Guidelines and Recommendations on Spear Phishing

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

ISSN: 1862-6947
https://eucrim.eu

On 4 November 2019, Europol's European Cybercrime Centre (EC3) published a report on how to prevent, respond to, and investigate spear phishing attacks.

Spear phishing describes the practice of targeting specific individuals within an organisation or business for the purposes of distributing malware or extracting sensitive information.

The report gives an overview of the threat of spear phishing from the perspective of law enforcement and industry. It explains the background of the concept of spear phishing, outlines the most common *modi operandi*, and offers guidance and recommendations on technical solutions, prevention, and awareness as well as on attribution and operational response.

According to the report, email is the most widely used vector for spear phishing. The most commonly used modus operandi is reconnaissance, i.e., deceiving the target. In order to achieve this aim, phishing emails try to include as much content that is familiar to the recipient as possible. Information used to create this familiar content is usually simply found online.

When attacking, a fraudulent link is often sent, leading to a replica of a trusted website (phishing site). Attackers also attempt to make the target download and open a malicious file in order to gain access to the system. Business Email Compromise (BEC) is often aimed at convincing employees to transfer large sums of money to the criminal's bank account.

Depending on the goal of the attacker, the target's files may be encrypted and a ransom payment (ransomware) demanded, remote control may take over the target's system (Remote Access Trojan), relevant credentials may be stolen (key loggers), or the network may be monitored and files extracted.

In order to respond to phishing, the report recommends two sorts of technical solutions, namely policies and software. By means of security policies, users can be prevented from engaging in risky behaviour. Commercial and open source software solutions can help mitigate the threat of phishing and automatically detect phishing attempts. Furthermore, the report recommends investing in prevention and awareness raising measures to establish a resilient user base, e.g., by offering anti-phishing training to employees.

When launching an investigation, law enforcement should have in place procedures and methods for handling this type of incident, e.g., reporting tools between the private sector and law enforcement and other public-private partnerships.

In order to reduce abuse of the Domain Name System (DNS), the report recommends that registrars and registries adopt aggressive anti-abuse measures. Ultimately, the report regrets the loss of the WHOIS data. The

WHOIS database contained personal information on registrants of domain names. Law enforcement have no longer direct access due to the new GDPR rules.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union