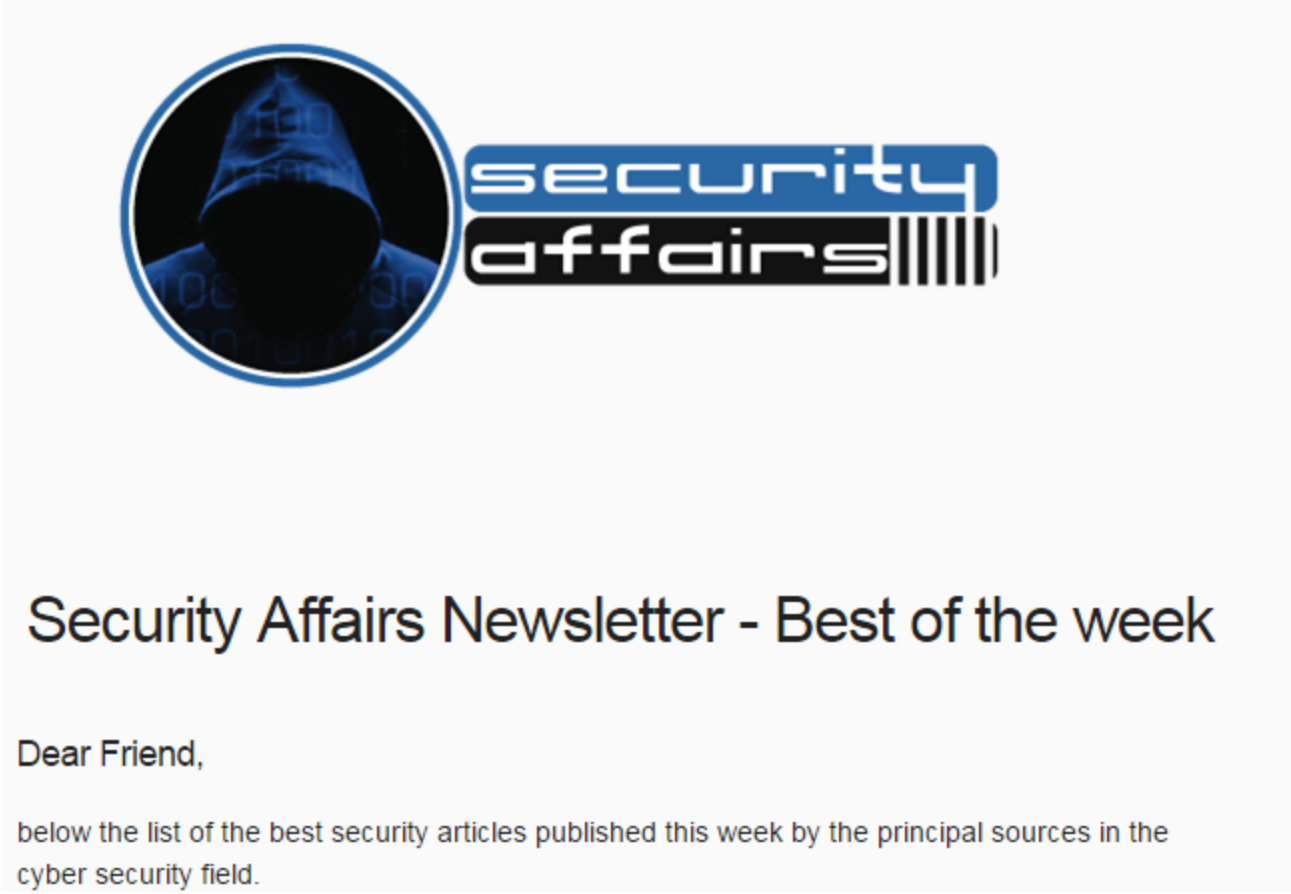
‘Ransomed.vc’ in the Spotlight – What is Known About the Ransomware Group Targeting Sony and NTT Docomo

securityaffairs.com/151550/data-breach/ransomed-vc-sony-ntt-alleged-attacks.html

September 27, 2023



Pierluigi Paganini September 27, 2023

Following the recently announced data leak from Sony, Ransomed.vc group claimed the hack of the Japanese giant NTT Docomo.

Following the recently announced **data leak from Sony**, the notorious ransomware syndicate Ransomed.vc announced a new victim today in face of the largest Japanese telecommunication giant NTT Docomo. Notably, the announcement came almost synchronously with the publication of the new leaked data from Sony shedding some light on the precursor of the data breach. The bad actors are asking for $1,015,000 to be paid by the largest NTT Docomo. After Sony rejected to pay ransom demands, the bad actors leaked the exfiltrated data.

Resecurity, a global cybersecurity company protecting major Fortune 500 companies and government agencies, detailed Ransomed.vc in their recent threat intelligence report. According to cybersecurity experts, Ransomed.vc, is the syndicate emerged from an underground forum and later became one of the most rapidly developing groups for today in the Dark Web threatening large enterprises from the U.S., the U.K and European Union (EU). Notably, the actors chose a creative motto of being “online agency that is looking forward to put sanctions on the less that dared not to pay”. They used GDPR laws and data protection regulations to extort affected companies in EU – if companies do not pay up, they make the stolen information public, which will lead to a regulatory fine, in some cases exceeding the ransom payment in times.

Ransomed.vc released a 2.4 GB dump with leaked data from Sony containing source codes from SVN repository along with credentials and a private SSH key presumably belonging to one of the software engineers.

Resecurity uncovered interesting connections to independent hacktivist groups which later united in alliances like “Five Families”, a coalition of several groups (STORMOUS, GhostSec, SigedSec, ThreatSec) previously responsible for large-scale cybersecurity incidents. Collectively, their activities range from attacks on various governments to the publication of sensitive data from enterprises. For example, one of them, SiegedSec was previously responsible for the publication of stolen data from NATO COI. These findings have been also confirmed in the analysis by Karol Paciorek released by CSIRT KNF responsible for cybersecurity of the Polish financial sector. It is possible the actors behind the attack originate from several competing hacktivist groups which later transformed into ransomware operators.

The research follows a recent report by the Department of Homeland Security (DHS). According to the new Department of Homeland Security 2024 Homeland Threat Assessment between January 2020 and December 2022, the number of known ransomware attacks in the United States increased by 47 percent. Ransomware attackers extorted at least $449.1 million globally during the first half of 2023 and are expected to have their second most profitable year. This is due to the return of “big game hunting”—the targeting of large organizations—as well as cyber criminals’ continued attacks against smaller organizations. Ransomware actors continue to target a variety of victims, almost certainly reflecting malicious cyber actors’ target refinement to entities perceived as the most vulnerable or likely to pay a ransom. In addition to disrupting the activities of targeted victims, financially motivated criminal cyber actors will likely impose significant financial costs on the global economy in the coming year.

Pierluigi Paganini

(SecurityAffairs – hacking, Sony)

you might also like

leave a comment