



Fundamentals of Breach Avoidance

Written by Steve King & Andy Jenkinson

Cyber**Ed**.io

Introduction

The Common Vulnerabilities and Exposures (CVE) database lists publicly disclosed computer security flaws.

On May 31, 2023 Progress released a security bulletin about CVE-2023-34362, a vulnerability in MOVEit Transfer that was being actively exploited. At the time we had a few details about how it was being exploited, but not by whom.

- Over the next few days it became clear that the CIOp ransomware group had been testing the vulnerability since July 2021 and decided to deploy it over the Memorial Day weekend. The first victims became known.
- GDPR requires that breach victims notify of Cyber-attacks not later than 72 hours following a breach. The US has yet to adopt similar legislation.
- A second vulnerability was found while new victims were still coming forward. After the first vulnerability was discovered, MOVEit's owner, Progress Software partnered with third-party cybersecurity experts to conduct further detailed code reviews of the software and found CVE-2023-35036.
- Progress posted a new bulletin about it on June 9, 2023.
- On June 15, 2023, Progress published information about a third critical vulnerability which got listed as CVE-2023-35708 on June 16.

This latest vulnerability could lead to escalated privileges and potential unauthorized access to the environment.

Please note that it is critically important to follow the instructions outlined in the latest advisory in which it explains how the patches need to be applied including knowledge about how many patches have already been applied.

The best advice provided by Progress is probably to disable all HTTP and HTTPS traffic to MOVEit Transfer on ports 80 and 443 to safeguard the environments while a patch is being prepared to address the vulnerabilities and in case even more of them come to the surface.

Meanwhile the Cybersecurity and Infrastructure Security Agency (CISA) says it's providing support to several federal agencies that have experienced intrusions affecting their MOVEit applications. Among the probably hundreds of victims are Payroll provider Zellis who serves British Airways and the BBC, oil giant Shell, several financial services organizations, insurance companies, and many others. Reportedly, multiple

US Department of Energy (DOE) entities were also compromised.

Victims have been identified in the UK, US, Germany, Austria, Switzerland, Luxembourg, France, and the Netherlands. Organizations in the US make for most of the victims, but no ransom demands have been made of federal agencies according to a CISA spokesperson.

We know that the CIOp ransomware group sat on a zero-day vulnerability it discovered in the MOVEit file transfer app for two years before pressing the detonate button. They had the keys to the house, so why hurry?

Over that period, they periodically launched payloads of malicious activity against vulnerable systems to test their access and identify the right targets. The Microsoft IIS logs prove it.

In 2021, the CIOp pushed the button on yet another file-transfer zero-day, that time in the Acellion's File Transfer Appliance, making life difficult for over 100 companies. CIOp was also behind the 2021 SolarWinds Serv-U Managed File Transfer attacks, in particular, the Secure FTP remote code execution vulnerability, tracked as

CVE-2021-35211, which allows a remote threat actor to execute commands on a vulnerable server with elevated privileges. Sound familiar?

Why weren't they patched?

In the case of MOVEit, reports of attack activity targeting a SQL injection vulnerability began surfacing in the discovery community on June 1. Mandiant and other investigators found the flaw in full exploit, enabling CIOp's subsequent ransomware demands.

On June 4, the first reports of organizations victimized by the attacks began to roll in, which included the BBC, British Airways, the government of Nova Scotia, Disney, Chase, GEICO, PWC, EY, Universities, Healthcare, and 'multiple' US federal agencies – the list grows daily.

CIOp itself claims hundreds of victims, but as we've pointed out, notification remains in drip mode because the breach doesn't fall under GDPR authority. CISA likely got it right however, when on June 7, they warned of potentially widespread impact: "FBI and CISA expect to see widespread exploitation of unpatched software services in both private and public networks."



How to Avoid Ransomware



- Train your employees on a regular basis and enforce the “security first” mindset – we are not in a nuclear cold war, but we need to practice crawling under our ‘desks’ – include table top exercises for IR and Escape rooms for teams, we need to observe attack simulations and visualize outcomes – regular means monthly.
- Comprehensive cybersecurity awareness programs are crucial to educate employees about the evolving threat landscape and instill a culture of cyber consciousness throughout the organization. By fostering a collective responsibility for cybersecurity, we can strengthen our defenses and mitigate the potential devastation that threats like the recent MOVEit-related cyberattacks can cause.
- Ensure that all technical employees who are tasked with Secure Website technical responsibilities are trained and experienced with the design, implementation, maintenance, monitoring, troubleshooting, and mitigation of Secure Websites.
- Ensure that all technical employees who are tasked with DNS-related technical responsibilities are trained and experienced with the design, implementation, maintenance, monitoring, troubleshooting, and mitigation of DNS Security.
- Block all common forms of entry based on principles of least privilege. Create a plan for patching vulnerabilities in internet-facing systems quickly; and disable or harden remote access like RDP and VPNs.
- Your VPN is leaky and can’t match the current threat landscape – migrate to ZTNA ASAP.
- Ensure ALL websites use HTTPS encryption and maintain valid Digital Certificates to establish secure connections. Run frequent vulnerability assessments/scans to assure patching is up to date. Block access to all DNS and provision them on a per device basis.

