United States Secret Service [INFO]

6/12/2020

[INFO] Information Only Alert – GIOC Reference #20-032-I
TLP Green

Compromised Managed Service Providers

The United States Secret Service is continuing to see an increase in cyber related attacks involving compromised Managed Service Providers (MSP). A MSP is a company that provides management services for a customer's IT infrastructure using remote administration tools. Due to the fact a single MSP can service a large number of customers, cyber criminals are specifically targeting these MSPs to conduct their attacks at scale to infect multiple companies through the same vector.

MSPs utilize multiple open source and enterprise software applications in the facilitation of remote administration. In the event of an MSP compromise, these applications are often used by bad actors to access their customer's networks and conduct attacks.

Cyber criminals are leveraging compromised MSPs to conduct a variety of attacks including point-of-sale intrusions, business email compromise (BEC), and specifically ransomware attacks.

Best practices for MSPs

- Have a well defined service level agreement
- Ensure remote administration tools are patched and up to date
- Enforce least privilege for access to resources
- Have well defined security controls that comply with end users regulatory compliance
- Perform annual data audits
- Take into consideration local, state, and federal data compliance standards
- Proactively conduct cyber training and education programs for employees

Best practices for MSP Customers

- Audit Service Level Agreements
- Audit remote administration tools being utilized in your environment
- Enforce two-factor authentication for all remote logins

GLOBAL INVESTIGATIVE OPERATIONS CENTER
WASHINGTON, D.C.

[INFO] - Indicates informational or educational content.

- Restrict administrative access during remote logins
- Enforce least privilege for access to resources
- Utilize a secure network and system infrastructure, capable of meeting current security requirements
- Proactively conduct cyber training and education programs for employees

For any additional information or questions related to this alert, the GIOC can be contacted at GIOC@usss.dhs.gov.

[INFO] - Indicates informational or educational content.