NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

August 2018, Edition 2.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and breaches. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	**Severity**
DarkHydrus - A threat actor using Open-Source Tools for targeted Spear Phishing Attacks	● High
CactusTorch - A Fileless Threat that abuses .NET Framework to compromise systems	● High
Zero-Day vulnerabilities in Microsoft VBScript Engine are being exploited by Darkhotel APT	● Critical
A Remote Code Execution vulnerability found in Apache Struts	● Critical
Ryuk Ransomware	● Critical

ALSO INSIDE

NEWSLETTER

Latest Data Breach Highlights

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

DarkHydrus - A threat actor using Open-Source Tools for targeted Spear Phishing Attacks

Severity: High
Date: August 9, 2018

IMPACT

DarkHydrus, a threat actor found executing targeted Spear Phishing Attacks against Government and Educational institutions using Phishery (an Open-Source) Tool. This Spear Phishing Attacks involves a malicious Word document that leverages the “attachedTemplate” technique to load a template from a remote server and prompts a user to enter login credentials upon execution of malicious Word document. Such targeted spear phishing attack can cause credential breach, unauthorized access to the system/email account, data breach incident, and it can help the attacker for lateral movement when they’re already on the corporate network.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Block IP/Domain/Hashes mentioned under Indicator of Compromise section below, on security devices.
- An active subscription to Anti-Phishing service and Security Awareness training is highly recommended to identify and eliminate the weak chain in Organization’s Cyber Defence.

THREAT CAPABILITIES

- DarkHydrus, a threat actor uses Phishery (an Open-Source) Tool, for executing targeted Spear Phishing Attacks.
- They’re using “attachedTemplate” technique to load a template from a remote server, which prompts users to enter their login credentials.
- This “attachedTemplate” technique can help the attacker for lateral movement in a corporate network.

READ

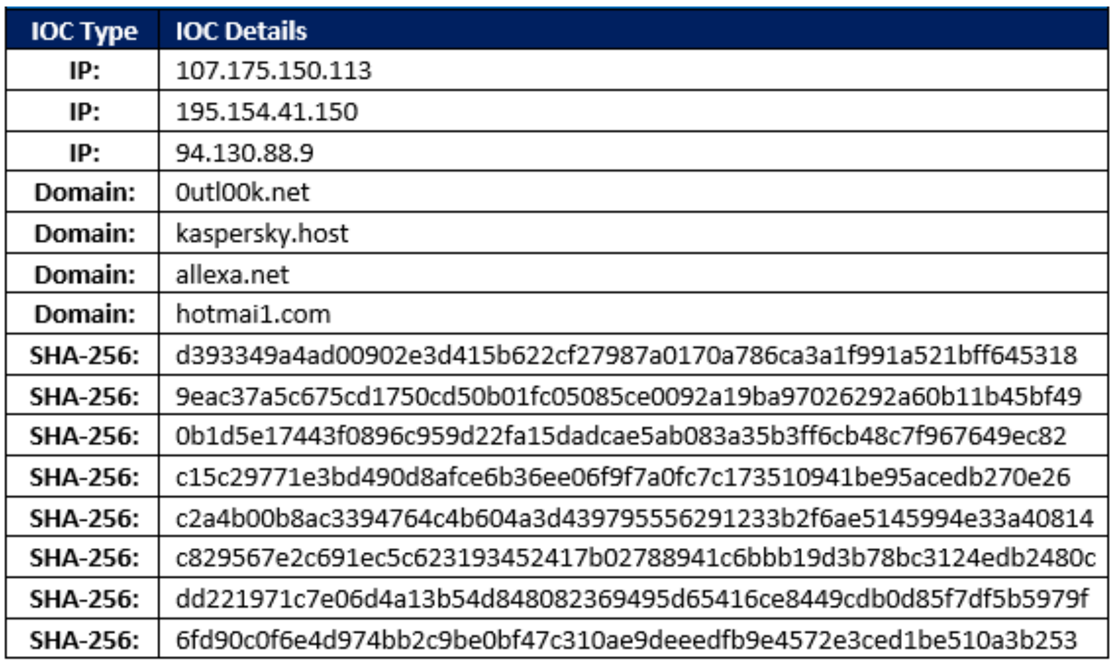
- DarkHydrus Relies on Open-Source Tools for Phishing Attacks

