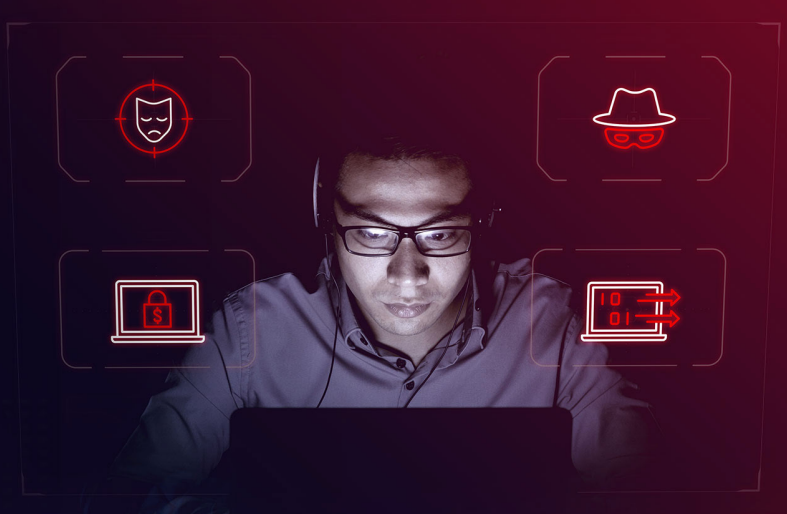
MANDIANT

MULTIFACETED EXTORTION: THE EVOLUTION OF RANSOMWARE

Ransomware attacks have transformed into more than monetary payoffs and now present further business risks with severe consequences. Learn about this evolution and protect your business from its harmful outcomes.



2018

Big game hunting emerged

39%

An estimated 39%[1] of victims succumbed to ransomware payment demands

$6,733

Average ransom (Q4) reported as $6,733[1]

FIN6

Threat group: Actors who historically focused on payment card theft, like FIN6, shift to ransomware operations

2019

The introduction of naming and shaming

$84,116
1149%
increase from previous year

Average ransom (Q4) reported as $84,116[1]

Following the creation of the MAZE blog, victim naming and shaming trend began (Q4)

MAZE blog registered in December

2020

Record breaking ransoms

25%
UP 11% FROM 2019

25% of the global incidents responded to by Mandiant involved ransomware

51%

Survey of 5,000 IT managers found that 51%[1] experienced ransomware

57%
UP 18% FROM 2018

An estimated 57%[2] of victims paid ransomware demands

$154,108
83%
increase from previous year

Average ransom (Q4) reported as $154,108[2]

4.5m

A world record for the largest publicly reported ransom payment of $4.5 million in bitcoin was made

FIN11 threat group (graduated by Mandiant) uses multifaceted extortion tactics[3]

FIN11

>60%

Ransomware attacks involving data exfiltration increased from <15% in Q1 to >60% in Q4[1]

4.4m

A major US critical infrastructure organization made ransom payment of $4.4 million in bitcoin

Public shaming sites associated with multiple ransomware families, like DoppelPaymer, are created

2021

Ransomware cited as a national security threat

$40 MILLION

One of the largest US insurance companies publically reported a ransom payment of $40 million (March 2021).[4] The largest ransomware payment to-date

Almost 2,400[1] US based governments, healthcare facilities and schools were victims of ransomware

The IST Ransomware Task Force cited ransomware as a national security threat

5
DAYS

The global median dwell time of ransomware attacks is 5 days[3]

Media reports ransomware gang offered traders inside information on attack victims to short sell stocks

THE EVOLUTION OF RANSOMWARE TO **MULTIFACETED EXTORTION**

Ransomware attacks see increasing success against organizations of all kinds.

It used to be simple: They locked down your data and demanded money for the key.

Now, attackers steal your data before locking it down. They threaten to publish stolen data on "name-and-shame" websites, amplify stories of security incidents (and their victims) via media outlets and notify business partners of data theft.

Ultimately, adversaries gain leverage to demand higher payouts by threatening to create relationship friction and prompt breach disclosures.

The Top 5 Observations of Multifaceted Extortion Attacks

1. Multifaceted extortion is the number one cyber security threat to organizations world-wide
2. The impact may be significant, as it combines business disruption, data theft, public shaming and other harmful extortion techniques
3. Implementing resilient system backups addresses part of the problem, but more needs to be done to mitigate the risk and impact of mutlifaceted extortion attacks
4. Multifaceted extortion typically requires the victim to disclose the breach. Victims often lose control of this because threat actors may disclose the incident according to their own schedule
5. Multifaceted extortion payment demands usually fall within the 6, 7 and 8-figure ranges

THE TIME TO ACT IS **NOW**

Evaluate and improve your ability to prevent, detect, contain and remediate a ransomware and multifaceted extortion attack with our solution offerings led by frontline experts.

To learn more, visit experience.mandiant.com/multifaceted-extortion

[1] IST (2021). A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force.
[2] Cybereadge Group (2021). Cyberthreat Defense Report.
[3] FireEye (2021). M-Trends 2021.
[4] Business Insider (2021). One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack.

MANDIANT