Emotet trojan implicated in Wolverine Solutions ransomware attack

portswigger.net/daily-swig/emotet-trojan-implicated-in-wolverine-solutions-ransomware-attack

James Walker March 8, 2019

James Walker 08 March 2019 at 16:43 UTC
Updated: 06 July 2021 at 09:31 UTC
Healthcare Data Breach Ransomware
Malware outbreak at healthcare firm spawns data breach fears

Bimbim / Shutterstock

The notorious Emotet trojan has been linked to a ransomware attack against Wolverine Solutions Group (WSG) that resulted in the personal data of potentially hundreds of thousands of US healthcare patients being compromised.

Detroit-based WSG – which provides IT, printing, and logistics services for health-related business clients – fell victim to a ransomware attack on September 25, 2018.

It eventually paid, and over the last week new details have emerged about the techniques and tactics of the attackers, which featured the deployment of Emotet – a trojan usually delivered through traditional phishing emails.

An alert posted on the company’s website detailed how the malware encrypted many of WSG’s records, making them inaccessible unless it caved in to the attackers’ ransom demands.

Ransomware is not commonly associated with data breaches, and WSG said there is currently no indication that any data was extracted from the firm’s servers.

However, given the nature of the files (some of which contained sensitive patient information), WSG has been busy informing all impacted individuals of the incident – a task made all the more difficult given the company’s position as a third-party service provider.

“The final count of healthcare clients and their affected individuals has not yet been finalized, but the number of covered entities and their sub-entities would be in the high 100s and the number of affected individuals would be in the high six-figures,” WSG president Darryl English told The Daily Swig via email this week.

The patients and customers of a number of Michigan-based healthcare organizations have already been revealed as potentially impacted by the malware outbreak.

These organizations include healthcare providers Three Rivers Health and Blue Cross Blue Shield, along with healthcare insurer Health Alliance Plan.

Emotet: From banking trojan to ransomware loader

While the WSG president said certain information related to the incident remains confidential as it is part of an ongoing HHS/OCR investigation, he did provide a few additional technical details in relation to the attack.

“The strain of malware that impacted WSG’s network was the trojan Emotet,” English told The Daily Swig.

Those familiar with Emotet will know it is primarily associated with looting online banking accounts. US-CERT describes Emotet as “an advanced, modular banking trojan that primarily functions as a downloader or dropper of other banking trojans”.

However, WSG’s confirmation that Emotet was used to push ransomware onto its network comes just two months after security firms CrowdStrike and Kryptos Logic separately confirmed that the trojan had been implicated in Ryuk ransomware attacks.

In its 2019 State of Malware report, Malwarebytes said it expected to see Emotet/Trickbot combo malware impacting not just the banking, but also the education, government, manufacturing, and healthcare sectors throughout the year.

“Originally a banking trojan, Emotet has evolved over the years to become a loader as a service, although mostly keeping up with banking and stealer families as well,” explains Jérôme Segura, head of threat intelligence at Malwarebytes.

“There were some noteworthy attacks where Emotet was found to be at the root cause of ransomware infections, in particular by working with Trickbot actors.

"Malware distributors willing to deliver their payload are always looking for the best ways to do so. Emotet campaigns have a wide reach with daily onslaught of maliciously crafted documents using social engineering to deliver the malware.

“For this reason, partnerships with Emotet and its wide botnet are a great way to achieve this malware delivery goal.”

When it comes to protecting against Emotet-based attacks, Segura said: “The risk is greater for businesses than consumers, but there are many steps that can be taken to mitigate it.

“System administrators can disable Office macros and harden endpoint security. Since social engineering plays a big part in the majority of these campaigns, training staff on recognizing malicious emails is also a big step towards protecting an organization.”

The Daily Swig asked WSG for further details relating to the ransomware strain that impacted its systems, via Emotet, thus far without any further information.

Regardless of the particular strain of ransomware that was involved in this latest attack, English confirmed the company did eventually submit to the attackers' demands.

"Ultimately, a ransom was paid," he said.

RELATED AccuDoc data incident highlights 'growing calamity' of third-party breaches

James Walker
James Walker

@jameswalk_er