BLEEPINGCOMPUTER

- DarkHydrus Uses Phishery to Harvest Credentials in the Middle East

paloalto

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	107.175.150.113
IP:	195.154.41.150
IP:	94.130.88.9
Domain:	0utl00k.net
Domain:	kaspersky.host
Domain:	allexa.net
Domain:	hotmai1.com
SHA-256:	d393349a4ad00902e3d415b622cf27987a0170a786ca3a1f991a521bff645318
SHA-256:	9eac37a5c675cd1750cd50b01fc05085ce0092a19ba97026292a60b11b45bf49
SHA-256:	0b1d5e17443f0896c959d22fa15dadcae5ab083a35b3ff6cb48c7f967649ec82
SHA-256:	c15c29771e3bd490d8afce6b36ee06f9f7a0fc7c173510941be95acedb270e26
SHA-256:	c2a4b00b8ac3394764c4b604a3d439795556291233b2f6ae5145994e33a40814
SHA-256:	c829567e2c691ec5c623193452417b02788941c6bbb19d3b78bc3124edb2480c
SHA-256:	dd221971c7e06d4a13b54d848082369495d65416ce8449cdb0d85f7df5b5979f
SHA-256:	6fd90c0f6e4d974bb2c9be0bf47c310ae9deeedfb9e4572e3ced1be510a3b253

Ryuk Ransomware

Severity: Critical

Date: August 23, 2018

IMPACT

An active North Korean based campaign found distributing Ryuk Ransomware through drive-by-download exploit code hosted on compromised websites. This campaign uses combination of phishing attack and shorten URL service to trick users for visiting compromised website hosting exploit code which drops a trojan downloader and then Ryuk Ransomware during the infection chain. This pose a serious risk of data loss and disruption in business operation.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Ensure VBScript execution in Internet Explorer is Disable.
- Ensure Macros are Disabled in Microsoft Office Product.
- Ensure the least privilege accounts are using on servers across production line.
- Block IP/Domain/Hashes mentioned under Indicators of Compromise section below, on security devices.

THREAT CAPABILITIES

- Ryuk Ransomware encrypts data on computer drives and network shares using AES encryption key.
- It acts as a banking trojan and keylogger to steal credentials and Payment card data.
- It deletes shadow copy on the computer to prevent data recovery.
- It can help attacker for lateral movement and remain persistent on the compromised system or network.

READ

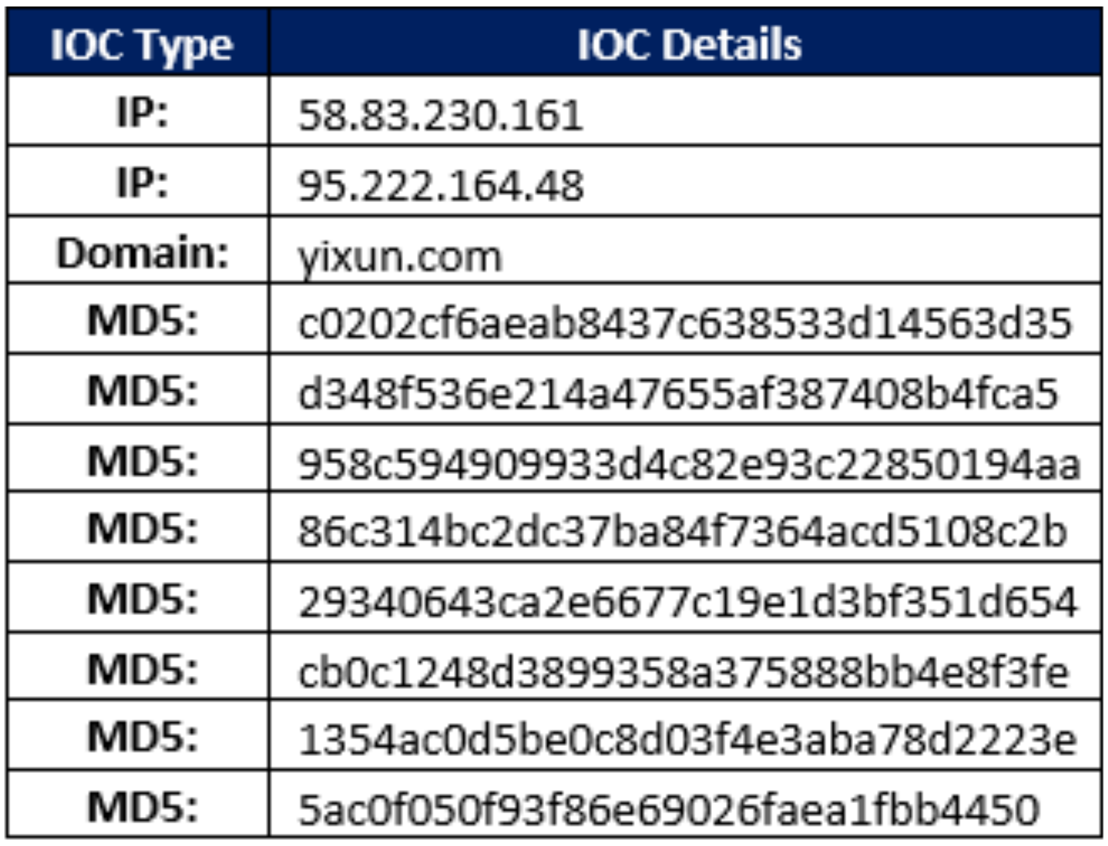
Ryuk Ransomware Crew Makes $640,000 in Recent Activity Surge

