MITRE-ID: G0071

Name: Orangeworm

Country: Unknown

Description:

Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage. Reverse engineering of Kwampirs, directly associated with Orangeworm activity, indicates significant functional and development overlaps with Shamoon.

TTPs:

1. The APT targeted special groups, especially in the Healthcare industry.
2. The Malware named Kwampairs was detected on medical devices like X-Rayand MRI machines.
3. The APT also targeted including Manufacturing, IT, Agriculture...etc. domain and those victims were medical service related.
4. When the APT infected targets, a backdoor Trojan. Kwampirs was deployed to provide remote access services to attackers.
5. Kwampirs could generate random string in the decrypted payload to avoid being detected.
6. When the attacker detected high valued victims, they would create file shares like admin$, E$Windows to steal data.
7. While the APT is active for a few years, security professionals do not think it is State-Sponsored actor and believe it is more likely an individual or small group

Reference:

https://symantec-enterprise-blogs.security.com/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia