TRICKBOT/RYUK HEALTHCARE ATTACKS

By John Limb, CTO at Braintrace
November 3, 2020 7:56 am ET

The FBI and CISA have issued a warning for ransomware attacks targeting the healthcare industry since there has been a significant increase in these attacks. Last week, four healthcare institutions were hit by Ryuk ransomware attacks facilitated by a modular banking trojan named Trickbot.

Ransomware attacks on the healthcare industry become a life and death problem. Ryuk affects the human interface (HMI) for operational technology (OT) devices. The computers used in conjunction with the medical equipment are ransomed; thus, they will not use them—effectively knocking out the medical devices because they will not have any computers to run.

This Ransomware-as-a-Service was used heavily in the banking industry back in 2019. These bad actors have now shifted focus on the more vulnerable Healthcare industry. They know these organizations will pay anything to take care of their patients. The timing with COVID-19 is not a coincidence.

For Ryuk to be installed, Trickbot is first installed by a user enabling a macro in a Microsoft Word or Excel file. In earlier Ryuk attacks, another banking trojan named Emotet was used to exploit the system before pulling down Trickbot and finally Ryuk. Once Trickbot is installed, it begins reaching out to its command and control (C2) servers. The latest versions of Trickbot tagged as ono76 and ono77 have a few new tricks, one being a new reconnaissance module named Anchor_DNS that provides connectivity checks for C2 activities and TLS only communications over ports 443, 449. We also observed these versions not working on 32bit windows, with rewritten DLL files for 64bit windows only.

Traditionally, we would first see Emotet malware used to install Trickbot to do the exploit. Trickbot then runs Ryuk. With this new version of Trickbot, Emotet does not have to be used. However, we have proof that it still is in use. Since August, BraintraceLABS has observed more than a 1,000% increase in Emotet infections.

Earlier versions of Trickbot used HTTP over port 8082, allowing for deep packet inspection content matching. This is no longer the case in later versions. All C2 activity observed was over encrypted channels except for DNS.

Braintrace's Dragonfly NTA recognizes Trickbot and Emotet via Encrypted Payload Analytics (EPA), which identifies encrypted flows by the patterns generated by malware and C2 servers. The latest versions of Trickbot have changed substantially, requiring a new deep learning prediction model training with Trickbot ono76 and ono77 as a new malware family.

The first wave of defense for a healthcare provider to protect against these attacks is to have a good antivirus on the endpoint. The second line of defense is to have some network traffic analysis (NTA) capable of detecting Emotet and Trickbot. Once detected, an analyst can use firewall techniques to block communication. We can confidently confirm, Braintrace's Dragonfly users are well protected with Dragonfly's Encrypted Payload Analytics. It detects Emotet and TrickBot effectively.

REACH OUT TO US

If you have any questions or concerns about protecting your organization from the newest threats, please feel free to contact us at info@braintrace.com.