

EXPLORE MALWARE AND TOOLS

Mandiant Advantage Threat Intelligence (MATI) lets you explore highly contextualized details about Malware families and the Tools used to leverage them.

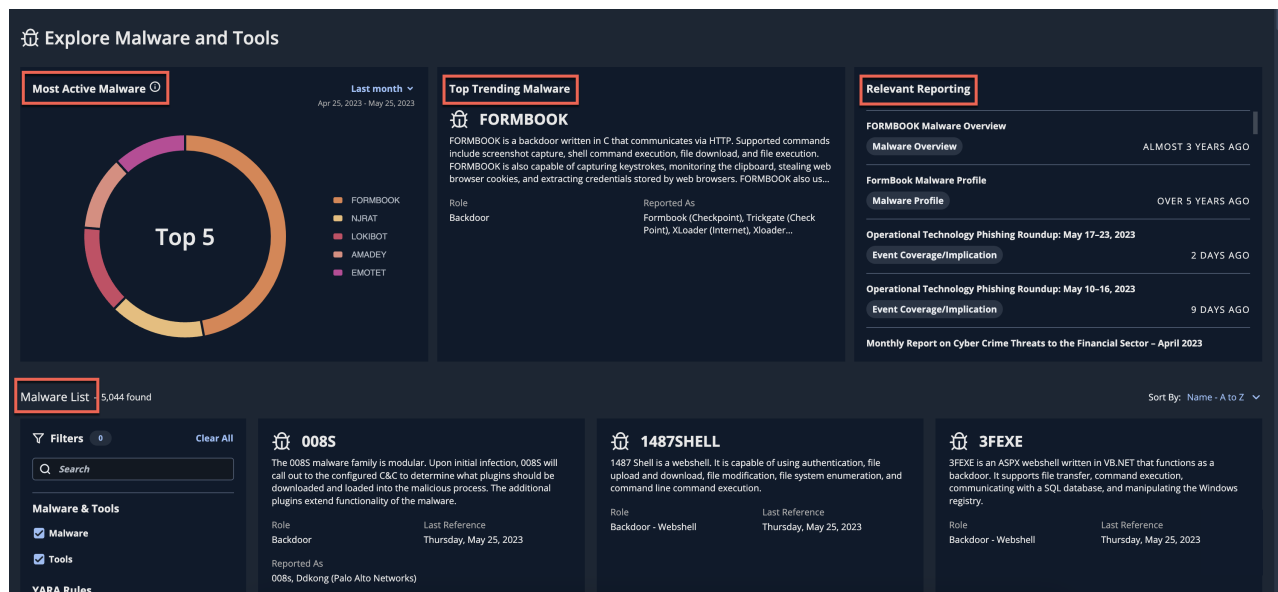
The Explore Malware and Tools dashboard

To view the **Explore Malware and Tools** dashboard, go to **Explore > Malware and Tools**.

- **Most Active Malware:** Visualization of the five most prolific Malware families that Mandiant is tracking, based on detection rates.
- **Top Trending Malware:** The single most prolific Malware family currently being tracked by Mandiant, including a brief description and other Malware details at a glance.
- **Relevant Reporting:** The most recent finished intelligence reporting from Mandiant related to the most active Malware families.



Mandiant does not specifically endorse any third-party claims made in this material or related links, and the opinions expressed by third parties are their own.



Most Active Malware (Last month: Apr 25, 2023 - May 25, 2023)

Top Trending Malware

FORMBOOK
FORMBOOK is a backdoor written in C that communicates via HTTP. Supported commands include screenshot capture, shell command execution, file download, and file execution. FORMBOOK is also capable of capturing keystrokes, monitoring the clipboard, stealing web browser cookies, and extracting credentials stored by web browsers. FORMBOOK also us...

Role: Backdoor
Reported As: Formbook (Checkpoint), Trickgate (Checkpoint), Xloader (Internet), Xloader...

Relevant Reporting

FORMBOOK Malware Overview (ALMOST 3 YEARS AGO)

FormBook Malware Profile (OVER 5 YEARS AGO)

Operational Technology Phishing Roundup: May 17-23, 2023 (2 DAYS AGO)

Operational Technology Phishing Roundup: May 10-16, 2023 (9 DAYS AGO)

Monthly Report on Cyber Crime Threats to the Financial Sector - April 2023

Malware List (5,044 found) | Sort By: Name - A to Z

Filters (Clear All)

Malware & Tools

- Malware
- Tools

YARA Rules

008S
The 008S malware family is modular. Upon initial infection, 008S will call out to the configured C&C to determine what plugins should be downloaded and loaded into the malicious process. The additional plugins extend functionality of the malware.

Role: Backdoor
Last Reference: Thursday, May 25, 2023
Reported As: 008s, Ddkong (Palo Alto Networks)

1487SHELL
1487 Shell is a webshell. It is capable of using authentication, file upload and download, file modification, file system enumeration, and command line command execution.

Role: Backdoor - Webshell
Last Reference: Thursday, May 25, 2023

3FEYE
3FEYE is an ASPX webshell written in VB.NET that functions as a backdoor. It supports file transfer, command execution, communicating with a SQL database, and manipulating the Windows registry.

Role: Backdoor - Webshell
Last Reference: Thursday, May 25, 2023

Filter Malware and Tools

In the **Filters** pane, select the desired filters based on the following options to view only the Malware or Tools you seek to explore.

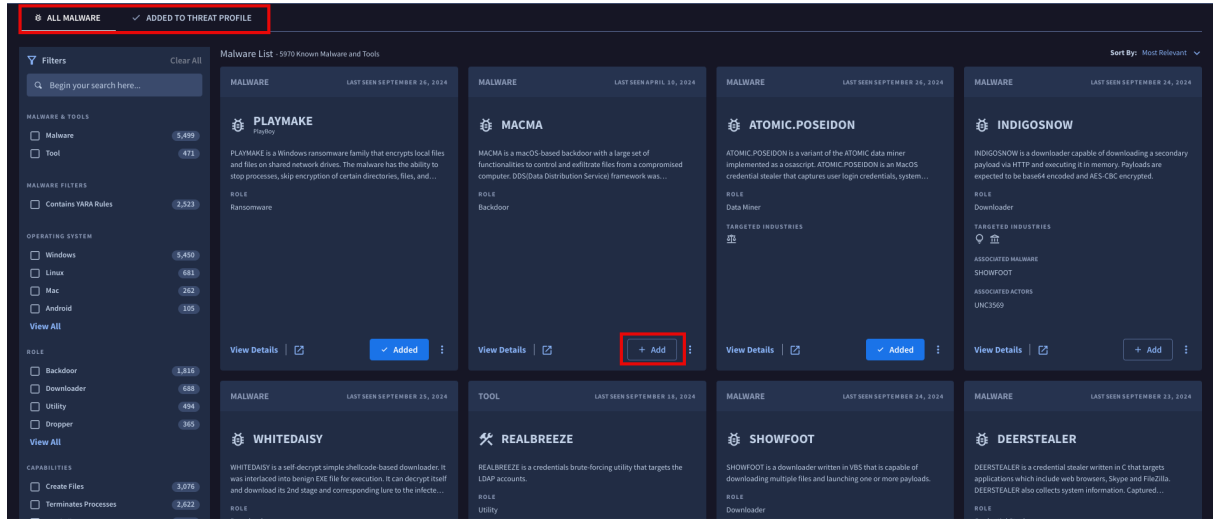
- **Contains YARA Rules:** Display only Malware or Tools that include YARA rules for detection within your environment.
- **Operating System:** Show Malware or Tools that have been observed to target the designated operating systems.
- **Role:** Select the roles of interest that have been observed to be used by the Malware or Tools to be displayed in search results.
- **Capabilities:** Select the capabilities of interest that have been observed to be used by the Malware or Tools to be displayed in search results.

Follow Malware or Tools

In the **All Malware** tab, click **Add** for any Malware or Tool to add it to your Threat Profile. This monitors changes to

selected entities over time, including new variations, associations, or reporting.

- Navigate to the **Added to Threat Profile** tab to view all the Malware being followed.



View Malware Details

Select any Malware or Tool for a quick view of a detailed summary. Click **View Full Link** to drill down further into specific components of the Malware profile.