BLEEPINGCOMPUTER

Ryuk Ransomware: A Targeted Campaign Break-Down

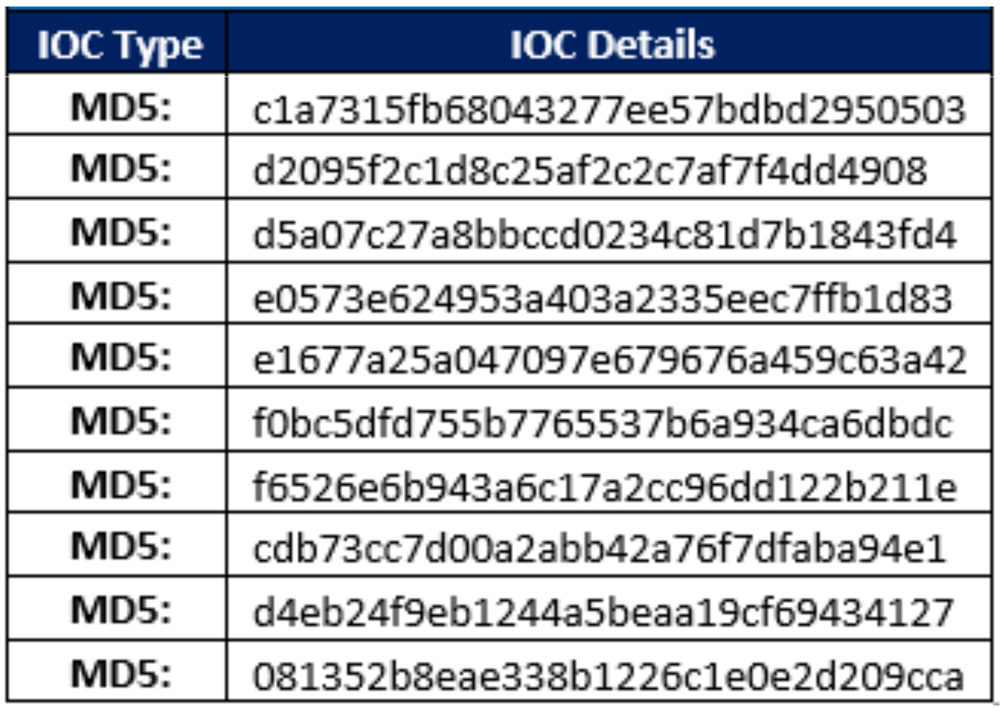
cp<r> CHECK POINT RESEARCH

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	58.83.230.161
IP:	95.222.164.48
Domain:	yixun.com
MD5:	c0202cf6aeab8437c638533d14563d35
MD5:	d348f536e214a47655af387408b4fca5
MD5:	958c594909933d4c82e93c22850194aa
MD5:	86c314bc2dc37ba84f7364acd5108c2b
MD5:	29340643ca2e6677c19e1d3bf351d654
MD5:	cb0c1248d3899358a375888bb4e8f3fe
MD5:	1354ac0d5be0c8d03f4e3aba78d2223e
MD5:	5ac0f050f93f86e69026faea1fbb4450

