BLACKFOG™

A Guide to MSP Cybersecurity:

TOP 6 PRACTICES TO MITIGATE RANSOMWARE RISKS



Contents

Overview 3

1. MSPs - Prime Targets 4

2. Recent High-Profile MSP Ransomware Incidents 5

3. 6 Best Practices To Mitigate Ransomware 7

Get Protection From Ransomware With BlackFog 14

This guide explores the top 6 practices Managed Service Providers (MSPs) should follow to reduce the risks of ransomware. It emphasizes the importance of securing remote access, restricting network access, training employees on cybersecurity, integrating an anti data exfiltration (ADX) solution and having a comprehensive plan for responding to incidents.

1

MSPs – Prime Targets

Managed Service Providers (MSPs) are becoming prime targets for cybercriminals, particularly those who use ransomware.

The recent lawsuit against an MSP for failing to protect a Sacramento law firm from Black Basta emphasizes the importance of implementing cybersecurity measures to stop ransomware. MSP networks are attractive targets for cybercriminals because they provide access to large amounts of customer data. Their widespread use and direct access to customer networks increases the risk of vulnerabilities spreading and being exploited quickly.

2

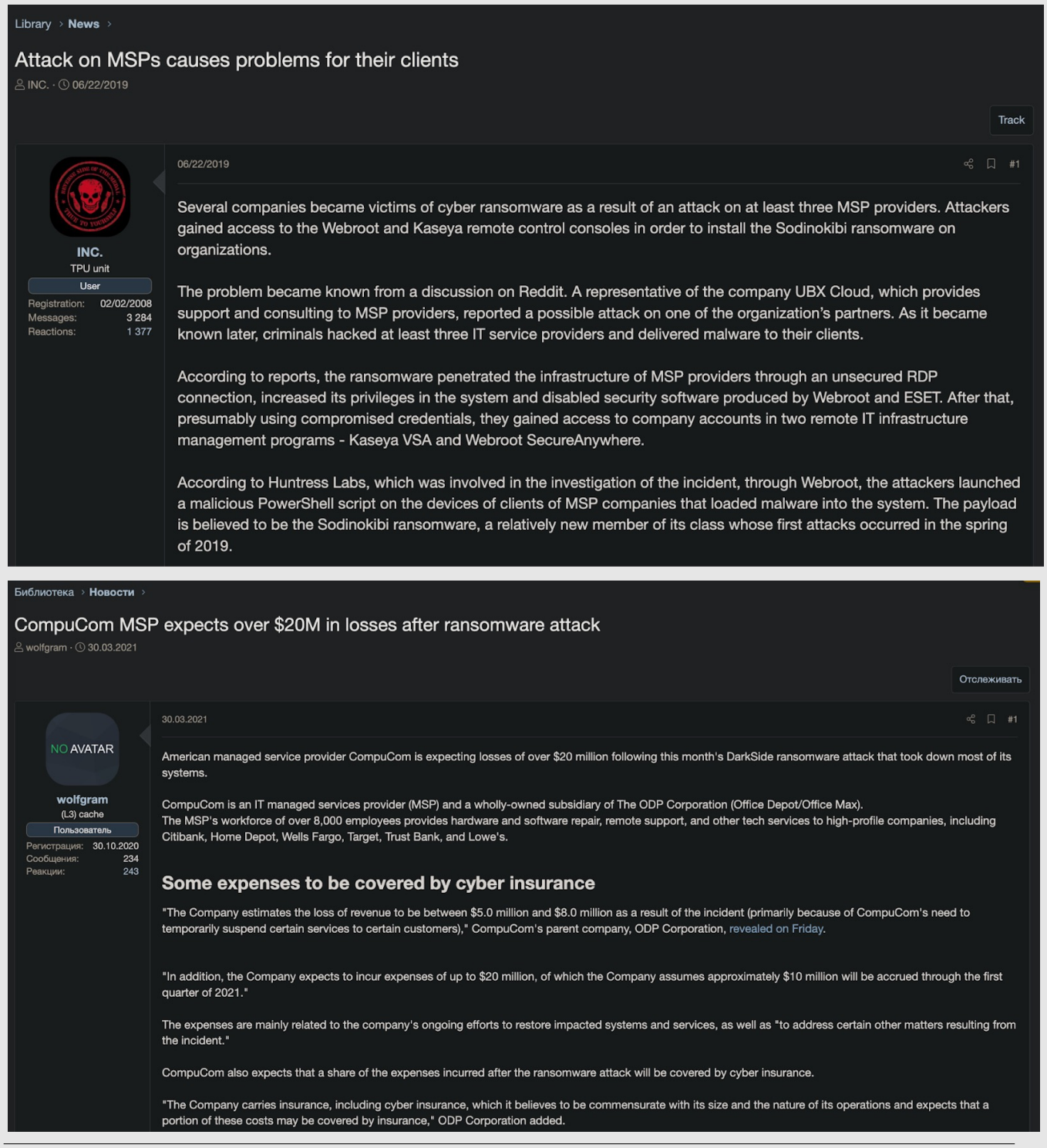
Recent High-Profile MSP Ransomware Incidents

