DXC.technology

March 2019

Threat Intelligence Report

About this report

The DXC Threat Intelligence Report provides a monthly roundup of key developments related to the cyber threat landscape.

Leveraging a mix of open source and proprietary information feeds, including DXC Technology's global network of Security Operations Centers and cyber intelligence services, this report delivers a succinct overview of major incidents, insights into key trends and awareness of strategic threats so that you can take action.

This report is produced by DXC as part of DXC Labs | Security, which provides insights and thought leadership to the security industry.

Month in numbers

151m

MyFitnessPal account details leaked to dark web

$20,000

Price for all 620m leaked accounts on Dream Market

70,000

Security logs reportedly left exposed by B&Q due to a poorly protected Elasticsearch server

50

Companies and government agencies affected by DNSpionage campaign in the Middle East

Key takeaways

- **Financial services remains the most targeted industry sector.**
- **CEOs and chief executives are being targeted in new phishing campaign.**
- **Widespread attacks on DNS services allow attackers access to sensitive information without directly compromising the target organization.**
- **Availability of cheap account information on the dark web will continue to drive credential-stuffing attacks.**

Incidents and Cybercrime

UK home improvement retailer exposes sensitive data

A publicly accessible database was left without password protection, exposing 70,000 sensitive logs pertaining to store thefts. Details exposed include product codes, value of stolen goods, location information, incident summaries, suspected offender names and vehicle identifiers.

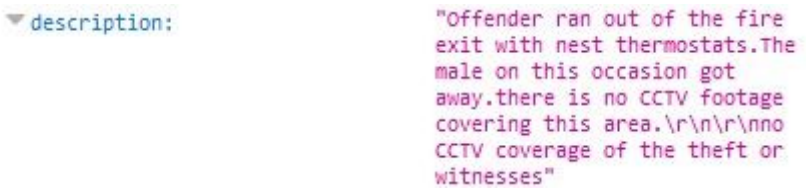

Figure 1: An example of the accessible database entries posted by Ctrlbox.

The sensitive nature of information exposed could result in GDPR sanctions. Incident logs also highlighted wider security gaps, such as CCTV black spots and other potentially useful information for those with malicious intentions.

B&Q, a large UK home and hardware retailer, disconnected the server following repeated warnings from security researchers.

DXC Assessment

This exposure could have been prevented through basic cybersecurity practices, such as proper authentication configuration on the server. Such information sources should be protected by preventing public IP access, the use of isolated or protected networks, avoiding common ports and the use of proxy services for access.

Source: BBC, Ctrlbox

DNS Hijacking/Poisoning enables attackers to redirect internet traffic to servers that they control, harvest login credentials, SSL certificates or other sensitive information. VPN and email traffic were affected by the DNSpionage campaign.

Active Threat Actors

Magecart

Prominent card-skimming group stealing payment card details from online retailers worldwide

Grim Spider

Russian cybercriminal group operating Ryuk Ransomware against enterprises using emotet and TrickBot banking trojans for initial access

APT10 aka Stone Panda

Chinese espionage group using sophisticated techniques to breach MSPs and enterprises

APT 39

Iranian espionage group targeting Middle East

Lazarus Group

North Korean linked APT, which has conducted significant attacks against Sony Corp, South Korea and international banks

New phishing campaign targets C-suite and executives

Phishing emails claiming to be from the company's CEO and requesting to reschedule a board meeting are being sent to senior corporate executives. The emails provide a URL link to a counterfeit "Doodle" poll site asking executives to identify a new meeting date. In reality, it is a well-constructed Office 365 credential theft site.

Intelligence suggests that the attacks are not limited to specific industry verticals or organization size. If viewed on a mobile device, the sender changes to "Note to Self," a feature in Microsoft Outlook that activates when a person emails their own account. This feature adds a sense of legitimacy, which is likely to increase attacker success. Some email clients have been found to auto-filter this campaign to the "Spam" folder.

DXC Assessment

Phishing is consistently the leading attack vector for advanced persistent threats and cybercrime adversaries. Layered phishing protection should be a top security priority. Mailbox protection with URL defense, next-`core of an effective defense. Regular phishing awareness training can also generate a security-conscious culture and last line of defense. Mature organizations should automate escalation of VIP incidents to security analysts to detect and stop breaches early.

Source: GreatHorn, Anomali

620 million stolen accounts for sale on dark web

Account information stolen from 16 websites — including MyFitnessPal, MyHertiage, ShareThis, Whitepages and CoffeeMeetsBagel — are listed for sale on the "Dream Market" marketplace alongside drugs, weapons and other illicit items. Some of these sites were already reported to have suffered a breach while others, such as photography site 500px, had not.

Packaged databases of details are listed individually and are available for less than $20,000. Depending on the breach, details consist of account holder names, email addresses and hashed passwords. Some sites lost further personal details and social media authentication tokens. All databases are being sold by the same vendor known as "gnosticplayers," which exploited security vulnerabilities within web applications to extract data from the sites.

