

MANDIANT ADVANTAGE THREAT INTELLIGENCE BROWSER PLUG-IN

The Mandiant Advantage Threat Intelligence (MATI) Browser Plugin streamlines threat research and investigation efforts by integrating Mandiant Threat Intelligence directly into your browser. The plugin automatically scans the web page that you're browsing and tags any mention of known Threat Intel entities, including the following:

- Indicators
 - IPv4 addresses
 - Domains
 - URLs
 - File Hashes
- Actors
- Campaigns
- Malware
- Vulnerabilities (Common Vulnerabilities and Exposures, or CVEs)

The MATI Browser Plugin includes features and capabilities specific to each supported browser.

Chrome

- Tap into instant ratings for millions of indicators from open source feeds, using over 225,000 hours per year of Mandiant Incident Response engagements.
- Quickly and easily overlay Threat Intelligence to prioritize the investigation of suspicious indicators in your logs, tools, and systems.
- Pivot directly into Mandiant Advantage from the browser plugin to gather more contextual information on attributed actors and malware families.
- Integrate and share threat insights with your teams and workflows for collaboration, investigation, and remediation.
- Highlights web page elements that may be associated with vulnerability data, such as matching Common Vulnerabilities and Exposures (CVEs) or designated keywords.
- Overlay threat information directly with **Google Security Operations** (<https://cloud.google.com/solutions/security-information-event-management>).
- Authenticate less frequently, including support for Federated Authentication.
 - All Mandiant Advantage subscribers have access to the MATI Browser Plugin using the same credentials as those used for the Mandiant Advantage platform.



The server *auth.mandiant.com* must be added to any firewall or proxy allowlists to enable authentication.

- Mandiant Advantage subscribers that use federated authentication can access the MATI Browser Plugin using their federated credentials. For more information, see **Federated Access** (<https://docs.mandiant.com/home/ma-federated-access>).



Federated Authentication is currently in Public Preview and is not supported in previous versions of the MATI Browser Plugin. You must upgrade to the latest version to use federated authentication with the Chrome browser extension.

Edge

- Tap into instant ratings for millions of indicators from open source feeds, using over 225,000 hours per year of Mandiant Incident Response engagements.
- Quickly and easily overlay Threat Intelligence to prioritize the investigation of suspicious indicators in your logs,

tools, and systems.

- Pivot directly into Mandiant Advantage from the browser plugin to gather more contextual information on attributed actors and malware families.
- Integrate and share threat insights with your teams and workflows for collaboration, investigation, and remediation.
- View highlighted web page elements that may be associated with vulnerability data, such as matching Common Vulnerabilities and Exposures (CVEs) or designated keywords.
- Overlay threat information directly with [Google Security Operations \(https://cloud.google.com/solutions/security-information-event-management\)](https://cloud.google.com/solutions/security-information-event-management).
- Authenticate less frequently, including support for Federated Authentication.
 - All Mandiant Advantage subscribers have access to the MATI Browser Plugin using the same credentials as those used for the Mandiant Advantage platform.



The server *auth.mandiant.com* must be added to any firewall or proxy allowlists to enable authentication.

- Mandiant Advantage subscribers that use federated authentication can access the MATI Browser Plugin using their federated credentials. For more information, see [Federated Access \(https://docs.mandiant.com/home/mandiant-federated-access\)](https://docs.mandiant.com/home/mandiant-federated-access).



Federated Authentication is currently in Public Preview and is not supported in previous versions of the MATI Browser Plugin. You must upgrade to the latest version to use federated authentication with the Chrome browser extension.

Firefox

- Tap into instant ratings for millions of indicators from open source feeds, using over 225,000 hours per year of Mandiant Incident Response engagements.
- Quickly and easily overlay Threat Intelligence to prioritize the investigation of suspicious indicators in your logs, tools, and systems.
- Pivot directly into Mandiant Advantage from the browser plugin to gather more contextual information on attributed actors and malware families.
- Integrate and share threat insights with your teams and workflows for collaboration, investigation, and remediation.
- View highlighted web page elements that may be associated with vulnerability data, such as matching Common Vulnerabilities and Exposures (CVEs) or designated keywords.
- Overlay threat information directly with [Google Security Operations \(https://cloud.google.com/solutions/security-information-event-management\)](https://cloud.google.com/solutions/security-information-event-management).
- Authenticate less frequently, including support for Federated Authentication.
 - All Mandiant Advantage subscribers have access to the MATI Browser Plugin using the same credentials as those used for the Mandiant Advantage platform.



