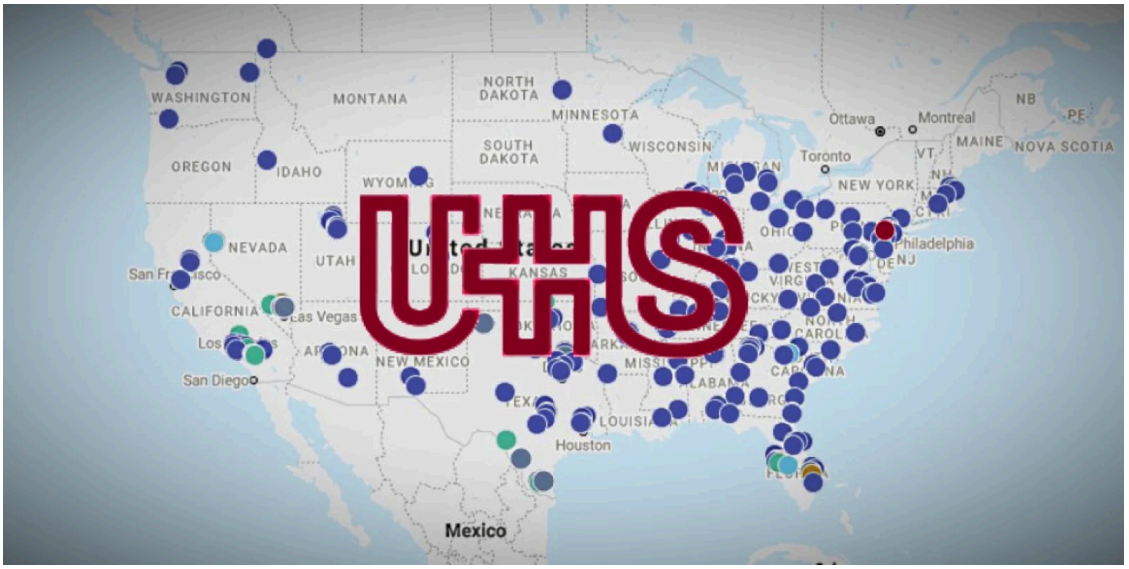
UHS hospitals hit by reported country-wide Ryuk ransomware attack

By Sergiu Gatlan

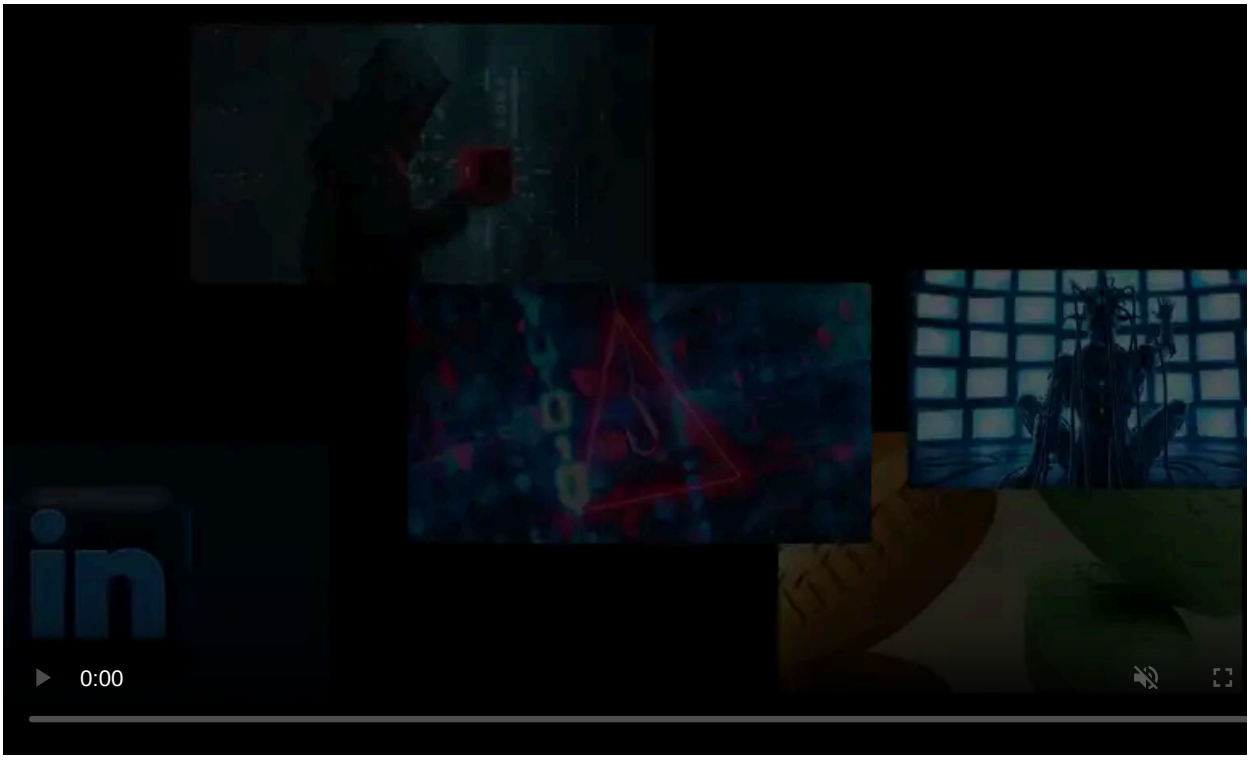
Published: 2020-09-28 · Archived: 2026-04-05 17:54:36 UTC

