RANSOMWARE SUSCEPTIBILITY

PREPARED FOR

TATA CONSULTANCY SERVICES

REPORT GENERATED ON

2022-09-06

ABOUT

RANSOMWARE SUSCEPTIBILITY INDEX (RSI) REPORT

How to read this report?

Ransomware was the most common threat to organizations, especially operations in finance, e-commerce, and healthcare. In addition to security incidents, ransomware also had the highest impact on victims' production, reputation, and finances. In order to alert companies and their third parties to ransomware attacks, Black Kite developed the Ransomware Susceptibility Index (RSI) as a metric for customers to understand which of their vendors are susceptible to a ransomware attack. The RSI follows a process of inspecting, transforming, and modeling data with the goal of discovering the likelihood of a ransomware incident. Black Kite's data is collected from a variety of OSINT sources such as internet-wide scanners, hacker forums, the deep/dark web, and more. The data is also curated from sensors in the environment, including DBdigest, Sophos, Group IB, Coveware. By using the data and machine learning, Black Kite identified the correlation between control items in the Cyber Risk Assessment and Ransomware Entry Methods to provide these approximations.

About Black Kite

In 2016, Black Kite began its journey to redefine third-party risk management (TPRM), building the world's first security ratings service designed from a hacker's perspective. With 200+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence.

While other security ratings service (SRS) providers try to narrow the scope, our non-intrusive, powerful scans tell the full story. Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: **technical, financial and compliance.**

Sections

This assessment is provided for informational purposes only. Risk related analyses and statements in this assessment are statements of opinion of possible risks to entities as of the date they are expressed, and not statements of current or historical fact as to the security of any entity YOUR USE OF THIS ASSESSMENT IS AT YOUR OWN DISCRETION AND RISK. THE ASSESSMENT IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE BASIS TO THE MAXIMUM EXTENT PERMITTED BY LAW. BLACK KITE EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND. WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. BLACK KITE DOES NOT WARRANT THAT (i) THE ASSESSMENT WILL MEET ALL OF YOUR REQUIREMENTS: (ii) THE ASSESSMENT WILL BE UNINTERRUPTED, TIMELY SECURE OR ERROR FREE OR (iii) THAT ALL ERRORS IN THE ASSESSMENT WILL BE CORRECTED.

OVERVIEW

Tata Consultancy Services

COMPUTER SYSTEMS DESIGN AND RELATED SERVICES (NAICS: 5415)

You are **18% more** susceptible to ransomware than the industry average

Cyber Rating

C

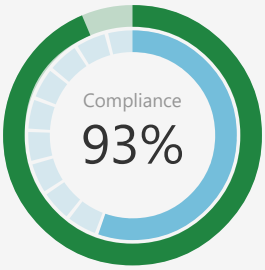
Probable Financial Impact Rating

Risk
(Annualized)

5.2K MINIMUM | **792.2K** MOST LIKELY | 5.3M MAXIMUM

The forecasted annualized loss based on the given parameters in the FAIR Model.

Compliance Rating

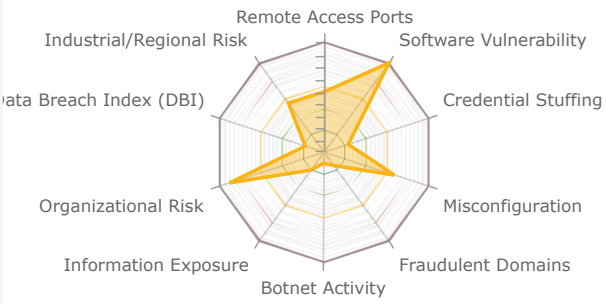


The Black Kite RSI follows a process of inspecting, transforming, and modeling collected from a variety of OSINT sources (internet wide scanners, hacker forums, the deep/dark web and more). Using the data and machine learning, the correlation between control items is identified to provide approximations.

Ransomware Indicators

Remote Access Ports:	4 findings
Software Vulnerability:	37 findings
Credential Stuffing:	66357 findings
Misconfiguration:	5 findings
Fraudulent Domains:	7 findings
Botnet Activity:	Minimal
Information Exposure:	1 finding
Organizational Risk:	0.9
Data Breach Index (DBI):	0.18
Industrial/Regional Risk:	0.55

Ransomware Radar



FINDINGS

REMOTE ACCESS PORTS (4)

Module	Asset	Detail	Severity
Network Security	ext-ultimatix.net	**Publicly available SMB Service** Failed NETSEC-010 Open smb ports were found: Ip: 159.60.11.12 Status: SMB Open	Medium CWSS: 5.7
Network Security	ultimatix.net	**Publicly available SMB Service** Failed NETSEC-010 Open smb ports were found: Ip: 34.110.238.157 Status: SMB Open	Medium CWSS: 5.7
Network Security	ext-ultimatix.net	**Publicly Visible Remote Administration Ports** Failed NETSEC-008 There are some open management ports: Ip: 159.60.11.12 Ports: 3389,22	Low CWSS: 2.5
Network Security	ultimatix.net	**Publicly Visible Remote Administration Ports** Failed NETSEC-008 There are some open management ports: Ip: 34.110.238.157 Ports: 3389,22	Low CWSS: 2.5

FINDINGS

SOFTWARE VULNERABILITY (37)

Module	Asset	Detail	Severity
Patch Management	tcs.com	**Patch Management** Failed PATCH-001 governance.tcs.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmssecurityapp.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 contacttracingapi.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 talence.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 tdaf.tcscognix.tcsapps.com (Product: apache/2.4.46) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 test.leopharmapi.tcsapps.com (Product: sap netweaver application server/7.53) In SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an unauthenticated attacker could submit a crafted HTTP server request which triggers improper shared memory buffer handling. This could allow the malicious payload to be executed and hence execute functions that could be impersonating the victim or even steal the victim's logon session.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 qa.leopharmapi.tcsapps.com (Product: sap netweaver application server/7.53) In SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an unauthenticated attacker could submit a crafted HTTP server request which triggers improper shared memory buffer handling. This could allow the malicious payload to be executed and hence execute functions that could be impersonating the victim or even steal the victim's logon session.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmsstms.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 byoa.tcsapps.com (Product: apache/2.4.52)	Critical CWSS: 9.8

Module	Asset	Detail	Severity
		Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 addregprod-az.tcsapps.com (Product: apache/2.4.52) Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	Critical CWSS: 9.8
Patch Management	tcs.com	**Patch Management** Failed PATCH-001 governance.tcs.com (Product: apache/2.4.6) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 byoa.tcsapps.com (Product: apache/2.4.52) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 addregprod-az.tcsapps.com (Product: apache/2.4.52) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 tdaf.tcscognix.tcsapps.com (Product: apache/2.4.46) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmsstms.tcsapps.com (Product: apache/2.4.6) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmssecurityapp.tcsapps.com (Product: apache/2.4.6) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 contacttracingapi.tcsapps.com (Product: apache/2.4.6) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 talence.tcsapps.com (Product: apache/2.4.6) Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	Critical CWSS: 9.8
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 54.81.68.101 (Product: nginx/1.20.0) A security issue in nginx resolver was identified, which might allow an attacker who is able to	Critical CWSS: 9.4

Module	Asset	Detail	Severity
		forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.	
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 clickfit.tcsapps.com (Product: nginx/1.14.0) A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.	Critical CWSS: 9.4
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 tag.tcsdigifleet.tcsapps.com (Product: nginx/1.16.1) A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.	Critical CWSS: 9.4
Patch Management	tcs.com	**Patch Management** Failed PATCH-001 governance.tcs.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmssecurityapp.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 contacttracingapi.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 talence.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 tdaf.tcscognix.tcsapps.com (Product: apache/2.4.46) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmsstms.tcsapps.com (Product: apache/2.4.6) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 byoa.tcsapps.com (Product: apache/2.4.52) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code	Critical CWSS: 9.1

Module	Asset	Detail	Severity
		distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	
Patch Management	tcs.com	**Patch Management** Failed PATCH-001 governance.tcs.com (Product: apache/2.4.6) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 byoa.tcsapps.com (Product: apache/2.4.52) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 addregprod-az.tcsapps.com (Product: apache/2.4.52) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 tdaf.tcscognix.tcsapps.com (Product: apache/2.4.46) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmsstms.tcsapps.com (Product: apache/2.4.6) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 etmssecurityapp.tcsapps.com (Product: apache/2.4.6) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 contacttracingapi.tcsapps.com (Product: apache/2.4.6) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 talence.tcsapps.com (Product: apache/2.4.6) If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	Critical CWSS: 9.1
Patch Management	tcsapps.com	**Patch Management** Failed PATCH-001 addregprod-az.tcsapps.com (Product: apache/2.4.52) Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	Critical CWSS: 9.1

FINDINGS

CREDENTIAL STUFFING (265)

Module	Asset	Detail	Severity
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: hub4tech_com_leak Leaked Credential Count: 16	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: livepure_com_leak Leaked Credential Count: 37	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: bajajauto_com_leak Leaked Credential Count: 23	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: smartinvestor_business-standard_com_leak Leaked Credential Count: 70	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: fitternity_com_leak Leaked Credential Count: 45	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: bookcrossing_com_leak Leaked Credential Count: 15	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: nterone_com_leak Leaked Credential Count: 87	Critical CWSS: 8
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: nsdl_co_in_leak Leaked Credential Count: 333	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: bestroofernyc_com_leak Leaked Credential Count: 91	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: linuxforums_org_leak Leaked Credential Count: 165	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: vivaair_com_leak Leaked Credential Count: 42	High CWSS: 6

Module	Asset	Detail	Severity
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: vbforums_com_leak Leaked Credential Count: 51	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: zepo_in_leak Leaked Credential Count: 260	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: releasemyad_com_leak Leaked Credential Count: 101	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: cska-emaildatapro_com_leak Leaked Credential Count: 79	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: netprospex_com_leak Leaked Credential Count: 4051	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: megacabs_com_leak Leaked Credential Count: 104	High CWSS: 6
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: proptiger_com_leak Leaked Credential Count: 856	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: disqus_com_leak Leaked Credential Count: 26	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: saleraja_com_leak Leaked Credential Count: 14	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: adecco_com_leak Leaked Credential Count: 30	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: religareonline_com_leak Leaked Credential Count: 33	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: theasianbanker_com_leak Leaked Credential Count: 19	Medium CWSS: 4

Module	Asset	Detail	Severity
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: amazepromos_com_leak Leaked Credential Count: 14	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: solidworks_com_leak Leaked Credential Count: 40	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: desidieter_com_leak Leaked Credential Count: 15	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: indiandatabases_com_leak Leaked Credential Count: 1585	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: abhinav_com_leak Leaked Credential Count: 33	Medium CWSS: 4
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: Anti Public Combo List Leaked Credential Count: 7533	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: АП191 Leaked Credential Count: 1439	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: АП214 Leaked Credential Count: 1189	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: www.thuglak.com Leaked Credential Count: 21	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: thehinduimages.com Leaked Credential Count: 29	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: www.realtimepublishers.com Leaked Credential Count: 87	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: АП125 Leaked Credential Count: 102	Low CWSS: 2

Module	Asset	Detail	Severity
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: ADOBE Leaked Credential Count: 1247	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API202 Leaked Credential Count: 28	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API182 Leaked Credential Count: 16	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: AndroidForums.com Leaked Credential Count: 26	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: MoneyGood Leaked Credential Count: 61	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API118 Leaked Credential Count: 16	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: www.commoditiescontrol.com Leaked Credential Count: 13	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API152 Leaked Credential Count: 104	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API32 Leaked Credential Count: 14	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API68 Leaked Credential Count: 29	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-003 Source: LEAKFORUMS Leaked Credential Count: 102	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: API86 Leaked Credential Count: 30	Low CWSS: 2

Module	Asset	Detail	Severity
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: AΠ162 Leaked Credential Count: 26	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-002 Source: AΠ25 Leaked Credential Count: 36	Low CWSS: 2
Credential Mgmt.	tcs.com	**Leaked Credentials** Failed LEAK-001 Source: PSBDMP Leaked Credential Count: 46	Low CWSS: 2

There are more 215 records. Please go to portal to see all of them.

FINDINGS

MISCONFIGURATION (5)

Module	Asset	Detail	Severity
Email Security	tcsion.com	**DMARC Record** Warning SMTP-003 Please check DMARC policy: v=dmarc1; p=none; pct=100; rua=mailto:dmarc-reports@mail.tcsion.com	Medium CWSS: 4.7
Email Security	tcsprocesscloud.com	**SPF Record** Failed SMTP-002 SPF Record not found.	Medium CWSS: 4.7
Email Security	tcsprocesscloud.com	**DMARC Record** Failed SMTP-003 DMARC Record Not Found	Medium CWSS: 4.7
Email Security	tcsion.com	**DKIM Record** Warning SMTP-004 DKIM Record Not Found	Low CWSS: 3
Email Security	tcsprocesscloud.com	**DKIM Record** Warning SMTP-004 DKIM Record Not Found	Low CWSS: 3

FINDINGS

FRAUDULENT DOMAINS (7)

Module	Asset	Detail	Severity
Fraudulent Domains	tcsapps.com	**Fraudulent Domain** Failed FRADOM-001 tcdapps.com (%84)	High CWSS: 6
Fraudulent Domains	ext-ultimatix.net	**Fraudulent Domain** Failed FRADOM-001 extultimatix.net (%90)	High CWSS: 6
Fraudulent Domains	ultimatix.net	**Fraudulent Domain** Failed FRADOM-001 ultimtaix.net (%79)	High CWSS: 6
Fraudulent Domains	ultimatix.net	**Fraudulent Domain** Failed FRADOM-001 uitimatix.net (%88)	High CWSS: 6
Fraudulent Domains	ultimatix.net	**Fraudulent Domain** Failed FRADOM-001 wwwultimatix.net (%82)	High CWSS: 6
Fraudulent Domains	ultimatix.net	**Fraudulent Domain** Failed FRADOM-001 ultimatis.net (%88)	Medium CWSS: 4
Fraudulent Domains	tcsion.com	**Fraudulent Domain** Failed FRADOM-001 tcsionw.com (%88)	Low CWSS: 2

