



CYBER THREATS TO THE ENTERTAINMENT AND MEDIA INDUSTRIES

ENTERTAINMENT AND MEDIA COMPANIES FACE CYBER THREATS FROM THE FOLLOWING ACTORS:

- Advanced Persistent Threat (APT)¹ groups assisting their sponsoring government in controlling its national image by stealing information related to media organizations' reporting activities, including personnel, sources, local partnerships, anticipated public releases, general country operations, and specific areas of research.
- APT groups engaging in economic espionage to provide their indigenous entertainment and media companies with a competitive advantage through stealing data related to other companies' mergers, acquisitions, or distribution; technologies or processes for advanced production; and creative intellectual property.
- Hacktivists and APT groups seeking to disrupt a victim company's operations to promote a cause, control reporting, or contain the dissemination of content that they consider politically sensitive or controversial. APT groups may potentially try to mask the identity of their government sponsor by posing as an independent hacktivist group when targeting a victim company.
- Enterprise-like cybercriminals seeking personal profit through targeting the gaming industry and stealing account credentials, activation codes, in-game valuables, and personally identifiable information (PII).

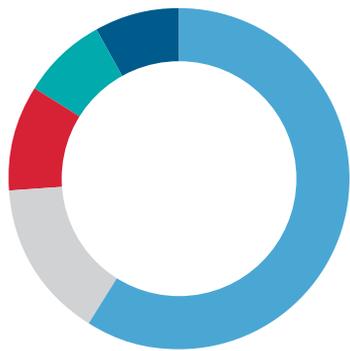
CASE STUDY: APT28 SUSPECTED IN FALSE FLAG OPERATION ON FRENCH MEDIA COMPANY

In April 2015, threat actors compromised TV5 Monde, a French news station with a global audience. The actors damaged equipment, disrupting broadcasts for several hours, and defaced the company's website and social media accounts with propaganda pertaining to ISIS and the CyberCaliphate, a hacktivist group allegedly associated with ISIS. However, although the activity initially appeared to be the work of the CyberCaliphate,

WE HAVE OBSERVED AT LEAST 17 ADVANCED THREAT GROUPS COMPROMISE COMPANIES IN THESE SUBSECTORS:

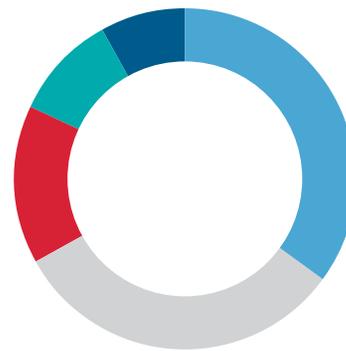
- Entertainment & Games Software
- Diversified Entertainment
- Information Collection & Delivery
- Internet Publishing, Broadcasting & Search Portals
- Magazine Publishers
- Multimedia, Graphics & Publishing Software
- Newspaper Publishers
- Television Station Groups

¹ Advanced Persistent Threat (APT) actors are assessed to take direction from a nation state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.



TOP 5 MALWARE FAMILIES

- 59% ChinaChopper
- 15% SOGU (aka Kaba)
- 10% Gh0stRAT
- 8% PoisonIvy
- 8% Page



TOP 5 CRIMEWARE FAMILIES

- 35% Upatre
- 32% Delf
- 15% ZeroAccess (aka SIREFEF)
- 10% Allapple
- 8% Muxif

FireEye Threat Intelligence suspects that APT28, a group associated with the Russian government, was instead responsible for the activity. APT28 likely posed as the CyberCaliphate to capitalize on Western fears over Islamic extremism, particularly following the Charlie Hebdo-inspired attacks of several months prior. The compromise of TV5 Monde was likely a Russian information operation intended to alarm the French, with whom Russia's relations have been declining (as with the rest of the West), and draw the West's attention away from Russia's ongoing role in the Ukraine crisis and towards the threat of terrorism in the Middle East.

THREAT HORIZON & INDUSTRY OUTLOOK

The entertainment and media industries play a key role in shaping public opinion and even national image, making it a valuable target for APT groups and hacktivists seeking influence. The following factors may further influence threat activity towards these sectors:

- Concerns over domestic stability and government legitimacy will likely result in increased targeting from APT groups seeking to assist their associated government in monitoring public opinion, shaping its image, promoting its message, and otherwise leveraging its soft power to maintain and spread its influence.
- A desire to discourage publication of controversial stories and views may prompt some threat actors to attempt to gain access to a relevant media organization's raw reporting and acquire information on the identities of its sources. State-sponsored threat actors aiming to suppress a certain story, for example, may target a media organization reporting on the topic in an effort to evaluate what the organization knows about the issue, and identify its sources.
- Efforts to intimidate or punish a media organization for publishing a critical or unflattering story might prompt the threat actors to retaliate by targeting the offending media organization. Threat actors may steal data on employees and sources

DATA STOLEN FROM ENTERTAINMENT & MEDIA COMPANIES

- Address Books
- Calendar Files
- Executive Communications
- Negotiations Information
- Network Infrastructure Documents
- PR and Marketing Materials
- Reporters' Communications
- User Credentials

in an effort to intimidate or monitor them. There is also the possibility that threat actors may try to steal and then publicly release sensitive data, in an attempt to embarrass the targeted organization and damage its credibility.

- Tensions or conflicts between adversaries, whether state or non-state, will probably lead to increased threat activity from associated threat actors aiming to prevent their adversary from spreading its own message or propaganda, while potentially seeking to spread its own propaganda through its opponents' channels.

- Increased popularity and use of social media will likely lead to continued targeting of providers and platforms by APT groups, cybercriminals, and hacktivists aiming to facilitate further targeting through social engineering, and/or promote their own views through disrupting services or defacing webpages.

TOP MALWARE FAMILIES		
<p>TOP MALWARE FAMILIES</p> <p>FireEye most frequently detected threat actors using the following targeted malware families to compromise organizations in the entertainment and media sectors:</p>	ChinaChopper	is a small webshell that provides threat actors unauthorized access to an information system using a simple password for authentication and is capable of executing Microsoft .NET code within HTTP POST commands.
	SOGU	(aka Kaba, PlugX), a backdoor that is capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the command and control (C2) server with graphical access to the desktop.
	GHOSTRAT	is a remote access tool (RAT) derived from publicly available source code. It can perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs, and create, manipulate, delete, launch, and transfer files.
	POISONIVY	is a publicly available RAT that provides comprehensive remote access capabilities on a compromised system. Its variants are configured, built, and controlled using a graphical Poison Ivy management interface available online. It can be configured to produce shellcode, which can be packaged into an executable or combined with an existing executable to hide its presence. It is typically configured to inject multiple shellcode stubs into the explorer.exe process.
	Page	(aka ELISE) is a downloader that attempts to retrieve encoded DLLs from a pre-configured command and control server, which it communicates with using HTTP requests. Once the DLLs are downloaded, the downloader loads them into memory. It also incorporates several source-level anti-reverse engineering functions.
TOP CRIMEWARE FAMILIES		
<p>TOP CRIMEWARE FAMILIES</p> <p>FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the entertainment and media sectors:</p>	Upatre	is a Trojan downloader that often arrives via a spam email, drive-by download or exploit. Upatre will download one or more additional types of malware onto an infected system and has been observed distributing a wide variety of malware including, but not limited to, Zbot, Dyre, Rovnix, CryptoLocker, and Necurs.
	Delf	is a family of Trojans whose files are often compiled in Delphi. It has the ability to connect to remote server for downloading and installing additional malware onto the system without the consent or knowledge of the user and may also have the ability to steal sensitive information.
	ZeroAccess	(aka SIREFEF) is a Trojan with advanced rootkit capabilities. Initially developed as a delivery mechanism for other types of malicious software, it has been re-architected to perform click fraud.
	Allapple	is a worm that will perform denial of service attacks on specific targets and attempt to propagate to other systems on the same network.
	Muxif	is a Trojan downloader that communicates with a C2 server to send system information, receive instructions, and download additional malicious executables. It also modifies the registry to maintain persistence.