From: Kimberly Lile Dowty
To: Kimberly Lile Dowty
Subject: FW: [Security] Texas Cybersecurity Weekly: TLP Green
Date: Friday, April 3, 2020 10:39:56 AM
Attachments: image001.png
image002.png
image004.png
image005.png

From: security <security-bounces+tarc=txregionalcouncil.org@lists.state.tx.us> on behalf of DIR Security via security <security@lists.state.tx.us>
Reply-To: DIR Security <dirsecurity@dir.texas.gov>
Date: Thursday, April 2, 2020 at 5:51 PM
To: DIR Security <dirsecurity@dir.texas.gov>
Subject: [Security] Texas Cybersecurity Weekly: TLP Green

Texas Cybersecurity Weekly

VOL. II - NO. 76
April 2, 2020

TLP: GREEN

Top of the News

Cybercriminals targeting Zoom, Google and Teams domains

April 1, 2020 – SC Media

The increased video conferencing activity due to COVID-19 has given cybercriminals the opportunity to use typosquatting and URL hijacking by imitating many of the top conferencing platforms. Popular video conferencing applications such as Zoom, Teams and Google are seeing their names used by malicious actors to create newly registered fake domains with Zoom seemingly being singled out at this time. Since January 1 the security firm has seen about 1,700 new domains registered using the word “zoom” in some fashion with 25 percent of these new registrations happing in the last seven days.

Cyber gangs have also noted and are taking advantage of the increase in online learning with K-12 and universities opting to continue teaching remotely. This has resulted in domains using Google Classroom in some manner being created replacing googleclassroom.com with googloclassroom\.com and googieclassroom\.com.

Omer Dembinskey, Check Point’s manager of threat intelligence said the fake domains fall in to three categories. Those known to be malicious those that at least for the moment, benign and URLs that are legitimate and just happen to have the word “zoom” in their name.

The malicious domains can be used for any number of attacks. Two specific variety’s sees so far by Check Point are fake Google Classroom, Microsoft Teams URLs and some of those using zoom were being used to spread the InstallCore PUA.
Full Report

COVID-19 Tools from DIR

All Texans need to remain vigilant and practice good cyber hygiene, especially during critical incidents. DIR has provided tools everyone should consider for working remotely. Protect your organization by understanding policies addressing virtual meetings, information security and records retention.

- Virtual Collaboration Tools Security Tips
- Teleworking Tips

Additional resources can be found on the DIR site pages COVID-1 Preparedness for Information Technology and Cyber Hygiene.

OCISO News

HB 3834 Certified Training Program Application Information

April 30, 2020 - 2019-2020 Certified Training Program **application deadline**.
May 15, 2020 - 2020-2021 certification requirements will be published.
June 1 - July 31 - 2020-2021 Certified Training Program applications acceptance period.

New Developer Training Program added to Info Sec Academy

DIR is pleased to announce the DIR Secure Developer Training Program as a part of current Info Sec Academy offerings in addition to the Cybersecurity Program. Agency participation in developer courses will not take away allotted seats for security courses. Please share with your application development team.

These certification prep courses will provide guidance to application developers on how to build secure software. Our program begins on April 14th with the EC - Council CASE Java course. Course and exam voucher at no cost to Texas state agencies and higher educational institutions. Course will be offered virtual online live for the near term due to COVID-19 guidelines.

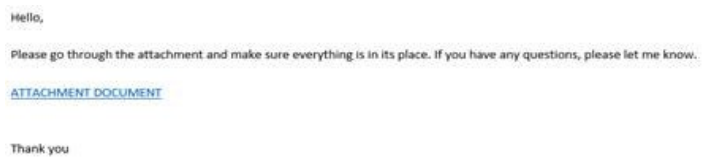
News Highlights

- **Microsoft Delays Disabling Insecure TLS in Browsers Until July**
- **Patching Poses Security Problems with Move to More Remote Work**
- **Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites**
- **Coronavirus: Microsoft directly warns hospitals, 'Fix your vulnerable VPN appliances'**
- **Upgraded malicious Word, Excel attachments targeting WFH employees**
- **Online Credit Card Skimmers Are Thriving During Pandemic**

Texas Phishing Campaigns

DIR is seeing emails being sent to SoT entities that appear to come from a project manager or official business which indicate the recipient has an important document to review. However, instead of an actual attachment it provides a link to the attachment which directs you to a malicious site. Users are warned to be cautious of these emails.

Example: Phishing email being sent to SoT employees.


Hello,

Please go through the attachment and make sure everything is in its place. If you have any questions, please let me know.

ATTACHMENT DOCUMENT

Thank you

Phishing Summary: March 22nd- 29th, 2020

The week of March 22nd – 29th, 2020 saw 12 reports of phishing campaigns sent to the NSOC from State of Texas organizations. A total of 6 agencies forwarded phishing campaigns this week, resulting in 3 URLs and 0 IPs being blocked.

Should you receive suspicious emails, attach them to an email and send to security-alerts@dir.texas.gov.
DIR encourages you to share this information with your staff to further their education and awareness on spotting and reporting phishing campaigns before they gain traction.

Cybersecurity Incidents

Marriott hit by second data breach exposing "up to" 5.2 million people

March 31, 2020 – Verdict

Hotel chain Marriott International has today announced that it has been hit by a second data breach exposing the personal details of "up to approximately 5.2 million guests".
Full Report

Med group's breach disclosure claims SSNs unaffected; leaked docs suggest otherwise

April 1, 2020 – SC Media

The Affordacare Urgent Care Clinic, a network of medical providers based in Texas, has officially confirmed a combination data breach-ransomware attack that exposed sensitive information.
Full Report

Advisories & Vulnerability Alerts

Multiple Vulnerabilities in DrayTek Products Could Allow for Arbitrary Code Execution

MS-ISAC Advisory Number: 2020-043
Date Issued: April 1, 2020

OVERVIEW:
Multiple vulnerabilities have been discovered in DrayTek devices which could allow for arbitrary code execution. DrayTek is a manufacturer of broadband CPE, including firewalls, VPN devices, routers and wireless LAN devices. Successful exploitation of these vulnerabilities could result in an attacker executing arbitrary code on the affected system. This could allow an attacker to eavesdrop on network traffic, operate SSH and Web based backdoors, and create system accounts.
Full Advisory Details

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

MS-ISAC Advisory Number: 2020-044
Date Issued: April 1, 2020

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary

code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.
Full Advisory Details

Texas Cybersecurity Weekly

Collected news & information for Texas' cybersecurity community

The periodical aggregates information about cybersecurity and information technology to promote shared awareness, cyber hygiene, and information sharing amongst government, the private sector, and all Texans.

TLP: GREEN

Limited disclosure, restricted to the community. Recipients may share TLP: **GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: **GREEN** information may not be released outside of the community.
https://www.us-cert.gov/tlp

Visit Our Website

Assistance/Feedback/Questions?

Office of the Chief Information Security Officer
DIRSecurity@dir.texas.gov
Texas Department of Information Resources

Transforming How Texas Government Serves Texans