Don’t Let Celebrity Vulnerabilities Steal Your Focus

Introduction

Worldwide spending on cybersecurity technology and services is forecast to grow 12.4% to reach $150.4 billion in 2021, according to the latest forecast from Gartner, Inc. In 2020 it was 6.4%.

Despite the continued growth in cybersecurity investment, the number of data breaches and records being compromised, as well as ransomware attacks, reached an all-time high last year. Over 12 billion records containing a range of personally identifiable information were reportedly compromised in 2020, while the number of known ransomware attacks increased by nearly 60%, according to research firm Canalys. Key factors were misconfigurations of cloud-based databases and phishing campaigns targeting unsecured and poorly trained remote workers' systems.

The worse cybercrime gets, and the more publicity certain vulnerabilities attract, the more money companies budget to combat well-publicized threats. Celebrity cybersecurity challenges get all the attention because their names appear in the cybersecurity, and even mainstream, media. Everyone rushes to defend against them because that's where the money is. Many take up the whole front page of the newspaper and consume Twitter feeds, despite being a mere small percentage of the overall total vulnerabilities that are exploited worldwide.

The clock is ticking - while organizations find one vulnerability every 12 hours, it takes attackers **less than** 45 minutes to do the same as they scan the vastness of the internet for vulnerable business assets using malicious automation (MIT Technology Review).

Are celebrities really where security teams should focus though, or are they just shiny objects that distract them from urgent and important?

By the Numbers...

Here are some statistics that demonstrate how difficult it is to protect against vulnerability exploits:

42%: Determined cyberattacks were the result of application software bugs

More than one-third (35%) stated they were attacked via a vulnerable web application. The most common web application vulnerabilities continue to be SQL injection, cross-site scripting, and remote file inclusion.
Source: The State of Application Security, 2020 (Forrester Research)

44%: Say risk assessment and audit are the biggest cloud compliance challenges

Other top regulatory concerns include compliance monitoring (42%); vulnerability monitoring, and staying current with new regulations.
Source: AWS Cloud Security Report 2020 for Management: Managing the Rapid Shift to Cloud (CloudPassage)

80%: Determined data breaches originated with a third party, and 29% of companies have no visibility into the security of their third-party partners.

Third-party breaches are becoming increasingly common, with eight in 10 organizations experiencing at least one such breach over the past year. These organizations reported an average of 2.7 third-party-related breaches.
Source: Third-party cyber risk management survey (BlueVoyant)

85%: Sacrificed security to quickly enable remote work

Nearly 90% of organizations implemented remote work capabilities for employees without addressing security issues first. Unsurprisingly, 25% reported ransomware or other malware attacks in the first three months of the pandemic.
Source: 2020 Cyber Threats Report (Netwrix)

History of Bug Branding Over Time

Bug branding used to be limited to simple CVE numbers, but researchers have recently used a new branding tool with edgy names, eye-catching logos, and websites to match. As an advantage, bug branding raises awareness and catches the attention of people who wouldn't typically understand or care about cyberattacks. Through marketers, they grab and hold the attention of clients, customers, and the general population who may have less knowledge than those with computer-systems backgrounds, distracting security teams from what is truly urgent and important.

Though some note the disadvantages of the marketing aspect being too prominent, claiming it's simply a ploy and draws more attention to cyberattacks than necessary. Some argue that time spent branding these bugs would be better served researching vulnerabilities in order to serve clients better. Branding does get people to pay attention, though, which with emerging trends is more necessary than before.

Trends show that the frequency of unpatched vulnerabilities has increased in recent years and will likely continue to do so.

"More than 600 ICS vulnerabilities were disclosed during the 1H of 2021, affecting 76 vendors. A large percentage of those vulnerabilities were both remotely exploitable and classified as either critical or high risk."

Source: https://security.claroty.com/1H-vulnerability-report-2021

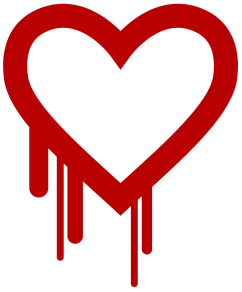
Top celebrities

- **2010:** Stuxnet - CVE-2010-2772

Stuxnet was the first weaponized cyber attack against an industrial system. It infiltrated Windows and PC systems in order to steal data while also concealing its detection from the victim. This targeted attack was conceptualized with the victim and stolen information in mind beforehand through an infected device such as a USB drive.

- **2014:** Shellshock - CVE-2014-6271 and Heartbleed CVE-2014-0160

Shellshock allowed attackers to exploit through remote code execution, executing a command remotely on a server. Found in Unix Bash shell, the vulnerability is easy to exploit through web applications as the attacker creates an HTTP request.



Heartbleed was a vulnerability in SSL which tricks a computer into sending secure and private information through a heartbeat message. It reveals the contents of the RAM and can allow one access to a private encryption key that can even lead to server impersonation. Affected websites such as Tumblr, Google, Yahoo, Intuit, Dropbox, Netflix, and Facebook have since fixed the bug.

- **2018:** Spectre CVE-2017-5753, CVE-2017-5715 and Meltdown CVE-2017-5754

Spectre is a class of security vulnerabilities that affects modern microprocessors that perform branch prediction and other forms of speculation. On most processors, the speculative execution resulting from a branch misprediction may leave observable side effects that may reveal private data to attackers.

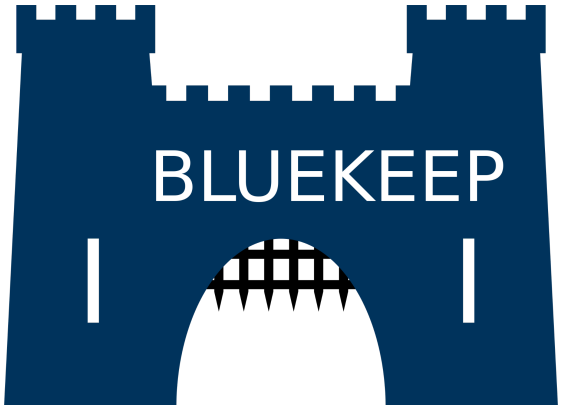
Meltdown is a hardware vulnerability affecting Intel x86 microprocessors, IBM POWER processors, and some ARM-based microprocessors.It allows a rogue process to read all memory, even when it is not authorized to do so. At the time of disclosure, this included all devices running any but the most recent and patched versions of iOS, Linux, macOS, or Windows.

The basic difference between Spectre and Meltdown is that Spectre can be used to manipulate a process into revealing its own data. On the other hand, Meltdown can be used to read privileged memory in a process's address space which even the process itself would normally be unable to access.

In early 2018, Intel reported that it would redesign its CPUs to help protect against the Spectre and related Meltdown vulnerabilities. Almost every computer system could be affected by Spectre, including desktops, laptops, and mobile devices. Specifically, Spectre has been shown to work on Intel, AMD, ARM-based, and IBM processors.

Since Spectre and Meltdown represent a whole class of attacks, there cannot be a single patch that makes this type of attack so difficult to mitigate without efficient and effective processes and technology in place to inhibit a rapid response.

- **2019:** BlueKeep CVE-2019-0708



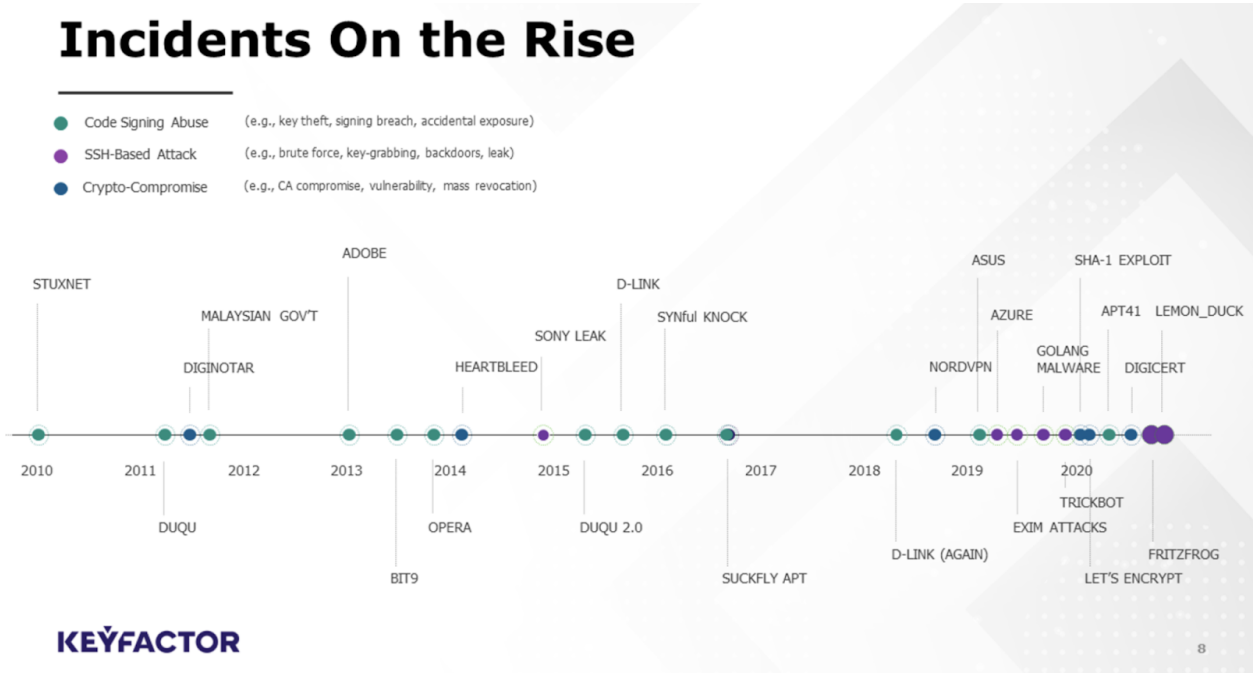
BlueKeep is a software breach that disturbs older versions of Microsoft Windows, attacking a system's RDP and spreading rapidly. The threat could continue from one computer to the next, without users even interacting with one another, and resulted in the changing of data, creation of new user profiles, and installation of malicious programming. Microsoft began insisting that users who ran older versions update their operating systems immediately in order to avoid the vulnerability, while also patching and updating current systems to avoid the attack.

