Threat Thursday: Arkei Infostealer Expands Reach Using SmokeLoader to Target Crypto Wallets and MFA

blogs.blackberry.com/en/2022/02/threat-thursday-arkei-infostealer

The BlackBerry Research & Intelligence Team

1. BlackBerry ThreatVector Blog
2. Threat Thursday: Arkei Infostealer Expands Reach Using SmokeLoader to Target Crypto Wallets and MFA

Summary

The criminal group behind the Arkei information stealer appears to be interested in more than just picking our pockets. While cryptocurrency remains a primary target for the malware, which has recently been tied to use of the stealthy SmokeLoader downloader, a new analysis of Arkei shows that it has now expanded its reach to collect multifactor (MFA) authentication data as well.

It's not currently clear what attackers are looking to do with this information, but a threat group that is specifically targeting this information has the capacity to impact people using MFA both at home and at work.

Arkei also downloads a variety of legitimate components, which are often hosted via compromised websites, and puts them to use for malicious purposes. Much of Arkei's flexibility relies on its configuration file, often hosted alongside these legitimate components, to receive its marching orders. Depending on what is enabled in this file, the malware will perform different activities, such as stealing saved password details, raiding auto-complete forms, and purloining saved credit card details and browser cookies.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	Medium
Risk	Medium

Technical Analysis

Attack Vector

Like many modern information-stealer families such as RedLine, Arkei is often sold and distributed as Malware-as-a-Service (MaaS), which means its initial attack vector can vary. However, over the past few weeks, this threat has been spotted utilizing the notorious downloader SmokeLoader as a method of deployment. Both Arkei and SmokeLoader have been identified using the same Indicators of Compromise (IOCs) and known-malicious URLs to conduct their malicious functionality.

Information-stealers and banking Trojans commonly use malware downloaders like SmokeLoader to get onto a victim device. Often, these types of malware rely on phishing websites or Trojanized download pages for hosting, offering seemingly benign software – cracked paid-applications or other potentially-trojanized downloads – to entice people to accept their poisoned offerings.

Components

On execution, Arkei will attempt to make several HTTP web-requests to a malicious URL. These GET HTTP Requests are designed to download known-legitimate components that the malware will then use to achieve some of its malicious functionality.

Once downloaded, Arkei will typically store the following Dynamic Link Libraries (DLLs) into the %\ProgramData\% directory for use throughout its execution process.

Name	Description
sqlite3.dll	SQLite Database Management DLL
freebl3.dll	Freebl Network Security Service Library for Mozilla
mozglue.dll	Browser Library for Mozilla
nss3.dll	Network System Service Library for Mozilla Firefox
softokn3.dll	Part of the Network Security Services for Mozilla
msvcp140.dll	Constituent file for Visual C++ for Visual Studio 2015

vcruntime140.dll Runtime library for Visual Studio (Visual C++)

Configuration

Once Arkei has obtained its components, it will make one final GET Request to the same malicious URL to obtain its configuration file, as shown in Figure 1. This file is a small Base64-encoded .PHP file.

Arkei interprets the data within this configuration file and, depending on which flags are enabled within it, will carry out different malicious activities. This strategy makes the malware extremely flexible, as it allows the threat actor to extend the threat's capabilities, or to focus on specific information to steal. For example, depending on which items in the configuration file are enabled, it determines which applications to automatically exfiltrate data from.

Figure 1: Request for Arkei's configuration

Using the CyberChef tool, the data contained within the config file can be de-obfuscated, as shown in Figure 2.

