Copy-paste compromises

cyber.gov.au/acsc/view-all-content/alerts/copy-paste-compromises

The Australian Government is aware of, and responding to, a sustained targeting of Australian governments and companies by a sophisticated state-based actor. The title ‘Copy-paste compromises’ is derived from the actor’s heavy use of tools copied almost identically from open source.

Alert status

HIGH

The Australian Government is aware of, and responding to, a sustained targeting of Australian governments and companies by a sophisticated state-based actor.

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

The actor has been identified leveraging a number of initial access vectors, with the most prevalent being the exploitation of public-facing infrastructure — primarily through the use of remote code execution vulnerabilities in unpatched versions of Telerik UI. Other vulnerabilities in public-facing infrastructure leveraged by the actor include exploitation of a deserialisation vulnerability in Microsoft Internet Information Services (IIS), a 2019 SharePoint vulnerability and the 2019 Citrix vulnerability.

The actor has shown the capability to quickly leverage public exploit proof-of-concepts to target networks of interest and regularly conducts reconnaissance of target networks looking for vulnerable services, potentially maintaining a list of public-facing services to quickly target following future vulnerability releases. The actor has also shown an aptitude for identifying development, test and orphaned services that are not well known or maintained by victim organisations.

When the exploitation of public-facing infrastructure did not succeed, the ACSC has identified the actor utilising various spearphishing techniques. This spearphishing has taken the form of:

- links to credential harvesting websites
- emails with links to malicious files, or with the malicious file directly attached
- links prompting users to grant Office 365 OAuth tokens to the actor
- use of email tracking services to identify the email opening and lure click-through events.

Once initial access is achieved, the actor utilised a mixture of open source and custom tools to persist on, and interact with, the victim network. Although tools are placed on the network, the actor migrates to legitimate remote accesses using stolen credentials. To successfully respond to a related compromise, all accesses must be identified and removed.

In interacting with victim networks, the actor was identified making use of compromised legitimate Australian web sites as command and control servers. Primarily, the command and control was conducted using web shells and HTTP/HTTPS traffic. This technique rendered geo-blocking ineffective and added legitimacy to malicious network traffic during investigations.

During its investigations, the ACSC identified no intent by the actor to carry out any disruptive or destructive activities within victim environments.