APT 18

APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.

Wekby was described by Palo Alto Networks in a 2016 report as: ‘Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of Hacking Team’s Flash zero-day exploit.’

The Wekby APT group, implicated in a number of targeted attacks against health care organizations such as Community Health Systems and major pharmaceutical companies, is reportedly making use of the Adobe Flash Player zero-day found in the Hacking Team data dump.

According to Virginia-based security company Volexity, spear phishing messages purporting to be from Adobe have been found spreading a modified version of the Hacking Team exploit that affects Flash Player versions up to 18.0.0.194. Labels found in the code, in fact, refer to Hacking Team, the company said.

Internal emails, sales invoices and other documents leaked since the breach was made public implicate Hacking Team in selling exploits and intrusion software to oppressive governments and sanctioned countries.

The spear phishing message found by Volexity urges the victim to download and install an updated version of Flash and includes a link to http://get[.]adobe[.]com that instead redirects the recipient to a site hosted by PEG TECH Inc. The site loads a malicious .swf file exploiting the Flash vulnerability patched yesterday by Adobe.

ID: G0026

Associated Groups: TG-0416, Dynamite Panda, Threat Group-0416

Version: 2.1

Created: 31 May 2017

Last Modified: 30 March 2020

Techniques 1

ID: T1133

Sub-techniques: No sub-techniques

Tactics: Persistence, Initial Access

Platforms: Containers, Linux, Windows

Permissions Required: User

Data Sources: Application Log: Application Log Content, Logon Session: Logon Session Metadata, Network Traffic: Network Traffic Flow

CAPEC ID: CAPEC-555

Contributors: Alfredo Oliveira, Trend Micro; Ariel Shuper, Cisco; Brad Geesaman, @bradgeesaman; Daniel Oakley; David Fiser, @anu4is, Trend Micro; ExtraHop; Idan Frimark, Cisco; Jay Chen, Palo Alto Networks; Magno Logan, @magnologan, Trend Micro; Rory McCune, Aqua Security; Travis Smith, Tripwire; Vishwas Manral, McAfee; Yossi Weizman, Azure Defender Research Team; Yuval Avrahami, Palo Alto Networks

Version: 2.2

Created: 31 May 2017

Last Modified: 22 April 2021

External Remote Services

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.

Access to Valid Accounts to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.[1] Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard

APT18 actors leverage legitimate credentials to log into external remote services

Techniques 2

ID: T1078

Sub-techniques: T1078.001, T1078.002, T1078.003, T1078.004

Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

Platforms: Azure AD, Containers, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS

Permissions Required: Administrator, User

Effective Permissions: Administrator, User

Data Sources: Logon Session: Logon Session Creation, User Account: User Account Authentication

Defense Bypassed: Anti-virus, Application control, Firewall, Host intrusion prevention systems, Network intrusion detection system, System access controls

CAPEC ID: CAPEC-560

Contributors: Mark Wee; Netskope; Praetorian; Yossi Weizman, Azure Defender Research Team

Version: 2.2

Created: 31 May 2017

Last Modified: 12 April 2021

Valid Accounts

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.

APT18 actors leverage legitimate credentials to log into external remote services.

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/22cb049e-ad3b-4c28-896d-2eea182a9bac/(Stuxnet).pdf

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/beea537f-bb30-4004-94a8-d26c7a72f51c/APAC13_Ihn-Hyuk._Song.pdf

https://attack.mitre.org/groups/G0026/

https://www.venafi.com/blog/infographic-how-an-attack-by-a-cyber-espionage-operator-bypassed-security-controls

https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/