ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 1/21 (September)

Introduction

1 Over the last month, ACICE continued to observe significant levels of activity across cyberspace from a variety of actors, ranging from Advanced Persistent Threats (APTs) to cyber-criminals.

APT Trends

2 Southeast Asian (SEA) telecommunications providers (telcos) continued to be victims of cyber espionage from state-sponsored APTs. At least five major SEA telcos were compromised. The attacks compromised the telcos' Call Data Records (CDR), billing systems, and Microsoft Exchange servers, with the earliest intrusion dating back to 2017. Separately, US and Israeli based employees of aerospace, defence, IT and communications sector firms became victims of sophisticated social engineering campaigns, which leveraged recruitment platforms such as LinkedIn.

3 Ransomware. Ransomware continued to proliferate, with the global attack volume reportedly increasing by 151% in the first six months of this year.

a. Targets. There is an emerging trend of downtime-sensitive targets, such as hospitals, being targeted. Reports note that 48% of US hospitals have disconnected their networks in the past six months due to ransomware.

b. New Ransomware Variants. On 5 Aug, Australian Cyber Security Centre (ACSC) warned of an increase in Lockbit 2.0 ransomware attacks targeting Australian organisations. Unique to Lockbit 2.0 is its engagement of company insiders to plant ransomware within corporate networks.

c. New Cyber-Criminal Group. A cyber-crime group called Altdos is reportedly breaching firms across SEA to deploy ransomware. Pressure tactics the group typically adopts include: (i) the use of "hack and leak" extortion, to leak businesses' sensitive data on dark web sites unless ransom is paid, as well as (ii) Distributed Denial of Service (DDoS) attacks against victims.

Critical Information Infrastructure Targeting

4 Governments and telcos worldwide continued to be victims of cyber attacks. On 21 Aug, it was reported that a US Government Department was breached, although it is currently not known what information was stolen. Separately, on 15 Aug, a threat actor claimed to have hacked T-mobile's servers, stealing databases containing the personal data of approximately 100 million customers. One such database was apparently sold on the Dark Web for six bitcoin (~ USD$280,000), containing birth dates, license numbers, and social security numbers for 30 million people.

Notable Vulnerabilities

5 Several software vulnerabilities were recently disclosed in Windows and Microsoft products, as well as Internet-of-Things (IoT) devices.

a. Windows. Plugging in a Razer mouse, keyboard, or any device that used the Razer Synapse utility provided the threat actor with admin privileges to a Windows 10 system. This vulnerability is currently not known to have been exploited yet.

b. Microsoft. Zero-day vulnerabilities were found in Microsoft's Windows Print Spooler service, and firewall. These respectively enabled attackers to run arbitrary code with system privileges; as well as elevate privileges and infiltrate organisations through intranet locations. Separately, threat actors are now reportedly exploiting Microsoft Exchange servers using the ProxyShell vulnerability to install backdoors.

c. IoT Devices. Vulnerabilities in IoT devices continued to proliferate. Threat actors exploited critical authentication bypass vulnerabilities in home routers installed with the Arcadyan firmware to deploy Mirai malware, in order to harness the compromised routers in a botnet.

Contact Details

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

....

ANNEX A

News Articles

1 Five Southeast Asian Telcos Hacked
[Link: https://therecord.media/five-southeast-asian-telcos-hacked-by-three-different-chinese-espionage-groups/]

2 Defense Contractor Lured in Catfishing-Malware Scam
[Link: https://threatpost.com/iranian-apt-defense-contractor-catfish/168332/]

3 Govt Hackers Impersonate HR Employees to Hit Israeli Targets
[Link: https://www.bleepingcomputer.com/news/security/govt-hackers-impersonate-hr-employees-to-hit-israeli-targets/]

4 Ransomware Volumes Hit Record Highs as 2021 Wears on
[Link: https://threatpost.com/ransomware-volumes-record-highs-2021/168327/]

5 Half of US Hospitals Shut Down Networks Due to Ransomware
[Link: https://www.infosecurity-magazine.com/news/half-us-hospitals-shut-networks/]

6 Angry Conti Ransomware Affiliate Leaks Gang's Attack Playbook
[Link: https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/]

7 Australian Government Warns of Escalating Lockbit Ransomware Attacks
[Link: https://www.bleepingcomputer.com/news/security/australian-govt-warns-of-escalating-lockbit-ransomware-attacks/]

8 ALTDOS Hacking Group Wreaks Havoc across Southeast Asia
[Link: https://therecord.media/altdos-hacking-group-wreaks-havoc-across-southeast-asia/]

9 U.S. State Department Recently Hit by a Cyber Attack - Fox News
[Link: https://www.reuters.com/world/us/us-state-department-recently-hit-by-cyber-attack-fox-news-2021-08-21/]

10 Hacker Claims to Steal Data of 100 Million T-Mobile Customers
[Link: https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-data-of-100-million-t-mobile-customers/]

11 Razer Bug Lets You Become a Windows 10 Admin by Plugging in a Mouse
[Link: https://www.bleepingcomputer.com/news/security/razer-bug-lets-you-become-a-windows-10-admin-by-plugging-in-a-mouse/]

12 Google Publishes Zero-Day Vulnerability in Windows Firewall and App Container Affecting Every Version, Patch Not Available
[Link:https://www.securitynewspaper.com/2021/08/20/google-publishes-zero-day-vulnerability-in-windows-firewall-and-appcontainer-affecting-every-version-patch-not-available/]

13 Microsoft Confirms another Windows Print Spooler Zero-Day Bug
[Link: https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-another-windows-print-spooler-zero-day-bug/]

14 Actively Exploited Bug Bypasses Authentication on Millions of Routers
[Link: https://www.bleepingcomputer.com/news/security/actively-exploited-bug-bypasses-authentication-on-millions-of-routers/]

....