MDR CYBER
Part of the Mishcon de Reya Group

May 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

May 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
Exploitation of vulnerability in the GlobalProtect feature of Palo Alto Networks "PAN-OS".	Likely state-sponsored attacker used sophisticated techniques and stole data but proof of concept code is available to a wider range of threat actors.	Apply Palo Alto hotfixes, read and actions advisory, enhance detection, and respond swiftly to mitigate attack impacts.
Attackers compromise Dropbox e-signature platform known as Dropbox Sign	Unidentified threat actors were able to gain unauthorized access to the e-signature platform and acquired customer information.	Reset all passwords used, register authenticator applications again. Deploying enhanced monitoring tools to alert on patterns of anomalous behaviour.

Preparing decision makers

Our monthly report prepares cybersecurity practitioners to make better tactical, operational and strategic decisions. We have distilled analysis of key events from the previous month which have learning points that can be actioned to improve security.

The document has three main purposes to assist cybersecurity leaders:

1. To be 'threat-led' and help prioritise defences against particular types of attackers
2. To justify business decisions on cybersecurity changes, technology or services
3. To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Severe vulnerability in Palo Alto VPN product fixed but still actively exploited

What?

On 10 April 2024, Volexity detected a zero-day exploit targeting a vulnerability in the GlobalProtect feature of Palo Alto Networks "PAN-OS". At the time of writing, there were an increasing number of attacks exploiting this vulnerability. Proof of concepts for this vulnerability were publicly disclosed by third parties, meaning they are easily available for attackers.

Alerts for suspicious network traffic led to the discovery that a device that had been compromised. The next day, a similar breach occurred at another customer's firewall by the same threat actor, known as UTA0218. This actor was able to remotely exploit the firewall, create a reverse shell, and download additional tools to aid in their attack, focusing on exporting configuration data and moving laterally within the organisations.

Volexity and Palo Alto Networks identified the vulnerability as an OS command injection issue, identified as CVE-2024-3400 with a CVSS score of 10.0, the highest possible, underlining its severity. Palo Alto Networks issued an advisory and released a threat protection signature.[1] Around 14 April, Palo Alto started releasing out-of-normal-workflow "hotfixes" for the flaw.[2]

Volexity's further investigation revealed that the exploitation dated back to 26 March 2024, with the threat actor testing the vulnerability and later successfully deploying malicious payloads. UTA0218 also attempted to install a custom Python backdoor named UPSTYLE, which allows command execution via crafted network requests.

The scale of the exploitation was not fully known, but evidence suggests both targeted and reconnaissance activities. On 12 April, a security researcher found over 82,000 PAN-OS devices exposed online and vulnerable to the attacks.[3]

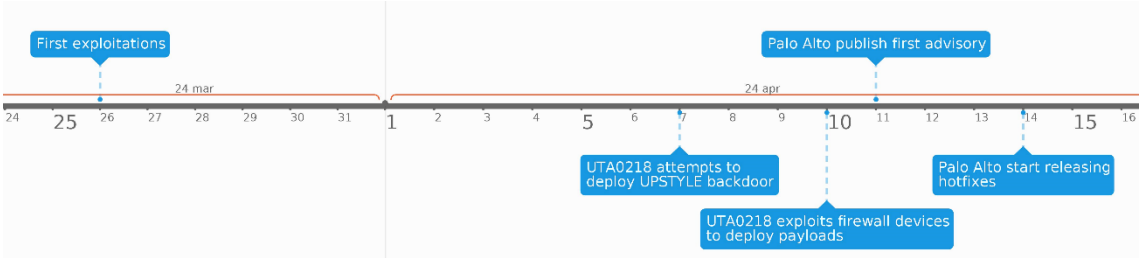

Figure 1 - Timeline of events

[1] Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400), https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

[2] CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect, https://security.paloaltonetworks.com/CVE-2024-3400

[3] https://twitter.com/nekono_naha/status/1778716137582457301

So what?

The exploitation of this vulnerability by UTA0218 indicates a highly skilled and resourceful threat actor, likely state-backed, given the sophistication of the attack. The actor's objectives included stealing domain and Active Directory credentials, browser data, and DPAPI keys, which could enable prolonged access to victim networks.

