

Date of Publication
December 30, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

23 to 29 December 2024

Table Of Contents

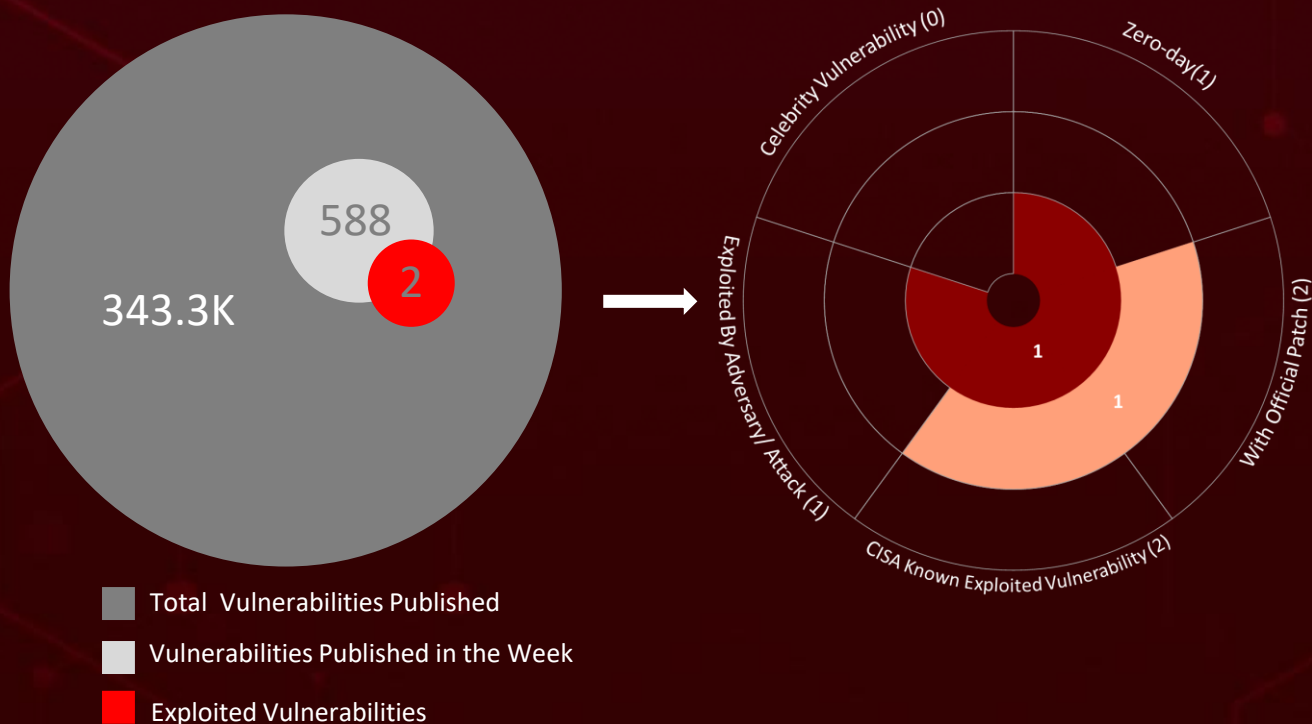
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	13
<u>Adversaries in Action</u>	15
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	23

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **eight** attacks, reported **two** vulnerabilities, and identified **two** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Additionally, **Cloud Atlas**, a cyber threat group, has deployed a new toolset using phishing emails to exploit known vulnerabilities (**CVE-2018-0802**). The attack delivers **VBShower** and **PowerShower** backdoors, enabling stealthy system infiltration while evolving to evade detection.

Furthermore, this week, a new **BellaCiao** malware variant, **BellaCPP**, rewritten in C++, enhances versatility and stealth. Linked to the **Charming Kitten APT group**, it operates as a Windows service, using DLL files and domain generation algorithms for covert communication. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

8

Attacks
Executed

2

Vulnerabilities
Exploited

2

Adversaries in
Action

- [VBShower](#)
 - [VBCloud](#)
 - [PowerShower](#)
 - [BellaCPP](#)
 - [BellaCiao](#)
 - [OtterCookie](#)
 - [PlugX](#)
 - [Rakshasa](#)
- [CVE-2018-0802](#)
 - [CVE-2024-3393](#)
- [Cloud Atlas](#)
 - [Charming Kitten](#)



Insights

A China-linked APT

targeted Southeast Asia, using advanced techniques, custom malware, and secure proxies for stealthy intelligence gathering.

Palo Alto Networks reported a high-severity DoS vulnerability (**CVE-2024-3393**) in PAN-OS, enabling attackers to force firewall reboots and disrupt operations via crafted packets.

Apache Software

Foundation revealed critical vulnerabilities in Tomcat and Traffic Control, risking remote code execution and database compromise.

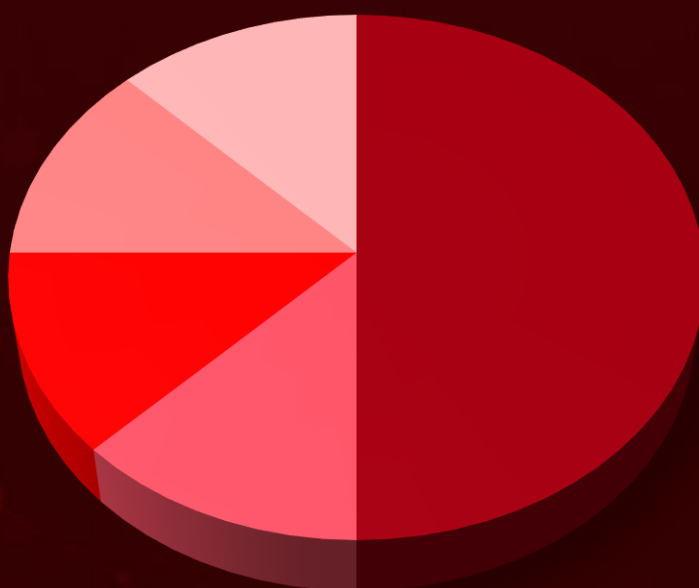
BellaCPP, a new C++ variant of BellaCiao

malware linked to Charming Kitten, uses DLL files and domain generation algorithms for stealthy communication.

Cloud Atlas, targets victims with phishing emails exploiting known vulnerabilities (**CVE-2018-0802**), deploying VBShower and PowerShower backdoors for stealthy infiltration and evasion.

OtterCookie is a malware used in the **Contagious Interview campaign**, targeting financial data with advanced techniques like remote code execution and real-time control.

Threat Distribution



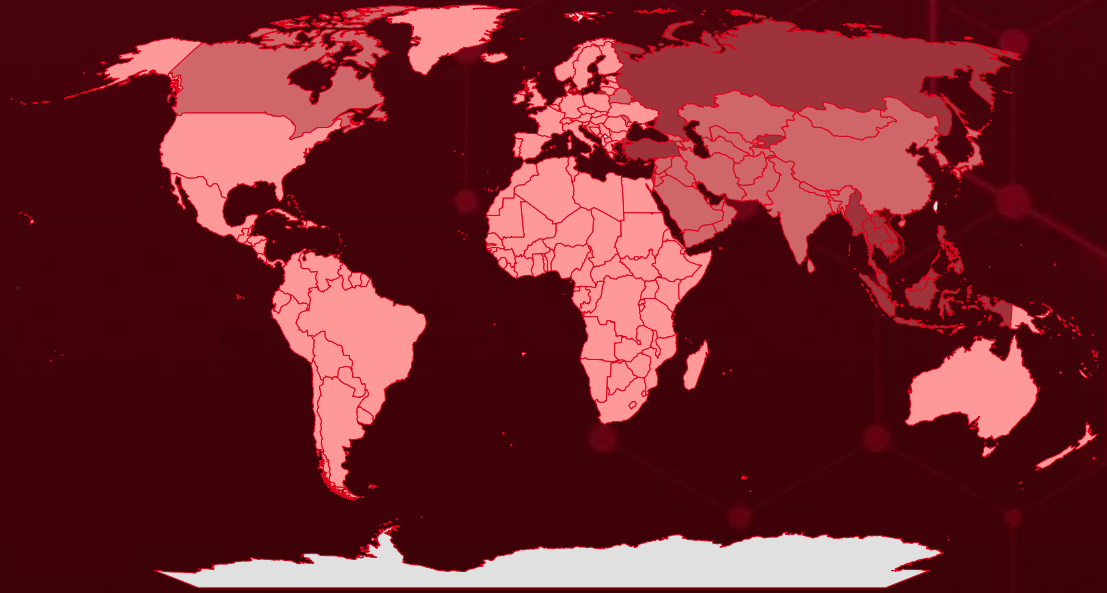
■ Backdoor ■ Trojan ■ Dropper Trojan ■ Loader ■ Hack tool



