THE OPPOSITE OF BLACKMAIL – NOT WHITE-MAIL, BUT GREY-MAIL!

The recent spate of security attacks have exposed the severity of loopholes that stay hidden until a hacker uncovers them. The question is – what can enterprises do to be a step ahead – about these unborn bugs?

Pratima H

It is easy to swat a fly or rein in a T-Rex, when it is visible. Of course, the effort, the skills and the expenditure would vary – but at least one knows where to hit. That's exactly what makes hurricanes, bedbugs and unfriendly meteors scary and slippery. How to confront a problem that is not visible!

But that's the advantage that the other side would absolutely love to play with. And that's happening. With a lot of fury and swagger in the last few months. If that surprises you a lot, strap yourself for the stinginess and dismissal that IT players show in sharing avowal and information about these attack-cracks, and their risk-levels. That makes some questions come to life all over again – can vendors and enterprises afford to play an ostrich with a head in the sand or a porcupine? Should we not be clipping the claws of the attacker by being ready, transparent and collaborative? Let's see if that's plausible.

Day Zero is Dooms Day now

Google Chrome, SolarWinds, Microsoft Exchange – one after the other – we have seen how much an unknown bug can cost an enterprise. We have, consequently, also spotted the sheer absence of transparency in the industry – and to what extent it can make an enterprise suffer.

A Ponemon Institute survey – from Intel – unlocked a wide gap between what decision-makers expect from security and what vendors offer. It was noticed that 66 per cent prefer vendors with the "ability to identify vulnerabilities in its own products and mitigate them." But just 46 per cent of these people affirmed that their technology providers have that capability. About 30 per cent expressed confidence in patching a vulnerability in a week or less, but it still takes about six weeks to patch a bug from the time it is first detected. What does not help much is that a lot of it is due to humans – yes, 63 per

cent expressed that delays are caused by "human error."

Consider what CyberArk's CISO 2021 Survey on 'Zero Trust and Privileged Access' sniffed out. Looks like attackers recognize the value of non-IT identities and exploit weaknesses in protecting these identities. People who are facing increased attacks is end-users – including business users with access to sensitive data. About 56 percent reported that such users as being increasingly targeted by attackers. Interestingly, 88 percent of respondents said adopting more of a Zero Trust approach is "very important" or "important."

Zero-day vulnerabilities are undisclosed holes in software packages that have not been publicly acknowledged or patched by the software provider, spells out Sean Duca, Vice President and Regional Chief Security Officer, Asia Pacific & Japan Palo Alto Networks. "There have been reports of activity from several threat actors exploiting four zero-day vulnerabilities affecting Microsoft Exchange Servers. When these vulnerabilities are chained together, threat actors are able to exploit and gain access to Microsoft Exchange servers."

The importance of UX optimization

- Attacks are high against senior leadership (48 per cent), third-party vendors and contractors (39 per cent), and DevOps and cloud engineers (33 per cent).
- Widespread increases in credential theft attempts were reported for personal data (70 percent) and financial systems and data (66 percent). This is clear evidence of attackers' interest in gaining "high-value" access – access to highly sensitive systems that are often held by end-users rather than administrators for example.
- 86 per cent indicate that user experience optimization is "important" or "very important" – this highlights a need for security tools and policies that will not be bypassed or ignored due to security fatigue.

(Source: CyberArk Survey)

- *70 per cent of all attacks involved zero day malware for a 12 per cent jump over the previous quarter - more malware variants evaded signature-based detection and required more advanced detection engines to prevent*
- *67 per cent of all threats were zero day malware*

(Source: WatchGuard Q2 2020 Internet Security Report)

JOHN SHIER, Sr. Research Scientist, Sophos

He argues that for this attack to be successful, the adversary would first need to identify an on-premises Microsoft Exchange Server that is able to receive untrusted connections from an external source on port 443. "If an adversary is successful in securing a connection, they can then exploit CVE-2021-26855 to authenticate themselves as a Microsoft Exchange server. This can be followed by the exploitation of CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 post-authentication, allowing the adversary to gain remote access. If access is achieved, the exploited vulnerabilities will allow threat actors to execute commands remotely, which can include uploading a China Chopper web shell to establish persistence in the compromised system. The web shell would then allow the adversary to steal data and execute additional malicious actions, such as downloading remote files or network service scanning."

Rohan Vaidya, regional director, India at CyberArk encourages the importance of a Zero-trust approach. "The SolarWinds attack and the pace of digital transformation are two factors which have only increased attention on the Zero Trust model in India.

In the Ponemon survey, almost 64 per cent asserted the importance of transparency about security updates and mitigations that are available and yet, we have only 48 per cent who agree that they're getting this kind of communication. Note that about 74 per cent also attach high importance to ethical hacking/bug-hunting to find vulnerabilities within products.

Transparency when it comes to hidden threats and zero-day loopholes – worth talking about?

Honesty Vs. Image – Tough to Juggle

So what can software makers, enterprise vendors and security teams learn from the dust that is settling after what we have seen in the recent months?

John Shier, Sr. Research Scientist, Sophos interprets the recent two events – SolarWinds and Exchange – in light of zero-day readiness. "The search for and disclosure of vulnerabilities has been a healthy business for several years. It may seem like there's been an increase lately, but this is largely due to the media attention being paid to a couple of very high profile events. The concern is the extent to which organizations have been impacted by the SolarWinds incident is still unknown, and the quick adoption of the Exchange vulnerabilities by common cybercriminals. We probably haven't seen the end of the fallout from these two attacks.

