



CYBERATTACK REPORT No.2

The inCREDible attack

Building healthy habits to fight off credential attacks

A little over a year ago, a large enterprise customer asked Microsoft Incident Response (Microsoft IR) to investigate an incursion into their on-premises Active Directory (AD) environment. The IR team immediately stepped in to manage the crisis and facilitate cross-company communication. Microsoft Incident Response helped with operations, investigative tasks, and tactical mitigations that led to a full compromise recovery. The team also worked with members of the Microsoft Threat Intelligence (Microsoft TI) to successfully prevent the threat actor from causing further harm.

Like getting in your steps or eating your vegetables, healthy habits can help prevent security problems like credential attacks before they happen. Read on to see how the team identified what happened, disrupted the threat actor, and helped this customer recover faster.



**inCREDible
attack flow**



**How it began
and Microsoft's
response**



**Building healthy
habits**



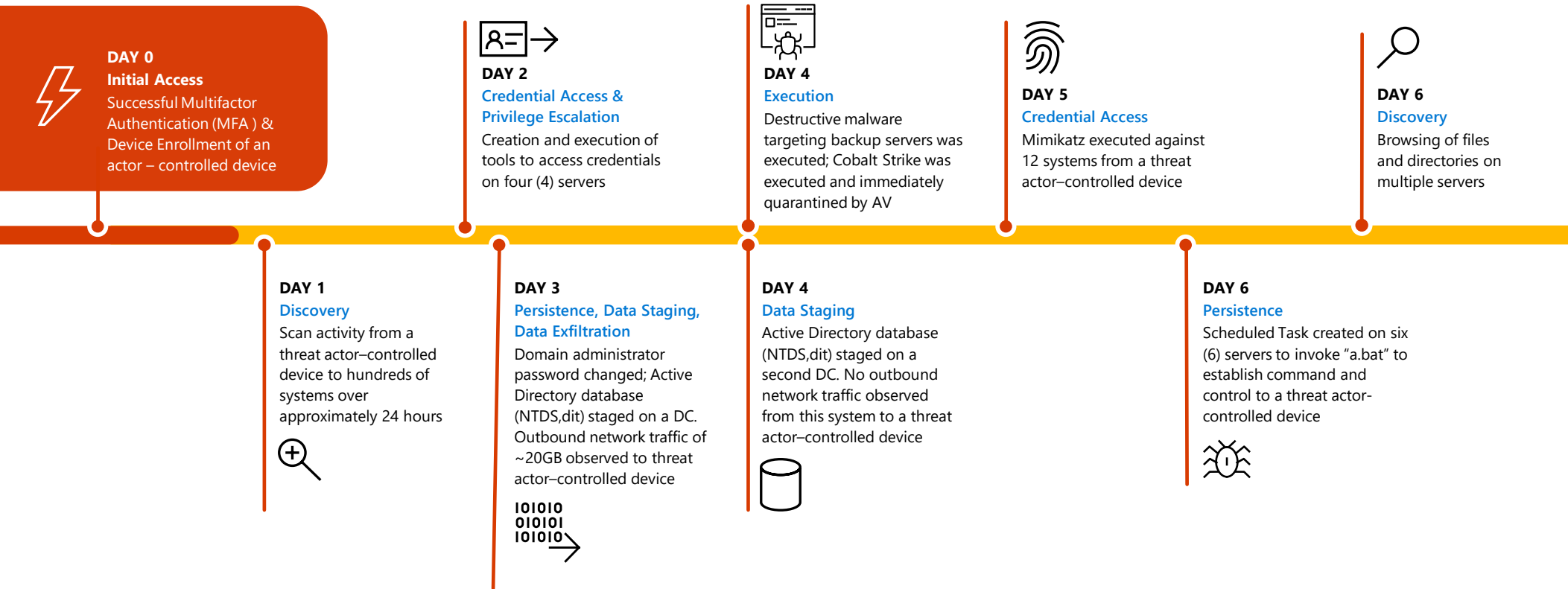
**How to stay
in control**



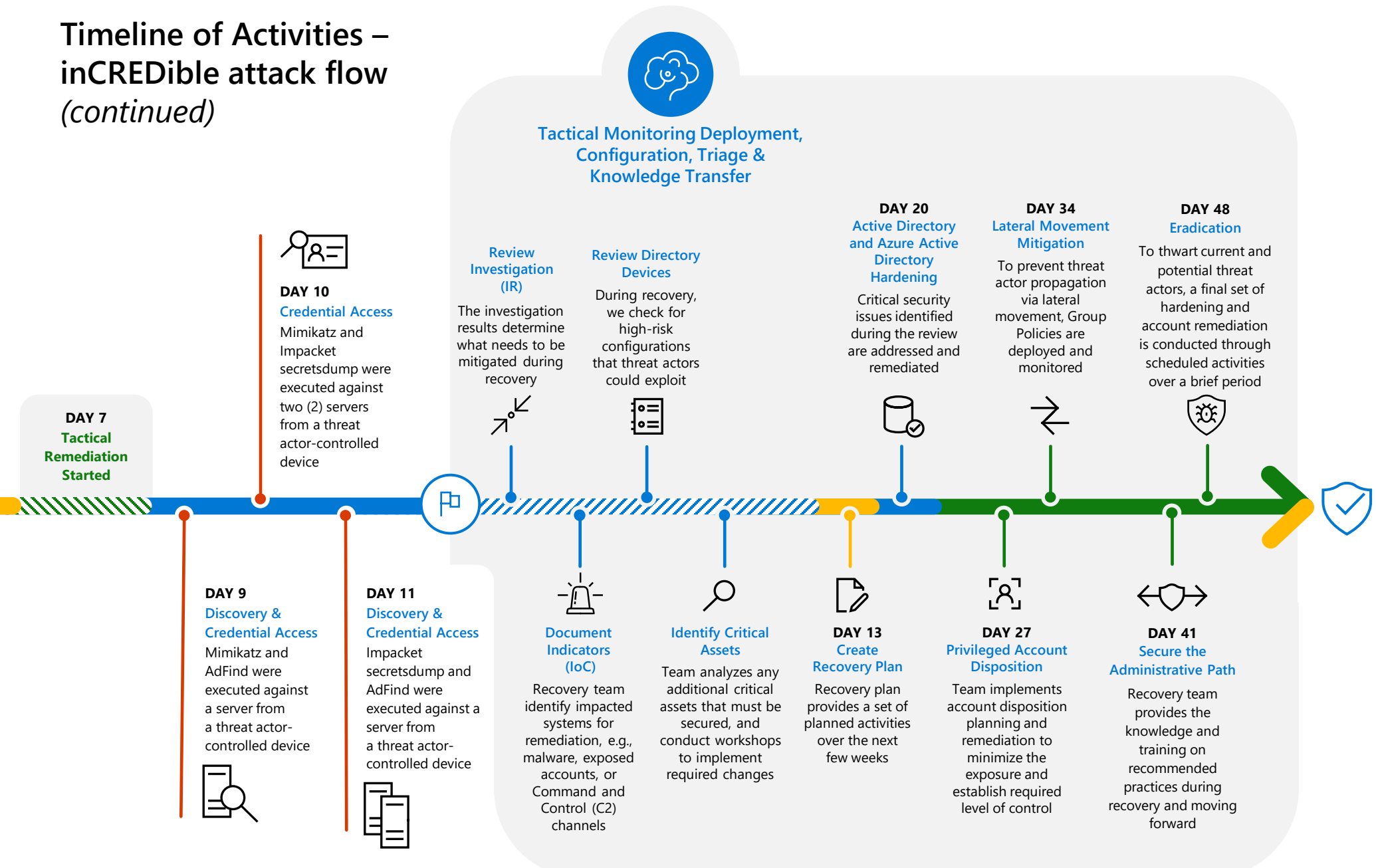


Timeline of Activities – inCREDible attack flow

The threat actor authenticated and registered a mobile device by “push bombing” – sending continued unsolicited MFA push requests to a legitimate user.



Timeline of Activities – inCREDible attack flow (continued)

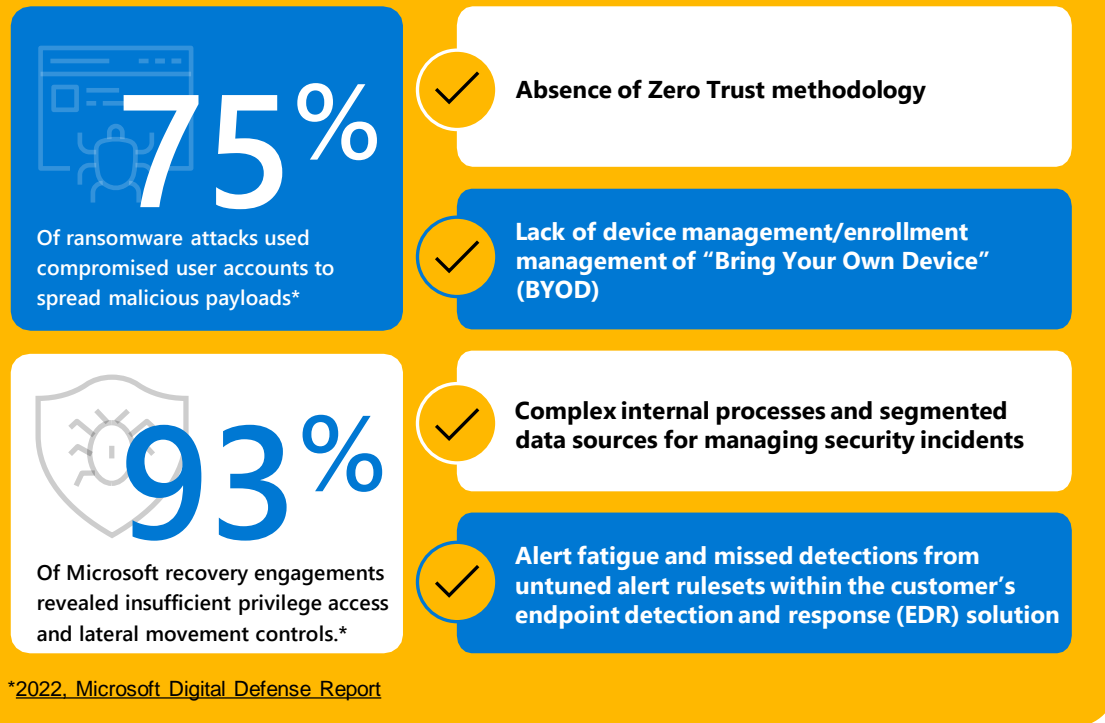




How it began

With the inCREDible attack, our threat actor first attempted to gain access to the customer's environment through several means of social engineering, including phone calls. Eventually they successfully authenticated and registered a mobile device with the customer's multifactor authentication (MFA) system through continued, unsolicited MFA push requests to a legitimate user—an increasingly common tactic known as "push bombing." Once authenticated, the threat actor had continued access to the environment with their registered mobile device.

Factors contributing to the threat actor's initial incursion



Microsoft's response

Microsoft responded immediately by aggregating investigative findings and facilitating communications between internal response teams, Microsoft IR, and other Microsoft security teams. With a better understanding of the incident, Microsoft IR requested additional data to identify further threat activity and fill in the information gaps, leveraging the customer's own existing solutions to augment the investigation.

The customer's security information and event management (SIEM) system, which included firewall log data, enabled Microsoft IR to correlate the creation of large archive files on servers of interest with suspicious outbound network traffic flows. In tandem, the customer's virtual private network (VPN) provided process auditing information collected by the SIEM. Using this data, Microsoft IR identified execution of credential theft tools and other malware within the customer environment before more damage could be done. In addition, working with the customer, the team identified that unmanaged endpoints were allowed to connect to the Remote Access VPN. As a tactical mitigation, the VPN configuration was changed to only allow trusted endpoints to connect.

What could have happened?

Prompt tactical mitigation efforts thwarted this attack before the threat actor could complete their actions on objectives. Based on past experiences, it is likely the threat actor would have executed some or all of the following, had mitigation factors not been in place:

- Deployed and executed ransomware within the environment
- Taken intellectual property and other data from the company (to perform extortion)
- Destroyed data, including critical assets and backups; and/or caused an interruption to normal business operations



Building healthy habits: Tactical solutions

While Microsoft Incident Response was investigating the threat actor's movements, they also partnered the customer's internal teams to perform an audit of their Active Directory configuration. The purpose of this was to pair it with the investigative findings to help re-establish positive control of the identities in question.

Microsoft's recovery experts follow a demonstrated methodology that has been repeated and refined worldwide. Our experts seamlessly utilize Microsoft Incident Response investigation data to understand the scope of the incident of impacted identities and prioritize privileged and non-privileged accounts. In this case, they implemented both tactical (short-term) and long-term remediation steps and made numerous high-impact changes to increase the overall security posture of the customer environment while minimizing any impact to the customer's ongoing operations.

One of the most difficult changes involved deprivileging—or securing of applications and associated service accounts that have been identified as “Domain Admin Equivalent.” Often, these applications are owned and controlled by business units outside of the Identity or Security teams. This increases the difficulty of implementing proper security controls and strains existing customer ACM (Adoption Change Management) and MSM (Modern Service Management) processes. Successful deprivileging often requires executive level sponsorship and immediate action by the customer to act on recommended changes.

Every customer environment is different, and their ability to absorb change differs as well—especially after the immediate threat is remediated by the IR team and the customer no longer feels an immediate threat to their business. Their standard change control processes kicks in and they are much more resistant to making necessary changes to their environment during our short engagement. Those customers who are willing to make the required changes have a much better chance of avoiding repeated incidents. This customer was on top of their change control and did a lot of required changes—almost on daily basis—by speeding up all required approvals.

The primary objective of this Microsoft Incident Response's compromise recovery project was to assist the customer with planning, staging, and performing reinforcement of positive administrative control of the customer's Active Directory Domain Services (AD DS) and Azure Active Directory (AAD) configuration. The secondary objective was to implement a minimal level of protection and detection to help prevent a potential re-compromise, and to increase the likelihood of immediate detection should the threat actor succeed in reentering the environment.

In the initial Planning Phase, Microsoft recovery experts worked with the customer to identify priorities for mitigating the environment. The Staging Phase followed, where recovery experts work with the customer to stage and test recommended changes. And finally, both the customer and the recovery team entered the Eradication Phase, where all the planning and staging culminates in a carefully executed set of activities to evict the threat actor and reinforce Positive Administrative Control over customer AD DS and AAD.

Recovery phases



Planning phase

Microsoft recovery experts work with the customer to identify priorities for mitigating the environment.



Staging phase

Recovery experts work with the customer to stage and test recommended changes.



Eradication phase

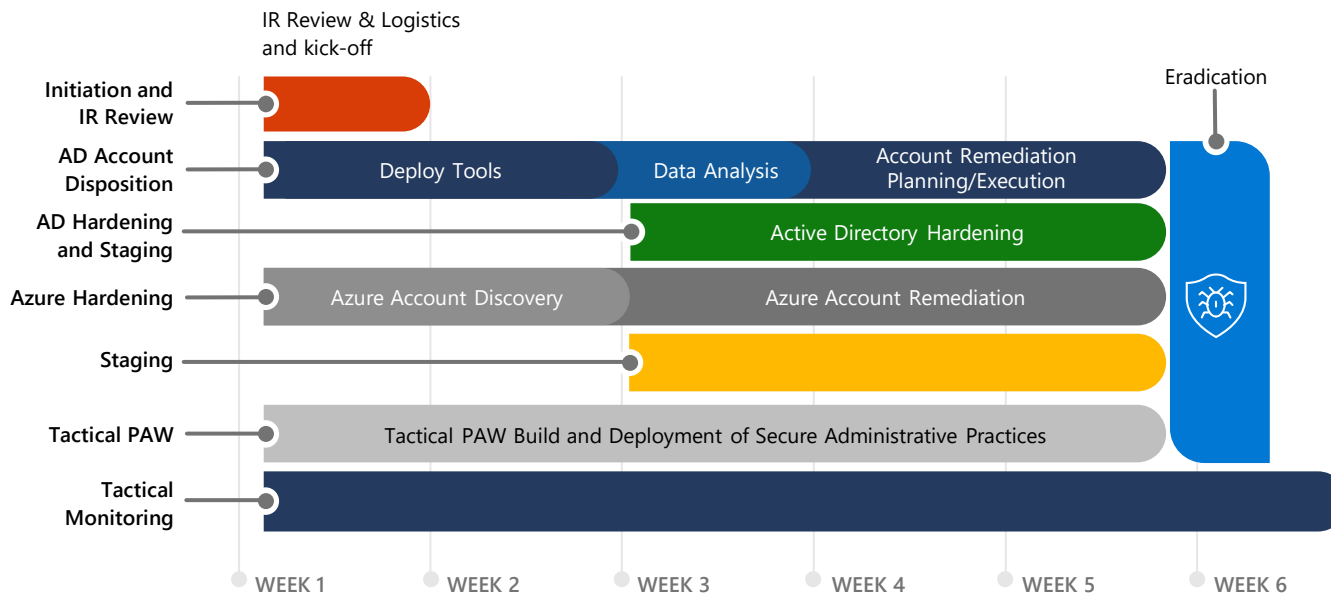
Eradication phase where planning and staging culminate in a carefully-executed set of activities to reinforce control over customer Active Directory Directory Services (AD DS) and Azure Active Directory (AAD).



