

JANUARY 2025 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats within the cyber landscape. We are excited to share our most recent Monthly Bulletin to cover the most prominent security incidents over the past month and discuss new Digital Forensics and Incident Response measures used by both adversaries and security professionals.

Key Takeaways

- Attackers employed various techniques, including phishing, vulnerability exploitation, and registry modifications, to deploy RATs and maintain unauthorized control over the system.
- Proactive monitoring of mshta.exe, PowerShell scripts, and registry entries, along with endpoint detection tools, are essential for detecting and mitigating these types of attacks.
- Black Basta actors are using Microsoft Teams and social engineering to gain remote access and deploy ransomware.



Case Study

Investigation into Remote Access Tool Installation and Persistence Mechanisms

In December, the CyberForce|Q Security Operations Center (SOC) detected multiple attacks involving mshta.exe. This case study outlines the investigation of an alert where attackers used various techniques to install remote access tools (RATs) and establish persistence on a compromised system. These activities were uncovered through analysis of suspicious behaviors such as the use of mshta.exe, PowerShell, code obfuscation, and registry modifications. The SOC quickly contained the threat to limit potential damage.

Alert Discovery

The investigation began when the security monitoring system flagged unusual activity on an internal host. A review of the process tree revealed mshta.exe, a legitimate Microsoft tool, executing with a suspicious URL indicating potential delivery of a malicious payload. Further analysis uncovered additional signs of compromise, including obfuscated PowerShell commands and attempts to install RATs, signaling an attacker's effort to gain unauthorized control.

