

THE VISION

INSIGHTS DELIVERED STRAIGHT FROM THE FRONTLINES OF CYBER ATTACKS



A GLOBAL RESET: CYBER SECURITY PREDICTIONS 2021

EDITION HIGHLIGHTS

Cyber Security
Predictions Related to
the Global Pandemic

The new standard
In cyber threat
intelligence is here

The Graduation
of FIN11

Front and Center
on Ransomware.



All articles in this PDF are hyperlinked. Click or tap on a link to navigate to that article

ARTICLES

Cyber security predictions 2021: Looking ahead	3
Cyber security predictions related to the global pandemic	5
The new standard in cyber threat intelligence is here	9
The graduation of FIN11	13
FireEye Chat Episode 7: Front and Center on Ransomware	17



CYBER SECURITY PREDICTIONS 2021

Looking ahead



The capriciousness of 2020 has driven security practitioners to defend their organizations against a multitude of attacks that included threats to the U.S. presidential election and financially motivated actors looking to further disrupt business operations in an already unsettled time. FireEye and Mandiant experts have identified a number of cyber security trends set to affect our industry over the coming 18 months to help security practitioners in their planning efforts.



FireEye and Mandiant experts have identified two overarching cyber security trends to help teams effectively plan their investment programs over the next 18 months.

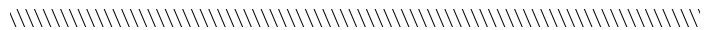


Nation-State Activity

Major nation-state sponsors of threat activity in 2021, both regionally and globally, will continue to include Russia, China, Iran and North Korea. However, security teams should expect to see increased activity from Vietnam and South Asia as well.



WATCH ONLINE >



Ransomware



The high levels of ransomware activity in 2020 will only increase into 2021. The tactics, techniques and procedures used for compromise will continue to evolve, and increasingly aggressive attackers will demand higher ransoms as they begin digesting what is actually in the data.



WATCH ONLINE >



Cyber security predictions related to the global pandemic

////////////////////////////////////

The ongoing COVID-19 pandemic has paved the way for a wave of cyber security incidents this year which FireEye and Mandiant experts predict will affect security operations into 2021. Hot on the heels of the recent Mandiant webinar; A Global Reset: Cyber Security Predictions 2021, the latest predictions report covers several trends that will continue to alter the course of security activities around the world over the coming months.





Industries at Risk of Attack

The race for a vaccine is now well and truly underway, stimulating an increased attempt by nation state threat actors to appropriate critical research documents. Government, healthcare, pharmaceutical and non-governmental organizations have become targets for attack. To protect their environments, some organizations have been introducing air-gapped computers with no Internet access, a move recommended by FireEye and Mandiant experts for those undertaking sensitive research.



////////////////////////////////////
Educational institutions relying on web interfaces for lessons and telehealth which involves the discussion of patient details over the phone or online are two additional high-risk sectors that should remain alert for threats.



Technology Considerations

High levels of remote working and social distancing regulations will drive increased spend on perimeter security and ecommerce security in 2021. Securing or servicing remote access users will remain a trending topic next year, particularly for helpdesk activities interfacing with employees and those operating webcam technologies. As 2021 progresses, FireEye and Mandiant experts anticipate organizations will launch solutions which attempt to facilitate a return to normalcy, but fresh security risks with regards to the protection of personal and private information may emerge.



High levels of remote working and social distancing regulations will drive increased spend on perimeter security and ecommerce security in 2021.




Cloud Asset Management

The adoption of cloud security solutions will continue to rise. Almost 95% of organizations have some type of cloud presence now and security teams must take stock of their entire cloud portfolio, and implement and validate appropriate access management policies for all users.

The speed in which new cloud software and services are introduced will undoubtedly result in some teams playing catch-up when it comes to security, especially in the first quarter of 2021. To minimize the risk of a successful attack, FireEye and Mandiant experts recommend a focus on prevention and detection strategies to guard against the following three threats in particular:

1. **Stolen credentials, typically as a result of phishing**
2. **Exploitation of cloud misconfigurations**
3. **Vulnerable cloud application hacking**

Organizations new to the cloud are likely to make security mistakes which will inevitably increase their attack surface. Teams can mitigate this risk by improving their awareness of the distribution of cloud security responsibilities to prevent common misunderstandings and misconfigurations.





Security Validation

Remote work has led to increased demand of security validation services that ascertain the effectiveness of cyber security controls. Pre-pandemic, organizations were keen to manage and operate validation platforms onsite. Post-pandemic, the demand for co-managed or fully-managed validation solutions is expected to rise as teams need to know whether their VPN is working, where vulnerabilities or gaps exist in remote infrastructures and whether their current privilege settings are appropriate.

The 2020 trend for optimization and rationalization of security controls is set to continue into 2021 as the pressure mounts on CISOs to justify the effectiveness of their cyber security investments. Security leaders will need accurate and reliable data to regularly provide CIOs and CFOs with evidence to prove how their cyber security activities are performing over time. Security validation will not only assess how effective a security stack is, it will also identify gaps and overlaps to help teams optimize tools and reduce their spend.

No matter what 2021 brings, one thing is for certain - the impact of the pandemic will require continuing cyber security agility. To stay abreast of the changing landscape, organizations should make good use of the latest cyber threat intelligence to prioritize strategy and investment and turn to validation services to optimize practices currently in place. Organizations will launch solutions which attempt to facilitate a return to normalcy, but fresh security risks with regards to the protection of personal and private information may emerge.

Read the full trend report, A Global Reset: Cyber Security Predictions 2021.

[GET THE REPORT>](#)

FIREEYE™

GARTNER REPORT

5 MUST-DOs FOR CLOUD SECURITY

Know and apply critical actions to secure your cloud assets

[DOWNLOAD THE REPORT>](#)



The new standard in cyber threat intelligence is here

Intelligence-led security has never been so important in the battle to protect organizations against attackers. Knowing who is attacking, as well as why, how and when they will target your environment is critical for prioritizing security activities to patch vulnerabilities, shore up defenses and effectively invest for the future.

To continue supporting organizations with their security efforts, Mandiant has launched the new, accessible-to-all security-as-a-service (SaaS) Mandiant Advantage platform, delivering cyber threat intelligence (CTI) directly from the frontlines of incident response. With this platform, security defenders can easily prioritize the threats that matter the most and take action—regardless of the SIEM or security controls they have deployed. Security teams have access to the same data and tools that Mandiant threat analysts and incident responders rely on.



“Every security team is plagued by the same problem: there’s never enough time or resources. Yet, they have no effective way to prioritize the threats that matter most”

said Chris Key, EVP of Products, Mandiant Solutions. “Mandiant Advantage reimagines how defenders track relevant threats, including uncategorized groups and clusters (UNC), so they can apply insights as they unfold directly to their existing workflows.”

Featuring threat intelligence from live events, machine learning and research initiatives, Mandiant Advantage customers will now be able to access unrivalled threat insight from a unique blend of breach, operational, machine and adversary intelligence.

**Breach intelligence:**

Mandiant Solutions executes more than 850 global incident response engagements every year, representing 200,000 hours responding to breaches. This gives our analysts in-depth insight into the specific steps malicious actors take post-compromise. Mandiant Advantage: Threat Intelligence ingests this data continuously so we can develop the most comprehensive view of cyber attacks, what attackers do once inside, and how customer security controls fail.

**Operational Intelligence:**

Our Managed Defense team performs detection and response services for over 300 customers from four international Cyber Threat Operations Centers, ingesting 99+ million events and validating 21+ million alerts. This continuous monitoring gives us the unique ability to identify emerging global threat campaigns within specific customers or industry verticals.

**Machine Intelligence:**

We have approximately four million virtual guest images deployed globally in 102 countries, generating tens of millions of sandbox detonations per hour, confirming 50,000 - 70,000 malicious events per hour.

**Adversary Intelligence:**

Mandiant Threat Intelligence deploys 300+ intelligence analysts and researchers located in 23 countries. We collect up to one million malware samples per day from more than 70 different sources. Our intelligence analysts are deeply entrenched where cyber attackers plan, design and execute their attacks, giving our customers early visibility into hacker motives and cyber security trends.

The information we gather is analyzed, evaluated and tracked via the Mandiant Graph Database, a unique tool which centralizes all intelligence findings. The data is enriched by Mandiant experts and machine learning to form Mandiant Advantage.



“For years, Mandiant Threat Intelligence has led the industry with credible, high-quality finished reporting that characterizes the threat environment to manage cyber security risk within organizations. But watching and packaging threat intelligence is not enough. With how rapidly threats shift, it’s time that our customers know more about the adversary than anyone else as well. As we collectively take on today’s threat actor, we’re making emerging intelligence accessible to all, as it is discovered.”

Sandra Joyce, Mandiant EVP and Head of Global Intelligence

Many organizations rely on open source intelligence via paid subscriptions, but this only provides an historical perspective on the threat landscape. Mandiant Solutions is raising the industry standard for threat intelligence, making open source intelligence available to all organizations free of charge via the Mandiant Advantage platform or browser plugin. Users can effortlessly pivot customizable threat information panels and search the latest threat news related to their region or industry.

Subscription packages that access real-time data and specific threat insights are also available, including threat intelligence for prioritizing vulnerabilities, detection and response, and dark web monitoring. This information can be integrated into all third-party applications via an API.

To date, no single vendor has brought this level of visibility into adversary intent, opportunities and capabilities to the market. With Mandiant Advantage, security professionals can focus on the threats that matter, serving all layers of the security organization with data that has been curated, connected and enriched, marking the dawn of a new standard in threat intelligence.

Subscribe to Mandiant Advantage threat intelligence today for FREE

SUBSCRIBE NOW>



The Graduation of FIN11



Newly “graduated” as part of the Mandiant Threat Intelligence continuous actor-validation process, FIN11 is a financially motivated threat group that conducts widespread and highly successful phishing campaigns that have impacted organizations across sectors and geographies.

Mandiant Threat Intelligence has observed FIN11 attempting to monetize their operations at least once using named point-of-sale (POS) malware and, more frequently, using post-compromise ransomware deployment combined with additional extortion techniques. FIN11 is also notable due their consistent evolution of malware delivery tactics and techniques.



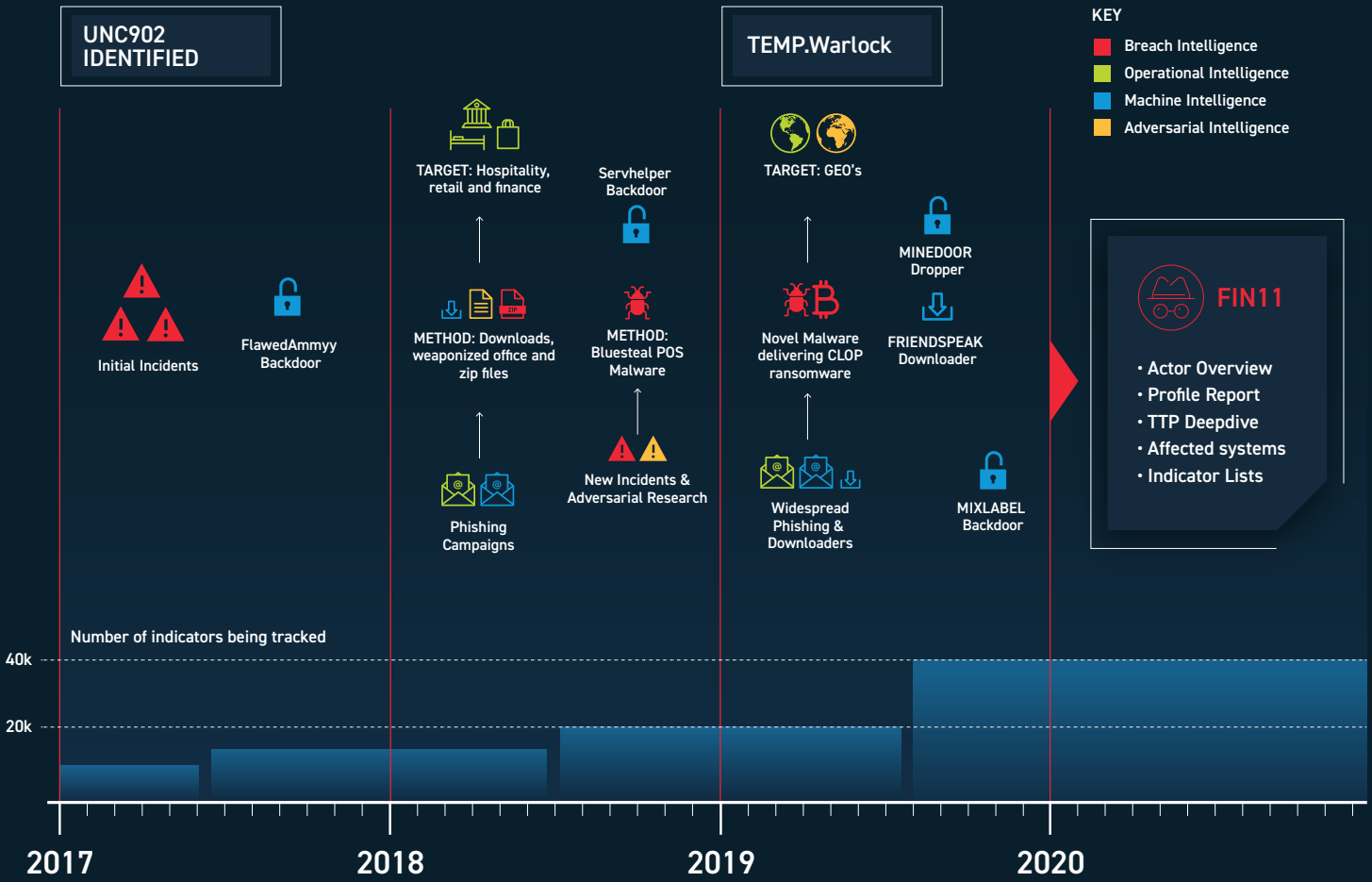
Quantity Over Quality

FIN11 is notable because they use high-volume spam campaigns that many network defenders may dismiss as low priority to create an entry point for damaging, disruptive attacks. When active, the group conducts up to five high-volume campaigns a week. While many financially motivated threat groups are short lived, FIN11 has been conducting these widespread phishing campaigns since at least 2016. From 2017 through 2018, the threat group primarily targeted organizations in the financial, retail and hospitality sectors. In 2019, FIN11's targeting expanded to include a diverse set of sectors and geographic regions. At this point, it would be difficult to name a sector or geography that FIN11 hasn't targeted.

Following the Money

Mandiant experts have also responded to numerous FIN11 intrusions, but we've only observed the group successfully monetize access in few instances. This could suggest that the actors cast a wide net during their phishing operations, then choose which victims to further exploit based on characteristics such as sector, geolocation or perceived security posture. Recently, FIN11 has deployed

The graduation of FIN11



CLOP ransomware and threatened to publish exfiltrated data to pressure victims into paying ransom demands. The group's shifting monetization methods—from POS malware in 2018, to ransomware in 2019, and hybrid extortion in 2020—is part of a larger trend in which criminal actors have increasingly focused on post-compromise ransomware deployment and data theft extortion.





A Familiar Footprint

FIN11 includes a subset of the activity security researchers call TA505, but we do not attribute TA505's early operations to FIN11 and caution against using the names interchangeably. Attribution of both historic TA505 activity and more recent FIN11 activity is complicated by the actors' use of criminal service providers. Like most financially motivated actors, FIN11 doesn't operate in a vacuum. We believe that the group has used services that provide anonymous domain registration, bulletproof hosting, code signing certificates, and private or semi-private malware. Outsourcing work to these criminal service providers likely enables FIN11 to increase the scale and sophistication of their operations.

To learn more about FIN11's evolving delivery tactics, use of services, post-compromise TTPs and monetization methods, register for the free Mandiant Advantage security-as-a-service (SaaS) platform. The full FIN11 report is also available through the FireEye Intelligence Portal.

[SUBSCRIBE NOW>](#)

FireEye Chat | Episode 8: Front and Center on Security Predictions - A Year in Review

JOHN HULTQUIST
Sr. Director, Mandiant Threat Intelligence

SANDRA JOYCE
EVP and Head of Mandiant Threat Intelligence



[WATCH ONLINE >](#)

FRONT AND CENTER ON SECURITY PREDICTIONS

Join our FireEye Chat expert-to-expert discussion for a look back on the predictions from last year's Security Predictions report to see how we fared. We'll also highlight other major cyber security occurrences of this year that has altered the course of direction for the industry as we move into 2021.

Be sure to see what other webinars are available from FireEye

[VIEW OUR WEBINARS >](#)


GARTNER REPORT
5 Steps to Cost Optimization for Security and Risk Leaders in Uncertain Times
[DOWNLOAD NOW >](#)




We hope you enjoyed this edition. Get the latest cyber security news from the frontlines by reading The Vision online.

vision.fireeye.com

Get in touch to find out how our security solutions can help protect your organisation.

contact-us@fireeye.com

www.fireeye.com