

## University Hospital New Jersey hit by SunCrypt ransomware, data leaked

By Ax Sharma

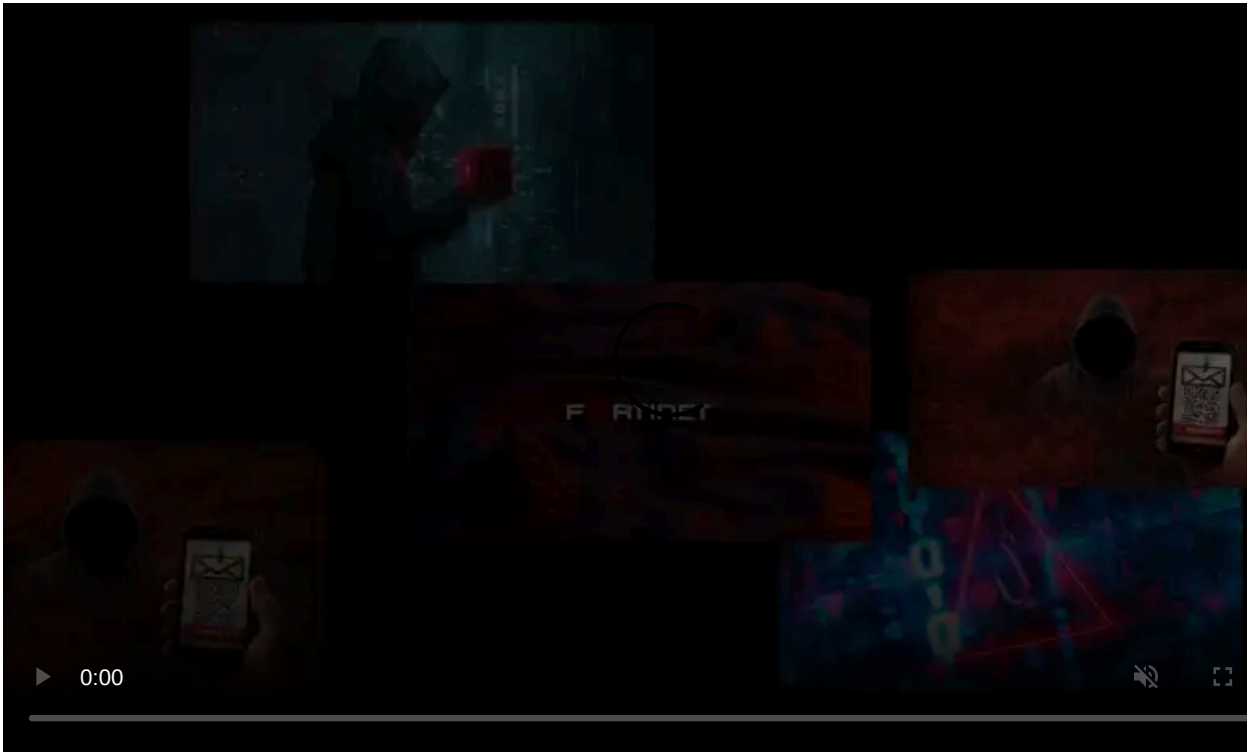
Published: 2020-09-16 · Archived: 2026-04-05 22:44:58 UTC



University Hospital New Jersey (UHNJ) has suffered a massive 48,000 document data breach after a ransomware operation leaked their stolen data.

Established in 1994, the [University Hospital](#) is a New Jersey state-owned teaching hospital that provides medical care to residents.

The hospital runs on a \$626 million budget and has over 3,500 employees, 519 licensed beds, and over 172,000 annual outpatient visits.



Visit Advertiser website [GO TO PAGE](#)

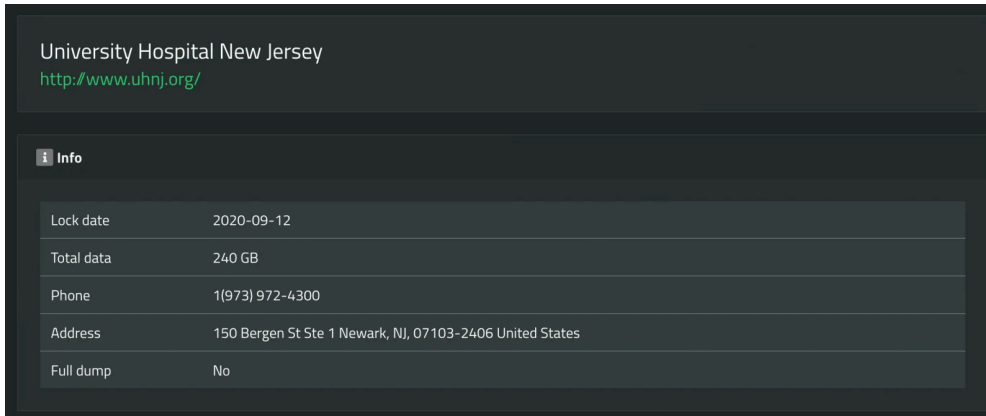
### Sensitive info leaked after a ransomware attack

The SunCrypt ransomware operation has leaked data allegedly stolen from UHNJ in a September ransomware attack.

SunCrypt is a ransomware operation that began its activities in October 2019 but was not very active. Over the past few months, they have become much more active since [releasing a dedicated leak site](#).

While BleepingComputer has not corroborated all of the attacker's claims, the data seen by BleepingComputer does appear to belong to UHNJ.

Of the 240 GB of data allegedly stolen from University Hospital New Jersey, the attackers have leaked a 1.7 GB archive containing over 48,000 documents.