DXC Assessment

Several sites with data exposed in this breach had not previously reported a security incident, suggesting that they were either unaware of the breach or had opted not to reveal it — which could lead to GDPR implications.

It is expected that the databases will be purchased by spammers and "credential stuffers," who will target the accounts in phishing attacks

and attempt to access other services/sites where individuals have used the same credentials.

The passwords are protected by obsolete MD5 or SHA1 hashing algorithms which can be cracked quickly using commercial or open-source tools. Cybercriminals often increase the speed and mass of their "cracking" activity through the use of cloud-based services.

Credential stuffing remains one of the most common methods of account compromise. Where possible, organizations should use 2FA and complex password policies to reduce this risk.

Source: theregister, theIndependent

Nation State and Geopolitical

Australian Parliament breached by 'state actor' in build up to election

Australia's prime minister confirmed a "malicious intrusion" of the Australian Parliament servers. Networks of Liberal, Labor and National parties also were affected. The extent of any data loss is not yet known, and Prime Minister Scott Morrison would not confirm which foreign states are under suspicion. However, he stress that "there is no evidence of electoral interference."

Cyber security experts at the Australian Strategic Policy Institute and International Cyber Policy Centre have suggested that China is the most likely culprit due to the country's history of attacking Australian national interests. The Chinese foreign ministry denied any involvement.

Russia's Fancy Bear group also has been touted as a potential culprit due to its history of electoral interference and political espionage.

Source: BBC

Widespread DNS hijacking attacks

A widespread attack on DNS services has allowed suspected Iranian threat actors to access large amounts of email, passwords and other sensitive information.

The sophisticated espionage campaign, dubbed DNSpionage by Cisco Talos, affected DNS services that translate domain names into internet addresses and prompted the U.S. Department of Homeland Security to issue an emergency directive to all U.S. federal civilian agencies mandating they complete a four-step action plan to secure their systems.

The list of internet addresses abused by this campaign centers on targets in the Middle East, heavily featuring the UAE, Lebanon, Egypt and Jordan

Most Targeted Industries

- Financial Services
- Professional Services/ Consulting
- Telecommunications

Data Source: FireEye (Feb. 2019)

with government being the most targeted sector. Internet infrastructure in Sweden and the U.S. also have been targeted.

DXC Assessment

The U.S. action plan highlights useful DNS security steps, which can apply beyond U.S. government agencies. The global scope and varied target set of the hijacking campaign means all organizations associated with government or telecommunications should consider adoption.

Source: computerweekly.com, KrebsOnSecurity, FireEye, CrowdStrike

Hacktivism and Insider Threat

Anonymous targets Zimbabwe after government crackdown

Anonymous targeted 72 government websites with DDoS attacks and posted warnings to the "banking system" after the government shut down internet access following a crackdown on protesters in the country.

Government and state institutions targeted in the attack included the reserve bank of Zimbabwe, the Zimbabwe Republic Police and the defense ministry.

DXC Assessment

Anonymous' threats are rarely empty. The group previously disrupted 200 Sudanese government websites and their electronic payment systems. Anonymous has global reach and support. Last year's growth in the availability of ransomware and DDoS-as-a-service providers only increases the ease in which the Anonymous franchise can conduct attacks. Any organization which generates public controversy could be targeted. Sentiment analysis is a useful method of highlighting risk in this area.

Source: telecoms.com, Bulawayo24

Vulnerability and Threat Developments

SpeakUp backdoor Linux trojan discovered

A campaign targeting Linux servers is implanting a new backdoor that evades security vendors. The new Trojan, dubbed "SpeakUp" (after its C2 name), exploits known vulnerabilities in six Linux distributions and is capable of running commands on infected hosts.

The attack is gaining momentum and targeting servers in East Asia and Latin America, including AWS-hosted machines. SpeakUp propagates internally within the infected subnet and beyond to new IP ranges,

exploiting remote code execution vulnerabilities. Once installed, the malware checks for new instructions from its command and control infrastructure with regular cadence.

The threat actor behind this trojan is still unconfirmed; however, elements of the malware imply a connection to East Asia.

Source: Check Point

Increase in Emotet activity

A significant increase in the spread of Emotet, one of the most significant financial malware threats of the last two years, has been reported since November.

Threat actors use email accounts harvested during breaches, along with other malicious activity, to expand the reach of the malware.

Emotet is used by several sophisticated cybercriminal groups from Eastern Europe. Blocking known command and control URLs and IPs, and ensuring that endpoint protection systems and system patches are up-to-date are the most effective ways to block the malware.

Source: MenloSecurity

Keep up to date on the latest threats

Get the latest DXC threat intelligence updates. Visit www.dxc.technology/threats