FINDINGS

INFORMATION EXPOSURE (I)

Module	Asset	Detail	Severity
Information Disclosure	tcs.com	**Data Breach Index** Failed INFDIS-010 Breach Dates: - 2016-10-10, (published_date) Other Sources: - https://www.ehackingnews.com/2019/06/china-hacked-tcs-7-other-major-firms.html CompanyName: tcs.com Desc: The HackNotice security research team discovered a data leak file associated with this domain. According to the hacker, this domain was allegedly hacked. If there are no other sources attached to this hack notice, then we don't have an official disclosure of a data incident, so this hack is only implied. SourceType: leakreport TotalRec: 7327 Domain: tcs.com Hacker: Team YHI BreachDate : 2016-10-10 Maintainer : Hacknotice MaintainerUrl : https://www.hacknotice.com	Low CWSS: 2

FAQ

FREQUENTLY ASKED QUESTIONS

What types of data does Black Kite collect to inform its cybersecurity ratings?

Black Kite uses open-source intelligence (OSINT) techniques to collect data from 400+ OSINT resources via a span of internet-wide scanners. As an authorized IP zone transferer with one of the largest IP & Domain Whois databases, we hold more than one billion historical items. The asset-discovery engine detects all company-related IP address ranges and domain names.

How does the Black Kite provide transparency to rated companies about how their rating was derived?

Black Kite utilizes the MITRE Cyber Threat Susceptibility Assessment (CTSA) as a foundational scoring matrix to map every vendor in the system. Black Kite uses additional standard scoring models like the Common Weakness Risk Analysis Framework (CWRAF), Common Weakness Scoring System (CWSS), Common Vulnerability Scoring System (CVSS), and Factor Analysis of Information Risk (FAIR). Mining data from other sources enables customers to eliminate false positives and audit results. See https://blackkitetech.com/black-kites-methodology for more information

How many suppliers are currently in your portal?

We collect data on all companies which are added to our data lake. Our data lake comprises information on over 34 million companies which allows our customers to add and start monitoring any company within a few hours. If the company is previously monitored by another customer, the company's data will be available in minutes.

Is any of the data proactively provided by the suppliers?

No. Suppliers can share their policies, such as their information security policy, or questionnaires if necessary.

Do you get permission, acknowledgment, etc. from the companies you monitor?

No, all information is publicly available and curated from open sources.

What are your Data Sources?

Black Kite collects data from 400+ resources. There are several categories that Black Kite collects data from:

- Threat Intelligence
- Exploits & Advisories
- Dark Web
- Archives
- Forums / Blogs / IRC
- Search Engines
- Business Records
- Public Records
- Social Networks
- Internet Wide scanners

GLOSSARY

- **Botnet:** A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- **Brute Force:** A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.
- **Cryptanalysis:** The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the ciphertext to plaintext without knowing the key.
- **Denial of Service:** The prevention of authorized access to a system resource or the delaying of system operations and functions.
- **Domain Name:** A domain name locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.
- **Domain Name System (DNS):** The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.
- **Encryption:** Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
- **Fingerprinting:** Sending strange packets to a system in order to gauge how it responds to determine the operating system.
- **Hardening:** Hardening is the process of identifying and fixing vulnerabilities on a system.
- **Internet Protocol (IP):** The method or protocol by which data is sent from one computer to another on the Internet.
- **IP Address:** A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.
- **Network Mapping:** To compile an electronic inventory of the systems and the services on your network.
- **Patching:** Patching is the process of updating software to a different version.
- **Penetration Testing:** Penetration testing is used to test the external perimeter security of a network or facility.
- **Phishing:** The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.
- **Plaintext:** Ordinary readable text before being encrypted into ciphertext or after being decrypted.
- **Port:** A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.
- **Port Scan:** A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
- **Ransomware:** A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.
- **Reverse Lookup:** Find out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.
- **Secure Sockets Layer (SSL):** A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.
- **TCP Fingerprinting:** TCP fingerprinting is the use of odd packet header combinations to determine a remote operating system.
- **WHOIS:** An IP for finding information about resources on networks.

- END OF REPORT -