مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malware Campaign: Operation PhantomBlu

Tracking #:432315722

Date:22-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an emerging malware campaign dubbed as “PhantomBlu”– actively targeting users globally.

TECHNICAL DETAILS:

Security researchers have uncovered a sophisticated malware campaign named "PhantomBlu" targeting various organizations worldwide. This campaign utilizes advanced techniques to deploy the NetSupport RAT through malicious Microsoft Office documents, exploiting legitimate features to evade detection. Attackers trick victims into enabling macros and double-clicking a specific element within the document, allowing for the download and installation of the RAT.

Attack Type: Phishing, Malware (NetSupport RAT)
Delivery Method: Email with a malicious Microsoft Office document (usually Word) disguised as a salary report.
Infection Vector: Macros and Object Linking and Embedding (OLE) functionality within the document.

Impact:

- Remote access to victim's machine.
- Data theft.
- Installation of additional malware.

In the PhantomBlu campaign, threat actors send phishing emails disguised as messages from an accounting service. These emails contained a password-protected Office Word file (.docx) that recipients were enticed to download under the pretense of viewing their "monthly salary report." The attackers used social engineering tactics to manipulate recipients into interacting with the malicious document.

Upon opening the attached .docx file, targets were prompted to enter a specific password and then instructed to click "enable editing" and interact with an embedded image of a printer to view their supposed "salary graph." This printer icon was actually an Object Linking and Embedding (OLE) package, a legitimate feature in Microsoft Windows that allows for embedding and linking various elements within documents.

By leveraging OLE template manipulation (Defense Evasion – T1221), the PhantomBlu campaign exploited document templates to execute malicious code without triggering traditional security measures. This sophisticated technique concealed the payload outside the document, ensuring execution only upon user interaction. Notably, this

was the first recorded instance of T1221 being used to deliver the NetSupport RAT via email, showcasing the campaign's innovative approach to evading detection and deploying malware.

INDICATORS OF COMPROMISE(IoCs):

Attached File

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Regular Backups: Implement a robust backup routine with backups stored offline and regularly tested for recoverability.
- User Awareness: Train employees to identify suspicious emails, including those from seemingly legitimate sources.
- Disable Macros: By default, disable macros in Microsoft Office documents unless absolutely necessary.
- Security Software: Keep antivirus and endpoint detection and response (EDR) solutions up-to-date.
- Application Control: Implement application control measures to restrict unauthorized software execution.
- Patch Management: Ensure timely patching of Microsoft Office and operating systems.
- Incident Response: Have a plan in place to identify, contain, and remediate security incidents.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://perception-point.io/blog/operation-phantomblu-new-and-evasive-method-delivers-netsupport-rat/