SECURITY ADVISORY

CYBER STASH

November, 2023

BiBi Wiper Malware

Context

In a recent surge of cyber threats, Israeli organisations are increasingly facing data-wiping attacks perpetrated by variants of the BiBi malware family. Researchers have identified these destructive elements affecting both Linux and Windows systems. The attacks are part of a broader cyber offensive targeting various sectors in Israel.

Security Joes' Incident Response team exposed 'BiBi-Linux' on October 30th, a malware strain explicitly crafted to cause irreversible data corruption and operational chaos. This discovery was followed on October 31st by ESET researchers who confirming the presence of a Windows variant.

CyberStash foresees the malware's strategic targeting directed at nations, media conglomerates, and diplomatic circles aligned with Israel, representing an imminent and far-reaching threat extending beyond the geographical bounds of Israel.

Mitigation

Defending against the BiBi Wiper Malware involves more than just backing up important data. It requires a comprehensive strategy that includes:

Adversary Behavior Detection: Monitor for unusual behavior patterns to detect adversary attacks early, gaining insights into their tactics. This includes the detection of related IOCs on endpoints.

Forensic Depth Analysis: Conduct static and dynamic analysis of operating system artifacts with a focus on detecting post-breach compromises, allowing for timely response and mitigation of security incidents.

Application Control Policies: Enforce stringent application control or whitelisting policies to prevent unauthorised system modifications, ensuring that only trusted and validated applications can access and alter critical system components.

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

Technical Details

BiBi Wiper perpetuates an infinite loop of data destruction, systematically overwriting files in the target directories with random bytes. The continuous execution renders the files unrecoverable, showcasing a destructive impact on the compromised system. The malware contained the commonly used nickname 'Bibi,' associated with the Israeli Prime Minister, Benjamin Netanyahu, hardcoded within it and in the extension of every compromised file. Bibi Wiper stands out from typical ransomware as it doesn't encrypt files; instead, it corrupts them by overwriting with useless data, causing harm to both the data and the operating system.

On Linux, the payload labelled as bibi-linux.out, enables attackers to selectively encrypt folders using command-line parameters. On Windows, when the malware runs without any specified arguments, it initiates a sequence to identify target directories for destruction. It first checks if there are any specified arguments denoting the directory to be destroyed, like this: `bibi.exe <directory_to_destroy>`. If no such argument is provided, it follows these steps:

1. Reads the default path: "C:\Users".

2. Retrieves the available disk drives using the GetLogicalDrives() function, which returns a bitmask representing the drives.

3. It iterates through the A-Z drives (26 in total) by using a bitmask to identify accessible drives on the system. Each drive name is formed by appending ":\\" to the drive letter.

4. It excludes the C drive (identified by the bitmask position 2) from consideration.

5. For the remaining available drives (excluding the C drive), it uses GetDriveTypeA() to determine their drive types. BiBi-Windows Wiper specifically targets DRIVE_FIXED, DRIVE_REMOVABLE and DRIVE_RAMDISK types.

The full technical analysis of the Windows sample can be found on knight0x07's GitHub page :

- https://github.com/knight0x07/BiBi-Windows-Wiper-Analysis

Tactics, Techniques and Procedures

The notable TTPs related to the BiBi-Windows Wiper malware are:

T1059: Execution - Command-Line Interface

The BiBi-Windows Wiper checks for command-line arguments, specifically the directory to be destroyed, using the syntax bibi.exe <target_directory>.

T1082: Discovery - System Information Discovery

The wiper fetches information about available disk drives and their types using functions like GetLogicalDrives() and GetDriveTypeA().

T1490: Inhibit System Recovery

Wiper deletes shadow copies from the system, preventing the user from recovering their files. It also disables Windows Recovery Environment (WinRE) repair/recovery options of an infected system using BCDEdir.

T1486: Impact - Data Encrypted for Impact

The BiBi-Windows Wiper employs a Mersenne Twister algorithm to generate random numbers, which are then used to overwrite data in target files, destroying their contents irreversibly.

Cyber Threat Intelligence

It is more than likely that the malware was developed by an APT group sponsored by Iran. The discovery of the Windows variant validates the persistence of the threat actors behind the wiper, showcasing their ongoing development of the malware. This expansion signifies an intent to broaden the attack scope, extending towards end-user machines and application servers.

CyberStash predicts that these pro-Hamas groups might target countries supporting Israel financially and politically. Pro-Israeli media outlets and Individuals who serve as diplomats, representing their respective countries in foreign relations, are also likely targets.

References

Related IOC's & Yara Rules:

- https://otx.alienvault.com/pulse/6541122c0c8464fa2b4921e4

Related Windows Command Lines:

- cmd.exe /c bcdedit /set {default} recoveryenabled no - Disables Windows Recovery Environment
- cmd.exe / c bcdedit / set {default} bootstatuspolicy ignoreallfailures - Force the system to boot normally rather than into the Windows Recovery Environment
- cmd.exe /c wmic shadowcopy delete - Delete Volume Shadow Copies using WMIC
- cmd.exe /c vssadmin delete shadows /quIet /all - Delete Volume Shadow Copies using VssAdmin

Public Intelligence:

- https://github.com/knight0x07/BiBi-Windows-Wiper-Analysis/tree/main
- https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group
- https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows