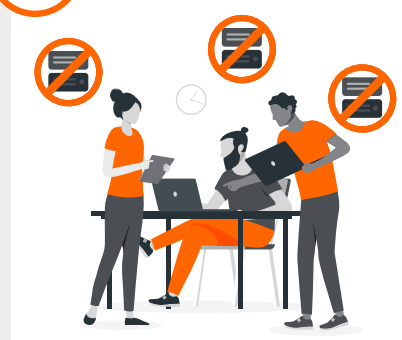
Neglected software vulnerabilities

Many losses can be prevented by patching vulnerable software before cyber criminals have an opportunity to exploit it. The loss examples below highlight the importance of keeping software up to date, and detail the investigative process to assess how known vulnerabilities are exploited and the resulting losses adjusted.

- Server vulnerability wake-up call

1



1. The Event

On 16 July, Example Company's IT team was contacted by external sales to say that they were unable to use any systems. The monitored server statistics showed that many systems were offline. During an initial investigation, the IT team uncovered a message which stated that servers were encrypted. They concluded that the company was the victim of a ransomware attack. Example Company's IT team contacted Chubb's Cyber Incident Response Centre and an incident manager and IT forensics experts were brought on to support the investigation.

Initial inspection of the systems revealed that the threat actor had compromised large parts of the network and infrastructure.

2

2. The Problem

In response, Example Company quickly contained the attack by shutting down servers. By that time, however, the threat actor had already encrypted the virtualised servers and hypervisors in the company's datacentres. While assessing recovery options, they found that it was possible to fully restore the IT environment using backups, as the threat actor was not able to encrypt or damage the backups. Example Company's backup strategy had been updated in the previous 12 months to better protect its IT from ransomware attacks by maintaining cold storage backups and keeping authentication to backup servers that were separate from the Active Directory.

From the next day onwards, IT investigators and forensic experts assisted Example Company by assessing the situation and communicating with the threat actor, while prioritising asset recovery. At the same time, they forensically investigated the root cause and impact of the incident to support a secure and safe recovery. This investigation included examining if the threat actor exfiltrated data for extortion, including verifying the nature and amount of data as claimed in the ransom note.

On reviewing log data within backups, the data showed that on 19 June, nearly one month earlier, the threat actor logged in from 6X.XXX.XX.232 to an SSL-VPN server hosted in Europe with credentials belonging to the account "Fred.Bloggs". The VPN server was managed locally and running version 6.2.0-vr, a version which was not up to date. This login originated from an IP known to be a TOR exit node, which was suspicious as normally a user would not login using the TOR network. The threat actor authenticated again around 25 minutes later, this time using an IP which was geolocated in a country that Example Company did not operate in.

The threat actor increased their access privileges less than an hour later by gaining access to a domain admin account. They were able to do this because the credentials for this account were stored in a configuration file on every domain-connected windows device. This allowed the threat actor to move laterally between the servers and hypervisors located in the UK and Germany which supported Example Company's European operations.

In July, the threat actor created persistence by installing remote access software and a software distribution tool. This allowed them to deploy and spread the ransomware to all servers on the domain. Thankfully, the endpoints — namely laptops and workstations — successfully managed to block the ransomware through an advanced antivirus agent which did not run on the servers.

With no logs showing failed login attempts from the account 'Fred.Bloggs' it was determined that the threat actor had valid credentials rather than performing a brute force attack. Logs also show code activity from the threat actor exploiting a known vulnerability — CVE-2022-123XXX — within the VPN software version 6.2.0-vr. The vulnerability, when exploited, allows a user to obtain recently used valid credentials. The threat actor confirmed this method of entry in the ransom note and during negotiations.

3

3. The Solution

After confirming that the backups were not affected by malware, the data and system recovery efforts and updated configuration work continued for the next five days. These efforts were successful, so there was no need to negotiate further with the threat actor, and no ransom demand was paid.

As listed on the National Vulnerability Database and the VPN software provider's support website, there was a critical vulnerability discovered in version 6 of the software. This allowed credential theft and system entry, and it was first identified in January of this year. It was given a criticality rating in the Common Vulnerability Scoring System (CVSS) of 9.8 and given the identifier of CVE-2022-123XXX. The software provider created a patch for these vulnerabilities on 2 February (version 6.2.1-vr), and on the same day sent an email to their customers, including Example Company, advising users to apply the patch as soon as possible.

4

4. The Outcome

Example Company had 137 days between the patch release and the time that the vulnerability was exploited. The incident response, data and system recovery costs, cyber extortion, and business interruption loss insuring clauses were all initially triggered in response to the cyber incident, subject to the applicable neglected software event limits, excess, and coinsurance listed in the policy schedule for 137 days.

Chubb then adjusted the claim in the standard method, reviewing incident response costs for the Incident Response Manager, IT forensic experts, lawyers and public relations specialists, business interruption loss, data & system recovery costs and the cyber extortion expenses.

Neglected software vulnerabilities

- Known vulnerability, no patching

1

1. The Event

One weekend, Example Company detected unauthorised access to their computer systems and servers. Access was gained through a known, severe, common vulnerability, enabling the hackers access to Example Company's computer systems, servers and data thereon. The hackers encrypted both the systems and exfiltrated data.

2

2. The Problem

With its servers down, Example Company was unable to process or fulfil clients' orders. Employees estimated that for every 24 hours that servers were down the company would lose €750,000 in profit. The hacker demanded a $2m ransom to provide decryption keys and to not publish the exfiltrated data, with a threat to increase the demand periodically if they didn't receive payment.

3

3. The Solution

Example Company reported the incident upon discovery, quickly engaging an Incident Response Manager, who was able to triage the incident based on the initial facts. The Incident Response Manager immediately involved a specialist IT forensic company to assist Example Company with the investigation and containment.

The incident response team further assisted Example Company. They quickly engaged lawyers, public relations personnel and extortion specialists. The team then implemented a mitigation strategy which included identifying servers which could be restored from backups.

Ultimately, no ransom was paid following the IT team and extortion specialists' determination that the exfiltrated data was not sensitive. They discovered that the systems could largely be restored from safely segregated backups that were unaffected by the incident.

The incident response team aided the removal of ransomware from the affected servers, and restoration of the systems, including the patch which would have prevented exploitation of the known vulnerability. The public relations team assisted with communications to clients and the lawyers supported Example Company with notifying the required legal and regulatory bodies.

4

4. The Outcome

Finally, operations were fully restored. The IT forensic team provided a report 10 days after the incident that explained the method by which access was gained, the specific CVE relating to the vulnerability, and the recommended mitigation, including the date on which patches were available but were not deployed.

The incident response, data and system recovery costs, cyber extortion, and business interruption loss insuring clauses were all initially triggered in response to the cyber incident. However, the incident arose from a known vulnerability that was exploited. This was confirmed by the IT forensic report, which established that a patch was available at time of the incident but was not deployed. The report detailed exactly when the hacker gained access to the system and highlighted the length of time that Example Company's systems were unpatched. This enabled them to apply the correct co-insurance and sublimit under the neglected software event limits.