

BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows

 blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows



Summary

On Oct. 30, Israeli-based incident response company SecurityJoes posted findings about a new wiper malware for Linux systems used by pro-Hamas hackers in the Israel-Hamas war. The company is currently tracking the malware as the BiBi-Linux Wiper.

The next day, the BlackBerry Research and Intelligence Team found a variant that targets Windows systems, which we’ve labeled the **BiBi-Windows Wiper**.

Context

Following the Hamas terrorist attack on Israel on Oct. 7, the physical war between Hamas and Israel has broken through into the cyber realm. A suspected Hamas-affiliated hacker group broke into Israeli companies across the nation, compromising Internet-facing hosts to access their networks, and deployed a new and highly specific cyberweapon in an apparent attempt to damage the companies’ infrastructure. The new malware, BiBi-Linux Wiper, was uncovered by an IR (incident response) team providing assistance for the Israeli companies.

The attack had no ransom note or command-and-control (C2) servers, which led responders to surmise that the BiBi-Linux malware is a wiper, deployed for the sole reason of causing data destruction. Upon analysis, the team discovered that the Israeli Prime Minister’s commonly-used nickname, **Bibi** (aka Benjamin Netanyahu), was hardcoded in the malware and in the extension of every destroyed file.

SecurityJoes’ team theorizes that the wiper may have been created “by a group of hackers affiliated with Hamas, with the intent to sow chaos amidst the backdrop of war.”

The Windows variant detected by BlackBerry confirms that the threat actors who created the wiper are continuing to build out the malware, and indicates an expansion of the attack to target end user machines and application servers. By diversifying their target systems, the attackers will very likely ensnare additional machines that run on Windows — an operating system that at the time of writing currently accounts for 68% of total desktop users worldwide, versus a mere 2.9% who use Linux.

Technical Analysis of the BiBi-Windows Wiper

MD5	e26bba0304f14ef96beb60376791d32c
SHA256	40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17
File Name	bibi.exe
File Size	203.00 KB (207872 bytes)

File Type	Win PE x64
Compiler	Visual Studio (2019)

The timestamp on the BiBi-Windows Wiper suggests the implant was compiled on Saturday, Oct. 21, 2023, just 14 days after Hamas' initial terror attack on Israel. The malware sample is a x64 Windows portable executable (PE) compiled using Visual Studio 2019, with a file size of 203KB.

