Increased Activity from 8Base Ransomware Group

8Base is a ransomware group which has been known since March 2022, but has been especially active during June 2023. Based on a report from **VMware**, 8Base utilizes encryption and "name and shame" techniques to demand payment from their victims. Describing themselves as pen testers, they use similar verbiage as another known ransomware group, "RansomHouse", leading VMware to believe they are not a new group. The financial industry is one of their main targets and they have been in the top two performing ransom groups within the past 30 days.

It looks as though they use Phobos Ransomware version 2.9.1 loaded with SmokeLoader and that the encrypted files are appended with the extension ".8base". Analysis conducted by VMware found that the ransom notes and leak sites of RansomHouse and 8Base were nearly identical in the used verbiage. The major differences between the two at this point are that RansomHouse advertises its partnerships, while 8Base does not, and the layout of their leak pages. You can find indicators of compromise for 8Base in the VMware report.

Cyberattack on European Investment Bank

Several weeks ago, the European Investment Bank (EIB) was **victim to a cyberattack** where malicious actors successfully infiltrated the EIB's systems. The attack coincide with threats from Russian hackers indicating their intentions to negatively affect the Western financial markets. Through a social media post, the EIB **confirmed** the ongoing cyberattack announcing that their websites have been experiencing issue making them inaccessible. This cyberattack on EIB occurred shortly after Russian-speaking hackers issued warnings on their intent to target Western financial institutions with support for Ukraine.

New Malicious Tool Named PindOS Deploys Malware

Security researchers have discovered a new malicious JavaScript tool dubbed **PindOS** designed to deliver the **Bumblebee** and IcedID malware which is used for ransomware attacks. Researchers describe the PindOS as a simple JavaScript malware dropper that appears to be built specifically to fetch the next-stage payloads that deliver the final payload for the attackers. Researchers say that the JavaScript has only one function that comes with four parameters for downloading either Bumblebee trojan or the IcedID banking trojan. Its configuration included the option to define a user agent to download the DLL payload, two URLs where the payload is stored and the RunDLL parameter for the payload DLL function to be called. Researchers state when executed, the JavaScript will attempt to download the payload initially from the URL in its configuration and execute it by calling on the specified export directly using the rundll32.exe executable file. Researchers are unclear if the threat actors are just testing how PindOS fares against security products or if they plan to include it in their toolkit.

Javascript Public Registry At-Risk for Supply Chain Attacks

A former staff engineering manager at the npm Command Line Interface, which hosts a database of JavaScript packages called the Public Registry, posted a **blog** warning of a potential risk that could make the software supply chain vulnerable. Darcy Clarke indicated that there is an opportunity for the installation and execution of malicious files due to the failure of the Public Registry to compare the npm package manifest data with the archive of files that data describes. The issue stems from the way the JavaScript packages are submitted to the database. The manifest data (aka 'metadata') is not submitted with the tarball file, which is a compressed archive of files meant to contain a mirror of the manifest data in package.json. There is no validation conducted which creates risk for cache poisoning, installation of unanticipated dependencies, execution of unanticipated scripts, and version downgrade attacks. The npm Public Registry is used by more than 17 million developers and hosts more than three million packages. It served over 215 billion downloads in May 2023.