Cyber Intelligence Brief

Aug 28 - Sep 3, 2021

See Threats. Stop Breaches. Together

*Prepared by **deepwatch Threat Intelligence Team***

Denver Office & SOC

7800 East Union Avenue, Suite 900

Denver, CO 80237 USA

855.303.3033

Purpose

This report is provided to you to improve your situational awareness and educate recipients of cyber events to aid in protecting organizations' networks, proprietary and personally identifiable information from unauthorized access, theft, or espionage. In addition, deepwatch includes additional insights and recommendations and any actions we may have taken if applicable.

Sources of Information

This publication incorporates open-source news articles to educate readers on cybersecurity matters IAW USC Title 17, section 107, Para a. All articles have been truncated to avoid the appearance of copyright infringement.

Use and Definitions

To help you use this document to its full potential, a few items may be helpful to know:

- You can click on any item in the table of contents to take you to that portion of the report.
- Links throughout this document are identified by the font color of "deepwatch" Green.
- Your feedback will be extremely valuable to the deepwatch Threat Intelligence Team; please take a few minutes to send us your feedback here. Your feedback submission can be anonymous. We read each submission carefully. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.
- Each headline will be categorized; these categories quickly let you know what the main topic of the headline is.
- Each headline this report covers includes the following information:
    - A headline, publication date, and a link to the source material.
    - Key Points section to get the most important information first.
    - Summary - This is a brief synopsis of the reporting to bring you only the most relevant information. If applicable, deepwatch will link items of interest for further context; these will be in "deepwatch" Green.
    - deepwatch Insights - This section may include additional analysis and reporting on the activity if applicable, any recommendations, and any actions deepwatch may have taken with the available information.
- If MITRE ATT&CK tactics and techniques and/or IOCs are listed, these can be found in the accompanying Appendixes.

Table of Contents

Quick Look

Vulnerability | Headline: A New Vulnerability in Exchange Server

Key Takeaway

- Trend Micro's Zero Day Initiative disclosed a new vulnerability in Microsoft's Exchange Server. The vulnerability, which has proof-of-concept code published, allows an unauthenticated threat actor to perform configuration actions on mailboxes.

deepwatch Outlook

- deepwatch Threat Intelligence Team has moderate confidence that this vulnerability will be exploited along with the other Exchange vulnerabilities recently released. Even though this vulnerability has a relatively low CVSS score, this vulnerability could allow a threat actor to configure mailboxes. deepwatch encourages all organizations to ensure that the appropriate patches have been applied (KB500177).

Ransomware | Headline: CISA Issues Alert for Ransomware Awareness for Holidays and Weekends

Key Takeaway

- CISA and the FBI issued a joint advisory detailing best practices and mitigations for ransomware for the upcoming holidays and weekends. There is no current intelligence indicating a potential cyber-attack occurring over the upcoming holidays and weekends.

deepwatch Outlook

- deepwatch advises customers to engage their squad manager to establish a preemptive threat hunt on their networks. CISA states that "Threat hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack."

Phishing | Headline: ICYMI: Microsoft Tracks a Widespread Credential Phishing Campaign

Key Takeaway

- Microsoft has been monitoring a widespread phishing campaign that uses redirects and reCAPTCHA to avoid being blocked by analysis systems. The emails seemed to follow a familiar pattern that presented all the email content in a box with a large button that, when clicked, led to credential harvesting pages.

deepwatch Outlook

- The Threat Intelligence Team has moderate confidence that the use of reCAPTCHA will continue to be used by threat actors due to the possible prevention of automated analysis coupled with the appearance of the site being legitimate.

Bad Practices | Headline: CISA Adds Single-Factor Authentication to list of Bad Practices

Key Takeaway

- CISA added the use of single-factor authentication for remote or administrative access systems to the Bad Practices catalog, a list of cybersecurity practices, techniques, and exceptionally risky configurations.

deepwatch Outlook

- deepwatch urges all organizations to review the "Bad Practices" catalog and to implement the necessary steps to address these.

Back to Table of Contents

Headlines

Vulnerability | A New Vulnerability in Exchange Server

August 30, 2021
Source: *Zero Day Initiative*

Key Points:

- Trend Micro's Zero Day Initiative disclosed a new vulnerability in Microsoft's Exchange Server.
- The vulnerability allows an unauthenticated threat actor to perform configuration actions on mailboxes.
- This vulnerability is tracked as CVE-2021-33766.
- A proof-of-concept code has been published for this vulnerability.

Summary:

In March, a new vulnerability in Microsoft's Exchange Servers 2019, 2016, & 2013 was reported to the Zero Day Initiative (ZDI) by researcher Le Xuan Tuyen of VNPT ISC. Microsoft patched it in the July Exchange cumulative updates. This vulnerability is tracked as CVE-2021-33766, with a CVSS score of 6.5.

ZDI says that "*this vulnerability, an unauthenticated attacker can perform configuration actions on mailboxes belonging to arbitrary users. As an illustration of the impact, this can be used to copy all emails addressed to a target and account and forward them to an account controlled by the attacker.*"

Shortly after ZDI publicly disclosed the vulnerability, security researcher @Bhadresh Tweeted his proof-of-concept (PoC) code for the exposure he published to his GitHub repository.

deepwatch Threat Intelligence Outlook

deepwatch Threat Intelligence Team has moderate confidence that this vulnerability will be exploited along with the other Exchange vulnerabilities recently released. Even though this vulnerability has a relatively low CVSS score, this vulnerability could allow a threat actor to configure mailboxes. deepwatch encourages all organizations to ensure that the appropriate patches have been applied (KB500177).

deepwatch suggests customers discuss threat hunt and detection strategies to observe unintended mailbox misconfigurations.