Before diving into the best practices, let's examine some high-profile ransomware incidents that have impacted MSPs in recent years:

1. The CompuCom Incident: In March 2021, CompuCom, an American MSP and a wholly-owned subsidiary of The ODP Corporation (Office Depot/Office Max), was hit by a DarkSide ransomware attack that took down most of its systems. The company estimated a loss of revenue between $5 million and $8 million and expects to incur expenses of up to $20 million as a result of the incident.
2. The BOLDMOVE Attack: In October 2022, a threat actor believed to have ties to China carried out a cyberattack known as the BOLDMOVE attack. This attack targeted a Fortinet FortiOS SSL-VPN vulnerability and utilized malware called BOLDMOVE. An African MSP and a European government were the attack's primary targets.
3. The Kaseya Breach: In July 2021, Kaseya experienced a significant ransomware attack that targeted its VSA software, impacting MSPs and their clients worldwide. This attack highlighted the far-reaching consequences of supply chain vulnerabilities and was briefly described by the FBI as a supply chain ransomware attack. The ransomware was cleverly disguised as a fake software update, allowing it to rapidly spread and encrypt not only the systems of MSPs but also those of their clients.

Cybercriminal Discussions About MSP Attacks

The high-profile incidents mentioned have not gone unnoticed by cybercriminal communities. Cybercrime forums and networks often feature discussions where cybercriminals openly share information about successful attacks on MSPs and the financial losses incurred by both the MSPs and their clients.



The images above showcase two examples of cybercriminals sharing details about multiple attacks on MSPs. Unfortunately, these discussions are quite frequent on forums and networks, highlighting the ongoing interest in targeting MSPs among cybercriminal groups.

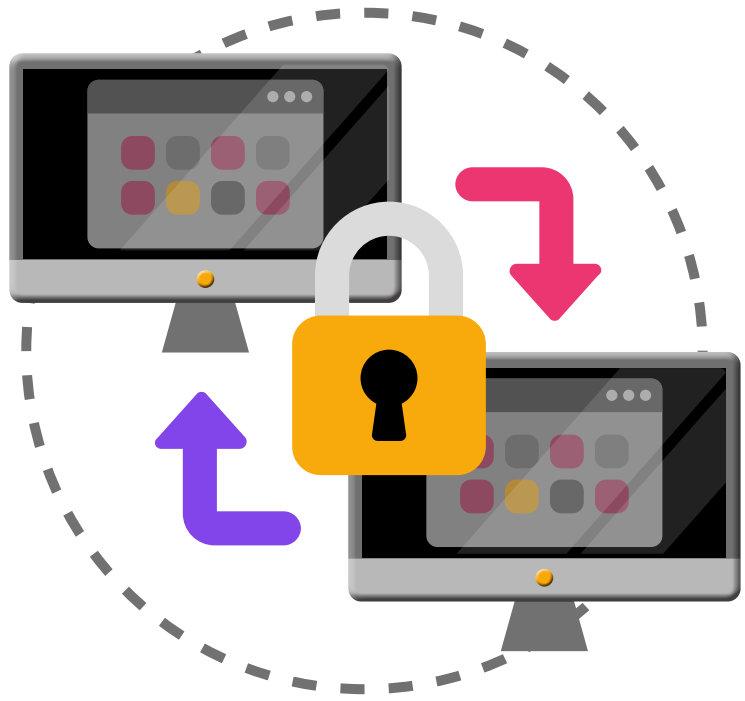
3

6 Best Practices To Mitigate Ransomware

Moving on, we will now explore the top 6 best practices that MSPs should implement to mitigate the risks posed by ransomware and protect their own networks as well as their clients' assets.

These best practices include securing remote access tools, restricting network access, disabling PowerShell if it's not in use, conducting regular employee training, integrating an anti data exfiltration solution (ADX), and developing an effective incident response plan.