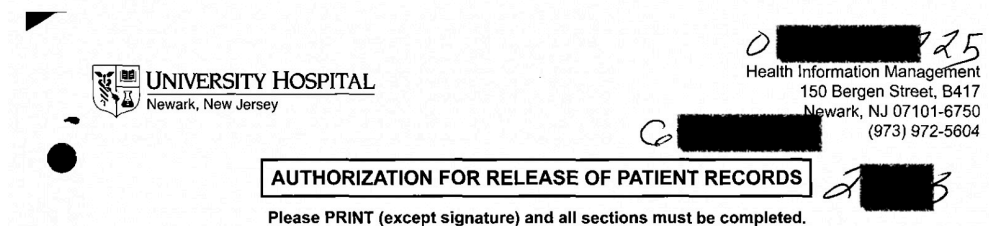
### Alleged data leak for University Hospital New Jersey

This data leak includes patient information release authorization forms, copies of driving licenses, Social Security Numbers (SSNs), date of birth (DOB), and records about the Board of Directors.

Имя	Размер	Сжатый	Изменен	Атрибуты
..				
Agri...	2 553 198 175	1 648 503 888	2020-07-30 15:16	DCI
Arc...	1 607 167 982	1 492 044 432	2019-12-05 11:30	DCI
Att...	4 416 704 344	1 524 319 728	2020-05-19 14:21	DCI
Boa...	73 873 690	0	2019-11-20 10:25	DCI
Cre...	770 762	0	2020-07-01 13:51	DCI
Em...	756 677 954	1 864 816 016	2020-08-25 13:17	DCI
Ins...	454 846 211	1 614 028 224	2020-09-04 12:31	DCI
Inv...	612 555 011	0	2020-08-17 14:49	DCI
Lav...	58 258	0	2020-08-25 13:04	DCI
Lec...	82 235 597	0	2020-08-28 12:15	DCI
Liti...	17 967 285 550	14 620 174 304	2020-09-11 13:05	DCI
No...	590 362 810	0	2019-08-16 12:55	DCI
OP...	1 765 888 591	885 794 928	2020-05-06 11:39	DCI
Ph...	602 688	0	2020-01-22 14:50	DCI

### UHNJ Data leak

Shown below is a partial image of one such record leaked in the dump, with PII redacted:



### **An example patient information release form**

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at [+16469613731](tel:+16469613731).

### **Employee infected with TrickBot prior to the attack**

A source in the cybersecurity industry has told BleepingComputer that an employee of UHNJ was infected with the TrickBot trojan at the end of August.

When a computer is infected with TrickBot, it usually leads to a full compromise of the network with ransomware eventually being deployed.

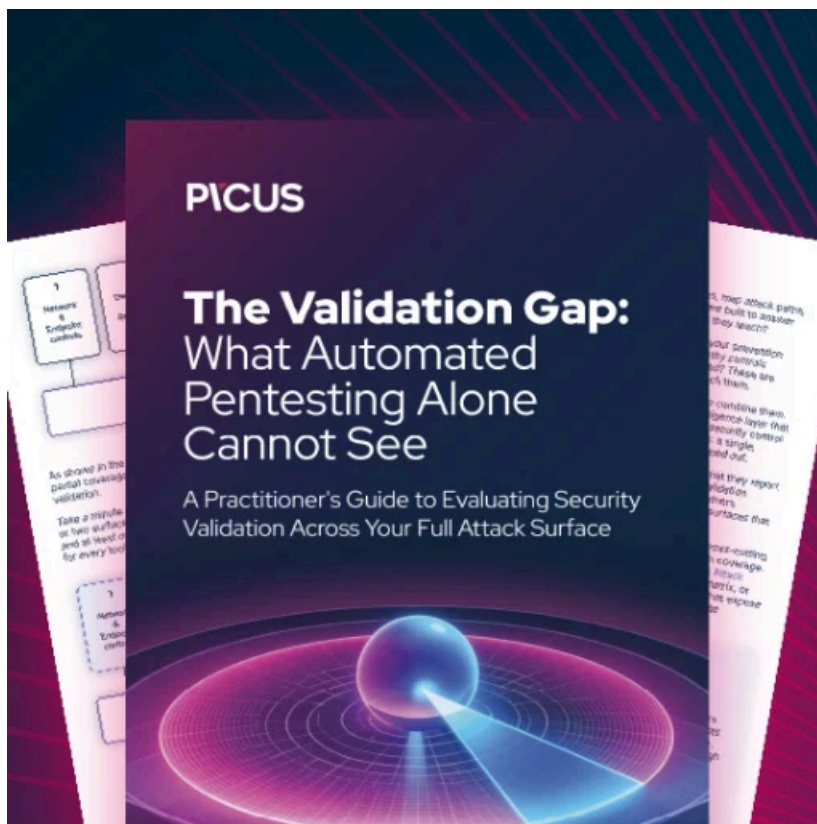
TrickBot has historically been known to [lead to Ryuk ransomware attacks](#) and an occasional [Maze ransomware](#) attack. Now TrickBot is predominately pushing the [Conti ransomware](#).

While Maze denies any affiliation with SunCrypt, the SunCrypt ransomware operators have told BleepingComputer that they are part of the Maze Cartel.

Furthermore, when infecting a victim, SunCrypt will connect to an IP address previously associated with Maze infections.

The SunCrypt operators may have also partnered with TrickBot to provide access to compromised networks, such as the network of UHNJ.

BleepingComputer has reached out to UHNJ multiple times but did not receive a response to our emails and calls.



### **[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/university-hospital-new-jersey-hit-by-suncrypt-ransomware-data-leaked/>