Venafi

Global Security Report: Rapid Increase in Ransomware Threats Drives Need for Security Controls That Break the Kill Chain

93%

Ransomware has plagued organizations for years. But now it's increasing faster than ever, with the number of ransomware attacks increasing by 93% in the first half of 2021 over the same time period in 2020[1].

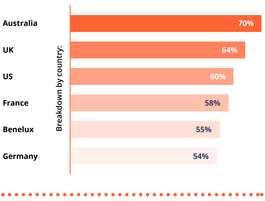
By the end of 2021, it's estimated that an organization will be hit by ransomware every

11 seconds.

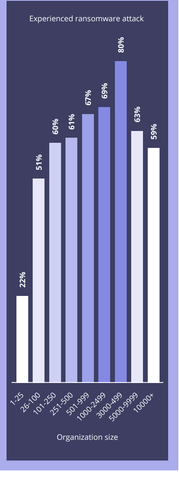
The U.S. Department of Justice (DOJ) said the agency would now treat ransomware attacks at the level it previously reserved only for terrorism[2].

Overall, 60% of InfoSec leaders agree with the DOJ's decision to prioritize ransomware threats at the same level as terrorism.

60%

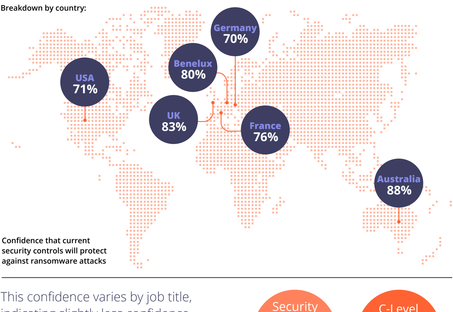


Larger organizations are experiencing more ransomware attacks.



77% are confident that their current security tools will protect them from a ransomware attack.

Breakdown by country:



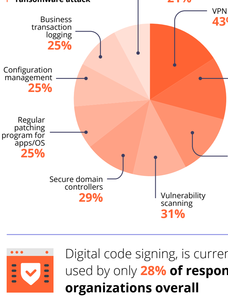
Confidence that current security controls will protect against ransomware attacks

This confidence varies by job title, indicating slightly less confidence from security team leaders than from C-level executives in the efficacy of their current toolsets

Security Leader Confidence 69%

C-Level Executive Confidence 80%

Organizations use a wide variety of security controls designed to protect against or limit the impact of a ransomware attack



Only three are designed to add specific new layers of control for cloud and DevOps environments that help to break the ransomware kill chain. Yet these three tools have very low adoption rates.

Ransomware-specific security controls

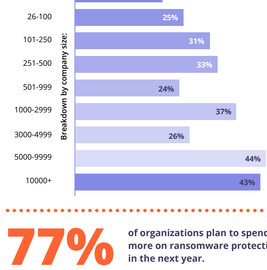
28% Require all software be digitally signed by their organization before employees are allowed to execute it

21% Restrict execution of all macros within Microsoft Office documents[3]

18% Restrict use of PowerShell using group policy

Digital code signing, is currently being used by only **28% of respondent organizations overall**

Percentage of respondents that say they require all software be digitally signed by their organization before their employees are allowed to execute it is relatively low (divided by company size):



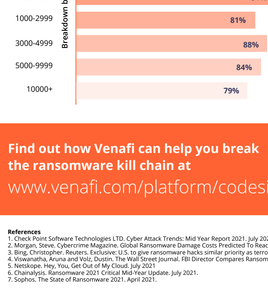
43%

of all malware downloads are malicious Office documents in July 2021, up from 20% at the beginning of 2020

Restrict execution of all macros within Office documents (21% overall):		Restrict use of PowerShell using group policy (18% overall):	
1-25	15%	1-25	12%
26-100	21%	26-100	17%
101-250	23%	101-250	17%
251-500	18%	251-500	26%
501-999	23%	501-999	22%
1000-2999	25%	1000-2999	18%
3000-4999	33%	3000-4999	21%
5000-9999	30%	5000-9999	30%
10000+	28%	10000+	24%

77% of organizations plan to spend more on ransomware protection in the next year.

These numbers suggest that security teams realize their current strategies do not provide enough protection, along with the likelihood that ransomware threats will continue to increase in 2022.



$416 million

In 2020, the total amount of ransom paid by cyberattack victims added up to nearly $416 million in cryptocurrency. This figure is projected to double in 2021 and double again in 2022[4].

Moreover, Sophos predicts the total average cost to remediate ransomware attacks will be US$1.85 million in 2021, more than double the US $761,106 cost reported in 2020[7].

Find out how Venafi can help you break the ransomware kill chain at

www.venafi.com/platform/codesign-protect

References

1. Check Point Software Technologies LTD. Cyber Attack Trends: Mid Year Report 2021. July 2021.
2. Morgan, Steve. Cybercrime Magazine. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. October 21, 2019.
3. Bing, Christopher. Reuters. Exclusive: U.S. to give ransomware hacks similar priority as terrorism. June 3, 2021.
4. Viswanatha, Aruna and Volz, Dustin. The Wall Street Journal. FBI Director Compares Ransomware Challenge to 9/11. June 4, 2021.
5. Netskope. Hey, You, Get Out of My Cloud. July 2021.
6. Chainalysis. Ransomware 2021 Critical Mid-Year Update. July 2021.
7. Sophos. The State of Ransomware 2021. April 2021.