19859

LETTER 1 – CURRENT PARTICIPANT OF CURRENT PEAK TPA CLIENT

Notice of Data Breach

Dear PARTICIPANT NAME:

Your privacy is important to CLIENT NAME. We work very hard to protect your data. More than that, we partner with vendors who share this standard.

On February 9, 2021, we were contacted by a vendor of ours, PEAK TPA. (PEAK TPA conducts administrative services for claims payment for us.) PEAK informed us that our participant data was stolen. The theft took place on two of PEAK's cloud servers. I am sorry to share that they told us that at your data was included in the breach. The affected information may include full name, home address, date of birth, social security number.

What are we doing?
We are notifying you as quickly as possible so that you may best protect yourself.

PEAK has retained a company named Kroll to provide identity monitoring at no cost to you for 3 years. These services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Kroll's team has a track record of helping people who have faced such an event.

You can sign up for your identity monitoring services by visiting URL before FINAL DATE. When signing up for services, please use this Membership Number: MEMBER ID.

(If you choose not to use these credit monitoring services, we urge you to check your account statements for improper activity. This includes credit card statements and explanations of benefits.)

In addition, PEAK TPA has set up a toll-free number to answer your questions. Contact them at INSERT NUMBER between the hours of 9 a.m. and 6:30 p.m. Eastern Time. Please have your Membership Number ready.

On January 27, 2021, the criminal group behind the attack, Netwalker, was broken up by the FBI. Its leader was arrested, and its assets were seized. Still, PEAK TPA has assured us it has put in more protections to prevent a theft like this from happening again.

We care for your privacy, and we are deeply sorry for the inconvenience this may cause. We thank you for your understanding and your trust in CLIENT NAME.

CLIENT SIGN OFF

Netwalker FAQ

What is malware?

Malware is malicious software designed to cause damage or negatively affect computers, networks, and information technology systems.

What is ransomware?

Ransomware is a type of malicious software (malware) designed specifically to prevent the availability and usage of information technology systems until victims pay a ransom to unlock their access. This is typically achieved by encrypting files on a computer so that they are inaccessible by victims until a decryption mechanism is released after payment. In addition to encrypting the files, some variants of ransomware exfiltrate files and data from systems.

What is Netwalker?

Netwalker is a form of ransomware that operates on a closed-access ransomware-as-a-service (RaaS) portal. This operating model revolves around granting portal access to vetted third-party hackers ("affiliates") where they may build custom versions of the ransomware and deploy to targets as they see fit. Netwalker ransomware itself works similarly to other variants of ransomware by encrypting files on victim machines and leaving a message with instructions for paying the ransom. However, unlike typical ransomware malware, Netwalker attacks also exfiltrate data from victim machines and threaten to release data if the ransom is not paid. The leverage introduced by this risk prevents many victims from simply ignoring ransom-demands and returning to normal operations by restoring systems from backups.

How does Netwalker malware spread?

Malware in general spreads through the download and installation of infected software on a computer system or network device. The way malware is downloaded and installed can vary greatly. Often times, attackers will send fake emails containing infected files or links to malicious websites to unsuspecting victims. The victims may accidentally click on a file or navigate to a website, resulting in the installation of malware on the computer. Other ways that attackers can install malware on machines are through exploiting known vulnerabilities within software systems or through the usage of compromised account credentials. Once malware acquires an initial foothold on a machine, it can perform a number of activities to acquire more information about the computer system, user accounts, and network environment in an attempt to spread to different systems and cause further harm.

Netwalker hackers are known to use similar techniques to install and spread the malware. In March 2020, attackers using Netwalker ransomware spread the malware by sending phishing emails to victims with information about the COVID-19 pandemic. When victims clicked on the phishing emails, a Visual Basic Scripting (VBS) script contained within would be executed, delivering the malware to the computer system. Netwalker actors are also known to exploit vulnerabilities within Virtual Private Network (VPN) appliances, vulnerabilities within web applications, and weak passwords for Remote Desktop Protocol (RDP) connections to deliver malware onto information systems. Our forensic analysis suggests the actors exploited weak passwords for RDP in the case of PEAK TPA., a vulnerability we have now addressed across our systems.

Once Netwalker actors have successfully installed the malware within a network, they use various techniques to carve administrator credentials, exfiltrate sensitive data, and encrypt files. The actors typically execute commands via PowerShell to achieve their goals and have been known to use the popular exploitation tool, Mimikatz, to discover passwords and other sensitive information on a system.

What is a vulnerability?

A vulnerability is a weakness or flaw in an information system, security procedure, security control, or other implementation that can be exploited by an actor or threat, leading to unintended results.

How can credentials become compromised?

Credentials can be compromised in a variety of ways ranging from accidentally disclosing usernames and passwords to individuals, websites, or other locations they should not be disclosed, to being exposed during a data breach. Credentials can also be compromised through brute-force and password guessing attacks. If passwords are not strong enough or are reused across different websites and information systems, they may be easily guessable.

What is brute-forcing?

Brute-forcing is the process of rapidly guessing possible combinations of characters and numbers until a correct username and password is found. If passwords do not use enough variety of characters and do not have the appropriate length, brute-force attacks do not have to guess as many possible combinations, making the credentials quicker and easier to crack. Utilizing multi-factor authentication (MFA) in addition to a username and password can make credentials significantly more secure and difficult to crack, ultimately preventing access to a system.

What is multi-factor authentication (MFA)?

Multi-Factor Authentication is a security enhancement used for authentication that allows individuals to provide two or more pieces of evidence (or factors) to prove their identity. MFA can assist in preventing attacks from actors using compromised credentials since they would have to compromise an additional piece of evidence about a user. Some different types of factors are knowledge, possession, and inherence.

- Knowledge – Something only a user knows such as a username and password combination.
- Possession – Something only a user has like a smart card or smart phone.
- Inherence – Something only a user is such as biometric information (iris scan, fingerprint, etc…).

Sincerely,

Michael McGarrigle, MS
Senior Vice President, Third Party Administration