High-Impact Tabletop Exercise - University Data Transfer Software Vulnerability (45 minutes)

Scenario Introduction (5 minutes)

- Present the scenario: "A critical vulnerability has been discovered in 'SecureTransfer', a widely-used file transfer software in the education sector. Your institution, a large public university, uses SecureTransfer for exchanging sensitive data including student records, research data, and financial information."

Round 1: Initial Detection and Response (10 minutes)

- Inject: "The software vendor has just released an urgent security advisory about a zero-day vulnerability in SecureTransfer. There are reports that a ransomware group is actively exploiting this vulnerability."
- Group discussion: What are your immediate actions? How do you prioritize your response?

Round 2: Impact Assessment and Containment (10 minutes)

- Inject: "Initial analysis shows signs of unauthorized access to your SecureTransfer server. The extent of data exposure is unknown, but the server has handled transfers of sensitive student data, cutting-edge research files, and financial records over the past month."
- Group discussion: How do you assess the potential impact? What containment measures do you implement?

Round 3: Stakeholder Communication and Compliance (10 minutes)

- Inject: "Students and faculty are reporting issues accessing certain systems. Local media has caught wind of a potential data breach at the university. The IT department is receiving questions about GDPR compliance."
- Group discussion: How do you manage communication with various stakeholders? How do you address potential regulatory compliance issues?

Debrief (10 minutes)

- What were the key challenges in responding to this scenario?
- How does the diverse nature of university data complicate the response?
- What preparatory steps could help universities better respond to similar incidents?
- How might this scenario impact ongoing research projects or academic operations?
- What are the implications for third-party software use and evaluation in academic settings?

MOVEit Transfer Attack: Quick Reference

Source: Emsisoft Blog July 18, 2023

MOVEit is a file transfer platform made by Progress Software Corporation. The platform is used by thousands of governments, financial institutions and other public and private sector bodies all around the world to send and receive information.

In late May 2023, data started to be transferred from hundreds of MOVEit deployments, however, these were not normal file transfers initiated by legitimate users. MOVEit had been hacked and the data was being stolen by a ransomware operation called Cl0p.

The current tally of organizations and individuals known to have been impacted by this incident is shown below. The data is sourced from state breach notifications, SEC filings, other public disclosures, as well as Cl0p's website, and is current as of June 28th, 2024.

Organizations:	2,773
Individuals:	95,788,491

The MOVEit breaches to have impacted the most individuals are:

Organization	Individuals
Maximus	11.3 million
Welltok	10 million
Delta Dental of California and affiliates	6.9 million
Louisiana Office of Motor Vehicles	6 million
Alogent	4.5 million
Colorado Department of Health Care Policy and Financing	4 million
Oregon Department of Transportation	3.5 million
BORN Ontario	3.4 million
Gen Digital (Avast)	3 million
Teachers Insurance and Annuity Association of America	2.6 million
Genworth	2.5 million
Arietis Health	1.9 million
PH Tech	1.7 million
NASCO	1.6 million
State of Maine	1.3 million
Milliman Solutions	1.3 million
Nuance Communications	1.2 million
Wilton Reassurance Company	1.2 million

U.S.-based organizations account for 78.9 percent of known victims, Canada-based 13.5 percent, Germany-based 1.3 percent, and U.K.-based 0.7 percent.

The most heavily impacted sectors are education (39.1 percent), health (20.1 percent), and finance and professional services (13.3 percent).

While it is impossible to accurately calculate the cost of the MOVEit incident, it is possible to illustrate the potential cost. According to IBM, data breaches cost an average of $165 USD per record. Based on the numbers of individuals confirmed to have been impacted, that puts the cost of the MOVEit incident at $15,805,101,015.

Some of the organizations impacted provide services to multiple other organizations, and so the numbers above are likely to increase significantly as those organizations start to file notifications.

It should be noted that there will be some overlap in terms of individuals impacted. With so many organizations affected, it is inevitable that some individuals will have been affected more than once, and we have no way to account for this.

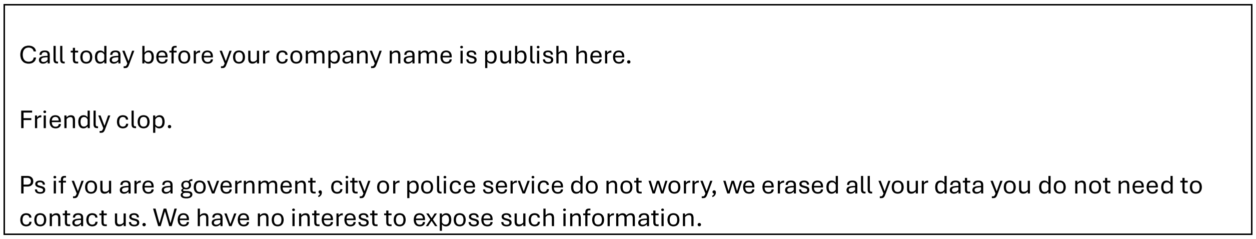
How did it happen?

On May 31st, Progress Software issued an advisory and patch for a vulnerability subsequently identified as CVE-2023-34362 and assigned a severity rating of 9.8 out of 10. The company stated the vulnerability "could lead to escalated privileges and potential unauthorized access to the environment." In other words, it was a vulnerability which could enable hackers to access MOVEit and steal data – something which it later emerged had been happening since at least May 27th.

