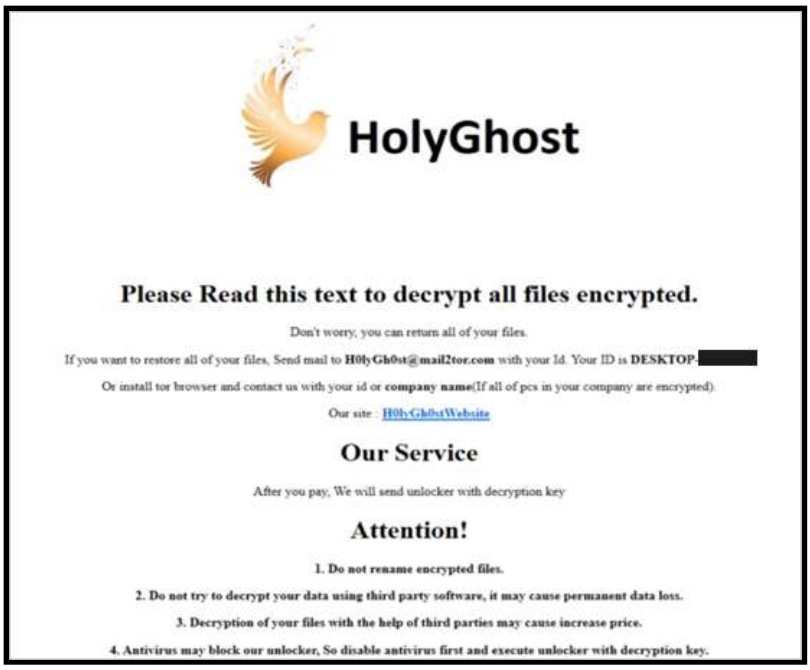
Feds Exorcize the H0lyGh0st



Source: https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

Less than two weeks after publishing news on the Maui strain of ransomware that North Korea had unleashed on US based healthcare entities, **the FBI shutdown these cyber crooks, and actually recovered over 500 thousand dollars in ransom money**. "**The seized funds include ransoms paid by health care providers in Kansas and Colorado,"** according to Justice.

Eleven days ago, as of this writing, on July 8, 2022, **the Dispatches reported that on July 6, 2022**, a joint press release **Alert (AA22-187A)**, was issued by CISA, the FBI, and the Treasury Department with the inspiring title of "**North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector**." The stated purpose of the Alert release was rather complex and quite a deep dive into the nuts and bolts of the attack.

> **This joint CSA provides information—including tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs)—on Maui ransomware obtained from FBI incident response activities and industry analysis of a Maui sample. The FBI, CISA, and Treasury urge HPH Sector organizations as well as other critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the likelihood of compromise from ransomware operations. Victims of Maui ransomware should report the incident to their local FBI field office or CISA.**

The secret sauce that made this arrest of culprits and recovery of ill gotten gains was the "**rapid reporting and cooperation from a victim,**" according to the **Department of Justice Press Release of July 19, 2022**. Indeed, Microsoft was on top of this cyberattack from its beginnings. If you would like a deep dive into the history of and techniques employed by DEV-053, **then try the full write up by MS of July 14, 2022.** And, as it is wont to do, Microsoft's recommended mitigation procedures are extensive and go far beyond tots, pears, and change your password.

> **A group of actors originating from North Korea that Microsoft Threat Intelligence Center (MSTIC) tracks as DEV-0530 has been developing and using ransomware in attacks since June 2021. This group, which calls itself H0lyGh0st, utilizes a ransomware payload with the same name for its**

campaigns and has successfully compromised small businesses in multiple countries as early as September 2021.

As Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division said in the press release, "**Reporting cyber incidents to law enforcement and cooperating with investigations not only protects the United States, it is also good business.**" Olsen went on to declare that "**The reimbursement to these victims of the ransom shows why it pays to work with law enforcement.**"

The F.B.I. credited the help they received in tracking this group by a victim of the attack. In this case, a Kansas hospital paid a ransom in 2021. The hospital, however, **"also contacted the FBI, which traced the payment and identified China-based money launderers who assisted the North Korean hackers in cashing out the illicit proceeds. The FBI ultimately recovered half a million dollars, including the entire ransom payment from the hospital, according to a FoxNews report.**

But let's give some credit where credit due. The group responsible for the attacks had their activities tracked beginning in May 2021. **Justice noted that**:

> **After more than a week of being unable to access encrypted servers, the Kansas hospital paid approximately $100,000 in Bitcoin to regain the use of their computers and equipment. Because the Kansas medical center notified the FBI and cooperated with law enforcement, the FBI was able to identify the never-before-seen North Korean ransomware and trace the cryptocurrency to China-based money launderers.**
>
> **Then, as a result, in April 2022, the FBI observed an approximately $120,000 Bitcoin payment into one of the seized cryptocurrency accounts identified thanks to the cooperation of the Kansas hospital. The FBI's investigation confirmed that a medical provider in Colorado had just paid a ransom after being hacked by actors using the same Maui ransomware strain. In May 2022, the FBI seized the contents of two cryptocurrency accounts that had received funds from the Kansas and Colorado health care providers. The District of Kansas then began proceedings to forfeit the hackers' funds and return the stolen money to the victims.**

Kudos to the Kansas hospital not yet named for recognizing the critical nature of the problem, and not shrinking from their duty, first as a sworn adherent to the Hippocratic oath that says first do no more harm. The hospital did the responsible thing and accepted the hard reality of the situation.

Contrast the depth of this coverage with the absolute vapid and vacuous almost non-reporting of the breach of water systems in Rhode Island, as discussed in the previous posting herein. There are many questions that must be asked of the Rhode Island situation, and indeed any type of cyberattack. The bigger question than "What did the crooks take?", is "What did the crooks leave behind?" Did the the nondescript generic attack on a water treatment plant leave behind backdoors for other cyber capers to be launched against other related entites?

We can only speculate, pontificate, and wonder if the leadership of **Springhill Memorial Hospital, Mobile County, Alabama, July 9, 2019**, and for the next few ensuing weeks, had admitted that their hospital had been rendered unable to provide the requisite standards of quality of care we have come to expect from our modern medical providers due to an ongoing ransomware attack, then the tragic outcome of the case of baby Nicko Silar might have been very different. Maybe little Nicko would be alive today.

Just sayin'

> ***"... once evil is invited in, tremendous effort is required to show it to the door and kick its cloven hoof off the threshold."***
>
> ***— E.A. Bucchianeri, Vocation of a Gadfly***

Back to Top

Gerald Reiff

Back to Top ← previous post next post → TBA