

Ransomware Payments Hit New Records in 2021 as Dark Web Leaks Climbed, According to New Report from Palo Alto Networks Unit 42

March 24, 2022

*Average ransom demand rose 144% to \$2.2 million. Average payment rose 78% percent to \$541,010.
Posts on name-and-shame Dark Web leak sites climbed 85%.*

SANTA CLARA, Calif., March 24, 2022 /PRNewswire/ -- Ransomware payments hit new records in 2021 as cybercriminals increasingly turned to Dark Web "leak sites" where they pressured victims to pay up by threatening to release sensitive data, according to research released today from Unit 42 by Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader.

The average ransom demand in cases worked by Unit 42 incident responders rose 144% in 2021 to \$2.2 million, while the average payment climbed 78% to \$541,010, according to [The 2022 Unit 42 Ransomware Threat Report](#). The most affected industries were Professional and Legal Services, Construction, Wholesale and Retail, Healthcare, and Manufacturing.

"In 2021, ransomware attacks interfered with everyday activities that people all over the world take for granted – everything from buying groceries, purchasing gasoline for our cars to calling 911 in the event of an emergency and obtaining medical care," said Jen Miller-Osborn, deputy director, Unit 42 Threat Intelligence.

The Conti ransomware group was responsible for the most activity, accounting for more than 1 in 5 of cases worked by Unit 42 consultants in 2021. REvil, also known as Sodinokibi, was No. 2 at 7.1%, followed by Hello Kitty and Phobos (4.8% each). Conti also posted the names of 511 organizations on its Dark Web leak site, the most of any group.

The report describes how the cyber extortion ecosystem grew in 2021, with the emergence of 35 new ransomware gangs. It documents how criminal enterprises invested windfall profits into creating easy-to-use tools in attacks that increasingly leverage zero-day vulnerabilities.

The number of victims whose data was posted on leak sites rose 85% in 2021, to 2,566 organizations, according to Unit 42's analysis. 60% of leak site victims were in the Americas, followed by 31% for Europe, the Middle East and Africa, and then 9% in the Asia-Pacific region.

Detailed commentary, analysis and breakdowns on activity by region, industry and ransomware groups are available in the [2022 Unit 42 Ransomware Threat Report](#), which can be downloaded on the Palo Alto Networks Website. A summary of the report is available on the [Unit 42 blog](#).

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners. Any unreleased services or features (and any services or features not generally available to customers) referenced in this or other press releases or public statements are not currently available (or are not yet generally available to customers) and may not be delivered when expected or at all. Customers who purchase Palo Alto Networks applications should make their purchase decisions based on services and features currently generally available.

About Unit 42

Unit 42 brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide state-of-the-art incident response and cyber risk management services. Our consultants serve as your trusted advisor to 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. Visit paloaltonetworks.com/unit42.



View original content to download multimedia: <https://www.prnewswire.com/news-releases/ransomware-payments-hit-new-records-in-2021-as-dark-web-leaks-climbed-according-to-new-report-from-palo-alto-networks-unit-42-301509636.html>

SOURCE Palo Alto Networks, Inc.