CYBER SECURITY BULLETIN

Protecting your systems from CLOP Ransomware

WHAT IS CLOP RANSOMWARE?	• CLOP is a type of ransomware found by MalwareHunterTeam which runs on Microsoft Windows • CLOP means Bug in Russia and it belongs to CryptoMix Family. It targets the entire network of a system rather than a single computer and is also used as a final payload by the APT group called TA505 • This malware works by encrypting the file and adding the ".clop" extension to the file. Once successfully encrypted, it generates the "ClopReadMe.txt" file and retains its copy in every folder. Also, this file contains the ransom-demand message. • FACT ABOUT CLOP: After stealing 2 million credit card details using a POS malware and threatening a German conglomerate for $23 million, it was recently noticed going after top executives to pressure businesses into paying ransom
HOW IS CLOP RANSOMWARE TRANSMITTED?	• Clop ransomware is transmitted using executables that are digitally signed. A digital signature looks legit and makes it easy to bypass the security detections. It also transmits through infected email attachments (macros), torrent websites, and malicious ads. • It may arrive in one or many arrival methods including the form of infection as illustrated above. Some of the most common behaviors of the Clop ransomware is that it resides in the memory and creates mutual extension object to process termination
HOW DOES THE CLOP RANSOMWARE INFECT SYSTEMS?	• It will first stop most of the Windows services and try to disable antivirus software like Windows Defender and Malwarebytes and close all the files for encryption. • To disable Windows Defender, it configures various registry values which disable behavior monitoring, tamper protection, real time protection, antispyware detection and cloud detection • If Tamper protection is enabled, it tends to reset the Windows Defender. Apart from Windows Defender, it affects older computers by uninstalling Microsoft Security Essentials. As Clop runs with administrative privileges, removing any software becomes an easy task. • By adding the ".clop" extension to the file, the ransomware starts to encrypt the file Clop can terminate a total of 663 processes including new Windows 10 apps, popular text editors, debuggers, programming languages, terminal programs, and programming IDE software. It then creates a batch file named clearnetworkdns_ 11-22-33.bat that executes soon after the ransomware is launched. This batch file disables Windows' automatic startup repair, removes shadow volume copies, and resizes them to clear orphaned shadow volume copies. • Ransom note named ClopReadMe.txt is created by the ransomware. This ransom note contains the emails unlock@eqaltech.su, unlock@royalmail.su, and kensgilbomet@protonmail.com that can be used to contact the attackers for payment instructions. • Recently it has been reported that actor FIN11 is using the Clop ransomware It has been targeting large corporate networks, banks, hospitals, etc • It initially spreads using the Covid-19 theme via sphere phishing. Once the attack is succeeded, it collects the information and shares it to Command-and-

	control server (C&C) of the attacker and demands the ransom.
WHAT IS THE POTENTIAL IMPACT OF A SUCCESSFUL CLOP RANSOMWARE ATTACK?	• Temporary or permanent loss of sensitive and important data • Disruption to regular operations and tasks • Financial losses incurred to restore systems and files which are affected • Potential harm to an organization's reputation
MITIGATION & RESPONSE	• Paying attention while browsing, downloading, or installing any application in the system. • Taking care of Emails and attachments. • Downloading the file from the official source. • Having reputed antivirus/antispyware software active. • If the system is already infected with Clop ransom, then run Malwarebytes for windows to automatically eliminate the ransomware. • Keeping Windows patch up to date. • The blocking of a C2 communication in the midst of an infection chain can stop the infection from spreading. Thus, web filters can be used for such actions. • One of the most important ways to stop any ransomware from entering a system is to have a strong endpoint security solution.