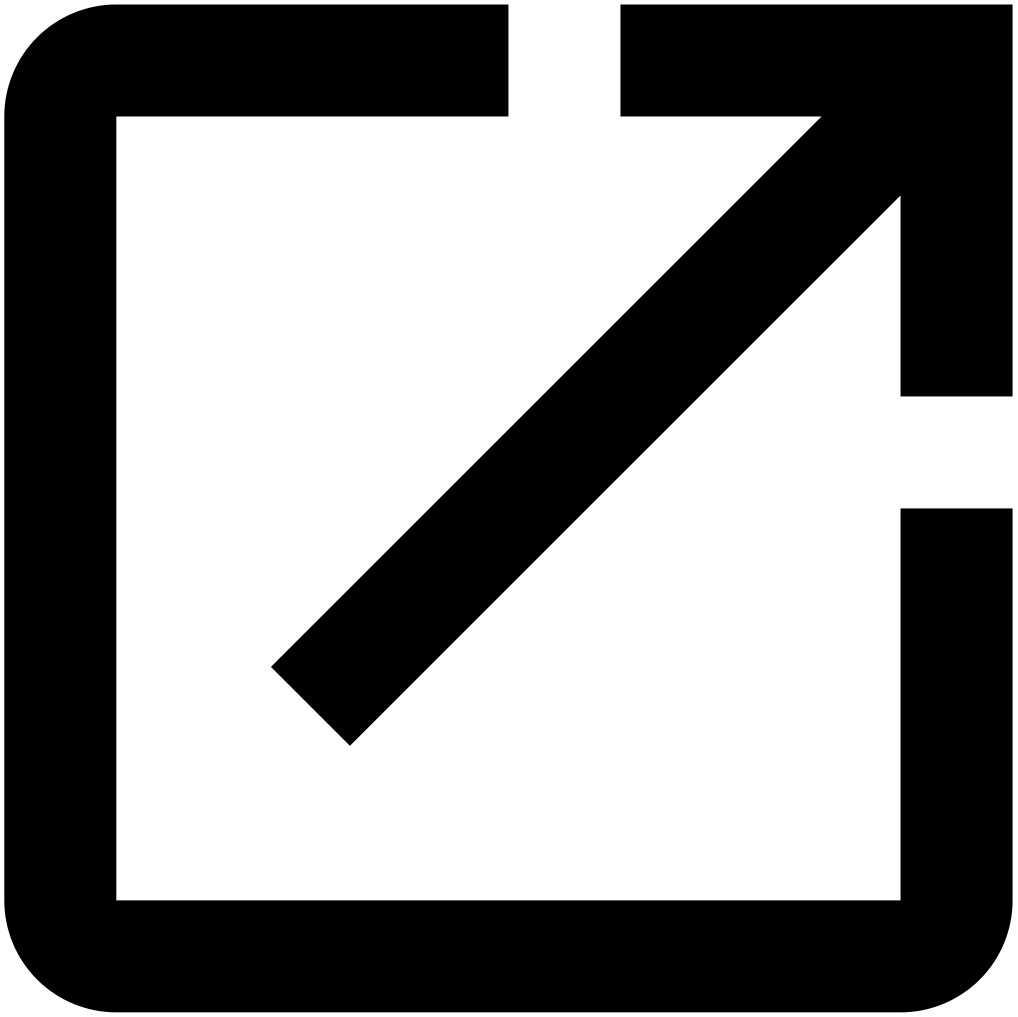


Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider, has reportedly shut down systems at healthcare facilities around the US after a cyber-attack that hit its network during early Sunday morning.

