SUCCESS STORY

FLARE

How Flare Helped a Top North American Investment Firm Prevent a Portfolio Company Breach

The Customer

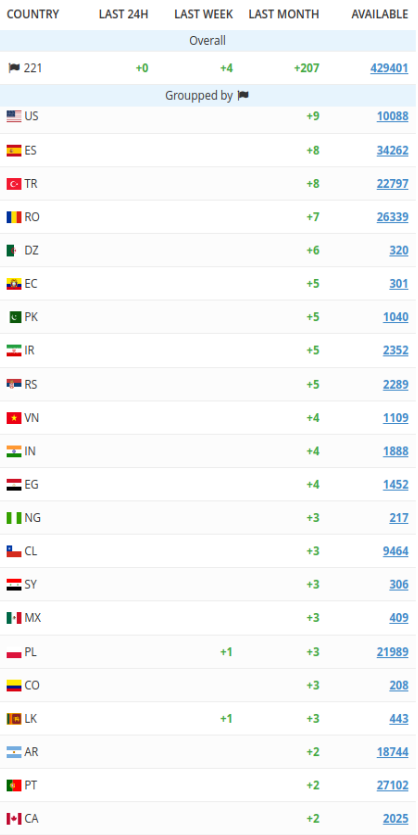
Financial Services

$10 Billion in Assets

North America

Overview

The exploitation of any attack vector can cause a company to suffer from a large data breach. In this success story, we discuss how Flare helped our client manage this digital risk by discovering and alerting the organization of a bot for sale on the Genesis platform. This bot[1] contained cookies for a webmail server located inside the company's internal network.



COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
221	+0	+4	+207	429401
Groupped by				
US			+9	10088
ES			+8	34262
TR			+8	22797
RO			+7	26339
DZ			+6	320
EC			+5	301
PK			+5	1040
IR			+5	2352
RS			+5	2289
VN			+4	1109
IN			+4	1888
EG			+4	1452
NG			+3	217
CL			+3	9464
SY			+3	306
MX			+3	409
PL		+1	+3	21989
CO			+3	208
LK		+1	+3	443
AR			+2	18744
PT			+2	27102
CA			+2	2025

Total Bots For Sale Per Country - Feb 2022

Using a DRP platform like Flare can help organizations not only monitor these external risks, but can also assist in accelerating remediation and improving your cybersecurity team's cost-effectiveness and efficiency.

[1] A device infected as part of a botnet operation, for which the cookies and credentials are put on sale on the dark web.

The Challenge

A Single Cookie or Email Login Can Cause a Massive Data Breach

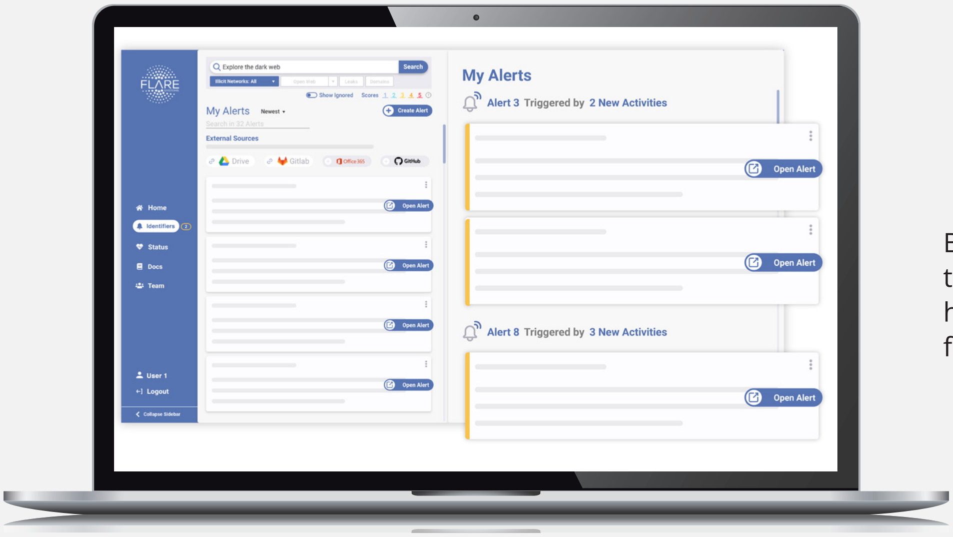
In September 2021 news broke out that Electronic Arts suffered a data breach. No user data was reportedly stolen but more than 750 GB of data was, including video game source code. It was reported that initial access was obtained through the Genesis market, a website selling infected computers, offering buyers a set of credentials and cookies belonging to the infected computer owner. Initial access was achieved through the company's Slack workspace, an internal messaging system, using a cookie giving access without additional authentication. From there, attackers used social engineering techniques to elevate their level of access all the way to source code.

Flare published an intelligence report and started monitoring this market back in February 2020 as we noticed an uptick in traffic and number of listings for sale. Today, more than 400,000 bots coming from more than 200 countries are listed on Genesis Market, while more than 800 new listings are added every day. This research is part of Flare's commitment to stay at the forefront of cyber threats and methods gaining popularity among cyber criminals and adding those data sources to our continuous monitoring.

The fact that a single string of text, a cookie, can lead to millions of dollars in costs and potential ransomware attacks is no news to anyone in the cybersecurity space. The pace at which things are moving, however, is impossible to keep up for most resource-strapped security teams. Enter Flare.

Product Highlights

Find and remediate potential data breaches proactively



Bringing context to an alert that helps remediate faster.

Higher-risk alerts are managed quickly thanks to the unique Flare scoring system.

Impacts and Benefits

Data Breach Prevention

A large investment firm in North America prevented a potentially catastrophic network intrusion for one of its portfolio companies. Using the Flare platform for a red-team mandate, alerts were raised about a bot for sale on the Genesis platform containing cookies for a webmail server located inside the company internal network among other banking and payment application credentials.

Due to the very specific subdomain shown in the Genesis listing (webmail.companyname.com), the red teamer had a high level of confidence that the infected computer belonged to an employee. Following the green light from the portfolio company, access to the credential for sale was obtained. From there, the red teamer was able to access the corporate mailbox of the employee, including a huge amount of attachments, personal information, and other documents that could easily be leveraged by a malicious actor. Both the investment firm and their portfolio company agreed that this infected computer access, sold on Genesis market for about USD$100 could have had disastrous consequences for the firm.

The Electronics Arts incident reinforces the fact that this level of basic access (employee Slack or email) is more than enough to leverage into elevated access that can result in data breaches that could have serious consequences.

Prioritized Digital Risk Detection

Flare Systems gives back bandwidth to security teams and service firms in two ways. First, our research team makes sure we stay up to date with trends, methods, and tools malicious actors use. Second, we add these tools and intel sources to our Flare monitoring and alerting platform. We enrich the collected data with our industry-leading prioritization scoring in order to reduce noise and alert our customers instantly when data found publicly on the internet could be leveraged by malicious actors.