Targeted Countries

Most

Least

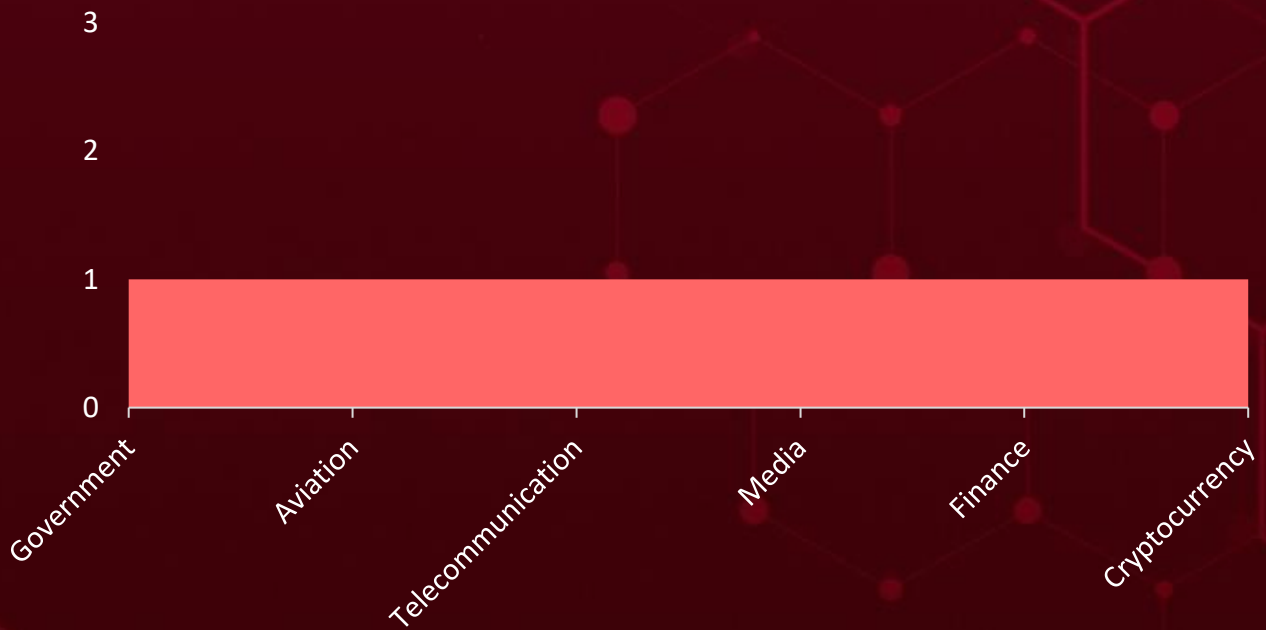


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Countries	Countries	Countries	Countries
Vietnam	Jordan	Tunisia	Senegal
Russia	Tajikistan	Samoa	Gambia
Myanmar	Kazakhstan	Central African Republic	Somalia
Brunei	Turkmenistan	El Salvador	Andorra
Thailand	Kuwait		Sudan
Cambodia	Bahrain	Spain	Germany
Philippines	Belarus	Equatorial Guinea	Denmark
Indonesia	Azerbaijan	Egypt	Ghana
Singapore		Eritrea	Uganda
Israel	Bhutan	Poland	Greece
Turkey	Canada	Estonia	Venezuela
Kyrgyzstan	Lebanon	Congo	Grenada
Laos	China	Eswatini	Nicaragua
Malaysia	Yemen	Cuba	Guatemala
Timor-Leste	Sri Lanka	Ethiopia	Senegal
Saudi Arabia	Maldives	United States	Gambia
Pakistan	Syria	Fiji	Somalia
Iran	Moldova	Nigeria	Andorra
State of Palestine	Cyprus	Finland	Sudan
Iraq	Mongolia	Papua New Guinea	Germany
Uzbekistan	Georgia	France	Denmark
Bangladesh	Armenia	Colombia	Ghana
Qatar	United Arab Emirates	Gabon	Uganda
Japan		Guatemala	Greece
South Korea	Nepal	North Macedonia	Venezuela
Oman	India	Guinea	Grenada
Afghanistan	North Korea	Palau	Nicaragua
		Guinea-Bissau	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1566.001

