Major Ransomware Attacks, Groups and Variants Since WannaCry

CyberTalk.org

2017 | 2018 | 2019 | 2020 | 2021 | 2022

WannaCry
May 2017

This large-scale and highly publicized attack demonstrated that ransomware attacks were possible and profitable. Since then, dozens of ransomware variants have been developed and used in a variety of attacks.

NotPetya
Jun 2017

NotPetya is not ransomware at all; it's wiper malware that masquerades as ransomware. It demanded payments, but the code had no way to provide the malware's operators with a decryption key thereby, making recovery of encrypted files impossible.

Ryuk
Aug 2018

Ryuk ransomware is extremely targeted and each victim must receive the individual attention of the cyber criminals operating the malware. As a result, Ryuk is used in targeted campaigns with highly tailored infection vectors and high ransom demands.

REvil / Sodinokibi
May 2020

REvil is one of the most well-known ransomware groups. It has been responsible for many big breaches such as 'Kaseya' and 'JBS' and is known to have demanded $800,000 ransom payments.

Microsoft Exchange
Jan 2021

Volexity reported exploitation of Microsoft Exchange Server vulnerabilities. An investigation uncovered that an attacker was exploiting a zero-day, using the vulnerability to steal full contents of mailboxes. This vulnerability is remotely exploitable and doesn't require authentication or access to a specific environment.

JBS Meat
May 2021

This widely covered attack targeted JBS S.A., the biggest meat processing company in the world. It had international impacts, causing shutdowns of plants in the US and Australia that resulted in cancellations of 3,000 workers' shifts and furloughs of 7,000 employees.

Colonial Pipeline
May 2021

With this attack, ransomware groups demonstrated their ability and willingness to impact organizations beyond their direct targets. IT is the work of the Dark Side ransomware and caused a week-long shutdown of one of the main pipelines servicing the US East Coast.

Kaseya
Jul 2021

This supply chain exploit leveraged relationships between MSPs and customers to distribute ransomware using MSPs' remote monitoring and management software. Months later, an attacker with access to the npm account of a widely-used library, modified the code so that malware was installed on the systems of anyone who downloaded and used the malicious version of the library.

Lapsus$
Dec 2021

This South American ransomware gang attacks high-profile targets and is known for extortion, threatening the release of sensitive information if demands aren't met. They use stolen source code to disguise malware files as trustworthy.

Conti
Mar 2022

Structured like a high-tech company, Conti is a Ransomware-as-a-Service (RaaS) group, that allows affiliates to rent access to its infrastructure to launch attacks. Industry experts have said Conti is based in Russia and may have ties to Russian intelligence.