The server *auth.mandiant.com* must be added to any firewall or proxy allowlists to enable authentication.

- Mandiant Advantage subscribers that use federated authentication can access the MATI Browser Plugin using their federated credentials. For more information, see [Federated Access \(https://docs.mandiant.com/home/mandiant-federated-access\)](https://docs.mandiant.com/home/mandiant-federated-access).



Federated Authentication is currently in Public Preview and is not supported in previous versions of the MATI Browser Plugin. You must upgrade to the latest version to use federated authentication with the Chrome browser extension.

Videos

There are two additional Browser Plugin videos:

- **MATI Browser Plugin Onboarding** (<https://docs.mandiant.com/home/onboarding-mati-browser-plugin-overview>)
- **Using the Browser Plugin with Splunk** (<https://docs.mandiant.com/home/how-to-use-mandiant-advantage-browser-plugin-with-splunk>)

This video is for version 1.0 of the plugin so is not 100% up-to-date

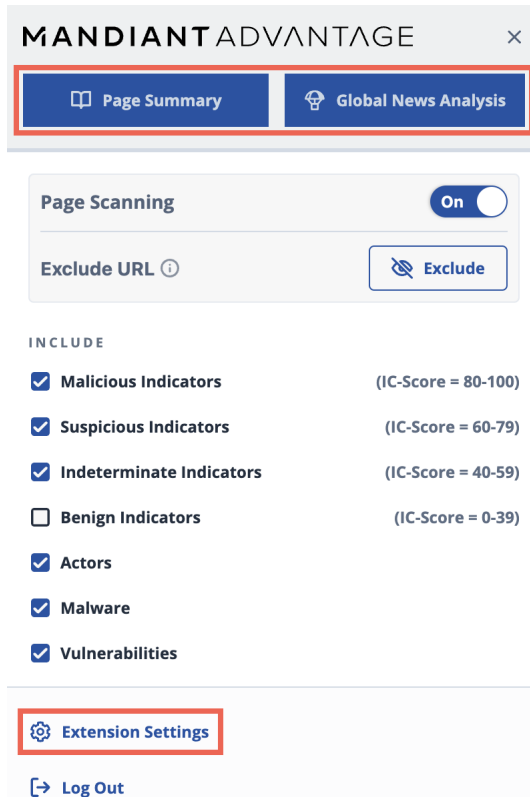
Download and install

Download and add the latest MATI Extension to your browser. If the available features don't match what you are seeing, go to the Browser's plugin page & verify you have the latest version.

- **Chrome** (<https://chrome.google.com/webstore/detail/mandiant-advantage-threat/aghmgfkjfbckokededacdhemkpgdcko>)
- **Firefox** (<https://addons.mozilla.org/en-US/firefox/addon/mandiant-advantage/>)
- **Edge** (<https://microsoftedge.microsoft.com/addons/detail/mandiant-advantage-thre/bbbhekpifeagoagebiifoiedkckkfcfl>)

Configure the plugin

1. Once installed, click the Threat Intelligence extension to authenticate with your Mandiant Advantage platform credentials.
2. Select the Threat Intelligence extension again to configure what Threat Intelligence artifacts you want to highlight on your web browser page.
3. (Optional) Click **Page Summary** to display the ongoing results of the scan as you scroll.
4. (Optional) Click **Global News Analysis** to view our latest article analysis.
5. (Optional) Click **Extension Settings** to configure webhooks to share content directly in your organization's chat client (Teams, Slack, or Google Chat).



MANDIANT ADVANTAGE ×

Page Summary Global News Analysis

Page Scanning **On**

Exclude URL ⓘ Exclude

INCLUDE

- Malicious Indicators (IC-Score = 80-100)
- Suspicious Indicators (IC-Score = 60-79)
- Indeterminate Indicators (IC-Score = 40-59)
- Benign Indicators (IC-Score = 0-39)
- Actors
- Malware
- Vulnerabilities

