THE MSP HELD TO RANSOM

MSPs are vulnerable to cyberattacks, and so are their clients

25%

of MSPs experienced a ransomware attack in 2021

73%

of companies identify ransomware as the top method of infiltration

In addition, MSPs can be found liable for any data loss or breach into the companies that have outsourced their IT services from them.

92%

of businesses that pay ransoms do not get their data back

$42 BILLION

the predicted amount of global ransomware damage by 2024

The average cost of a data breach in 2021?

$4.24 MILLION

Here's a fictional scenario representing a typical MSP ransomware attack

DAY ONE

FRIDAY

Jake, a remote working MSP employee, prepares to log out from work and end his day.

Jake receives an email that seems to be from an executive, telling him to download a data report (as an xls file) which will be presented to a client on Monday.

Jake opens the document and skims it. Eh, seems legit, he thinks, then downloads the document.

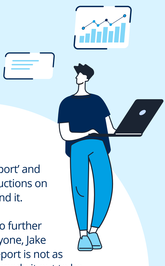
It's 6pm, and Jake logs out for the day.

Unknown to Jake, the document isn't only an xls file; it is carrying malicious ransomware.

Over the weekend, the attackers begin to move laterally in the network, gathering information and carefully exfiltrating files to avoid detection.

DAY FOUR

MONDAY



Jake reviews the 'report' and awaits further instructions on who or where to send it.

When he receives no further instruction from anyone, Jake assumes that the report is not as urgent as the email made it out to be and leaves it to work on other tasks.

It is the middle of the day, and Jake realizes that he is unable to access some company files from his laptop.

Jake emails the security team, thinking it's another connection problem – they've been experiencing these frequently in recent days, ever since they've moved to remote working.

Jake ends his day and logs off.

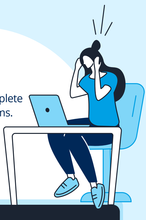
By this point, the attackers have gone through about 25 of the MSP's clients and pulled gigabytes of information from them – passwords, credentials, and PIIs.

A few minutes later, IT receives and reviews Jake's ticket. Unfortunately, they have been too busy preparing the system for two new clients they've signed on.

An IT personnel addresses the ticket by sending instructions to re-configure his connections, adding a note to call the next day if that didn't solve the problem.

DAY FIVE

TUESDAY



The attackers now have complete control over the MSP's systems.

Jake and his coworkers, upon logging in, are greeted by this message dominating their screen:

12:11

We are the Viper999 Ransomware Group, and we have successfully locked you out of your systems and stolen your information.

To get everything back, wire us $300,000 worth of Bitcoin (BTC) through this link, or you'll never get your files back again.

PS. We've taken some important things from your clients, too. That's an extra 100 grand to get those back. ;)

MSP operations grind to a halt. Jake and his coworkers can no longer connect to their entire network. The IT team, aware of the situation, starts scrambling to figure out the spread of the attack.

An hour after receiving the ransom note, a PDF file containing sensitive information of one of their clients is posted online. Attached is a note:

There's plenty more where that came from, MSP XYZ. We'll leak another set of documents in the next hour until we receive the payment.

Internal and client panic ensues.

Executives decide to release a public statement about the data breach. The CEO's phone blows up with calls from the media eager to know the extent of the damage.

After initial analysis, the CFO regretfully reports they will be missing their agreements until the issue is resolved. Because the company doesn't have a backup of their systems, rebuilding the network will take a while.

The CFO also brings up the fact that it's only a matter of time before they receive fines and penalties as a result of the incident.

Sales and CSR teams receive cancellation after cancellation from customers and clients that have been affected by the breach.

DAY TWELVE

THE FOLLOWING TUESDAY

Specialists called to investigate the breach have pinpointed the source of the attack: the email that Jake has received, and the infected attached document that he downloaded.

The high levels of activity on Jake's account over the weekend and outside of office hours have helped the specialists zero in on the delivery method, as well as the type of ransomware that was used in the attack.

Some basic services are returned, but a great swath of the network is still inaccessible. Many employees are still not able to work.

CIO briefs the execs on what the specialists have discovered and their recommendations. A rebuilding of the entire network is indeed necessary, and the CEO acquiesces.

CEO and CFO discuss the financial impact of the incident and prepare a public briefing.