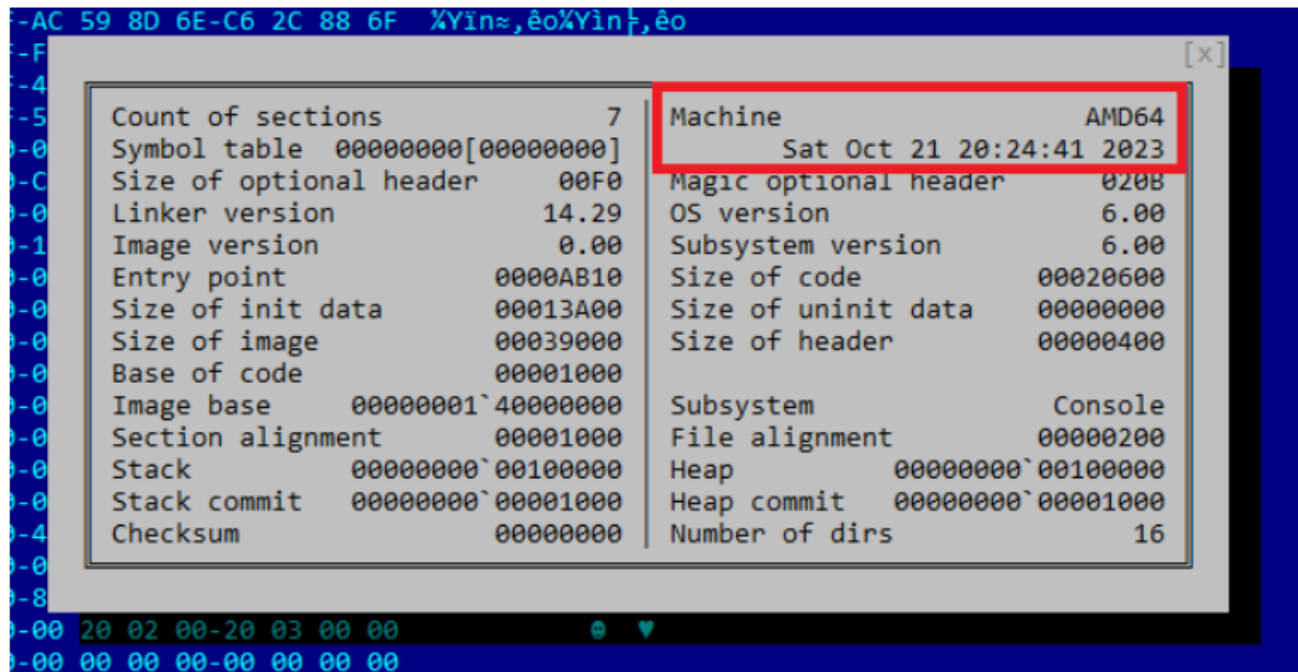


Figure 1: BiBi-Windows Wiper's timestamp

While the infection vector is currently unknown, once the implant is executed, it checks the processor architecture and the number of threads in the intended victim's system. For the fastest possible destruction action, the malware runs 12 threads with eight processor cores. During execution, the wiper outputs the result to the console.

```
14002c0fd          00 00 00          ...
14002c100 char const data_14002c100[0x9] = "C:\\Users", 0
14002c109          00 00 00          ...
14002c10c data_14002c10c:
14002c10c          3a 5c 00 00          :\\..
14002c110 char const data_14002c110[0xe] = "[+] Path: %s\\n", 0
14002c11e          00 00          ..
14002c120 char const data_14002c120[0x20] = "[+] CPU cores: %d, Threads: %d\\n", 0
14002c140 char const data_14002c140[0x1a] = "send attempt while closed", 0

[+] Path: C:\\Users
[+] Path: F:\\
[+] CPU cores: 8, Threads: 12
[+] Round 0
[+] Stats: 3 | 0
[+] Round 1
[+] Stats: 4 | 0
[+] Round 2
[+] Round 3
[+] Round 4
[+] Round 5
[+] Round 6
[+] Round 7
[+] Round 8
[+] Round 9
[+] Round 10
[+] Round 11
[+] Round 12
```

Figure 2: BiBi's console output

The sample destroys all files except those with .exe, .dll, and .sys extensions, because those types of files are essential for the computer to operate. Those extensions are hardcoded in the code for skipping, so that the malware can run its course of destruction.

The wiping process is performed so the targeted files are filled out with random bytes, essentially rendering the file unusable—and unrecoverable. Then, the files are renamed to a random sequence of letters that consists of 10 characters, and the extension **BiBi1** from 1 to 5 is added. A typical filename would follow the structure: **[Filename].BiBi[number]**.

The implant also deletes shadow copies from the system, preventing the user from recovering their files, unless they have an offline backup handy. Shadow Copy is a technology included in Windows that creates backup copies or snapshots of computer files or volumes, even when they are in use.

```
cmd.exe /c vssadmin delete shadows /quiet /all
cmd.exe /c wmic shadowcopy delete
```

It also disables the system's trigger to call the Error Recovery screen on startup.

```
cmd.exe / c bcdedit / set {default} bootstatuspolicy ignoreallfailures
```

Finally, it turns off the Windows Recovery feature so the system may not be recovered.

```
cmd.exe /c bcdedit /set {default} recoveryenabled no
```

All CMD commands in the code are stored with a right-to-left technique to bypass simple pattern detection rules typically used by legacy antivirus products.

