COLORTOKENS

THREAT RESEARCH

Cyber Attacks Targeting Australian Organizations

What Happened?

On 19th June, 2020, Australia Prime Minister Scott Morrison said, “Australia’s government and institutions are being targeted by ongoing sophisticated state-based cyber hacks”. He declined to identify a specific state actor and said no major personal data breaches had taken place.

This type of cyber hack is called ‘copy-paste compromises’. The title is derived from the threat actor’s heavy use of proof-of-concept exploit code, web shells and other tools copied almost identically from open source.

Who Has Been Targeted?

Although the government did not name specific cases, they said that the cyber hack had spanned “government, industry, political organizations, education, health, essential service providers and operators of other critical infrastructure”.

However, incidents were reported across major Australian firms including steel maker BlueScope, logistics firm Tol Group, and state government agency Services New South Wales.

In addition, the Australian Cyber Security Centre (ACSC) has mentioned that Advanced Persistent Threat (APT) actors are actively targeting health sector organizations and medical research facilities such as Covid-19 essential services.

What Techniques Are Used?

Initial Access- Exploiting vulnerabilities (CVE-2019-18935, CVE-2019-19781, CVE-2019-0604 & Exploitation of VIEWSTATE handling in Microsoft IIS Servers) in public facing websites and by sending Spear Phishing emails to gain credentials

Execution- Multiple PowerShell and used various scripts like jscript, .net, macros to execute payloads

Privilege Escalation- Using RottenPotato/JuicyPotato family of exploits to escalate privileges

Defense Evasion- Evading security tools by using dl hijacking, software packing methods

Credential Access- using ProcDump/ Ntdsutil to dump LSASS which is staged for exfiltration to steal credentials

Lateral Movement – Accessing windows admin shares, Using WinRM via PowerShell to move laterally through network

Command & Control- Utilized web shells as a SOCKS proxy to facilitate the tunneling of SMB traffic; also HTTP/HTTPS web shell traffic as primary usage of C2

Exfiltration- Exfiltrating using C2 and non C2 channels (Internet accessible locations)

Impact- No use of any Impact techniques were identified by the ACSC during its investigations related to this campaign.

How Are The Attacks Staged?

Initial Access

- Attacker has gained initial access by exploiting mentioned vulnerabilities on public facing servers
  - Exploitation of Telerik UI CVE-2019-18935
  - Exploitation of VIEWSTATE handling in Microsoft IIS Servers
  - Exploitation of Citrix Products CVE-2019-19781
  - Exploitation of Microsoft SharePoint CVE-2019-0604
  - Attacker also used Spear Phishing attacks with links to credential harvesting websites to steal Office 365 credentials
- Once initial access is achieved, the actor utilized a mixture of open source and custom tools to persist on, and interact with, the victim network
- Legitimate remote accesses using stolen credentials
- Compromised legitimate Australian web sites were identified as command and control (C&C) servers.

Execution

Once initial access is achieved, the threat actor utilized a mixture of open source and custom tools to persist on, and interact with, the victim network:

- Using Windows tools at.exe and schtasks.exe to execute software on remote hosts as a means of lateral movement and remote data collection
- Command line interface to execute commands like "C:\Windows\system32\cmd.exe /c powerShell.exe –exec bypass –c " to have reverse shell created , "DisableActivitySurrogateSelectorTypeCheck" to have .NET deserialization will succeed
- Usage of various scripts languages like Jscript, .net, macros, etc
- Execution through API
- Cmd.exe spawned PowerShell .exe to create reverseShell

How Are You Protected With ColorTokens solutions?

1. Xprotect's protection levels have been enhanced by updating Security profiles to block execution of unwanted scripts/processes such as JScript/macros/.NET and others.
2. Advanced Rule rings are implemented to stop misuse of processes such as 'cmd.exe spawning PowerShell.exe'
3. Xshield ensures the impact radius is minimized through enforced policies.
4. Our Threat Intelligence is consistently updated with identified IOCs of hash, IP and Domains.
5. This provides real-time protection to customers from any such known attacks.
6. Our round-the-clock Breach Protection Service experts are continuously monitoring and detecting attack patterns and suspicious behaviours related to this threat e.g. usage of suspicious commands, suspicious behaviour on execution of authorized and whitelisted processes etc.

References

https://www.cyber.gov.au/acsc/view-al -content/alerts/copy-paste-compromises
https://www.cyber.gov.au/acsc/view-al -content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks
https://www.abc.net.au/news/2020-06-19/why-would-china-launch-cyber-attack-against-australia/12374990
https://www.bbc.com/news/world-australia-46096768
https://www.cyber.gov.au/acsc/view-al -content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks