From Growing Supply Chain Attacks to Ransomware Gangs Putting lives at Risk: Top Cybersecurity Predictions for 2022

By HP'S Security Experts & Advisors

From ransomware pile-ons to increasingly commoditized supply chain TTPs, weaponized firmware exploits and targeted attacks on hybrid workers – the threat landscape is set to evolve at a worrying pace in the year ahead.

As 2021 draws to a close, our HP security experts and advisors have been reflecting on what the year ahead has in store. Here, we include insights from a range of HP security experts – including: Michael Heywood, Supply Chain Security Lead; Joanna Burkey, CISO; Dr. Ian Pratt, Global Head of Security for Personal Systems; Patrick Schläpfer, Malware Analyst; Alex Holland, Senior Malware Analyst; Julia Voo, Global Lead Cybersecurity and Tech Policy; and Michael Howard, Head of Security and Analytics Practice; alongside HP Security Advisory Board member and Partner at Deloitte, Robert Masse – identifying four key trends to look out for.

1. Increasing commoditization of software supply chain attacks could result in more high-profile victims targeted

Supply chain attacks are likely to continue to present new opportunities for threat actors in 2022. According to Michael Heywood: "We'll see supply chain attacks continue to rise over the next year as threat actors search for weak links in software supply chains, targeting software being used widely and globally, or used by a specific company."

As Joanna Burkey explains, this approach could create economies of scale for threat actors: "With the Kaseya breach – which impacted over 1,500 companies – we saw that supply chain attacks can be financially rewarding. This could lead to the continued commoditization of the tactics, techniques, and procedures (TTPs) used to conduct such attacks. This only adds fuel to the fire, giving threat actors more than enough motivation to exploit software supply chains in the next year."

Ian Pratt says both SMBs and high-profile victims may be targeted: "Kaseya demonstrated a pathway to monetization for independent software vendor (ISV) breaches. This should be a wakeup call to all ISVs that even if their customer base doesn't consist of enterprise and government customers, they can still be caught in the crosshairs of attackers looking to exploit their customers. Now that this blueprint is in place, we could see these types of attack become more widespread in the year ahead, targeting both SMBs and high-profile names."

Some verticals are more likely to be targets of supply chain attacks than others, as Robert Masse explains: "Healthcare firms, as well as those in Energy and Resources (E&R), that use lots of different hardware and software from various vendors will be interesting targets for software supply chain attacks. Supply chain integrity will be vital in 2022, as attackers begin launching attacks quicker than organizations can invest in secure software development cycles."

Organizations should also be aware of the threat posed by vulnerabilities in open-source software, as Patrick Schläpfer explains: "We'll see an increase in open-source software packages containing malicious code. Attackers will proactively inject new threats into open-source libraries that feed into software supply chains. This could lead to more companies being compromised, regardless of whether they have a secure perimeter or good overall posture."

2. Ransomware gangs could put lives at risk and engage in 'pile-ons'

Ransomware will continue to be a major risk into 2022, with victims potentially being hit more than once, as Burkey outlines: "What we'll see will be akin to 'social media pile-ons', with ransomware victims repeatedly targeted by threat actors. Once an organization has been shown to be 'soft', others will pile-on to get their share of the action. In some instances, threat actors will hit a company multiple times in double or even triple dip extortion rackets.

Extortion methods could also extend beyond the victim as ransomware gangs apply the pressure, comments Alex Holland: "Ransomware operators will almost certainly intensify the ways they pressure victims into paying their demands. Beyond data leak websites, attackers are using increasingly varied extortion methods, such as cold calling, and contacting customers and business associates of victim organizations." Heywood highlights that ransomware gangs won't just encrypt data, they will steal it too, turning the screws on victims: "As we have seen this year, threat actors will continue stealing data before encrypting devices, putting pressure on victims to pay ransoms to unencrypt systems, and prevent the release of data."

Threat actors could also focus on specific verticals and use cases, as highlighted by Masse: "Attackers have noticed that hitting certain industries will produce a higher likelihood of payment. We could see more attacks on healthcare and E&R organizations. Threat actors may well target high risk devices, such as critical medical support systems and their supporting infrastructure, where the risk of significant harm will be highest and therefore a payout will come quickly. This has already started to happen in regions such as Canada, with surgeries being delayed due to ransomware attacks."

