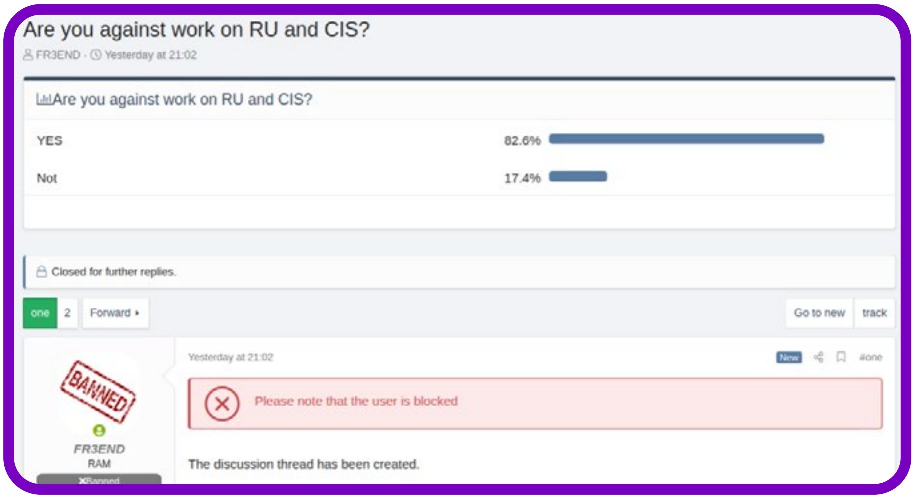
# Global Incident Report:

## Threat Actors Divide Along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums

## Scenario

By and large, criminal underground forums—particularly ones associated with ransomware—on which the most-skilled and respected cybercrime actors operate are Russian-language forums. These forums previously employed a strict, "no work in CIS" policy, meaning that these forums prohibited membership by those involved in attacks targeting entities operating within the Commonwealth of Independent States (CIS) region. However, following Russia's invasion of Ukraine on February 24, 2022, threat actors on the criminal underground are increasingly dividing themselves, sympathizing with either Russia or Ukraine, which is sending ripples through the Russian-language underground and beyond. A recent survey ***(Exhibit 1)*** by a member of one such forum examined how many actors were willing to target Russian entities; as of March 7, 2022, 83% said they were not, but a surprisingly high 17% indicated they were. Given the historical absence of CIS targeting and the fact that this forum is pro-Russia this indicates an unprecedented ideological divide.



Are you against work on RU and CIS?

FR3END · Yesterday at 21:02

Are you against work on RU and CIS?

YES 82.6%

Not 17.4%

Closed for further replies.

Yesterday at 21:02

Please note that the user is blocked

FR3END

RAM

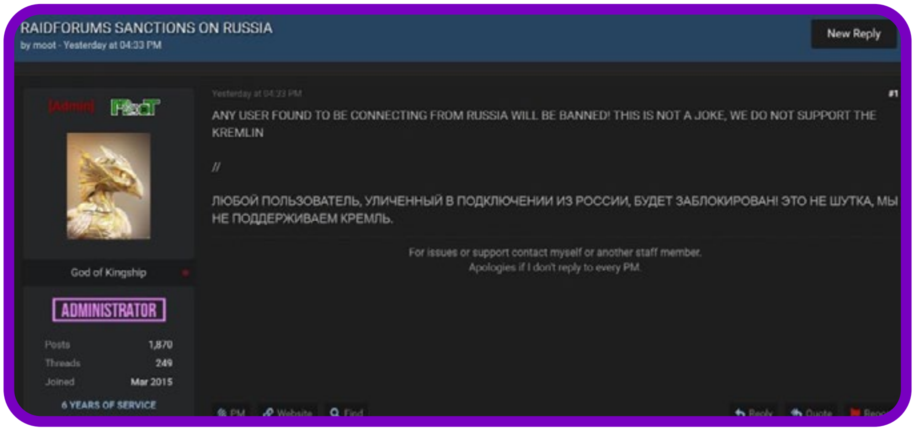
The discussion thread has been created.

**Exhibit 1:** Poll on pro-Russian activity sentiments on the XSS forum *(March 3, 2022).*

# Evaluation

## A Divided Criminal Underground

For the first time, in the more than 10 years that Accenture's Cyber Threat Intelligence (ACTI) team has been tracking Dark web activity, we're seeing previously coexisting, financially motivated threat actors divided along ideological factions. These actors, who previously acted opportunistically, with financial motivations and a global (minus CIS) outlook are now following a highly targeted attack pattern. Pro-Ukrainian actors are refusing to sell, buy, or collaborate with Russian-aligned actors ***(Exhibit 2)*** and are increasingly attempting to target Russian entities in support of Ukraine. However, pro-Russian actors are increasingly aligning with hacktivist-like activity targeting "enemies of Russia," especially Western entities due to their claims of Western warmongering. This change in targeting and motivation has had several far-reaching consequences for underground actors and the threat they pose.



RAIDFORUMS SANCTIONS ON RUSSIA
by moot - Yesterday at 04:33 PM

Yesterday at 04:33 PM

ANY USER FOUND TO BE CONNECTING FROM RUSSIA WILL BE BANNED! THIS IS NOT A JOKE, WE DO NOT SUPPORT THE KREMLIN

//

ЛЮБОЙ ПОЛЬЗОВАТЕЛЬ, УЛИЧЕННЫЙ В ПОДКЛЮЧЕНИИ ИЗ РОССИИ, БУДЕТ ЗАБЛОКИРОВАН! ЭТО НЕ ШУТКА, МЫ НЕ ПОДДЕРЖИВАЕМ КРЕМЛЬ.

For issues or support contact myself or another staff member.
Apologies if I don't reply to every PM.

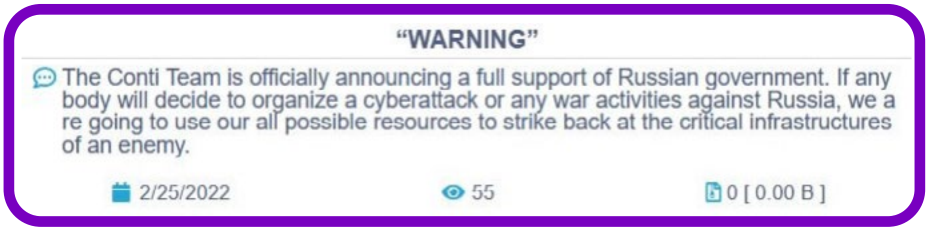
**Exhibit 2:** RaidForums administrator banning pro-Russian activity on the entire forum *(February 28, 2022).*

Unfortunately, the old motto "united we stand, divided we fall" does not apply to criminal underground actors, as this divide has led to pro-Russian actors galvanizing against Western targets, especially in the resources, government, media, financial and insurance industries. The targeting of financial and insurance entities is due to the perception that they are the working arms of Western financial sanctions, whereas the targeting of utilities and resources entities is due to those organizations' importance as critical national infrastructure. This targeted intent has led some actors to exclusively sell their services, such as network accesses, to pro-Russian actors; it has led other actors to extend discounts to pro-Russian actors interested in buying their accesses but has also caused those same actors to refrain from selling accesses associated with Russian entities.

**> Unfortunately, the old motto "united we stand, divided we fall" does not apply to criminal underground actors...**

Moreover, it is likely that pro-Russian actors are foregoing available attacks against non-Western entities to centralise their focus and resources. This is significant as since 2020, network access selling has become a central pillar of underground cybercrime forums with Initial Access Brokers being actors who specialize in compromising corporate networks for the intent of reselling to other threat actors, often ransomware groups. This industry has allowed ransomware groups to scale their activity significantly.

Clear examples of pro-Russian actors are members of the Conti Team ***(Exhibit 3),*** LockBit and CoomingProject ransomware collectives publicly stating their support for the Russian government. However, taking a stance does have consequences—shortly after Conti Team's statement of support, the threat group suffered a devastating breach by a Ukrainian security researcher resulting in the disclosure of Conti Team's source code, tactics, techniques and procedures and internal group communications, causing LockBit actors to retract their support and claim apolitical neutrality, presumably to avoid similar dissent[1]. Similarly, RaidForums' main domain was seized by unknown entities shortly following that forum's statement of pro-Ukrainian support; this domain remains offline as of March 4, 2022.



"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 55 0 [ 0.00 B ]

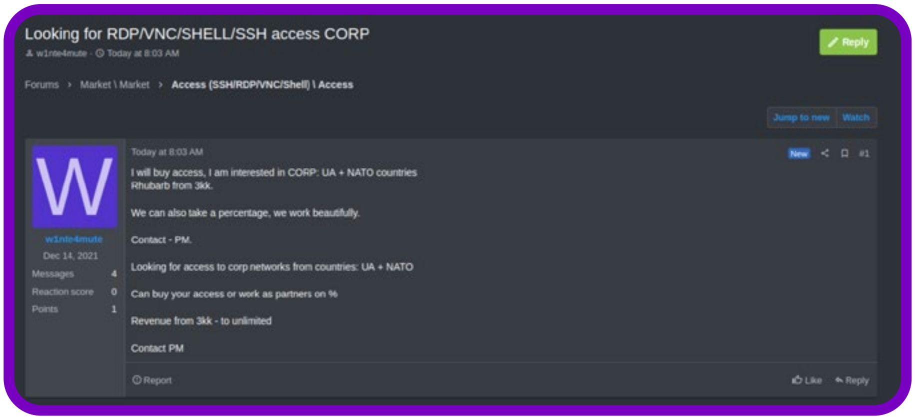
**Exhibit 3:** A February 26, 2022, posting by the Conti Team ransomware collective, showcasing its support for Russia and its willingness to target critical national infrastructure.

# The Return of Ransomware Groups

ACTI assesses ransomware groups' shifts from purely financial motivations to quasi-hacktivist ones may have several far-reaching consequences for both the types of threats emanating from underground actors and for the overall threat level.

First, financially motivated actors such as ransomware collectives or initial access brokers (the latter being a sub-category of threat actors supplying ransomware groups with corporate network access) are choosing targets based on political motives rather than looking for opportunistic prospects for financial gains; this target switch is leading to a higher threat level for Western organizations ***(see Exhibit 4).*** Western organizations usually merely face threats from hacktivists who traditionally employ cheap or free tools that rarely impact victim business operations significantly. On the contrary, ransomware collectives are well-funded, employ one-day or zero-day exploits, have elevated tradecraft levels and large budgets (typically in the form of bitcoin), and are organized, allowing them to disrupt businesses more efficiently and for prolonged periods.

[1] **"Conti Ransomware Gang Internal Chats Leaked by Ukraine Security Researcher,"** Bitdefender, February 28, 2022.



Looking for RDP/VNC/SHELL/SSH access CORP

w1nte4mute · Today at 8:03 AM

Forums › Market \ Market › Access (SSH/RDP/VNC/Shell) \ Access

w1nte4mute
Dec 14, 2021
Messages 4
Reaction score 0
Points 1

Today at 8:03 AM

I will buy access, I am interested in CORP: UA + NATO countries
Rhubarb from 3kk.

We can also take a percentage, we work beautifully.

Contact - PM.

Looking for access to corp networks from countries: UA + NATO

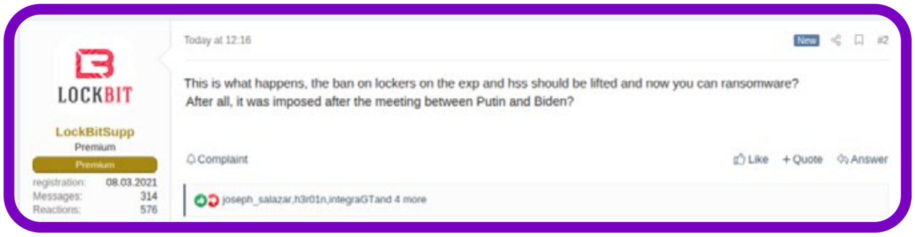
Can buy your access or work as partners on %

Revenue from 3kk - to unlimited

Contact PM

**Exhibit 4:** Actor on pro-Russian forum RAMP seeking to buy access to any corporation in Ukraine or NATO *(March 1, 2022).*

Second, the ideological split has led many underground actors to call for the return of ransomware groups to the mainstream underground ***(see Exhibit 5).*** In May 2021, following the DarkSide ransomware attack on Colonial Pipeline, forum administrators banned ransomware groups and their affiliates from some of the most-popular forums to pre-empt increased scrutiny from law enforcement, which ultimately pushed actors and groups to other forums[2]. While ransomware actors did not disappear from the underground (they instead masqueraded as network access buyers or congregated on new forums like RAMP), the ban did make it harder for them to acquire tools, recruit affiliates, or gain exploits or accesses, thereby reducing ransomware actors' abilities to scale their operations. Overtly allowing ransomware actors to return to forums would not only enable those actors to target Western organizations more efficiently but also embolden them, as other underground actors would likely herald ransomware actors' return and give those ransomware actors perceived moral reason to conduct attacks, especially against critical national infrastructure.



LockBitSupp
Premium
registration: 08.03.2021
Messages: 314
Reactions: 576

Today at 12:16

This is what happens, the ban on lockers on the exp and hss should be lifted and now you can ransomware?
After all, it was imposed after the meeting between Putin and Biden?

joseph_salazar,h3r01n,integraGTand 4 more

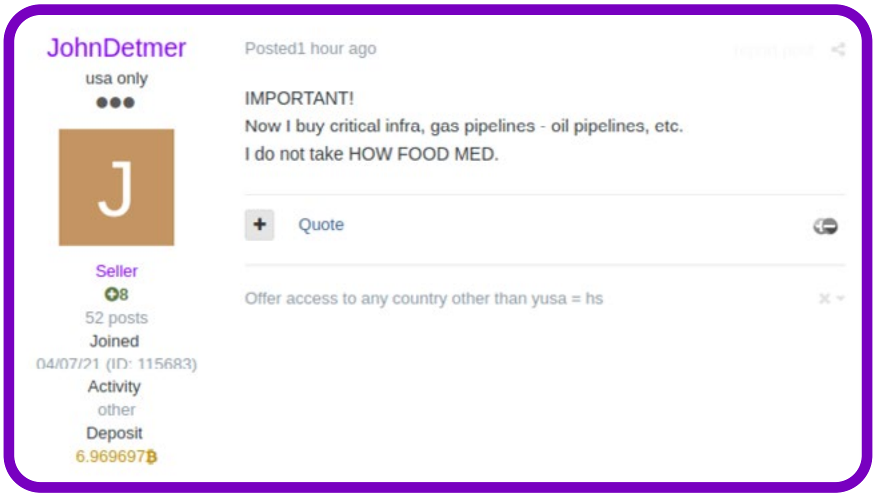
**Exhibit 5:** LockBitSupp calling for the return of ransomware groups to the mainstream Russian-language criminal underground forums *(February 28, 2022).*

> **the ban did make it harder for them to acquire tools, recruit affiliates, or gain exploits or accesses...**

[2] **"Three Major Hacking Forums Ban Ransomware Ads as Some Ransomware Gangs Shut Down",** The Record, May 17, 2021.

# Threats to Critical National Infrastructure Loom

The shift to acting with political motivations is leading to threat actors reinstating the targeting of Western critical national infrastructure. This is in stark contrast to the near complete absence of such targeting by ransomware groups, access sellers and their associated actors following the ransomware ban in 2021. ACTI has observed multiple actors specifically stating desires to target Western critical infrastructure to support Russia; those making these statements include the Conti collective and prolific actors such as JohnDetmer ***(see Exhibit 6).*** Critical national infrastructure entities' have gone from being a low-medium target to the focus of targeted ransomware campaigns due to political motivations significantly increasing these entities' threats from ransomware groups. It will likely also threaten entities relying on uninterrupted continuity and services from critical national infrastructure entities.



JohnDetmer
usa only
●●●

Seller
8
52 posts
Joined
04/07/21 (ID: 115683)
Activity
other
Deposit
6.969697Ƀ

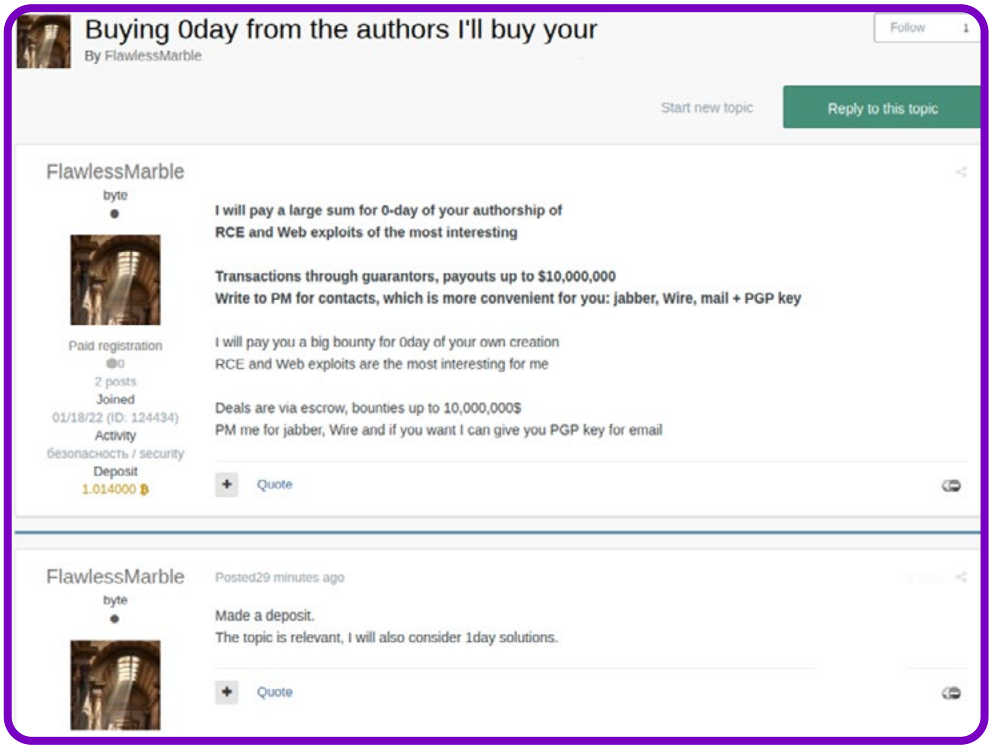
Posted1 hour ago

IMPORTANT!
Now I buy critical infra, gas pipelines - oil pipelines, etc.
I do not take HOW FOOD MED.

Offer access to any country other than yusa = hs

**Exhibit 6:** JohnDetmer seeking to buy access to critical national infrastructure *(February 28, 2022).*

These trends must be seen in the context of an already increasingly professionalized criminal underground able to endure and cater to a varied array of criminal activity. This underground is populated with actors able to outsource various steps of the cyber kill chain, which allows ransomware groups to scale their activity and increase targeting of specific organizations instead of merely taking opportunistic approaches to attacking. Moreover, ACTI has seen some of the biggest and seemingly ever-rising budgets for custom malware and exploits by these actors, with some actors like Integra and FlawlessMarble having budgets of $5–10 million USD ***(Exhibit 7),*** allowing them to acquire almost any tool or exploit desired. We're also seeing budgets up to $500,000 for actors seeking network access.



Buying 0day from the authors I'll buy your

By FlawlessMarble

FlawlessMarble
byte

Paid registration
0
2 posts
Joined
01/18/22 (ID: 124434)
Activity
безопасность / security
Deposit
1.014000 ฿

**I will pay a large sum for 0-day of your authorship of**
**RCE and Web exploits of the most interesting**

**Transactions through guarantors, payouts up to $10,000,000**
**Write to PM for contacts, which is more convenient for you: jabber, Wire, mail + PGP key**

I will pay you a big bounty for 0day of your own creation
RCE and Web exploits are the most interesting for me

Deals are via escrow, bounties up to 10,000,000$
PM me for jabber, Wire and if you want I can give you PGP key for email

FlawlessMarble
byte

Posted29 minutes ago

Made a deposit.
The topic is relevant, I will also consider 1day solutions.

**Exhibit 7:** Threat actor FlawlessMarble showing a budget of $10 million USD to buy zero-day exploits *(February 28, 2022).*

# Outlook

Having monitored underground forums for more than a decade, ACTI notes that the current split on the underground and the large-scale transitions to an ideological motivation by what were previously financially motivated groups is unprecedented and may bring about far-reaching consequences. The primary effect of this political divide so far is an increased and prolonged threat from underground actors aimed at Western targets, owed to the galvanization of pro-Russian actors and their targeted efforts that focus on “enemies of Russia.” It also ushers the return of overt ransomware groups on the largest mainstream criminal underground forums and brings about a strong desire by these groups to target critical national infrastructure. Organization of efforts or cross-collaboration of these pro-Russian collectives will ensure a prolonged, heightened threat to Western entities.

ACTI assesses that this motivational shift will be long lasting, however, not permanent because the primary driver of these threat actors’ is financial gain. Finally, if large pro-Russian ransomware groups and their auxiliary services ideologically align with themselves ACTI assesses cyber attack activity will increase significantly.

# Mitigation

To protect against Conti and other ransomware, ACTI suggests:

- Patching to protect against the recently dumped Conti source code, as Conti is the malware associated with the greatest number of ransomware attacks in 2021.
- Maintaining standard cybersecurity patching hygiene practices and incorporating into vulnerability and attack surface management programs an intelligence-driven approach that goes beyond incorporating intelligence on available proof-of-concept code and active exploitation for patch prioritization.
- Patching against server-side exploits, as actors can scan the entire IPv4 address space in hours to find vulnerable systems.
- Achieving a resilient security posture by creating and maintaining both a hunting program that actively looks across an attack surface and an intelligence capability that can operate responsibility in the Darknet to provide indications and warnings about threats' operating environments.
- Creating and regularly testing a business continuity of operations plan.
- Ensuring supply chain partners are following strict security policies.
- Patching against the following vulnerabilities, which are associated with Conti breaches:
    - CVE-2015-2546
    - CVE-2016-3309
    - CVE-2017-0101
    - CVE-2017-0199
    - CVE-2018-8120
    - CVE-2019-0543
    - CVE-2019-0708
    - CVE-2019-0841
    - CVE-2019-1064
    - CVE-2019-1069
    - CVE-2019-1129
    - CVE-2019-1130
    - CVE-2019-1215
    - CVE-2019-1253
    - CVE-2019-1315
    - CVE-2019-1385
    - CVE-2019-1388
    - CVE-2019-1405
    - CVE-2019-1458
    - CVE-2020-0609
    - CVE-2020-0638
    - CVE-2020-0688
    - CVE-2020-0787
    - CVE-2020-0796
    - CVE-2020-1472
    - CVE-2020-5135
    - CVE-2021-1675
    - CVE-2021-1732
    - CVE-2021-21985
    - CVE-2021-22005
    - CVE-2021-26855
    - CVE-2021-34527
    - CVE-2021-44847

# About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at **accenture.com**.

**Accenture Security** is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence.

**FOLLOW US:**

**@AccentureSecure** on Twitter,

**LinkedIn**

or visit us at **accenture.com/security**.

**Accenture Cyber Threat Intelligence,** part of Accenture Security, has been creating relevant, timely and actionable threat intelligence for more than 20 years. Our cyber threat intelligence and incident response team is continually investigating numerous cases of financially motivated targeting and suspected cyber espionage. We have over 150 dedicated intelligence professionals spanning 11 countries, including those with backgrounds in the intelligence community and law enforcement. Accenture analysts are subject matter experts in malware reverse engineering, vulnerability analysis, threat actor reconnaissance and geopolitical threats.

All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from ACTI. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.

ACCENTURE PROVIDES THE INFORMATION ON AN "AS-IS" BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS ALERT.