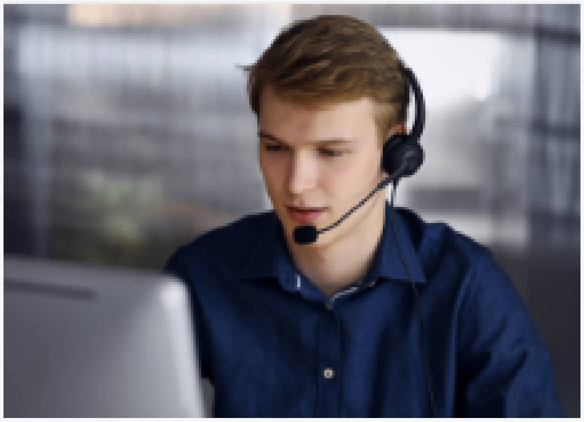
EINPRESSWIRE

# Ransomware attacks becoming threats to personal data: Cyber-Forensics.net offers damage-mitigating steps

*Ransomware is an encryption program that demands payment to release company data. The ransomware attack is usually launched through a pop-up form.*



Cyber Forensic Specialist

SOFIA, BULGARIA, February 21, 2022 /EINPresswire.com/ -- In 2020, The Federal Bureau of Investigation received 2,474 ransomware attack complaints. Unfortunately, these attacks have only become more prevalent since last year. To add to the issue, cybersecurity ventures expect that most businesses will become victims of ransomware attacks by the end of 2022.

Cyber-Forensics.net, providers of cyber forensics services for online scam victims, sums that ransomware attacks impact all industries alike. From healthcare to tech, the oil industry to higher education, all domains are equally affected.

> “
> Simple investigative ways can reduce risk in organizations by implementing intrusion-prevention software, regularly watching for evidence of evasion and unexpected privilege escalation.”
>
> *Timothy Benson*

Attackers not only demand astronomical payments to release company data but also threaten cybersecurity protocols. This major concern is forcing government agencies to issue urgent warnings and lay out preventive steps.

How Ransomware Attack Works?
Ransomware typically spreads via phishing emails, spam, or social engineering efforts. Attackers can also send malicious links through websites or drive-by downloads to penetrate a system's network and affect an endpoint. Infection methods consistently involve a step by step attack, which are as followed:

Steps in a typical ransomware attack:

Cyber-Forensics.net

Step 1: Infection: The receiver's system is infected via a corrupted attachment, phishing email, application, or another file. The ransomware installs itself when the device connects to any network.

Step 2: Securing Key passwords: The ransomware gives access and command of the control server to the cybercriminal. The criminal gets keys/passwords in the system.

Step 3: Encryption: The ransomware initiates encrypting the files it can find on the device and the network.

Step 4: Extortion: After encrypting the system files, the ransomware displays instructions for extortion and payment. The malware threatens to destroy available data if payment is not made.

Step 5: Releasing Data: The individuals or organizations pay the ransom and hope that cybercrooks free the affected data or attempt to recover the data by removing infected files. Unfortunately, negotiating with such attackers is often a lost cause, as found in recent fraud reports.

Recent trends
Ransomware attackers target firms of all sizes- from small to medium to large.

Fraud recovery specialist Timothy Benson studied one of the most recent cases of ransomware attacks. In December 2021, a giant in payroll and time-sheet software suffered a ransomware attack leading the company to announce going offline for weeks.

The company became aware of the attack in the first week of December and began investigating. According to a spokesperson, the company sent a message to its consumers that it was working with leading cyber-security experts to assess and resolve the situation.

Presenting his thoughts on the issue, Timothy Benson emphasizes that "simple investigative ways can reduce risk in organizations by implementing intrusion-prevention software, regularly watching for evidence of evasion and unexpected privilege escalation. It's all about making it more expensive for the cybercrooks."

How to stop a Ransomware attack?
The most effective way to mitigate ransomware attacks is by training company employees and staying alert to spot social engineering tactics.

Slow Down and Control emotions: Cyber attackers usually try to manipulate targets' emotions to

make them react quickly. The more time an individual thinks about a situation, the more likely they will realize something is missing. By slowing down, human rationality allows us to overcome feelings.
Isolate the Infection: Prevent the rest of the data by quickly separating all infected computers from each other and then disconnecting the network.

Identify the Infection: From pop up clicked to message opened, determine which malware strain corrupted the system. If the victim is an individual, they can reach out to cyber experts for help.

Report the matter: Immediately contact the authorities for support and coordinate measures to launch counter-attack measures.

Wipe all the systems: Remove the malware by completely formatting or wiping the previous files from all storage devices and reinstalling everything.
Determine the following option: Carefully plan out the best-suited mitigation measures. Either approach a cyber expert or contact the police.
Restore and Refresh: Use safe backups and software sources to restore computer files.

Plan to Prevent Attacks: Assess how the infection occurs and what measures can be put to keep the files in place and prevent another attack from happening.

The Fund Recovery Process in a Ransomware Attacks
Ransomware attacks would never happen if ransoms were never paid. But the reality is that organizations and victims choose to pay the ransom because the consequences of not doing so generally outweigh the paid cost.

In most cases, threatening the criminals with reporting the matter doesn't work because it is generally hard to prove the true identity of perpetrators. And recovery typically becomes a longer process.

However, given the involvement of multiple law enforcement like police, cyber experts, lawyers can help build a relevant case against the suspects and ultimately bring them to justice.

The involvement of law enforcement and fund recovery companies is critical. They are equipped with the skills, knowledge, and tools to investigate such crimes properly. The odds of attempting to identify the criminals on their own can damage the case.

The alternative way to recover funds is to intercept the funds when the attackers try to liquidate, cash out or launder them through various exchange mediums like bitcoin.

Whether or not funds can be intercepted depends on various factors like cyber help chosen by the attack victims.

Generic support from experienced cyber expert professionals like Cyber-Forensics.net can present real-time assessments and guarantee maximum refunds.

About Cyber-Forensics.net
Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. Cyber-Forensics.net commonly deals with bitcoin scams and forex withdrawal problems. For more information, please visit https://cyber-forensics.net/.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here