ALPHV/BlackCat Ransomware

Date: 19th February 2024 | Severity: High

Summary

The ALPHV/Blackcat ransomware gang has claimed responsibility for the recent network breaches of Fortune 500 company Prudential Financial and mortgage lender loanDepot. The two companies were added to ALPHV's dark web leak site.

Attack Vectors

ALPHV surfaced in November 2021 and is believed to be a rebrand of the DarkSide and BlackMatter ransomware operations. The group gained worldwide notoriety after the Colonial Pipeline attack, which led to extensive investigations by law enforcement agencies worldwide and the operation going through two rebrands.

LoanDepot revealed in January 2024 that at least 16.6 million people had their personal information stolen in the ransomware attack they confirmed on January 8, 2024 two days after disclosing it as a "cyber incident" on January 6 2024.

On Tuesday, Prudential Financial also revealed that a suspected cybercrime group breached its network on February 4, 2024, and stole employee and contractor data.

The FBI disrupted the gang's operation in December and temporarily took down its Tor negotiation and leak sites after breaching its servers' months earlier and creating a decryption tool. ALPHV has since "unseized" their data leak site with the help of private keys they still owned and has now launched a new Tor leak site the FBI has yet to take down.

Indicator of Compromise

Chrome for Linux and macOS: Chrome 116.0.5845.110

IOCs of ALPHV-BlackCat Ran

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes. Block all IOCs at controls. Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

https://www.bleepingcomputer.com/news/security/alphv-ransomware-claims-loandepot-prudential-financial-