IDC IN CONVERSATION
Sponsored by: Lumen

Cybersecurity is an ongoing concern for all organisations. As attackers become increasingly sophisticated and disruptive, organisations also need to implement better tools, policies and processes as well as ensure that user awareness is in place.

Avoiding Ransomware : Practical or Pipedream

July 2021

Questions posed by: Simon Piff, Vice President of Security Practice, IDC Asia Pacific

Answers by: Cheah Wai Kit, Director of Product Management (Security), Lumen Asia Pacific

IT security is an ongoing battle between cybercriminals and the organisation under attack. Whilst the threat actors are highly motivated, well equipped and funded, those under attack are challenged to find and retain the resources needed to defend their data and network. About 74% of Asia Pacific organisations state that it is hard to recruit talent with digital skills – the number 1 skill in demand is cybersecurity. The only solution is to find a partner that can help improve the organisation's risk profile.

Q1. Security attacks are continually evolving and have become very sophisticated. How should organisations address threats like ransomware which are increasingly targeting work-from-home environments?

A. I firmly believe cyber attacks are already both extremely sophisticated and highly disruptive, therefore it is essential to have visibility of threats, vulnerabilities and weaknesses across the entire network – including endpoints and user activities, to help mitigate cybersecurity attacks. A combination of the "right" tools, policies, processes and user awareness is extremely important. However, tools and software alone are inadequate for tackling multifaceted cybersecurity threats such as ransomware and other advanced persistent threats (APTs).

Furthermore, with attackers often exfiltrating sensitive data and using it as leverage to force victims to pay the ransom, it is no longer sufficient to focus purely upon cyber defence mechanisms that can respond or recover from an attack. Nowadays, organisations must also have robust systems and processes which will alert at the first sign of an intrusion, well before an actual attack is carried out.

As a consequence, it is imperative to have dedicated security experts who are accomplished at hunting, identifying, analysing and mitigating nascent cyberthreats. Nevertheless, for most organisations it is likely to be both time and cost prohibitive to have their security analysts continually trained in identifying and mitigating every single threat. Instead, it is more advisable that they bring in a managed security service provider (MSSP).

This is where Lumen can help. We have one of the largest and most deeply peered IP backbones in the world, giving us expansive, near-real-time visibility into the threat landscape. Plus, through our continued investments in Black Lotus Labs, we have harnessed the power of our global visibility of ~195 billion netflow sessions to quickly identify and disrupt global malicious actors.

Furthermore, through a combination of managed security behavioural analytics (MSBA) or user and entity behavioural analytics (UEBA) and managed endpoint detection and response (MEDR) solutions, Lumen can detect and mitigate most ransomware and advanced persistent threat type attacks in real time. MSBA gives advanced visibility into potential threats including malicious insiders, anomalous activities, data exfiltration attempts and suspicious privilege account activities which can catastrophic repercussions if not mitigated in a timely manner.

With eight 24/7 security operations centre (SOC) facilities, global threat intelligence feeds and comprehensive monitoring/analysis/assessment capabilities, Lumen can provide fast detection, minimise dwell time and protect critical assets, data and applications.

Lumen strongly advocates for foundational cybersecurity hygiene, which encompasses proper patch management policy, strong password and MFA policies, regular backup, VPN access, regular backups, etc. To assist with this objective, Lumen provides our customers with vulnerability assessments, penetration testing and ransomware assessment services allowing organisations a view of potential exploits which may be taken advantage of by threat actors.

Q2. Are there some examples you can share with us?

A. As organisations accelerate their digital transformation journey and increasingly adopt cloud services to support their business, they expect their MSSPs to be able to monitor both on-premise infrastructure as well as cloud environments. With our combination of in-house solutions, skilled people and extensive networking, cloud and managed services experience, Lumen is well suited to support the monitoring, threat detection and response across hybrid environments. For example, for a mid-size organisation on a typical day we are currently detecting an average of 12 incidents of O365 Azure sign-ins from suspicious geolocations, and an average of 10 cases where O365 Sharepoint detects a malware in a file. This illustrates that even on cloud platforms - where many businesses assume they are safe, there are eminent dangers and cyber risks.

In the past couple of years, there has been a steep rise in the volume of ransomware attacks.

In the past couple of years, there has been a steep rise in the volume of ransomware attacks. Even more concerning is that the publicly available statistics are typically reflecting the reported cases, and there are many more attacks which go unreported.