Spearphishing Attachment

T1566

Phishing

T1190

Exploit Public-Facing Application

T1574

Hijack Execution Flow

T1041

Exfiltration Over C2 Channel

T1588

Obtain Capabilities

T1204.002

Malicious File

T1204

User Execution

T1059.001

PowerShell

T1068

Exploitation for Privilege Escalation

T1140

Deobfuscate/Decode Files or Information

T1204.001

Malicious Link

T1547

Boot or Logon Autostart Execution

T1027

Obfuscated Files or Information

T1036

Masquerading

T1588.006

Vulnerabilities

T1083

File and Directory Discovery

T1071.001

Web Protocols

T1059.005

Visual Basic

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>VBShower</u>	<p>VBShower is a backdoor used by the Cloud Atlas APT group to facilitate cyberattacks, primarily through phishing emails. It operates by downloading and executing malicious modules, erasing traces of its presence, and communicating with command-and-control servers for further instructions.</p>	Phishing and Exploit vulnerabilities	CVE-2018-0802
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		<p>Data Theft, System compromise and Espionage</p>	Microsoft Office and Word
ASSOCIATED ACTOR			PATCH LINK
Cloud Atlas			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802
IOC TYPE	VALUE		
SHA256	<p>75b2e65bebea849d0bd0bab6599f477e6ebd0e74c2ffa960d2360db771e3f583, 1aaf4c0e8653d11adf5d36096130bb3d76384e932a476ae104eefcc0f9823d72, 97497246227ef159a1bedf6ce97c8b81eb9cc86d34f5fbd00d7fe31862b3946d, 678b30bcb599663bc7c26b4dc2ba49ee34048841c83531ca7c7f5ea2e3dee962, aa509fe7b7d6531866c3506e2c006e31926504685e685d93f658e3efb709400e</p>		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>VBCloud</u>	VBCloud is a sophisticated backdoor malware utilized by the Cloud Atlas cybercriminal group, primarily targeting cloud environments. It is delivered through phishing attacks that exploit vulnerabilities in Microsoft Office documents, allowing it to infiltrate systems and exfiltrate sensitive data to cloud storage.	Phishing and Exploit vulnerabilities	CVE-2018-0802
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			Microsoft Office and Word
ASSOCIATED ACTOR			PATCH LINK
Cloud Atlas			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802
IOC TYPE		VALUE	
SHA256	3d55f9a70a1b01432fc0432e5b43ff6c8fa4a8a7a9ed5a787d9cf2a579b12c80, 614e7290bf7974e22e7eac04c1443565ca52e626f9ce4f93f8f33468293c7556, b2769bc8a25ee6b65e58b6f2795316d67771c54b9a423bf02c3779d63b08bc4a, 9047d2116b226b35170d1e8a7c81ce0fd25822f6bdf21db39fa3fd28700420a8, 957bbadda00231d45959c3f900d6ac805afbb1cb086192ad68549f3cf0cb8ec2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PowerShower</u>	PowerShower is a PowerShell-based malware used by the Cloud Atlas APT group for reconnaissance and as a secondary payload in cyberattacks. It is designed to collect system information, exfiltrate documents, and facilitate the execution of additional malicious modules.	Phishing and Exploit vulnerabilities	CVE-2018-0802
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			Microsoft Office and Word
ASSOCIATED ACTOR			PATCH LINK
Cloud Atlas			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802
IOC TYPE		VALUE	
SHA256	7b0683a60a10657963cbcfcc9d0480e7812a3894ffb3b0d6d92bab0dc2fde0b4, c4f97cd48cc2ca11acc9e49ac18b8763752853beaabf149fe313b295fa01b2d6, a9f53fc9f350446632111b500550567a8273d0f7838d27099c41f523a0a550b9		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BellaCPP</u>	BellaCPP, a C++ variant of the BellaCiao malware family, attributed to the APT actor Charming Kitten. BellaCiao, which first appeared in April 2023, is notable for its stealthy persistence and ability to establish covert tunnels.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
Data theft		Windows	
		PATCH LINK	
		-	
TYPE			
Trojan			
ASSOCIATED ACTOR			
Charming Kitten			
IOC TYPE	VALUE		
MD5	222380fa5a0c1087559abbb6d1a5f889		
SHA1	dcdcf77dd2803b3c5a97af0851efa0aa5bbeeb		
SHA256	e4e3f09c4257269cef6cfbebc83c8a60376ce5e547080502e3e408a3f9916218		
File name	adhapl.dll		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BellaCiao</u>	BellaCiao is a sophisticated dropper trojan attributed to the Iranian APT group Charming Kitten, designed to deliver additional malicious payloads onto targeted systems. It primarily spreads through phishing emails and exploits vulnerabilities in software such as Microsoft Exchange, aiming to disable security measures like Microsoft Defender.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
Data theft		Windows	
		PATCH LINK	
		-	
TYPE			
Dropper Trojan			
ASSOCIATED ACTOR			
Charming Kitten			
IOC TYPE	VALUE		
MD5	327a1f32572b4606ae19085769042e51, 34eb579dc89e1dc0507ad646a8dce8be, b3bde532cfbb95c567c069ca5f90652c, 29362dcd6c57dde0c112e25c9706dcf, 882f2de65605dd90ee17fb65a01fe2c7		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>OtterCookie</u>	OtterCookie is a sophisticated malware used in the Contagious Interview attack campaign, primarily targeting financial data like cryptocurrency wallet keys. It employs advanced techniques such as Socket.IO for real-time communication with its command-and-control servers.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
Data theft		-	
		PATCH LINK	
		-	
TYPE			
Backdoor			
ASSOCIATED ACTOR			
North Korean Threat Actors			
IOC TYPE	VALUE		
SHA256	d19ac8533ab14d97f4150973ffa810e987dea853bb85edffb7c2fce13ad2106, 7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e, 4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79, 32257fb11cc33e794dfd0f952158a84b4475d46f531d4bee06746d15caf8236		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PlugX</u>	PlugX is a sophisticated remote access Trojan (RAT) that has been used in targeted cyberattacks since 2008, primarily linked to advanced persistent threat (APT) groups operating out of China. Known for its modular design, PlugX allows attackers to gain full control over infected systems, enabling activities such as data theft, monitoring user activity, and executing arbitrary code.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
Data theft		-	
		PATCH LINK	
		-	
TYPE			
Loader			
ASSOCIATED ACTOR			
China-linked APT			
IOC TYPE	VALUE		
SHA256	33cb9f06338a9ea17107abdbdc478071bbe097f80a835bbac462c4bb17cd0b798		




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Rakshasa</u>	Rakshasa is a Hack tool written in Go, specifically designed for multi-level proxying and internal network penetration. The tool is leveraged for advanced cyber-espionage operations, enabling attackers to bypass network defenses and establish covert communication channels within compromised environments.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Hack tool		Multi-level proxying and Data exfiltration	-
ASSOCIATED ACTOR			PATCH LINK
China-linked APT			-
IOC TYPE	VALUE		
SHA256	aa096f18e712ac0604e18d16441b672fcb393de9edf3ff4393519c48ab26a158		


The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.


Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2018-0802</u>		Microsoft Office: 2007 - 2016 Microsoft Word: 2007 - 2016	Cloud Atlas
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:a:microsoft:word:*:*:*:*:*:*	VBShower, VBCloud, PowerShower
Microsoft Office Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter, T1204 : User Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-3393</u>		PAN-OS 11.2: Versions below 11.2.3; PAN-OS 11.1: Versions below 11.1.5; PAN-OS 10.2: Versions upto 10.2.8, Versions below 10.2.10-h12 and Versions below 10.2.13-h2; PAN-OS 10.1: Versions upto 10.1.14 and Versions below 10.1.14-h8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Palo Alto Networks Denial of Service (DoS) Vulnerability		cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-754	T1498 : Network Denial of Service, T1068 : Exploitation for Privilege Escalation	https://security.paloaltonetworks.com/CVE-2024-3393

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Cloud Atlas (Inception Framework, Oxygen, ATK 116, Blue Odin, The Rocra, Clean Ursa)</u>	Russia	-	Russia, Belarus, Canada, Moldova, Israel, Kyrgyzstan, Vietnam, Turkey
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	VBShower, VBCloud, PowerShower	-	
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0006: Credential Access; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1001: Data Obfuscation; T1105: Ingress Tool Transfer; T1564.003: Hide Artifacts: Hidden Window; T1558.003: Steal or Forge Kerberos Tickets: Kerberoasting; T1087: Account Discovery; T1069.002: Permission Groups Discovery: Domain Groups; T1069.001: Permission Groups Discovery: Local Groups; T1615: Group Policy Discovery; T1201: Password Policy Discovery; T1557: : Adversary-in-the-Middle; T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1560: Archive Collected Data; T1566: Phishing; T1204.002: User Execution: Malicious File; T1059.005: Command and Scripting Interpreter: Visual Basic; T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder; T1070.004: Indicator Removal: File Deletion; T1140: Deobfuscate/Decode Files or Information; T1083: File and Directory Discovery; T1012: Query Registry; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery; T1053: Scheduled Task/Job; T1071.001: Application Layer Protocol: Web Protocols			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm, Ballistic Bobcat, CharmingCypress)</u></p>	Iran	-	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	BellaCiao, BellaCPP	Windows
TTPs			
<p>TA0005: Defense Evasion; TA0003: Persistence; TA0010: Exfiltration; TA0002: Execution; TA0011: Command and Control; T1041:Exfiltration Over C2 Channel; T1059.001: PowerShell; T1071.004: DNS; T1071: Application Layer Protocol; T1027: Obfuscated Files or Information; T1543.003: Windows Service; T1543: Create or Modify System Process; T1568.002: Domain Generation Algorithms; T1059: Command and Scripting Interpreter; T1568: Dynamic Resolution</p>			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **Cloud Atlas, Charming Kitten** and malware **VBShower, VBCloud, PowerShower, BellaCPP, BellaCiao, PlugX, Rakshasa, OtterCookie**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **two exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Cloud Atlas, Charming Kitten** and malware **VBCloud, OtterCookie** in Breach and Attack Simulation(BAS).

Threat Advisories

[Unveiling Cloud Atlas: A Novel Backdoor Expansion](#)

[New Apache Vulnerabilities Could Be a Hacker's Playground](#)

[BellaCPP: The New C++ Variant of BellaCiao Malware](#)

[Unmasking OtterCookie Malware in the Contagious Interview Campaign](#)

[PAN-OS Flaw Exploited Causing Firewall Crashes](#)

[Southeast Asia Becomes a Hotspot for China-Linked Cyber Espionage](#)

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>VBShower</u>	Domains	yandesks[.]net, yandisk[.]info, mirconnect[.]info, sber-cloud[.]info, gosportal[.]net, riamir[.]net, web-wathapp[.]com
	MD5	f45008bf1889a8655d32a0eb93b8acdd, 4b96dc735b622a94d3c74c0be9858853, 49f8ed13a8a13799a34cc999b195bf16, 3f12bf4a8d82654861b5b5993c012bfa, 3a54acd967dd104522ba7d66f4d86544, 389f6e6fd9dcc84c6e944dc387087a56, 36dd0fbd19899f0b23ade5a1de3c2fec, 2fe7e75bc599b1c68b87cf2a3e7aa51f, 242e86e658fe6ab6e4c81b68162b3001, 21585d5881cc11ed1f615fdb2d7acc11, 1bfb9cba8aa23a401925d356b2f6e7ed, 1af1f9434e4623b7046cf6360e0a520e, 184cf8660af7538cd1cd2559a10b6622, 160a65e830eb97aae6e1305019213558, 016b6a035b44c1ad10d070abcdfe2f66, aa8da99d5623fafed356a14e59acbb90
	SHA1	40bc307884ad84bc884c1f2b701e680c7ffc151, 3790e6f13b5927f3647bbf606b7d416d2aff8c4f, f6ee2629b0180e1cdc4a9603e7c783035a32d25d, 1deb1ed97dd971cedf81fe13e8dc86c3ef9d9851, cda338eb207311ff14e4f49306a972ba3759f03b, 0db2dcea98298669b2bb3cebeb9e72a66f5c84c2, d7dfda94d354ee218bf06cf232ca47858b0fc7ff,

