IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

The Top Three Security Lessons to Take Away from Aikido Wiper

Darren Mar-Elia

Darren Mar-Elia
Vice President of Product
Semperis

Biography

Darren Mar-Elia is Vice President of Product at Semperis (https://www.semperis.com). A 14-year Cloud and Datacenter Microsoft MVP, Darren has a wealth of experience in Identity and Access Management and was the CTO and founder of SDM software, a provider of Microsoft systems management solutions. Prior to launching SDM, Darren held senior infrastructure architecture roles in Fortune 500 companies and was also the CTO of Quest Software.

As a Microsoft MVP, Darren has contributed to numerous publications on Windows networks, Active Directory and Group Policy, and was a Contributing Editor for Windows IT Pro Magazine for 20 years.

Darren blogs at https://www.semperis.com/blog

Keywords Identity security, Aikido Wiper, EDR, APT, Active Directory, wiperware, Azure AD, AD backup, Malware
Paper type Research

Abstract

Earlier in the year cybersecurity circles were buzzing about Aikido Wiper, the discovery of SafeBreach security researcher Or Yair[1]. In short, Yair reported that cyberthreat actors can manipulate antivirus endpoint detection and response (EDR) tools to create a wiper that can delete system files – effectively destroying the data and making systems unbootable. As the author of this article explains, there are some valuable lessons which organizations need to take away from the discovery, and what can be done to protect organizations from Aikido Wiper and its ilk?

Introduction – what is wiperware?

Endpoint detection and response (EDR) bypass – tricking or bypassing EDR tools to allow a cyberattacker across the EDR security barrier—is not a new coercion strategy. Nor is wiperware. Shamoon, CaddyWiper, IsaacWiper, and others have wreaked havoc in the past. What makes Aikido Wiper unique is its ability to destroy files without using obvious Application Programming Interface (API) calls and to operate as an unprivileged user.

Regardless of its tactics, Aikido Wiper offers the same lesson as other wiperware: EDR is an important security tool, but it simply cannot be used as your only defense.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Wiperware attacks tend to be most popular with nation-state actors or terrorists whose goal is destruction rather than financial gain. This type of exploit is often used as part of advanced persistent threat (APT) attacks against critical infrastructure such as utilities, with the intent to cause havoc. Naturally, wiperware attacks typically increase during times of geopolitical strife.

The problem with EDR

EDR – and even extended detection and response (XDR) tools[2] – are an important part of your cyber defense strategy. But Aikido Wiper illustrates an important maxim: The best defense is a layered defense. You simply cannot trust one security tool to protect you, no matter how fantastic that tool might be.

Cyberattackers are becoming increasingly adept at finding ways past EDR protection, and once attackers make it into your network, their next target is usually your identity infrastructure. Gaining access to Active Directory (AD) – the identity system used by 90% of organizations today – or Azure AD can enable threat actors to take over even more critical assets in your environment.

Because identity systems are such prime targets for threat actors, with credential misuse being the most popular path to security breaches, Gartner emphasizes this need for “defense in depth”, with a concentration on identity.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Aikido Wiper operates on an endpoint, without relying on an identity system. The wiperware uses junction points (a Windows File System-based entity) to trick EDR into overwriting or deleting system files. Broader wiperware might attack multiple endpoints. But in most cases, attackers are after more than what resides on your endpoints. Getting privileged access to your data and systems is a much more common goal.

In either case, no amount of EDR protection will help you once attackers breach your endpoints. Protecting your identity systems as part of a layered defense strategy remains a priority. Maintaining a secure, malware-free AD backup can make the difference when it comes to a fast recovery of your environment, regardless of whether systems are brought down by malware, natural disaster, or another cause.

How to strengthen your cyber defenses

Good security is like an onion, with multiple layers of protection. If EDR is the outer layer, identity-first security is at the centre. Organizations are realizing that of those layers, identity protection should form the core of your cyber-resilience strategy. Here are the top three steps you can take today to defend your business against today's cyberthreats.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Avoid a single point of failure

Because Aikido Wiper leverages built-in operating system capabilities, the onus is on the affected EDR vendors to fix the weakness that this wiper exploits. Unfortunately, there's no magic bullet to turn off the exploited behavior within Windows. You can expect EDR vendors to eventually provide patches, making regularly updates of your EDR security tools especially critical.

Beyond the need to maintain EDR updates, Aikido illustrates an important aspect of robust defense in depth. As attractive as using one vendor to source your entire security toolset might sound, security vendor consolidation can have significant drawbacks. Aside from the potential business concerns around consolidation, cyber resilience – especially when it comes to identity systems – requires a certain level of redundancy to avoid a single point of failure, which is all too common in the EDR/ XDR world.

Gartner points out[3] that an XDR strategy requires a high level of dependence on a single vendor. Especially when it comes to ITDR, Gartner recommends a multivendor approach, noting that "a layered approach involving ITDR is the best way to enhance preparedness for cyberattacks…. Fill gaps in ITDR by assessing the full range of attack vectors and telemetry covered. Plan to use a mosaic of tools that complement each other, and may overlap, to meet the requirements for a comprehensive ITDR initiative."

When evaluating ITDR vendors, keep the importance of protecting the identity system front and center in the process. Look for a best-of-breed ITDR solution that focuses specifically on protecting the identity system—which is not the primary area of expertise for many XDR vendors.

Plan for recovery

Another lesson from Aikido Wiper: Tested, malware-free backups of your core identity systems are a must. Our recent survey of more than 50 organizations[4], focused on identity threat detection and response (ITDR) solution priorities, shows that 77% of respondents would experience a severe or catastrophic impact if a cyberattack were to take down AD.

An AD-centric backup – separate from standard backups of the operating system or other services – is an excellent defense against the ravages that wiperware and other attacks can generate. Other backup options, including domain controller (DC) snapshots[5], risk data consistency issues, data loss, or even malware reintroduction.

By contrast, an AD-specific backup enables a much faster recovery of your environment and has a smaller backup footprint than system state or bare-metal recovery (BMR) backups. A robust AD backup tool like Semperis Active Directory Forest Recovery (ADFR)[6] protects against the reintroduction of malware and can even be automated to avoid human error and reduce downtime to mere minutes.

Your disaster recovery plan should include specific steps for implementing and regularly testing your identity system backups and recovery process along with

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

other critical maintenance. After all, the best time to test your recovery plan is before you need it.

Monitor, monitor, monitor

Regular monitoring of your identity attack surface can help you spot and fix potential vulnerabilities before attackers can make significant progress. As Aikido Wiper illustrates, your monitoring strategy must go beyond antivirus, EDR, and security logs. Even security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions have limits[7] when it comes to protecting you from the most damaging cyberattacks.

As with your overall defense strategy, taking a multilayered approach to monitoring provides the best results. For optimal identity-first security, look for a solution that provides real-time insight and actionable guidance. You needn't break the budget to find these capabilities. For example, our free community tools, Purple Knight[8] and Forest Druid[9], enable monitoring of security indicators – both indicators of compromise (IOCs) and indicators of exposure (IOEs) – and Tier 0 attack path management at no cost. If you want additional capabilities such as automated rollback of suspicious activity, a paid solution like Semperis Directory Services Protector (DSP)[10] offers IOC and IOE monitoring plus automated remediation and extended incident response.

Don't fear the wiper

Cyberattackers continue to make gains in both sophistication and persistence. A layered, defense-in-depth cybersecurity strategy that protects both endpoints and your core identity foundation is your best defense against whatever they throw at you, be it wiperware like Aikido, ransomware, or an as-yet-to-be-discovered exploit. Put identity-first security on your 2023 priority list, and you'll have one less thing to worry about.

Reference

1 Yair, O., Aikido - Turning EDRs to malicious wipers using 0-day exploits. Safe-Breach. Available at: https://i.blackhat.com/EU-22/Wednesday-Briefings/EU-22-Yair-Aikido-Turning-EDRs-to-Malicious-Wipers.pdf

2 Deuby, S. (14 July 2022), How Cybersecurity is Evolving from EDR to XDR to ITDR. Semperis. Available at: https://www.semperis.com/blog/how-cybersecurity-is-evolving-from-edr-to-xdr-to-identity/

3 Teixeira, H., Firstbrook, P., Allan, A., and Archambault, R. (20 October 2022), Gartner. Available at: https://www.gartner.com/document/4020294?ref=solrResearch&refval=349991075

4 Evaluating Identify Threat Detection & Response (ITDR) Solutions - A Survey of Identity-Centric Security Leaders. Available at: https://www.semperis.com/wp-content/uploads/PDFs/resources-semperis-itdr-survey-report.pdf

5 Deuby, S. (13 October 2022), Why DC Snapshots are no Substitute for Active Directory Backups. Semperis. Available at: https://www.semperis.com/blog/hypervisor-dc-snapshots-are-no-substitute-for-proper-active-directory-backups/

6 https://www.semperis.com/active-directory-forest-recovery/

7 Deuby, S. (23 August 2022), SIEM and SOAR - and Identity Security. Semperis. Available at: https://www.semperis.com/blog/siem-and-soar-and-identity-security/

8 https://www.purple-knight.com/

9 https://www.purple-knight.com/forest-druid/

10 https://www.semperis.com/active-directory-security/