How to Avoid Ransomware continued

- Stop using duplicate DNS addresses from Microsoft. Implement DNSSEC (DNS Security Extensions) to optimize the authenticity and integrity of DNS responses. Utilize DNS monitoring and intrusion detection systems daily, to detect and respond to suspicious activities promptly. Regularly update DNS software and maintain strong access controls to protect against unauthorized changes.
- Understand the compliance requirements for every regulation under which you are covered, not because compliance equals security, but because most regulations espouse best practices and you will need a thorough understanding of the penalty structure for violations, so that you may avoid stepping into regulatory and enforcement traps.
- Prevent intrusions. Stop threats early before they can even infiltrate or infect your endpoints. Use endpoint security software that can prevent exploits and malware used to deliver ransomware, and AMTD (Automated Moving Target Defense) to shift target profiles so that attackers can't find the targets.
- Detect intrusions. Make it harder for intruders to operate inside your organization by segmenting networks and assigning access rights prudently. Use EDR or MDR to detect unusual activity before an attack occurs.
- Monitor and log DNS, system and network traffic, retaining it for at least 6 months with regular, thorough reviews, looking for anomalous behavior and alerting forensic and/or SOC analysts when it is found.
- Stop malicious encryption. Deploy EDR software that uses multiple detection techniques to identify ransomware, and ransomware rollback to restore damaged system files.
- Practice good hygiene. Asset inventory, visibility and observability, patching, etc.
 - Enable multi-factor authentication (MFA) across your organization for all accounts and devices to ensure that only authorized users gain access.
 - Encourage end-users to switch up passwords across applications, accounts, and websites. Use unique, strong passwords and a Password Manager.
 - Address the BYOD issue and err on the side of bad boss – you can lose 80% of your organization and still be fine – lots of examples of that in recent history – the tradeoff for convenience is a fatal breach.
- Keep backups offsite and offline, beyond the reach of attackers. Test them regularly to make sure you can restore essential business functions swiftly.
- Don't get attacked twice. Once you've isolated the outbreak and stopped the first attack, you must remove every trace of the attackers, their malware, their tools, and their methods of entry, to avoid being attacked again.

Vulnerabilites

Make sure the entire organization has a good understanding of the following vulnerabilities:

Insecure DNS

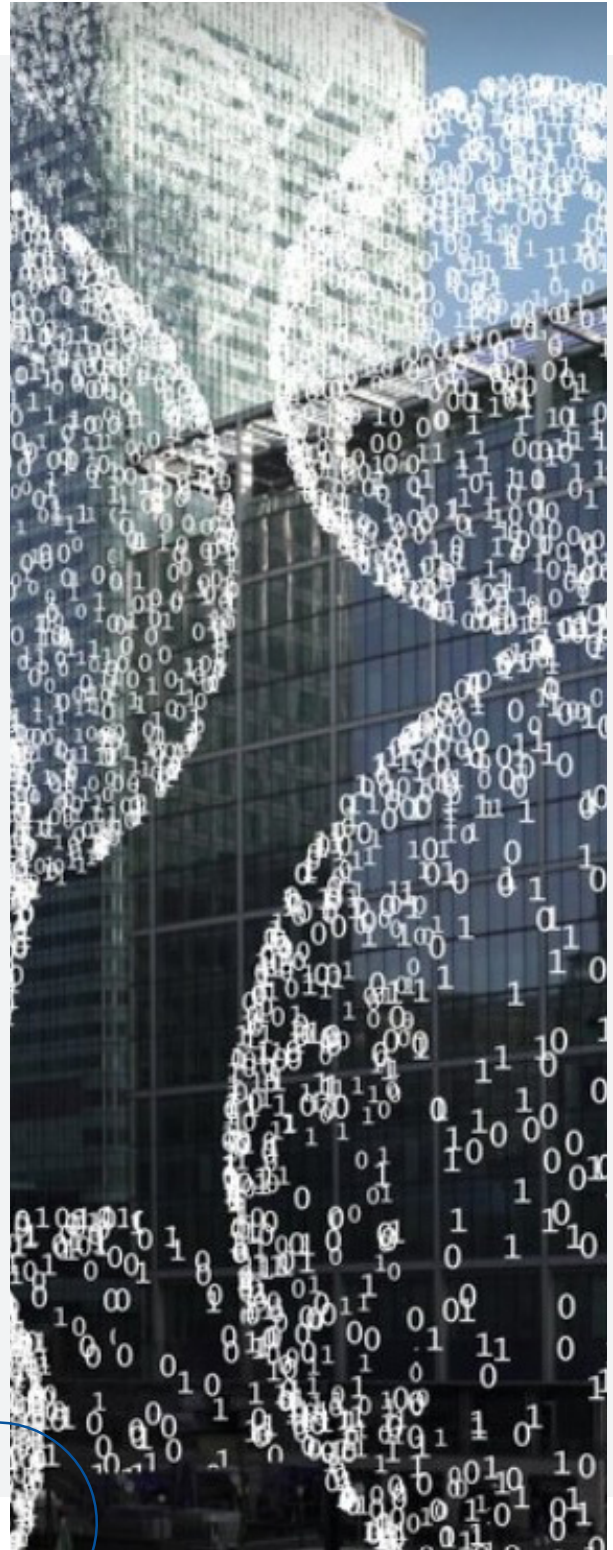
The Domain Name System (DNS) is responsible for translating human-readable domain names (e.g., website.com) into Internet Protocol (IP) addresses. For example, if a user wants to visit the Microsoft website, they type microsoft.com into the address field of the browser they are using.

Completely behind the scenes, a DNS server to which the user's computer is pointed will return this unique IP address, 20.112.250.133, back to the browser, so the browser can create well-formed HTTP Request to send to Microsoft.com and retrieve the information that is available at that website.

In addition to browsers, other Internet applications that utilize DNS to turn human-readable addresses into IP addresses for accessing other Internet domains include e-mail clients, e-commerce applications, business applications, artificial intelligence, gaming applications, education applications, social media applications, the Metaverse, quantum computing, etc.

Cybercriminals target Insecure DNS to redirect users to malicious websites and/or intercept their traffic (aka DNS Cache Poisoning).

DNS hijacking involves altering DNS settings to redirect users to fake websites, where they can be subjected to phishing, malware, and used for DOS attacks (aka DNS Redirection).



Vulnerabilities continued

Not Secure Websites

A website that is not secure means that the connection between the website and your web browser is not encrypted. This means that any information you enter on the website, such as passwords, credit card numbers, or personal information, can be intercepted by a third party.

You can tell if a website is secure by looking at the address bar in your web browser. If the website is secure, the address will typically start with “https” right before the domain name rather than “http.” The “s” stands for secure.



Exploiting Insecure DNS

Cybercriminals manipulate DNS settings, altering the routing of network traffic and redirecting inbound malware payloads to predefined targets.

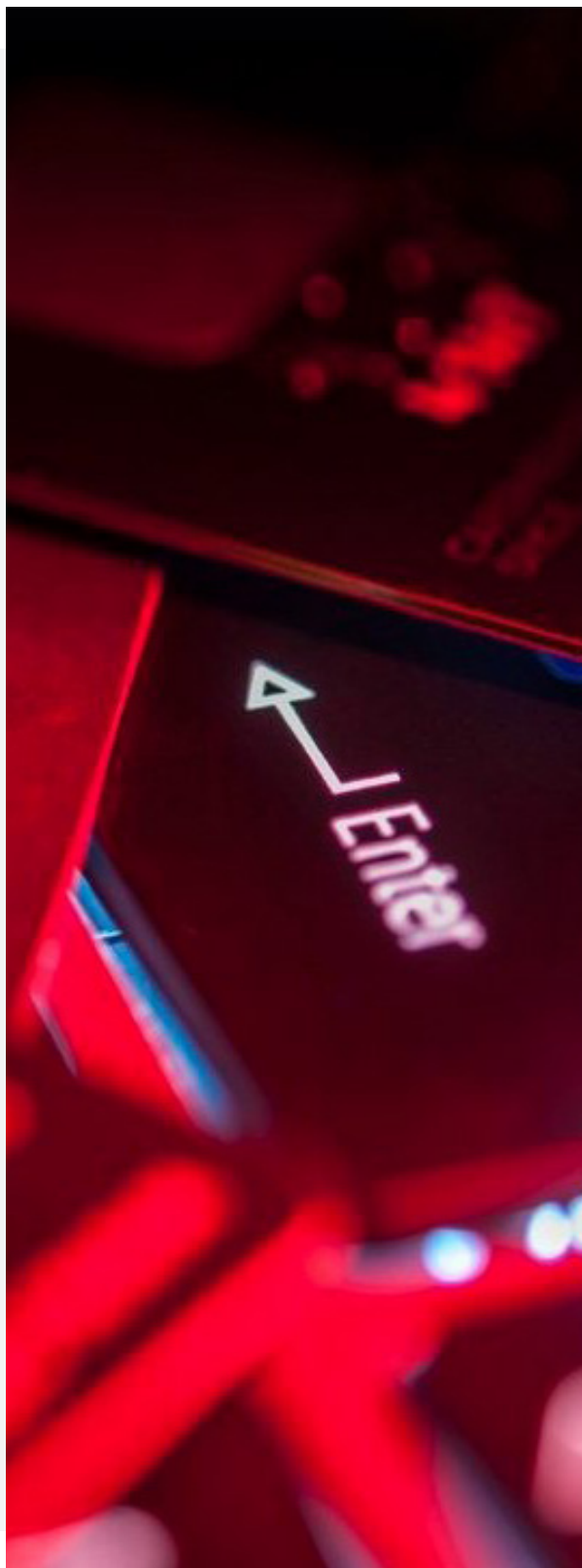
The purpose is to redirect users to fraudulent websites, intercept communications, and/or manipulate data. This attack technique is effective because of the limited visibility most organizations have into DNS and log activity, either because it isn’t monitored, isn’t logged or the log data that is captured is not retained for very long.

Identifying Targets

Cybercriminals have developed enhanced skills in identifying exposed victims and usually programmatically scan for organizations and individuals with Not Secure websites and/or vulnerable insecure DNS configurations.

They are looking for misconfigurations, outdated software, weak security measures, or lax patching practices. The extent to which you are able to eliminate the presence of these vulnerabilities is the extent to which you are able to improve your cybersecurity profile and further reduce the probability of attack.

Vulnerabilites continued



Exploiting Not Secure Websites

Once inside a network, cybercriminals can use Not Secure websites as an entry point for injection of malicious code into your network. The code is designed to capture user data and/or corporate data, distribute malware to invisible locations, establish communications with external C&C entities, and/or redirect users to other malicious sites.

Gaining Access

Exploiting known and exposed vulnerabilities and/or using social engineering techniques, cybercriminals gain unauthorized access to a target's network, websites, and DNS servers and inserting various threat vectors (like SQL injections) that carry payloads designed to capture control of your data and/or systems.

This usually involves exploiting unpatched software, weak passwords, or tricking employees into revealing sensitive information through social engineering. With advances in AI-enhanced messaging, audio and video, it has become nearly impossible to ferret out fakes from real messaging. The best advice is to always verify instructions from superiors or functional departments within your company via telephone, regarding finance or personal identification or the release of any PII or PHI to anyone

Conclusion

Since the Internet became business critical in the late 1990s, it has grown into a vital, essential medium that connects practically every modern business, and as of April 2023, there were about 5.18 billion Internet users worldwide, which amounted to 64.6 percent of the global population of approximately 8 billion people.

Understanding how cybercriminals exploit Not Secure websites and Insecure DNS is vital for organizations to bolster their security measures. By securing websites, implementing robust DNS security protocols, and maintaining vigilant regular monitoring, organizations can significantly reduce the risk of falling victim to cyberattacks.

In addition to these efforts, regular employee training for ALL Employees, especially the executive leadership on identifying phishing attempts and adhering to best security practices is also essential in combating these cyberattack threats.

Each day, safe, secure Internet access and use becomes more important as new users join the Internet, new technologies like generative AI and LLMs transform capabilities and as existing users increasingly expand the ways they use the Internet.

Security, privacy, and safety are no longer “nice to have” nor optional when it comes to Internet access - as the Internet becomes more powerful in light of emerging AI technologies, we might soon require a competency test to be granted an access token that will have to be renewed annually - that frequency matches to rate of change that Cybersecurity professionals must keep pace with in the modern world - the same should be expected of end-users.

A very compelling example of insidious and inadvertent threat can be found in almost every use case for ChatGPT. Completely unbeknown to users, every time source data is shared with the AI engine that is ChatGPT and/or the LLM that fuels it, that data is shared permanently with the world - mining smarts work both ways - as clever as ChatGPT is in responding to complex and inverted queries, it is equally clever in responding to apparently disconnected mining requests - if I were looking for trading insight from Blackstone on Energy Infrastructure futures, I am pretty sure I could get it.

We have a unique opportunity to avoid Internet driving licenses by paying attention to a few simple rules and modifying our own behavior. All it takes is discipline, rigor, some up-front hard learning and a commitment to change, and we can continue to be the masters of our own destiny.




For additional guidance and a greater understanding of custom coursework within the CyberEd.io curriculum that will help advance you and your team toward ransomware mitigation, contact us at CyberEd.io.



CLOSE THE GAP.

Talk to a CyberEd Expert today

Visit cybered.io

 [@cyberedio](https://twitter.com/cyberedio)  [CyberEd.io](https://www.linkedin.com/company/cybered-io)  [CyberEd.io](https://www.facebook.com/CyberEd.io)

CyberEd.io

+1-609-356-1499 • info@cybered.io • cybered.io
© 2023 Information Security Media Group, Corp.