Best Practice #1
Secure Remote Access Tools



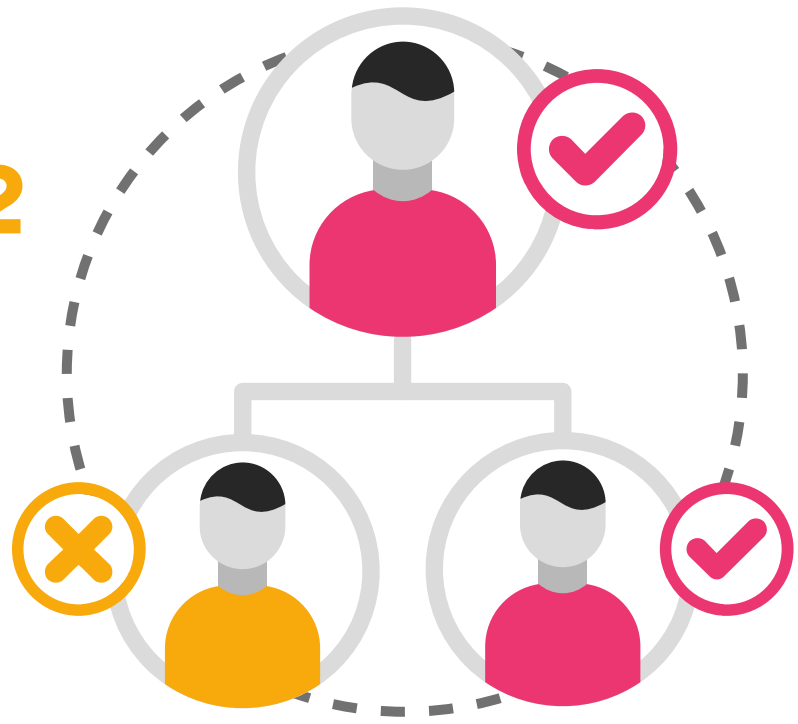
blackfog.com

Firstly, securing remote access tools is crucial for MSPs to prevent unauthorized access to their networks and their clients' systems.

To achieve this, MSPs should require multi-factor authentication (MFA) for all remote access tools, such as Remote Desktop Protocol (RDP), Virtual Private Networks (VPNs), and remote support software. MFA adds an additional layer of security by requiring users to provide a second form of authentication, such as a one-time password or biometric data, in addition to their login credentials.

Best Practice #2
Restrict Network Access

blackfog.com



Secondly, restricting network access is essential to limit the spread of potential ransomware infections within an MSP's network.

To achieve this, MSPs should implement network segmentation based on the principle of least privilege, granting users and devices access only to the resources they need to perform their roles. Firewalls, access control lists (ACLs), and virtual LANs (VLANs) can be used to enforce network segmentation and restrict communication between different network segments.

Best Practice #3
Disable PowerShell If Unused



blackfog.com

Thirdly, PowerShell, a scripting language built into Windows, is often exploited by ransomware attackers for various stages of their attacks, such as reconnaissance and lateral movement.

If PowerShell is not required for business operations, MSPs should consider disabling it on systems to reduce the attack surface. However, if PowerShell is necessary, strict controls should be implemented around its use, such as limiting execution to specific users or requiring script signing to ensure only approved scripts can run.

Best Practice #4
Issue Regular Employee Training

blackfog.com



Fourthly, employees play an important role in preventing ransomware attacks, as they are often targeted through social engineering techniques like phishing.

To mitigate this risk, MSPs should provide regular cybersecurity awareness training to all employees, covering topics such as identifying phishing emails, safe browsing, and proper password hygiene. Training should be engaging, relevant, and tailored to the specific roles and responsibilities of different employee groups.

Best Practice #5
Implement Anti Data Exfiltration (ADX)



blackfog.com

Fifthly, MSPs should consider implementing an ADX solution as part of their cybersecurity stack.

ADX generally works by investigating outgoing data on endpoint devices, providing a more lightweight and targeted approach compared to traditional data loss prevention (DLP) solutions. By focusing on user behavior and limiting the ability of all users, including privileged accounts, to send sensitive data outside the network, ADX can effectively prevent data exfiltration and double extortion ransomware attempts.

Best Practice #6
Develop An Incident Response Plan



blackfog.com

Sixthly, having a well-defined and tested incident response plan is essential for MSPs to effectively respond to a ransomware attack.

The plan should outline the steps to be taken in the event of an attack, including containment, eradication, and recovery procedures, and assign clear roles and responsibilities to incident response team members. Regular testing of the plan through tabletop exercises and simulated attacks can help identify gaps and areas for improvement, allowing the plan to be updated based on the results.

Get Protection From Ransomware With BlackFog

In recent years, double extortion ransomware attacks have become increasingly prevalent, exacerbating the risks faced by MSPs and their clients. Double extortion involves attackers not only encrypting data but also exfiltrating sensitive information before encryption, enabling them to threaten public release or sale of the stolen data if the ransom is not paid.

BlackFog provides a comprehensive solution to help MSPs prevent ransomware, safeguard their clients' valuable data, and mitigate the risks associated with extortion. BlackFog's anti data exfiltration (ADX) technology stops ransomware in its tracks by preventing unauthorized data transmission from infected devices, effectively neutralizing the threat.

As an MSP, implementing BlackFog can enhance your cybersecurity offerings, differentiate your services from competitors, and provide your clients with peace of mind knowing their data is protected against the growing threat of ransomware and double extortion attacks.

If this sounds interesting to you, contact us today for a demo and discover how BlackFog can help you stay ahead of data exfiltration and ransomware threats.

BLACKFOG™

ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

All contents copyright © 2024 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.