Volexity's analysis of the incidents involved zero-day exploitation, the development of a novel backdoor, and lateral movement within affected networks. Incidents included use of the UPSTYLE backdoor and post-exploitation activities, including the establishment of persistence and data theft.

However, proof of concepts for exploitation were available, meaning that this attack method was available to a wider range of threat actors with motives that almost certainly include financial gain.

Organisations using Palo Alto Networks GlobalProtect firewall devices are strongly advised to read the advisory, apply the hotfixes, and ensure their devices are protected or take mitigation actions. Volexity has also provided guidance on detecting compromise and responding to breaches. Robust detection capabilities and quick responses to these kinds of incidents are crucial to mitigate the impact of such attacks.

Dropbox Sign e-signature platform compromised and data stolen

What?

On 24 April 2024, the cloud file sharing provider Dropbox became aware that an unauthorised access had been made into their e-signature's production platform known as Dropbox Sign. The threat actor accessed customer information such as phone numbers, email addresses, usernames and multi-factor authentication, however no other Dropbox products were impacted. [4] The scale of the compromise was not known at the time of writing.

A service account of the e-signature platform was used as point of entry, the service account was part of the platform's back end which is a type of non-human account used for running automated tasks and executing applications. The account had privileges necessary to perform a variety of tasks in the production environment of the e-signature platform.[5]

Users who signed documents through this platform but did not have their accounts created, also had their username and email exposed. Dropbox confirmed that no customer content such as documents or payment information was not part of the unauthorized access.[6]

So what?

At the time of review, the breach was still being investigated. Victims were at an elevated risk of fraud and phishing attempts. Dropbox Sign users are urged to reset passwords , use a password manager to generate long and complex passwords and re-register multi-factor authentication apps for the Dropbox service.[7]

The breach highlights the need for a multi-faceted approach to cybersecurity, combining employee education, technical controls, and proactive monitoring. The following countermeasures are recommended to bolster security and prevent future compromises.

- Effective incident response planning: A clear and practiced incident response plan is essential for a swift and coordinated response to security incidents. This should include not only technical support, but legal and if necessary public communications.
- Regular security training for employees: regular, comprehensive training sessions should be conducted to educate employees on the latest phishing tactics and the critical role individuals play in maintaining security.
- Adoption of Multi-Factor Authentication (MFA): Where possible, MFA should be a standard requirement for accessing any sensitive systems to provide an additional

[4]Dropbox says hackers stole customer data, auth secrets from eSignature service
https://www.bleepingcomputer.com/news/security/dropbox-says-hackers-stole-customer-data-auth-secrets-from-esignature-service/
[5]A recent security incident involving Dropbox Sign
https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign
[6]Dropbox warns about a Dropbox Sign breach
https://www.kaspersky.co.uk/blog/dropbox-sign-breach/27548/
[7]Mitigating the Risk of Software Supply Chain Attacks: Insights From the Dropbox Sign Breach
https://www.kiteworks.com/cybersecurity-risk-management/dropbox-sign-breach/

security layer beyond passwords, including third party cloud services such as Dropbox Sign.

- Periodic security audits and penetration testing: Organisations should deploy proactive measures to test organisational security to identify and remediate security gaps before they can be exploited by malicious actors.
- Rigorous access control policies: Access to critical systems should be tightly controlled and regularly reviewed to ensure that only necessary personnel have access.
- Monitor systems: Configure security tools to detect unusual patterns of behaviour and potential security breaches early on. This is most effective when supported by continual threat intelligence.
- Maintain open communication and collaboration with third parties: Organisations should regularly communicate with vendors to address security issues and collaborate on reducing supply chain risks.

MDR CYBER
Part of the Mishcon de Reya Group

The Traffic Light Protocol (TLP) is a set of designations used to ensure that senstive information is shared with the appropriate audience.

This document is marked TLP:GREEN meaning recipients may share with peers and partner organizations within their sector or community, but not via publicly accessible channels.