MANDIANT

MULTIFACETED EXTORTION: THE EVOLUTION OF RANSOMWARE

A National Security Threat

Cyber adversaries have propelled ransomware to become the top attack vector across organizations of all shapes and sizes. Ransomware attackers have intensified their missions by threatening critical infrastructure shutdowns, risking public health and safety, diverting vital public resources, disrupting educational institutions and impacting data privacy to such an extent that in some cases it is now deemed a national security threat.

Increased Attacker Aggression

Since the first recorded ransomware attack in 1989, attackers have been maturing their tradecraft, creating a multibillion-dollar industry with the intent and capability to cripple business operations. Threat actor tactics have evolved to establish a lucrative business by stealing data, accompanied by harmful threats to publish that sensitive data if their demands are not met. These high stakes have resulted in extortion demands dramatically increasing, as experienced by a well-known critical infrastructure company who paid a ransom demand of $4.4 million in bitcoin[1] to reopen utility supplies to the east coast of America following an attack.

The significant change in ransomware activity was publicized in 2020, prompting Mandiant to label this "new ransomware" as multifaceted extortion. The proliferation of multifaceted extortion has been so impactful to the cyber security industry that it was featured in the Mandiant M-Trends 2021 report.

25%

25% of the global incidents responded to by Mandiant involved ransomware in 2020[2]

2,400

Almost 2,400[3] U.S. based governments, healthcare facilities and schools were victims of ransomware

5 DAYS

The global median dwell time of ransomware attacks is 5 days[2]

[1] Forbes (July 2021). The REvil Ransomware Hackers Have Gone Offline.

[2] FireEye (2021). M-Trends 2021.

[3] IST (2021). A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force.

Characteristics of Multifaceted Extortion

Although ransomware and multifaceted extortion threats are closely related, multifaceted extortion presents a more profound risk to organizations.

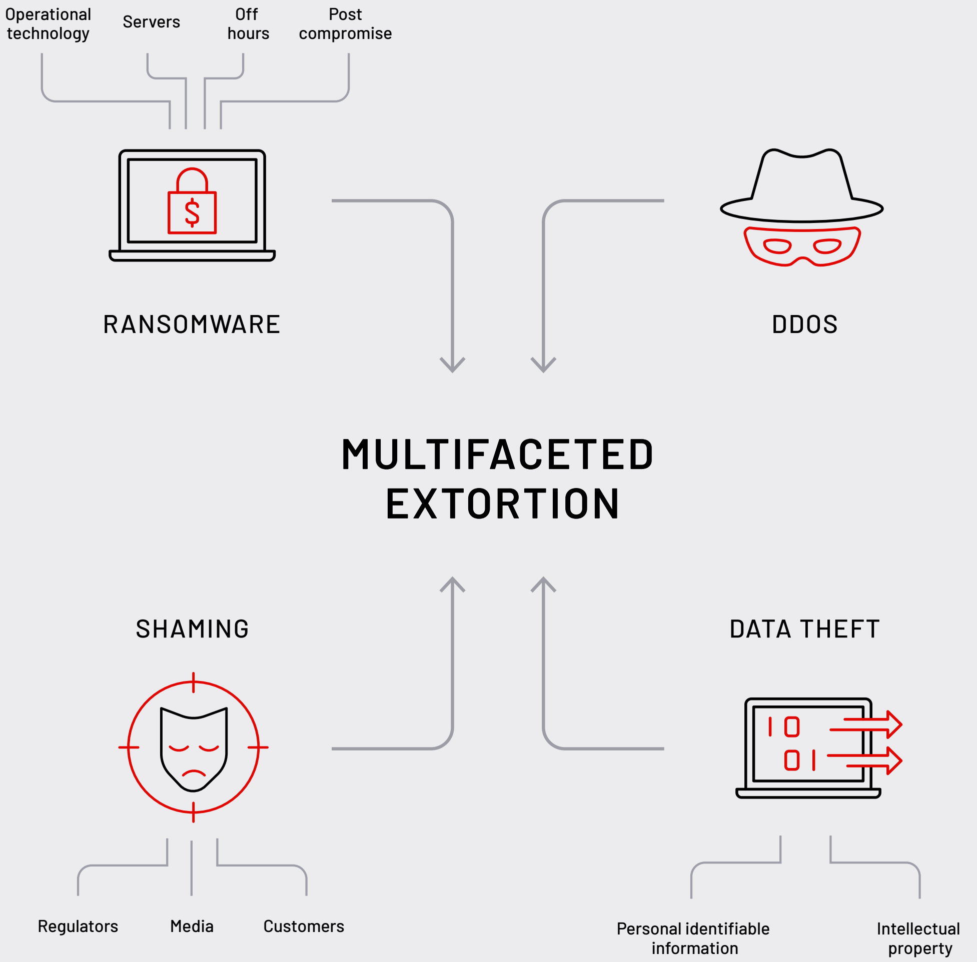
Typically, business leaders and risk managers relate ransomware to malware encrypted files that become inaccessible to legitimate users—ultimately resulting in a level of harmful business disruption. The most common mitigation strategy by security teams today against a ransomware attack is a solid offline backup program; however, this alone does not always deliver an easy or seamless recovery.

Multifaceted extortion takes what we have come to know as traditional ransomware up a notch, by publicizing the theft of critical data, turning service disruption into a full data breach. As the diagram below demonstrates, multifaceted extortion involves multiple attack points, including ransomware encryption, data theft and public "naming and shaming" of the victim organization.

> *A data breach can result in greater reputational damage, regulatory fines, class action lawsuits, and derailed digital transformation initiatives. These consequences were not typically seen with ransomware before 2019.*
>
> — M-Trends 2021

Putting the "Multi" in Multifaceted Extortion

During a multifaceted extortion event, data backups are still relevant for the disruption, however they don't assist with the actual data theft; the target remains at the mercy of both the attacker—applying coercion tactics and threatens to amplify news of the breach unless demands are met—and regulatory bodies that may fine the organization for not adequately protecting their customer's data. The organization can also suffer from extreme reputational damage.



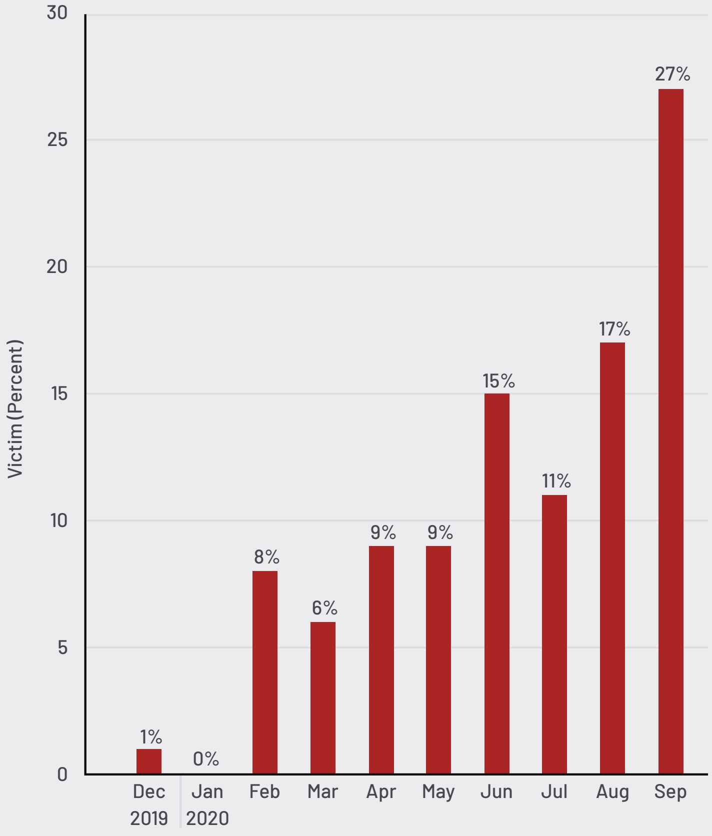
High-Pressure Tactics

Victims of multifaceted extortion have little control over the disclosure of their data theft incident. Attackers use the potential release of data during negotiations to increase the requested ransom amount or prompt immediate payment from the victim organization. To cause maximum disruption the attacker resorts to:

- Harassing employees
- Notifying business partners
- Sending email spam campaigns
- Informing stock traders so they can short sell stock before data is leaked
- Contacting news and media organizations
- Deploying social media advertisements to shame victims
- Creating and maintaining name-and-shame websites

Name and shame websites have proven successful for some multifaceted extortion operations. From March to September 2020, Mandiant recorded an average of at least one new shaming website a month.[4] This number continues to grow steadily. While victims span almost every industry, the manufacturing sector has been disproportionately represented.

Number of victims appearing on name and shame sites



[4] FireEye (April 2021). M-Trends 2021.

The Price of Paying Ransoms

Public disclosure of a multifaceted extortion attack can significantly affect the victim organization's reputation, resulting in a loss of confidence and trust from partners, shareholders and customers. The ripple effect can extend to stock prices, strategic business relationships, customer loyalty, turnover, profitability and employee retention. Many organizations dig deep into their pockets to pay the extortion demand, completing a vicious but lucrative transaction in favor of the attacker. Paying a ransom is a game of chance: organizations don't know their attacker or whether they will remain true to their word.

> *Ultimately, whether an organization pays a ransom demand depends on its individual circumstances, considering factors such as their recovery time with or without payment, threat actor reliability and the sensitivity of their stolen data.*

Mandiant has observed that modern ransomware attackers can take on any of the following approaches/characteristics:

They can't re-encrypt data, but usually have enough leverage to extort further

They are reliable–their business model depends on it–so they are likely to carry out the harmful consequences of non-payment

They typically move on to the next target when paid

They do not guarantee the stolen data will be deleted (despite receiving "proof" of deletion)

← | →

Preventative Action

With multifaceted extortion attacks on the rise, security teams should take a proactive approach to protect their environments. Mandiant experts have found that an event could have been rapidly contained or prevented in many cases if best practices for security configurations and continual security validation were in place before a multifaceted extortion incident.

Premediate your environment

"Premediation" is the practice of proactively implementing controls and security enhancements that are commonly applied as part of the remediation efforts following a cyber security breach.

Mandiant experts working incident response engagements throughout 2020 observed the following commonalities across victim organizations:

> *Prioritizing actions to address these issues can help you mitigate the risk of a ransomware or multifaceted extortion incident.*

- A large number of highly privileged accounts in Active Directory
- SPN Highly privileged non-computer accounts configured with service principal names (SPNs)
- Security controls not configured to minimize the exposure and usage of privileged accounts across endpoints
- Attackers modifying Group Policy Objects (GPOs) for ransomware deployment

Know The Threats That Matter to Your Organization

Access to the latest frontline threat intelligence enables your organization to improve its defenses by helping you understand the identity, targets, timing, motivation and methods of the latest threat actors. Threat intelligence can be used to prioritize and focus efforts on the specific threats facing your industry and organization, testing security procedures and remediating vulnerabilities.

Test your defenses

Safely testing your organization against real-world multifaceted extortion attack scenarios can help identify existing misconfigurations in an environment and help improve or develop a more robust security posture. The good news is that it's possible to significantly minimize the overall impact of an attack. After identifying the assets that multifaceted extortion attacks can reach in your environment, you can proactively realize your security weaknesses and make both strategic and tactical improvements by evaluating your ability to detect, contain and remediate ransomware and related threats with purpose-built security services.

Learn more at **www.mandiant.com**

Mandiant
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT