Confidential

Cyber Threats

Monthly Cyber Intelligence Summary

October 2024

Mishcon de Reya

It's business. But it's personal.

October 2024 - Cyber Threat Update

Summary

Incident	Threat	Key points
Notorious financially motivated "FIN7" cybercrime group use adult deepfake generators to spread infostealer malware	Users seeking out the software were directed to download malicious software disguised a legitimate browser extension. The malware is used to steal credentials for use in other attacks including ransomware.	Ensure employees are trained to understand the threats, use web filtering to block known bad sites, up-to-date antivirus, and enforce strong password policies.
Malicious insider behind ideologically-motivated cyber attack on Network Rail Wi-Fi Services	UK Railway's Wi-Fi page was compromised, and users directed to Islamophobic messages, an ISP insider was suspected and arrested.	Implement and/or review preventative measures such as user access controls. Have an incident response plan in place to deal with insider incidents including legal and communications strategies.

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.

1. The document has three main purposes to assist cybersecurity leaders:
2. To be 'threat-led' and help prioritise defences against particular types of attackers
3. To justify business decisions on cybersecurity changes, technology or services

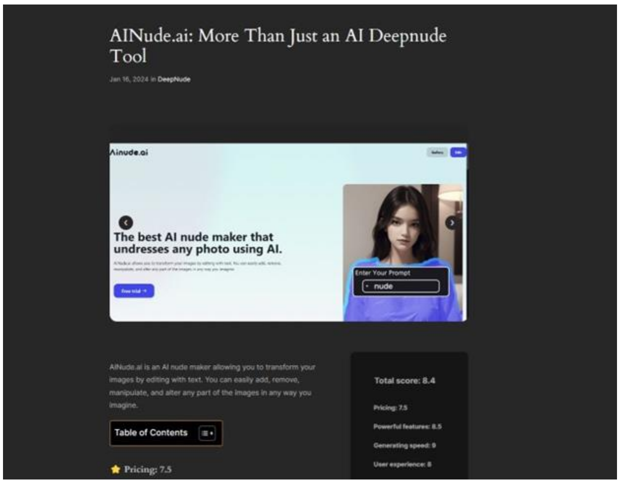
To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Deepfake nude generator sites spread malware

What happened?

On 2nd October 2024, researchers discovered that the notorious financially motivated cybercrime group known as "FIN7" had created several "AI Deepnude generator" websites serving infostealer malware to visitors.[1] The malware is designed to covertly take information from users such as usernames and passwords, for use in other attacks.

Users were lured to the sites, seeking the software to generate adult-themed images, and then encouraged to download the generator through the site or by signing up for a "free trial". The actions led to downloading of the "Lumma" and "Redline" information stealing malware.



AINude.ai: More Than Just an AI Deepnude Tool

Jan 16, 2024 in DeepNude

The best AI nude maker that undresses any photo using AI.

Enter Your Prompt

nude

AINude.ai is an AI nude maker allowing you to transform your images by editing with text. You can easily add, remove, manipulate, and alter any part of the images in any way you imagine.

Total score: 8.4

Pricing: 7.5

Powerful features: 8.5

Generating speed: 9

User experience: 8

Figure 1 - FIN7 deepfake malware site (source: Silent Push)

FIN7 have also been observed promoting a malvertising campaign which targeted corporate users with lures that include popular brands such as Thomson Reuters, SAP Concur and others. These campaigns typically spread the NetSupport Remote Access Trojan (RAT) which allowed operators to gain unauthorised control of infected devices. In these campaigns, users were asked to download a fake browser extension which deployed the malware.

The group have been active since at least 2013, and target a wide range of sectors including retail, technology, financial services and others. The group are widely assessed as one of the most successful cybercrime groups in the world and have been associated with the ALHV/BlackCat ransomware, and a high number of data breaches. Three alleged members of the group were also indicted in the US in 2018.[2]

The recent findings show that FIN7 has expanded its operations, targeted a wide range of industries and used sophisticated tactics to lure victims into downloading malicious software that can lead to credential theft and ransomware attacks.

[1] FIN7 hosting honeypot domains with malicious AI DeepNude Generators – New Silent Push research, https://www.silentpush.com/blog/fin7-malware-deepfake-ai-honeypot/

[2] Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies, https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

So what?

The implications of FIN7's activities are instructive for organisations, as they risk having their employees inadvertently compromise security by downloading these malicious files. The malware used by FIN7 includes information stealers and Remote Access Trojans (RATs), which can lead to further exploitation such as ransomware deployment. The group have used deceptive techniques, such as masquerading as legitimate software and using encrypted archives to evade detection. They have also been observed using search engine optimisation (SEO) tactics to spread their malware more effectively.

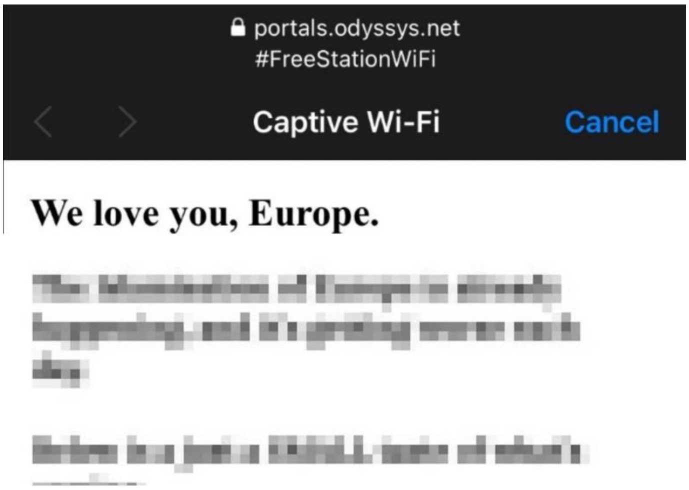
There are several steps that businesses can take to avoid employees inadvertently downloading malware from websites. Essential steps include cybersecurity training for employees to understand and recognise threats and web filtering, which automatically blocks access to known malicious sites.Similarly, the use of up-to-date antivirus, and enforcing strong password policies are helpful to mitigate these kinds of attacks.

The Indicators of Compromise (IOCs) for proactive threat hunting are available in the Appendix.

Network Rail Wi-Fi cyber attack underlines insider threat

What happened?

On 25th September 2024, the British Transport Police (BTP) responded to a cyber incident affecting public Wi-Fi services at 19 mainline railway stations across the UK. Passengers attempting to connect to Network Rail's Wi-Fi, managed by Telent, were greeted with Islamophobic messages instead of the usual login page. [3]



We love you, Europe.

Figure 2 - Pixellated snippet of the message (source: Em360tech)

The BTP's swift investigation led to the arrest of a Global Reach Technology employee, the service provider for the Wi-Fi network, under suspicion of offences related to the Computer Misuse Act 1990 and the Malicious Communications Act 1988. The cyber-attack, which involved an unauthorised modification to the

[3] Admin account blamed for rail terror message hackhttps://www.bbc.co.uk/news/articles/cr75znv47xpo

Wi-Fi service's landing page, was contained to the defacement of splash pages, with no personal data reported as compromised. [4]

So what?

The Incident involving Network Rail's Wi-Fi service highlights the persistent threat of malicious insiders, which can range from deliberate acts of sabotage to negligent behaviour that compromises security.[5]

The BTP's findings suggests that the attack was an isolated incident of cyber vandalism rather than a coordinated assault on the UK's critical infrastructure. However, the potential for damage from such insider threats is considerable, affecting not only IT systems but also reputation and trust of service providers and their customers.

Organisations can take several measures to mitigate the risk of insider threats:

- **Implement strict access controls**: Limit access to critical systems and regularly review user privileges.
- **Conduct regular security audits**: Regularly audit systems for unauthorised changes, especially on public-facing interfaces.
- **Monitor employee activity**: Use behavioural analytics to monitor for signs of unusual or unauthorised activity.
- **Educate employees**: Provide ongoing cybersecurity training to help employees recognise and prevent security breaches.
- **Establish clear reporting channels:** Encourage employees to report suspicious activities through confidential channels.
- **Secure post-employment access:** Ensure that access rights are revoked and monitored when employees leave the organisation.

As well as these preventative techniques, organisations should consider what to do in the event of a disruptive attack, or fraud from a malicious insider. Importantly, this should include a well-drilled incident response plan and associated playbooks which consider both criminal and civil actions against the perpetrators, and potential public communications strategies.

[4] Racist Network Rail Wi-Fi hack was work of malicious insider, https://www.computerweekly.com/news/366612056/Racist-Network-Rail-Wi-Fi-hack-work-of-malicious-insider

[5] Cybercriminals Hack UK Rail Network Wi-Fi https://www.infosecurity-magazine.com/news/cybercriminals-hack-uk-rail-wifi/

Appendix

See table below for a list of IOCs for threat hunting for the FIN7 threats.

IOC Type	Detail
NetSupport RAT MD5	ff25441b7631d64afefdb818cfcceec7
C2 Infrastructure IP	166.88.159[.]37
Malware Used	Redline Stealer (AI deepfake honeypots)
Malware Used	D3F@ck Loader (AI deepfake honeypots)
Malicious Domain	aiNude[.]ai
Malicious Domain	easynude[.]website
Malicious Domain	ai-nude[.]cloud
Malicious Domain	ai-nude[.]click
Malicious Domain	ai-nude[.]pro
Malicious Domain	nude-ai[.]pro
Malicious Domain	ai-nude[.]adult
Malicious Domain	ainude[.]site
C2 IP (Steam Profile)	78.47.105[.]28
C2 IP (Steam Profile)	159.69.26[.]61
C2 IP (Steam Profile)	116.203.15[.]73
C2 IP (Steam Profile)	116.203.8[.]165
C2 IP (Steam Profile)	116.202.0[.]236
C2 IP (Steam Profile)	116.202.5[.]195
C2 IP (Steam Profile)	78.47.105[.]28
C2 IP (Steam Profile)	78.46.129[.]163
C2 IP (Steam Profile)	88.198.89[.]4
C2 IP (Steam Profile)	5.75.232[.]183
Malware C2 Domain	pang-scrooge-carnage[.]shop
Malware C2 Domain	thesiszppdsmi[.]shop

Figure 3 - IOCs for FIN7 campaign (source: Silent Push)

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

mishcon.com/cyber-risk-and-complex-investigations

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.

This document has been prepared for general guidance only and does not constitute professional or legal advice. If you wish to receive legal advice, we will need to provide you with a separate retainer letter and additional terms of business, as such work will be separately regulated by the Solicitors Regulation Authority (SRA).

You should not act upon the information contained in this publication without obtaining specific professional or legal advice.

Mishcon de Reya refers to Mishcon de Reya LLP, which is a limited liability partnership, incorporated in England (number OC399969), whose registered office is at Africa House, 70 Kingsway, London WC2B 6AH. It is a body corporate which has members rather than Partners.