iZOOlogic

iZOOlogic Limited
Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com

Case Study: Leaked Account Credentials - Global Payment Platform

Introduction

This case study details a phishing incident targeting an Global Payment Platform that resulted in compromised data being available and distributed on an internet forum.

Overview

Phishing is the main method that attackers use to acquire account credentials throughout the cybercrime ecosystem, though the value of such an attack is within the distribution of this stolen information. Information and data acquired through nefarious means is readily shared on the dark web.

Many other platforms can also host such content, such as paste sites, social platforms, internet forums, blogs and messaging Apps such as Telegram Groups. In this instance, the phishing attack resulted in confidential information released on an internet forum, where freedom of speech and sharing of information is less monitored than that of more prominent sites like social media and news platforms.

Internet Forums

There are several internet forums that host content which are not for your average internet visitor, and some of these forums allow sharing of content and media that may or may not be safe for everyday viewing. Hence, attackers have been exploiting this loophole and have since used this platform to sell illegally acquired information.

Private and Sensitive Data

Private and sensitive data can be obtained from many sources, such as phishing, malware, data leaks, hacking or may even by distributed outside the organization through a genuine mistake.

Many parties can be the source of an information leak including employees, clients, partners, contractors and other agencies.

Often such information has an intrinsic value, so the sharing, sale, distribution of the data will be beneficial to the criminal holder.

The distribution of private and sensitive data can be from point to point, however, we readily observe cases where private or confidential data is hosted in a deliberate manner to allow the criminal to profit in a anonymous manner.

Online Merchant Sensitive Data Acquisition

A prominent online payment platform suffered a major phishing incident that resulted in the compromise of client data.

The compromised credentials were subsequently posted on an internet forum in the form of a text file. The forum administrators were unaware of the contents of the file, since they have non-disclosure agreements in which they cannot tamper with the media shared on their forum, unless its posted in raw text and visible to the public.

iZOOlogic was able to detect this hosting site through forensic analysis of the phishing attack, and quickly removed the file.

Challenges

Some of the issues and challenges we encountered during this incident targeting the payment provider:

- This file was not indexed or readily accessible.
- Through a forensic investigation of the original phishing attack, we are able to decipher the criminal intentions of distributing the compromised data with other threat actors.
- Several other users may have been affected, and their information is still at large, perhaps available on other repositories.
- Forums are always moderated and often under strict supervision regarding their compliance of their terms and conditions of use, some may have non-disclosure policies any so may not readily cooperative with third parties without some court or law enforcement assistance.
- Variations in medium of information sharing, and multiple cases with the same information, or multiple information in one share, due to the sensitivity of handling data.
- We had to prove the fraudulent case with the forums administrators and leverage the hosting provider to resolve the incident.

Conclusion

The hosting and distribution of compromised data and information is the cornerstone of the cybercriminal network. Cybercriminals can generally only profit from their operations by on-selling their good to other parties.

Obviously the dark web has opened a great channel for the criminals to facilitate their action in providing data and information.

However, there are many parts of the open and surface web where similar activities occur, often providing an easier route to market, and just as secure.

We often see paste sites and internet forums as a way of criminals to spread and disseminate their wares.

iZOOlogic has robust surveillance techniques to monitor known, and unknown, repositories of such data and information.

In additional, as in this case, it is critical to fully evaluate each incident to glean any available forensic information, to allow a comprehensive picture of the full attack cycle. The full investigation of the phishing attack gave evidence of other elements of the threat— such as the hosting of data on internet forums.

The recovery of the compromised data returned back to the client proved valuable in identifying victims and account mitigation.

iZOOlogic protects the world's leading organisations, across Banking, Finance, and Government.

The iZOOlogic platform provides real time Threat Intelligence and a seamless Global Security Response.

iZOOlogic helps organisation's manage Digital and Reputational Risks, and to reduce fraud and revenue losses.

To learn more, visit www.izoologic.com or ***Contact Us***

HQ / EMEA OFFICE

Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com

US OFFICE

Level 1, 444 Castro Street
Mountain View, California,
USA
+1 650 396 3352
sales@izoologic.com
www.izoologic.com

APAC OFFICE

Suite 18, Level 27, Rialto Tower
Collins Street, Melbourne, 3000,
AUSTRALIA
+61 3 9088 0338
sales@izoologic.com
www.izoologic.com

iZOOlabs / GSOC

Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com