

SOC Threat Radar

VOLUME 2 2025



Live threat activity

Over the last month, Barracuda Managed XDR's security solutions, threat intelligence, and SOC analysts identified the following developments that organizations should be aware of.

1

A 400%+ increase in the use of malicious macros

What's behind this?

In January, XDR Endpoint Security identified a significant rise in threats containing malicious macros – up more than 400% compared to the previous two months. Malicious macros have been around for a long time, but they remain an effective attack method.

What's the risk?

- Macros are scripts embedded in documents such as Microsoft Excel. They can be used by IT teams to automate tasks. Threat actors can exploit them for attacks on a victim's computer.
- Malicious macros are commonly delivered to targets via booby-trapped email attachments. These attachments might look like invoices, receipts, or other important documents.
- Employees may inadvertently click on the button to enable macros or fall for scammers convincing them to do so by saying it is urgent or important.
- Once enabled, the macro can perform various malicious activities. It can download and install other types of malware like ransomware or spyware, steal sensitive information, and alter system settings. It can also create backdoors for future exploitation or channels to communicate with command-and-control.
- Malicious macros can spread rapidly from an infected spreadsheet to other documents.

Am I exposed?

- Older IT systems and software may not have the security features or updates in place to block malicious macros.
- Employees who don't know the risks may be more likely to click on a link to enable macros.
- Many businesses are trying to find a balance between functionality and security: They rely on macros for automating complex tasks. Disabling macros as standard can disrupt these processes.

Action to take

- Ensure macros are disabled wherever possible in your Microsoft applications.
- Educate employees about the risks of opening unknown attachments, enabling macros, and how to spot phishing attempts.
- Keep all systems and software updated with the latest security patches.
- XDR Endpoint Security can protect infected systems by detecting and mitigating anomalous activity associated with malicious macros.

2

A 40% rise in spear phishing attacks

What's behind this?

Many of the spear phishing threats seen by XDR Email Security in January have a financial or IT systems-related theme. Threat actors often exploit seasonal trends, and annual taxation and financial year-ends may be contributing to the rise in detected incidents.

What's the risk?

- Spear phishing is a well-established attack method. It continues to succeed because the approach continues to evolve, becoming more sophisticated and evasive.
- Specific examples recently detected by Barracuda Managed XDR include financially themed spear phishing emails delivered to individuals in accounting and leadership roles, and IT systems-themed emails targeting network technicians and administrators.
- Threat actors target specific individuals, often drawing on publicly available information such as LinkedIn profiles to identify targets and personalize messages.

Am I exposed?

- Basic email defenses may struggle to detect or mitigate more sophisticated email-based attacks.
- A lack of security awareness training for existing or new employees may leave them vulnerable to social engineering threats.

Action to take

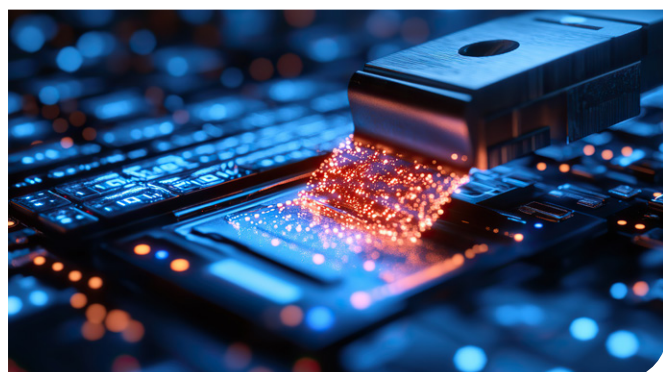
- Regular security awareness training for employees is essential.
- Deploy advanced, intelligent email protection.
- Layer email protection with XDR to detect and mitigate email-borne threats both before and after delivery.
- Introduce a transaction review and confirmation process for financial staff before the payment of invoices or wire transfers.

3

A 171% rise in the suspicious clearing of Windows event logs

What's behind this?

