VOLUME 25 | ISSUE 2

# PARTNERS IN CRIME PREVENTION

MARCH/APRIL 2021

INSIDE THIS ISSUE



Adam Fortney- Sheriff
Snohomish County
Sheriff's Office

3000 Rockefeller
M/S 606
Everett, WA 98201
425-388-3393
http://sheriff. snoco.org

## RANSOMWARE— A GROWING THREAT

Recent press reports of a data breach that affected local city and governmental entities has put the spotlight on ransomware.

Automatic Funds transfer Services (AFTS) was attacked by ransomware in early February. AFTS provides payment processing, billing, mailing, and other services for local governments and municipal utilities. The ransomware attack affected the data from Snohomish County governments that included the cities of Lynnwood and Monroe, as well as the Port of Everett, and the Alderwood Water & Wastewater District. Compromised information could include images of customers' checks that include banking and routing information.

Scammers have been changing tactics to make their money.

In the past they have relied on data breaches to gather personal information, then either sell that information to other scammers or use it themselves in a variety of criminal schemes. However, the Identity Theft Resource Center (ITRC) has noted a downturn in data breaches. U.S. data breaches fell 19% in 2020 from 1,473 in 2019 to 1,108 in 2020. And the number of people affected by data breaches has fallen by 66%.

But ransomware has grown in payouts for scammers. By one account, ransomware payouts averaged $10,000 per event in 2018 while in 2020 scammers could collect $233,000 per event.

Ransomware attacks require less effort and are largely automated. They also generate as much revenue in minutes as hundreds of individual ID attacks do over months or years.

Another trend is that ransomware attackers are targeting third parties and sub-contractors. This way they can access information from larger organizations or multiple organizations that might have better cybersecurity measures through businesses whose cybersecurity may not be as good.

Ransomware has become so serious that the Cybersecurity and Infrastructure Security Agency (CISA) has announced a Reduce the Risk of Ransomware Campaign.

The ITRC president and CEO points out that

"Cybercriminals are simply shifting their tactics to find a new way to attack businesses and consumers. It is vitally important that we adapt our practices, and shift resources, to stay one step ahead of the threat actors."

## RANSOMWARE-AS-A-SERVICE-

*Cyber-criminals can be entrepreneurial. Some cyber-criminals who have the skills to write ransomware malware will sell or rent their software to other criminals to use. This is called Ransomware-as-a-Service (RaaS).*

*RaaS criminals will also provide technical support and step-by-step guidance on how to launch a ransomware attack.*

*The RaaS service provider will get a cut of the proceeds to the attack.*

*The service provider benefits in being able to "earn" more money from the rental/sale of his software beyond any attacks that he might have initiated.*

*As for the attacker, he benefits in that he does not need to know how to write the code of the malicious software, expanding the number of people in the business of attacking computer systems with ransomware.*

## RANSOMWARE– WHAT IT IS

The Cybersecurity and Infrastructure Security Agency defines ransomware as

"...a type of malicious software, or malware, that encrypts data in a computer making it unusable."

The ransomware attacker will demand a ransom, usually through a pop-up message when users try to access data, to unencrypt the data and release it back to the user. The attacker might threaten to sell or leak data that they have collected before encrypting it if the ransom is not paid. They may publicly name and shame victims as a form of extortion. They also have used tactics such as deleting system backups to make restoration and recovery more difficult.

CISA's primary concern about ransomware focuses on computer networks of state, local, tribal, and city governments as well as police and fire departments, hospitals, and other critical infrastructure. It notes that ransomware incidents have been increasing among the nation's state, local, tribal, and territorial governmental entities. One New Zealand cybersecurity firm, Emsisoft, estimates that at least 2,354 U.S. government agencies, healthcare facilities, and schools were attacked by ransomware in 2020.

Emsisoft also estimates that over 1,300 companies, many in the U.S., lost data to ransomware.

Ransomware can interrupt or even stop a business' or organization's operations. Some organization pay the ransom, but this is no guarantee that the data will be restored.

Often small and medium sized businesses and organizations that may not be able to keep up with the latest security threats and prevention techniques can also be targets for ransomware.

A ransomware attack can be conducted through,

- Phishing email
- Malicious attachments in email
- Drive by downloading (a program that is automatically downloaded to your computer without your consent or even your knowledge)

Usually, the attacker demands that payment is made through means, such as bitcoin, that hide their identity.

Ransomware can affect large or small organizations and is often very complicated and difficult to resolve. Businesses may need to hire experts to help them recover their data and return to normal operations.