INDICATORS OF COMPROMISE



IOC Type	IOC Details
MD5:	c1a7315fb68043277ee57bdbd2950503
MD5:	d2095f2c1d8c25af2c2c7af7f4dd4908
MD5:	d5a07c27a8bbccd0234c81d7b1843fd4
MD5:	e0573e624953a403a2335eec7ffb1d83
MD5:	e1677a25a047097e679676a459c63a42
MD5:	f0bc5dfd755b7765537b6a934ca6dbdc
MD5:	f6526e6b943a6c17a2cc96dd122b211e
MD5:	cdb73cc7d00a2abb42a76f7dfaba94e1
MD5:	d4eb24f9eb1244a5beaa19cf69434127
MD5:	081352b8eae338b1226c1e0e2d209cca

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

CactusTorch - A Fileless Threat that abuses .NET Framework to compromise systems

Severity: High

Date: August 13, 2018

IMPACT

CactusTorch, a fileless malware that abuses .NET Framework using DotNetToJScript technique which loads and executes malicious .NET assemblies from memory without writing any part of the malicious .NET assembly on hard drive. This DotNetToJScript technique prevents Antivirus program from detecting fileless malware attack on the system. Such fileless malware remains persistent on the system, which can result in data breach incident, breach of login credentials, and unauthorized backdoor access on the system.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Block Hashes mentioned under Indicator of Compromise section below, on security devices.

THREAT CAPABILITIES

- CactusTorch, A Fileless Malware uses the DotNetToJScript technique, which uses the following COM objects:
- Text.ASCIIEncoding
- Security.Cryptography.FromBase64Transform
- IO.MemoryStream
- Runtime.Serialization.Formatters.Binary.BinaryFormatter
- Collections.ArrayList

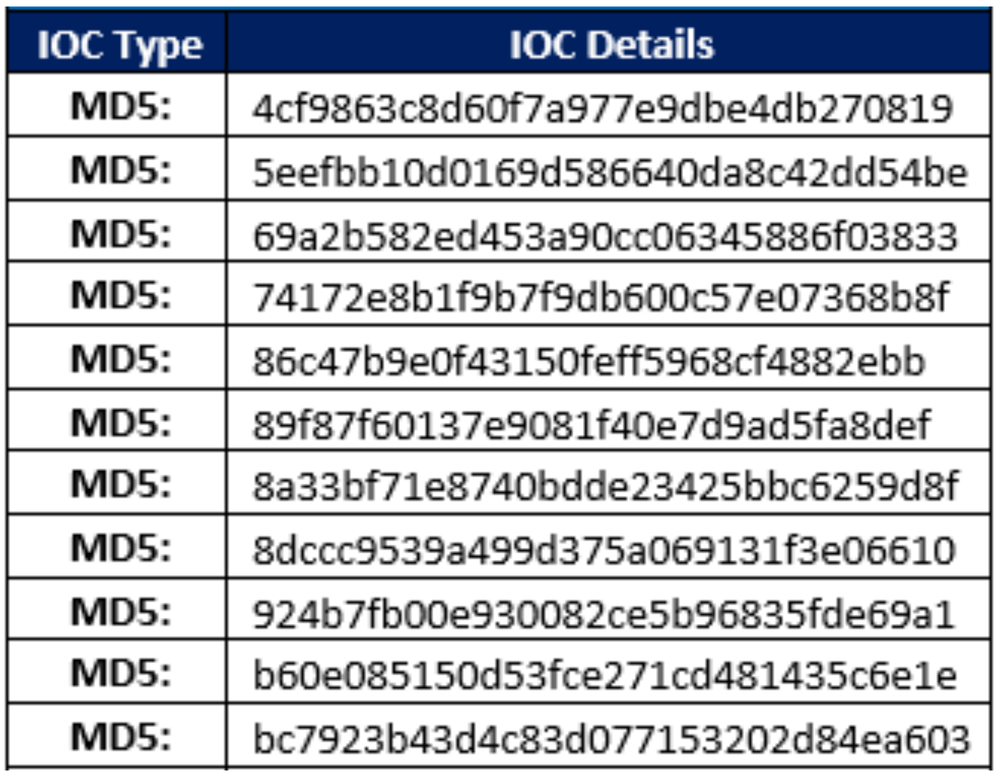
- The .NET assembly embedded in the CactusTorch script runs the following steps to execute the malicious shellcode:
- Launches a new suspended process using CreateProcessA (to host the shellcode)
- Allocates some memory with VirtualAllocEx() with an EXECUTE_READWRITE privilege
- Writes the shellcode in the target's process memory with WriteProcessMemory()
- Creates a new thread to execute the shellcode using CreateRemoteThread()

READ

- Fileless Malware CactusTorch Executes Harmful .NET Assemblies From Memory

- CactusTorch Fileless Threat Abuses .NET to Infect Victims

INDICATORS OF COMPROMISE



IOC Type	IOC Details
MD5:	4cf9863c8d60f7a977e9dbe4db270819
MD5:	5eefbb10d0169d586640da8c42dd54be
MD5:	69a2b582ed453a90cc06345886f03833
MD5:	74172e8b1f9b7f9db600c57e07368b8f
MD5:	86c47b9e0f43150feff5968cf4882ebb
MD5:	89f87f60137e9081f40e7d9ad5fa8def
MD5:	8a33bf71e8740bdde23425bbc6259d8f
MD5:	8dccc9539a499d375a069131f3e06610
MD5:	924b7fb00e930082ce5b96835fde69a1
MD5:	b60e085150d53fce271cd481435c6e1e
MD5:	bc7923b43d4c83d077153202d84ea603

NETWORK
INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Remote Code Execution vulnerability found in Apache Struts

Severity: Critical
Date: August 23, 2018

IMPACT

A Remote Code Execution vulnerability (CVE-2018-11776) in Apache Struts have affected many organizations on global scale. This vulnerability is due to insufficient validation of user provided untrusted inputs in the core of Apache Struts framework under certain configurations. On successful exploitation of this vulnerability, it would allow remote attacker to execute malicious code and take ownership of the target system running vulnerable Apache Struts instance. This is a serious security concern since this vulnerability might be used to distribute Banking Trojan or Ransomware onto the target system or network.

REMEDIATION

- K**indly upgrade A**pache Struts version 2.3 through version 2.3.34, to latest version 2**.3.35.**
- Kindly upgrade A**pache Strut**s version 2.5 through version 2.5.16, to latest version 2.5.17.
- Kindly upgrade Apache Struts version older than version 2.3, to latest version either 2.3.35 or 2.5.17.

VULNERABILITY

- Apache Struts version 2.3 through version 2.3.34 are affected,
- Apache Struts version 2.5 through version 2.5.16 are affected,
- All previous versions of Apache Struts older than version 2.3 are affected.

READ

New Apache Struts RCE Flaw Lets Hackers Take Over Web Servers
The Hacker News

Apache Struts 2 - Security Bulletin ID S2-057
Confluence

Zero-Day vulnerabilities in Microsoft VBScript Engine are being exploited by Darkhotel APT

Severity: Critical

Date: August 21, 2018

IMPACT

Total three Zero-Day vulnerabilities in Microsoft VBScript Engine are actively being exploited by Darkhotel APT group (based out of North Korea) through their mass spear-phishing campaigns targeting personnel from Defence, Government, and top private organizations on global scale. This is a serious threat since they're exploiting recently fixed zero-day vulnerability (CVE-2018-8373) in Microsoft VBScript Engine. And on successful exploitation of this vulnerability by this attacker, will lead to unauthorized access and data breach incident on later date.

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- 3. Ensure patches for Microsoft VBScript Engine Vulnerabilities (CVE-2018-8373, CVE-2018-8242, CVE-2018-8174) are applied on Windows Platforms.
- Ensure VBScript execution in Internet Explorer is Disable.
- Ensure Macros are Disabled in Microsoft Office Product.
- Block IP/Domain/Hashes mentioned under Indicators of Compromise section below, on security devices.

