MANDIANT

EBOOK

THREAT INTELLIGENCE

Data, people and processes

Contents

TERMINOLOGY

Mandiant Advantage:
Family of subscriptions and services, integrated and accessible through a SaaS environment that augments and helps automate every security team in the world with expertise and intelligence, regardless of SIEM or controls deployed.

Mandiant Graph Database:
Mandiant's database that contains historical and current threat intelligence, enrichment and adversarial knowledge produced by Mandiant experts, automated processes and machine learning.

Executive Summary

Finite resources and the continual urgency to prioritize alerts and make effective decisions puts many security teams under increasing pressure. One wrong decision at a strategic or operational level can impact the business with costly consequences.

Mandiant's data collection, expert staff, highly specialized teams and unique tracking of actors provides organizations with meaningful context on the threats relevant to their business. Delivering a 360° view of threat actors, their tactics and their targets, Mandiant Advantage can help security teams worldwide with defense strategies to protect their organizations from stealthy, fast-moving adversaries regardless of technical security controls.

Introduction

CISOs, SOC managers and other security practitioners must constantly make decisions to defend their organizations against sophisticated threats. Delayed or ill-informed decisions can have a significant impact; security operations teams may lose essential time on low-priority alerts, expensive security controls may turn out to be ineffective and attackers can breach defenses undetected.

To make operational, tactical or strategic decisions, security practitioners compare internal evidence or systems configurations against the information available to them on malicious behaviors or known attack techniques. This global set of information used by security teams to make decisions is often described as cyber threat intelligence (CTI).

A quick search on the Internet leads to hundreds of CTI sources, each built on different attack types or data sources. However, the volume of data, as well as the variety of CTI platforms and their lack of transparency can leave security practitioners with more questions than answers when tracking a threat. Teams are often unsure which data source to trust, whether the data on threat indicators is still relevant, who is behind an attack and their motivations, the likelihood of an attack, what an attacker's motivations are, and how likely they are to be attacked.

It soon becomes clear that CTI requires more than just data. Users need context to get a full picture of the threats, the targets that are at risk and the specific tactics an attacker deploys.

Mandiant Advantage Threat Intelligence: Data, People and Processes

Over the past 15 years, through investigations, incident consultancy and red team exercises around the globe, Mandiant has created and curated a unique portfolio of threat intelligence which is constantly updated with new evidence data, human expertise and unique analytic tradecraft. Mandiant now dominates the field of cyber threat intelligence, delivering several core competences to security teams worldwide.

Unparalleled Threat Visibility

Mandiant independently collects threat insights from a balanced set of sources, giving security teams unique visibility into attackers. These sources include:

Breach intelligence collected via Mandiant Consulting incident response engagements.

Every year, Mandiant conducts more than 200,000 hours of incident response engagements worldwide, giving analysts deep insight into the specific steps malicious actors take against targeted organizations.

Adversarial intelligence obtained by Mandiant researchers.

Engaging in 400+ red team exercises, through thousands of customer-driven intelligence research initiatives and speaking over 30 languages, Mandiant deploys more than 300 threat consultants across 26 countries to produce intelligence reports which detail threat activities discovered in the wild and on the dark web.

Operational intelligence derived from Mandiant Managed Defense services.

Five security operations centers proactively look for and investigate unidentified threat activity in customer environments, ingesting 99 million events annually, actively validating more than 21 million alerts.

Machine intelligence from FireEye security products.

FireEye products protect millions of devices across all industries worldwide, identifying globally malicious activity targeting users and their assets. This machine intelligence is extracted from 15,000 network sensors in 56 countries, that record tens of millions of malware detonations per hour and scan 65 million emails per day.

Specialist Investigative Teams

Mandiant has over 300 analysts investigating threats and developing intelligence. The team continuously evaluates collated threat data to identify any new findings, immediately updating and informing customers on changes to their threat landscape. The accuracy, relevance and quality of this information are a result of specialization and collaboration.

Specialization

Different experts specialize in assessing nation-state actors, criminal actors, vulnerabilities and their exploitation, malware, operational technology (OT) environments and information operations.

Collaboration

All source intelligence analysts and technical subject matter experts work closely to provide detail and context around each threat. For example, one Mandiant technical expert may uncover a new type of malware used in targeted attacks and another will develop an assessment of the risks it poses to organizations.

Tight, integrated collaboration between experts in multiple areas facilitate the development of unique findings to address an organization's risk-related needs, which contribute to the intelligence graph that powers Mandiant Advantage Threat Intelligence.

