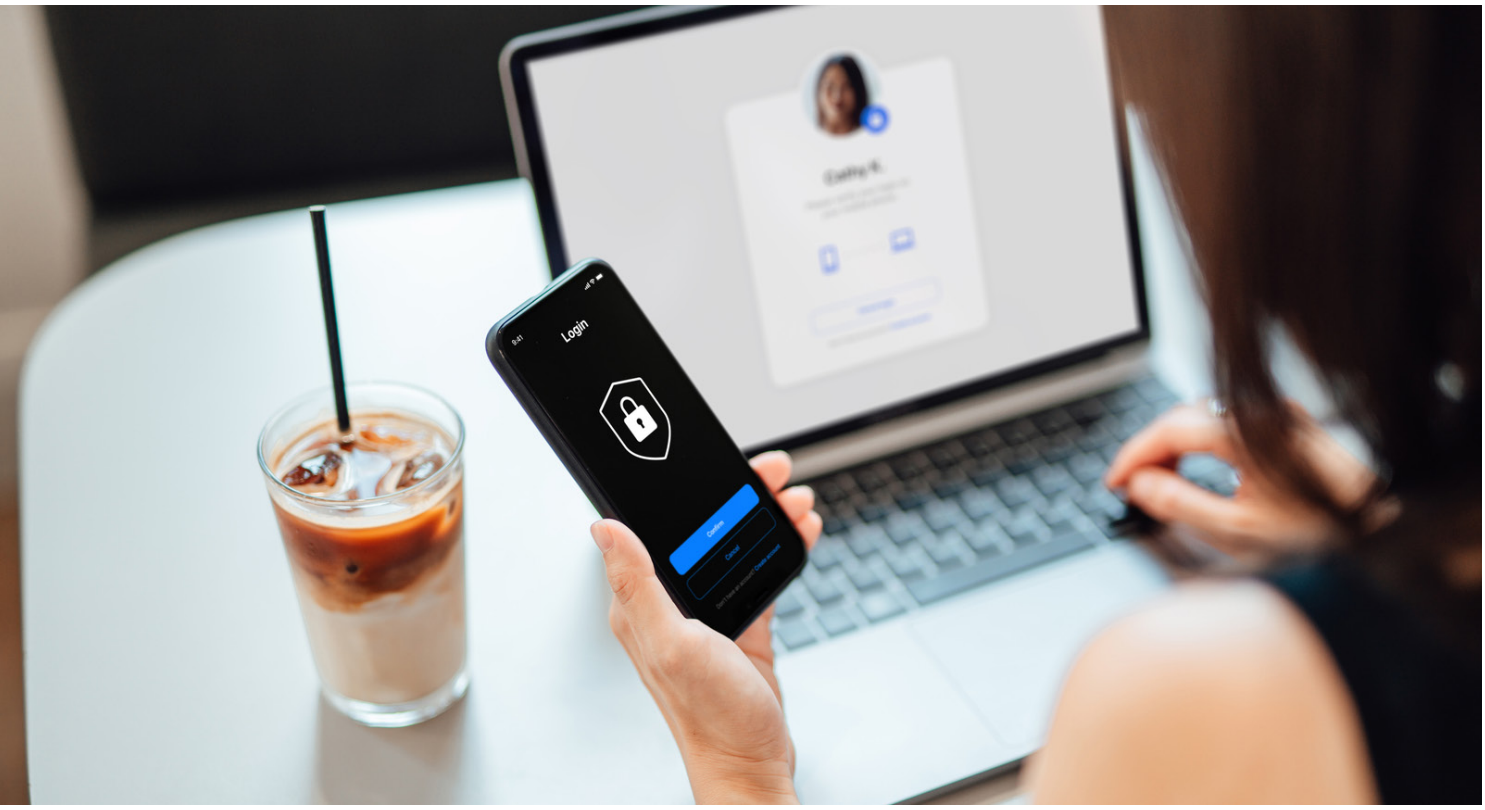
HPE

With ransomware resurging, enterprises need new strategies to build smart defenses — and speed recovery

Experts increasingly suggest a focus on minimizing damage over foolproof detection.



Ransomware is back, baby!

Businesses and individuals alike started to breathe a little easier in 2022 when ransomware attacks fell considerably from the end of 2021. Unfortunately, that trend has since reversed: Ransomware attacks are increasing again and, in fact, are now at an all-time high, up 72% year-over-year in the second quarter of 2023.[1]

"We're seeing a rampant rise in ransomware this year, and I expect that to continue well into 2024," says Chris Rogers, senior technology evangelist at HPE Zerto Software.

You can thank the rise of artificial intelligence for much of that resurgence. Gone are the days of obvious phishing messages filled with bad grammar and broken images. Today's AI-generated phishing attacks are far more sophisticated and look increasingly like the real thing.

"You can run a rough email through an AI, and it can become the most polished thing, with no grammar or spelling errors and with the right branding," says Rogers. "It's going to look exactly as if it was from a reputable company." And each email will be individualized for each recipient, making it even harder to detect.

Rogers adds that AI is also going to drive a new type of attack: deepfakes of people's voices. For example, your boss will call you and instruct you to withdraw money from the company's bank account or buy 100 gift cards to give out to employees as holiday bonuses. But the voice is just a computer simulation, trained to mimic your boss's exact pattern of speech based on a publicly available YouTube™ webinar they participated in.

Rogers says you're right to be scared but adds that in recent months, he's seen a noticeable change in attitude among customers, partners, and prospects. "Most people say they either haven't been hit by an attack or that an attack they experienced wasn't as bad as they thought it would be," says Rogers. That means many may be letting their guard down prematurely.

"People think they're doing pretty well at cybersecurity, even though the statistics back up the fact that most businesses are going to be attacked — and that the attack will be successful at some point."

The message is clear: Security preparations remain essential.

[1] "Q2 Ransomware Report: Global Attacks At All-Time High," Corvus, July 31, 2023

New advice on modernizing your security defenses

Given the grim outlook for ransomware and other attacks, what can you do to prepare for and protect yourself against a future attack?

Rogers says the best advice from prior years still applies but that businesses need to be realistic about their ability to detect attacks. "Ransomware is harder than ever to detect," he says. "And the dwell time is also trending down."

Dwell time is the length of time during which an attacker can linger before the attack is detected or the payload is activated, causing damage to the victim. According to a Cyberint report, the global median dwell time for ransomware was nine days in 2022.[2] It fell to just five days in the first half of 2023. In other words, victims have less time than ever to detect malware on their network before damage is done. "The less time you have, the less chance you have to find the attack," says Rogers.

While organizations will naturally continue to rely on third-party tools to detect incoming attacks, Rogers says this strategy ultimately fails with zero-day-style attacks that leverage brand new exploits. "Most businesses find themselves in a situation where they don't know anything has happened until a user calls and says there is a load of files they can no longer access," he says.

Various security tools are now using AI to assist them in detecting attacks, but today, these are far from a panacea. "I don't think there's any AI product that can make people stop clicking malicious links," Rogers says. "And I don't think cybersecurity products have caught up with attackers when it comes to using AI." That's because there's no penalty if an attacker fails; that time around, they simply don't get their prize and can try again. An AI-based cybersecurity tool would need to be nearly perfect, says Rogers, a promise that's still far off for the emerging technology.

Today, HPE Zerto is taking a more foundational approach to security by scanning data in real time and making a secure copy of it as it is being written to a storage device. "We're about five or so seconds behind real time," says Rogers, "so we're able to quickly raise a flag and tell the security team if something in the environment is going wrong." This approach can limit the blast radius of an attack and help analysts pinpoint where it originated before the attack has a chance to spread to other systems.

Backups get more intricate than ever

The flip side of detection is preparation. And now more than ever, that means taking a smart approach to backups. The days of dropping a tape drive in the corner of the server room and configuring it to run overnight are long gone. And even the long-trusted 3-2-1 rule — three copies of your data on two distinct types of media, with one stored off-site — no longer cuts it.

"All it takes is missing one patch" for an attack to make it through, says Paul Lloyd, a security strategist at HPE. "You must be correct every time. They need to be lucky once. It gets boring to keep hearing that in this business, but the fact is, it's unavoidably true."

The latest backup guidance suggests businesses follow a more aggressive 3-2-1-1-0 backup routine. The same rules as 3-2-1 still apply, but the extra 1 refers to an air-gapped backup that is physically disconnected from the primary network, making it immune to attack from ransomware that could propagate from the primary network.

Air gapping is critical today. "If you can get into the backup from home," says Lloyd, "that means a hacker can too." The new 0 stresses the importance of checking that those backups are reliable, accurate, and complete, with zero errors during recovery testing.

"Criminals want to get in, get their money, and move on to the next target," says Lloyd. The average time to exploit newly discovered vulnerabilities dropped from 63 days in 2018 and 2019 to 44 days in 2020 and early 2021, according to cybersecurity firm Mandiant.[3] By 2022, the average time fell to 32 days.

Lloyd continues, "Attackers are getting faster, and businesses are getting slower at installing patches — making them increasingly vulnerable to attack. We keep getting the fundamentals wrong, and these are bad habits going back decades," he says. "That means in some cases, limiting the spread of a successful attack is probably the best you can do."

A focus on expediting and improving recovery

The good news is that when it comes to recovery after an attack, the situation looks brighter than ever before. "We've got it down to the point where you can recover from an attack within minutes, with only a second's worth of data loss," Rogers says.

The trick isn't recovering data fast but recovering it cleanly. Understanding when an attack began is crucial to this; restoring a backup that has already been infected only compounds the problem.

The implementation of clean rooms and data vaults is a key part of this effort. Once only available to deep-pocketed businesses like large financial or healthcare companies, these environments are becoming more available to the masses as costs come down and usability improves.

[2] "Ransomware Trends Q3 2023 Report," Cyberint, October 11, 2023

[3] "Analysis of Time-to-Exploit Trends: 2021-2022," Mandiant, September 28, 2023

A clean room is an area of infrastructure that is disconnected from the production network, and a data vault is an architecture that stores data in an immutable format. By putting these two together, you get a network that is functionally isolated from any other environment, making it virtually impossible for an attacker to penetrate. With only verified backups stored in the clean room data vault, the user has far greater certainty that any files restored from this environment will be uninfected and safe.

Effective backup verification includes reviewing data during the recovery process to ensure it has not been encrypted or otherwise compromised by a malware product. It also involves restoring data and applications individually, checking and approving them on the fly. If anything is found to be amiss during this process, the restoration can be paused, and an older copy of the data or application can instead be retrieved. Modern security platforms like HPE Zerto's can perform all this work far faster than the previous generation of recovery tools, getting most environments back up and running in a matter of hours instead of weeks.

Today, having a backup and recovery architecture like this is all but mandatory. "If you're not willing to invest in these areas, you're adding risk to your organization," says Rogers.

Don't be discouraged by the complexity of the modern security environment, either. "Seek the expertise you need," says Rogers, "and engage with security service providers that can help manage these things for you."

Visit HPE.com

Learn more at

HPE.com/data

Chat now