The trend of cooperation between threat actors will continue in the year ahead too, as Pratt explains: "We've seen time and time again that threat actors are willing to cooperate on attacks. There is a vibrant cybercrime marketplace, empowering a criminal supply chain that enables even unsophisticated threat actors to obtain the tools and services needed to launch successful campaigns. Vendors may specialize in stealing credentials, creating exploits, writing email lures, or hosting backend services. The bottom line is that the availability of tools and expertise is enabling the sophistication of criminal attacks to rise."

3. Weaponization of firmware attacks will lower the bar for entry

We could also start to see the trickle down of Nation State developed firmware attacks, which will show the way for cybercriminal gangs to weaponize threats, as Pratt explains: "Firmware provides a fertile opportunity for attackers looking to gain long-term persistence or perform destructive attacks. The security of firmware is frequently neglected by organizations, with much lower levels of patching observed. In the last year we've also seen attackers performing reconnaissance of firmware configurations, likely as a prelude to exploiting them in future attacks. Previously these types of attacks were only used by Nation State actors. But in the next 12-months the TTPs for targeting PC firmware could trickle down, opening the door for sophisticated cybercrime groups to weaponize threats and create a blueprint to monetize attacks."

Masse believes a lack of visibility and control over firmware security will exacerbate the issue: "Certain industries where these attacks could be more probable should start thinking about the risks posed by the weaponization of hardware-level malware and exploits. They are very difficult to detect even in the best-case scenario. Rogue processes and memory mapping bypasses will be hot topics in 2022, and we can also expect to see threat actors targeting CPUs, the BIOS and microcode as part of a revised kill-chain for ransomware attacks."

Policy makers should take note of this trend and enforce change, according to Julia Voo: “The weaponization of hardware-level exploits means that policy makers must step in to develop standards that can help to improve firmware security. By working with industry through a bottom-up approach, policy makers can drive meaningful change in an area that has largely been overlooked.”

4. Hybrid work and sporting events will create more opportunities to attack users

The distribution of teams within hybrid working models means identity management will continue to play a key role, as Burkey highlights: “Identity must be solid, verified and robust. Organizations need to make sure that every activity coming from an endpoint is authentic. Is it really the user conducting these activities? Are they who they say they are? Too many organizations think being behind a firewall is enough to keep an endpoint safe, but this isn’t true. In the era of hybrid work, identity management will never be more important.”

The shift to hybrid work will also continue to create problems for organizational security, says Michael Howard: “Every single employee remains a target for attackers, with the volume of unmanaged and unsecure devices creating a huge attack surface to defend.” Masse believes this could make it easier for attackers to go after high-profile staff: “Threat actors could start to target the homes and personal networks of top executives, even government officials, as these networks are easier to compromise than traditional enterprise environments.”

Phishing will remain an ever-present threat in the era of hybrid work, Pratt explains: “Employees have been using personal devices for work or corporate devices for personal tasks, like checking emails. This will continue, and it’s likely there will be an increase in phishing attacks targeting both corporate and personal email accounts. This essentially doubles attackers’ chances of launching a successful attack, so organizations need to educate the workforce on the risks of their behavior and enforce technical controls to prevent compromise.”

High-profile sporting events will also present new opportunities for attackers to target users, according to Schläpfer: “The Winter Olympics in Beijing and FIFA World Cup in Qatar give threat actors plenty of scope for exploitation. Such large events attract opportunistic attackers, be it a direct attack on organizers, sponsors, participants and fans, or as phishing lures for malware and ransomware campaigns targeted at users. Organizations and individuals alike need to be aware of the risks.”

A new approach to security is needed

“The rise of hybrid working and continued innovation from threat actors means 2022 has plenty of nasty surprises in store for enterprise security,” comments Ian Pratt. “As a result, we need to go about securing the future of work in an entirely different way. Organizations should embrace a new architectural approach to security that helps to mitigate risk and enable resilience. By applying the principles of Zero Trust – least privilege access, isolation, mandatory access control and strong identity management – organizations can drastically reduce the attack surface and secure the future of work.”

HP Wolf Security can help organizations defend against the plethora of new attacks and risks facing them in 2022. By combining hardware-enforced software and security features with industry-leading endpoint security services, HP Wolf Security provides defense-in-depth and enhanced protection, privacy, and threat intelligence, gathering data at the endpoint to help protect the business at large.