Extension Settings

Log Out

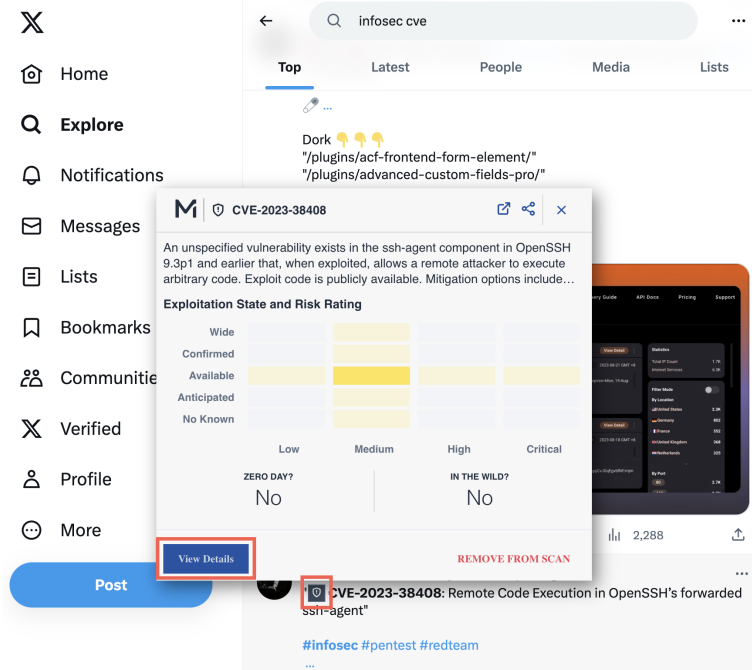
Use Case Scenarios

The following use cases provide exemplary persona-based workflows for using the MATI Browser Plugin.

Use Case Scenarios for a CTI Analyst

- **Review tweets**

While browsing an InfoSec Twitter thread with Threat Intelligence extension configured to include **Vulnerabilities**, you can quickly get details of a Vulnerability (CVE).



- Click **View Details** to display observed threat intelligence related to the Vulnerability.



The widgets displayed are dynamically populated based on live data in the Mandiant Advantage platform. If no supporting data is available, the associated widget will be hidden from the View Details modal.

- Click the respective icons to perform the following actions:
 - **View in Mandiant Advantage:** Pivot directly to the Mandiant Advantage platform to interact directly with the complete Vulnerability profile.
 - **Share:** Pivot directly to your organization's chat client to place a link to the Mandiant Advantage platform for the Vulnerability.
 - **Download CSV:** Download a CSV containing the details of the Vulnerability, including the following headers:
 - Name
 - Summary
 - Exploitation State
 - Risk Rating
 - Exploited in the Wild
 - Exploited as Zero-Day
 - Actors Associations
 - Malware Associations
 - CVSS Ratings
 - Relevant Reporting

MANDIANT ADVANTAGE
✕

←
Back

🛡️
CVE-2023-38408

🔗
🔄
📄

Summary

An unspecified vulnerability exists in the ssh-agent component in OpenSSH 9.3p1 and earlier that, when exploited, allows a remote attacker to execute arbitrary code. Exploit code is publicly available. Mitigation options includ...

[SHOW MORE](#)

Severity

Exploitation State and Risk Rating

	HIGHEST PRIORITY			
	Low	Medium	High	Critical
Wide				
Confirmed				
Available				
Anticipated				
No Known				

ZERO DAY?

No

IN THE WILD?

No

Vulnerable Products

98

Total Products

- Canonical Ltd.
- Fedora Project
- FreeBSD
- OpenBSD
- Red Hat Inc.
- Redhat
- SUSE Inc. (Formerly Nc
- Other

Exploit Grades

2

Total Exploits

- Weaponized

Details

EPSS Score	0.03651
EPSS Percentile	90.51%
CWE	Unquoted Search Path or Element (CWE-428)
Mitigation	Patch, Workaround
Date Of Disclosure	July 19, 2023
Days To Patch	0
Exploitation Consequence	Code Execution
Exploitation Vectors	General Network Connectivity, Malicious Server



- Explore Threat Actor details from a threat report

- While browsing a threat report, you can quickly get details of a Threat Actor and pivot directly into Mandiant Advantage.