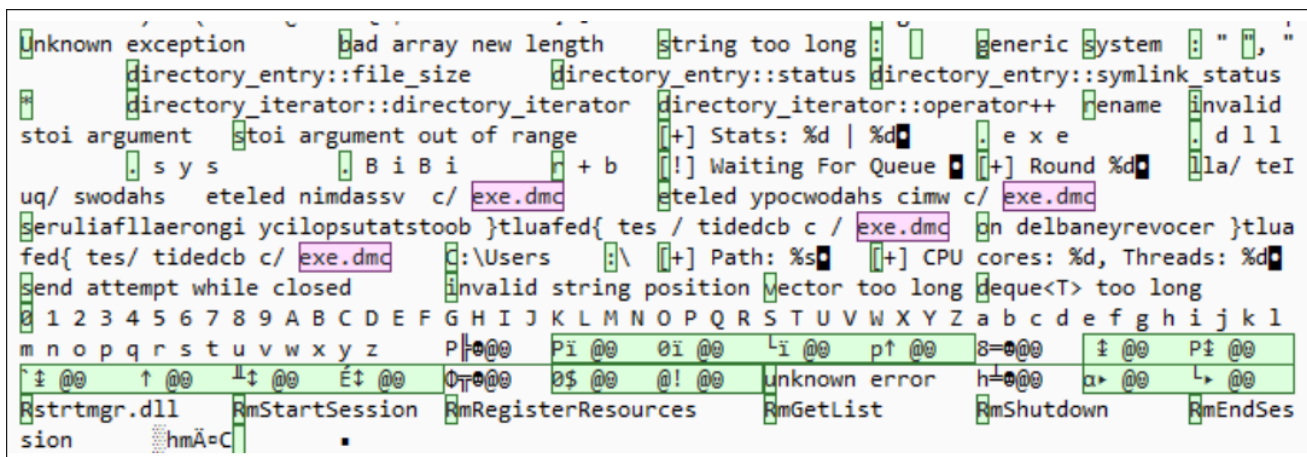


Figure 3: BiBi-Windows Wiper’s commands stored with a right-to-left technique

Finally, BiBi-Windows Wiper relies on the Restart Manager and its **Rstrtmgr.dll** to meet the process till the end.

Conclusion

As the Israel-Hamas war continues to escalate, it seems there are no safe harbors in either the physical or digital realm. Wipers are typically utilized in attacks prompted by geopolitical events because the goal of a wiper is destruction, plain and simple, rather than the monetary objectives that motivate attackers who spread non-wiping malware or ransomware.

As the conflict continues, it's likely we'll see more of this type of attack.

Indicators of Compromise (IoCs)

File Name	Size	SHA256
-----------	------	--------

bibi.exe	203.00 KB (207872 bytes)	40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17
----------	-----------------------------	--

Hunting Yara Rule

```
rule BIBI_Wiper_Windows {
  meta:
    description = "BiBi-Windows Wiper used in the Gaza War"
    author = "The BlackBerry Research and Intelligence Team"
    date = "2023-10-31"
    hash = "40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17"
    version = "1.0"

  strings:
    $a1 = "[+] Stats: " ascii wide
    $a2 = "C:\\Users" ascii wide
    $a3 = "[!] Waiting For Queue " ascii wide
    $a4 = "[+] Round " ascii wide
    $a5 = "[+] Path: " ascii wide
    $a6 = "[+] CPU cores: " ascii wide

  condition:
    uint16(0) == 0x5a4d and ((filesize < 2000KB) and all of ($a*))
}
```

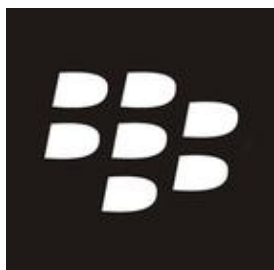
Related Reading:



About Dmitry Bestuzhev

Dmitry Bestuzhev is Senior Director, CTI (Cyber Threat Intelligence) at BlackBerry.

Prior to BlackBerry, Dmitry was Head of Kaspersky's Global Research and Analysis Team for Latin America, where he oversaw the company's experts' anti-malware development work in the region. Dmitry has more than 20 years of experience in IT security across a wide variety of roles. His field of expertise covers everything from traditional online fraud to targeted high-profile attacks on financial and governmental institutions. His main focus in research is on producing Threat Intelligence reports on financially motivated targeted attacks.



About The BlackBerry Research and Intelligence Team

The BlackBerry Research and Intelligence team is a highly experienced threat research group specializing in a wide range of cybersecurity disciplines, conducting continuous threat hunting to provide comprehensive insights into emerging threats. We analyze and address various attack vectors, leveraging our deep expertise in the cyberthreat landscape to develop proactive strategies that safeguard against adversaries.

Whether it's identifying new vulnerabilities or staying ahead of sophisticated attack tactics, we are dedicated to securing your digital assets with cutting-edge research and innovative solutions.

[Back](#)

© 2024 BlackBerry Limited. All rights reserved.