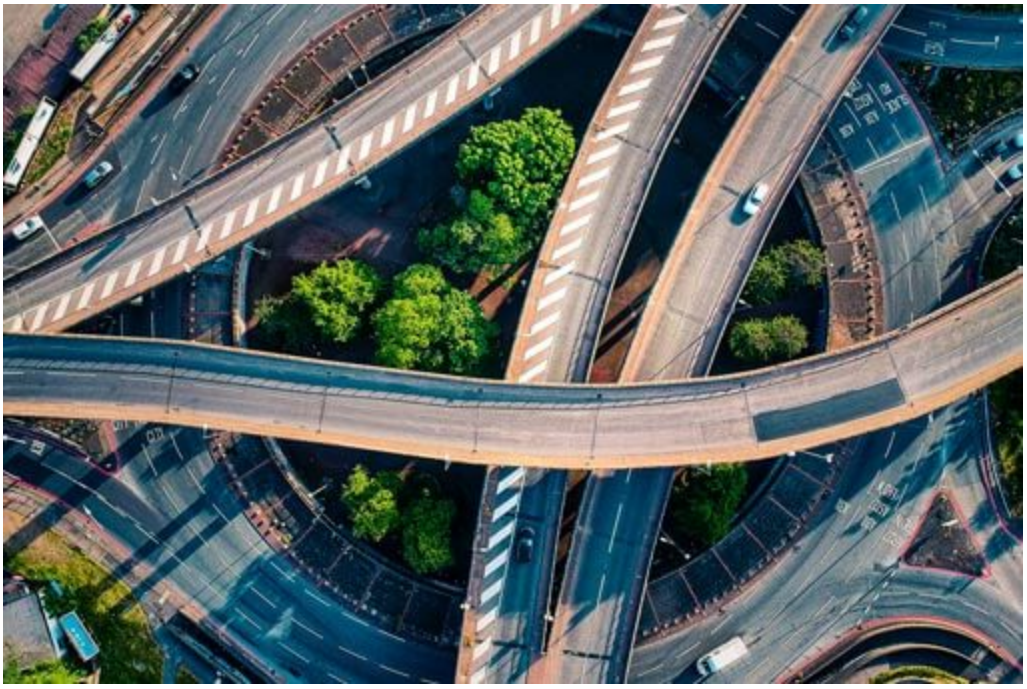
Trellix Global Defenders: Invasion of the Information Snatchers - Protecting against RedLine Infostealer

trellix.com/en-us/about/newsroom/stories/threat-labs/trellix-global-defenders-invaders-of-the-information-snatchers.html



Stories

The latest cybersecurity trends, best practices, security vulnerabilities, and more

Trellix

Threat Intelligence

By Taylor Mullins · February 7, 2022

What information are you storing in your Browsers?

Storing credentials and other important information in web browsers is a helpful method to not have to remember or reenter login or payment information for regularly visited sites, but threat actors also see this as an opportunity to steal credentials to either sell on the dark web or use for further cyberattacks. Tools like Redline, Agent Tesla, and Raccoon Stealer target popular web browsers such as Chrome, Edge, Firefox, Safari, and Opera, demonstrating why storing important information in browsers is a critical security risk.

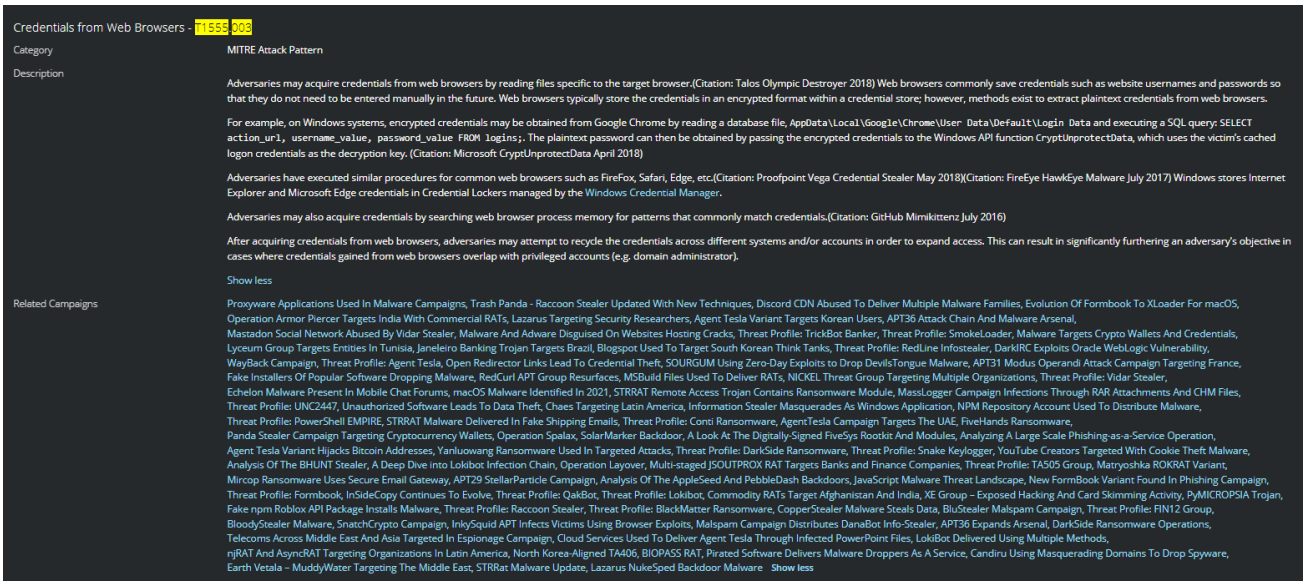


Figure 1. Description and Related Campaigns for MITRE Technique T1555.003. Source: MVISION Insights

Stealing the web browser credentials is a technique observed in many campaigns and utilized by numerous threat actors and APT groups, after acquiring the credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and accounts to expand access.

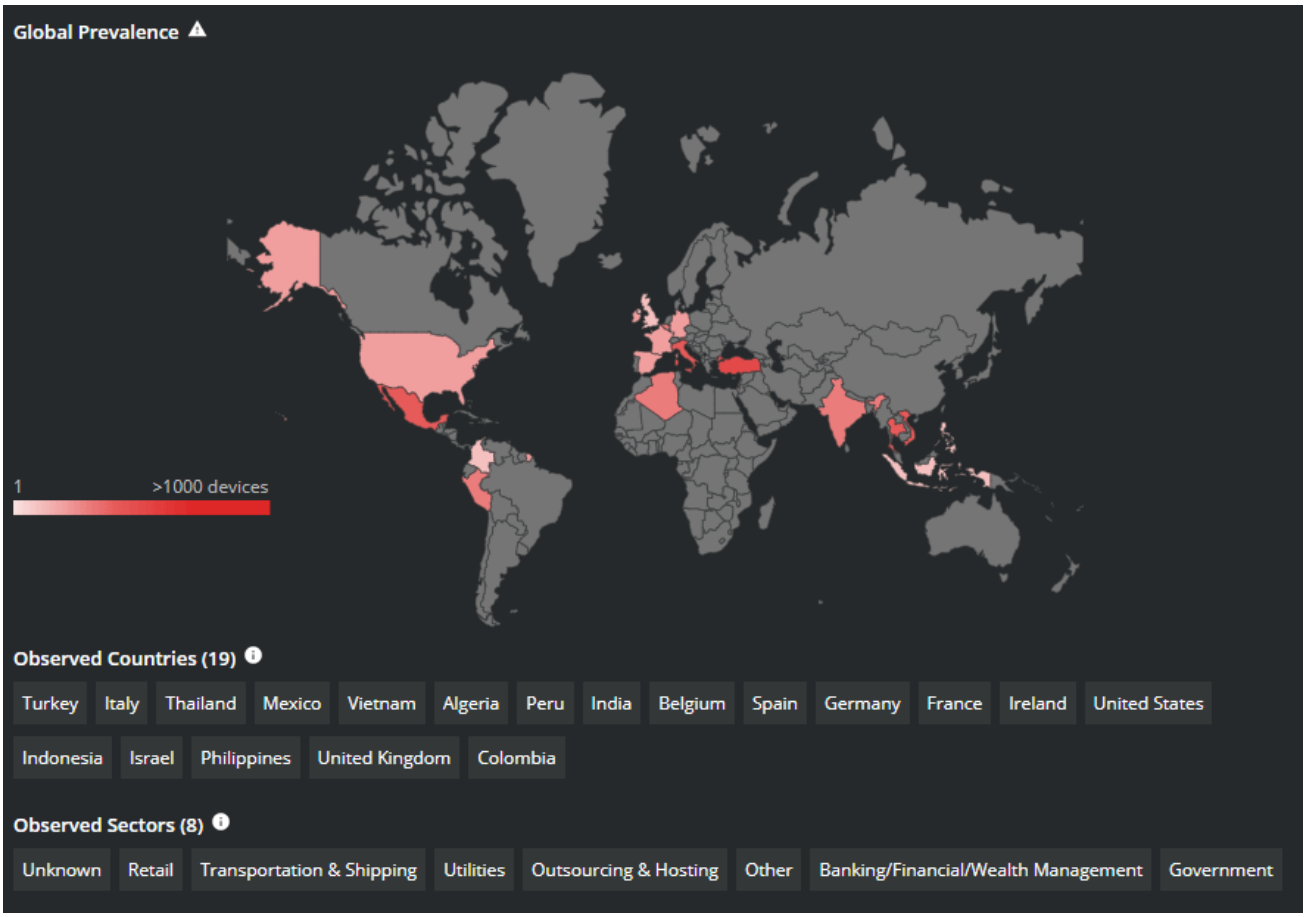


Figure 2. Global Prevalence and Observed Countries/Sectors of RedLine Infostealer. Source: MVISION Insights

While there are multiple variants of malware that can lift browser credentials, for this article we are going to highlight the activity of RedLine Infostealer due to its global reach and prevalence in recent attacks.

Main Features	Description
Collecting Information	- Collecting and stealing information saved to browsers - Login account and password - Cookies - Autofill - Credit card information - Browsers targeted for attack - All Chromium-based browsers - All Gecko-based browsers - Cryptocurrency wallet information - Seed file saved to the system
Collecting System Info	- Collecting default system info such as the IP address of system and OS info - Collecting hardware information such as the processor of the system, memory size, and GPU - Collecting information of browsers and software installed in the system - Collecting processes and anti-malware programs installed
C&C	- Controlling target system via SOAP protocol communication - Uploading and downloading files - Accessing arbitrary URL and running files

Figure 3. Features of the RedLine Stealer. Source: ASEC/Bleeping Computer

Redline Infostealer is available either as a standalone application or on a subscription basis on underground forums. As noted in the above table, RedLine gathers and exfiltrates a range of data including system information and credentials, autocomplete data, and credit card information from browsers, and FTP and IM clients. The malicious software also steals cryptocurrency and can download additional files onto the infected device.

Unfortunately, if you are a victim of RedLine malware, it's not enough to just change the passwords associated with that email account. Since RedLine targets all available data, you must change the password for all accounts used on the infected machine, including corporate VPN and email accounts, and other personal accounts.

RedLine Infostealer is commonly delivered by phishing emails, as well as social media messaging. The phishing email can often lure the recipient by something topical, ongoing current events, an often-used example being COVID-19 information.

Even if the users decline to store their credentials on the browser, the password management system will still add an entry to indicate that the website is "blacklisted." While the adversaries may not possess the actual passwords for the "blacklisted" accounts, it does tell them of the account existence, thus allowing them to perform credential stuffing or social engineering/phishing attacks.

Recommended Steps to Prevent Theft of Web Browser Credentials

Several mitigations can be put into place to prevent users from utilizing browser password managers or preventing the theft of browser credentials. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from these credential stores.

- Utilizing two-factor authentication can help reduce the risk of theft.
- Incorporating third-party password managers that can provide additional security controls.
- Disabling the ability for users to utilize Browser Password Managers via the local settings or Group Policy Object.

Dashlane Support: Disabling Chrome, Edge, Firefox, IE password managers via GPO

Trellix Protections and Global Detections

Trellix Global Threat Intelligence is currently detecting all known analyzed indicators and behavior associated with infostealer malware variants such as RedLine.

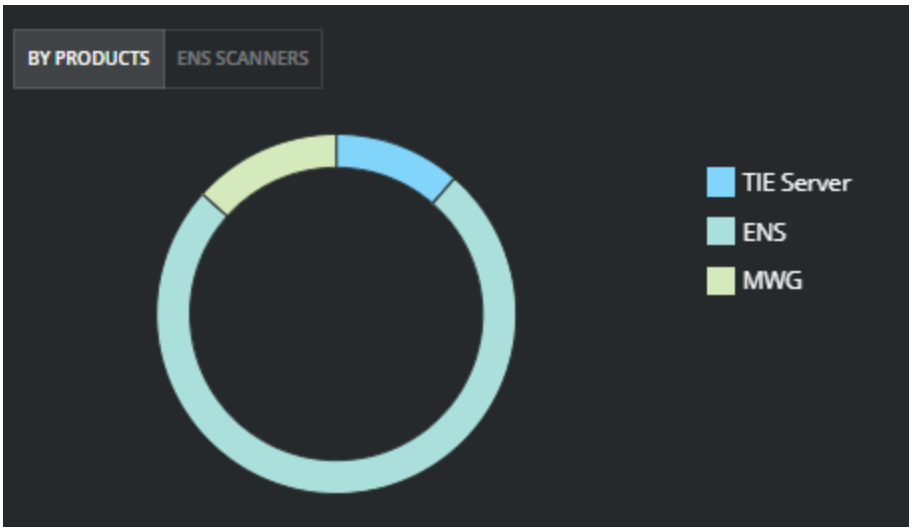


Figure 4. Trellix Products detecting this threat globally. Source: MVISION Insights

RedLine Payloads and Associated Activity Detections

Trellix Endpoint Security (ENS), Web Gateway (MWG), and Network Security Manager (NSP) are detecting RedLine Infostealer IOCs from the standpoint of signature detections and malware behavior.

RedLine Infostealer Detection Names:

redline_stealer
redline-fufi
Trojan:MSIL/RedLine.RPS!MTB
Trojan:Win32/RedLineStealer.DF!MTB
PWS:MSIL/RedLine.GG!MTB

X97M/Redline
Avira: TR/AD.RedLineSteal.nphvp
Redline
redline stealer
Trojan:Win32/RedlineStealer!MSR
TrojanSpy:MSIL/Redline.STA
Trojan:MSIL/RedLine!MTB
Redlinestealer
Trojan-Redline.a
Trojan:MSIL/RedLineStealer.MK!MTB
MALWARE: Redline Stealer Activity Detected
MALWARE: Redline Stealer Activity Detected – Trellix Network Security Platform/IPS

RedLine Payloads and Associated Activity Detections

MVISION Insights will provide the current threat intelligence and known indicators for Redline Infostealer. MVISION Insights will also alert to detections and process traces that have been observed in your environment and systems that require additional attention to prevent widespread infection. MVISION Insights will also include Hunting Rules for threat hunting and further intelligence gathering of the threat activity and adversaries known to utilize Redline.

Campaign Name -Threat Profile: RedLine Infostealer

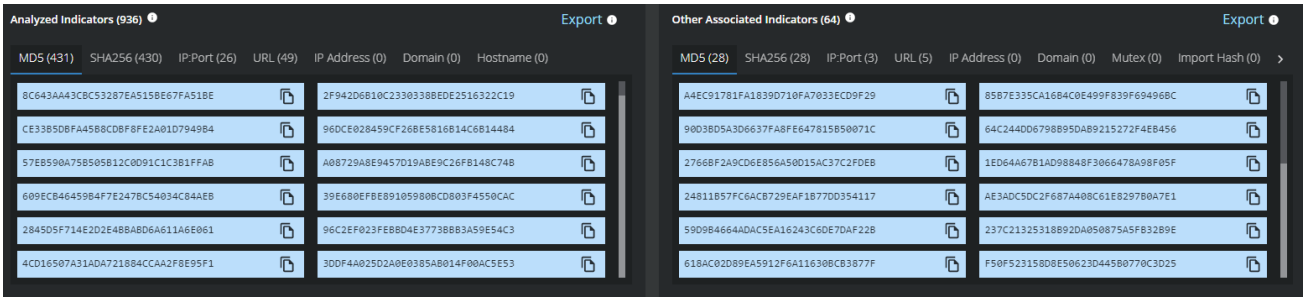


Figure 5. Analyzed and Other Associated Indicators for RedLine Infostealer

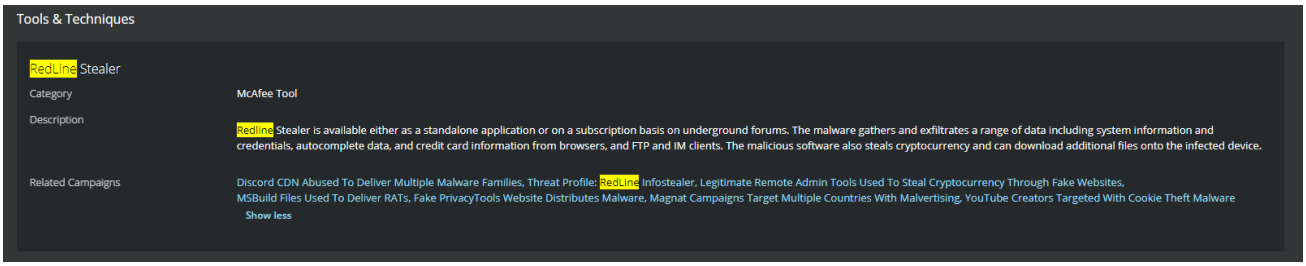


Figure 6. Redline Infostealer Description and Campaigns Observed using this tool

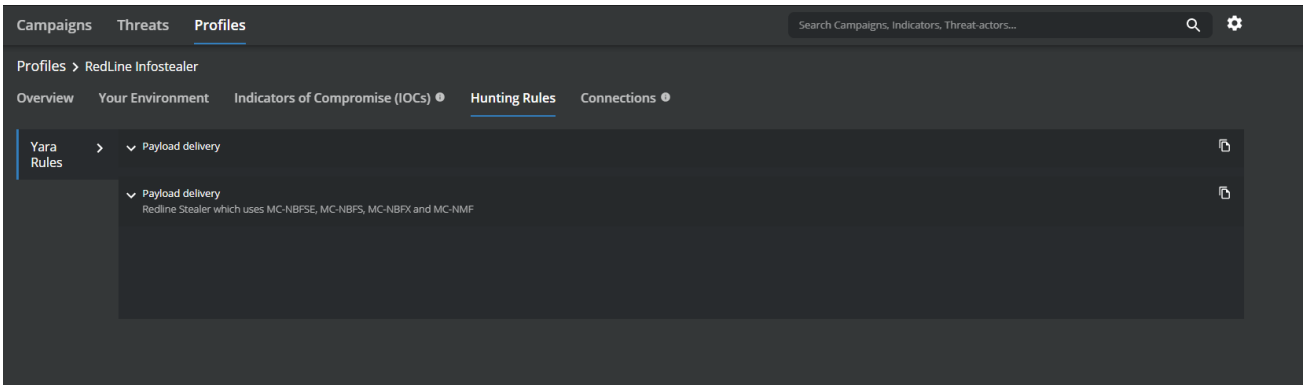


Figure 7. Yara Hunting Rules for RedLine in MVISION Insights

Detecting Malicious Activity with MVISION EDR

MVISION EDR is currently alerting to all known threat behavior and MITRE techniques associated with RedLine Infostealer. The below examples are filtered to show where the Redline malware accessed the encrypted login data within the Chromium based browsers and was able to recover and decrypt the data using the Native APIs built into Windows.

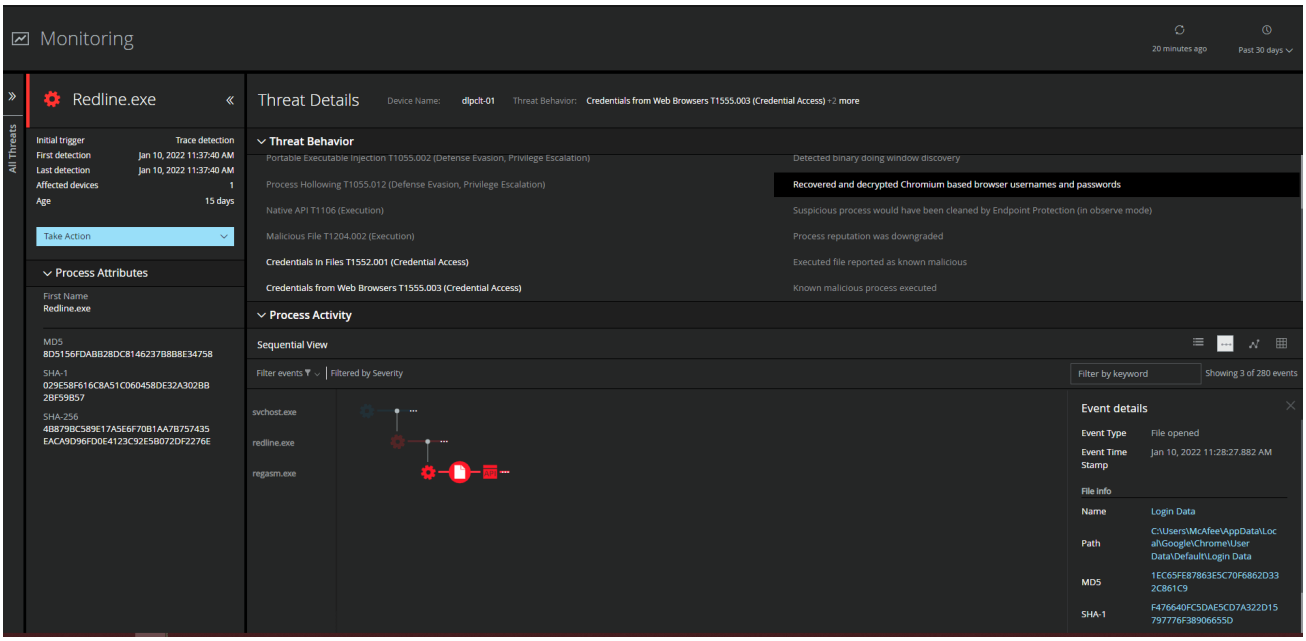


Figure 8. Recovery and decryption of browser credentials shown in MVISION EDR

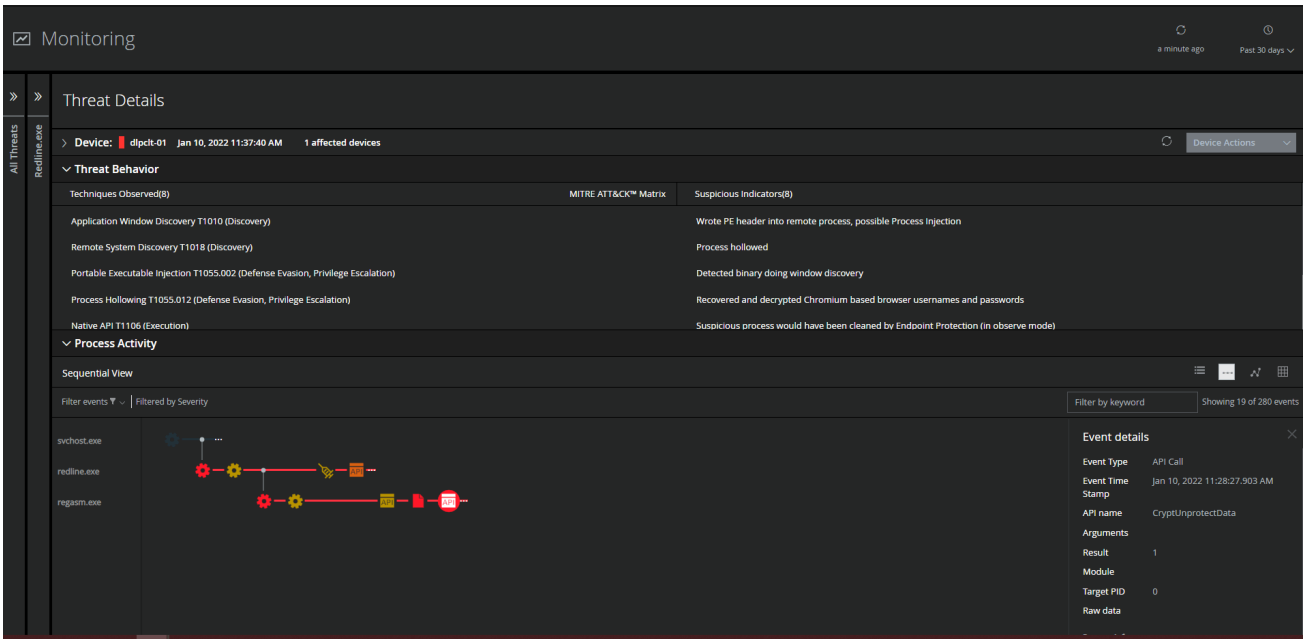


Figure 9. Accessing the CryptUnprotectData API to decrypt the browser login data

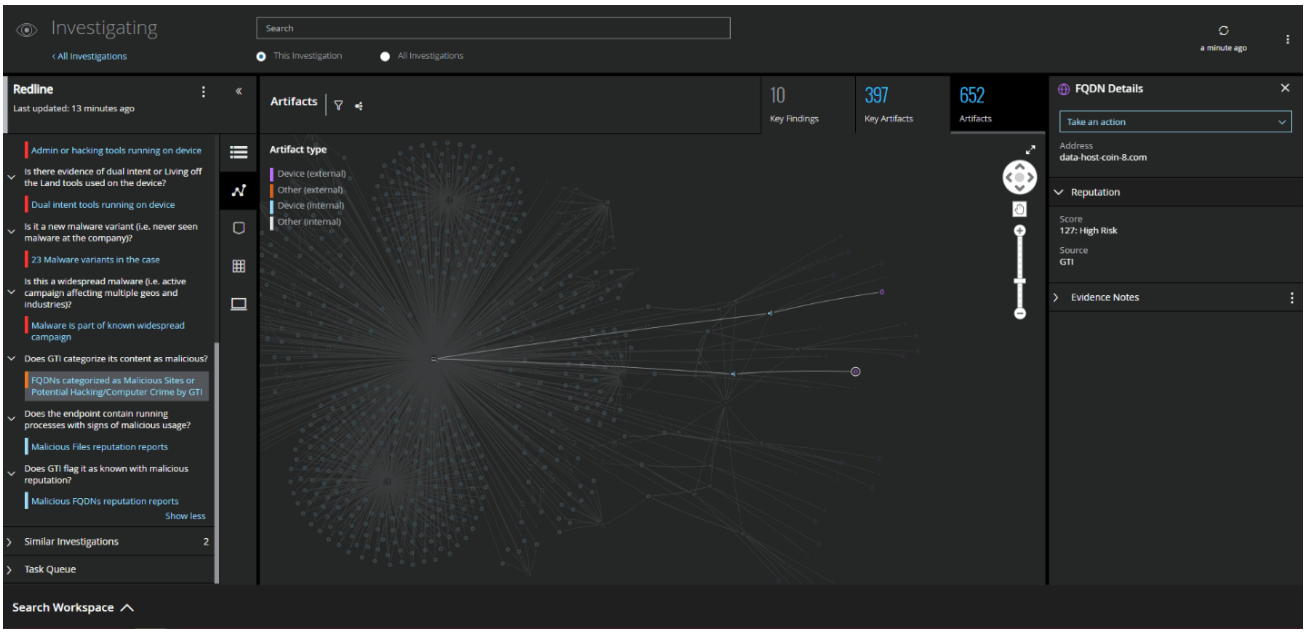


Figure 10. EDR Guided Investigation detailing observed malicious network activities

Monitoring of Cloud Account Activity Post Infection

If an infostealer infection has been detected and possible credential theft is suspected to have taken place, it is recommended to monitor for abnormal behavior within your cloud accounts even after changing passwords. MVISION Cloud/Unified Cloud Edge provide UEBA capabilities that can alert to abnormalities across your cloud environment looking at numerous Anomaly Categories to detect possible abnormal and malicious behavior. Additionally, adding impacted users to watchlists can help alert to suspicious activity from monitored users that might have their credentials compromised.

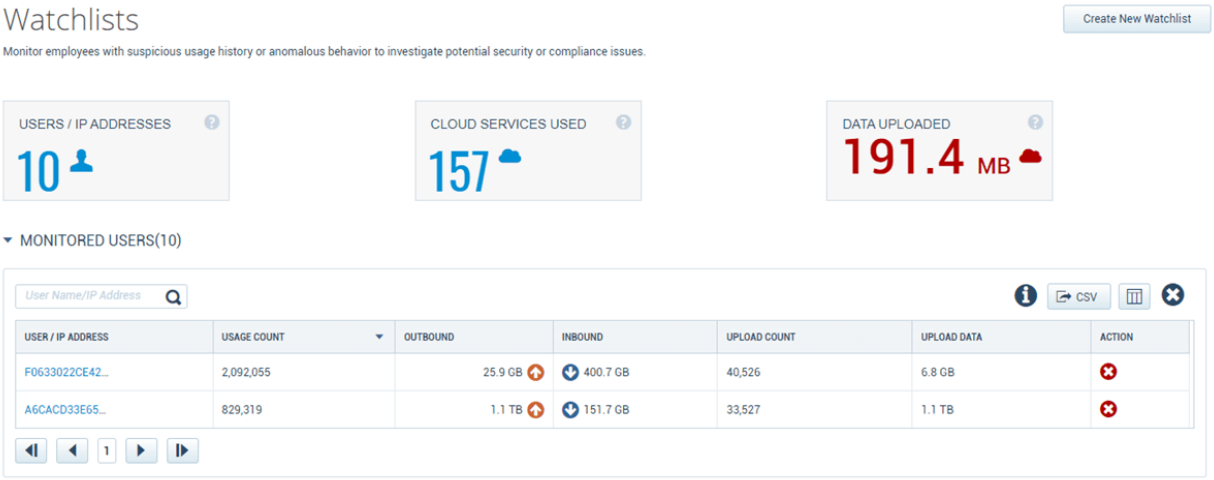


Figure 11. Watchlists can help alert to suspicious activity from monitored users

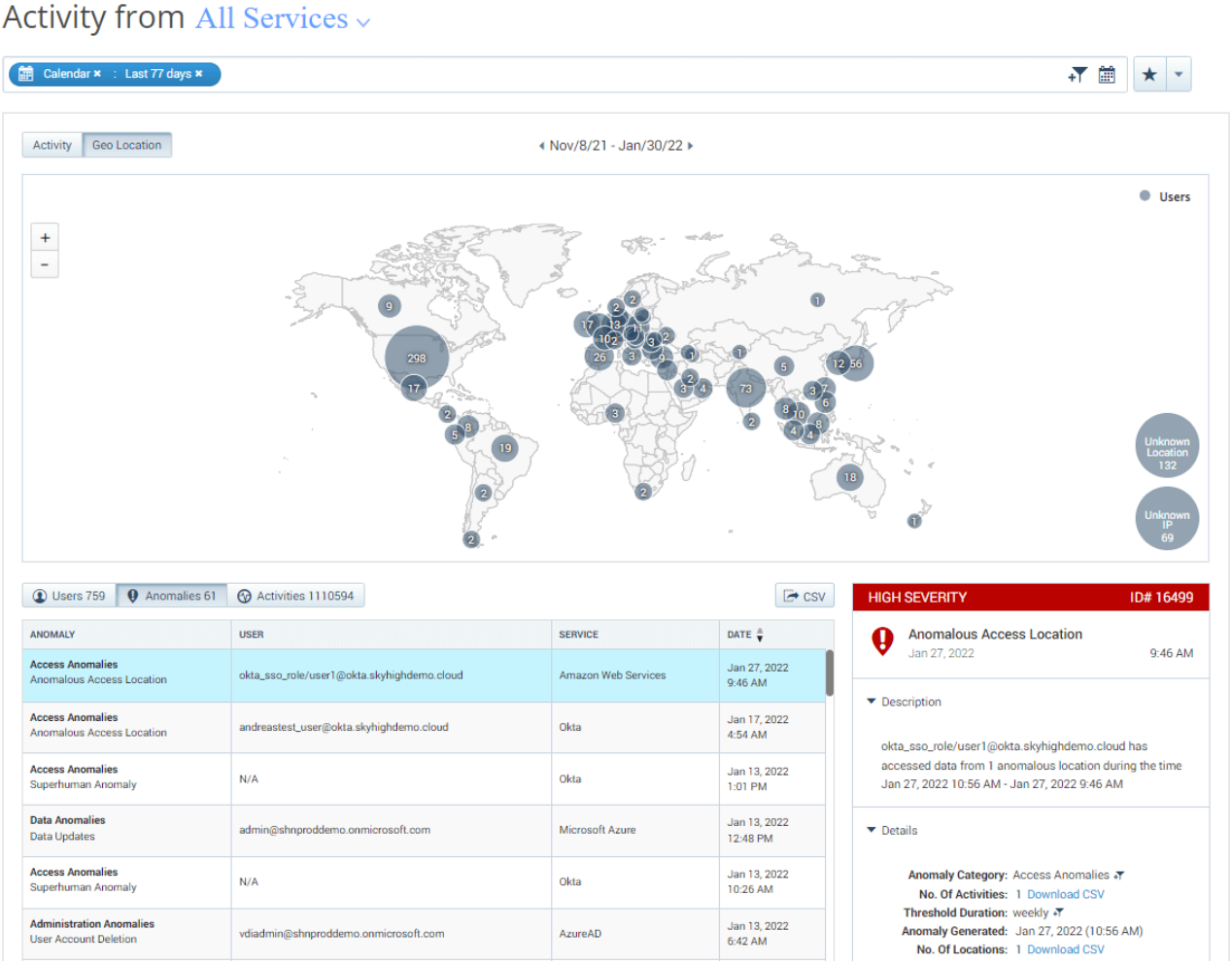


Figure 12. User Activity and Anomalies across Cloud Services

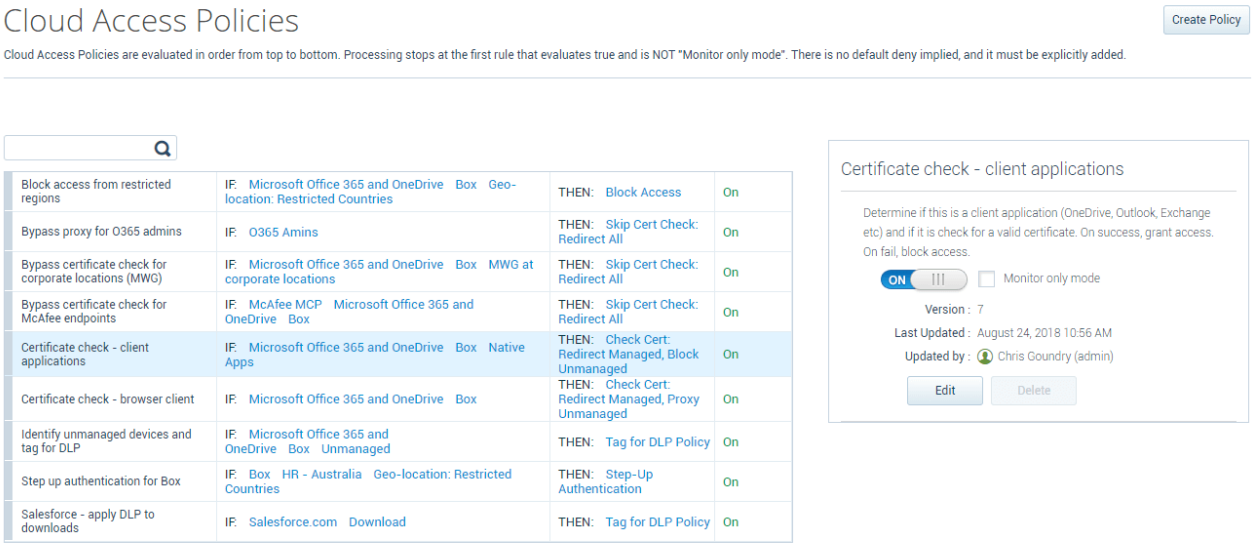


Figure 13. Cloud Access Policies to set rules and reactions for accessing your cloud environment.

Along with tracking user anomalies, an additional protection that can be utilized is setting Cloud Access Policies to block access to your cloud applications by Unmanaged Devices or connections from Restricted Countries. Setting cloud access policies can help stop the successful reuse of stolen cloud application credentials being utilized on unmanaged company devices.

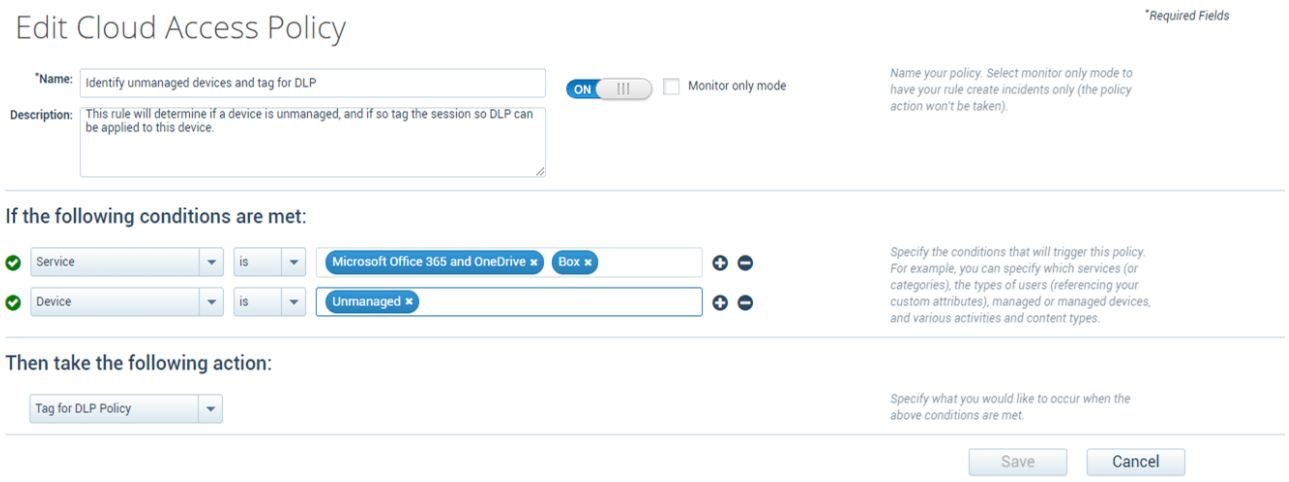


Figure 14. DLP Policy automatically applied to Unmanaged Devices accessing Cloud Services

The cloud access policy protections can also apply specific data protection policies on unmanaged devices to limit the types and sensitivity of data that is allowed to be accessed and to prevent the downloading of data based on specific cloud applications.

Trellix offers Threat Intelligence Briefings along with Cloud Security, Data Protection, and Security Operation workshops to provide customers with best practice recommendations on how to utilize their existing security controls to protect against adversarial and insider threats, please reach out if you would like to schedule a workshop with your organization.

Sign-off,

Taylor Mullins

Featured Content

PERSPECTIVES

Our CEO On Living Security

By Bryan Palma · January 19, 2022

Trellix CEO, Bryan Palma, explains the critical need for security that's always learning.

Read More

XDR

Time to Drive Change by Challenging the Challengers

By Michelle Salvado · January 19, 2022

Dynamic threats call for dynamic security – the path to resiliency lies in XDR.

Read More

THREAT LABS

2022 Threat Predictions

By Trellix · January 19, 2022

What cyber security threats should enterprises look out for in 2022?

Read More

Get the latest

We're no strangers to cybersecurity. But we are a new company.
Stay up to date as we evolve.

Please enter a valid email address.

Zero spam. Unsubscribe at any time.