البنك المركزي المصري
CENTRAL BANK OF EGYPT

مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المصرفي
Egyptian Financial Computing Incident Response

Alert Summary

LockBit Ransomware

Alert Summary

⚠	Critical	⚠	High	⚠	Medium	⚠	Informative

Report ID & Issuance Date:	07/2020	**Reported Date:**	03 September 2020
Alert Title:	LockBit Ransomware		
Severity:	⚠	High	
Description:	EG-FinCIRT team detected an ongoing Ransomware campaign that targets the Financial Sector in the region. The mentioned Ransomware named LockBit. LockBit is a file-encryption ransomware that restricts access to data by encrypting files with the "[.] lockbit" extension. The mentioned ransomware is used by various APT's as the author is selling it in the Dark-Web as RaaS (Ransomware As A Service)		
Analysis:	**Initial Access (One of the two below methods may be used)** • The attacker performs a brute force attack on a web server containing an outdated VPN service or RDP. • Phishing Attack. The attacker then uses advanced tools to disable the security defenses of the compromised host with a program masquerading in the user "Appdata" location ("%APPDATA%\svchost[.]exe". The mentioned program will issue the following commands: • "netsh firewall set opmode disable" • "net stop security center" • "net stop WinDefend" **Lateral Movement:** LockBit has a new feature which allows it to spread itself from one computer to other Computers that are connected to the same VLAN. The mentioned ransomware does this by looking for devices on a network by using advanced scanning tools to find other hosts in the same VLAN. When the tool finds a host alive it attempts to connect to it over the Server Message Block Protocol. After successful connection, LockBit runs a PowerShell command that downloads and executes the ransomware.		

Deployment of the Ransomware:

- **The First Scenario:** is a classic hit and run. After gaining access to the initial system, the attacker will log in and deploy the ransomware almost immediately. For the attacker, this was a relatively straightforward process since the ransomware spreads itself. This scenario is used by low skilled attackers and APT's.

- **The Second Scenario:** is a more persistent attack. The ransomware focuses on gaining persistent on the network, exfiltrating sensitive data, deleting backups and finally launching the Ransomware attack. This scenario is used by advanced and high skilled attackers and APT's.

The list of services LockBit tries to stop are:

- DefWatch (Symantec Antivirus)
- ccEvtMgr (Norton AntiVirus Event Manager)
- ccSetMgr (Common Client Settings Manager Service of Symantec)
- SavRoam (Symantec Antivirus)
- sqlserv
- sqlagent
- sqladhlp
- Culserver
- RTVscan (Symantec Antivirus Program)
- sqlbrowser
- SQLADHLP
- QBIDPService (QuickBooksby Intuit.)
- QuickBoooks.FCS (QuickBooksby Intuit.)
- QBCFMonitorService (QuickBooksby Intuit.)
- sqlwriter
- msmdsrv (Microsoft SQL Server Analysis or Microsoft SQL Server)
- tomcat6 (Apache Tomcat)
- zhundongfangyu (this belongs to the 360 security product from Qihoo company)
- vmware-usbarbitator64
- vmware-converter
- dbsrv12 (Creates, modifies, and deletes SQL Anywhere services)
- dbeng8 (Sybase's Adaptive Server Anywhere version 8 database program)
- wrapper (Java Service)

LockBit Persistency Technique

The ransomware maintains the persistency on the compromised host by creating a registry key that will execute the mentioned ransomware every time when the compromised host startups.

Vulnerabilities Exploited:	N/A

Indicators of Compromise (IOCs):	An Excel Sheet named "LockBit IOCs" attached.
Mitigations:	• Enable machine learning, active adversary mitigations and behavioral detection in endpoint security. • If remote access is required, use a VPN with vendor best-practices multi-factor authentication, password audits and precise access control, in addition to actively monitoring remote accesses. • Users logged into remote access services should have limited privileges for the rest of the corporate network. • Administrators should adopt multi-factor authentication and use a separate administrative account from their normal operational account. • Develop and implement a patching policy and baseline configuration standards for operating system. • Conduct cybersecurity awareness training to End- users. • Search for existing signs of the indicated IoCs in your environment. • Block all URL and IP based IoCs at the organization's security devices. • Ensure anti-virus software and associated files are up to date. • Setup an alert on events when AV agent loses the connection with the main panel. • Backup your data using different backup destinations including Tape drives. • Adapt a proper network segmentation and avoid flat network designs.
References:	• EG-FinCIRT