TOP RANSOMWARE FAMILIES AND TECHNIQUES

REVIL

Main Entry Methods:
Made headlines in 2021 for using a zero-day vulnerability in Kaseya's VSA software for a widespread supply chain attack.

Impact:
The attack directly affected at least **60** firms—and it had downstream consequences for at least **1,500** companies.

Cost:
A post on the cybercrime gang's dark web page promoted a universal decryptor that could unscramble all data impacted by the attack—for the bargain price of **$70 million**.

[Source: Tessian & The Hacker News]

NETWALKER

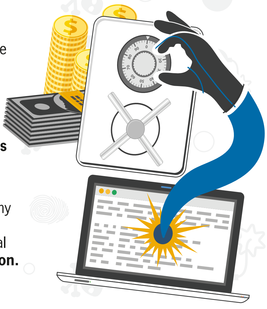
Main Entry Methods:
Operates as a closed-access Ransomware as a Service (RaaS) portal. The distribution is left to affiliates, and each group deploys it as they see fit.

Impact:
McAfee says that NetWalker poses a risk for companies all over the globe, and not just the US – or Western Europe.

Cost:
The **$25 million** figure puts NetWalker close to the top of the most successful ransomware gangs known today.

[Source: ND Zet and McAfee]

LOCKBIT 2.0



Main Entry Methods:
One of the fastest file-encrypting ransomware variants in the market known for exploiting Remote Desktop Protocols (RDP) and VPN accounts.

Impact:
LockBit has compromised **52 organizations** around the world since June.

Cost:
In a report from Accenture itself, the company said it found that **54%** of all ransomware or extortion victims were companies with annual revenues between **$1 billion** and **$9.9 billion.**

[Source: ZD Net and Tego Cyber]

RYUK

Main Entry Methods:
Spread mainly via malicious emails, or phishing emails, containing dangerous links and attachments.

Impact:
Engineering, industrial construction, and legal services company suffered incidents involving Ryuk.

Cost:
Caused more than **$60 million** in damage worldwide.

[Source: Gatefy]

SAMSAM

Main Entry Methods:
Broke into networks using a variety of tactics including brute force attacks and exploit kits.

Impact:
More than **200** organizations and companies in the U.S. and Canada, including hospitals, municipalities and public institutions.

Cost:
A loss of **$30 million** is estimated as a result of the attacks.

[Source: Cytelligence and Gatefy]

With ransomware attacks expected to hit a business every **11 seconds in 2021**, it's all too likely you or your company will be attacked in the near future. Clearly, individuals and businesses need to be proactive in preventing ransomware attacks and should be ready to act if an attack does occur.

StorCentric | 1289 Anvilwood Ave, Sunnyvale, CA 94089 | 1.408.724.9809

StorCentric