Palo Alto Networks Unit 42 Incident Response Report Reveals that Phishing and Software Vulnerabilities Cause Nearly 70% of Cyber Incidents

July 26, 2022

The 2022 Unit 42 Incident Response Report reveals trends, future implications and offers recommendations based on data gathered from a year's worth of investigations

SANTA CLARA, Calif., July 26, 2022 /PRNewswire/ -- According to a new report from Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, the heavy use of software vulnerabilities matches the opportunistic behavior of threat actors who scour the internet for vulnerabilities and weak points on which to focus. The 2022 Unit 42 Incident Response Report offers a multitude of insights gleaned from Unit 42 by Palo Alto Networks extensive incident response (IR) work, leveraging a sampling of over 600 Unit 42 IR cases, to help CISOs and security teams understand the greatest security risks they face, and where to prioritize resources to reduce them.

In the report, Unit 42 identified that finance and real estate were among the industries that received the highest average ransom demands, with an average demand of nearly $8 million and $5.2 million, respectively. Overall, ransomware and business email compromise (BEC) were the top incident types that the Incident Response team responded to over the past 12 months, accounting for approximately 70% of incident response cases.

"Right now, cybercrime is an easy business to get into because of its low cost and often high returns. As such, unskilled, novice threat actors can get started with access to tools like hacking-as-a-service becoming more popular and available on the dark web," said Wendi Whitmore, SVP and head of Unit 42 at Palo Alto Networks. "Ransomware attackers are also becoming more organized with their customer service and satisfaction surveys as they engage with cybercriminals and the victimized organizations:

Key trends covered in the report include:

Ransomware
A new ransomware victim is posted on leak sites every four hours. Identifying ransomware activity early is critical for organizations. Typically, ransomware actors are only discovered after files are encrypted, and the victim organization receives a ransom note. Unit 42 has identified that the median dwell time — meaning the time threat actors spend in a targeted environment before being detected — observed for ransomware attacks was 28 days. Ransom demands have been as high as $30 million, and actual payouts have been as high as $8 million, a steady increase compared to the findings of the 2022 Unit 42 Ransomware Report. Increasingly, affected organizations can also expect threat actors to use double extortion, threatening to publicly release sensitive information if a ransom isn't paid.

BEC
Cybercriminals used a variety of techniques in business email compromise wire-fraud schemes. Forms of social engineering, such as phishing, offer an easy and cost-effective way to gain covert access while maintaining a low risk of discovery. According to the report, in many cases cybercriminals are simply asking their unwitting targets to hand over their credentials — and getting them. Once they have access, the median dwell time for BEC attacks was 38 days, and the average amount stolen was $286,000.

Affected Industries
Attackers follow the money when it comes to targeting industries; however, many attackers are opportunistic, simply scanning the internet in search of systems where they can leverage known vulnerabilities. Unit 42 identified the top affected industries in incident response cases as finance, professional and legal services, manufacturing, healthcare, high tech, and wholesale and retail. Organizations within these industries store, transmit and process high volumes of monetizable sensitive information that attracts threat actors.

The report also reveals some statistics from IR cases that cyberattackers don't want you to know:

- The top three initial access vectors used by threat actors were phishing, exploitation of known software vulnerabilities and brute-force credential attacks focused primarily on remote desktop protocol (RDP). Combined, these attack vectors make up 77% of the suspected root causes for intrusions.
- ProxyShell accounted for more than half of all vulnerabilities exploited for initial access at 55%, followed by Log4J (14%), SonicWall (7%), ProxyLogon (5%) and Zoho ManageEngine ADSelfService Plus (4%).
- In half of all IR cases, our investigators discovered that organizations lacked multifactor authentication on critical internet-facing systems, such as corporate webmail, virtual private network (VPN) solutions or other remote access solutions.
- In 13% of cases, organizations had no mitigations in place to ensure account lockout for brute-force credential attacks.
- In 28% of cases, having poor patch management procedures contributed to threat actor success.
- In 44% of cases, organizations did not have an endpoint detection and response (EDR) or extended detection and response (XDR) security solution, or it was not fully deployed on the initially impacted systems to detect and respond to malicious activities.
- 75% of insider threat cases involved a former employee

Unit 42 Incident Response Services
Palo Alto Networks Unit 42 has an experienced team of security consultants with backgrounds in public and private sectors who have handled some of the largest cyberattacks in history. They manage complex cyber risks and respond to advanced threats, including nation-state attacks, advanced persistent threats, or APTs, and complex ransomware investigations. Unit 42 incident response experts are available 24/7 to help clients understand the nature of the attack and then quickly contain, remediate and eradicate it. They utilize a proven methodology and battle-tested tools developed from real-world experiences investigating thousands of incidents.

Further detail on future predictions, tips to stay safe, additional data points and more can be found in the "2022 Unit 42 Incident Response Report," which can be downloaded on the Palo Alto Networks website. A summary of the report is available on the Unit 42 blog.

About Unit 42
Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach and respond to incidents in record time so that you get back to business faster. Visit paloaltonetworks.com/unit42.

About Palo Alto Networks
Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-unit-42-incident-response-report-reveals-that-phishing-and-software-vulnerabilities-cause-nearly-70-of-cyber-incidents-301593041.html

SOURCE Palo Alto Networks, Inc.

Kelly Kane, Senior Manager, Threat Communications, Palo Alto Networks, kkane@paloaltonetworks.com