UHS operates over 400 healthcare facilities in the US and the UK, has more than 90,000 employees and provides healthcare services to approximately 3.5 million patients each year.

The Fortune 500 corporation had annual revenues of $11.4 billion in 2019 and it is 330th on Forbes' ranking of US largest public companies.


0:00



Attacked during the night

According to reports coming from UHS' employees, UHS hospitals in the US including those from California, Florida, Texas, Arizona, and Washington D.C. are left without access to computer and phone systems.

At the moment the affected hospitals are redirecting ambulances and relocating patients in need of surgery to other nearby hospitals.

"When the attack happened multiple antivirus programs were disabled by the attack and hard drives just lit up with activity," one of the reports reads.

"After 1min or so of this the computers logged out and shutdown. When you try to power back on the computers they automatically just shutdown.

"We have no access to anything computer based including old labs, ekg's, or radiology studies. We have no access to our PACS radiology system."

Employees were also told to shut down all systems to block the attackers' from reaching all devices on the network.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Ryuk ransomware behind the attack

While UHS has made no official statement regarding the attack, reports coming from employees show all the signs of a ransomware attack, starting with its launch during the night to avoid detection before encrypting as many systems as possible and the immediate shut down of all systems after it was discovered to prevent more devices getting locked.

An employee told BleepingComputer that, during the cyberattack, files were being renamed to include the .ryk extension. This extension is used by the Ryuk ransomware.

Another UHS employee told us that one of the impacted computers' screens changed to display a ransom note reading "Shadow of the Universe," a similar phrase to that appearing at the bottom of Ryuk ransom notes.

Based on information shared with BleepingComputer by Advanced Intel's Vitali Kremez, the attack on UHS' system likely started via a phishing attack.

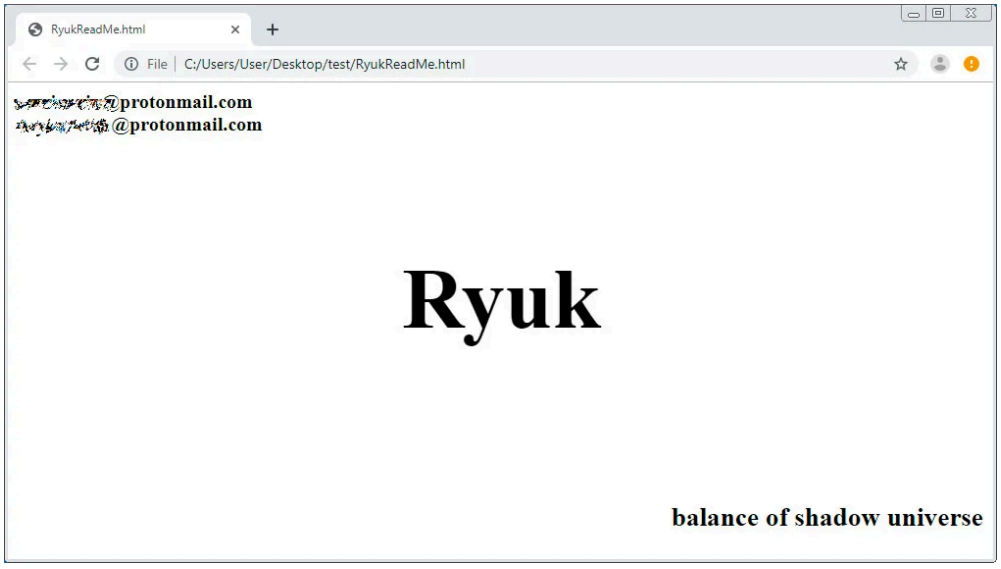
> Our team has observed the following: Phishing -> #KEGTAP -> #BEACON -> #RYUK.
>
> — Andrew Thompson (@anthomsec) September 28, 2020

According to Kremez, their Andariel intelligence platform detected both the Emotet and TrickBot Trojans affecting UHS Inc. throughout 2020, and more recently, in September 2020.

The Emotet trojan is spread via phishing emails containing malicious attachments that install the malware on a victim's computer.

After some time, Emotet will also install TrickBot, which ultimately opens a reverse shell to the Ryuk operators after harvesting sensitive information from compromised networks.