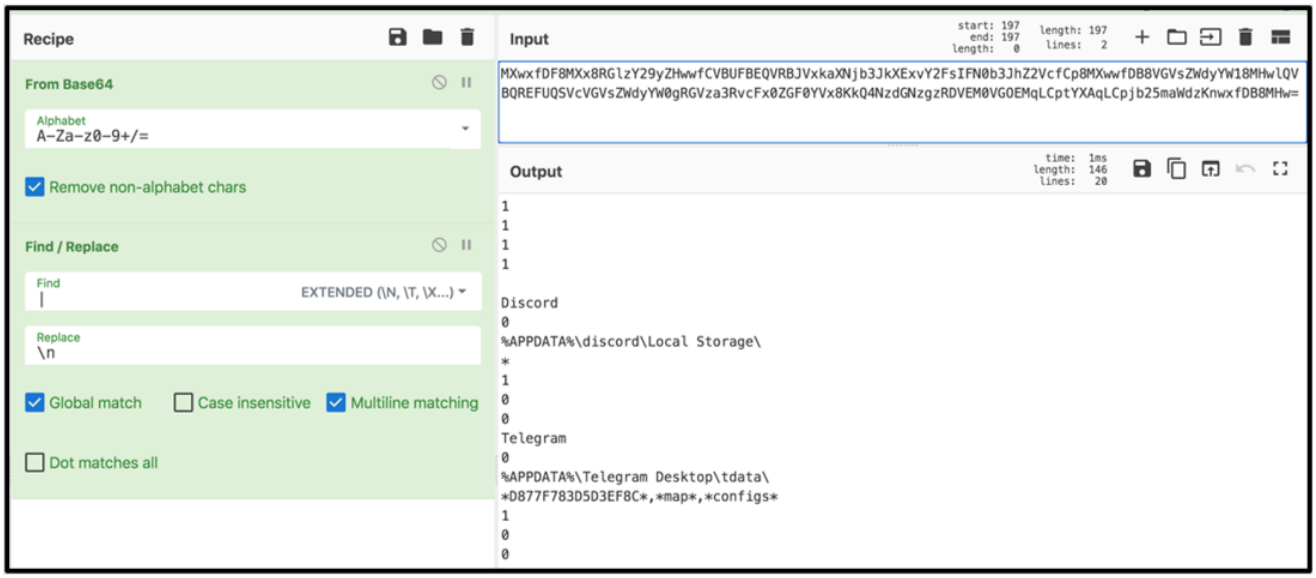

Figure 2: CyberChef output of Arkei config

Anti-Emulation and Region Checks

Arkei will check both the region of the device and the computer name. If the malware is executed with the computer name "HAL9TH," it will terminate its execution chain. This computer name check is done because it is the name given to the Windows Defender Emulator; this technique is used by malware to prevent itself from running in an emulated environment.

The malware will also exit if it finds it's being run in one of the following regions:

- Russian (Russia)
- Uzbek (Latin, Uzbekistan)
- Azerbaijani (Cyrillic, Azerbaijan)
- Kazakh (Kazakhstan)
- Belarusian (Belarus)

Browser Targets

One of the first pieces of information Arkei will attempt to steal is information about the victim's Internet browser. Arkei searches for the presence of many popular browsers, including Google Chrome™ and Firefox, before attempting to scrape various pieces of data from them to exfiltrate.

The following applications are typically targeted:

Targeted Browsers		
Google Chrome	Chromium	Microsoft Edge
Kometa	Amigo	Torch
Orbitum	Comodo Dragon	Nichrome
Maxthon5	Sputnik	Epic Privacy Browsers NEW
Vivaldi	CocCoc	Uran
QIP Surf	CentBrowser	Elements
TorBro	CryptoTab	Brave
Opera	OperaGX	OperaNeon
FireFox	SlimBrowser	PaleMoon
Waterfox	Cyberfox	BlackHawk
IceCat	KMeleon	Thunderbird

Grabber

Arkei has an internal function labelled "Grabber," which finds valuable information stored in Internet browsers. Because information is stored differently in each browser, Arkei has specific locations of a victim device where it looks for data to steal.

If enabled via the configuration file, Arkei will initially attempt to store different types of information in text files with the following file names.

Name	Description

Cookies.txt	Browser cookies
Autofill.txt	Auto-filled stored information
History.txt	Internet browser history
CC.txt	Stored credit card details
Downloads.txt	Internet download paths
Passwords.txt	Stored passwords

Browser Extensions

One of most notable functions of Arkei is its ability to steal data from Google Chrome browser extensions. For each Chrome-based extension, an “Extension ID” is given. The malware uses this information to harvest data stored within.