Attack Name	TYPE	VALUE
<u>VBShower</u>	SHA1	0cd6b538b3db7c8f48b05ab456ca673bad8068dc, 93dec8070a822b63eb6b23c342e56272642d9128, cf3cf5df1206b14f7d528c5e58d7ff6ace719ed2, 54129ab2bc800982a99bda32002620ec572cc1bf, 6e94c09756b6dcba5ce9ea7e34af19e5e1777de0, c1fcf0db984815dcee8b6323f173ba4097a0fc24, ed492410a934c27b4b1cd81d2cb01190ad24faa6, ce843abe13b0178e0e12dc0719be1cb164b158e4, 7bb42d09cdae0c34592bd4bfe5125836812bd765
	SHA256	75b2e65bebea849d0bd0bab6599f477e6ebd0e74c2ffa960d2360db77 1e3f583, 1aaf4c0e8653d11adf5d36096130bb3d76384e932a476ae104eefcc0f9 823d72, 97497246227ef159a1bedf6ce97c8b81eb9cc86d34f5bd00d7fe31862 b3946d, 678b30bcb599663bc7c26b4dc2ba49ee34048841c83531ca7c7f5ea2e 3dee962, aa509fe7b7d6531866c3506e2c006e31926504685e685d93f658e3efb 709400e, f482cfe98e589bffd7eee76be5caf4040c69d4c0a8efbd10dcffaefab146 ecd4, 9ca81de013b9f9de63c80275fb662510241f97c4d1daab10ab6418a9d 0a89cb6, 69b3f4877c7e051dc87d78b8d760e34b6a60000a10ea64351b577d6c b4df8967, 26295b543d1cb6cce1337cc06c1c8a8a0ee30e9aac580710f26bff7d5c c18193, 366f6984d8aa9e78bca46788162f510bbafc10ede3d3ad4c4f53fb42be e00c55, a8bf032dea0fec1c6ef2926edcc03baedcadae149fcbcfb75925a98f290 408cf, d9c670f4b5c67958c8f8d705d66c0dbc2ab95e8edc441903e0c68de0a a7b4379, 25230923690d4ce004d0592eac057f8d4ceb942f8334fb9d28d136327 1ad3c89, 55f3f668364b3986a2c4ea528d00031c7a0ab67df54cef8affe92a2173 7f86c9, 81ab65c7b54f501a2e2962346764a6dcb587f32d5ee62b3569a4ba348 152fdb9, a5ad86dd7e6b35b45957e9b0986b5fc633a0968d2887b702e1753a46 9ec57407
<u>VBCloud</u>	Domains	webdav[.]opendrive[.]com, webdav[.]mydrive[.]ch, webdav[.]yandex[.]ru, kim[.]nl[.]tab[.]digital
	MD5	0139f32a523d453bc338a67ca45c224d, 01db58a1d0ec85adc13290a6290ad9d6, 0f37e1298e4c82098dc9318c7e65f9d2, 6fcee9878216019c8dfa887075c5e68e, d445d443ace329fb244edc3e5146313b, f3f28018fb5108b516d802a038f90bde