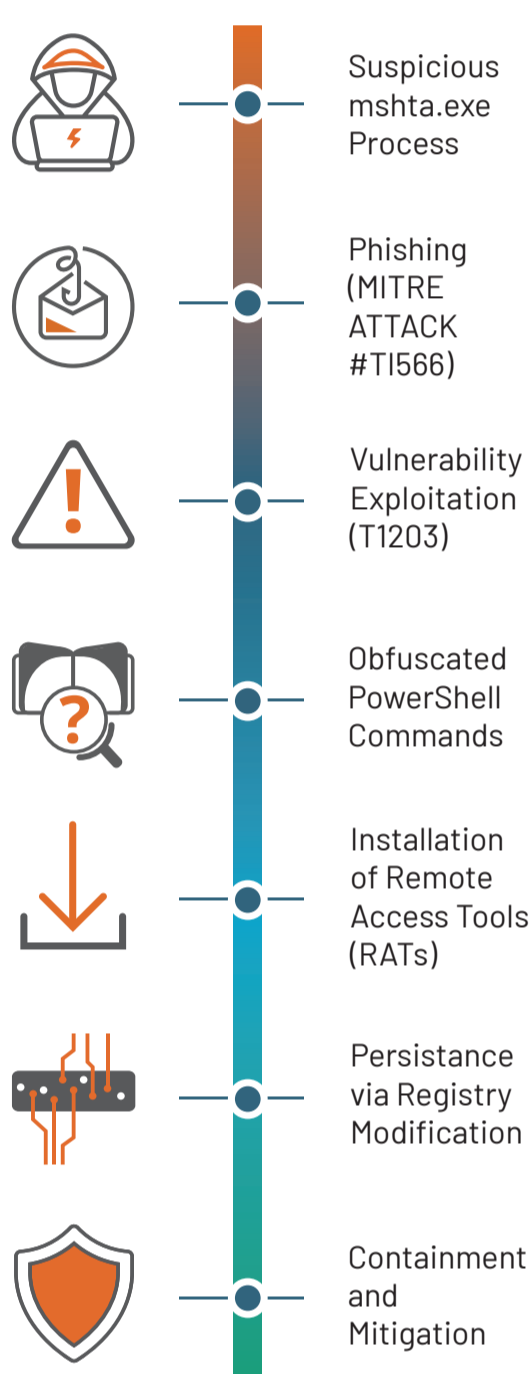
Attack Timeline and Techniques

The attack sequence begins with the exploitation of the mshta.exe process, which initiates a connection to a suspicious URL that points to a remote server. This step likely serves as a vector for delivering further exploits or payloads, compromising the system at a deeper level. The initial entry point into the environment is likely facilitated through phishing or the exploitation of vulnerabilities. Specifically, spearphishing techniques involving malicious attachments, such as HTML Application (HTA) files, are often used in conjunction with mshta.exe to trigger the attack sequence (MITRE ATT&CK T1566). Additionally, the exploitation of existing vulnerabilities (T1203) in software or system configurations may allow attackers to leverage mshta.exe to download and execute secondary payloads, such as remcmdstub.exe and client32.exe, which deploy NetSupport, a remote access tool (RAT).






Once inside, the adversary executes obfuscated PowerShell scripts designed to evade detection, a common tactic to bypass security monitoring and analysis tools. The obfuscation ensures that these malicious scripts remain difficult to analyze and identify as they install the RATs and establish footholds within the network. The two RATs, remcmdstub.exe and client32.exe, are used to facilitate remote access, enabling the attacker to maintain control over the system for surveillance, data exfiltration, or further lateral movement. To ensure persistence, the attacker modifies the system's registry, specifically targeting startup keys (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run) to execute the RATs automatically upon system reboot, a technique classified under Registry Run Keys/Startup Folder (T1547).

In response, the Security Operations Center (SOC) swiftly isolates the affected host from the network to prevent further communication with command-and-control (C2) servers and mitigate the risk of data exfiltration. A comprehensive forensic analysis of the compromised system, focusing on processes, registry modifications, and file integrity, ensures that all traces of the attacker's activity are eradicated. This proactive approach to containment, along with the removal of any persistence mechanisms, is critical in preventing reinfection and ensuring the security posture of the network is restored.

ATTACK TIMELINE



Recommendations

-  **Proactive Detection:** Security systems should monitor mshta.exe and PowerShell for suspicious behavior, especially with obfuscated code or unusual commands, to detect attacks earlier. Block mshta.exe if it's not essential for business purposes.
-  **PowerShell Security:** PowerShell scripts should be monitored closely, with suspicious or unauthorized scripts flagged. Application whitelisting and restricted execution policies reduce the risk of PowerShell-based attacks.
-  **Persistence Mechanisms:** Regular audits of critical registry entries may help prevent persistent attempts through registry modifications.
-  **Remote Access Tool Detection:** Regular vulnerability scans and endpoint detection tools are crucial to identifying and removing RATs from compromised systems.
-  **Incident Containment and Communication:** Swift containment and clear communication between security teams and stakeholders minimize the impact of an attack.





External Trend

Increase in Black Basta Ransomware Using Social Engineering

Black Basta attackers have been observed using Microsoft Teams to impersonate IT help desk staff. They begin by sending large amounts of subscription-based emails and follow up with phone calls, offering support to victims overwhelmed by the email influx.

The attackers then convince victims to grant remote access through Microsoft's Quick Assist tool. Once inside, they execute cURL commands to download malicious batch/ZIP files, which deploy payloads such as EvilProxy, ScreenConnect, NetSupport, or Cobalt Strike. These tools enable the attacker to establish persistence, enumerate the domain, harvest credentials, and move laterally, ultimately deploying Black Basta ransomware.

Recommendations

-  **Block Quick Assist's online version at <https://remoteassistance.support.services.microsoft.com/>**
-  **Disable Quick Assist via Group Policy or uninstall using PowerShell**
-  **Ensure Endpoint Detection and Response (EDR) software is installed on all endpoints**
-  **Educate end users on security best practices**

How CyberForce|Q Can Help

For 29 years, CyberForce|Q has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForce|Q, in collaboration with our participants, is protecting the cyber realm.

Contact Us For More Information
248-837-1400 • solutions@cyberforceq.com

