Intel's Habana Labs hacked by Pay2Key ransomware, data stolen

bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/

Lawrence Abrams

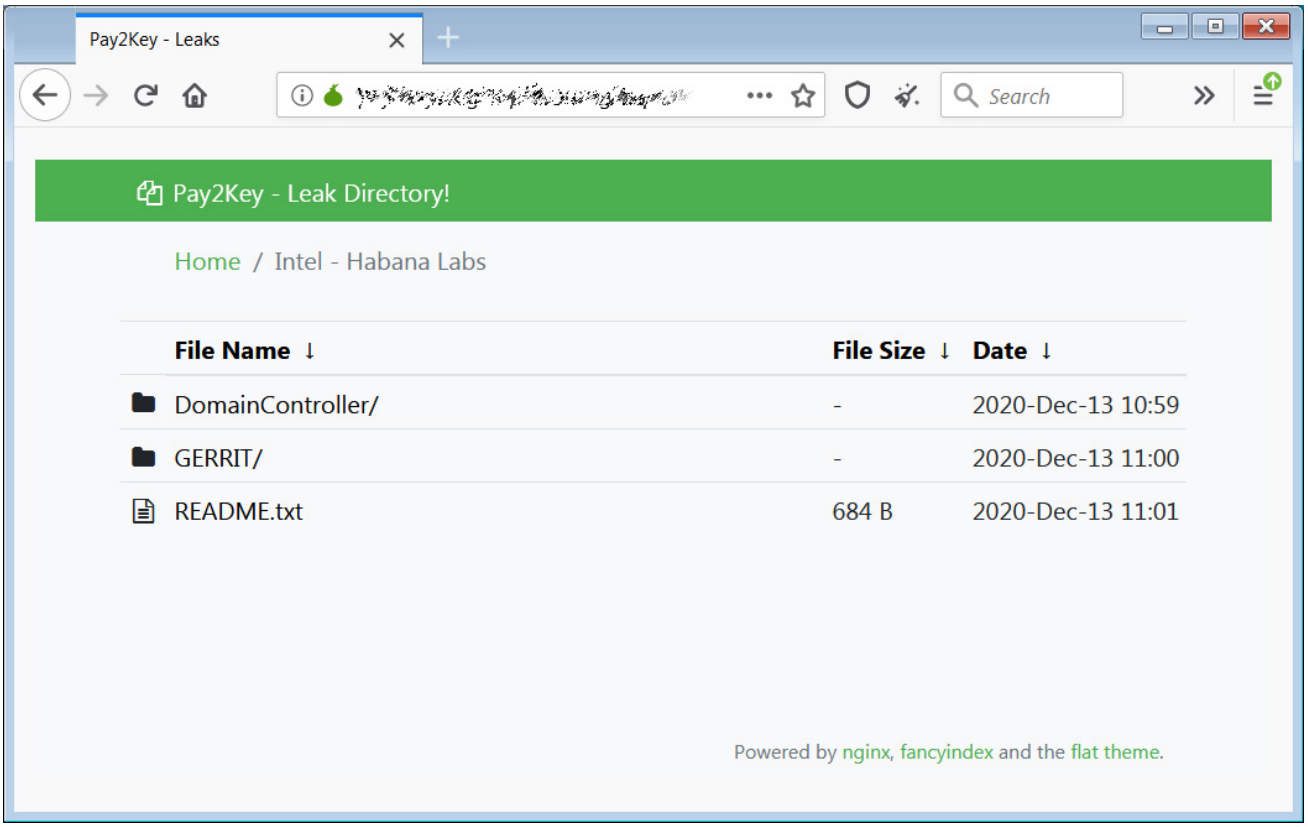
By
Lawrence Abrams

- December 13, 2020
- 01:19 PM
- 0

Intel-owned AI processor developer Habana Labs has suffered a cyberattack where data was stolen and leaked by threat actors.

Habana Labs is an Israeli developer of AI processors that accelerate artificial intelligence workloads in the datacenter. Intel purchased the company in December 2019 for approximately $2 billion.

Today, the Pay2Key ransomware operation leaked data allegedly stolen from Habana Labs during a cyberattack. This data includes Windows domain account information, DNS zone information for the domain, and a file listing from its Gerrit development code review system.



Pay2Key data leak page for Habana Labs

In addition to the content posted on their data leak site, the Pay2Key operators have leaked business documents and source code images.

```
/* SPDX-License-Identifier:     GPL-2.0+
 *
 * Copyright (C) 2017-2020 HabanaLabs Ltd.
 * All Rights Reserved.
 *
 */

#ifndef ZEPHYR_INCLUDE_WATCHDOG_H_
#define ZEPHYR_INCLUDE_WATCHDOG_H_

#define WDT_DEV_NAME        DT_LABEL(DT_ALIAS(watchdog0))
#define WD_TIMEOUT      5000U   /* 5 sec */
#define STACK_SIZE      1024
#define WD_THREAD_PRIORITY  3

int hl_watchdog_init(void);
void hl_feed_wd(void *p1, void *p2, void *p3);

#endif /* ZEPHYR_INCLUDE_WATCHDOG_H_ */
```

Alleged source code stolen from Habana Labs

In a threat posted to Pay2Key's data leak site, the threat actors have stated that Habana Labs has "72hrs to stop leaking process..." It is not known what ransom demands are being made, if any, to stop the leaking of data.

It is believed that this attack is not meant to generate revenue for the threat actors but rather to cause havoc for Israeli interests.

BleepingComputer has contacted Habana Labs with questions regarding the attack but has not heard back.

Pay2Key responsible for recent Israeli cyberattacks

Pay2Key is a relatively new ransomware operation behind a series of attacks against Israeli businesses in November 2020, as reported by Israeli cybersecurity firms Check Point and Profero.

Profero believes Iranian threat actors are behind the ransomware operation after tracking the group's ransom payment wallets to Iranian bitcoin exchanges.

> This week @_CPResearch_ released an analysis of ransomware targeting Israeli SME dubbed "Pay2Key". Using intelligence sources and our latest CryptoCurrency monitoring capabilities, we have been able to track the exit strategy of the threat actors leading to Iranian exchange. pic.twitter.com/64WzsonAjQ
>
> — Profero (@ProferoSec) November 11, 2020

Israeli media has reported that threat actors breached Israeli shipping and cargo software company Amital this week and used their access to compromise forty of the software company's clients in a supply chain attack.

While performing incident response, Profero and Israeli cybersecurity firm Security Joes have linked IOCs from these attacks to those discovered in previous Pay2Key attacks.

> Our joint @ProferoSec & @SecurityJoes IR teams have been able to correlate infrastructure of previous pay2key ransomware attacks to the current shipment and cargo infiltration. This is another major escalation in the current cyber-conflict between Israel and Iran. pic.twitter.com/idIWAm8JTb
>
> — Profero (@ProferoSec) December 13, 2020

Profero CEO Omri Moyal is warning Israeli companies to harden their network's defenses as further cyberattacks from Iran are expected.

Another threat actor known as BlackShadow was responsible for a recent cyberattack against Israeli insurance company Shirbit whose data was stolen and leaked. While the Shirbit attack is similar to the Pay2Key's attacks, it is unknown if they are linked.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Quantum ransomware seen deployed in rapid network attacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Data Exfiltration
- Intel
- PAY2KEY
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: