

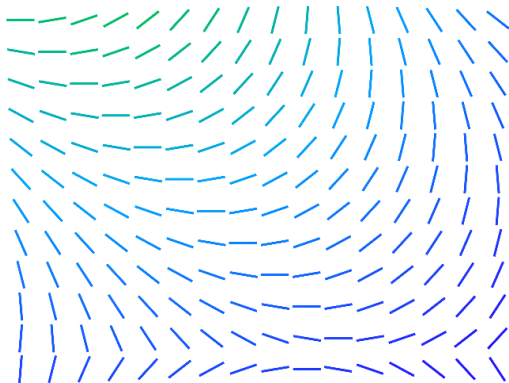
Trellix Global Defenders: Invasion of the Information Snatchers - Protecting against RedLine Infostealer

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.

Credentials from Web Browsers - T1555.003

Category: MITRE Attack Pattern

Description:

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, AppData\Local\Google\Chrome\User Data\Default\Login Data and executing a SQL query: SELECT action_url, username_value, password_value FROM Logins;. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function CryptUnprotectData, which uses the victim's cached logon credentials as the decryption key. (Citation: Microsoft CryptUnprotectData April 2018)

Adversaries have executed similar procedures for common web browsers such as Firefox, Safari, Edge, etc.(Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the Windows Credential Manager.

Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mmakkintenz July 2016)

After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials from web browsers overlap with privileged accounts (e.g. domain administrator).

Show less

Related Campaigns:

Proxyware Applications Used In Malware Campaigns, Trash Panda - Raccoon Stealer Updated With New Techniques, Discord CDN Abused To Deliver Multiple Malware Families, Evolution Of Formbook To XLoader For macOS, Operation Armor Piercer Targets India With Commercial RATs, Lazarus Targeting Security Researchers, Agent Tesla Variant Targets Korean Users, APT36 Attack Chain And Malware Arsenal, Mastodon Social Network Abused By Vidar Stealer Malware And Adware Disguised On Websites Hosting Grads, Threat Profile: TrifBot Banker, Threat Profile: SmokeLoader Malware Targets Crypto Wallets And Credentials, Lysium Group Targets Entities In Tunisia, Janeiro Banking Trojan Targets Brazil, Blogspot Used To Target South Korean Think Tanks, Threat Profile: RedLine InfoStealer, DarkIRC Exploits Oracle WebLogic Vulnerability, WayBack Campaign, Threat Profile: Agent Tesla, Open Redirector Links Lead To Credential Theft, SOURGUM Using Zero-Day Exploits to Drop DevilsTongue Malware, APT31 Modus Operandi Attack Campaign Targeting France, Fake Installers Of Popular Software Dropping Malware, RedCurl APT Group Resurfaces, MSBuild Files Used To Deliver RATs, NICKEL Threat Group Targeting Multiple Organizations, Threat Profile: Vidar Stealer, Echelon Malware Present In Mobile Chat Forums, macOS Malware Identified In 2021, STRRAT Remote Access Trojan Contains Ransomware Module, MassLogger Campaign Infections Through RAR Attachments And CHM Files, Threat Profile: UNC2447, Unauthorized Software Leads To Data Theft, Chaos Targeting Latin America, Information Stealer Masquerades As Windows Application, NPM Repository Account Used To Distribute Malware, Threat Profile: PowerShell EMPIRE, STRRAT Malware Delivered In Fake Shipping Emails, Threat Profile: Conti Ransomware, AgentTesla Campaign Targets The UAE, FiveHands Ransomware, Panda Stealer Campaign Targeting Cryptocurrency Wallets, Operation Spalax, SolarMarker Backdoor, A Look At The Digitally-Signed FiveSys Rootkit And Modules, Analyzing A Large Scale Phishing-as-a-Service Operation, Agent Tesla Variant Hijacks Bitcoin Addresses, Yanluowang Ransomware Used In Targeted Attacks, Threat Profile: DarkSide Ransomware, Threat Profile: Snake Keylogger, YouTube Creators Targeted With Cookie Theft Malware, Analysis Of The BHUNT Stealer, A Deep Dive Into Lokibot Infection Chain, Operation Layover, Multi-staged JSOUTPROX RAT Targets Banks and Finance Companies, Threat Profile: TA505 Group, Matryoshka ROKRAT Variant, Mircop Ransomware Uses Secure Email Gateway, APT29 StellarParticle Campaign, Analysis Of The AppleSeed And PebbleDash Backdoors, JavaScript Malware Threat Landscape, New FormBook Variant Found In Phishing Campaign, Threat Profile: Formbook, InsideCopy Continues To Evolve, Threat Profile: QakBot, Threat Profile: Lokibot, Commodity RATs Target Afghanistan And India, XE Group - Exposed Hacking And Card Skimming Activity, PjMICROPSIA Trojan, Fake npm Roblox API Package Installs Malware, Threat Profile: Raccoon Stealer, Threat Profile: BloodMatter Ransomware, CopperStealer Malware Steals Data, BlueStealer Malspam Campaign, Threat Profile: FRITZ Group, BloodyStealer Malware, SnatchCrypto Campaign, InfoSquid APT Infects Victims Using Browser Exploits, Malspam Campaign Distributes DanaBot Info-Stealer, APT36 Expands Arsenal, DarkSide Ransomware Operations, Telecoms Across Middle East And Asia Targeted In Espionage Campaign, Cloud Services Used To Deliver Agent Tesla Through Infected PowerPoint Files, Lokibot Delivered Using Multiple Methods, njRAT And AsyncRAT Targeting Organizations In Latin America, North Korea-Aligned TA406, BIOPASS RAT, Pirated Software Delivers Malware Droppers As A Service, Candiru Using Masquerading Domains To Drop Spyware, Earth Vetala - MuddyWater Targeting The Middle East, STRRat Malware Update, Lazarus NukeSped Backdoor Malware Show less

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.

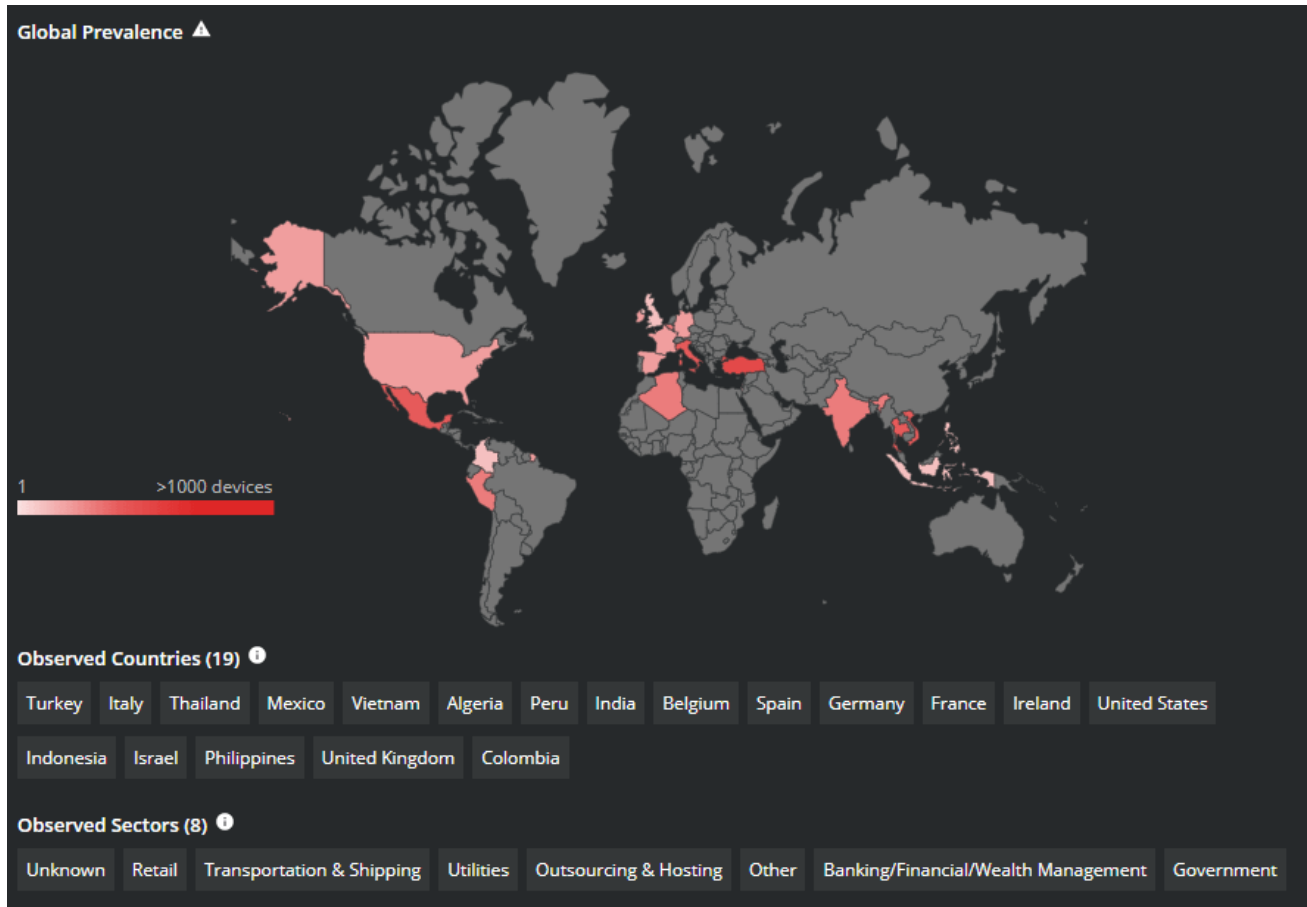


Figure 2. Global Prevalence and Observed Countries/Sectors of RedLine Infostealer.
Source: MVISION Insights

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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

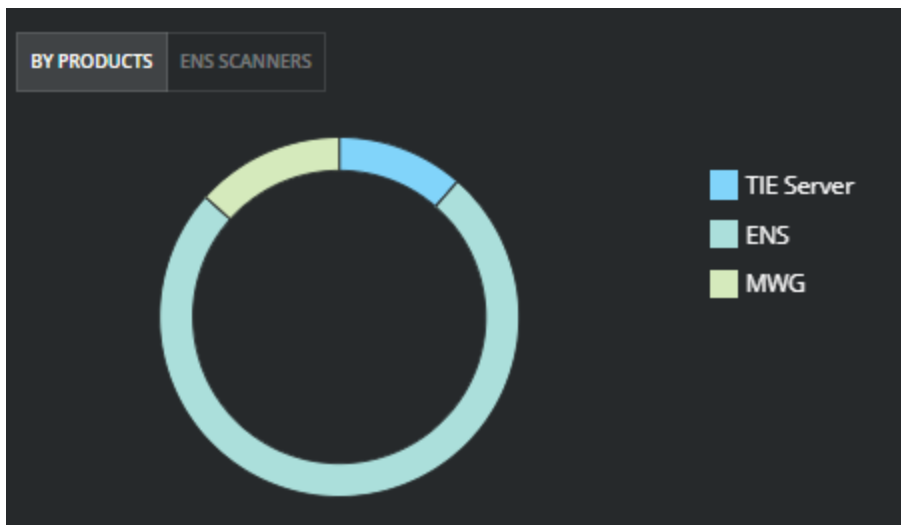


Figure 4. Trellix Products

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

Analyzed Indicators (936)							Other Associated Indicators (64)							
MD5 (431)	SHA256 (430)	IP:Port (26)	URL (49)	IP Address (0)	Domain (0)	Hostname (0)	MD5 (28)	SHA256 (28)	IP:Port (3)	URL (5)	IP Address (0)	Domain (0)	Mutex (0)	Import Hash (0)
8C643AA43C8C53287EA5158E67FA518E	2F942D6810C23303388EDE2516322C19						A4EC91781FA1839D710FA7833ECD9F29	8587E335CA1684C0E499F839F694968C						
CE3385D8FA4588CDBF8FE2A01D7949B4	96DC6028459CF268E5816B14C6814484						90038D5A3D6637FA8F647815B50071C	64C244D06798B95DA892152724E8456						
57E8590A758505612C0D91C1C381FFAB	A08729A8E9457D19ABE9C26FB148C748						2766BF2A9CD6E856A50D15AC37C2FDEB	1ED646781AD98848F3066478A98F05F						
609EC046459E4F7E2478C54034C84AE	39E680EF8E891059808CD803F4550CAC						24811857FC6AC8729EAF1877D0354117	AE3ADC5DC2F687A408C61E829780A7E1						
284505F714E202E488A8D6A611A6E061	96C2EF023FEB804E37738BB3A59E54C3						59D9E4664ADAC5EA16243C6DE7DAF22B	237C21325318B92DA050875A5F83289E						
4CD16507A31ADA721884CCA2F8E95F1	30DF4A025D2A0E0305AB014F00AC5E53						618AC02D89EA5912F6A116308CB3877F	F50F523158D8E50623D44580778C3D25						

Figure 5. Analyzed and Other Associated Indicators for RedLine Infostealer

RedLine Stealer
 Category: McAfee Tool
 Description: RedLine Stealer is available either as a standalone application or on a subscription basis on underground forums. The malware 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.
 Related Campaigns: Discord CDN Abused To Deliver Multiple Malware Families, Threat Profile: RedLine Infostealer, Legitimate Remote Admin Tools Used To Steal Cryptocurrency Through Fake Websites, MSBuild Files Used To Deliver RATs, Fake PrivacyTools Website Distributes Malware, Magnat Campaigns Target Multiple Countries With Malvertising, YouTube Creators Targeted With Cookie Theft Malware
[Show less](#)

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

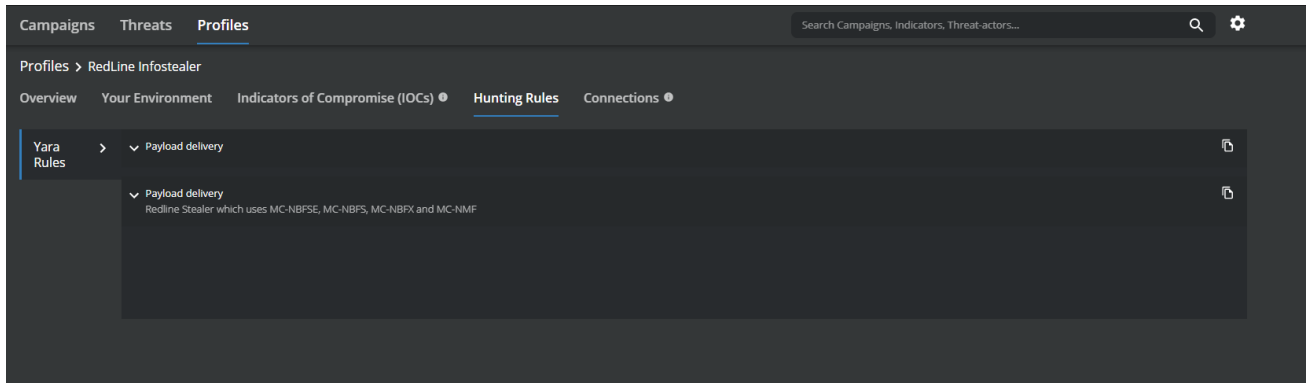


Figure 7. Yara Hunting Rules for RedLine in MVISION Insights

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.

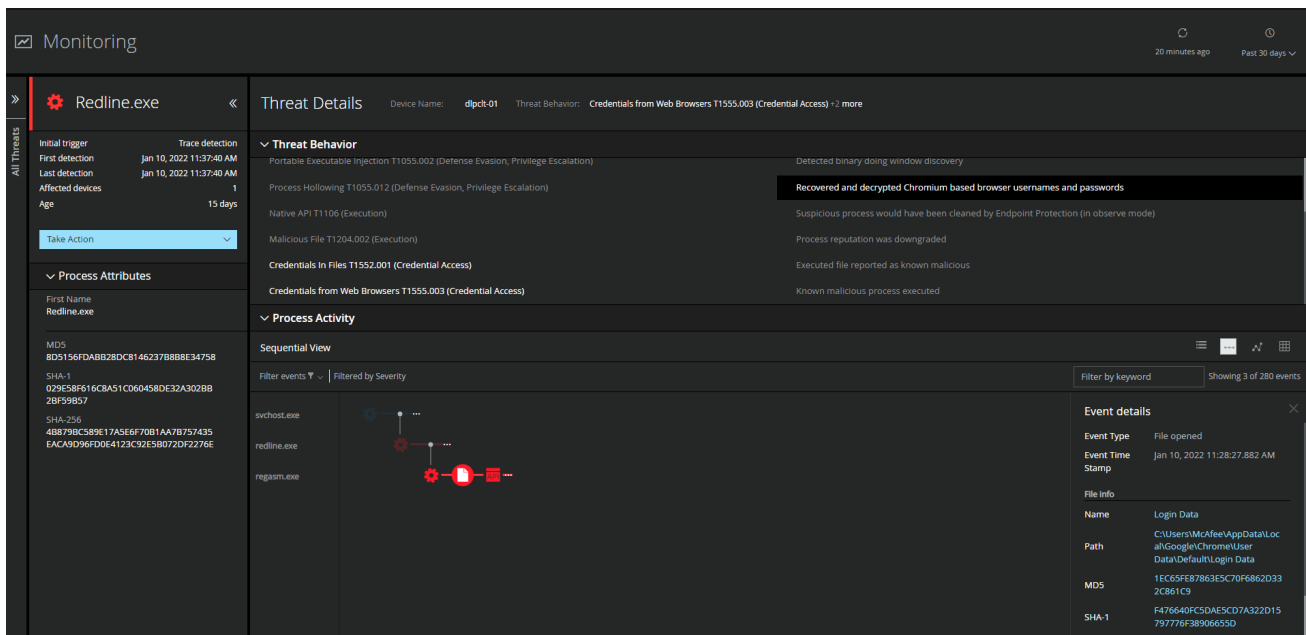


Figure 8. Recovery and decryption of browser credentials shown in MVISION EDR

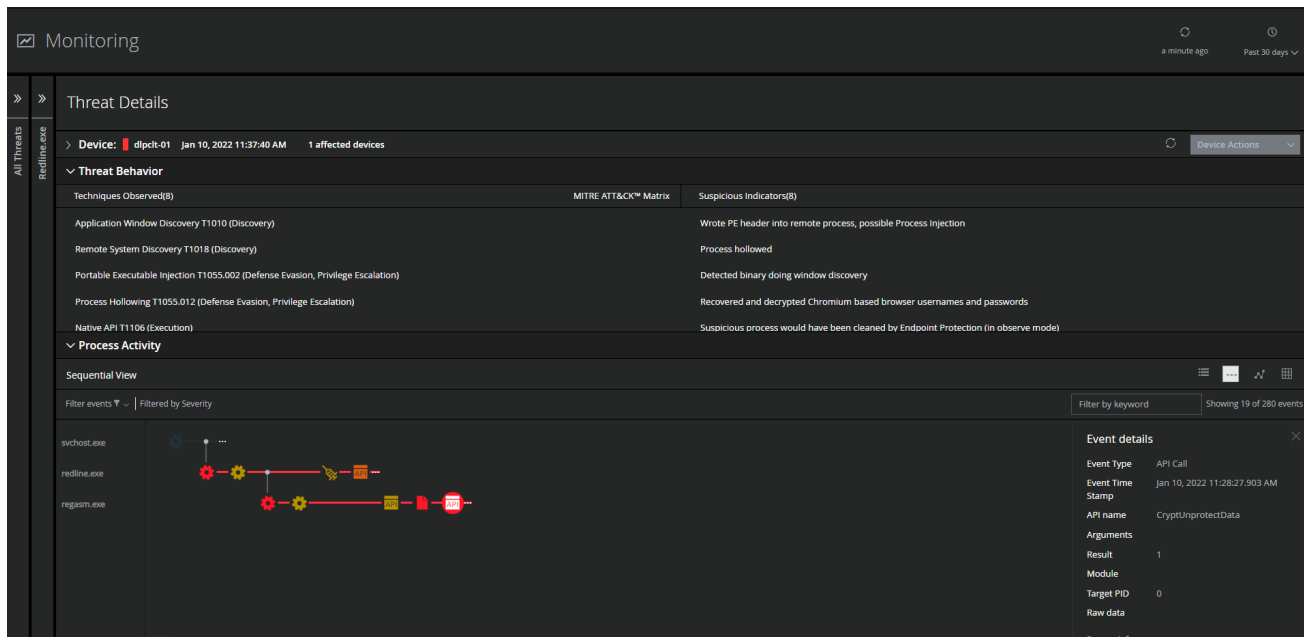


Figure 9. Accessing the CryptUnprotectData API to decrypt the browser login data

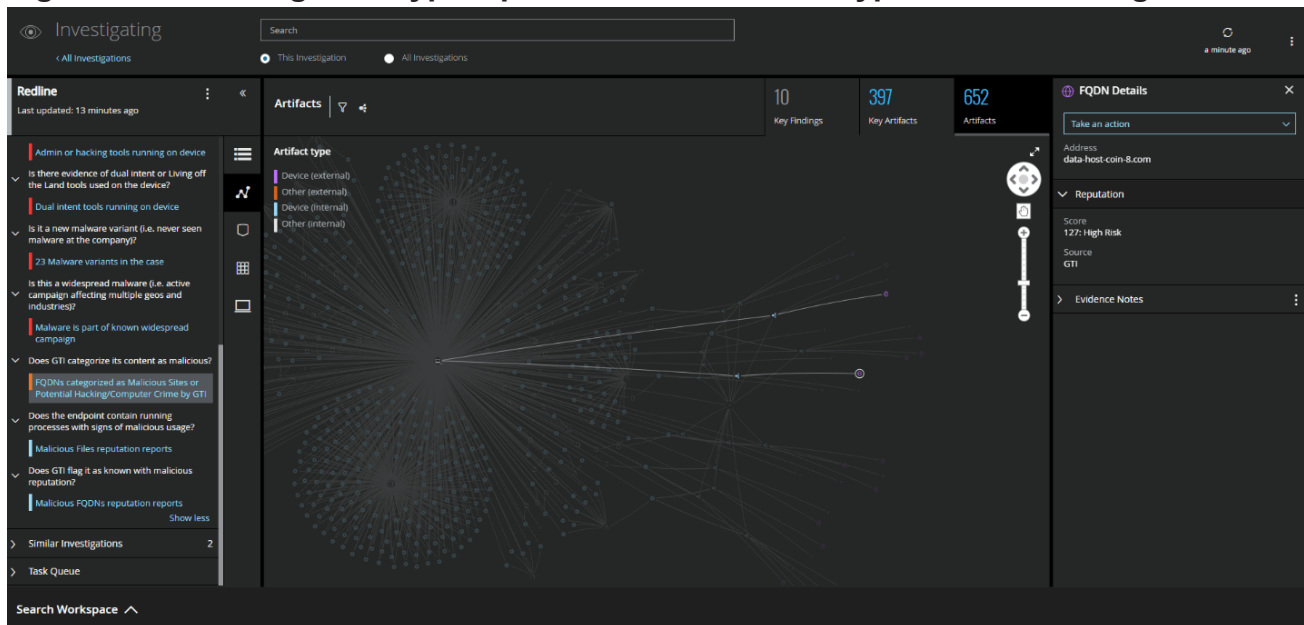


Figure 10. EDR Guided Investigation detailing observed malicious network activities

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.

Watchlists

Monitor employees with suspicious usage history or anomalous behavior to investigate potential security or compliance issues.

Create New Watchlist



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

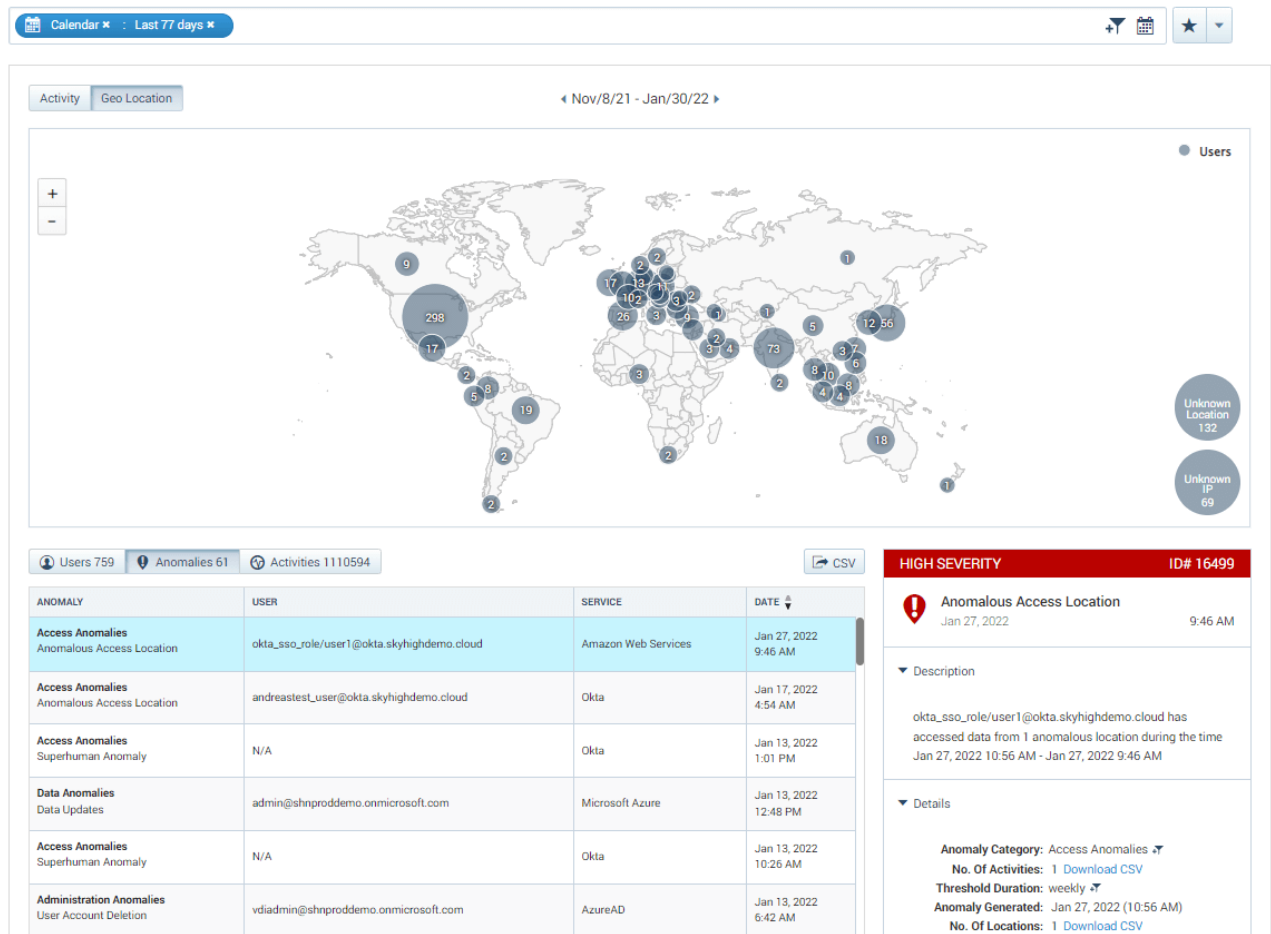


Figure 12. User Activity and Anomalies across Cloud Services

Cloud Access Policies are evaluated in order from top to bottom. Processing stops at the first rule that evaluates true and is NOT "Monitor only mode". There is no default deny implied, and it must be explicitly added.

IF	THEN	On	
Block access from restricted regions	IF: Microsoft Office 365 and OneDrive location: Restricted Countries	THEN: Block Access	On
Bypass proxy for O365 admins	IF: O365 Amins	THEN: Skip Cert Check: Redirect All	On
Bypass certificate check for corporate locations (MWG)	IF: Microsoft Office 365 and OneDrive Box MWG at corporate locations	THEN: Skip Cert Check: Redirect All	On
Bypass certificate check for McAfee endpoints	IF: McAfee MCP Microsoft Office 365 and OneDrive Box	THEN: Skip Cert Check: Redirect All	On
Certificate check - client applications	IF: Microsoft Office 365 and OneDrive Box Native Apps	THEN: Check Cert: Redirect Managed, Block Unmanaged	On
Certificate check - browser client	IF: Microsoft Office 365 and OneDrive Box	THEN: Check Cert: Redirect Managed, Proxy Unmanaged	On
Identify unmanaged devices and tag for DLP	IF: Microsoft Office 365 and OneDrive Box Unmanaged	THEN: Tag for DLP Policy	On
Step up authentication for Box	IF: Box HR - Australia Geo-location: Restricted Countries	THEN: Step-Up Authentication	On
Salesforce - apply DLP to downloads	IF: Salesforce.com Download	THEN: Tag for DLP Policy	On

Certificate check - client applications

Determine if this is a client application (OneDrive, Outlook, Exchange etc) and if it is check for a valid certificate. On success, grant access. On fail, block access.

ON Monitor only mode

Version: 7

Last Updated: August 24, 2018 10:56 AM

Updated by: Chris Goundry (admin)

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.

Edit Cloud Access Policy *Required Fields

Name: ON Monitor only mode

Description:

If the following conditions are met:

- Service is Microsoft Office 365 and OneDrive * Box *
- Device is Unmanaged *

Specify the conditions that will trigger this policy. For example, you can specify which services (or categories), the types of users (referencing your custom attributes), managed or managed devices, and various activities and content types.

Then take the following action:

Specify what you would like to occur when the above conditions are met.

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.