THREAT INTELLIGENCE REPORTS

Mandiant Advantage Threat Intelligence (MATI) provides continuously updated reports and analysis of threat actors, campaigns, vulnerabilities, malware, and tools in the **Reports & Analysis** tab of the Threat Intelligence platform. Threat Intelligence tags are automatically extracted from the report for easy reference, including a report summary, any associated threat indicators, and targets referenced in the report. Reports can be downloaded as PDF documents, and all Indicators associated with the report can be downloaded in CSV format for further analysis.

The following fields are included in the exported CSV file when you download indicators:

- Indicator Value
- Indicator Type
- IC Score
- Associated Actors
- Associated Malware
- Associated Tools
- Associated Campaigns
- Exclusive
- First Seen
- Last Seen

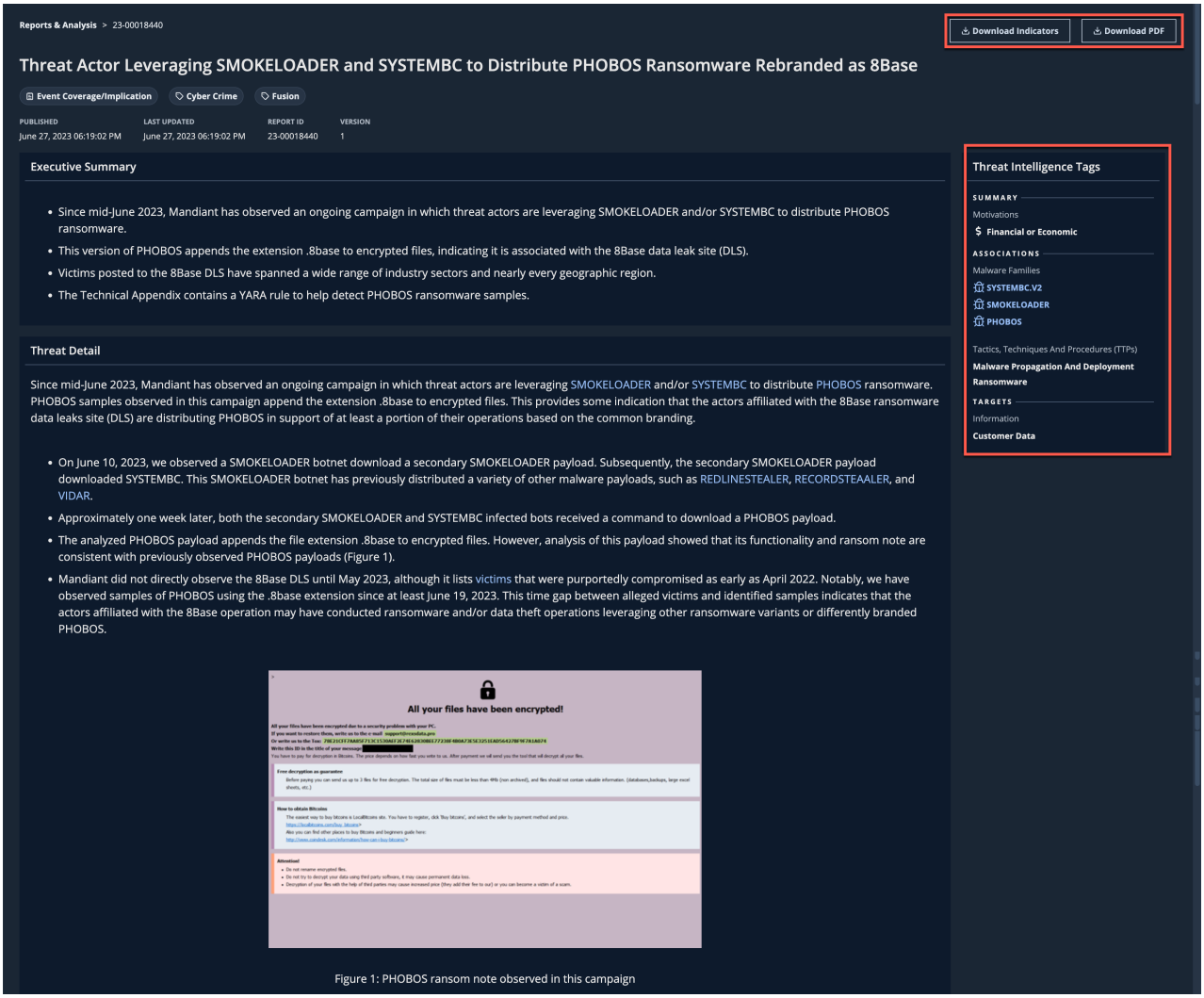

Figure 1: PHOBOS ransom note observed in this campaign

The following table provides an overview of all current Threat Intelligence Reports:

Report Type	Description
Actor Profile	These reports provide an in-depth look into a specific threat actor's tactics, techniques, and procedures.
Country Profile	These reports describe threats to a country or geographic region, across adversary motivations.

Report Type	Description
Credit Card Shop Report	The Card Shop Trends Report is designed to facilitate high-level insights and trends based on customer payment card data for sale on underground card shops. It compares the numbers and percentages of the customer's cards on card shops to the total numbers and percentages of all cards identified on card shops. Specific comparisons may be by card locations, prices, shop information, and/or tracking data from card not present (CNP) transactions where the physical card is not presented to the merchant. This deliverable is limited to financial institutions and payment processors that issue payment cards, as well as any organization having BIN numbers solely allocated for its use. Customers must provide a list of its BINs to their designated CSM to initiate collection and report generation. If you've historically used the FireEye Intelligence Portal (FIP) to access Credit Card Shop Reports, add or update your **Email Delivery Profile** in your **Threat Intelligence Account Management** (https://docs.mandiant.com/home/mati-manage-account-settings) settings to ensure continued delivery of the report. Be sure to select **Report** from the **Level of Detail** drop-down.
Event Coverage / Implication	These reports generally contain analysis on the implications of a recent event or campaign conducted by a threat actor. This report type also includes first glance reports, which provide preliminary information on an incident when analysis of related malware or other campaign aspects may be ongoing.
Executive Perspective	These reports provide brief analysis about cyber threats relevant to events or business circumstances, geared toward a strategic leadership audience. This report type also includes Intelligence-at-a-Glance reports, which provide a weekly snapshot into newly produced reports, blogs, webinars; as well as some insight into customer interests based on top search terms and most read reports.
ICS Security Roundup	These reports are published periodically and provide analysis of public and third party materials related to relevant topics for ICS/OT (industrial control systems/operational technology) security.
Industry Reporting	These reports describe threats to an industry vertical, across adversary motivations.
Malware Profile	Malware Profile reports contain technical analysis of a representative sample of a code family. This report type typically includes file characteristics, host- and network-based indicators, configuration information, and details of code execution.
Net Assessment	Net assessments provide an overview of the top threats that Mandiant reported on or observed throughout the past quarter.
Network Activity Reports	The weekly Network Activity Reports (NAR) matches network flow data from Mandiant's third-party sources with a list of standard and vendor-specific ports that are commonly transmitted over Transmission Control Protocol/User Datagram Protocol (TCP/UDP) in industrial environments. We then analyze the IPs that meet these criteria by leveraging Mandiant's **Indicator Confidence Score** (https://docs.mandiant.com/home/understanding-ic-score) technology, which uses enrichment data from a number of sources.

Report Type	Description
News Analysis	Mandiant News Analysis (MNA) is a low confidence product offering brief, daily intelligence insights into cyber security topics discussed in the news. The MNA team typically selects 2-5 news articles that it predicts will be of interest to our diverse client base and publishes these on weekdays. Topics can include stories with relevance to cyber espionage, cyber crime, vulnerability exploitation, critical infrastructure threats, information operations, hacktivism, and other developments that may impact the cyber threat landscape. Currently, we use only English language source articles.
Patch Report	This report summarizes the vulnerabilities addressed in a specific patch to help customers better consider and prioritize their patching efforts holistically across an entire patch instead of as individual vulnerabilities.
Threat Activity Alert	Threat Activity Alerts relay immediate observations of notable activities within the cyber threat environment. Activities continue to be monitored and may result in additional alerts or reports if anything significant occurs, or the issue warrants further analysis.
Threat Activity Report	Threat Activity Reports relay historical and recent activities observed within the cyber threat environment whose relevance has become elevated by current circumstances. Activities continue to be monitored and may result in additional alerts or reports if anything significant occurs, or the issue warrants further analysis.
Trends and Forecasting	These reports provide analysis into threat actor tactics, trends, or types of threat activity, which may include review over a specified time frame and/or predictions based on identified trends.
TTP Deep Dive	These reports provide an in-depth look into a threat actor and the tactics, techniques, and procedures (TTPs) they use to achieve specific goals.
Vulnerability Report	This report captures information that Mandiant knows about a given vulnerability and the risk and threat it poses to customer organizations. The information provided includes, Risk Rating, Exploitation State, known exploits, a list of vulnerable products and technologies, and many other technical details.
Weekly Vulnerability Exploitation Report	The Weekly Vulnerability Exploitation Report (WVER) summarizes important developments concerning vulnerabilities that may pose a critical or high risk to enterprises that have been observed by Mandiant on a weekly basis. This report is intended as a resource for decision makers on out-of-cycle patching decisions.

The following table represents Threat Intelligence Reports that are no longer used as a separate report but have either been repurposed into other reports or made available directly in the Threat Intelligence platform as indicated:

Report Type	Description	Status
Actor Overview	These reports provide a brief overview of a threat actor.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but this information is now viewable on the Actor pages in Mandiant Advantage (found by clicking **Explore > Actor**).

Report Type	Description	Status
FireEye Labs Research	These reports provide an in-depth look into a threat actor, malware, or tactics used by threat actors to achieve specific goals.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but this information is now included in the TTP Deep Dive report.
Futures Scenario	These reports provide analysis into threat actor tactics, trends, or types of threat activity, which may include review over a specified time frame and/or predictions based on identified trends.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but this information is now included in the Trends & Forecasting report.
Horizons	These reports provide analysis into threat actor tactics, trends, or types of threat activity, which may include review over a specified time frame and/or predictions based on identified trends.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but this information is now included in the Trends & Forecasting report.
Indicator Report	These reports contain malicious indicators associated with the respective malware family.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but indicator data is now found directly using Advanced Search or pivoting from associated malware families.
Industry Intelligence Quarterly	These reports provide a high-level summary of threats to an industry vertical, across adversary motivations, on a quarterly basis.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but these are now "Industry Snapshots" in the Industry Reporting report.
Malware Overview	Malware overviews provide a brief overview of a malware family.	Decommissioned; legacy reports can still be **searched (https://docs.mandiant.com/home/mati-search-intel)** but these are now the summaries on the malware pages in Mandiant Advantage (found by clicking **Explore > Malware**).
Operational Net-Assessment	Operational Net-Assessments provide an overview of the top threats that Mandiant reported on or observed throughout the past quarter.	Decommissioned; this is included in the Net Assessment report.
Targeted Malware Lures	This report highlights potential malware lures that threat actors may exploit or use in social engineering attempts based on previously observed operational patterns, specific subjects, events, and topics.	Decommissioned; these appear as snapshots in the Trends and Forecasting report and are also available by **searching (https://docs.mandiant.com/home/mati-search-intel)** "lures" in Mandiant Advantage).