A Patient Dies After Ransomware Attack Paralyzes German Hospital Systems

September 21, 2020 Ravie Lakshmanan

German authorities last week disclosed that a ransomware attack on the University Hospital of Düsseldorf (UKD) caused a failure of IT systems, resulting in the death of a woman who had to be sent to another hospital that was 20 miles away.

JOINT
CYBERSECURITY ADVISORY

TLP:WHITE

FBI | CISA

Zeppelin actors gain access to victim networks via RDP exploitation [T1133], exploiting SonicWall firewall vulnerabilities [T1190], and phishing campaigns [T1566]. Prior to deploying Zeppelin ransomware, actors spend one to two weeks mapping or enumerating the victim network to identify data enclaves, including cloud storage and network backups [TA0007]. Zeppelin actors can deploy Zeppelin ransomware as a `.dll` or `.exe` file or contained within a PowerShell loader. [1]

Prior to encryption, Zeppelin actors exfiltrate [TA0010] sensitive company data files to sell or publish in the event the victim refuses to pay the ransom. Once the ransomware is executed, a randomized nine-digit hexadecimal number is appended to each encrypted file as a file extension, e.g., `file.txt.txt.C59-E8C-929` [T1486]. A note file with a ransom note is left on compromised systems, frequently on the desktop (see figure 1 below).

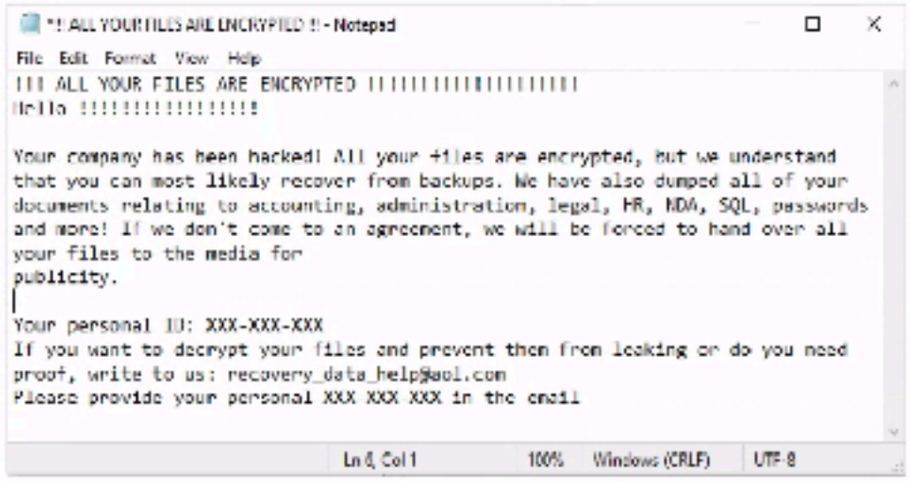

Figure 1: Sample Ransom Note

The FBI has observed instances where Zeppelin actors executed their malware multiple times within a victim's network, resulting in the creation of different IDs or file extensions, for each instance of an attack; this results in the victim needing several unique decryption keys.

Cybersecurity and Infrastructure Security Agency

August 2022

Federal Bureau of Investigation

May 2022

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2022

Alert Number
I-050422-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Business Email Compromise: The $43 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and