected and funds from the adverts' wallets have not flowed away. We send a subtle hello.

Question: How are you going to work in the light of the recent ban of all ransomware activity on DarkWeb forums?
Answer: We are setting our own rules and laws now. Forums are no longer interested in us, and so are we in them. We don't have problems with new hires and we have about 8 candidates for 1 position.

Question: Can I publish your answers for the Media on my channel with your approval?
Answer: Yes, you can.

Reference(s)	Twitter, Youtube, Twitter, NPR, Linkedin, CISA, Softpedia, Threat Post, Intel471, Cyberreadinessinstitute

Recommendations

Ransomware Mitigations:

The most effective mitigations for ransomware and other malware will include a defense in-depth approach that makes it more difficult to successfully deploy malware and reduce the impact or spread of a successful infection. We therefore recommend that long term, Health-ISAC member organizations should seek to:

- Backup your data, system images, and configurations, regularly test them, and keep the backups offline.
- Provide social engineering and phishing training to employees. Most incidents originate from successful phishing campaigns.
- Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.
- Ensure emails originating from outside the organization are automatically marked before received.
- Apply applicable patches and updates immediately after testing; Develop and maintain patching program if necessary.
- Implement Intrusion Detection System (IDS).
- Implement spam filters at the email gateways.
- Block suspicious IP addresses at the firewall.

- Implement whitelisting technology on appropriate assets to ensure that only authorized software is allowed to execute.
- Implement access control based on the principal of least privilege.
- Implement and maintain anti-malware solution.
- Conduct system hardening to ensure proper configurations.
- Disable the use of Remote Desktop Protocol (RDP) or, if absolutely needed, restrict its use applying the principle of least privilege and monitor/log its usage.

Additional ransomware resources and guidance is available at the DHS CISA website here.

Please review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication for additional best practices available here.

For small and medium sized businesses, the Cyber Readiness Institute Ransomware Playbook provides help on how to prepare for, respond to, and recover from a ransomware attack. The playbook is here.

Sources

Intel 471 - Alleged REvil member says gang has no fear over U.S. government's major ransomware focus

Threatpost - REvil Ransomware Gang Spill Details on US Attacks

Softpedia - REvil is Not Afraid of the US Ransomware Focus

CISA - RANSOMWARE GUIDANCE AND RESOURCES

Cyber Readiness Institute - Ransomware Playbook

Twitter - Russian OSINT

Youtube - Russian OSINT

Telegram - Russian OSINT

LinkedIn - Telegram Translation

NPR - REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says

Alert ID 303e5d72

View Alert

Tags Russian OSINT, REvil

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**