Attack Name	TYPE	VALUE
<u>VBCloud</u>	SHA1	3f8094e77185af6143eb7dd7ea5c51e9add7f5f1, 10c647af079537c18a1b9f94af596e65a238fcc0, 93bb6307a5dde45d92c8bdc7279d6ff63be8c541, b5b67df4643043aab9533cc1156e44532b4d26c6, 06393cf9bd61e1894dc90e2720f8cbb8778f726f, f5eae20a841a8b44350226522271cc805372dac6
	SHA256	3d55f9a70a1b01432fc0432e5b43ff6c8fa4a8a7a9ed5a787d9cf2a579 b12c80, 614e7290bf7974e22e7eac04c1443565ca52e626f9ce4f93f8f3346829 3c7556, b2769bc8a25ee6b65e58b6f2795316d67771c54b9a423bf02c3779d6 3b08bc4a, 9047d2116b226b35170d1e8a7c81ce0fd25822f6bdf21db39fa3fd287 00420a8, 957bbadda00231d45959c3f900d6ac805afbb1cb086192ad68549f3cf0 cb8ec2, 5928b83d2626a85231618d6ba169a0133530a71bb71104c948b4b30 e45aef0e0
<u>PowerShower</u>	Domains	yandisk[.]info, yandesktop[.]com, web-wathapp[.]com
	MD5	15fd46ac775a30b1963281a037a771b1, 31b01387ca60a1771349653a3c6ad8ca, 389bc3b9417d893f3324221141edea00
	SHA1	ac8ec1e17bd90430113b2c083793682e68e03311, 7c75f00f89fbd1e4977032e945c2468590c60450, 9c60869ae3697662102c8dd54bd45fbf2588d02e
	SHA256	7b0683a60a10657963cbcfcc9d0480e7812a3894ffb3b0d6d92bab0dc 2fde0b4, c4f97cd48cc2ca11acc9e49ac18b8763752853beaabf149fe313b295fa 01b2d6, a9f53fc9f350446632111b500550567a8273d0f7838d27099c41f523a0 a550b9
<u>BellaCPP</u>	MD5	222380fa5a0c1087559abbb6d1a5f889
	SHA1	dccdfc77dd2803b3c5a97af0851efa0aa5bbeeb
	SHA256	e4e3f09c4257269cef6cfbebc83c8a60376ce5e547080502e3e408a3f9 916218
	File name	adhapl.dll

Attack Name	TYPE	VALUE
<u>BellaCiao</u>	MD5	327a1f32572b4606ae19085769042e51, 34eb579dc89e1dc0507ad646a8dce8be, b3bde532cfbb95c567c069ca5f90652c, 29362dcd6c57dde0c112e25c9706dcf, 882f2de65605dd90ee17fb65a01fe2c7, 5f4284115ab9641f1532bb64b650aad6, 0fea857a35b972899e8f1f60ee58e450, 20014b80a139ed256621b9c0ac4d7076, 7f0ee078c8902f12d6d9e300dabf6aed, 63647520b36144e31fb8ad7dd10e3d21, 8096e00aa7877b863ef5a437f55c8277, 12ab1bc0989b32c55743df9b8c46af5a, 50dc5faa02227c0aefa8b54c8e5b2b0d, e760a5ce807c756451072376f88760d7, b03c67239e1e774077995bac331a8950, ba69cc9f087411995c64ca0d96da7b69, 051552b4da740a3af5bd5643b1dc239a, edfb8d26fa34436f2e92d5be1cb5901b, 3e86f6fc7ed037f3c9560cc59aa7aacc, ae4d6812f5638d95a82b3fa3d4f92861, 67677c815070ca2e3ebd57a6adb58d2e, 17a78f50e32679f228c43823faabedfd, b9956282a0fed076ed083892e498ac69, 1b41e64c60ca9dfadeb063cd822ab089
<u>OtterCookie</u>	SHA256	d19ac8533ab14d97f4150973ffa810e987dea853bb85edffb7c2fcef13ad2106, 7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e, 4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79, 32257fb11cc33e794fdfd0f952158a84b4475d46f531d4bee06746d15caf8236
	Domains	zkservice[.]cloud, w3capi[.]marketing, payloadrpc[.]com
	IPv4	45[.]159[.]248[.]55
<u>PlugX</u>	SHA256	33cb9f06338a9ea17107abddc478071bbe097f80a835bbac462c4bb17cd0b798
<u>Rakshasa</u>	SHA256	aa096f18e712ac0604e18d16441b672fcb393de9edf3ff4393519c48ab26a158

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON

December 30, 2024 • 11:45 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com