Once the Ryuk actors manually get access to the network they start with reconnaissance and, after gaining admin credentials, they deploy ransomware payloads on network devices using PSExec or PowerShell Empire.



Ryuk ransom note

Unfortunately, with ransomware attack, there is also a high chance of the attackers stealing patient and employee data which will further increase the damage.

Last week, BleepingComputer reported that a ransomware attack affecting a German hospital led to the death of a patient in a life-threatening condition after she was redirected to a more distant hospital.

Four deaths were also reported after the incident impacting UHS' facilities, caused by the doctors having to wait for lab results to arrive via courier. BleepingComputer has not been able to independently corroborate if the deaths were related to the attack.

If UHS decided to pay the Ryuk ransom, they need to be careful of using their decryptor as it is known to corrupt certain types of files.

Emsisoft is offering free ransomware recovery services to healthcare organizations during the pandemic, which include custom decryptors that are known to recover files 50% faster than the threat actor's decryptors.

"There are multiple factors and it depends a bit on the hardware, but there are three major factors: We heavily optimised I/O (so the reading and writing has been optimised a lot and been adjusted for modern mass storage), we use hardware accelerated cryptography, and we make creating a backup first unnecessary, because unlike the TA's tool, we operate on copies of data."

"The real benefit is in the fact that we focus on data safety first. So our decryptors generally are more stable, are safer to use, and produce correct results," Emsisoft CTO Fabian Wosar told BleepingComputer in a conversation.

BleepingComputer has contacted UHS for more information about the attack but has not heard back.

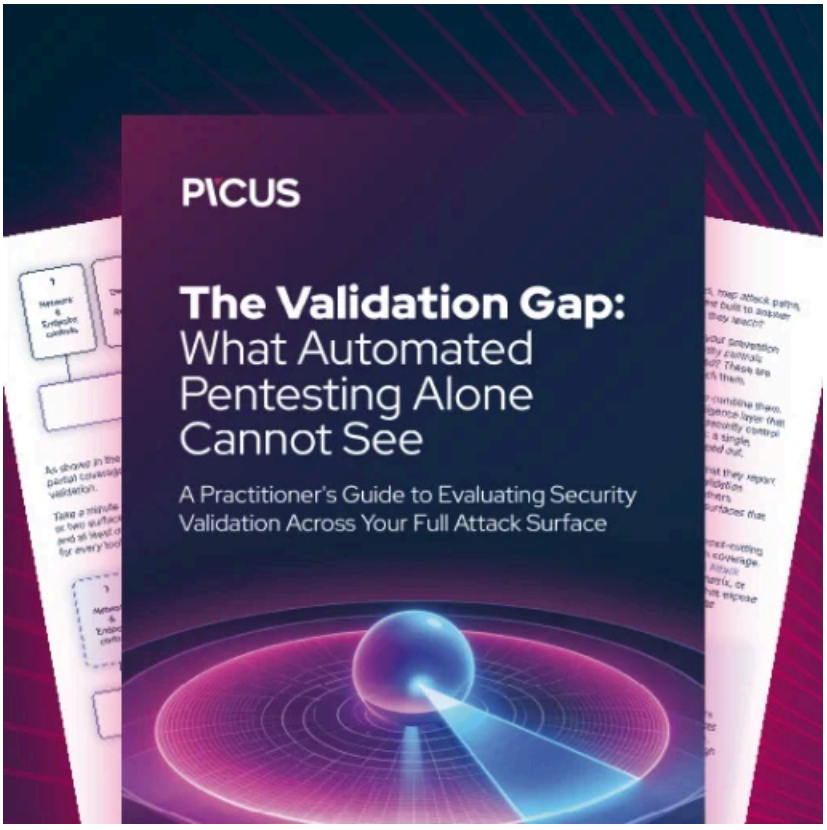
Update September 29, 18:45 EDT: Added information about Emsisoft decryptors.

Update September 28, 12:23 EDT: UHS confirmed that it was the victim of a security incident and says that no patient or employee data was impacted in the incident:

The IT Network across Universal Health Services (UHS) facilities is currently offline, due to an IT security issue.

We implement extensive IT security protocols and are working diligently with our IT security partners to restore IT operations as quickly as possible. In the meantime, our facilities are using their established back-up processes including offline documentation methods. Patient care continues to be delivered safely and effectively.

No patient or employee data appears to have been accessed, copied or otherwise compromised.



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/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/