Threat Intelligence Report

Threat's : As general findings, threats are focused on bypassing authentication control by sending customized packets to Remote Services and Public Applications systems by impersonating other systems or services. In the command execution phase, malicious shell code execution methods are applied in the shell through various vulnerabilities. For authorization escalation, dll injections come to the forefront. In addition, backdoors and system scheduled tasks are often used to ensure persistence, and sometimes exploiting open ports is preferred. As a security bypass, it disguises itself as one of the system services to avoid attracting attention and creates a balanced traffic on the network. Common targets are theft of data to be used for various reasons and ransomware attacks. However, data manipulation and project sabotage have also been seen from time to time.

Affected Products: System firewall devices, Network management systems, Email services, FTSP services, Database servers

MITRE ATT&CK Matrix:

Initial Access:

Exploit Public-Facing Application(T1190)
External Remote Services(T1133)
Content Injection(T1659)

Execution:

Command and Scripting Interpreter(T1059)
Exploitation for Client Execution(T1203)
System Services: Service Execution(T1569.002)

Persistence:

Boot or Logon Autostart Execution: Port Monitors(T1547.010)
Boot or Logon Initialization Scripts: Startup Items(T1037.005)
Create or Modify System Process(T1543)
Hijack Execution Flow(T1574)

Defense Evasion:

Direct Volume Access(T1006)

BITS Jobs(T1197)

Access Token Manipulation(T1134)

Traffic Signaling(T1205)

System Script Proxy Execution(T1216)

System Binary Proxy Execution(T1218)

Hide Artifacts(T1564)

Exfiltration:

Scheduled Transfer(T1029)

Data Transfer Size Limits(T1030)

Automated Exfiltration(T1020)

Impact:

Data Destruction(T1485)

Financial Theft(T1657)

Endpoint Denial of Service(T1499)

Data Manipulation(T1565)

Data Encrypted for Impact(T1486)

Mitigations:

- Setting up applications to work with sandbox.

- Filtering network operations

- Use security systems that monitor network traffic

- Vulnerability scans should be performed regularly

- Installing the latest updates of apps

- Disabling unused features and applications

- Limit user authorizations in detail

- Closing unused ports

- Use firewalls whose protocols are regularly updated to keep up to date.

- Encrypting important information

- Using two-step verification

- Take regular data backups.

- Limiting authorizations for file operations.

- Using security systems that instantly monitor movements in the system.

- Informing and training employees about cyber threat

IOC'S:

- System logs

- Network log records

- Registry entries

- File paths inside the system

- Abnormal system tools or applications

Github repository:

https://github.com/umutsertkaya/CTI_Project_Team_My_Progress