While preventing ransomware may take expertise at a technical and enterprise level, each worker can be effective in preventing their organization from becoming a victim of ransomware.

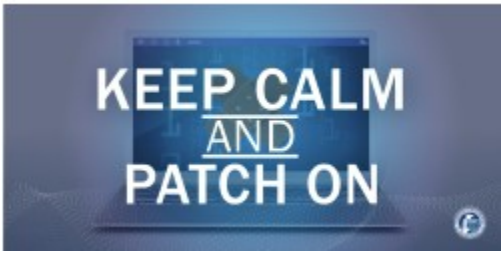
## RANSOMWARE– HOW TO PREVENT IT

Whether you work for a large corporation, or a small or medium sized business, or are an independent contractor, you have an important part to play in preventing ransomware from affecting you and your organization.

CISA makes the following recommendations for organizations and individuals to prevent ransomware,

- **Back up your files.** Backing up your data is the number one thing you can do to prevent ransomware from making your data unusable.


- **Keep backups separate from your computer and network.** Make backups to an external hard drive that can be disconnected from your computer or network.
- **Patch/keep up with security and other updates.** Be sure that your software is set to automatically update itself with the latest security updates.




- **Use Multifactor Authentication.** Use MFA whenever possible. Some cybersecurity professionals say that it can prevent 99% of all attacks.
- **Lookout for Phishing emails.** Be sure that the email sender is genuine. Be careful of clicking on links and attachments in emails. Delete emails that you suspect of being "phishy."
- **Keep up to date.** Inform yourself about the current cybersecurity threats and ransomware techniques. IT departments should have a consistent training program for users on cybersecurity.
- **Organizations should have a ransomware response plan.**

What should you do if your computer is infected with ransomware?

Law enforcement agencies strongly recommend that you DO NOT pay the ransom! Paying does not guarantee that you will get your data back.

**For home users**– Restore your data from your latest backup. Notify the local office of the FBI or Secret Service.

**For organizations** – Immediately notify your IT helpdesk or security office.

**Everyone**– Change all system passwords once ransomware is removed.

## RANSOMWARE- PLEASE REPORT IF YOU ARE ATTACKED

*Your organization should have a plan if it is attacked by ransomware. Part of that plan should be to report the attack to authorities.*

*The FBI encourages ransomware victims to report their experiences even if they were able to quickly recover their files.*

*The FBI is especially interested in knowing about ransomware attacks. It welcomes any information about ransomware attacks to help it understand the nature of the attacks and to hold perpetrators accountable.*

*You can report a ransomware attack to the FBI at.*

*https://www.ic3.gov/Home/Ransomware*

*Or to the Seattle FBI fild office at,*

*(206) 622-0460*

## RANSOMWARE– PREVENTION RESOURCES

The Cybersecurity and Infrastructure Security Agency (CISA) is an excellent resource for information on ransomware. CISA, which is under the Department of Homeland Security, is tasked with improving cybersecurity across all levels of government. It also coordinates cybersecurity programs with the states and it improves the government's cybersecurity protections against private and nation-state hackers.

CISA has extensive resources that can help you learn how to prevent ransomware. The resources can help both IT professionals and the average computer user.

You can find its resources at,

https://www.cisa.gov/ransomware

This article from The Seattle Times talks about a recent ransomware attack on a vendor that affected several local governments and utilities,

https://www.seattletimes.com/seattle-news/hack-of-seattle-payments-firm-puts-local-governments-on-alert/

This posting from the Identity Theft Resource Center gives an overview of ransomware trends,

https://www.idtheftcenter.org/ransomware-attacks-viewed-as-the-top-cybersecurity-threat-in-2021-by-many-experts/


### OFFICE OF NEIGHBORHOODS

**MAKING OUR NEIGHBORHOODS SAFER**

https://www.snohomishcountywa.gov/311/Office-of-Neighborhoods

**Homeless Outreach**-
Sgt. Troy Koster
Phone: (425) 508-8301
Email:
troy.koster@snoco.org

**Nuisance Properties**-
Deputy David Chitwood
Email:
David.Chitwood@snoco.org

**SHERIFF'S OFFICE CRIME PREVENTION WEB PAGE:**

http://www.snohomishcountywa.gov/289/Crime-Prevention

### NEWSLETTER INFO

**EDITOR**
Steve Moller

If you have questions regarding this newsletter or any articles that appear in it, please contact the editor at neighborhoodwatch@snoco.org

### TIP LINES

Snohomish County Sheriff's Office: 425-388-3845

http://snohomishcountywa.gov/303/Anonymous-Tips

Crime Stoppers of Puget Sound: 1-800-222-8477