This Extension ID is often stored within the following folders:

- %AppData%\Local\Google\Chrome\User Data\Default\Local Extension Settings
- %AppData%\Local\Google\Chrome\User Data\Default\Sync Extension Settings
- %AppData%\Local\Google\Chrome\User Data\Default\IndexedDB\Domain Name.indexeddb.leveldb

Arkei will attempt to harvest any files located within the extension folder. For cryptocurrency holders, this malware poses a significant threat due to the large number of wallets and crypto services it targets.

However, Arkei is not solely focused on stealing cryptocurrency. Arkei appears to also target additional Chrome-based browser extensions related to two-factor and multifactor authentication (2FA/MFA) and password management, increasing its risk to both corporate and private environments. It’s not entirely clear what attackers seek to do with this information; they could be seeking to change the device used to verify 2FA access (such as someone’s cell phone) to one controlled by attackers.

Browser Extension List – Passwords and Authentication

Extension Type	Extension Name	Extension ID
Password Manager	Trezor	lmjoifkgjagghnncjkhggdhalmcnfklk
2FA	Phantom	bfnaelmomeimhlpmgjnjophhkkoljpa
2FA	Authenticator 2FA	bhghomapcdpbohigoooaddinpkbai
2FA	Authy 2FA	Gaedmjdfmmahhbjefcbgaolhhanlaolb
2FA	EOS Authenticator	oeljdldpnmdbchonielidgobddfffla l
2FA	GAuth Authenticator	llgcnhelpchnceeipipkaljkblbcpbl

Browser Extension List – Cryptocurrency Wallets

Extension Name	Extension ID	Extension Name	Extension ID
TronLink	ibnejdfjmmkpcnlpebklmnkoeoihofec	**Auro Wallet**	cnmamaachppnkjgnildpdmkaakejnhae
MetaMask	nkbihfbeogaeaoehlefnkodbefgpgknn	**Polymesh Wallet**	jojhfeoedkpkglbfimdfabpdfjaoolaf
Binance Chain Wallet	fhbohimaelbohpjbbldcngcnapndodjp	**ICONex**	flpiciilemghbmfalicajoolhkkenfel
Yoroi	ffnbelfdoeiohenkjibnmadjiehjhajb	**Nabox Wallet**	nknhiehlklippafakaeklbeglecifhad
Nifty Wallet	jbdaocneiiinmjbjlgalhcelgbejmnid	**KHC**	hcflpincpppdclinealmandijcmnkbgn
Math Wallet	afbcbjpbpfadlkmhmclhkeeodmamcflc	**Temple**	ookjlbkiijinhpmnjffcofjonbfbgaoc
Coinbase Wallet	hnfanknocfeofbddgcijnmhnfnkdnaad	**TezBox**	mnfifefkajgofkcjkemidiaecocnkjeh
Guarda	hpglfhgfnhbgpjdenjgmdgoeiappafln	**Cyano Wallet**	dkdedlpgdmmkkfjabffeganieamfklkm
EQUA Wallet	blnieiiffboillknjnepogjhkgnoapac	**Byone**	nlgbhdfgdhgbiamfdfmbikcdghidoadd
Jaxx Liberty	cjelfplplebdjjenllpjcblmjkfcffne	**OneKey**	infeboajgfhgbjpjbeppbkgnabfdkdaf
BitApp Wallet	fihkakfobkmkjojpchpfgcmhfjnmnfpi	**LeafWallet**	cihmoadaighcejopammfbmddcmdekcje
iWallet	kncchdigobghenbbaddojjnnaogfppfj	**DAppPlay**	lodccjjbdhfakaekdiahmedfbieldgik
Wombat	amkmjjmmfldd ogmhpjloimipbofnfjih	**BitClip**	ijmpgkjfkbfhoebgogflfebnmejmfbml
MEW CX	nlbmnnijcnlegkjjpcfjclmcfggfefdm	**Steem Keychain**	lkcjlnjfpbikmcmbachjpdbijejflpcm
GuildWallet	nanjmdknhkinifnkgdcggcfnhdaammmj	**Nash Extension**	onofpnbbkehpmmoabgpcpmigafmmnjhl
Saturn Wallet	nkddgncdjgjfcddamfgcmfnlhccnimig	**Hycon Lite Client**	bcopgchhojmggmffilplmbdicgaihlkp
Ronin Wallet	fnjhmkhhmkbjkkabndcnnogagogbneec	**ZilPay**	klnaejjgbibmhlephnhpmaofohgkpgkd
NeoLine	cphhlgmgameodnhkjdmkpanlelnlohao	**Coin98 Wallet**	aeachknmefphepccionboohckonoeemg
Clover Wallet	nhnkbkgjikgcigadomkphalanndcapjk	**Terra Station**	aiifbnbfobpmeekipheeijimdpnlpgpp
Liquality Wallet	kpfopkelmapcoipemfendmdcghnegimn	**Keplr**	dmkamcknogkgcdfhhbddcghachkejeap
Sollet	fhmfendgdocmcbmfikdcogofphimnkno		

Crypto Wallets

Arkei does not just stop at targeting crypto currencies via browser extensions. Many people prefer not to use third-party applications and services to store their digital currency. So, like the BlackJack component of BHunt we discussed in last week's *Threat Thursday* blog, Arkei performs a similar routine to look for specific crypto wallets stored locally on the victim's device.

Arkei will sweep through various folders looking for specific files related to cryptocurrency. This threat will search specific folders for terms like "wallet.dat," which is a file-name format used by a wide range of different currencies. If a match is found, the malware attempts to store the content of the file in a SQL database, which it will exfiltrate back to its command-and-control (C2) server.

Though Arkei has the ability to target a wide range of crypto wallets, observed samples have had dedicated functionality to target the following crypto wallets:

Crypto Wallets		
Exodus	Atomic	Bitcoin
Binance	JAXX	ElectrumLTC
Ethereum	MultiDoge	Coinomi
Electron Cash		

Exfiltration

Once Arkei has finished ransacking the victim's computer, it will attempt to bundle all the data it has obtained and exfiltrate it back to its C2. It collects this information in a folder with a name that is typically comprised of 12 random letters and numbers [0-9A-Z], as shown in Figure 3.

As Arkei obtains data, it will catalog that information before sending it back to the C2. As part of this catalog, the malware will also take a screenshot of the victim device and gather system information into a file called "system.txt."

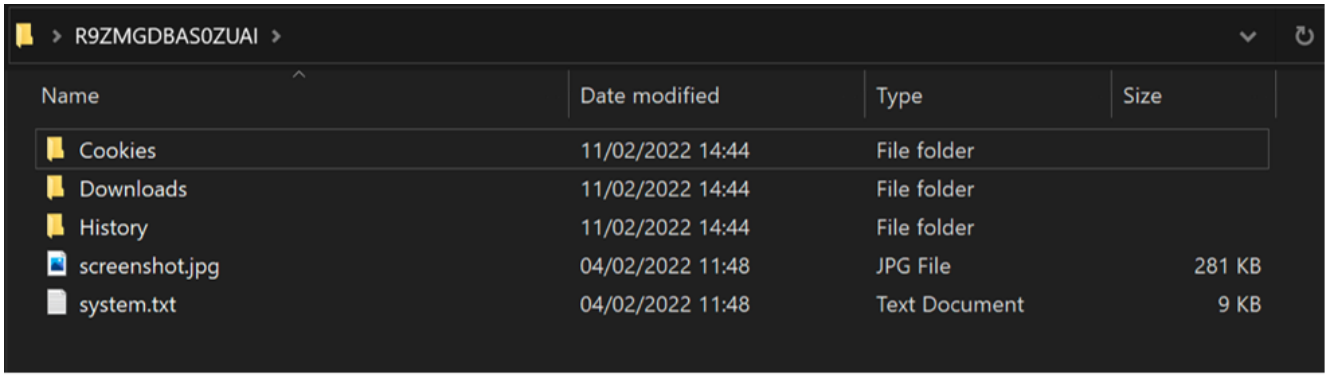

Figure 3: Example of Arkei exfiltration file

System Information

The system.txt file contains the following information about the victim's device:

System Info

IP Address	Display Resolution
Country	PC Name
Working Path	Username
Display Language	Domain Name
Keyboard Language	MachineID
Is Laptop	GUID
Processor	OS
Installed RAM	Video card

Arkei will also append a list of all installed software to this text file before exfiltrating the data. The data from Arkei is then sent to a new C2 and exfiltrated to the URL it initially reached out to.

Once Arkei has completed this step and exfiltration is successful, it will kill the process and delete itself. This is done as a clean-up mechanism to remove the malware from the device and prevent the victim from discovering they have been targeted.

Conclusions

Arkei is a flexible and stealthy information stealer that can impact both personal and corporate devices. As a MaaS, it bundles together several desirable features for attackers to use, allowing them to change infection tactics to suit their needs.

Inclusion of a configuration file allows threat actors to tailor exactly what information they choose to steal from the victim. And using legitimate files to perform nefarious functions makes Arkei more difficult for legacy anti-malware products to detect.

As more people both use cryptocurrencies and work from home, it is becoming more common to store personal financial information, as well as corporate data, on personal devices. This makes information-stealing an extremely rewarding pursuit for threat actors, who will continue pushing boundaries in their attempts to pursue bigger financial rewards.

Who is Typically Affected?

- Commercial and Professional Services
- Consumer Durables and Apparel
- Telecommunication Services
- Public Sector
- Insurance

Mitigation Tips

- Avoid downloading cracked software, or software from unknown/unverified links.
- Make sure corporate login credentials and personal passwords are not saved in your browser.
- Use two-factor authentication on a separate device, such as an authentication application installed on a mobile phone or tablet.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this blog:

```
import "pe"

	rule Mal_Win32_Arkei_Stealer_2022
	{
		meta:
			description = "Detects Arkei Stealer"
			author = "BlackBerry Threat Research"
			date = "2022-01-26"
			license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"

		strings:
			$s1 = "Copyrighz (C) 2021, fudkorta" wide ascii
			$s2 = "bomgveoci.iwa" wide ascii
	$s3 = { 4a 00 61 00 6b 00 61 00 72 00 6f 00 3d 00 48 00 65 00 77 00 61 00 6e 00 75 00 72 00 65 00 6b 00 69 00 67 00 65 00 20 00 70 00 65 00 63 00 65 00 67 00 65 00 63 00 65 00 64 00 20 00 68 00 69 00 70 00 75 00 66 00 69 00 7a 00 6f 00 77 00 6f 00 6d 00 6f 00 63 00 65 00 73 00 20 00 7a 00 65 00 6a 00 61 00 68 00 69 00 78 00 65 00 76 00 69 00 20 00 79 00 61 00 64 00 61 00 72 00 65 00 74 00 75 00 73 00 65 00 78 00}

		condition:
			// MZ header at the end of the file
			uint16(0) == 0x5a4d and

			// Must be less than
	filesize > 325KB and
			filesize < 380KB and
				// Must have import
			pe.imports("winhttp.dll") and

			// Must have the following sections in the following order
			pe.section_index(".text") == 0 and
			pe.section_index(".rdata") == 1 and
			pe.section_index(".data") == 2 and
			pe.section_index(".rsrc") == 3 and

			//All noted strings
			all of them
	}
```

Indicators of Compromise (IoCs)

C2 Addresses

- 185[.]7[.]214[.]239:80/poendxychb[.]php
- coin-file-file-19[.]com:80/tratata[.]php
- tuntutul[.]link/gate1[.]php
- googe[.]link/gate1[.]php
- 85[.]208[.]185[.]13/kyhvowljlf[.]php
- homesteadr[.]link/ggate[.]php
- 37[.]252[.]15[.]126/dhbuc2mgys[.]php
- panel[.]computer/gate[.]php

SQL Library Addresses

- hXXp[:]//homesteadr[.]link/sqlite3[.]dll
- hXXp[:]//tuntutul[.]link/sqlite3[.]dll
- hXXp[:]//coin-file-file-19[.]com/sqlite3[.]dll
- hXXp[:]//saskatche[.]link/sqlite3[.]dll
- hXXp[:]//googe[.]link/sqlite3[.]dll
- hXXp[:]//85[.]208[.]185[.]13/sqlite3[.]dll
- hXXp[:]//homesteadr[.]link/sqlite3[.]dll

- hXXp[:]//37[.]252[.]15[.]126/sqlite3[.]dll
- hXXp[:]//panel[.]computer/public/sqlite3[.]dll

Files Created on System

C:\ProgramData\sqlite3.dll

Files Modified on System

%AppData%\Local\Temp\PH4EU37Q

Registry Keys Modified

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

C2 Configurations (Base64 Encoded)

- MHwwfDF8MXx8REVTS19URVNUNXwwfCVERVNLVE9QJVx8Ki50eHR8MXwwfDB8
- MXwxfDF8MXx8RGlzY29yZHwwfCVBUFBEQVRBJVxkaXNjb3JkXExvY2FsIFN0b3JhZ2VcfCp8MXwwfDB8VGVsZWdyYW18MHwlQVBQREFUQSVcVGVsZWdyYW0gRGVza3RvcFx0ZGF0YVx8KkQ4NzdGNzgzRDVEM0VGOEMqLCptYXAqLCpjb25maWdzKnwxfDB8MHw=
- MHwxfDF8MXwxfERFU0t8OTl8JURFU0tUT1AlXFx8Ki50eHQsKi5kb2N4LCpVVEMtL SouKiwqd2FsbGV0Ki4qLCptZXRhbWFzayouKiwqcHJpdmF0ZWtleSouKiwqbGVkZ 2VyKi4qLCpjYXJ0ZWlyYSouKiwqMmZhKi4qLCpvcGVuc2VhKi4qLCpleG9kdXMqLi osKmNoaWEqLnR4dHwxfDF8MHxET0NTfDk5fCVVU0VSUFJPRklMRSVcXERvY3V tZW50c1xcfCouZG9jeCwqVVRDLS0qLiosKndhbGxldCouKiwqbWV0YW 1hc2sqLiosKnByaXZhdGVrZXkqLiosKmxlZGdlciouKiwqY2FydGVpcmEqLiosKjJmYS ouKiwqb3BlbnNlYSouKiwqZXhvZHVzKi4qLCpjaGlhKi50eHR8MXwxfDB8RE9XTnw 5OXwlVVNFUlBST0ZJTEUlXFxEb3dubG9hZHNcXHwqLnR4dCwqLmRvY3gsKlVUQ y0tKi4qLCp3YWxsZXQqLiosKm1ldGFtYXNrKi4qLCpwcml2YXRla2V5Ki4qLCpsZWR nZXIqLiosKmNhcnRlaXJhKi4qLCoyZmEqLiosKm9wZW5zZWEqLiosKmV4b2R1cyo uKiwqY2hpYSoudHh0fDF8MXwwfA==
- MXwxfDF8MXx8Q3J5cHRvfDB8JVVTRVJQUk9GSUxFJVxcfCoyZmEqLiosKnRva2Vu Ki4qLCpzZWVkKi4qLCpiaXRjb2luKi4qLCpidGMqLiosKmV0aCouKnwxfDF8MHw=
- MXwxfDF8MXx8REVTS3wxMDB8JURFU0tUT1AlXFx8Ki50eHQsKlVUQy0tKi4qLCp3 YWxsZXQqLiosKm1ldGFtYXNrKi4qfDF8MXwwfERPQ1N8MTAwfCVVU0VSUFJPRkl MRSVcXERvY3VtZW50c1xcfCoudHh0LCpVVEMtLSouKiwqd2FsbGV0Ki4qLCptZXR hbWFzayouKnwxfDF8MHxET1dOfDEwMHwlVVNFUlBST0ZJTEUlXFxEb3dubG9hZ HNcXHwqLnR4dCwqVVRDLS0qLiosKndhbGxldCouKiwqbWV0YW1hc2sqLip8MXwxfDB8
- MXwxfDF8MXx8

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back