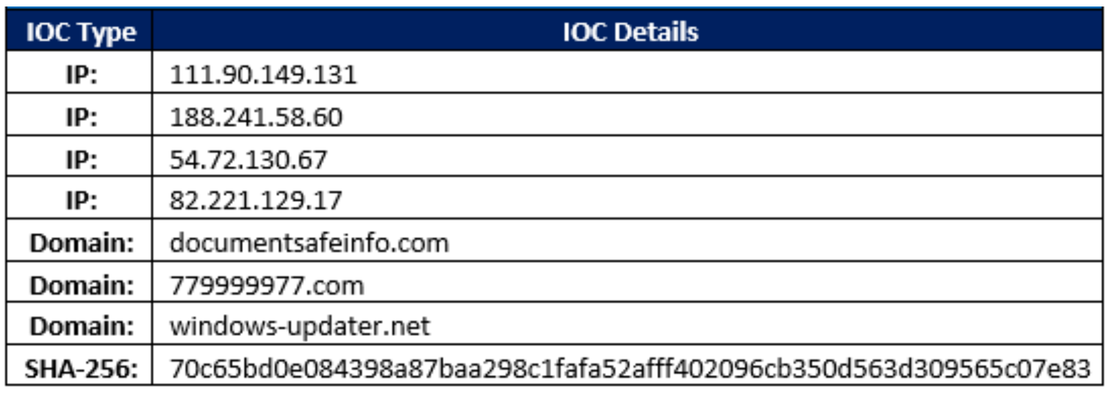
THREAT CAPABILITIES

- Darkhotel APT group (based out of North Korea) is actively exploiting three zero-day vulnerabilities (CVE-2018-8373, CVE-2018-8242, CVE-2018-8174) in Microsoft VBScript Engine.
- They're targeting through spear-phishing campaigns which either contains an obfuscated Word document or .GIF image with embedded exploit code.
- They remain undetected for a long time on compromised network or system and continue with lateral movement until they achieve their intended goals.

READ

- Zero-Day In Microsoft's VBScript Engine Used By Darkhotel APT BLEEPINGCOMPUTER
- Analysis of the CVE-2018-8373 0day vulnerability attack related to the Darkhotel gang 360

INDICATORS OF COMPROMISE



IOC Type	IOC Details
IP:	111.90.149.131
IP:	188.241.58.60
IP:	54.72.130.67
IP:	82.221.129.17
Domain:	documentsafeinfo.com
Domain:	779999977.com
Domain:	windows-updater.net
SHA-256:	70c65bd0e084398a87baa298c1fafa52afff402096cb350d563d309565c07e83

DATA BREACH HIGHLIGHTS

Credit Card Issuer TCM Bank Leaked Applicant Data for 16 Months

Aug 3, 2018

TCM Bank, a company that helps more than 750 small and community U.S. banks issue credit cards to their account holders, said a Web site misconfiguration exposed the names, addresses, dates of birth and Social Security numbers of thousands of people who applied for cards between early March 2017 and mid-July 2018.

Group-IB experts record a massive surge of user data leaks form cryptocurrency exchanges

Aug 7, 2018

Group-IB researchers have investigated user data leaks from cryptocurrency exchanges and has analyzed the nature of these incidents.

World’s Largest Web Hoster GoDaddy Exposed Massive Amount Of Sensitive Data Online

Aug 11, 2018

GoDaddy data leaked from an unsecured S3 bucket, exposed the data contains configuration information such as hostname, operating system, workload, AWS region, memory and CPU specs, and more.

2.6 billion records exposed in 2,308 disclosed data breaches in H1

Aug 18, 2018

According to a report from cyber threat intelligence firm Risk Based Security some 2.6. billion data records have been exposed to data breaches in the first half of 2018.

Personal details of 37,000 Eir customers stolen in data breach

Aug 22, 2018

The personal details of 37,000 Eir customers have been affected by the breach

Cheddar’s security breach exposes 567,000 customers to data theft

Aug 23, 2018

An estimated 567,000 Cheddar’s Scratch Kitchen customers may have had their charge-card numbers stolen during a two-month-long data security breach at the casual chain, parent company Darden Restaurants revealed yesterday.

T-Mobile Database Breach Exposes 2 Million Customers' Data

Aug 27, 2018

T-Mobile says it quickly shut down a cyberattack against a database, but the incident may have exposed personal data for 2.3 million of its 77 million customers. And it appears that the person responsible for the breach may be keen to sell the stolen data.