The main lesson is that supply chain compromises can happen to anyone, at any time, Shier advises."Organizations need to have a comprehensive on-boarding process. This means they need to assess potential business partners based on a set of requirements that are both security and business focused. In other words, trust but verify."

He also recommends to have a plan for failure. "What happens if you or one of your vendors or business partners experiences a supply chain attack? How do you minimize the impact on your business from a partner's incident?"

Sudarshan Sivaperumal - Security Solutions Architect - F5 agrees thattoday enterprises need to acknowledge and understand that no one is safe from cyber-attacks, not even the authority and security corporations. "I believe that a faster response can save companies millions. Even the most sophisticated attacks are executed with at least one of the key approaches, such as the "Watering hole" technique to distribute malware which has a larger impact and widespread use of the impacted code or software. The use of freely-available code, especially executables and packages needs to be highly scrutinized. It re-emphasizes the fact that credibility and integrity of the code before usage as a crucial step as part of the safe coding practices cannot be neglected. The secure System Development Life Cycle (SDLC) process might have made it possible to catch the attackers in real-time and prevent the catastrophe."

Thankfully, opinions and intents converge when it comes to vendors creating more dialogue and more visibility in the space for everyone – despite competitive boundaries.

SUDARSHAN SIVAPERUMAL, Security Solutions Architect - F5

Vendors – Fight The Common Rival Please

Industry vendors need to make it easy for security researchers to report vulnerabilities, affirms Shier. "Once the vulnerabilities have been analysed and acknowledged, vendors must give as much relevant detail as necessary to allow affected organizations to assess their exposure. Patches must be made available as quickly as possible, and any additional mitigations clearly communicated. Finally, anyone producing software must continuously review their code, at each stage of development, and monitor the deployment process to ensure no unwanted alterations or additions have been introduced anywhere along the development and deployment path."

That does not mean that customers can pass the hot potato every time. "I don't think they should- every organisation should be more or less prepared for one threat over another, in the end it is all risk. An organisation should know what is of value to them, would it cause a material impact if they lost it, someone changed the data or prevented them from getting access to that. That then drives behaviour on if a threat targeted the valuable assets, would they accept the risk, try and avoid the risks targeting them, mitigate it or depending on circumstances could they transfer the risk. This is an organisations risk appetite. Preparedness and planning is key." Duca emphasises.

As the digital and physical worlds become more connected, threat intelligence sharing is becoming an increasingly integral component of any security strategy, explains Sivaperumal. "This includes collecting and sharing intelligence locally across devices in your network, sharing threat intelligence between industries or regional peers, or subscribing to global threat feeds. Some of the biggest and most

complex challenges in the communications world today is when IT vendors deliver products, services, and solutions that interconnect in unique ways, and your customers' expectations around security, stability, and speed are incredibly high Today IT vendors and software makers have the ultimate ownership to ensure that their code does not have any vulnerability and are free from malware."

He stresses that enterprises also need to make sure that they have the right mechanisms for the end-users to check the authenticity and integrity of the code.

As to whether false red-flags, white-hat hackers and zero-day alerts help or complicate the lives of QA teams in enterprises, Srikanth Manoharan, SVP, QA Solutions, Indium Software feels that all these terms are branches of Cyber Security field, which are a manifestation of a carelessly written, mis-managed code or configuration or even an un-tested entity. "They expose the weakness of the Application, though in some cases identified or exploited by insiders. Traditionally, vulnerability-assessments are carried out only after the application becomes functionally stable. In this new transformational era, security testers should be involved much earlier in the development by means of SAST and Threat modelling techniques."

Duca wraps it best. "Our message isn't for the companies that confirmed they were breached – it's for those who are celebrating they dodged this bullet. This is a wake-up call to modernize cybersecurity.

Threat actors use compression utilities

When the web shell is deployed, post-exploitation activity typically occurs in the system, most commonly the use of Procdump to dump Local Security Authority Subsystem Service (LSASS) process memory to obtain credentials. There have also been instances in which threat actors downloaded additional tools, such as Nishang and Powercat, to support their actions. Following the extraction of credentials and data from the compromised system, threat actors often use compression utilities such as 7zip or Winrar to compress and stage the stolen data for exfiltration. It's worth noting that since different groups have leveraged these vulnerabilities, post-exploitation activities may vary depending on the actor behind the attack.

(Source: Palo Alto networks)

SRIKANTH MANOHARAN, SVP, QA Solutions, Indium Software

There are immediate areas that organizations need to focus on to prepare." As the world focuses on the growing list of organizations that have been compromised, there's also a growing list of those that believe they're ok. Many have taken the approach that if they are not running SolarWinds, or a particular version of it, then they can go back to business as usual. He recalls how he saw a security researcher post a picture of a whisky glass with ice and a cigar recommending other security folks to take a break, because he was fearful this could be a long winter. "There is something wrong with this picture. Cyber activity is going to go up, not down. If we all thought cybersecurity was important before, 2020 made it more so. Your brick-and-mortar store is closed, your employees are all connecting from home – your entire business just went digital."

"Against this backdrop, SolarWinds has exposed infrastructure weaknesses in organizations. It's amazing how many were struggling that time to figure out where they were running related products, and how many, and which were affected. Next time it shouldn't take us so long." He warns.

So there it is – the writing on the wall. It might help to be swift. It may work in an enterprise's, and a vendor's, favour to be proactive. It might help more to have a blacklist that helps every customer and vendor without hesitation or competitive hold-backs. But what would help every time, and for everyone - is to be humble, be honest and be ready for the white fox, in a white room while you are tempted to play with snowmen.

The black mail in the paws of a black cat in the black room would suddenly look less eerie.