Reduce exposure and take back control: Active Directory account disposition and hardening

To take back positive administrative control of Active Directory, the team worked with the customer to review all identities with “Domain Admin Equivalent” level access in the AD DS domains and determine the business justification for the assigned level of permission. These identities are usually used by Administrators for different administrative tasks and by over-privileged applications running in the customer’s environment. This is common in large enterprise environments where the initial number of identities with “Domain Admin Equivalent” permissions can number in the hundreds. Our goal is to reduce number of these accounts to an absolute minimum required to manage Active Directory. In most cases we can reduce the number of accounts to be less than ten in total.

In parallel, the recovery team ran discovery tools against each Domain Controller, and systems that have been identified as “Domain Controller” equivalent, to identify specific configurations (e.g., software, Services, Scheduled Tasks). Microsoft worked with the customer to reduce the overall exposure of unneeded configuration across all Domain Controllers.





* It takes around 6 weeks for large enterprise customers.
Can be less time for smaller and less complex environments.



Eat your vegetables

4 steps customers can take to establish healthy habits to help minimize risk of attack.

- 1 Reduce exposure by actively preventing privilege escalation
- 2 Validate identities and remove/de-escalate permissions regularly
- 3 Isolate and rebuild controls
- 4 Establish ongoing tactical monitoring



Validate identities and minimize/remove permissions: Azure Account Disposition and Hardening

Like on-premises Active Directory, the recovery team ran discovery scripts against the customer's Azure Active Directory and Azure subscriptions to identify the following:

- All identities with high privilege AAD roles
- All identities with high privilege RBAC roles on Azure subscriptions
- All AAD applications that have risky permissions

The team then worked with the customer to review each identified account/application and established a plan to reduce the number of accounts to an absolute minimum required to manage Azure Active Directory. Additionally, applications that can control Azure Active Directory and accounts that can control Azure subscriptions with the most critical resources were reviewed and removed as needed.

Isolate and rebuild controls: Privileged Access Workstations

Isolation is a fundamental protection for regaining control. Without isolation and strict control of communications and access between the security zones, this security model fails. As such, remote administration requires a computer in the same security zone. This is also known as a Privileged Access Workstation (PAW), which is described in more detail in Microsoft's "[Securing Privileged Access](#)" guidance.

The recovery team worked with the customer to design and build a temporary version of the PAW, which we have called a "Tactical PAW." The Tactical PAW is not joined to either the on-premises domains nor to Azure Active Directory until the completion of the eradication phase.

Tactical Monitoring

In addition to the preventive controls, it is crucial to establish tactical monitoring targeted at identifying potential malicious activity or further attempts to compromise. Just like getting in your steps or eating your vegetables, this preventative measure helps ensure ongoing security. Several monitoring tools were implemented by the customer to achieve a comprehensive view of the enterprise in a short period of time, any time it is needed. These included Microsoft Defender for Identity (MDI) and Microsoft Defender for Endpoint (MDE).

How can customers avoid this scenario?

To prevent a ransomware attack, organizations must "eat their vegetables," and adopt a defense-in-depth approach. First, use MFA with "Number Matching" or similar functionality to enhance MFA protection. This involves accepting a push notification and inputting a matching number. Secondly, configure Windows Auditing Policies following the best practices, including Sysmon and process auditing with command line. Next, centrally collect OS and network infrastructure logs for a minimum of 180 days—and ideally—implement a Security Information and Event Management (SIEM) system. Also, implement an Endpoint Detection and Response (EDR) solution for all endpoints. And lastly, businesses should implement an Active Directory Tiering Model and follow Microsoft's "Best Practices for Securing Active Directory." These actions are part of the recommended daily allowance of "vegetables" that help businesses maintain a robust defense against ransomware attacks.



Conclusion

Organizations often focus on protecting against elaborate, sophisticated cyber attacks when the most common breaches exploit every day human vulnerabilities.

Many attacks can be prevented—or at least made more difficult—through implementation and maintenance of basic security controls. Organizations that "eat their vegetables" can strengthen their cyber security defenses. Start by establishing a solid inventory of all technology assets. Continually update operating systems and software and maintain secure administrative practices. Finally, implement comprehensive centralized log collection with a well-defined retention policy. Those few key "healthy habits" will go a long way to ensuring better protection against attacks.

To learn more about Microsoft's specialized support before, during, and after an incident, please visit: <https://aka.ms/MicrosoftIR>

