مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

DragonForce Ransomware Campaign

Tracking #:432316331

Date:25-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the DragonForce ransomware group has emerged as a significant threat to organizations, particularly in the Manufacturing, Real Estate, and Transportation sectors.

TECHNICAL DETAILS:

The DragonForce ransomware group has emerged as a significant threat to organizations, particularly in the Manufacturing, Real Estate, and Transportation sectors. Operating as Ransomware-as-a-Service (RaaS) affiliate program, utilizing variants of well-known ransomware families, notably LockBit 3.0 and Conti v3. The group's operations are characterized by the use of double extortion tactics, where they not only encrypt victims' data but also threaten to leak sensitive information if the ransom is not paid. The group has successfully targeted numerous organizations, leveraging stolen credentials, PowerShell scripting, and sophisticated malware like Cobalt Strike and SystemBC.

Tactics, Techniques, and Procedures (TTPs):

Initial Access (T1078 Valid Accounts)
Suspicious Login Activity: The threat actor gained initial access through a public-facing remote desktop server using valid domain accounts. The following timestamps and source IP addresses were identified:
2023-09-21 20:11:08 - 2[.]147[.]68[.]96
2023-09-21 20:40:24 - 185[.]59[.]221[.]75
2023-09-21 22:34:47 - 69[.]4[.]234[.]20
2023-09-22 16:22:56 - 69[.]4[.]234[.]20

Execution (T1059.001 Command and Scripting Interpreter: PowerShell)
PowerShell Commands: PowerShell was used to remotely download and execute a malicious payload, identified as a Cobalt Strike beacon.

Persistence:
Valid Accounts: Domain Accounts (T1078.002): Compromised accounts were used to maintain persistence and move laterally within the organization.

Registry Run Keys / Startup Folder (T1547.001): SystemBC malware created a registry key under "Software\Microsoft\Windows\CurrentVersion\Run" with the name "socks5" to ensure persistence.

Create or Modify System Process: Windows Service (T1543.003): Attempts were made to install services on the system for persistence.

Defense Evasion (T1070.001 Indicator Removal: Clear Windows Event Logs)
Clearing Event Logs: The ransomware executable "df.exe" had the capability to clear Windows Event Logs after encryption to hinder forensic investigation.

Credential Access (T1003.001 OS Credential Dumping: LSASS Memory)
Mimikatz Execution: Mimikatz was used to dump credentials from LSASS memory, resulting in the creation of a file named "123.txt" containing clear text credentials.

Discovery:
Domain Trust Discovery (T1482): ADFind tool was used to gather information about the network's Active Directory.

Remote System Discovery (T1018): Network scanner tool "netscanold.exe" was executed to map out the network.

System Network Configuration Discovery (T1016): The attacker collected information about the network configuration.

System Information Discovery (T1082): General system information was gathered.

File and Directory Discovery (T1083): The attacker searched for specific files and directories.

Lateral Movement (T1021.001 Remote Services: Remote Desktop Protocol)
RDP Connections: The attacker used RDP to move laterally within the network after gaining initial access.

Command and Control (T1071.001 Application Layer Protocol: Web Protocols)
Cobalt Strike Beacons: C2 communication was established using the HTTP protocol with the address 185[.]73[.]125[.]8.
SystemBC Malware: An additional C2 address associated with SystemBC malware was identified as 94[.]232[.]46[.]202.

Impact (T1486 Data Encrypted for Impact)
Ransomware Execution: The malicious executable "df.exe" was deployed to encrypt files across the network.

Indicators of Compromise(IOCs):

IPs
185[.]73[.]125[.]8
94[.]232[.]46[.]202
69[.]4[.]234[.]20
2[.]147[.]68[.]96
185[.]59[.]221[.]75
SHA256
df903c620508011ca8eb2aaaf9712a526b31a12c800b856cd524ebb3fde854b2
55befb5de5d9bc45978efd1a960ae21ed81e4be9c6521aaeebf8d5884444e3c9
572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b
MD5
C111476F7B394776B515249ECB6B20E6

RECOMMENDATIONS:

- Strengthen Access Controls: Implement multi-factor authentication (MFA) and regularly review and update access controls to prevent unauthorized access.
- Monitor and Secure Remote Desktop Services: Ensure that Remote Desktop Protocol (RDP) is properly secured and monitored to detect and prevent unauthorized access.
- PowerShell Execution Controls: Apply execution policies and controls to restrict the use of PowerShell and other scripting languages that can be used for malicious purposes.
- Endpoint Detection and Response (EDR): Deploy EDR solutions to detect and respond to suspicious activities and malware execution.
- Regular Security Audits and Patch Management: Conduct regular security audits and ensure timely patch management to address vulnerabilities that could be exploited by ransomware groups.
- Employee Training and Awareness: Educate employees about the risks of phishing, the importance of strong passwords, and the proper handling of sensitive information.
- Backup and Recovery: Regularly back up critical data and ensure the ability to recover quickly in the event of a ransomware attack.
- Incident Response Plan: Develop and regularly update an incident response plan to effectively respond to and recover from ransomware attacks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.group-ib.com/blog/dragonforce-ransomware/?utm_source=twitter&utm_campaign=Dragonforce%20Ransomware&utm_medium=social