Organized Intelligence Through the Mandiant Graph Database

The Mandiant Graph Database helps track the complex landscape of evolving threats and centralize intelligence findings. The data is enriched by both human experts and machine sources to form the foundations of Mandiant Advantage.

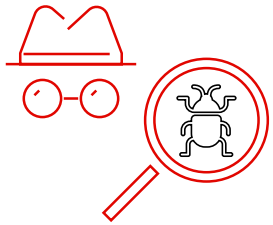
The Mandiant Graph Database tracks domains, actors and their relationships relationships (such as the IP address returned by a domain DNS lookup), as well as the characteristics of entities such as the malware family under which we categorize a file. The system also provides Mandiant threat analysts with a shared workspace in which individuals or teams can collaborate on building a more accurate picture of a threat.

Machine enrichment capabilities within the Mandiant Graph Database augment the system with new insights used by experts during their investigative workflows. Analysts can integrate passive DNS data from providers to understand an adversary's infrastructure, or the system can proactively enrich the entire dataset, automatically linking malicious indicators to new findings from inhouse malware detonation or analysis systems.

The Mandiant Graph Database powers FireEye and Mandiant offerings with real-time context on the latest threats. The Graph Database is fully integrated into the Mandiant Advantage platform, providing customers with the expertise and intelligence they need to stop threats regardless of what SIEM or security controls the user deploys.

Actor Attribution and Insight

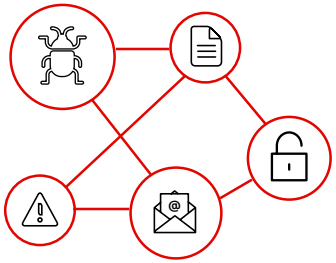
Behind every attack is an actor. Understanding an attacker's motivation and array of tactics helps cyber defenders respond to an attempted attack and proactively assess which external threats could impact their business. To connect threat data with refined attribution analysis, Mandiant experts use a detailed process to define actors, describe their activities and provide customers with end-to-end insight into actor groups.



01.

Actors and Malware

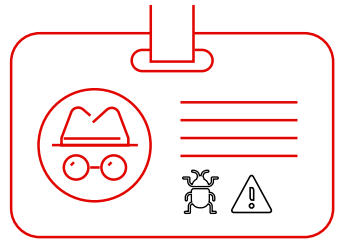
Mandiant regularly identifies new actors and malware. An "actor" is a cohesive set of activities believed to be linked to the same people, conducting similar operations over time. Understanding these groups allows threat defenders to allocate security resources to the most relevant threats. To track an actor or a type of malware, Mandiant threat researchers use a unique combination of characteristics such as tools, techniques, infrastructure, targets and post-compromise behaviors.



02.

Creating an Activity Set

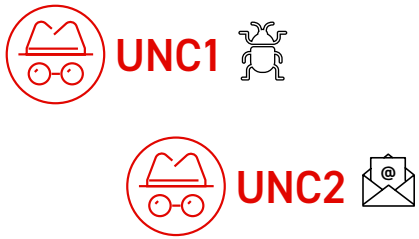
When threat activity characteristics are consistent enough over multiple incidents, they can be tied into an "activity cluster" attributed to a single individual or group of people working together. Similarly, a malware type would be defined by the functionality and characteristics that differentiate it from others. After establishing the initial activity sets or clusters, the analysis work continues and each activity set evolves.



03.

UNC Groups

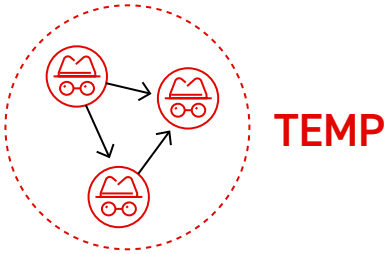
Users of Mandiant Threat Intelligence have access to extracted intelligence findings—activity sets, actors, malware—at multiple stages of the analysis. When Mandiant starts tracking a set of malicious activity, analysts create an uncategorized (UNC) actor entity to describe the early stages of investigation. At this point, the relationships between the new activity, tracked activity and actor intentions may be unclear. An uncategorized entity could cover an activity set as simple as two spear phishing emails with the same lure and malware. With further investigation, this could reveal an end-to-end intrusion operation.



04.

Merging UNC Groups

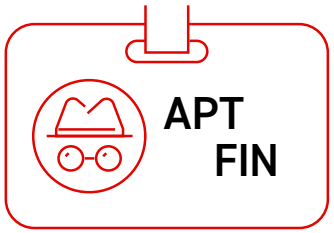
Mandiant has identified over 2,000 UNC groups. While many still exist, others have been merged into combined entities as observations connect them over time. For example, Mandiant analysts might discover evidence during an incident response engagement that forensically shows UNC1 to be associated with the same operators as UNC2 and merge UNC2 into UNC1. However, if analysis indicates that two UNCs may be related, the connection will be noted and Mandiant analysts will continue tracking the activity sets separately. Should further findings change this view, the system will maintain an historical record of the two distinct components. UNCs are merged only when data proves that they are not different operations.



05.

TEMP Groups

Mandiant uses the TEMP designation when one or more potentially related UNCs have reached a level of that requires customers to follow the activity on an ongoing basis to protect themselves. An example of this in action is TEMP.Veles; an operation linked to deployment of the TRITON framework against industrial safety systems. Due to the highly specialized nature of this type of operation, there are fewer observations of TEMP.Veles compared to many other groups tracked, but it remains important to at-risk organizations.



06.

APT and FIN Groups

The most analytically complete actors are those labeled “APT” or “FIN.” Mandiant analysts identify an APT or FIN group after correlating the activity of multiple UNC groups based on high-confidence analysis of the associated risks and how the group operates. The APT designation is used for intrusion sets believed to be state-sponsored and FIN designation is for groups believed to be criminal in nature.

Graduation of FIN11

May 2017—UNC902 identified

Mandiant responded to multiple incidents in which threat actors delivered the FlawedAmmyy backdoor. Mandiant started tracking this cluster of activity as UNC902. Subsequent research revealed related activity dating to 2016.

2018—Specific verticals at risk

Mandiant observed UNC902 conducting phishing campaigns that appeared to target the financial, retail and hospitality sectors. The actors used a variety of methods such as ZIP archives and macro-laden Office files to deliver FlawedAmmyy.

Late 2018—Optimized with POS malware and backdoors

The actors occasionally delivered other backdoors such as ServHelper. In multiple confirmed or suspected UNC902 intrusions, Mandiant observed the groups deploying BLUESTEAL point-of-sale malware.

2019—Widespread attacks, phishing campaigns and exclusive malware forming TEMP.Warlock

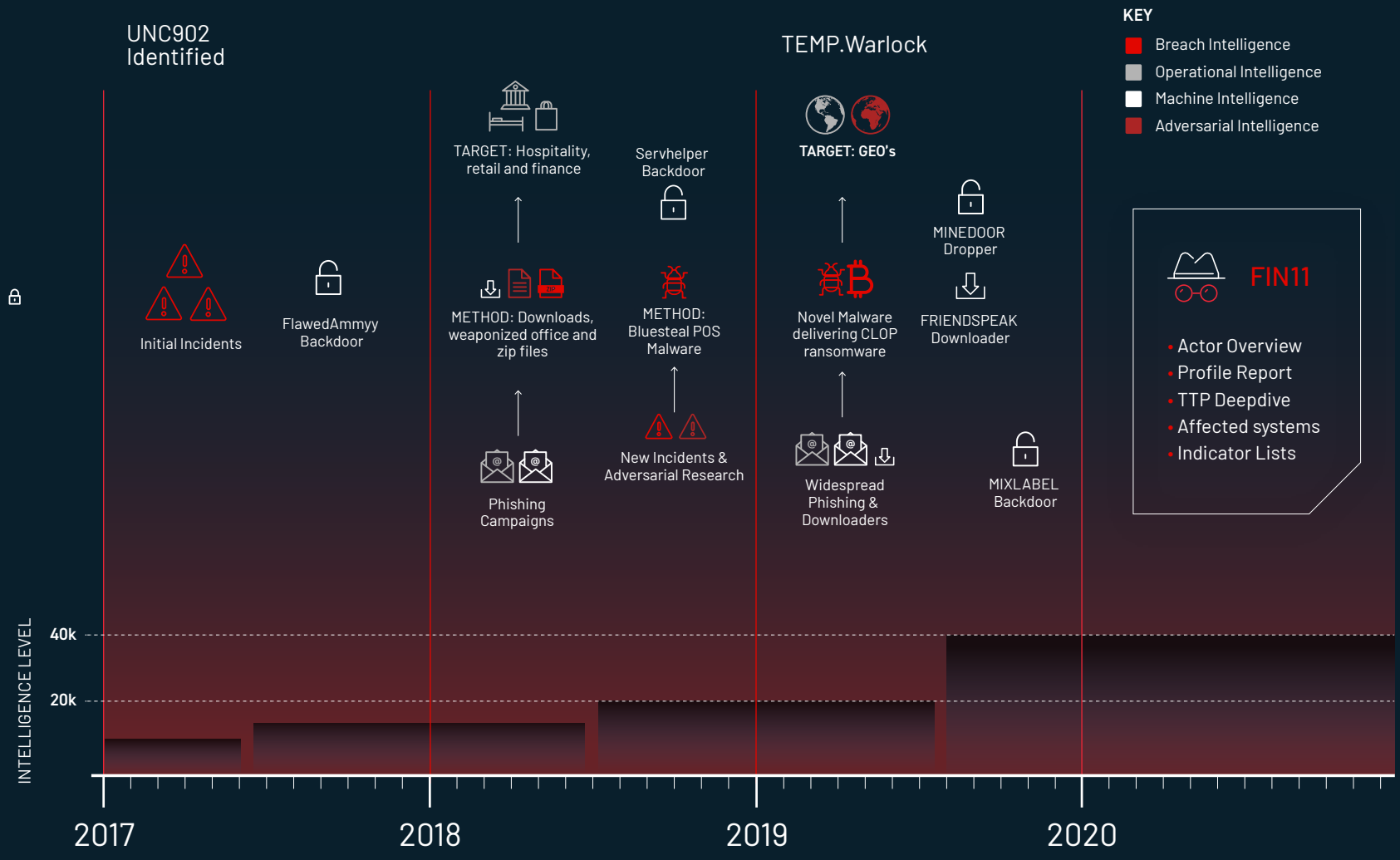
UNC902 conducted widespread, high-volume phishing campaigns leading to a variety of backdoors and downloaders. The threat group targeted organizations in a broad range of sectors and geographic regions. In August 2019, Mandiant observed an UNC902 phishing campaign impacting numerous organizations using macro-laden Office files to deliver a FlawedAmmyy payload. Mandiant responded to multiple incidents that were traced back to this phishing campaign. The team observed post-compromise activity in which the actors used a variety of publicly available and seemingly exclusive malware to move laterally within the environment, before deploying CLOP ransomware. This activity was reported under the name TEMP. Warlock. The use of CLOP ransomware dated back to February 2019.

Second Half 2019—Refined new dropper and downloader

In September 2019, the threat group began using the newly identified MINEDOOR dropper and FRIENDSPEAK downloader. Although the September 2019 campaigns were delivering FlawedAmmyy, by early October the group had shifted to delivering the MIXLABEL backdoor.

In 2020, Mandiant publicly identified the FIN11 group, covering this financially motivated intrusion set.

FIN11 Graduation Timeline

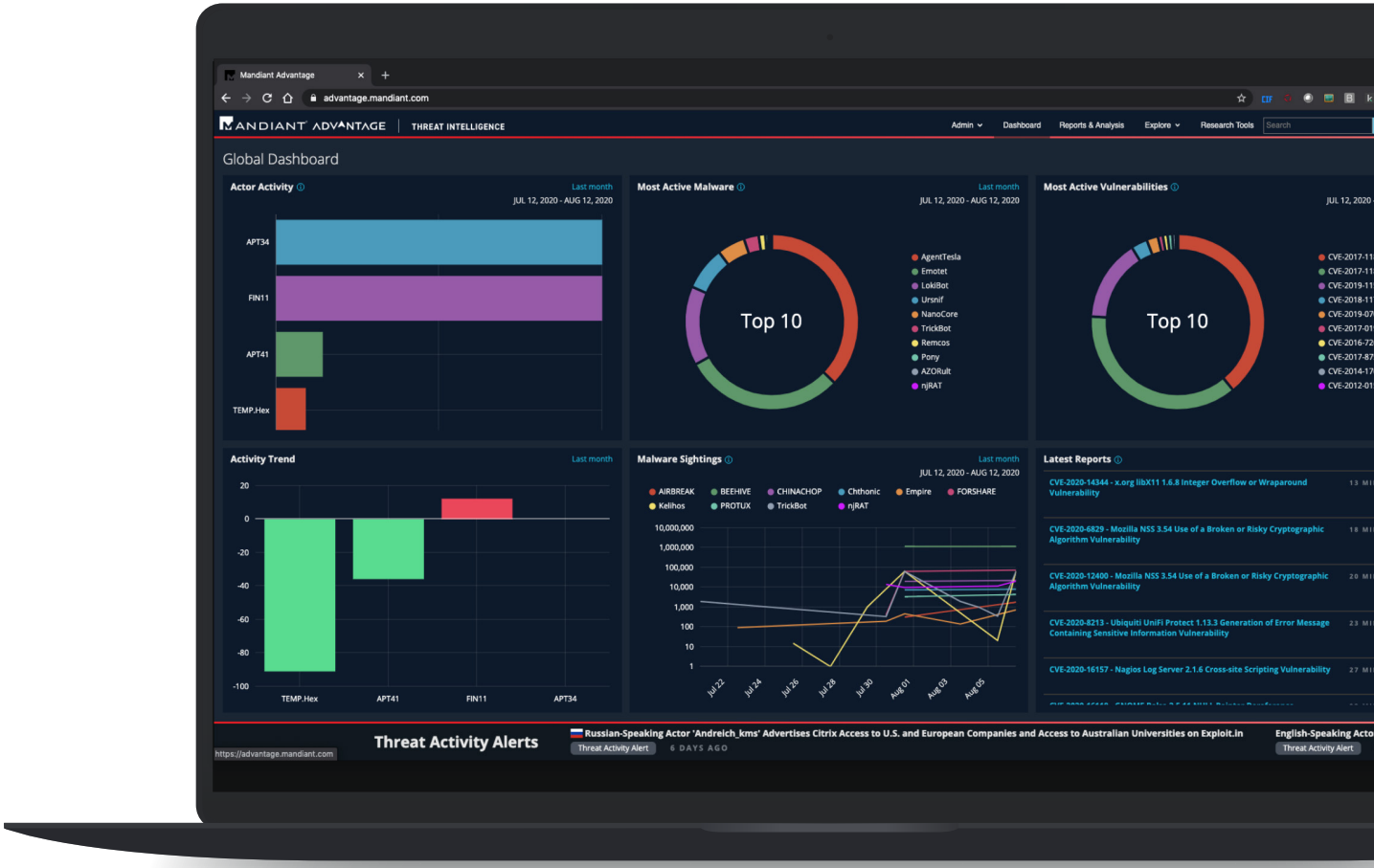


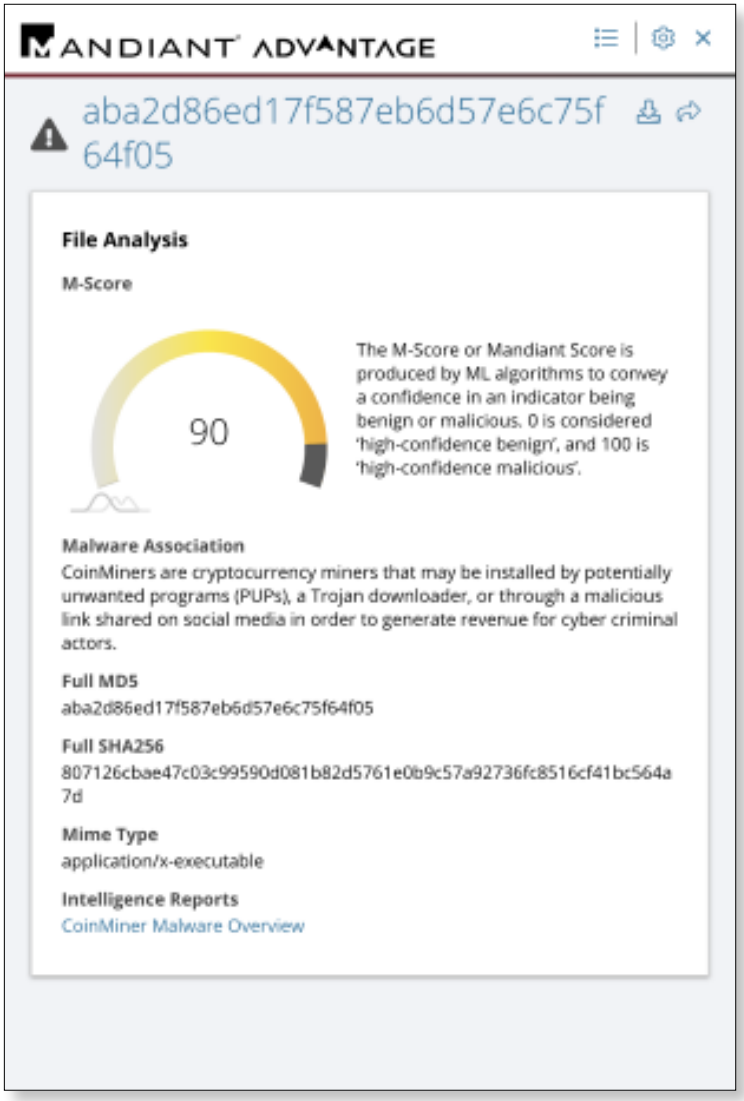
Frontline Threat Access Through a Multitude of Interfaces

As new evidence, expertise and actor context unfolds, security practitioners can access the analysis and expertise from the Mandiant Graph Database through multiple interfaces.

Mandiant Advantage

By logging in to Mandiant Advantage, any security practitioner can review trending threats and search for tactical indicators (IP, DNS, URL, CVE, MD5), threat campaigns, malware, actors, vulnerabilities (and their risk score), tactics, techniques and MITRE ATT&CK mappings. Mandiant Advantage allows users to deeply investigate the threats that matter most to them.





Mandiant Browser Plugin

The Mandiant Browser Plugin is compatible with multiple browsers (Google Chrome, Mozilla Firefox), highlights any threat keywords and observables recognized by the Mandiant Graph Database in any web page. Highlight color is based on a priority score and users can click to view more detailed information on a specific observable or keyword. This approach allows users to focus on the threats that matter most at that moment and get additional insights without opening new tools or windows.

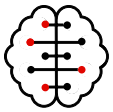
Web API and Integrations

Data represented through Mandiant Threat Intelligence is also available via an application program interface (API) for direct integration to third-party applications including security information and event management (SIEM) tools, threat intelligence platforms (TIP), investigative tools and vulnerability management tools.

Finished Intelligence Reports

These reports include analytical and technical updates that are timely, relevant, actionable and connected to customer-specific operational, tactical and strategic needs. The intrusion and malware information used when producing finished intelligence reports is also included in the Mandiant Graph Database and powers Mandiant Advantage Threat Intelligence.

The Benefits of Mandiant Advantage Threat Intelligence

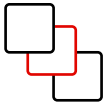


Knowledge from over 300 experts at your fingertips

When Mandiant experts or the enrichment processes learns about a new actor, tactic or target, Mandiant Advantage customers will know. Instant access to continually updated threat intelligence and unique knowledge helps security teams of all sizes make the right security decisions to disrupt stealthy, fast-changing adversaries.

Seamless integration

Mandiant Advantage Threat Intelligence can augment and assist any security team with expertise and intelligence, integrating seamlessly into any current SIEM or security tool.



Serving all layers of the security organization

SOC analysts can look up indicators to validate SIEM alerts or search for actor activity by downloading indicator tables. Vulnerability risk analysts can quickly prioritize discovered CVEs through the browser plugin. Security executives can increase the efficiency of investments by focusing spend on the threat tactics directed at their environment.

Focus on threats that matter most to you

Mandiant Advantage Threat Intelligence data has been curated, connected and enriched with unique tags. Users can rapidly review threat data in different ways and search the latest threat news related to their region, industry or other business technology elements to find relevant, timely content.

Effective Decisions Based on Accurate Attack Analytics

The foundation of Mandiant Advantage Threat Intelligence is the Mandiant Graph Database that contains fifteen years of structured information and analysis on intrusion actors, their tools, activity and techniques. Based on a broad set of sources, collaboration with hundreds of experts and machine enrichment, the data is readily available to Mandiant Advantage users and can help organizations make the best use of their finite security resources.

Mandiant tracks actors and malware to provide organizations with meaningful context on the threats they see in their environment. The Mandiant Advantage interface and API allow users to flexibly search and filter through millions of threat entities to gains insights on the actors and malware relevant to their organizations. Security teams can easily work with this data to reveal indicators, MITRE ATT&CK techniques, targeting information, vulnerabilities exploited and other characteristics. Mandiant Advantage users can get current, comprehensive detail on how threat actors compromise victims by cross-referencing detected threat indicators with useful attack analysis contained in finished intelligence reports.

When a security team of any size is armed with the best possible threat intelligence, they can vastly improve their ability to make faster, proactive and better decisions to protect their organization. Mandiant Advantage is the only platform in the world that offers such breadth and depth of intelligence information and data, reporting on incidents and threat actors as and when they are discovered.

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

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT