Mphasis
The Next Applied

HelloKitty Ransomware

Date: 21st April 2024 | Severity: High

Summary

The HelloKitty ransomware family emerged in late 2020, operating out of Ukraine. The ransomware family gained attention via the attack against CD Projekt Red. The name is derived from the “HelloKittyMutex” created upon execution of the threat.

HelloKitty is known for being nimble and rapidly adopting new TTPs. Later variants of HelloKitty used a Golang-based packer to improve detection evasion. In early 2021, a Linux variation of HelloKitty was observed in the wild.

Attack Vectors

- HelloKitty is deployed in multiple ways: via Cobalt Strike or a similar framework, and through email phishing. HelloKitty ransomware has also been deployed as a later-stage payload in previously infected environments (example: Qakbot, IcedID)
- Once launched, HelloKitty will try to disable and terminate several processes and services to reduce interference with the encryption process. This includes processes and services associated with IIS, MSSQL, QuickBooks, SharePoint, and more.
- These actions are carried out via taskkill.exe and net.exe. If HelloKitty is unable to stop any specific processes or services, it will engage the Windows Restart Manager API (Application Programming Interface) to further assist in termination.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• h39ea2394a6e6c39c5d7722dc996daf05 • 6d321248c816c61a973c9195af30b25b • 06ce6cd8bde756265f95fcf4eecadbe9 • 85cd7c6931b44a14f4899dfd0039e8b4 • 8e4a887acab5f9475c5fa9a26fb9e720

	• 02a08b994265901a649f1bcf6772bc06df2eb51eb09906af9fd0f4a8103e9851 • 38d9a71dc7b3c257e4bd0a536067ff91a500a49ece7036f9594b042dd0409339 • 56978ab3cb8172239da8742ebe41ef099bb9e1b58e23956a82bf495d7cc94c00 • 613f9fb99d927e02ba4d7b7122df577fe775e2e56d7ddce5636fd810fc1392ad • fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb • ca010ca1e7d5104049c09eefca128cc0e50729e1 • 4501fdf303206d0692f6d717dd2f1deb16a1ccab • bacf50b20f1cf2165ac96535aeac36b49c8a8677 • 3294a12a583d2634f6e3d1232052dfe0cd51a44a • 5822f65dec879ba585112976a632b2c4435abf90
Domain	• http[:]//172.245.16[.]125/m2[.]png • http[:]//172.245.16[.]125/m4[.]png

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR (Endpoint Detection & Response) solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing 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.sentinelone.com/anthology/hello-kitty/
- https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-rebrands-releases-cd-projekt-and-cisco-data/