Government of India
National Critical Information
Infrastructure Protection Centre
(A Unit of NTRO)

Date: 12 Dec 2019

Advisory No: Adv/2019/Dec/001

Cyber Security Advisory: Threat Actor Winnti Group (Wicked Panda) develops a new backdoor to access MSSQL Servers

Our trusted partner reported that threat actor Winnti group has developed a malware named "Skip-2.0" that alters 'MS-SQL Server databases' and deploys a backdoor as a post-infection tool, after compromising networks. It targets specifically MS-SQL servers 11 and 12, allowing attackers to gain access on any MS-SQL account using a "magic password" that also disables the compromised machine's logging, event publishing, and audit capabilities in order to remain undetected. The backdoor may allow the attacker to stealthily copy, modify or delete the database.

IOC:The list of IoC's is attached (IOC_ Adv2019Dec001.txt).

Recommendations:

- Keep your operating system, application servers, SQL servers, browsers, browser plugins & Antivirus Software up-to-date with the latest patches.
- Maintain and actively monitor centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions.
- Create / Configure SRP's(SCSI RDMA Protocol)/ APPLOCKER based on SHA/MD5 hashes to prevent malware running them on the client machines.
- Add appropriate Host firewall rules, Active Directory structuring, and/or Group Policy settings.
- Disable the execution of MACROS in office docs, remote Desktop Connections and employ least-privileged accounts.
- Establish a Sender Policy Framework (SPF) for your domain.
- Strict External Device (USB drive) usage policy.
- Users are advised to patch their window SMB server with latest patch to avoid its exploitation.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP).
- Block the attachments of file type:
  exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|

Reference: CERT-In

Links:
https://www.bleepingcomputer.com/news/security/chinese-hackers-use-new-malware-to-backdoor-microsoft-sql-servers/ mid=1#cid=8589499
https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

Advisory No: Adv/2019/Dec/002

Cyber Security Advisory: Targeted attack via exploiting the Google Chrome zero day exploit

This data is to be considered as **TLP:AMBER**

Our trusted partner reported that Google Chrome (version 78.0.3904.87) for Windows, Mac and Linux, zero-day vulnerability (CVE-2019 -13720) is actively exploited. Attacker insert their malicious Java Script on large number of sites by compromising them, when a victim visits that site, the Java Script executes in the backend, which then loads another Java Script from remote Command and Control (C2) server controlled by attacker. This script checks the browser version of victim's machine, if it found compatible with its exploit, attacker drops the exploit payload in encrypted form on victim's machine, then it attacks the victim's machine with full remote code execution capabilities.

IOC:The list of IoC's is attached (IOC_ Adv2019Dec002.txt).

Recommendations:

- Monitor Connection attempts towards the listed domains /IP. The list may include compromised domains /IP resources as well.
- Users are advised to update their Google chrome with recent stable version.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Enforce application whitelisting on all endpoint workstations.
- Both ingress and egress traffic of the listed Domains / IP and all hash values should be kept under an active watch-list in the respective endpoints and security solutions.

Reference: CERT-In

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Advisory No: Adv/2019/Dec/003

Cyber Security Advisory: BlackRemote RAT

This data is to be considered as **TLP:AMBER**

Our trusted partner has observed a new undocumented Remote Access Trojan(RAT) named BlackRemote RAT. The malware on its detection, disables common application settings running on the targeted machine such as anti malware, firewall settings, system registry settings. The malware reported for its notorious activities is described as a powerful remote administration tool that provides full access and control over the machine, thereby monitoring and manipulating user's activity.

Analysts Notes:

The attack functionality of this malware on targeted system includes stealing personal and sensitive data. On infecting the system it has the following capabilities record screen, record videos using webcam, remote file manager, keystroke capture & remote audio.

IOC:The list of IoC's is attached (IOC_ Adv2019Dec003.txt).

Recommendations:

- Keep checking the web proxy logs for users downloading the file having MD5 from an external host using a non-standard or high TCP port.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Enforce application whitelisting on all endpoint workstations.
- Restrict execution of Power shell in enterprise environment. Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled script block logging and transcription enabled.

Reference: CERT-In

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Advisory No: Adv/2019/Dec/004

Cyber Security Advisory: APT Campaign

This data is to be considered as **TLP:AMBER**

Our trusted partner has reported an ongoing APT campaign. The exact initial mode of spreading the infection of the threat actor is not known but the domain used by the threat actor is similar to legitimate application like Microsoft, Kaspersky etc. so that it remain undetected from SIEM,IPS/IDS devices for a long duration.

IOC:The list of IoC's is attached (IOC_ Adv2019Dec004.txt).

Recommendations:

- Monitor Connection attempts towards the listed domains /IPs. The list may include compromised domains /IP resources as well.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Enforce application whitelisting on all endpoint workstations.
- Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled script block logging and transcription enabled.
- Enable code signing feature for all types of users in Power script so that only signed script will execute in Power shell and practice "least privilege" of access.
- Segment the critical networks and vulnerable or hard to secure systems from the rest of the network intelligently to restrict the lateral movement.

Reference: CERT-In

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Advisory No: Adv/2019/Dec/005

Cyber Security Advisory: EMOTET now comes disguised as a "SOC WEEKLY REPORT "

This data is to be considered as **TLP:AMBER**

Our trusted partner observed that Emotet Trojan is using a new attack in which the malware is spread via a fake SOC"weekly report". The victim receives a specially crafted email from grecia[@]ambientehomedecor[.]com, containing a highly obfuscated Microsoft Word document disguised as a SOC weekly report titled "SOC report 10 12 2019.doc". In order to persist itself on the compromised system, Emotet launches a local service named "khmerdefine", adds it in c:\Windows\SysWOW64 and creates a system service in autorun. Post execution, the Trojan gathers a range of information from the infected device, seeks the local public IP address by querying an external resource and transfers all the collected data to its Command-and-Control (C2) server.

Analyst's Notes:

The attackers adopted this approach because the target organization is protected by a SOC and receiving the SOC weekly report would not arouse suspicion in the minds of the recipients. Emotet is a banking Trojan malware program which gathers financial information by injecting computer code into the networking stack of an infected computer, thereby allowing sensitive data to be stolen via transmission. The malware also inserts itself into software modules which are then able to steal address book data and perform Denial of Service(DoS) attacks on other systems.

IOC: The list of IoC's is attached (IOC_ Adv2019Dec005.txt).

Recommendations :

- Monitor Connection attempts towards the listed domains /IPs. The list may include compromised domains /IP resources as well.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution. Majority of the infection vectors are primarily introduced via phishing emails.
  - Deploy anti-spam solutions which prevent delivery of unsolicited bulk emails and support screening of specific type of files (e.g. MS-Office docs, PDFs, RTFs archives etc.) and detect the presence of binaries / scripts for all incoming emails with attachments.
- Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints.

Reference: CERT-In

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430