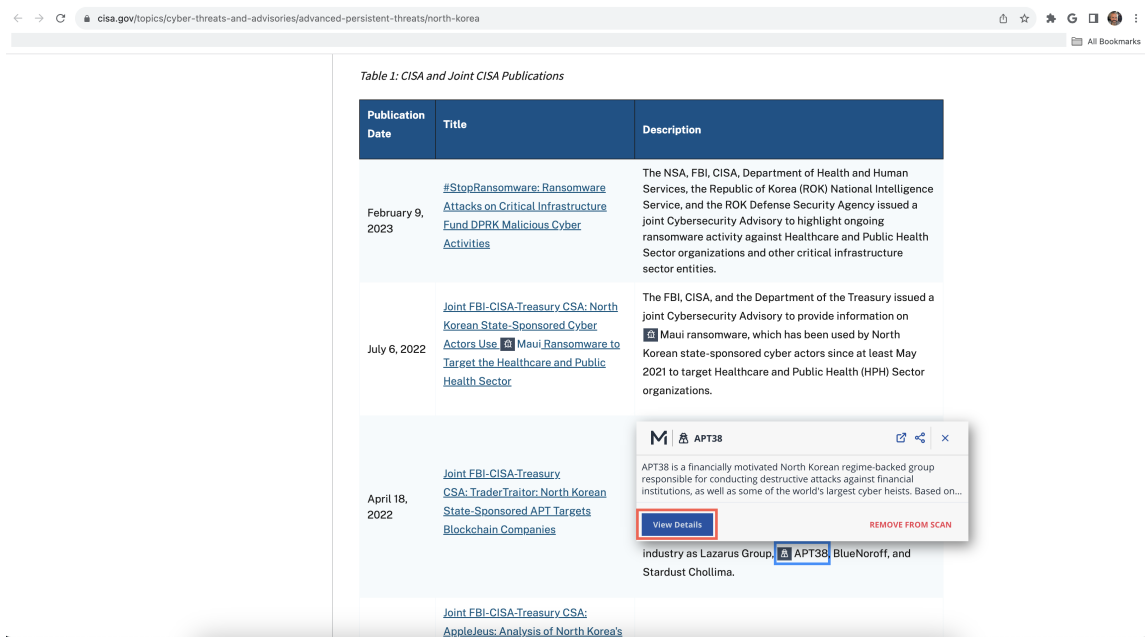


Table 1: CISA and Joint CISA Publications

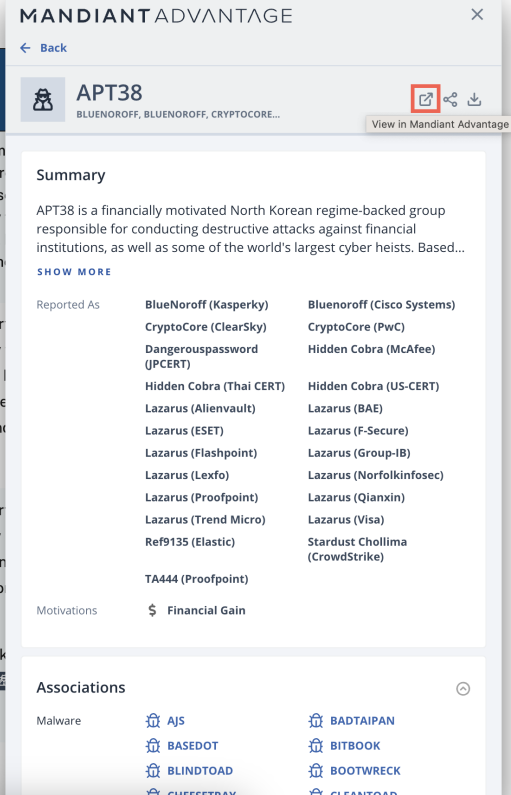
Publication Date	Title	Description
February 9, 2023	#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities	The NSA, FBI, CISA, Department of Health and Human Services, the Republic of Korea (ROK) National Intelligence Service, and the ROK Defense Security Agency issued a joint Cybersecurity Advisory to highlight ongoing ransomware activity against Healthcare and Public Health Sector organizations and other critical infrastructure sector entities.
July 6, 2022	Joint FBI-CISA-Treasury CSA: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector	The FBI, CISA, and the Department of the Treasury issued a joint Cybersecurity Advisory to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.
April 18, 2022	Joint FBI-CISA-Treasury CSA: Trader-Traitor: North Korean State-Sponsored APT Targets Blockchain Companies	APT38 is a financially motivated North Korean regime-backed group responsible for conducting destructive attacks against financial institutions, as well as some of the world's largest cyber heists. Based on... industry as Lazarus Group, APT38, BlueNoroff, and Stardust Chollima.
	Joint FBI-CISA-Treasury CSA: AppleJeus: Analysis of North Korea's	

View Details (highlighted) REMOVE FROM SCAN

- Click **View Details** to display observed threat intelligence related to the Threat Actor.

Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
February 9, 2023	#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities	The NSA, FBI, CISA, Department of Justice, the Republic of Korea Service, and the ROK Defense Cybersecurity Advisory Group announced joint cybersecurity activity against ransomware activity against Sector organizations and other sector entities.
July 6, 2022	Joint FBI-CISA-Treasury CSA: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector	The FBI, CISA, and the Department of Justice announced joint cybersecurity activity against a North Korean state-sponsored ransomware, which is used to target Healthcare and Public Health organizations.
April 18, 2022	Joint FBI-CISA-Treasury CSA: TraderTractor: North Korean State-Sponsored APT Targets Blockchain Companies	The FBI, CISA, and the Department of Justice announced joint cybersecurity activity associated with cryptocoins and a North Korean state-sponsored threat.
	Joint FBI-CISA-Treasury CSA: AppleJus: Analysis of North Korea's	This group is commonly tracked in the industry as Lazarus Group, and Stardust Chollima.



MANDIANT ADVANTAGE

APT38
BLUENOROFF, BLUENOROFF, CRYPTOCORE...

Summary

APT38 is a financially motivated North Korean regime-backed group responsible for conducting destructive attacks against financial institutions, as well as some of the world's largest cyber heists. Based...

Reported As

BlueNoroff (Kasperky)	Bluenoroff (Cisco Systems)
CryptoCore (ClearSky)	CryptoCore (PwC)
Dangerouspassword (JPCERT)	Hidden Cobra (McAfee)
Hidden Cobra (Thai CERT)	Hidden Cobra (US-CERT)
Lazarus (Alienvault)	Lazarus (BAE)
Lazarus (ESET)	Lazarus (F-Secure)
Lazarus (Flashpoint)	Lazarus (Group-IB)
Lazarus (Lexfo)	Lazarus (Norfolkinfosec)
Lazarus (Proofpoint)	Lazarus (Qianxin)
Lazarus (Trend Micro)	Lazarus (Visa)
Ref9135 (Elastic)	Stardust Chollima (CrowdStrike)
TA444 (Proofpoint)	

Motivations

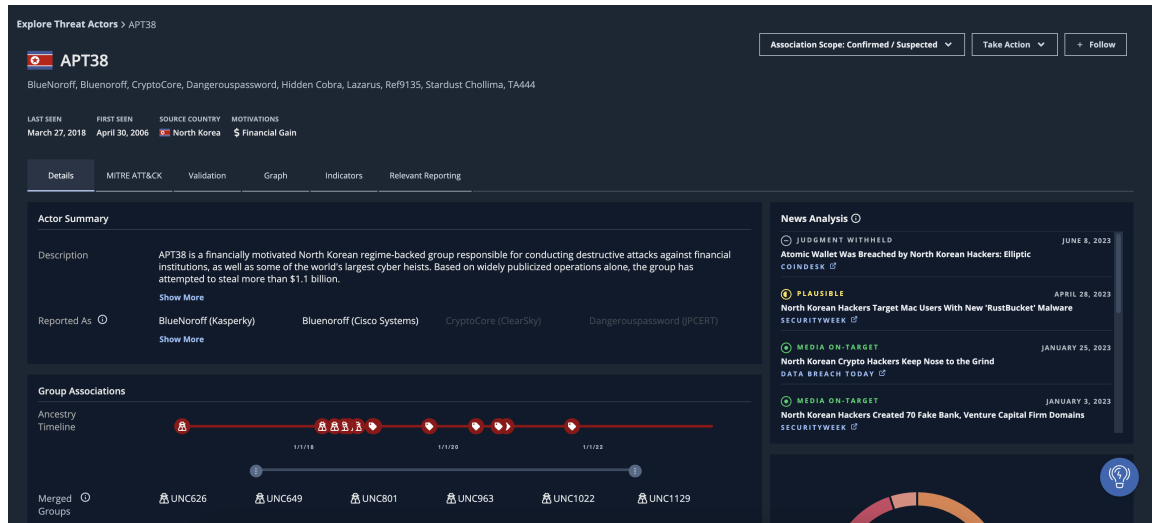
- Financial Gain

Associations

Malware

- AJS
- BASEDOT
- BLINDTOAD
- QUEEERDAY
- BADTAIPAN
- BITBOOK
- BOOTWRECK
- CLEANROAD

- Click the **View in Mandiant Advantage** icon to pivot directly to the Threat Actor profile in the Mandiant Advantage platform.



Explore Threat Actors > APT38

APT38
BlueNoroff, Bluenoroff, CryptoCore, Dangerouspassword, Hidden Cobra, Lazarus, Ref9135, Stardust Chollima, TA444

LAST SEEN: March 27, 2018 | FIRST SEEN: April 30, 2006 | SOURCE COUNTRY: North Korea | MOTIVATIONS: Financial Gain

Actor Summary

Description: APT38 is a financially motivated North Korean regime-backed group responsible for conducting destructive attacks against financial institutions, as well as some of the world's largest cyber heists. Based on widely publicized operations alone, the group has attempted to steal more than \$1.1 billion.

Reported As: BlueNoroff (Kasperky), Bluenoroff (Cisco Systems), CryptoCore (ClearSky), Dangerouspassword (JPCERT)

Group Associations

Timeline: 1/1/18 to 1/1/22

Merged Groups: UNCG526, UNG649, UNC801, UNC963, UNCI022, UNCI129

News Analysis

- JUDGMENT WITHHELD: Atomic Wallet Was Breached by North Korean Hackers: Elliptic COINDESK (JUNE 8, 2023)
- PLAUSIBLE: North Korean Hackers Target Mac Users With New 'RustBucket' Malware SECURITYWEEK (APRIL 28, 2023)
- MEDIA ON-TARGET: North Korean Crypto Hackers Keep Nose to the Grind DATA BREACH TODAY (JANUARY 25, 2023)
- MEDIA ON-TARGET: North Korean Hackers Created 70 Fake Bank, Venture Capital Firm Domains SECURITYWEEK (JANUARY 3, 2023)

- Get details of a file hash Indicator from a security advisory
 - While browsing a threat report, you can quickly get details of an Indicator such as a file hash.



The Indicator Confidence Score (IC-Score) is displayed for Indicators that have been reviewed by Mandiant. IC-Score is a measure of the degree of confidence that an Indicator is malicious, but not a measure of severity. For more information, see [Understanding IC-Score](https://docs.mandiant.com/home/understanding-ic-score) and [Indicator Threat Score and Confidence Score Source Descriptions](https://docs.mandiant.com/home/mati-ic-score-source-descriptions).

Appendix B: Indicators of Compromise (IOCs)

The IOC section includes hashes and IP addresses for the Maui and HolyGh0st ransomware variants—as well as custom malware implants assumedly developed by DPRK cyber actors, such as remote access trojans (RATs), loaders, and other tools—that enable subsequent deployment of ransomware. For additional Maui IOCs, see joint CSA [North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector](#).

Table 2 lists MD5 and SHA256 hashes associated with malware implants, RATs, and other tools used by DPRK cyber actors, including tools that drop Maui ransomware files.

Table 2: File names and hashes of malicious implants, RATs, and tools

MD5Hash	SHA256Hash
079b4588eaa99a1e802adf5e0b26d8aa	f67ee77d6129bd1bcd5d856c0fc5314169b946d32b8abaa4e680bb98130b38e7
2d02f5499d35a8dff4c8bc0b7fec5c2	83020729d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
2e18350194e59bc6a2a3f6d59da11bd8	655aa64860f1655081489cf85b77f72a49de846a99dd122093db4018434b83ae
3bd22e0ac965ebb6a18bb71ba39e96dc	6b7f566889b80d1dba4f92d5e2fb2f5ef24f57fcd56bb594978dffe9edbb9eb

- Click **View Details** to display observed threat intelligence related to the associated file.

Appendix B: Indicators of Compromise (IOCs)

The IOC section includes hashes and IP addresses for the Maui and HolyGh0st ransomware variants—as well as custom malware implants assumedly developed by DPRK cyber actors, such as remote access trojans (RATs), loaders, and other tools—that enable subsequent deployment of ransomware. For additional Maui IOCs, see joint CSA [North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector](#).

Table 2 lists MD5 and SHA256 hashes associated with malware implants, RATs, and other tools used by DPRK cyber actors, including tools that drop Maui ransomware files.

Table 2: File names and hashes of malicious implants, RATs, and tools

MD5Hash	SHA256Hash
079b4588eaa99a1e802adf5e0b26d8aa	f67ee77d6129bd1bcd5d856c0fc5314169b946d32b8abaa4e680bb98130b38e7
0e9e256d8173854a7bc26982b1dde783	--
12c15a477e1a96120c09a860c9d479b3	26263e421e397db821669420489d2d3084f408671524fd4e1e23165a16dda2225
131fc4375971af391b459de33f81c253	--
17c46ed7b80c2e4d8ea6d0e88ea0827c	b9af4660da00c7fa975910d0a19fda072031c15fad1eef935a609842c51b7f7d
1875f6a68f70bee316c8a6eda9ebf8de	672ec8899b8ee513dbfc4590440a61023846ddc2ca94c88ae637144305c497e7
1a74c8dbb74ca241c1d3d22373a6769	ba8f9e7afe5f78494c11197c39a8911ef9262bf23e8a764c6f65c818837a44
1f6d9f8fbd4e6ed8cd73b9e95a928	4f089afa51fd0c1b2a39cc11cedb3a4a32611837a5408379384be6fe846e016
2d02f5499d35a8dff4c8bc0b7fec5c2	83020729d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
2e18350194e59bc6a2a3f6d59da11bd8	655aa64860f1655081489cf85b77f72a49de846a99dd122093db4018434b83ae
3bd22e0ac965ebb6a18bb71ba39e96dc	6b7f566889b80d1dba4f92d5e2fb2f5ef24f57fcd56bb594978dffe9edbb9eb

- **Reading or Perusing a Blog Post**
 - While browsing a cybersecurity blog, you can quickly get details of a ransomware. Again, click **View Details** for more detailed information, including a link to the ransomware in Mandiant Advantage.

The operations of ransomware operators themselves continue to mature. **LockBit** 3.0, for example, now offers a bug bounty program to crowd-source the criminal community to improve the group's operations and their leak data.

All of this has happened against the backdrop of **ups** in Russian-language cybercrime groups and other ransomware groups. It also led to a rash of new fraud, using the government of Ukraine's appeal for funds as the lure for a **wave** of cryptocurrency scams and other financial fakery.



Use Case Scenarios for a SOC Analyst

- **Triage and prioritize alerts in your SOC**

Since many SIEMs and other security tools are browser-based, the MATI Browser Plugin can help you prioritize response efforts at a glance. Because the IC-Score is displayed for each highlighted Indicator in your view, you can focus on those Indicators that are known to be malicious.

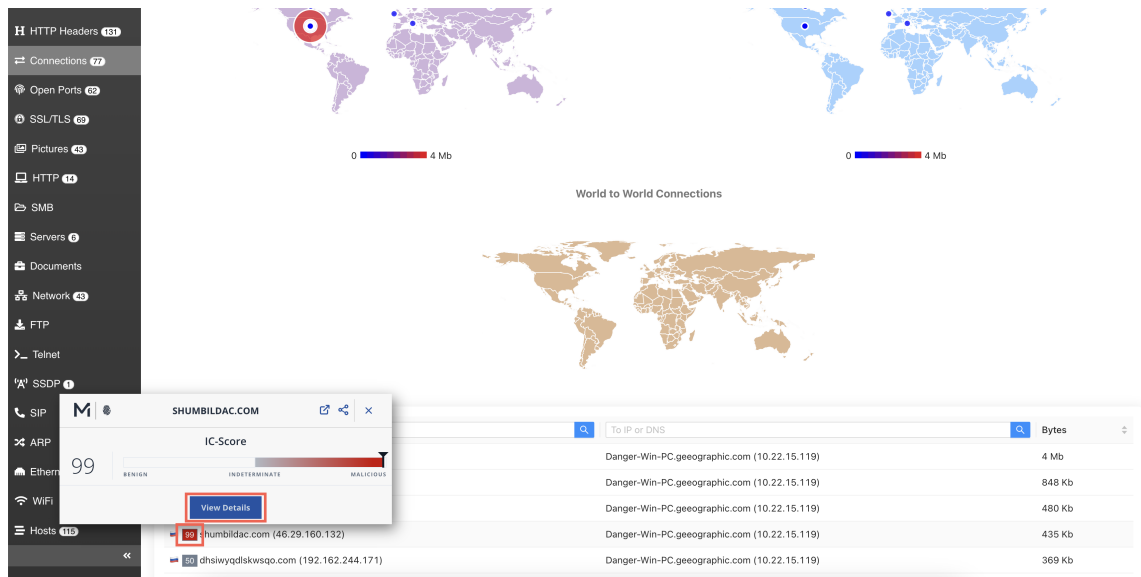


For more information about how IC-Scores are generated, see [IC-Score Source Descriptions](https://docs.mandiant.com/home/mati-ic-score-source-descriptions) (<https://docs.mandiant.com/home/mati-ic-score-source-descriptions>).

- **Investigate an uploaded PCAP file or firewall logs**

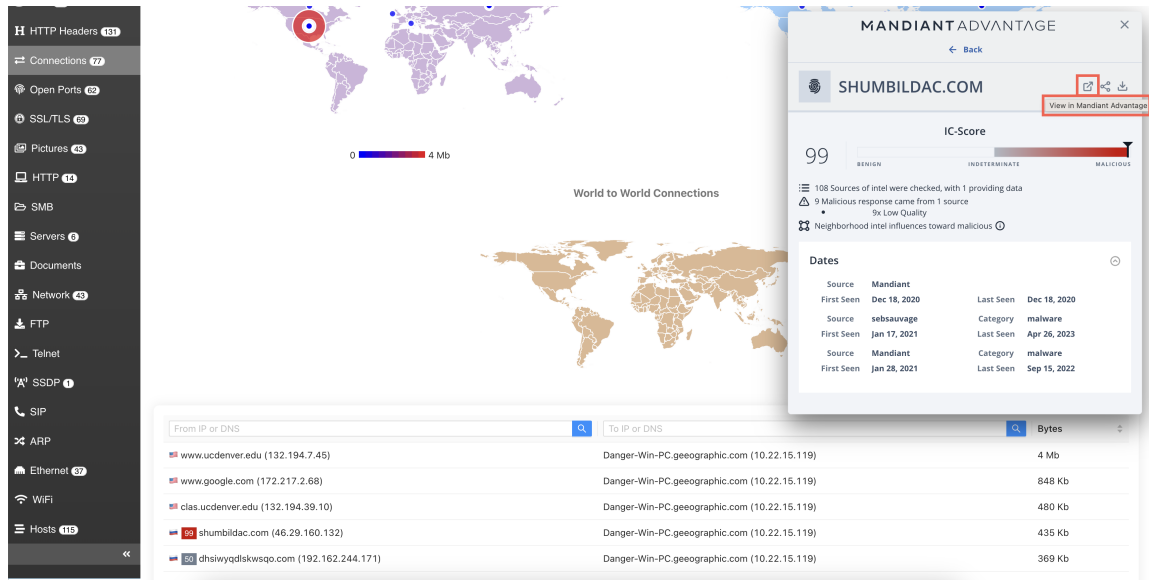
The MATI Browser Plugin applies critical context to packet capture (PCAP) files or firewall logs viewed in a web-based application.

- Click the highlighted IC-Score for more information about the associated Indicator. Click **View Details** to display observed threat intelligence related to the Indicator.



To IP or DNS	Bytes
Danger-Win-PC-geographic.com (10.22.15.119)	4 Mb
Danger-Win-PC-geographic.com (10.22.15.119)	848 Kb
Danger-Win-PC-geographic.com (10.22.15.119)	480 Kb
Danger-Win-PC-geographic.com (10.22.15.119)	435 Kb
Danger-Win-PC-geographic.com (10.22.15.119)	369 Kb

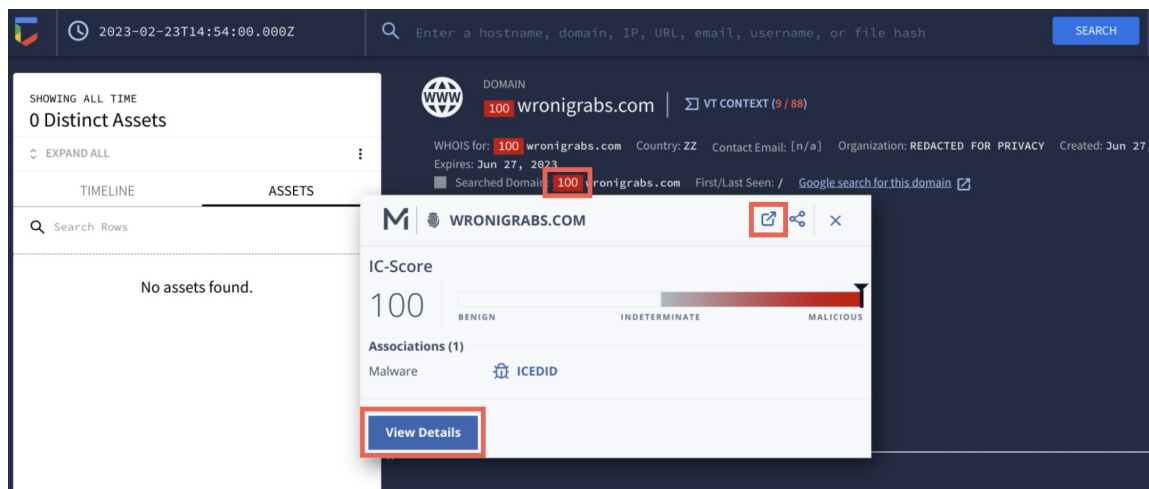
- Pivot directly into Mandiant Advantage by clicking **View in Mandiant Advantage**.



- **Domain Search in Google SecOps**

A search in Google Security Operations (SecOps) for suspicious domains provides the same pivot points to Mandiant Advantage.

- Click the highlighted IC-Score for more information about the associated domain. Click **View Details** to display observed threat intelligence related to the domain.



- Pivot directly into Mandiant Advantage by clicking **View in Mandiant Advantage**.