XDR Server Security has spotted a rise in the suspicious clearing or deletion of Windows event logs on an endpoint. Attackers often clear logs to cover their tracks and delay detection by making it harder for security teams to investigate an alert—so this rise may be connected to broader attack campaigns that XDR prevented from unfolding.



What's the risk?

- Event logs record the activities happening in a computer system, such as system errors, user activities, software updates, and more. They are essential for troubleshooting and monitoring system performance.
- Log clearing is a strong indicator that a malicious intruder is present in the network as IT admins or individual users rarely need to clear logs.
- Attackers may start by preventing the system from recording events to stop new logs from being created, making it easier to hide their activities.
- Attackers then move on to clearing existing logs to erase any evidence of their earlier actions. Sometimes they modify logs to remove or alter specific entries to further mislead investigators.

Am I exposed?

- The risk of intentional or accidental unauthorized log clearing can increase if too many employees have access to log files.
- A lack of log monitoring and alert systems may mean that suspicious log clearing goes unnoticed and attackers can continue with the next stage of their attack.

Action to take

- Implement continuous, centralized log monitoring (such as XDR Server Security) to detect any abnormal behavior or unusual activities, such as sudden gaps in logs or unexpected log clearing events.
- Regularly back up logs to a secure location. This ensures that even if logs are cleared or tampered with, a copy remains available for investigation.
- Having XDR in place helps to combat this type of threat, as all security events are logged and ingested into a security platform for detection and investigation.



XDR roundup 2024: Ransomware rises fourfold in a year of complex threats

In 2024, Barracuda Managed XDR logged nearly 11 trillion IT events to identify the critical security threats targeting organizations and neutralize malicious activity. Threat analysts in Barracuda Managed XDR's Security Operations Center (SOC) have drawn on this unique dataset to highlight the most common ways threat actors tried — and ultimately failed — to breach and disrupt targets in 2024.

Key findings

- Ransomware threats increased fourfold during 2024, likely driven by widespread Ransomware-as-a-Service (RaaS) activity. Barracuda Managed XDR's ransomware threat data is based on the detection of instances such as tools, techniques, or behaviors that indicate an unfolding or imminent ransomware attack. The data highlights how attackers hunt down and leverage unprotected devices and access points to further their attack.
- The most common threats targeting XDR-protected systems overall in 2024 show where threat actors expect customers to be most vulnerable: inadequate authentication measures for account logins, poor password policies, and a lack of education about social engineering, alongside under-protected VPNs and the poorly managed use of remote desktop protocols.

- Email threats that made it through to user inboxes were the fifth most detected threat overall, highlighting the growing risk of sophisticated and evasive attacks enabled by Phishing-as-a-Service (PhaaS) platforms.
- Attacks are fast—with attacks often unfolding in hours rather than days as security tools advance.

"The rise of as-a-service platforms is helping to power the growing sophistication, agility, and evasive nature of cyberattacks, from ransomware to phishing. The developers behind these platforms often have the time, resources, and skills to invest heavily in advanced and evasive toolsets and templates. A comprehensive XDR solution that integrates network, endpoint, server, cloud, and email security means that every corner of the digital infrastructure is monitored and protected with advanced security measures, a full spectrum of defensive tools, combined with proactive threat hunting and response strategies."

Attacks are fast — strong defense is faster

24 hours a day, 365 days of the year



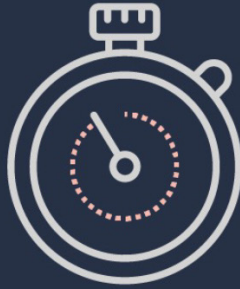
70 seconds — the time it took for attackers to install malware from a thumb drive and try to infect devices at an MSP



74 minutes — how long a threat actor lurked on an unprotected server, elevating privileges and releasing Akira ransomware



2 hours — how long Play ransomware attackers dwelled on unprotected devices in the network before being detected when they broke cover



Every second, 350K IT events are logged by Barracuda Managed XDR



Every 30 seconds, an IT event triggers a security red flag



Every 30 minutes, 1 high-severity threat is mitigated through immediate defensive action



Source: Detection and analysis data from Barracuda Managed XDR — further details in the XDR roundup 2024

The full XDR round up is available [here](#).

The SOC case files

Barracuda Managed XDR catches Akira ransomware exploiting 'ghost' account and unprotected server

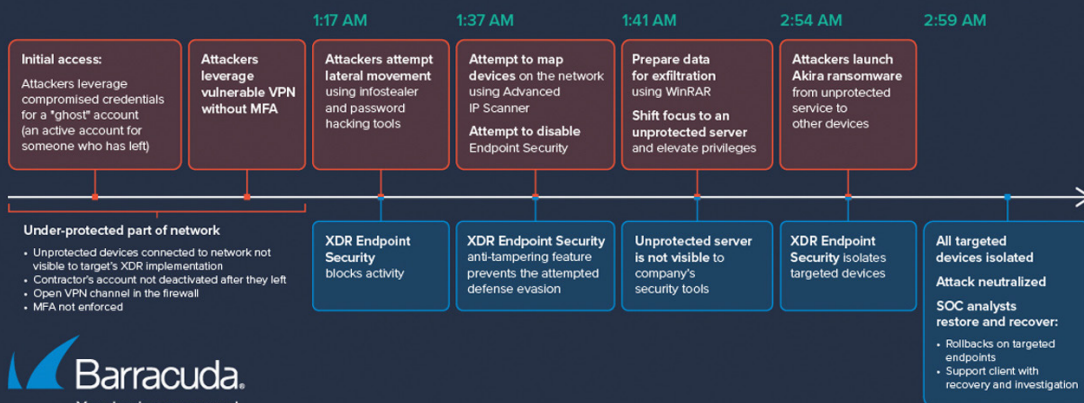
Incident summary

- A manufacturing company was hit with Akira ransomware in the early hours of the morning.
- The attackers breached the network through a 'ghost' account (an account that was created for a third-party vendor and not deactivated when the vendor left).
- At some point before deploying the main attack, the threat actor got hold of the credentials for the third-party 'ghost' account and used this to connect via an open VPN channel without multifactor authentication to gain access to the network.
- At 1:17 a.m. on the night of the main attack, the threat actor broke cover and tried to move laterally and disable endpoint security—both attempts were blocked by Barracuda Managed XDR.
- They then moved the focus of their activity to an unprotected server, elevating their privileges and launching the ransomware at 2:54 a.m.
- By 2:59 a.m. all impacted devices covered by Barracuda Managed XDR had been neutralized.
- SOC engineers worked with the target on recovery and investigation.

The SOC case files

Target: Manufacturing company

Threat actor: Akira ransomware



Key learnings

- This incident illustrates how cyberattacks have become increasingly multi-stage and multi-level, with attackers ready to pivot and adapt to changing or unexpected circumstances, hunting down and exploiting any areas that are left unprotected and exposed.
- The best protection against such attacks is comprehensive, layered defenses with integrated and extended visibility. This should be accompanied by a robust focus on cybersecurity basics, such as enforcing MFA, introducing robust password policies, and regularly auditing active user accounts and disabling any that are no longer in use.
- Every attempt to progress the attack that involved an XDR-protected endpoint was mitigated and remediated within minutes. XDR can help in other ways, including:
 - XDR Endpoint Security proactively provides data on unprotected devices, so organizations are made aware of devices on their network that do not have endpoint security deployed and could potentially be leveraged by attackers.
 - Extending XDR coverage to network security could have detected the suspicious VPN activity at an earlier stage of the attack.
 - Lastly, extending the XDR coverage to include server security could have detected the unusual activity and privilege elevation quietly taking place on the server.

For further details on the incident timeline, the main tools and techniques used, and Barracuda Managed XDR response, please see the full [case file](#).



