RANSOMWARE GANGS PROWLING WORLDWIDE

July 2023| Issue 2023:5

THE GROWTH OF RANSOMWARE

The proliferation of ransomware attacks has left organizations scrambling for help. Today, hacker groups—equal in size and sophistication to any S&P 500 company—are operating in pretty much every country around the world. Over the last two years alone, there have been more than 1.1 billion attacks costing corporations $1.2 billion, according to Korn Ferry.

Security researchers have linked the notorious Clop ransomware gang to a new wave of mass-hacks targeting a popular large file transfer tool, MOVEit. MOVEit is widely used by enterprises to share large files over the internet. The vulnerability allows hackers to gain unauthorized access to an affected MOVEit server's database.

Hackers have compromised the personal data of more than 15.5 million individuals and the number of victim organizations continues to grow.

The Clop ransomware gang apparently began following through on an earlier promise to begin posting onto its leak website the names of affected organizations that did not proactively contact it. The named companies include U.S.-based financial services firms, the Departments of Education in Illinois, Minnesota and Missouri and the Oregon Department of Transportation.

The U.S. State Department's **Rewards for Justice** program is offering a reward of up to **$10 million** for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious

RANSOMWARE IS GETTING PERSONAL

The FBI defines "ransomware" as a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom to regain your access. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even clone itself to other networked computers.

Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data, or you see computer messages letting you know about the attack and demanding ransom payments.

Ransomware attacks have become more personal in recent years. Ransomware gangs are now more aggressive against law enforcement. They are able to collect and store more personal information than ever before through advances in surveillance equipment and technologies such as artificial intelligence and facial recognition software. Ransomware attacks have also become more sophisticated and can now target both your data and threaten to destroy your reputation.

A case in point, **Fortune** reports that more than 300,000 personal student files were dumped online in March when Minneapolis Public Schools refused to pay a $1 million ransom. Some of these confidential documents contained deeply personal information about student sexual assaults, hospitalizations, and even suicide attempts.

"Ransomware likely has affected well over 5 million U.S. students by now, with educational institution attacks on track to rise this year," said analyst Allan Liska of the cybersecurity firm Recorded Future. Nearly one in three U.S. school districts had been breached by the end of 2021, according to a survey by the Center for Internet Security, a federally funded nonprofit.

Tips for Avoiding Ransomware

cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA).

Solomon Adote
Chief Security Officer

- Keep operating systems, software, and applications current and up to date.
- Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.
- Back up data regularly and double-check that those backups were completed.
- Secure your backups. Make sure they are not connected to the computers and networks they are backing up.
- Create a continuity plan in case your business or organization is the victim of a ransomware attack.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**