مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Ghost (Cring) Ransomware Threat

Tracking #:432316889

Date:20-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers reported Ghost actors have been conducting widespread ransomware attacks since early 2021, targeting organizations across more than 70 countries, including critical infrastructure, healthcare, education, government, and small- to medium-sized businesses.

TECHNICAL DETAILS:

Ghost actors have been conducting widespread ransomware attacks since early 2021, targeting organizations across more than 70 countries, including critical infrastructure, healthcare, education, government, and small- to medium-sized businesses.

Ghost actors exploit known vulnerabilities in internet-facing systems, particularly in outdated software and firmware, to gain initial access to victim networks. They deploy ransomware payloads such as **Cring.exe**, **Ghost.exe**, **Elysium0.exe**, and **Locker.exe**, which encrypt files and demand ransom payments in cryptocurrency. Ghost actors frequently rotate their ransomware payloads, modify ransom notes, and use multiple email addresses for communication, making attribution challenging.

This advisory provides detailed Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), and recommended mitigations to help organizations defend against Ghost ransomware attacks.

MITRE ATT&CK Tactics:

Phase	Technique	Description
Initial Access	Exploit Public-Facing Applications (T1190)	Exploits vulnerabilities (CVE-2018-13379, CVE-2010-2861, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
Execution	PowerShell & Command Shell (T1059)	Deploys Cobalt Strike via scripts
Persistence	Web Shell (T1505.003), Account Manipulation (T1098)	Creates new accounts & installs backdoors
Privilege Escalation	Token Impersonation (T1134), Exploitation (T1068)	Uses SharpZeroLogon, BadPotato, and GodPotato tools
Credential Access	OS Credential Dumping (T1003)	Uses Mimikatz and Cobalt Strike hashdump
Defense Evasion	Disable Security Tools (T1562.001)	Disables Windows Defender & antivirus
Discovery	Network & Remote System Discovery (T1135, T1018)	Uses SharpShares, Ladon 911, and SharpNBTScan
Lateral Movement	Remote Execution (T1047, T1132.001)	Uses WMIC & PowerShell commands

Exfiltration	Data Transfer Over C2 (T1041, T1567.002)	Uses Cobalt Strike & Mega.nz for limited data exfiltration
Command & Control	C2 Over Web Protocols (T1071.001)	Uses HTTP(S) for encrypted communication
Impact	Data Encryption for Ransom (T1486)	Encrypts files, deletes shadow copies (T1490)

Indicators of Compromise (IOC):
Attached File

RECOMMENDATIONS:

1. **Maintain Regular Backups**:
   - Ensure backups are stored offline or in a segmented network to prevent encryption by ransomware.
   - Regularly test backups to ensure they can be restored in the event of an attack.
2. **Patch Known Vulnerabilities**:
   - Apply timely security updates to operating systems, software, and firmware.
   - Prioritize patching for exploited vulnerabilities by Ghost actors.
3. **Segment Networks**:
   - Implement network segmentation to restrict lateral movement within the network.
   - Limit access to critical systems and data.
4. **Require Phishing-Resistant Multi-Factor Authentication (MFA)**:
   - Enforce MFA for all privileged accounts and email services.
   - Use phishing-resistant MFA methods such as FIDO2 or hardware tokens.
5. **Monitor and Limit PowerShell Usage**:
   - Monitor for unauthorized use of PowerShell, which Ghost actors frequently leverage for malicious purposes.
   - Implement allowlisting for PowerShell scripts and commands.
6. **Enhance Email Security**:
   - Implement advanced email filtering to block malicious attachments and phishing attempts.
   - Enable DMARC, DKIM, and SPF to prevent email spoofing.
7. **Disable Unused Ports and Services**:
   - Disable unused ports such as RDP (3389), FTP (21), and SMB (445).
   - Restrict access to essential services through securely configured VPNs or firewalls.
8. **Train Employees on Phishing Awareness**:
   - Conduct regular training sessions to help employees recognize and report phishing attempts.
9. **Implement Allowlisting**:
   - Use application allowlisting to prevent unauthorized execution of scripts and programs.
10. **Monitor for Unusual Network Activity**:
    - Identify and investigate abnormal network traffic, such as unusual scans, commands, or scripts.
    - Use intrusion detection systems (IDS) and security information and event management (SIEM) tools to detect potential threats.

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.cisa.gov/sites/default/files/2025-02/aa25-050a-stopransomware-ghost-cring-ransomware.pdf