- **2020:** Microsoft Exchange RCE CVE-2020-0688

In another attack on Microsoft systems, the Exchange RCE exploited targeted emails, enabling the vulnerability to browse and leak emails from various accounts. The attackers were able to bypass user authentication and steal login credentials, remotely executing commands and overtaking servers.

- **2021:** Solarwinds Serv-U CVE-2021-35211

SolarWinds was the victim of a major cyberattack that was undetected for several months and subjected the spread to its clients. The vulnerability allowed the attackers to spy on private companies and even elite sections of the US government. Malicious code was added to the company's regular updates sent to clients, to which the hackers would then infiltrate the clients' systems and install more malicious software.



Best practices

- **Speed:** Speed is key in preventing, detecting, and responding to cyber-attacks. As soon as a vulnerability is detected, it becomes a race to secure the breach before the attacker can steal any secure information from the user or asset. A plan must be prepared and rapidly implemented in order to safeguard impaired services, data, or capabilities.
- **Attack Surface Management:** Discover and manage organizational asset inventory, top priority for CISOs, and security teams. The smaller the attack surface, the less you have to protect. The overall range of attacks criminals could use to manipulate your computer system includes known assets, unknown assets, rogue assets, and vendors, all of which appear on the internet every day.
- **Risk-Based Vulnerability & Configuration Management:** Prioritize what is important for your specific organization (network, device, user, and asset). Focus efforts so that you can have insight into the most impactful parts of business threats. Protect and secure the most important data first and foremost and work backward from there, ensuring top tiers of valuable information receive the highest level of protection.
- **Security IT Operational Workflow & Collaboration**: Automated Remediation speeds up the process of problem-solving. This includes automatically creating vulnerability remediation tickets for IT teams to deploy patches and directing attention to the root cause of issues. Doing this also allows one to aid in the prevention of future attacks, as it automatically executes the best security practices that were previously defined.

- **Risk Simulation & Attack Emulation:** Gamification to improve operational readiness strengthens the combat in the event of an attack. These practices are an advanced form of security through threat modeling and are used by organizations to better prepare and defend against breaches before they happen. They invoke preparedness for when attacks eventually (and inevitably) happen. Simulation and emulation enable organizations to predict the effect on risk reduction of various alternative remediation efforts to determine how to most effectively utilize their limited resources to reduce risk from vulnerabilities.
- **Security Program & ROI Reporting:** Measure key metrics and drive results to evaluate and understand the cost and performance of your cybersecurity program over periods of time. Useful for executives and marketing teams to evaluate profitability and efficiency.
- **Risk is everyone's responsibility:** Leverage synergy across IT Operations and Security.

Summary

Even though one can't forewarn when a cybersecurity attack will occur, you can do your absolute best to prepare for one to keep data, clients, and your business secure. Staying vigilant is paramount and maintaining a routine of best practices makes for a more robust and secure system. Focus on the best practices for cybersecurity hygiene - keep routine things routine. Automation is the key to speed and quickly securing systems in the event of an attack. Regarding attacks, never focus on the latest craze by sacrificing the fundamentals, as that rabbit hole will be an endless and unnecessary journey in the wrong direction. Maintain clarity on the most critical assets so that security won't be a question; it will be a given.

Celebrity vulnerabilities are essential to track, but organizations cannot take their eyes off other vulnerabilities. For all vulnerabilities, they need to take a risk-based approach to prioritization and remediation.

Next Steps

NopSec operates with one mission - to help people make better decisions to reduce security risks. The NopSec Team is passionate about building technology to help customers simplify their work, manage exposure risks effectively, and empower them to make more informed decisions. NopSec's software-as-a-service approach to Cyber Exposure Management offers an intelligent solution to dramatically reduce the turnaround time between identifying critical vulnerabilities, despite their celebrity status, and automated remediation.

Learn how to manage your exposure to threats and request a demo today.

[Schedule a Demo Today!]