FIREEYE™ | MANDIANT®

THE PERFECT CYBER SECURITY STORM OF 2020

Contributing factors and strategies to reduce future risk

Introduction

In many ways, society was well-equipped to deal with the pandemic which began in 2020. Internet and remote access technologies were widely available and enabled many business operations to continue. Unfortunately, at the same time, several other complications contributed to a perfect cyber security storm.

Ransomware operators continued to expand attacks on state and municipal networks alongside hospitals and schools while the global response to COVID-19 diverted the growth plans of many organizations toward scaling out remote work capabilities. While organizations settled into a new understanding of "normal," FireEye Mandiant uncovered the highly advanced SUNBURST supply chain attack associated with UNC2452, a suspected nation-state threat actor. Many security teams were again forced to divert resources, this time away from wide-ranging analyses around the adoption of remote work policies toward mitigating the risk of a supply chain attack through a trusted platform.

Contributing Environmental Factors

Three factors contribute to enabling cyber attacks around the world:

- **Lack of international doctrine**
  There are no rules between nations to prevent and punish cyber attackers. Ideally, governments around the world should establish a cyber treaty, similar to treaties that address other forms of warfare.
- **Rise of professional threat actors**
  All attackers (nation-state, criminal, hacktivist) are highly motivated and trained and they conduct their operations worldwide without fear of repercussion. There is a global marketplace for hacking tools and different attack groups cooperate to achieve their goals.
- **Popularity of anonymous payments**
  Bitcoin and other cryptocurrencies create an anonymous, international payment mechanism that cannot be easily tracked, which has led to a rapid growth in ransomware attacks. Intercepting money trails has become increasingly complex and attackers are continuously refining their skills to take advantage of this complexity.

These factors, along with the work- and life-changing events of 2020, created a perfect cyber security storm that will shape security policies for years to come.

Exacerbating Factors in 2020

Mandiant experts repeatedly witnessed instances of how the perfect cyber security storm affected global businesses and governments. Three observations surfaced during incident response investigations:

- **Ransomware attack demands are obscene**
  Cyber adversaries have moved beyond traditional ransomware to multifaceted extortion, which includes data theft and name-and-shame websites. These tactics allow adversaries to extort greater sums of money from victims through fear of heightened reputational and operational damage.
- **Attackers are capitalizing on work-at-home infrastructures driven by the global pandemic**
  Organizations have had to quickly revisit remote work capabilities and assess the effectiveness of their defenses for remote business operations.
- **Targeted attacks are increasing faster than historically popular attacks seeking susceptible victims**
  This highlights the sophistication, organization and relentlessness of attack groups with a specific mission. Organizations must place focus on intelligence-led and risk-based approaches to address these targeted attacks, rather than relying on technology-based, generalized methods alone.

Learnings from M-Trends 2021

The **M-Trends 2021** report[1] provides qualitative and quantitative frontline cyber insights from real-world investigations, incident response engagements and threat intelligence research by FireEye Mandiant experts. The report's findings are based on Mandiant investigations of attack activity conducted between October 1, 2019, and September 30, 2020. Three major takeaways from the report connect directly to factors that fueled the perfect cyber security storm:

Ransomware Proliferation

Pandemic Effects

Targeted Attacks

1 FireEye (April 2021). M-Trends 2021.

LEARNINGS FROM M-TRENDS

Ransomware Proliferation

One of every four Mandiant incident response engagements in 2020 involved ransomware. Organizations are detecting these types of attacks inside their networks quickly—the **global median dwell time is five days**. However, organizations must remain vigilant because Mandiant red team experts have demonstrated that **ransomware actors can accomplish their mission in one to three days**.

To complicate matters further, attackers are compelling victims into paying extortion demands, using tactics such as posting samples of stolen data to name-and-shame websites, amplifying stories of security incidents and their victims via news and media sites, and notifying business partners of data theft to create friction in relationships and prompt breach disclosures. Labeled by Mandiant as **multifaceted extortion**, these tactics give threat actors the leverage they need to increase monetary demands.

You can take concrete action to reduce risks associated with multifaceted extortion:

Evaluate your environment for past and ongoing threat activity

Assess your ability to effectively defend against a ransomware attack

Align your automated detection and response capabilities

Continuously validate the effectiveness of your capabilities and controls

Mandiant Compromise Assessment
Identify currently active attacks as well as remnants of previous attacks that may have left your organization vulnerable.

Mandiant Ransomware Defense Assessment
Review your existing defense operations to uncover process gaps and emulate real-world ransomware attacks to test your technical controls.

Mandiant Advantage SaaS Platform
Disrupt highly sophisticated attackers and slash their dwell time with automated defenses.

Mandiant Security Validation
Continuously test your controls against the latest attacks to protect against rapidly evolving malware and monitor IT environmental drift.

LEARNINGS FROM M-TRENDS

Pandemic Effects

The global pandemic demanded a shift to infrastructures supporting a work-at-home environment. The additional tooling adopted by many organizations to enable remote work introduced significant security risks due to rushed deployment. Threat actors subsequently increased their focus on vulnerability exploitation for this expanded network surface.

Mandiant forecasts ongoing pandemic-related targeting of the healthcare, pharmaceutical, medical research and closely related industries while COVID-19 remains a concern. Most of this targeting will very likely continue to come from espionage actors. Contact tracing systems and applications deployed by governments, often developed and/or operated by third parties, will likely provide additional targets given the value of large-scale databases for intelligence gathering and development of phishing campaigns.

You can take steps to mitigate these risks:

Validate the effectiveness of architectural security controls adapted to enable remote work

Pinpoint security vulnerabilities and misconfigurations

Prepare for unknown events and business shift with retainer-based services and agile access to expert resources

Mandiant Red Team Assessments
Test your environmental defenses against real-world attacks and identify security weaknesses and gaps that require improvement.

Mandiant Penetration Testing
Evaluate security for systems and integrations with new technologies resulting from business changes.

Mandiant Incident Response Retainer
Be prepared to respond rapidly to incidents when attackers strike.

Expertise On Demand
Remain agile and apply specific skills, resources and knowledge tailored to solve unpredictable, unique challenges.

LEARNINGS FROM M-TRENDS

Targeted Attacks

Phishing attacks accounted for 23 percent of intrusions, which represent historically popular victim selection. Exploits were used as the initial attack vector in 29 percent of incidents, indicating threat actors are targeting specific organizations and "crown jewels" they want to access. Once an organization has been targeted, threat actors are persistent in their attempts to accomplish their goals. In fact, prior compromise accounted for 12 percent of the intrusions in which the initial compromise was identified, and approximately 3 percent of intrusions likely only served to compromise architecture for further attacks. Successful targeted attacks are often carried out by sophisticated, coordinated attackers. In 29 percent of cases, Mandiant experts identified more than one distinct threat group in the victim environment, nearly twice the percentage noted in 2019.

A significant targeted attack was reported by FireEye on December 13, 2020, which detailed a supply chain attack called SUNBURST, an implant in the SolarWinds Orion platform being used to compromise target environments. For solutions specific to the SUNBURST attack associated with the UNC2452 group, read **Navigating the UNC2452 Intrusion Campaign.**[2]

You can take steps to deal with targeted attacks:

Determine your organization's critical assets

Update your security stack to use intelligence-led solutions fed by frontline experience and research

Evaluate the security of your supply chain and systems outside of your control

Mandiant Crown Jewels Assessment
Think like an attacker to identify and secure your high-value assets, which can include intellectual property.

Mandiant Solutions
Extend and surpass technology-led solutions by identifying the threats and risks that matter most to your organization.

Mandiant Security Program Assessment
Conduct a thorough review that includes third-party applications, partner integrations and operational technology (OT) systems.

2 FireEye (February 2021). Navigating the UNC2452 Intrusion Campaign.

Conclusion

Over the last year, we were reminded how events in the physical world and cyber security can converge to dramatically change our environment. The global pandemic changed the way many businesses operated, increasing their attack surface and risk profile. Organizations around the world struggled with adapting to the new normal and maintaining their defenses. Attackers took advantage of the situation. This perfect cyber security storm should jolt us into action—to validate the security effectiveness of recent network and control changes and ensure we are prepared for the future.

To learn more about how Mandiant experts can help your organization mitigate harmful breaches and improve your overall security posture before, during, and after an incident, visit [www.FireEye.com/mandiant.html.](www.FireEye.com/mandiant.html)

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye
At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at www.FireEye.com.

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.