On June 9th, Progress issued a patch for a second vulnerability identified as CVE-2023-35036. On June 15th, patch was issued for a third vulnerability identified as CVE-2023-35708. Both vulnerabilities were critical and could have enabled the MOVEit platform to be further exploited.

Cl0p confirmed that it had been responsible for the attack on the MOVEit platform with the below June 6th post on the group's site on the dark web.

> Dear companies.
>
> Clop is one of top organization offer penetration testing service after the fact.
>
> This is announcement to educate companies who use progress MOVEit product that chance is that we download alot of your data as part of exceptional exploit we are the only one who perform such attack and relax because your data is safe
>
> We are to proceed as follow and you should pay attention to avoid extraordinary measures to impact you company.
>
> Important We do not wash to speak to media or researchers leave.
>
> Step 1 - f you had MOVEit software continue to step 2 else leave.
> Step 2 - email our team [redacted] or [redacted]
> Step 3 - our team will email you with dedicated chat url over tor
>
> We have information on hundreds of companies so our discussion will work very simple
>
> Step 1 - if we do not hear from you until June 14 2023 we will post your name on this page
> Step 2 - if you receive chat url go there and introduce you
> Step 3 - our team will provide 30% proof of data we have and price to delete
> Step 4- you may ask for 2-3 files random as proof we are not lying
> Step 5 - you have 3 day to discuss price and if no agreement you custom page will be created
> Step 6- after 7 days all you data will start to be publication
> Step 7 - you chat will close after 10 not productive day and data will be publish
>
> What warranty? Our team has been around for many years we have not even one time not do as we promise when we say data is delete it is cause we show video proof we have no use for few measle dollars to deceive you.



Call today before your company name is publish here.

Friendly clop.

Ps if you are a government, city or police service do not worry, we erased all your data you do not need to contact us. We have no interest to expose such information.

As shown in the above screenshot, Cl0p stated that the data which had been stolen from governments, cities and police services had been deleted. On July 17th, 2023, that claim was proven to be inaccurate when the group listed the UK's Office of Communications (Ofcom) and Ireland's Commission for Communications Regulation (Comreg).

The upstream/downstream in many MOVEit incidents is extremely complex, with some organizations being impacted because they used a vendor which used a contractor which used a subcontractor which used MOVEit. Additionally, some organizations have had MOVEit exposure via multiple vendors. This is especially true in the education sector with some institutions being affected by incidents involving the National Student Clearinghouse, the Teachers Insurance and Annuity Association of America-College Retirement Equities Fund (which was impacted by an incident at a vendor: PBI Research Services), as well as third party health insurance providers and other financial service providers.

Who is Cl0p?

Cl0p is a type of ransomware that has been used in cyberattacks since 2019. Data stolen in the attacks is published to a site on the dark web – a so-called "data leak site" or "DLS" – which the hackers refer to as "CL0P^_- LEAKS." The ransomware and website have been linked to FIN11, a financially-motivated cybercrime operation which has been connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505.

While the actors behind Cl0p have previously deployed file-encrypting ransomware, they have increasingly switched to a smash-and-grab, exfiltration-only strategy, relying on the threat of releasing stolen data as leverage to extort payment. This is likely so that Cl0p can quickly exfiltrate data from as many organizations as possible, before the vulnerability being exploited is patched.

This is not the first time the group has attacked a file transfer platform. MOVEit-like attacks were launched against Accellion File Transfer Appliances (FTA) in 2020/2021, SolarWinds Serv-U in 2021, and Fortra/Linoma GoAnywhere MFT servers in 2023.

Looking forward

The MOVEit incident highlights the challenges organizations face in securing their data. It's not only their own security they need to be concerned about, it's the security of their supply chains too. Complicating matters further is the fact that attacks which leverage zero-day vulnerabilities, as this one did, are extremely hard to defend against.

The incident will undoubtedly be extremely costly. Beyond remediation, organizations and their insurers will need to provide credit monitoring to individuals and will undoubtedly face multiple lawsuits. Additionally, there is significant potential for the stolen data to be used in spear phishing, BEC scams, etc., meaning that this one crime could act as an enabler for many other crimes.

The most important question is how we can stop a similar event from happening again. While that is not an easy question to answer, Secure by Design, Secure by Default initiatives could play a critical role.

The bottom line is that organizations cannot be expected to fend off attacks against vulnerable software, and so it needs to be made more secure. Unless we can improve the security of software, it is only a matter of time before there is another MOVEit-like incident.

Additional References

2023 MOVEit data breach
Wikipedia
https://en.wikipedia.org/wiki/2023_MOVEit_data_breach

#StopRansomware: CLOP Ransomware Gang: Exploiots CVE-2023-34362 MOVEit Vulnerrablity
Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

Mass exploitation of critical MOVEit flow is ransacking orgs big and small
Ars Technica
https://arstechnica.com/information-technology/2023/06/mass-exploitation-of-critical-moveit-flaw-is-ransacking-orgs-big-and-small/

Movin' Out: Identifying Data Exfiltration in MOVEit. Transfer Investigations
Crowdstrike Blog
https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/