Other current threat activity to be aware of

A critical security flaw enables remote access to Microsoft Windows directories on servers

What's the risk?

A critical Microsoft Windows vulnerability was discovered late last year that can crash unpatched Windows servers without any user interaction or authentication. All that's needed is for the server to have internet access.

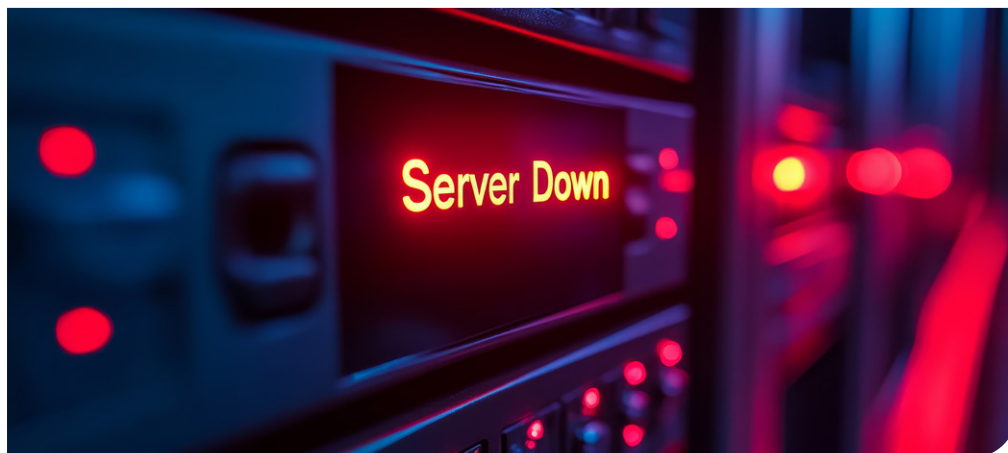
The flaw enables threat actors to execute code remotely. Organizations that rely heavily on Active Directory are at significant risk, with potential consequences including downtime, data breaches, and lateral movement by adversaries.

More information

Barracuda Cybersecurity Threat Advisory:
[Microsoft Windows zero-click RCE vulnerability](#)

Action to take

- Apply Microsoft's [December 2024 Patch Tuesday](#) patches immediately.
- Monitor for any suspicious activities on servers until patching is complete.
- Implement network segmentation if you haven't already to isolate critical systems and services and limit the potential impact of an exploit.
- Work with your security provider as needed to undertake security audits and penetration testing to identify and address vulnerabilities in your environment.



Active exploitation warning for Ivanti's Connect Secure VPN

What's the risk?

A critical Ivanti Connect Secure VPN vulnerability is being exploited in the wild, primarily targeting organizations relying on Ivanti's Zero Trust Access (ZTA) solutions.

The flaw allows attackers to gain control of affected systems without authentication. Once in, they can deploy malware to establish persistence, steal data or use the compromised VPN to penetrate deeper into the organization's network. The stealthy nature of this vulnerability makes it particularly effective, often evading traditional security measures focused on user authentication or endpoint protection.

Action to take

- Update systems as soon as possible with Ivanti's patch.
- Limit external access to the VPN management interface and enforce multifactor authentication (MFA) for all remote connections.
- Work with your service provider as needed on incident response to contain or remediate breaches if you suspect any exploitation.

More information

Barracuda Cybersecurity Threat Advisory:

[Active exploitation of Ivanti's Connect Secure VPN](#)



How Barracuda Managed XDR can help your organization

Barracuda Managed XDR delivers advanced protection against the threats identified in this report by combining cutting-edge technology with expert SOC oversight. With real-time threat intelligence, automated responses, and a 24/7/365 SOC team, Barracuda Managed XDR ensures comprehensive, proactive protection across your

network, cloud, email, servers, and endpoints, giving you the confidence to stay ahead of evolving threats.

For further information on how we can help please get in touch with [Barracuda Managed XDR](#).