- **Details:** This tab displays the same comprehensive summary of the Malware or tool profile as seen in the quick view. It also includes a visualization of the number of Indicators attributed to the Malware, broken down by type. A list of news analysis reports related to the Malware is also displayed.

Explore Malware > FORMBOOK

FORMBOOK

Details | MITRE ATT&CK | Validation | Graph | Indicators | YARA Rules | Relevant Reporting

Reported As

Formbook (Checkpoint) Needledropper (AVAST Software) Trickgate (Check Point) Xloader (Checkpoint)

Xloader (Internet)

Description

FORMBOOK is a backdoor written in C that communicates via HTTP. Supported commands include screenshot capture, shell command execution, file download, and file execution. FORMBOOK is also capable of capturing keystrokes, monitoring the clipboard, stealing web browser cookies, and extracting credentials stored by web browsers. FORMBOOK also uses hooks to intercept credentials and account information associated with web browsers and email clients.

Operating Systems

Windows

Associated Malware

ADWIND	AGENTTESLA	ASYNCRAT	AUTOLOG
DAVESHHELL	GULoader	HAWKEYE	LOKIBOT
MODILOADER	MOONDEV	NANOCORE	NESHTA
NETWIRE	PONY	VJWORM	WARZONE
XTREMERAT			

Role

Backdoor

Capabilities

Anti-VM capabilities	Anti-debug capabilities	Calculates MurmurHash3 hashes
Calculates SHA-1 hashes	Calculates hashes using CRC32B	Encodes using Base64
Encrypts data with RC4	Encrypts data with XOR	

Associated Actors

APT36 TEMP.Splinter UNC2589

Associated Vulnerabilities

CVE-2017-11882 CVE-2018-0802

Detection Names

FE_Trojan_Win32_FormBook_1 (http_inspect) unknown Content-Encoding used (Cisco Firepower)	Malicious.SSL.FormBook Downloader.Formbook	FE_Trojan_Win32_FormBook_3 Rt.Dropper.Agent-7512885-0 (ClamAV)
ET_TROJAN_VMPProtect_Packed_Binary_Inbound_via_HTTP_-_Likely_Hostile_(ET_OPEN)	FE_Trojan_Win32_Formbook_2	FILE-EXECUTABLE Portable Executable binary file magic detected (Cisco Firepower)
Virus.Win32.20180802.cft (Palo Alto Networks)	ET_POLICY_MSI_(microsoft_installer_file)_download_(ET_OPEN)	Snort Alert [1:2101390:9] (ET OPEN)
Trojan.Win32.FormBook.FEC3 (Trellix)	MALWARE-OTHER Win.Trojan.AZORult malicious executable download attempt (Talos)	Win.Malware.Generic-6750452-0 (ClamAV)
Backdoor.MSIL.FORMBOOK (Trellix)	FE_APT_Backdoor_Win32_FULLHOUSE_2 (Trellix)	ET_TROJAN_UPX_compressed_file_download_possible_malware_(ET_OPEN)
FE_APT_Backdoor_Win_FULLHOUSE_1 (Trellix)	Backdoor.win32.FORMBOOK.FEC2 (Trellix)	ET_SHELLCODE_Possible_TCP_x86_JMP_to_CALL_Shellcode_Detected_(ET_OPEN)
Trojan.Formbook (Trellix)	FE_APT_Tunneler_Win32_FULLHOUSE_1 (Trellix)	Win.Packer.MalwareCrypter-6620810-1 (ClamAV)
FE_Trojan_Formbook	Win.Trojan.Agent-7496948-0 (ClamAV)	Malware.Binary (Trellix)
ET_INFO_Dotted_Quad_Host_XLSX_Request_(ET_OPEN)	Win.Packed.Genericldr-9806508-0 (ClamAV)	(http_inspect) not HTTP traffic (Cisco Firepower)
ET_POLICY_exe_download_via_HTTP_-_Informational_(ET_OPEN)	ET_INFO_SUSPICIOUS_Dotted_Quad_Host_MZ_Response_(ET_OPEN)	Trojan.Formbook
trojan/Win32_EXE.noon.exe (Palo Alto Networks)	Win.Malware.Autoit-6979743-0 (ClamAV)	trojan/Win32_EXE.autoit.pjrd (Palo Alto Networks)
ET_POLICY_PE_EXE_or_DLL_Windows_file_download_HTTP_(ET_OPEN)	Trojan.Win.Formbook (Trellix)	ET_INFO_Executable_Download_from_dotted-quad_Host_(ET_OPEN)
Trojan.MSIL.FORMBOOK.FEC2 (Trellix)	Trojan.MSIL.AgentTesla.FEC2 (Trellix)	Malicious.SSL.FormbookCert
trojan/Win32_EXE.crypt.akbu (Palo Alto Networks)	FE_APT_Backdoor_Win32_FULLHOUSE_2.FEC2 (Trellix)	MALWARE-CNC Win.Trojan.FormBook variant outbound connection (Talos)

Indicators

19060

- Files
- URLs
- Domains

News Analysis

- MEDIA ON-TARGET** JANUARY 31, 2023
Researchers Uncover Packer Used by Several Malware to Evade Detection for 6 Years... THE HACKER NEWS
- PLAUSIBLE** AUGUST 18, 2022
DarkTorch: Malware Wraps in Sophistication for High-Volume RAT Infections DARK READING
- PLAUSIBLE** MARCH 5, 2021
Cybercriminals Target Industrial Organizations in Information Theft Campaign SECURITYWEEK
- PLAUSIBLE** APRIL 22, 2020
Microsoft Warns of "Prolific" Trickbot Malware Exploiting COVID-19 Crisis IT PRO
- PLAUSIBLE** JULY 17, 2019
SWEED Hackers Target Manufacturing, Logistics Organizations SECURITYWEEK
- PLAUSIBLE** MAY 25, 2018
New "ThreadKit" Office Exploit Builder Emerges SECURITY WEEK
- PLAUSIBLE** MAY 9, 2018
Office 365 Zero-Day Used in Real-World Phishing Campaigns BLEEPING COMPUTER
- PLAUSIBLE** NOVEMBER 9, 2017
Russia's Fancy Bear Hackers Exploit a Microsoft Office Flaw - and NYC Terrorism F... WIRED
- MEDIA ON-TARGET** OCTOBER 19, 2017
FIN7 Weaponization of DDE is Just Their Latest Slick Move, Say Researchers CYBERSCOOP
- MEDIA ON-TARGET** OCTOBER 6, 2017
Formbook Campaigns Target U.S., South Korea SECURITY WEEK

- MITRE ATT&CK:** This tab shows the Tactics, Techniques, and Procedures (TTPs) observed to be associated with delivering, deploying, or executing the selected Malware. All TTPs associated with the Malware can be downloaded by clicking Download TTPs from the Actions drop-down.

Explore Malware > FORMBOOK

FORMBOOK

Details MITRE ATT&CK Validation Graph Indicators YARA Rules Relevant Reporting

MITRE ATT&CK

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	
<ul style="list-style-type: none"> Develop Capabilities T1587 Obtain Capabilities T1588 	<ul style="list-style-type: none"> Phishing T1566 <ul style="list-style-type: none"> Spearphishing Attachment T1566.001 	<ul style="list-style-type: none"> Command and Scripting Interpreter T1059 System Services T1569 Windows Management Instrumentation T1047 	<ul style="list-style-type: none"> Boot or Logon Autostart Execution T1547 Create or Modify System Process T1543 	<ul style="list-style-type: none"> Access Token Manipulation T1134 Boot or Logon Autostart Execution T1547 Create or Modify System Process T1543 Process Injection T1055 	<ul style="list-style-type: none"> Access To T1134 Deobfuscate T1140 Hide Artifacts T1564 Indicator T1070 Malware T1036 Modify Registry T1112 Obfuscate T1027 Process Injection T1055 Subvert T1553 Virtualize T1497

Take Action

- Download Indicators
- Download TTPs**
- Download YARA Rules

- o Selecting a specific technique or subtechnique provides a brief description and a list of Actions that can be used to test your security controls against it. Click **Validate** to pivot directly to the Security Validation platform to execute any of the listed Actions.

A subscription to Security Validation is required to validate the Actions listed.

Spearphishing Attachment (T1566.001)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Validations

362 Actions Available **Validate**

Name	VID
> Copy of Phishing Email - Malicious Attachment, APT19, 2019 Financials Lure	A200-013
> Copy of Phishing Email - Malicious Attachment, EMOTET Downloader, Variant #4	A200-044
> Phishing Email - Malicious Attachment, TRICKBOT, Black Lives Matter Theme Lure	A101-218
> Phishing Email - Malicious Attachment, TRICKBOT, Order Confirmation Lure, Variant #3	A102-229
> Phishing Email - Malicious Attachment, TRICKBOT, Excel Lure, Variant #2	A102-255
> Phishing Email - Malicious Attachment, TRICKBOT	A100-413
> Phishing Email - Malicious Attachment, TRICKBOT, Excel Lure	A101-561
> Phishing Email - Malicious Attachment, TRICKBOT, Order Confirmation Lure	A101-894
> Phishing Email - Malicious Attachment, MOUSEISLAND, Variant #1	A102-257

Done

- **Validation:** This tab displays Actions that can be used to test your defenses against this Malware in the Security Validation platform by clicking **Validate**.

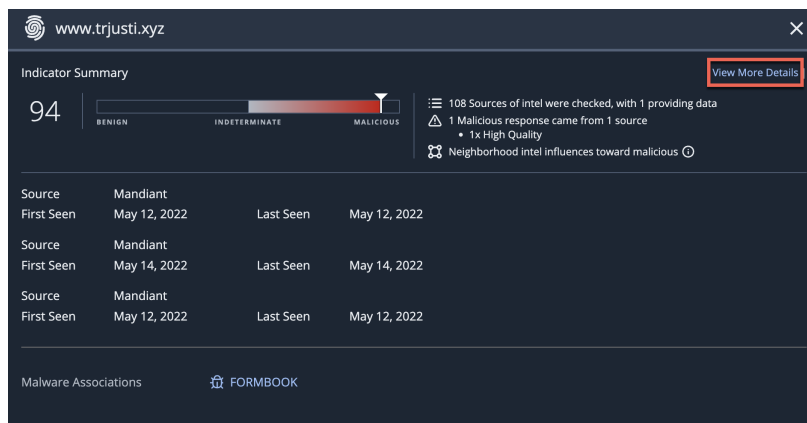


A subscription to Security Validation is required to validate the Actions listed.

- **Graph:** This tab provides an interactive graph to explore the various associations with this Malware family. The graph includes other associated Malware, attack patterns, Common Vulnerabilities and Exposures (CVEs), indicators of compromise (IOCs), targeted industries, and Threat Actors. Various layout options let you customize your view.



- **Indicators:** This tab includes a table with all known Indicators attributed to this Malware family, such as specific IP addresses, domains, and hashes.
 - **Indicator Value:** Indicators associated with the Malware, with links to pivot directly to the **Indicator Summary**. Click **View Full Link** to view the complete Indicator profile.



Indicator Summary

94

108 Sources of intel were checked, with 1 providing data
 1 Malicious response came from 1 source
 • 1x High Quality
 Neighborhood intel influences toward malicious

Source	First Seen	Last Seen
Mandiant	May 12, 2022	May 12, 2022
Mandiant	May 14, 2022	May 14, 2022
Mandiant	May 12, 2022	May 12, 2022

Malware Associations: FORMBOOK

- **Type:** The type of Indicator (such as IP address, URL, fully qualified domain name (FQDN), or hash).
- **IC Score:** The probability that a given Indicator is associated with malicious activity (in other words, a true positive).



The IC Score is not necessarily a measure of severity or criticality. For more information, see [Understanding IC-Score \(https://docs.mandiant.com/home/understanding-ic-score\)](https://docs.mandiant.com/home/understanding-ic-score).

- **Associated Actors:** Threat Actors known to be associated with the Indicator, with links to the Threat Actor profile.
- **Associated Malware:** Other Malware known to be associated with the selected Malware, with links to view

the complete Malware profile.

- **Associated Tools:** Tools observed to be used in association with this Malware.
- **Associated Campaigns:** Threat campaigns associated with the Malware, with links to view the complete Campaign profile.
- **First Seen:** Date when Mandiant last published updates regarding the Malware family.
- **Last Seen:** Date when information on the Malware was first made available to Mandiant customers.
- All Indicators associated with the Threat Actor can be downloaded either by clicking **Download Indicators**.

Indicator Value	Type	IC Score	Associated Actors	Associated Malware	Associated Tools	Associated Campaigns	File
http://2.59.254.18/_errorpages/obix.exe	URL	100	---	FORMBOOK	---	---	August 2, 2023 August 15, 2023
MD5 943b4e484151a97875e1ed46d77ffe SHA1 b477c9bc4867 20917d34a4e14 SHA256 19db4860329 ffa4d6de23de	Hash	100	---	FORMBOOK	---	---	August 15, 2023 August 15, 2023
MD5 b661633cfae6e392a3994073f6efc766 SHA1 a81a3805d4 17c85a0b77b69 SHA256 f8fcd7335247 8aa11b6d2f6ac	Hash	100	---	FORMBOOK	---	---	August 3, 2023 August 15, 2023
MD5 bb712812e3d293f7b3fb288b7681be7b SHA1 c81f7e74cf 80623a0f9668 SHA256 681b4f5d374 a8ad171585c0b	Hash	100	---	FORMBOOK	---	---	August 14, 2023 August 15, 2023
http://goxiba150.com/oy30/	URL	73	---	FORMBOOK	---	---	August 1, 2023 August 15, 2023
http://1.chaojqian.com/1w6f/	URL	73	---	FORMBOOK	---	---	June 20, 2023 August 15, 2023
MD5 872038d0d9dbbf8c2a68e0f2293248ea SHA1 e5d28d96688 df16c2932b148 SHA256 4246ac35e29b 57231abf222b8	Hash	100	---	FORMBOOK	---	---	August 10, 2023 August 15, 2023
MD5 6397cc13ef676dc11432dfb872f5ea5 SHA1 23a4da56e974 7229ffed9b735 SHA256 90a9a5a572cd 67ee94b336699	Hash	100	---	FORMBOOK	---	---	August 10, 2023 August 15, 2023
MD5 6e713e47f407f98a8633186138a52f8 SHA1 fa109a00fe1 a8ba86633438a SHA256 262f72e0322 151899f85666	Hash	100	---	FORMBOOK	---	---	August 4, 2023 August 15, 2023
MD5 785174884160278ca28421180544a17	Hash	100	---	FORMBOOK	---	---	August 2, 2023 August 15, 2023

- **YARA Rules:** This tab displays YARA rules that can be customized to detect this Malware in your environment. These YARA rules can be downloaded for use in threat hunt efforts or other workflows involving third-party security tools outside the MATI platform.

According to Mandiant's terms of service, any associated detections and subsequent reporting may be distributed as desired.

```

1 rule FE_Trojan_Win32_FormBook_3
2 {
3   meta:
4     author = "FireEye, inc"
5     date_created = "2020-05-20"
6     date_modified = "2020-05-20"
7     hash = "06acb35bb611ef2532b760afdcfd7d94"
8     rev = 4
9
10  strings:
11    $api1 = "FindResource*" fullword nocase
12    $api2 = "IsDebuggerPresent*" fullword nocase
13    $api3 = "QueryPerformanceCounter*" fullword nocase
14    $api4 = "GetTickCount*" nocase
15    $sdeLoop = { 88 C7 33 D2 F7 47 8A 82 [4] 30 44 37 FF 30 77 72 }
16
17  condition:
18    ( uint16(0)==0x5A4D) and ( uint32( uint32(0x3C))==0x80804550) and all of ($api1) and $sdeLoop
19  }
20
FE_Trojan_Win32_FormBook_1
1 rule FE_Trojan_Win32_FormBook_1
2 {
3   meta:
4     author = "FireEye, inc"
5     hash = "84C8CAE58EF39455DABD4844665D7DE"
6     rev = 5

```

- **Relevant Reporting:** This tab displays the latest reports generated by Mandiant that are related to or explicitly mention the selected Malware.

The following recording provides a deep dive into getting the most from Mandiant's intelligence related to Malware and



tools: