




CYBERATTACK REPORT No.3

Periwinkle Tempest remote ransomware attack


Patch me if you can

Ransomware attacks have become a significant threat to businesses and organizations worldwide, causing disruption to operations and reputational damage as a result of data exfiltration. In recent years, ransomware has moved from a model where a single bad actor would both develop and distribute a ransomware payload to a ransomware as a service (RaaS) model. RaaS allows one group to manage the development of the ransomware payload and provide services for payment and extortion via data leakage. That group then passes the leaked data to other cybercriminals who launch the ransomware attacks for a cut of the profits. This industrialization of cybercriminal tooling has increased the number of attackers and made it easier for them to perform intrusions, exfiltrate data, and deploy ransomware. We know that 93% of ransomware engagements seen by [Microsoft Incident Response](#) (Microsoft IR) revealed insufficient controls on privileged access and lateral movement.¹ So in this third part of our Cyberattack series, we share how the Microsoft IR team helped a customer deal with a recent ransomware attack, and how expert guidance can help limit the impact of an active ransomware threat.


> Ransomware attack flow


> What happened?

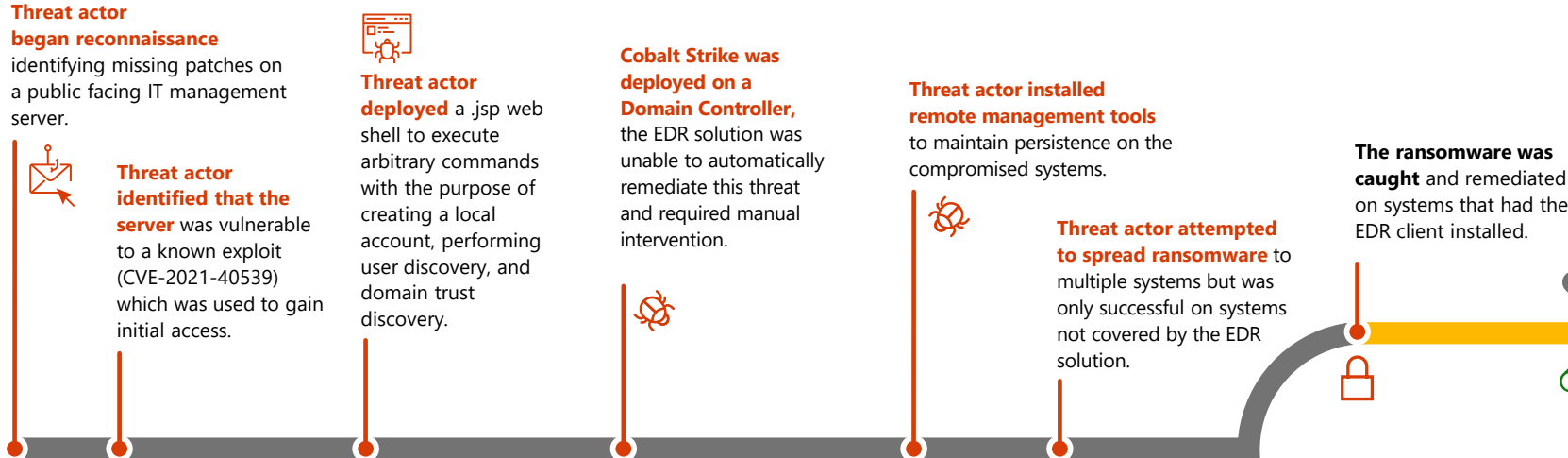

> How did Microsoft respond?


> How should other customers prepare?



Periwinkle Tempest is one of the most prolific threat actor groups active today that encompasses multiple other groups, including operators, developers and management of several of the most impactful Ransomware as a service (RaaS) and backdoor ecosystems.

Attack flow



Microsoft Incident Response Post-Event

Investigation began by deploying forensic tools across the environment.

Reverse Engineering of the web shell determined that it had the ability to perform file uploads, run arbitrary PowerShell commands and list directories.

Wide deployment of EDR system to remaining systems in the environment to increase visibility.

Active Directory hardening to reduce highly privileged accounts and reduce additional attack vectors.

Worked with the customer to highlight the importance of the investigation which identified opportunities for additional remediation activities.

Raised awareness on how to improve overall security, including prioritization of patch management.

The ransomware was able to execute and encrypt the systems that were not protected by the EDR solution.

EDR solutions prevent ransomware by detecting and blocking malicious activity, identifying suspicious behavior, and can contain or automatically remediate threats.





What happened?

The Microsoft Incident Response team engaged with a customer who had fallen victim to a ransomware attack. Upon investigation, it was determined that the threat actor had gained initial access to the environment through a public-facing server hosting an instance of third-party IT management system. Unfortunately, the server had not been patched for a significant period, allowing the threat actor to leverage an exploit for a known vulnerability (CVE-2021-40539) to gain access to the server. The threat actor was then able to deploy a web shell which provided them with a beachhead into the environment. With this web shell the threat actor was able to execute arbitrary commands with the purpose of creating local accounts, performing user discovery, and domain trust discovery.

The actor was then observed deploying tools to the environment to support lateral movement and to aid in maintaining persistence. A combination of common penetration testing tools such as Cobalt Strike, Mimikatz, and SharpHound were observed — in addition to remote access tools such as ScreenConnect, AnyDesk, and Itarian.

During the intrusion, the attacker was able to gain access to a Domain Controller and extract the NTDS.dit database of Active Directory, allowing them access to privileged credentials — and subsequently — gain positive administrative control over the environment.

One week later, the threat actor attempted to deploy ransomware across multiple systems. Fortunately, the organization's EDR solution was able to detect the malicious activity and isolate the affected systems using the built-in quarantine feature. The customer's prompt response effectively minimized the impact, confining it to just 8 servers in the environment.

68%



of organizations impacted by ransomware

did not have an effective vulnerability and patch management process, and many had a high dependence on manual processes versus automated patching capabilities.¹



How did Microsoft respond?

Microsoft IR took swift action to help the customer contain the ransomware attack and regain positive administrative control of the environment. Through identification of compromised accounts, persistence mechanism, and tooling leveraged by the threat actor, they were able to support the customer in coordination of containment actions. Identifying the primary entry point into the network—which was through the unpatched third-party IT management system—Microsoft IR was able to effectively eliminate the threat actor's foothold within the environment by taking the affected server offline.

The Microsoft IR team quickly deployed forensics tools across the customer's environment to gain more insight into the attack. Analysis of the logs collected confirmed that the threat actor was leveraging a Remote Code Execution Vulnerability (RCE) in the IT management system to deploy a web shell. Upon discovering this, Microsoft IR was able to reverse engineer the web shell which revealed that it contained the ability to perform file uploads, run arbitrary PowerShell commands, and list directories.

Additionally, Microsoft IR provided guidance on patch management and privileged access management best practices to reduce the likelihood of the actor re-establishing access and to reduce the likelihood of future attacks. The team worked with the customer to harden their Active Directory environment and to reduce highly privileged accounts which would reduce additional attack vectors.

Microsoft IR also worked with the customer to rapidly deploy their endpoint detection and response (EDR) solution to gain wider visibility across the network. While working to deploy their EDR solution, Microsoft helped the customer to proactively clean up and remove any remnants of malware from their systems. Then, they worked with the customer to provide "lessons learned" guidance on what went well and what could be improved in the future. These recommendations included enabling MFA (multifactor authentication), increased asset management, more robust patching, wider EDR coverage, and security of highly privileged accounts.



How can organizations prevent more ransomware attacks?



Multi-factor authentication (MFA)



Frequent security patches and a patch management process



Zero Trust principles across network architecture





How should other customers prepare?

This incident highlights the importance of proactive security measures and the need for expert guidance when dealing with ransomware attacks. Here are some key takeaways for customers to help them prepare for similar incidents:



1. Secure Identity Infrastructure

The threat actor had full control over the customer's identity infrastructure, which is why it is essential to secure the identity infrastructure by implementing privileged access management (PAM) solutions. PAM solutions allow customers to monitor and manage privileged accounts, ensuring that only authorized personnel have access to critical systems and data.

Microsoft IR performed the following containment actions:

- Reset passwords for the existing Domain & Enterprise admins immediately in all domains.
- Removed the metadata of the DCs which were identified malicious and isolated.
- Ensured replication with the Primary Domain Controller was functioning, in preparation for a KRBTGT reset.
- KRBTGT reset.
- Review of excessive permission on the Domain Root, such as AdminSD Holder.
- Remediated the null password attributes on users and groups.
- Remediated the high privilege group memberships by removing unnecessary, disabled and compromised accounts.
- Disabled SMBv1 and the print spooler on all DCS.
- Remediated the privileges on the Domain Controllers (user rights assignment).



Patch it or catch it!

5 proactive measures customers can take to better prevent and prepare for security incidents

- 1 Secure your identity infrastructure
- 2 Review overprivileged accounts
- 3 Revisit patch management
- 4 Strengthen remote access management
- 5 Engage expert guidance





2. Overprivileged Accounts

The threat actor in this case was able to gain privileged administrative control over the customer's environment, highlighting the need to limit the number of privileged accounts and ensure that they are only granted to authorized personnel who need them. Customers should establish a privileged access policy and regularly review their privileged access policies and remove any unnecessary accounts or permissions.



3. Patch Management

The customer's lack of effective patch management allowed the threat actor to gain initial access to their environment through a known vulnerability. Regular patching of systems, applications, and devices is critical to reducing the risk of exploitation by threat actors.

Organizations can improve their security posture by using a layered security approach, implementing [Windows Defender Application Control \(WDAC\)](#), using a centralized patch management system, creating a patch management policy, testing patches before deployment, and monitoring the results of patch deployments.



4. Application Control

The threat actor deployed various remote access tools to establish persistence in the customer's environment, highlighting the need to implement strong remote access management policies. Customers should restrict remote access to critical systems and data, use multi-factor authentication, and monitor remote access sessions for suspicious activity.



5. Expert Guidance

Ransomware attacks can be complex and challenging to deal with, and customers need expert guidance to ensure that they respond effectively. Customers should engage with incident response experts to develop a comprehensive incident response plan and ensure that security personnel are trained to respond to ransomware incidents.

- **Compromise Assessment** - Receive a point-in-time, deep analysis of your environment, including proactive investigation for persistent threats and security risks.
- **Incident Response** - Get global investigation and guidance all day, every day, to help evaluate incident scope, contain attacks, and restore critical systems, with options for onsite and remote.



Conclusion

As we've seen in recent years, the most common breaches often exploit lapses in everyday maintenance of basic security controls. Many ransomware attacks like this one can be prevented—or at least made more difficult—through regular review and hardening of controls, which starts with a clear picture of your organization's ever-changing identity infrastructure. But when an attack strikes, Microsoft's Incident Response experts follow a demonstrated methodology that has been repeated and refined worldwide. Having trusted, expert guidance to respond quickly and effectively can help minimize and mitigate damage to the business.

Learn more about how Microsoft Incident Response can help you before, during, and after a security incident"

[Click here](#)

[Microsoft Digital Defense Report 2022 | Microsoft Security](#)