Responding to any cyberattack is a painful exercise, with often significant disruption to operations, and negative impact to reputation or possibly goodwill. Hence, prevention is always better than the cure. We recently helped a non-profit organisation recover from a ransomware attack. It took ~10 days to recover and bring the organisation back online. In scenarios of this nature, it is important to ensure there is no second wave of attack and we prevented that through Lumen's MEDR service.

Q3. How are threat actors circumventing traditional risk mitigation controls?

A. Hackers are increasingly aware of the usual defences organisations typically have in place to mitigate against ransomware attacks. These may include solutions like backup and restore, or even automated tools to decrypt or unlock systems encrypted during a ransomware attack.

However, the primary motive of the attackers is to extort money from the organisation. To achieve their objectives, attackers are now first exfiltrating sensitive data before mounting attacks. Via this method, even if organisations are able to restore their systems, attackers seek to hold them at ransom with the threat of making their sensitive data public, thereby frequently forcing enterprises to pay the ransom amount.

Another approach taken by attackers is to locate the backup systems and either cause data corruption on these systems or encrypt them along with the organisation's IT setup, leaving organisations with limited choices to restore their setup.

These examples point to the importance of proactively defending your system before any malware packages have been delivered. Traditional endpoint detection and response (EDR) solutions and solutions that need manual response mechanisms are not effective against these sophisticated attacks. Modern best practices are that you deploy continuous monitoring, analytics and real-time mitigation to defend your organisation's reputation and data against these sophisticated cyberattacks.

Q4. Not all threats appear to be external, how can these be addressed?

A. Tools and processes are often inadequate if the users do not adhere to safe behaviours and can differentiate between malicious and legitimate engagements. Addressing this area requires effective and ongoing user training. Lumen provides organisations with cybersecurity training for their end users to help them in this endeavour.

Another common pitfalls relate to how most organisations structure their cybersecurity:

1. **The cybersecurity strategy is centred around network:** As the pandemic has demonstrated, employees are not always connected to the Internet via the corporate network (i.e., using enterprise VPN) when they work remotely. For many organisations, the network security apparatus is predominantly focused on hosted IT and applications, leaving endpoints vulnerable to malware and other APTs. Once compromised, these endpoints can be used to propagate to corporate IT systems whenever users connect to the corporate network.
2. **Security is CISO's job:** Often, all responsibility and accountability for security resides with the corporate IT security team.

   For example, many organisations use SAP as an enterprise ERP software. Traditionally, "SAP Security" equated to Segregation of Duties Controls (SoD) based upon user roles and profiles. SoD controls with least privilege is a critical piece of the SAP platform's security along with auditing. However, this approach is normally insufficient as the SoD controls SAP business layers, however, the SAP application layer remains exposed and vulnerable to attack.

Over the past years, Lumen have extended our insider threat detection capabilities into the application layer. As an example, we are monitoring for malicious user activities, excessive volume of data transfers, and file access anomalies of an SAP environment for one of our key customers today. Sometimes, it is the "obscure" activities that we need to keep an eye on (e.g., login from a dormant account into SAP).

This again points back to what I highlighted earlier on the need for organisations to think about security from a holistic perspective and not just from the lens of infrastructure or network.

About the Analyst

Simon Piff, *Vice President of Security Practice*

Simon Piff is Vice President for IDC's Asia Pacific region based in Singapore. He advises both technology and business leaders, as well as IT suppliers on Digital Transformation, the CIO Agenda and Digital Trust, as they relate to the ability of organisations to gain improved returns on their IT investments around hybrid cloud infrastructure, mobile productivity, the value of analytics and Artificial Intelligence (AI).

MESSAGE FROM THE SPONSOR

Lumen is an enterprise technology platform that enables companies to capitalise on emerging applications and power the 4th Industrial Revolution (4IR). This revolution is redefining how we live and work, creating an unprecedented need for an advanced application delivery architecture—designed specifically to handle the complex and data-intensive workloads of next-gen technology and businesses.

Lumen is one of the fastest, most secure platform for next-gen business applications and data, integrating global network infrastructure, cloud connectivity, edge computing, connected security, voice, collaboration and enterprise-class services into a seamless experience.

We integrate network assets, cloud connectivity, security solutions and voice and collaboration tools into one platform that enables businesses to leverage their data and adopt next-generation technologies.

Lumen and Lumen Technologies are registered trademarks of Lumen Technologies LLC in the United States. Lumen Technologies LLC is a wholly-owned affiliate of Lumen Technologies Inc.

IDC Custom Solutions

IDC Asia Pacific
83 Clemenceau Avenue,
#17-01 UE Square West Wing
Singapore 239920
T: 65 6226 0330
Twitter @IDCAP
https://www.idc.com/ap