Back to Table of Contents

Ransomware | CISA Issues Alert for Ransomware Awareness for Holidays and Weekends

August 31, 2021
Source: *CISA (PDF)*

Key Points:

- CISA and the FBI issued a joint advisory detailing best practices and mitigations for ransomware for the upcoming holidays and weekends.
- The alert states that CISA/FBI does not currently have intelligence regarding potential cyber threats occurring on the upcoming holidays and weekends.
- The report lists the six most frequently reported ransomware variants: Conti, PYSA, LockBit, RansomEXX/Defray777, Zeppelin, and Crysis/Dharma/Phobos.

Summary:

In a recent joint alert issued by The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), they "*have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends.*"

The FBI and CISA state in the report that they "*do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends.*" Threat actors may see holidays, weekends, and especially holiday weekends as reasonable time frames to target small and large businesses.

The report also states that the following ransomware variants have been the most frequently reported to the FBI over the last month: Conti, PYSA, LockBit, RansomEXX/Defray777, Zeppelin, and Crysis/Dharma/Phobos.

deepwatch Threat Intelligence Outlook

deepwatch advises customers to engage their squad manager to establish a preemptive threat hunt on their networks. CISA states that "*Threat hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack.*"

deepwatch agrees with the recommended mitigations from CISA: make an offline backup of your data, do not click on suspicious links, secure and monitor RDP and other risky services, update operating systems and software and scan for vulnerabilities, implement a strong password policy, implement multi-factor authentication, implement segmentation, filter traffic, and scan ports, secure user accounts, and develop an incident response plan.

Back to Table of Contents

Phishing | ICYMI: Microsoft Tracks a Widespread Credential Phishing Campaign

August 26, 2021
Source: *Microsoft*

Key Points:

- Microsoft has been monitoring a widespread phishing campaign that uses redirects and reCAPTCHA to avoid being blocked by analysis systems.
- The emails seemed to follow a familiar pattern that presented all the email content in a box with a large button that, when clicked, led to credential harvesting pages.
- Threat actors are using legitimate services to fool users and avoid detection by analysis systems.

Summary:

Microsoft has been following a broad credential phishing campaign using open redirector links. Threat actors combine these links with social engineering lures that impersonate well-known productivity tools and services to entice users into clicking. Doing so leads to a series of redirections, including a CAPTCHA verification page that adds a sense of legitimacy and attempts to evade automated analysis systems before taking the user to a fake sign-in page.

Microsoft noticed that the emails seemed to follow a common pattern that presented all the email content in a box with a large button that, when clicked, led to credential harvesting pages. In general, Microsoft saw that the subject lines contained the following items:

- [Recipient username] 1 New Notification
- Report Status for [Recipient Domain Name] at [Date and Time]
- Zoom Meeting for [Recipient Domain Name] at [Date and Time]
- Status for [Recipient Domain Name] at [Date and Time]
- Password Notification for [Recipient Domain Name] at [Date and Time]
- [Recipient username] eNotification

Once a user clicks on the redirect link, they are sent to a threat actor-controlled page. These pages used Google reCAPTCHA services to probably prevent analysis systems from attempting to advance to and check the contents of the actual phishing page.

deepwatch Threat Intelligence Outlook

The Threat Intelligence Team has moderate confidence that the use of reCAPTCHA will continue to be used by threat actors due to the possible prevention of automated analysis coupled with the appearance of the site being legitimate. To prevent phishing, organizations must establish a phishing awareness program and implement simulated phishing campaigns to reinforce best practices for identifying phishing emails.

deepwatch deploys numerous detections to observe potential phishing attempts; please reach out to your squad manager to ensure that these detections can be enabled in your environment. Appendix A lists the IOCs that Microsoft identified in this phishing campaign.

Back to Table of Contents

Bad Practices | CISA Adds Single-Factor Authentication to list of Bad Practices

August 30, 2021
Source: *CISA*

Key Points:

- CISA added the use of single-factor authentication for remote or administrative access systems to the Bad Practices catalog.
- Bad Practices is a catalog of cybersecurity practices, techniques, and exceptionally risky configurations.
- There are three "Bad Practices," and more will be updated over time.

Summary:

On June 24, the US Cybersecurity and Infrastructure Security Agency (CISA) launched a new project called "Bad Practices," a catalog of hazardous cybersecurity practices, techniques, and configurations.

On August 30, CISA added single-factor authentication for remote or administrative access systems to the Bad Practices catalog. CISA asserts that "*Single-factor authentication is a common low-security method of authentication. It only requires matching one factor—such as a password—to a username to gain access to a system.*"

The current list of "Bad Practices are:

- **The use of unsupported (or end-of-life) software**.
- **Use of known/fixed/default passwords and credentials**.
- **The use of single-factor authentication for remote or administrative access to systems**.

Cybersecurity experts can recommend other "bad practices" via CISA's GitHub page.

deepwatch Threat Intelligence Outlook

deepwatch urges all organizations to review the "Bad Practices" catalog and to implement the necessary steps to address these. For guidance on setting up strong authentication, see the CISA *Capacity Enhancement Guide: Implementing Strong Authentication* (PDF).

Back to Table of Contents

Appendix A

IOCs Featured This Week

Mass IOCs	
Source	**IOC**
ICYMI: Microsoft Tracks a Widespread Credential Phishing Campaign	The complete list of IOCs that Microsoft has identified can be found here.

Back to Table of Contents

Feedback

Please take a few minutes to send us your feedback here. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the deepwatch Threat Operations Team. Feedback should be specific to your experience with this written product to enable deepwatch to make quick and continuous improvements to these products.

Back to Table of Contents